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 概要 13

Prisma Accessを使った安全なインターネット トラフィック 17

インターネットセキュリティの重要性 17

Prisma Accessクラウドセキュア Webゲートウェイ (SWG) 17

Prisma Accessを使用してユーザーとエンドポイントを保護する 18

Prisma Accessの管理方法 19

Prisma AccessStrata Cloud Managerによる可視性と監視 23

Prisma Accessロケーション 25

ロケーション、都市、国を計算する 26

シアターとロケーショングループ 32

地域別ロケーション 36

明示型プロキシのロケーション 41

Colo-Connectの場所 42

サポートされているStrata Logging Serviceリージョン 43

リモートネットワーク - 高パフォーマンス、トラフィックレプリケーション、および安全なインバウンド アクセス ロケーション 44

Prisma Access中国のロケーション 47

FedRAMP中程度および高い場所 47

北米地域の地図 47

ローカルゾーンのロケーション 48

Prisma Accessおよび関連サービスの処理場所 49

Prisma Access インフラストラクチャ管理 51

Prisma AccessAPI 53

Prisma Access (Managed by Strata Cloud Manager)向けAPI 53

Prisma Access (Managed by Panorama)向けAPI 53

WebブラウザとWebインターフェースを使ったPrisma Access (Managed by Panorama)APIへのアクセス 54

curlコマンドを使用してPanoramaマネージドAPIコマンドを取得する 56

Prisma Access (Managed by Panorama)でCLIコマンドを使用する 57

Prisma AccessインサイトAPI 57

Prisma AccessをPanoramaからStrata Cloud Managerへ移行する 59

Prisma Access (Managed by Strata Cloud Manager)への移行の準備 59

Prisma Access (Managed by Panorama)デプロイメントをStrata Cloud Managerに移行する 60

Prisma Accessリリースとアップグレード 73

Prisma Access リリースタイプ 74

©2025 Palo Alto Networks, Inc.

緊急スケジュールアップグレード 75
Prisma Accessアップグレードタイプ 76
Prisma Accessのソフトウェアおよびコンテンツアップデートの頻度 79
Prisma Accessデータプレーンのアップグレード 86
アップグレードアラートと更新情報を受け取る 92
Prisma Access ソフトウェアバージョンを表示する 97
Prisma Access (Managed by Strata Cloud Manager) 97
Prisma Access (Managed by Panorama) 98
Prisma Accessセットアップ 103
Prisma Accessのセットアップ 105
Prisma Accessサービスインフラの設定 113
モバイルユーザー:IPアドレス割り当て 128
例:パブリックIPアドレスのスケーリングの例 (モバイル ユーザー) 129
ループバックIPアドレスの割り当て (モバイル ユーザー) 131
リモートネットワーク:IPSec終端ノードと サービスIPアドレス 134
リモートネットワーク:帯域幅割り当てに関連するIPアドレスの変更 135
リモートネットワーク:サービスIPアドレス と出力IPアドレスの割り当て 138
Prisma AccessのIPアドレスを取得する 139
モバイルユーザー向けのIP最適化：GlobalProtectとのデプロイメント 166
Prisma AccessIPアドレスを取得するためのAPI例 168
Prisma AccessIPアドレスが変更されたら通知を受け取る 171
レガシースクリプトを使用してIPアドレスを取得する 173
モバイルユーザーのIPアドレスを取得する 175
パブリック、ループバック、出口IPアドレスの取得 176
Prisma Access ゾーン 179
Prisma Access向けDNS 181
Prisma Accessの高可用性 (HA) 187
事前定義済みテンプレート:サービス接続またはリモートネットワークのオンボード 190
共通のSD-WANデバイスに対してサポートされているIKEおよびIPSec暗号プロファイル 195
Prisma Accessサービス接続 197
サービス接続を計画します 199
本社またはデータセンター情報を収集する 199
Prisma Accessでサービス接続を設定する 201
サービス接続を使用してモバイル ユーザーとリモート ネットワーク間のアクセスを有効にする 231
サービス接続のダイナミック ルーティングに関する考慮事項 233

©2025 Palo Alto Networks, Inc.

仕組み - サービス接続トラフィックのルーティング 233
Prisma Access デフォルトルーティング 234
ホットポテトルーティング 238

Prisma Access ZTNAコネクタ 243

ZTNA コネクタ コンポーネント 244
ZTNAコネクタの使用例 245
サービス接続と ZTNA コネクタでサポートされているユースケース 249
ZTNA コネクタ 2.0 の原則 250
ZTNA コネクタの要件とガイドライン 251
サポートされているPrisma Accessバージョンと要件 251
アプリサポート 252
機能の制限 252
スケールとスループットの考慮 253
サポートされているアプリケーションホスティング環境 254
ネットワーク要件 255
ZTNA コネクタで許可する IPアドレスと FQDN 257
証明書の管理 260
ZTNA コネクタを有効にする 262
ZTNAコネクタの設定 269
ZTNAコネクタのアップグレード 280
ZTNAコネクタ診断ツール 283
コネクタIPブロックの削除 291
Cloud Identity Engineを使用してアプリケーションの自動検出を設定する 296
プライベート アプリケーション ターゲットの検出 297
ZTNAコネクタ対応アプリのセキュリティ ポリシー 304
データセンターにZTNAコネクタVMを導入する 322
サポートされているZTNAコネクタのデプロイメント 322
ZTNAコネクタがサポートするMicrosoft Azureのデプロイメント 326
ZTNAコネクタでサポートされるGoogle Cloud Platformのデプロイメント 342
ZTNAコネクタでサポートされるAmazon Web Servicesデプロイメント 352
Prisma Access ZTNAコネクタがサポートするVMware ESXiのデプロイメント 359
Prisma Access ZTNAコネクタがサポートするKVMデプロイメント 370
Prisma AccessZTNAコネクタがサポートするHyper-Vのデプロイメント 375
ZTNAコネクタを監視する 389
ZTNAコネクタのログの表示 392

©2025 Palo Alto Networks, Inc.

送信元NATを使用した ZTNA コネクタ接続のユーザー ID マッピングを保持する 395

動的権限アクセス設定を構成する 405

動的特権アクセスとは何ですか? 406
AAからBBまでのダイナミック特権アクセスを有効にする 408
動的権限アクセスのためにCloud Identity Engineでユーザー グループ マッピングを承認する 410
Access Agentを有効にします。 418
動的権限アクセスのためのエージェント インフラストラクチャの設定 420
インフラストラクチャ設定を構成する 420
Prisma Accessロケーションの選択 422
動的な権限アクセスのSC-NATサポートを有効にする 426
動的権限アクセスのルート集約を有効にする 427
スニペットを作成する 430
プロジェクト固有のPrisma Access Agent設定を設定する 441
動的権限アクセスエージェントのエージェントトラフィックを管理するための転送プロファイルを設定する 441
動的特権アクセスのためのPrisma Access Agentアプリケーション設定 456
動的特権アクセスのためのDNS設定 462
動的権限アクセスのためのHIPデータ収集設定を構成する 464
プロジェクトを作成する 469
動的権限アクセスのためのトラフィックステアリング 472
動的な特権アクセスのためのPrisma Access Agentのセットアップ 474
Prisma Access Agentの段階的なロールアウトを設定する 474
Prisma Access Agents向けの一般的なグローバル設定を構成する 484
動的権限アクセスのHIP通知を構成する Prisma Access Agent 488
Prisma Access Agent設定をプッシュします。 497
動的特権アクセス有効化Prisma Access Agentパッケージをダウンロードする 500
Prisma Access Agentを使用してプロジェクトにアクセスする 502
Prisma Access Agentをインストールします 502
ダイナミック特権アクセス有効化Prisma Access Agentにログインする。 511
動的権限アクセスの設定を変更して有効にする Prisma Access Agent 515
ダイナミック特権アクセス有効Prisma Access Agentを別の場所に接続する 517
別のプロジェクトへの切り替える 518
ダイナミック特権アクセス有効Prisma Access Agentを別のサーバーに接続する 520
Prisma Access AgentとGlobalProtectアプリケーションの切り替え 522

 ©2025 Palo Alto Networks, Inc.

動的特権アクセス ユーザーの表示と監視 529
接続ユーザー 529
動的権限アクセス プロジェクトの表示と監視 535
プロジェクト 535
Prisma Access Colo-Connect 539
Colo-Connectの使用例 541
プライベートアプリへの高帯域幅アクセス 541
プライベートアプリケーション向けのプライベート接続 541
サードパーティのNaaSプロバイダーの使用 541
Colo-ConnectはService ConnectionsやZTNA Connectorと何が違いますか? 543
Colo-Connectのサポートされていない機能 544
Prisma Access Colo-Connectの要件と前提条件 545
Prisma Access Colo-Connect を設定する 547
Prisma Accessでのアプリの高速化 601
アプリの高速化の要件とガイドライン 603
App Accelerationを設定する 606
Prisma Access モバイルユーザー 629
モバイルユーザー:グローバルプロテクト 631
Prisma AccessのGlobalProtectの計画チェックリスト 632
GlobalProtect モバイルユーザーの設定 635
GlobalProtect – トンネル設定のカスタマイズ 669
GlobalProtect – アプリ設定をカスタマイズ 674
GlobalProtectを無効にするチケットリクエスト 685
GlobalProtectプレ ログオン 690
GlobalProtect – クライアントレス VPN 705
GlobalProtectモバイルユーザーを監視する 707
GlobalProtectモバイル ユーザーデプロイメントのIPアドレス プール 713
GlobalProtectアプリケーションがモバイルユーザーのためにPrisma Accessロケーションを選択する方法 719
GlobalProtectモバイルユーザーのリスト表示を許可する 721
GlobalProtectアプリケーションのアップグレード 732
Prisma Accessをオンプレミスの GlobalProtectゲートウェイと統合する 741
モバイルユーザー:明示型プロキシ 758
明示型プロキシの設定ガイドライン 761
プロキシモードでのGlobalProtect 765
トンネルおよびプロキシモードのGlobalProtect 780

©2025 Palo Alto Networks, Inc.

エージェント ベースのプロキシ トラフィックに対するプライベートIPアドレスの可視化と適用 804
明示型プロキシのSAML認証 806
明示型プロキシのセットアップ 809
明示型プロキシデプロイメント用のKerberos認証 833
Cloud Identity Engine 明示型プロキシ(Explicit Proxy)デプロイメントの認証 868
リモートネットワークのプロキシモード 874
明示型プロキシがユーザーを識別する方法 885
明示型プロキシ転送プロファイル 886
PACファイルガイドライン 895
明示型プロキシのベストプラクティス 902
明示型プロキシの監視とトラブルシューティング 903
明示的プロキシのブロック設定 906
特別なオブジェクトを使用して、明示型プロキシインターネットトラフィックを特定のIPアドレスに制限する 909
明示的なプロキシを使用してデータセンターにアクセスする 910
明示型プロキシを使用したアプリケーションベースのOffice 365統合 917
Blue Coat Proxyでプロキシ チェーンを構成する 921
GlobalProtect(またはサードパーティのVPN)で明示型プロキシを使用する 926
明示型プロキシ ユーザーのためのIPアドレス最適化 -プロキシ デプロイメント 939
モバイル ユーザー向けのDNS解決 - 明示型プロキシのデプロイメント 940
ユーザーと IP アドレスまたはユーザー グループのマッピングを表示する 943
モバイルユーザーのサイトアクセスの問題を報告する 948
モバイルユーザーがPrisma Accessに認証できるようにする 950
認証サポートと機能 952
認証のセットアップ 956
モバイルユーザーが企業リソースにアクセスできるようにする 962

Prisma Accessリモートネットワーク 967

リモート ネットワークの計画チェックリスト 968
リモートネットワーク帯域幅の割り当て 973
新しいモデルへの移行を計画する 989
移行された集約帯域幅デプロイメントの帯域幅割り当て 992
QoS移行ガイドライン 994
帯域幅管理設定を移行する 999
リモートネットワークのオンボーディング 1006
リモート ネットワーク サイトをPrisma Accessに接続する 1036

©2025 Palo Alto Networks, Inc.

プライマリおよびセカンダリ IPSec VPN トンネルの追加 1036
その他のIKEオプション 1037
その他のIPSecオプション 1039
リモートネットワークのルーティングを有効にする 1040
サイト接続のトラブルシューティング 1043
複数のリモートネットワークを搭載 1045
リモート ネットワーク テーブルのフィールド 1047
リモートネットワークがPrisma Accessに接続されているかどうかを確認する 1058
リモート接続BGPステータスの検証 1061
WAN リンクで接続されたリモート ネットワークとサービス接続を設定する 1063
リモートネットワークのQoS 1066
保証帯域幅を変更する 1085
リモート ネットワーク–ハイ パフォーマンス 1088
リモート ネットワーク - 高性能機能とガイドライン 1088
ターミナルサーバーを使用した共有デスクトップVDIとPrisma Accessの統合 1110

Prisma Access監視と可視性 1119

Prisma Accessログ 1121
外部ログおよびその他のデータ 1122
Prisma Access アクティビティダッシュボードとレポート 1123
Strata Cloud ManagerでのPrisma Accessの表示と監視 1125
Strata Cloud ManagerでPrisma Access Monitoringを開始する 1126
アプリケーションの表示と監視 1129
アプリの高速化の表示と監視 1132
モバイル ユーザーを表示する 1134
モバイル ユーザー向けのIPv6の表示と監視 1134
ブランチサイトの表示と監視 1136
データセンターの表示と監視 1145
ネットワーク サービスの表示と監視 1166
サブスクリプションの使用状況を表示 1171
Prisma Accessのロケーションを表示および監視する 1173
サードパーティデバイスIDの表示と監視 1175
リモートブラウザ分離の表示と監視 1177
Prisma Accessと自律型DEM 1179

Prisma Access ユーザーベースのポリシー 1181

Prisma Accessのユーザー ベース ポリシーを設定します 1182
Cloud Identity EngineとPrisma Accessを統合する 1185
Prisma Accessのユーザー–IDグループ マッピングの取得 1192

 ©2025 Palo Alto Networks, Inc.

アイデンティティ情報再配信....1202
Prisma Accessでサードパーティ デバイスIDを設定する.... 1218
サードパーティのデバイス ID API.... 1225
判決の更新.... 1225
すべての判定を削除する....1228
クエリ評決....1229
IPアドレスによるクエリ判定.... 1231
クエリ判定統計.... 1232
Prisma Accessマルチテナント.... 1235
マルチテナント設定の概要....1236
マルチテナントデプロイの計画.... 1241
まったく新しいマルチテナントのデプロイメントを作成する.... 1244
マルチテナントの有効化と最初のテナントの移行.... 1245
テナントをPrisma Accessに追加する....1252
テナントの削除.... 1258
テナントレベルの管理ユーザーの作成....1264
テナントレベルの管理ユーザーに対するロールベースアクセスの制御.... 1268
テナントレベル管理ユーザーのプラグインアクセスの削除....1269
マルチテナント デプロイメントでのデバイス グループIDによるログのソート.... 1274
FedRAMP環境でのPrisma Access.... 1277
Prisma Access FedRAMP要件.... 1278
事前インストールおよび製品アクティベーションの要件.... 1278
必要なPanorama、プラグイン、PAN-OS データプレーンのバージョン..1279
Prisma AccessがサポートするFedRAMPロケーション....1281
Prisma Access FedRAMPデプロイメントにおけるサポートされる機能とサポートされない機能....1281
FedRAMP環境でPrisma Accessを設定する.... 1283
Prisma Access高度なデプロイメント.... 1291
デプロイされたPrisma Accessロケーションに新しいコンピュート ロケーションを追加する。....1293
IPv6 サポート....1295
ネイティブIPv6サポートの概要....1298
Prisma Accessインフラストラクチャにおける IPv6 ネットワーキングと IP プールの有効化と設定....1301
モバイルユーザー向けIPv6ネットワークの有効化 - GlobalProtectのデプロイメント.... 1310
サービス接続のためのIPv6ネットワーキングを有効にする.... 1315

 ©2025 Palo Alto Networks, Inc.

リモートネットワークのIPv6ネットワーキングの有効化 1322
モバイルユーザーのためのDNS解決–GlobalProtectとリモートネットワークデプロイメント 1332
モバイルユーザー向けのDNS解決 – GlobalProtectデプロイメント 1334
リモートネットワークのDNS解決 1336
サービス接続およびリモートネットワーク接続用にBGPがモバイルユーザーIPアドレスプールをアドバタイズする仕組み 1338
Prisma AccessとStrata Logging Serviceのプロキシサポート 1340
特定の国からの着信接続をブロックする 1341
AWS WorkSpaceからの安全なインターネットトラフィック 1342
AWS WorkSpaceクライアントでPACファイルを設定する 1342
AWSとPrisma Access間のサイト間トンネルの設定 1344
デフォルトルートなしネットワークのPrisma Access 1345
デフォルトルートなしネットワークとは？ 1345
デフォルトルートネットワークに関する考慮事項なし 1345
デフォルトルートがないネットワークのインターネットアクセスを保護するためのデプロイメント上の推奨事項 1346
主な考慮事項 1346
Prisma Accessサービス接続の高度なデプロイメント: 1347
サービス接続マルチクラウド冗長性 1347
トラフィックステアリングを使用したインターネット宛てのトラフィックのサービス接続への転送 1358
サービス接続トラフィックのルーティング 1384
複数のサービス接続を使用して高帯域幅ネットワークを作成する 1397
送信元NATを使用したサービス接続のユーザーIDとデバイスIDのマッピングを保持する 1411
Prisma Accessモバイルユーザー - GlobalProtect 高度なデプロイメント 1420
Prisma Accessで複数のポータルを構成する 1420
リモートトラブルシューティングとアップデートのためのダイナミックDNS登録サポート 1431
モバイルユーザー向けの動的DNS登録サポート - GlobalProtect 1446
Prisma Access GlobalProtectのデプロイメントにおける侵害されたデバイスの識別と隔離 1453
モバイル ユーザーのIPv6トラフィックのシンクホール - GlobalProtectのデプロイメント 1462
Prisma Accessを使用したHIP情報の再配信 1468
HIPレポートの表示 1478
クライアントレスVPNでのGzipエンコーディングのサポート 1480
Prisma Accessでのトラフィック レプリケーション 1482
Prisma Accessリモートネットワークの高度なデプロイメント: 1496

 ©2025 Palo Alto Networks, Inc.

Prisma Access 内部ゲートウェイ 1496
リモートネットワークのロケーションへの安全なインバウンドアクセスの提供 1506

Clean Pipe向けPrisma Access 1535

Clean Pipe向けPrisma Accessの概要 1536
Clean Pipeの使用事例 1536
Clean Pipeの例 1537
Clean PipeおよびPartner Interconnectの要件 1538
Clean Pipe設定の完了 1540
マルチテナント機能の有効化とテナントの作成 1545

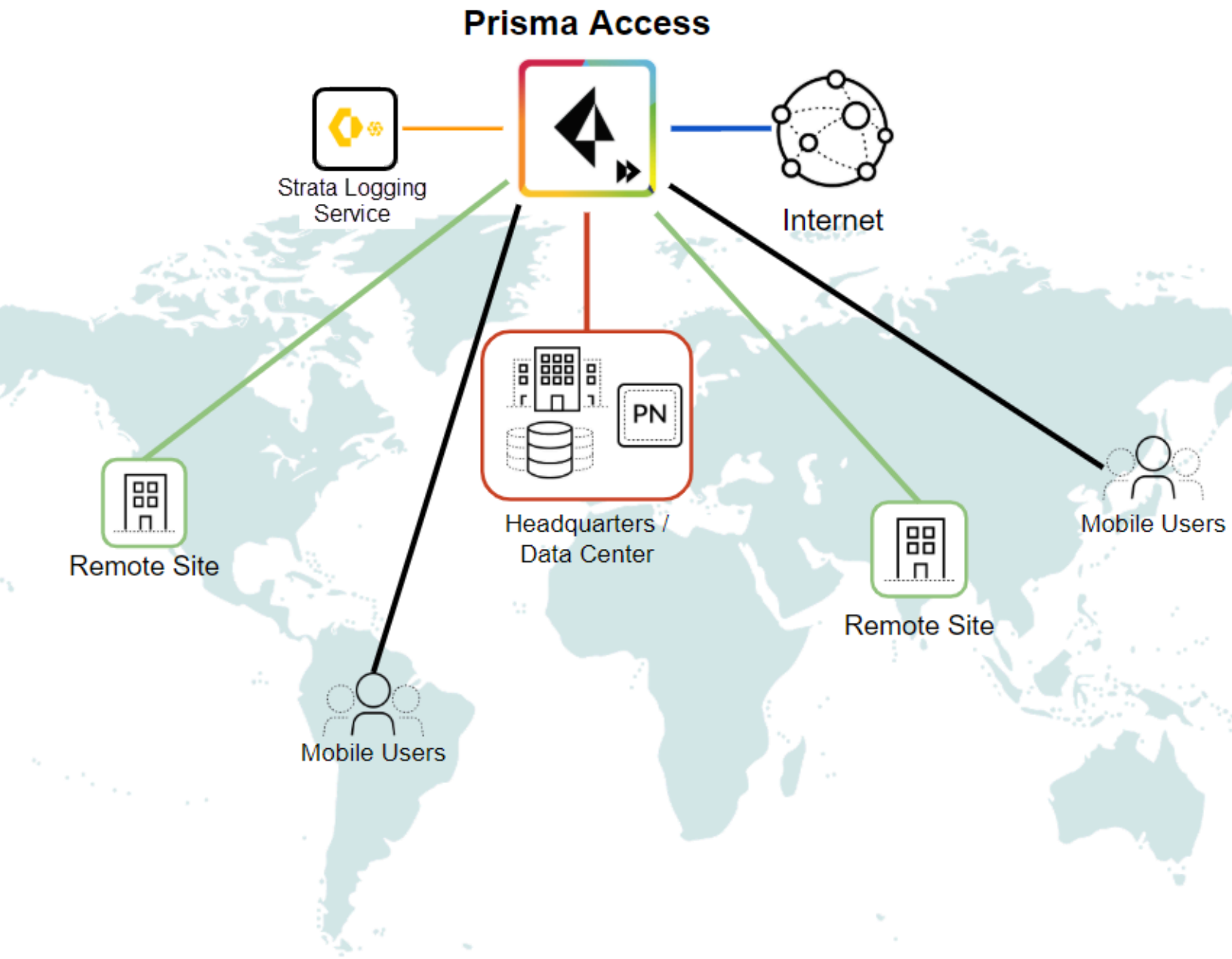
©2025 Palo Alto Networks, Inc.

Prisma Access 概要

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス

アプリケーションとデータを安全に保つには、常にあらゆる場所のすべてのユーザーを保護する必要があります。しかし、事業範囲が世界的に拡大し、モバイル ユーザーが増え、アプリケーションとデータがネットワークからクラウドに移行している場合、これをどのように実行すればよいのでしょうか。 Prisma Accessはユーザーが本社、支社、外出先などどこにいても、クラウドやデータセンターのアプリケーション、インターネットに安全にアクセスできるようにすることで、この一貫したセキュリティを実現します。 Prisma Accessはすべてのポートのすべてのトラフィックを一貫して検査し、インターネットだけでなく、承認されたSaaSアプリケーション、パブリック クラウド環境、データ センター、本社への安全なアクセスを可能にします。脅威防御、マルウェア防止、URL フィルタリング、SSL復号化、アプリケーション ベースのポリシー機能が組み込まれているため、ユーザーの場所やアクセスするリソースに関係なく、同じレベルのセキュリティが提供されます。Strata Logging Serviceに保管されたすべてのPrisma Accessログは、すべてのユーザー、アプリケーション、場所にわたって集中的な分析、レポート、フォレンジックを提供します。

Prisma Accessはグローバルなカバレッジで大規模な保護を提供するため、ブランチでのハードウェア ファイアウォールのサイズ設定や導入、コロケーション施設でのアプライアンスの構築や管理などを心配する必要がありません。 Prisma Accessは、 独自のグローバル セキュリティ インフラストラクチャを構築したり、運用能力を拡張したりすることなく、すべてのリモート ブランチ、本社サイト、データセンター、モバイル ユーザーを接続するネットワーク インフラストラクチャを提供します。



Prisma AccessのPalo Alto Networksは、リモート ネットワークとモバイル ユーザーを保護するために、セキュリティ インフラストラクチャをグローバルにデプロイおよび管理します。Prisma Accessは、モバイル ユーザー セキュリティ処理ノード (MU-SPN) とリモート ネットワーク セキュリティ処理ノード (RN-SPN) 間、SPNとサービス接続企業アクセス ノード (SC-CAN) 間、およびSC-CANとデータセンター間でデータをエンドツーエンドで暗号化します。

- サービスインフラ—Prisma Accessは、内部サービスインフラを使用して、組織のネットワークを保護します。インフラのサブネットを指定すると、Prisma Accessはそのサブネット内のIPアドレスを使用して、リモートネットワークロケーションとモバイルユーザー間のネットワークインフラ、および内部ネットワークリソースへのサービス接続（該当する場合）を確立します。クラウド内の内部通信は、ダイナミックルーティングを使って確立されます。

 ©2025 Palo Alto Networks, Inc.

- サービス接続—Prisma Accessライセンスに含まれている場合は、IPsec トンネルを確立して、ネットワーク内の内部リソースと、リモートネットワークロケーションのモバイルユーザーおよびユーザー間の通信を可能にすることができます。たとえば、組織の本社またはデータセンター内の認証サーバーへのサービス接続を作成することができます。

  本社やデータセンターにサービス接続が必要ない場合でも、モバイルユーザーとリモートネットワークロケーションの間、および地理的に異なる場所にいるモバイルユーザー間のネットワーク通信を可能にするサービス接続を作成することをお勧めします。

- モバイル ユーザー- データ センターのアプリケーションにアクセスする場合、SaaSアプリケーションを使用する場合、またはインターネットを閲覧する場合であっても、モバイル ユーザーに一貫したセキュリティを提供します。モバイル ユーザーがPrisma Accessに接続できるようにすることができます：

  - グローバルプロテクト

    GlobalProtectアプリケーションをユーザーにデプロイし（Microsoft Windows、Apple macOSおよびiOS、Android、Google Chrome OS、Linuxを実行するスマートフォン、タブレット、またはラップトップで利用可能）、トラフィックをPrisma Accessにトンネリングしてポリシーの実施と脅威防御を行うことができます。GlobalProtectアプリケーションは、ホスト情報プロファイル（HIP）レポートも提供しており、デバイスの状態に基づいて詳細なポリシーを作成し、エンドポイントがあなたのセキュリティ基準に準拠していることを確認できます。たとえば、最も最新のパッチ、暗号化、およびウイルス定義が装備されていることを確認し、最も機密性の高いアプリケーションにアクセスできるようにします。また、管理されていないデバイスのユーザーにも安全なアクセスを可能にするには、クライアントレス**VPN**を有効にします。 Prisma Accessは、ユーザーが現在どこにいるかに基づいて、地域ごとに動的にスケールイン/スケールアウトします。

  - 明示型プロキシ

    既存のネットワークですでに明示的なプロキシを使用し、クライアント エンドポイントにPACファイルをデプロイしている場合、Prisma Accessにスムーズに移行し、モバイル・ユーザーのアウトバウンドインターネット トラフィックを保護することができます。

- リモートネットワーク–クラウドベースの次世代型ファイアウォールで、支店やその支店内のユーザーなどの、リモートネットワークロケーションを保護するには、リモートネットワークを使用します。スタティックルート、BGPを使ったダイナミックルーティング、または両方のルートの組み合わせを使って、各リモートネットワークロケーションのサブネットワークへのアクセスを有効にすることができます。オンボーディングしたすべてのリモートネットワークロケーションは、完全にメッシュ化されます。

- **ZTNA** コネクター Zero Trust Network Access (ZTNA) コネクタを使用すると、組織のプライベート アプリに簡単かつ安全に接続できます。ZTNA コネクタ は、自動化された安全なトンネルを使用してモバイル ユーザーとブランチ ロケーションのユーザーにプライベート アプリへのアクセスを提供します。これにより、プライベート アプリにアクセスするためにIPSec トンネルとルーティング定義をセットアップする必要がなくなります。ZTNAコネクタは、顧客のインフラストラクチャからのルーティングを必要とせず、ネットワーク内で重複したIPアドレスを使用するアプリケーションへのアクセスを提供できます。

- **Strata Logging Service**—Prisma Accessは、すべてのログをStrata Logging Serviceに転送する。Prisma Accessをアクティブ化する一環として、Prisma Accessログを転送するStrata

 ©2025 Palo Alto Networks, Inc.

Logging Serviceインスタンスを指定します。ログのトラフィックは、Prisma Access用に購入したライセンス帯域幅を消費しません。

©2025 Palo Alto Networks, Inc.

Prisma Accessを使った安全なインターネット トラフィック

どこで使用できますか?	何が必要ですか?
• Prisma Access	❑ Prisma Accessライセンス

インターネットセキュリティの重要性

インターネット アクセスのセキュリティ保護は、これまで以上に重要かつ困難になっています。既存のレガシー ソリューションでは、回避型および標的型のフィッシングやその他のWebベースの攻撃を検出するのが困難である一方で、セキュリティ保護されていないDNSトラフィックによってもたらされる新たな脅威を無視しています。Palo Alto NetworksのPrisma Accessは、業界初のMLパワーによる高度なURLフィルタリングとDNSセキュリティサービスによるインターネットセキュリティを提供しています。Prisma Accessを使用することで、回避型の標的型フィッシング攻撃やファイルレス攻撃をリアルタイムで防止し、最新の巧妙なDNSベースの攻撃から保護することができます。

Prisma Accessクラウドセキュアwebゲートウェイ (SWG)

サイバー脅威の複雑さと頻度が増しているため、安全なWebゲートウェイは今日のデジタル環境において重要な要素となっています。サイバー犯罪者は、セキュリティ防御を突破するための新しい戦術や手法を絶えず考案していますが、その1つは、一見正当なWebサイトに悪意のあるコードを偽装することです。ユーザーがこれらの侵害された Web サイトにアクセスすると、不注意で認証情報が漏洩したり、組織が有害なコードにさらされたりする可能性があり、気付かなければ大混乱を引き起こす可能性があります。

このようなリスクの高い環境では、堅牢なセキュリティ ゲートウェイがないと、組織のデジタル資産に対するリスクが大幅に増大します。このようなリスクは、特にフィッシングやランサムウェア攻撃の蔓延が進むにつれて、不正アクセス、データ盗難、業務運営の混乱につながる可能性があります。SWG が提供するセキュリティ バリアがなければ、ランサムウェア攻撃によって組織が人質に取られ、金銭的損害や評判の損失につながる可能性があります。

暗号化されたトラフィックの使用は現在では一般的になり、HTTPSがWebトラフィックの大部分を占めるようになりました。組織に、このトラフィックを効果的に復号化して検査できるSWGがない場合、暗号化されたチャネル内に隠されたセキュリティの脅威にさらされるリスクがあります。

ただし、SWG、プライベート アプリ アクセス、CASBに複数のポイント製品を使用すると、問題は複雑になるだけです。サイロ化された製品を1つの製品としてまとめると、機能の不一致やセキュリティの低下が生じ、攻撃に対して脆弱になります。これらのソリューションを使用すると、インターネットとプライベート アプリのセキュリティが一貫性を失います。

これらの課題に対処するために、 Prisma AccessはZTNA、SWG、NG-CASB、FWaaS、DLPなど、すべての機能にわたってすべてのユーザーとアプリの管理、ポリシー、データを統合する統合製品を提供します。

©2025 Palo Alto Networks, Inc.

顧客は、従来のオンプレミスやクラウドベースのプロキシ・ソリューションからPrisma Accessに簡単に移行でき、業界をリードするAIを活用したセキュリティ保護により、インターネットやSaaSアプリのトラフィックをインラインで可視化・制御できます。

Prisma Accessを使用してユーザーとエンドポイントを保護する

Prisma Access は、サイバー攻撃の成功を防ぐように設計されており、Webのセキュリティ保護以上の機能を備えています。サイバー攻撃を阻止するには、すべてのトラフィックを検査する必要があります。すべてのトラフィックを完全に検査しないと、セキュリティに大きなギャップが生じます。 Prisma Accessはすべてのポートとすべてのアプリケーションからのすべてのトラフィックを一貫して保護し、組織で次のことが可能になります。

- 実績のあるセキュリティ哲学と脅威インテリジェンスを使用してサイバー攻撃を防ぎ、組織全体にわたる詳細な可視性と正確な制御を実現します。
- インターネット、クラウド、ブランチ間の通信を問わず、すべてのポートで、SSLまたはTLSで暗号化されたトラフィックを含むすべてのアプリケーション トラフィックを双方向で完全に検査します。
- Palo Alto Networks からの自動化された脅威データと何百ものサードパーティ フィードを活用した包括的な脅威インテリジェンスのメリットを享受できます。

Prisma Accessとその解決策についてもっと読む

©2025 Palo Alto Networks, Inc.

Prisma Accessの管理方法

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

Prisma Accessを管理するには2つの方法がありますが、Prisma Access ライセンスをアクティベートした後は、管理インターフェースを切り替えることはできません（からへのデプロイに移行ワークフローを使用する場合を除く）。開始するに先立ってPrisma Accessをどのように管理するか決める必要があります。

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

  クラウドからPrisma Accessを管理する場合は、Strata Cloud Managerを使用します。クラウド管理を使用すると、タスク駆動型のワークフローを通じてブランチやモバイル ユーザーを迅速にオンボードし、数分で環境をセットアップしてテストできます。Strata Cloud Managerによるクラウド管理では、ベスト プラクティスに基づいて事前定義済みのインターネット アクセスと復号ポリシー ルールが提供されるため、オンボーディング プロセスが簡素化されます。最も一般的なIPSec対応デバイスに適したデフォルトを使用してIPSecトンネルをすばやくセットアップし、推奨されるURLカテゴリに対してSSL復号化をオンにします。

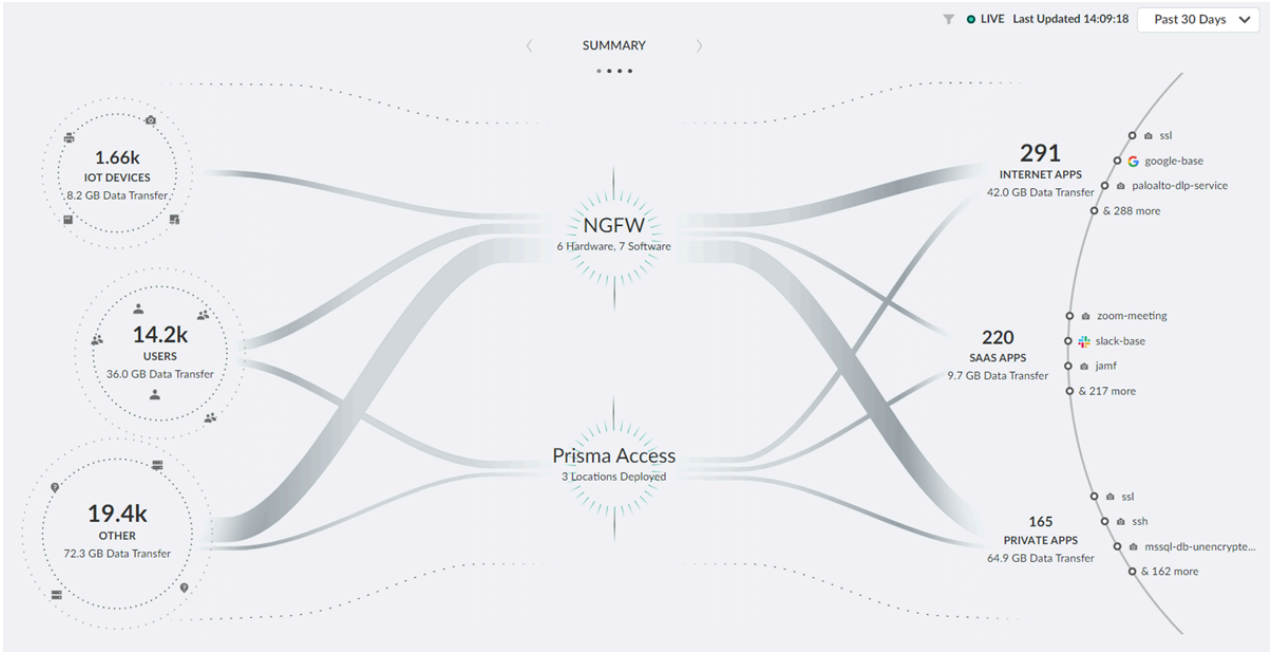
  Strata Cloud Managerコマンドセンター

  Strata Cloud Managerを起動すると、Strata Cloud Managerコマンド センター ページが表示されます。このコマンド センターは、ネットワークの健全性、可視性の向上、データの概要を

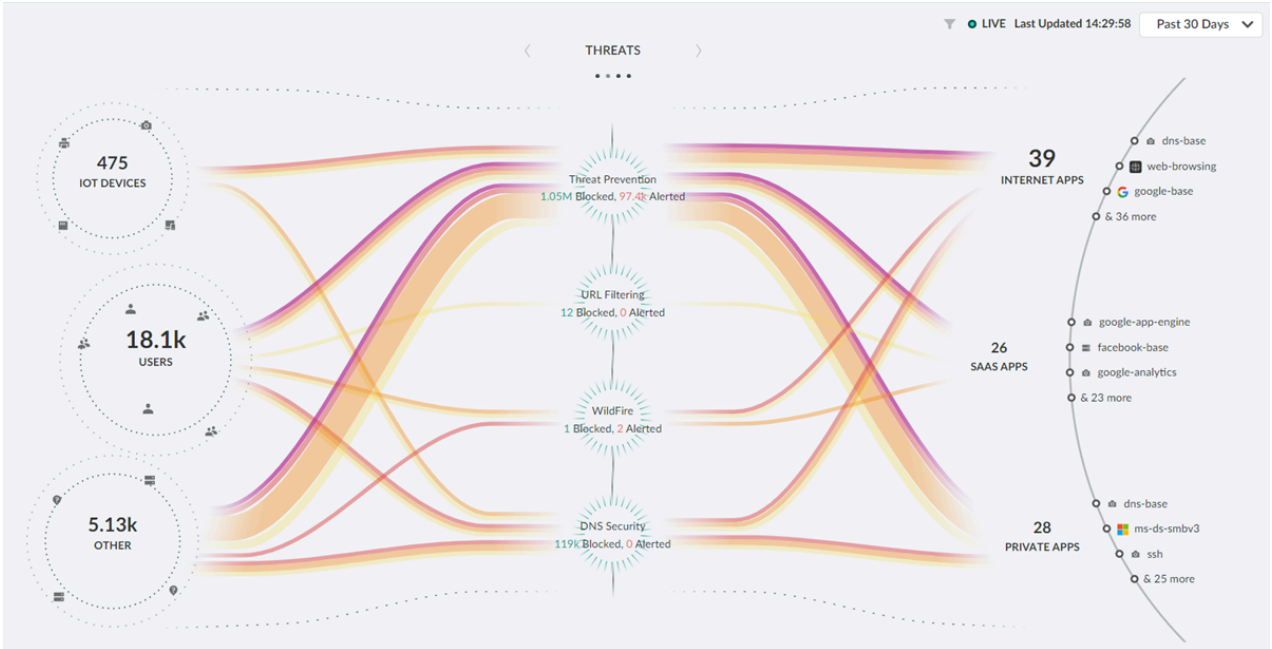
©2025 Palo Alto Networks, Inc.

評価するのに役立ちます。コマンド センターには、さまざまな種類のレポートを表示するためのさまざまなダッシュボードがあります。

- 概要:概要ダッシュボードでは、さまざまなデータ ソースからネットワーク内のさまざまなアプリケーションにデータが流れる、さまざまな種類のデータ ソースやプラットフォーム インフラストラクチャ (NGFW やPrisma Accessなど) を表示できます。

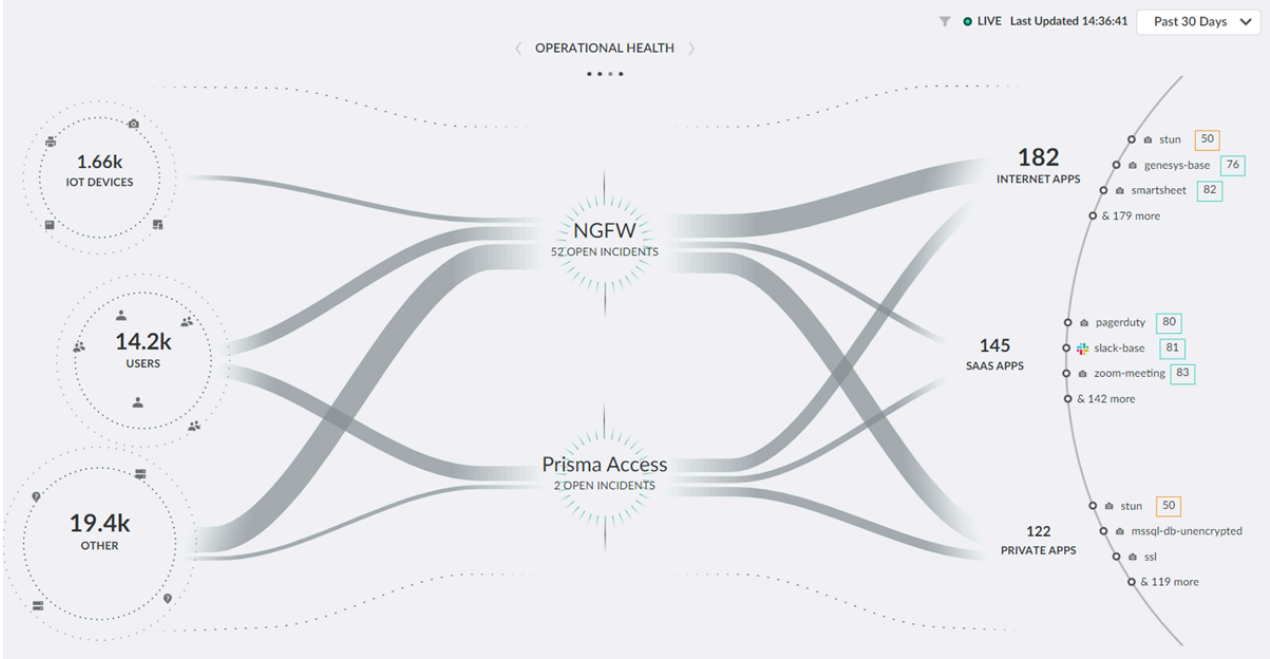


- 脅威:脅威ダッシュボードでは、セキュリティ アプリケーションによって検出された脅威を表示できます。このダッシュボードを使用すると、ネットワーク上でブロックされた脅威と許可された脅威を監視したり、検査されたトラフィックの割合が低い可能性があるネットワーク領域を調査したりできます。



 ©2025 Palo Alto Networks, Inc.

- 運用健全性:ADEMによって監視されているネットワークの健全性とユーザー エクスペリエンスを表示します。このビューを使用して、ネットワーク上のユーザー エクスペリエンスを監視し、未解決のインシデントの重大度を確認できます。



- データセキュリティ:DLPおよびSaaSセキュリティ サブスクリプションによって機密データがあるとフラグが付けられたネットワーク内のトラフィックを表示します。このビューを使用すると、ファイアウォールや接続されたSaaSアプリケーションを通過するデータと、ネットワーク上のデータ リスクの重大度を監視できます。



ダッシュボードでこれらのカテゴリのいずれかをクリックすると、それに応じて結果がフィルタリングされます。

©2025 Palo Alto Networks, Inc.

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

  PanoramaのCloud Servicesプラグインを使用して、Prisma Accessをセットアップおよび管理します。すでにPanoramaを使用して次世代ファイアウォールを管理しており、企業アプリケーションへのアクセスに使用する共通ポリシーがある場合には、これが適切なオプションです。

  *Panorama*を使用して*Prisma Access*を管理している場合でも、*Strata Cloud Manager*を使用して多くの*Prisma Access*の可視化および監視機能を使用することができます。詳しくはこちらをご覧ください

使用する管理オプションを決定したら、選択したオプションのライセンスおよびアクティベーション ワークフローに従って開始します。

- Prisma Access (Managed by Panorama) Access を使い始めるには、カスタマー サポート ポータル（CSP）からライセ ンスのアクティベーションを行い、Panorama にクラウド サービス プラグインをインストー ルします。
- Cloud Managed Prisma Access の使用を開始するには、ハブからライセンスのアクティベーションを実行します。



Panorama とクラウド管理の機能の同等性

*Prisma Access (Managed by Panorama) Access*と*Prisma Access (Managed by Strata Cloud Manager)*でサポートされているものと*.NET*でサポートされているものにはいくつか違いがあります。*Prisma Access (Managed by Panorama)*と*Prisma Access (Managed by Strata Cloud Manager)*の機能サポートリストについては、互換性マトリックスを参照してください。

©2025 Palo Alto Networks, Inc.

Prisma AccessStrata Cloud Managerによる可視性と監視

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access(Panorama管理)	• Prisma Accessライセンス

Prisma Access を管理するには、次の2つの方法から選択できます。

- Prisma Access (Managed by Strata Cloud Manager)では、**Strata Cloud Manager**を使用できます。
- あるいは**Panorama**を使ってPrisma Accessを管理することもできる。

これら2つの管理インターフェースは、Prisma Access環境のオンボーディング、設定、およびセキュリティ ポリシーの施 行を処理する方法です。ただし、Prisma Accessには、Prisma Access環境の堅牢な可視化と監視も含まれており、これらの機能はStrata Cloud Managerで提供されます。

重要な点:

Prisma Accessに使用している管理インターフェース（Strata Cloud ManagerまたはPanorama）に関係なく、Prisma Accessの可視化機能の多くにStrata Cloud Managerを使用し、AIを搭載した自律型DEMのようなアドオン サブスクリプションとやり取りすることができます。

Prisma Access Strata Cloud Managerの可視性と監視機能	
自律型 DEM	セキュア アクセス サービス エッジ (SASE) 環境内のすべてのユーザー トラフィックに対して、ネイティブのエンドツーエンドの可視性と分析情報を提供します。ADEM機能は、GlobalProtectアプリケーションとPrisma Accessにネイティブに統合されているため、追加のアプライアンスやエージェントを導入する必要はありません。デジタル エクスペリエンスの問題の原因を迅速に特定し、修復を簡素化できます。 この機能を*Prisma Access (Managed by Panorama)* *Access*で使用するには、Autonomous DEM (自律型DEM) アドオンライセンスが必要です。
Strata Cloud Managerのダッシュボードとレポート	Strata Cloud Managerの可視性機能は、ポリシーの更新を通知し、企業のセキュリティとユーザーの生産性のギャップを埋めるために使用できる重要な調査結果を識別します。

©2025 Palo Alto Networks, Inc.

Prisma Access Strata Cloud Managerの可視性と監視機能	
	• インタラクティブなダッシュボード ネットワークで稼働しているアプリケーション、脅威、ユーザー、セキュリティサブスクリプションに関するデータを調査します • レポート 多くのダッシュボードはレポートをサポートしており、オフラインでデータを共有したり、定期的な更新をスケジュールしたりできます。
Strata Cloud Managerコマンドセンター	コマンド センターは、ネットワーク上のIoTデバイス、ユーザー、ホスト、トラフィックのインタラクティブな視覚的な概要を提供します。コマンド センターは、クラウド配信のセキュリティとADEMサブスクリプションのデータを活用して、ネットワーク上のデータの脅威、ユーザー エクスペリエンス、セキュリティに関する重要な情報を表示します。 この図表形式の表現によりデータとの対話が可能になり、ネットワークで発生したイベントの関係性も可視化できるため、異常な状況を発見し、ネットワーク セキュリティ ルールの強化方法を見つけることができます。

©2025 Palo Alto Networks, Inc.

Prisma Accessロケーション

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

データロケーションの好みやユーザーの多い場所に基づいて、お好みのロケーションにPrisma Accessをデプロイすることができます。 Prisma Accessは世界中に100以上のロケーションを提供しており、ユーザーはそれぞれのロケーションに合った体験をすることができます。すべてのPrisma Accessロケーションは、最適化されたパフォーマンスとレイテンシに基づいて、セキュリティコンピュートロケーションにマッピングされています。このことは、特定の国のトラフィックが定義されたコンピュートロケーションに向けられることを意味します。

特定の国にコンピュートロケーションを制限する必要がある場合は、*Prisma Access*の処理国とその関連サービスを示す表を参照してください。

異なるPrisma Accessロケーションタイプがあります:

- コンピュートロケーションによってソートされたロケーション - リモートネットワークを構成する際、コンピュートロケーションによって帯域幅を割り当てます。地理的に近接する少なくとも2つ（多くの場合、それ以上）のPrisma Accessロケーションが、コンピュート ロケーションごとにグループ化されています。これは、個々のPrisma Accessロケーションまたは特定のリモートネットワークサイトに帯域幅を割り当てるのではなく、帯域幅を割り当てるレベルであり、Prisma Accessは負荷または需要に基づいて、コンピュートロケーション内のサイトに動的に帯域幅を割り当てることができます。
- シアターとロケーショングループ–モバイルユーザー–GlobalProtectデプロイメントでIPアドレスプールを割り当てるとき、ロケーショングループ（シアターよりも小さいロケーションのグループ）、シアター、または全世界によってIPプールを指定できます。ユーザーの詳細（位置情報ベースのサービスやユーザーグループまたは機能に基づくサービスなど）を特定するために、ユーザーのソースIPアドレスに依存するサービスがある場合は、ロケーショングループ固有のIPアドレスプールを使用してください。これにより、アクセス制御ポリシーを適用したり、異なるコンピューティングリージョンにある国々に対してルーティングやポリシー操作を実行したりできます。
- 地域別のロケーション - すべてのPrisma Accessロケーションには関連する地域があります。
- 明示型プロキシのロケーション–明示型プロキシには、Prisma Accessロケーションのサブセットである独自のロケーションのセットがあります。
- **Colo-Connect**のロケーション - Colo-Connectには、Prisma Accessロケーションのサブセットである独自のロケーションセットがあります。
- **Strata**ロギングサービス地域 - Prisma AccessはStrataロギングサービス地域のサブセットをサポートします。

©2025 Palo Alto Networks, Inc.

- リモートネットワーク - 高性能、トラフィック複製、および安全なインバウンドアクセスロケーション - 高性能のリモートネットワーク、トラフィック複製、および安全なインバウンドアクセスの導入は、Prisma Accessロケーションのサブセットを使用します。
- **Prisma Access中国のロケーション**–Prisma Access中国のデプロイメントは、中国本土のロケーションを使用します。
- **FedRAMPモデレートおよびハイロケーション** - Prisma AccessFedRAMPモデレートおよびハイデプロイメントは、Prisma Accessロケーションのサブセットを使用します。
- 北アメリカのロケーションマップ–北アメリカのロケーションを選択するのに役立つように、北アメリカのロケーションの地理的範囲を示すこのマップを参照してください。
- ローカルゾーン - ローカルゾーンは、コンピューティング、ストレージ、データベース、およびその他のサービスを大規模な人口および産業の中心に近接して配置します。これらの場所には、それぞれ独自のコンピュートロケーションがあります。

  ローカル ゾーンを追加するには、*Palo Alto Networks*の担当者にお問い合わせください。

  ローカルゾーンをデプロイする際は、以下のガイドラインを考慮してください:

  - ローカルゾーンの場所はIPv6をサポートしていません。
  - ローカルゾーンの場所は、Palo Alto Networksに登録されたIPアドレスを使用しません。
  - リモートネットワークの1 Gbpsサポートはサポートされていません。
  - リモートネットワークおよびサービス接続ノードの冗長性は、同じローカルゾーンにデプロイした場合、利用可能なゾーン間では利用できません。両方のノードが単一のゾーンにプロビジョニングされるためです。
  - これらのローカルゾーンは、Palo Alto Networksの登録IPを使用していません。URLにアクセスする際に問題がある場合は、https://reportasite.gpcloudservice.com/ を使用してウェブサイトの問題を報告するか、Palo Alto Networksのサポートに連絡してください。

Prisma Accessプライバシーのデータシートで、*Prisma Access*のロケーションと*Prisma Access*がトラフィックを処理する場所についてご確認ください。

ロケーション、都市、国を計算する

各コンピュートロケーションにリストされている最初のロケーション（太字）は、コンピュートロケーションの都市と国を示しています。

二つのアスタリスク（**）で示された場所はローカルゾーンであり、すべてのPrisma Access機能をサポートしていません。

Compute ロケーション	Prisma Access場所	都市と国
アジア北東部	日本中部	東京、日本
アジア南	インド西部 バングラデシュ	ムンバイ、インド ダッカ、バングラデシュ

©2025 Palo Alto Networks, Inc.

Compute ロケーション	Prisma Access場所	都市と国
	インド南部 パキスタン南部 パキスタン西部	チェンナイ、インド カラチ、パキスタン ラホール、パキスタン
アジア南東部（インドネシア）	インドネシア	ジャカルタ、インドネシア
アジア南東部（シンガポール）	シンガポール カンボジア マレーシア ミャンマー パキスタン西部（II） フィリピン スリランカ タイ ベトナム	シンガポール プノンペン、カンボジア クアラルンプール、マレーシア ヤンゴン、ミャンマー イスラマバード、パキスタン ケソン市、フィリピン コロンボ、スリランカ バンコク、タイ ホーチミン市、ベトナム
オーストラリア南部	オーストラリア南部	メルボルン、オーストラリア
オーストラリア南東部	オーストラリア南東部 オーストラリア東部 ニュージーランド パプアニューギニア	シドニー、オーストラリア ブリスベン、オーストラリア オークランド、ニュージーランド ポートモレスビー、パプアニューギニア
オーストラリア西部（パース）**	オーストラリア西部（パース）**	パース、オーストラリア
バーレーン	バーレーン	マナーマ、バーレーン
ベルギー	ベルギー ラトビア セネガル	聖ギスラン、ベルギー リガ、ラトビア ダカール、セネガル
カナダ中央（モントリオール）	カナダ東部	ケベック、カナダ

©2025 Palo Alto Networks, Inc.

Compute ロケーション	Prisma Access場所	都市と国
カナダ中央（トロント）	カナダ中部	トロント、カナダ
カナダ西部（カルガリー）	カナダ西部	カルガリー、カナダ
ヨーロッパ中央	ドイツ中部 オーストリア ブルガリア クロアチア チェコ共和国 エジプト ドイツ北部 ドイツ南部 ギリシャ ハンガリー クウェート リヒテンシュタイン ルクセンブルク モルドバ ナイジェリア ルーマニア スロバキア スロベニア トルコ ウクライナ ウズベキスタン	フランクフルト、ドイツ ウィーン、オーストリア ソフィア、ブルガリア ザグレブ、クロアチア プラハ、チェコ共和国 カイロ、エジプト ハンブルク、ドイツ ミュンヘン、ドイツ アテネ、ギリシャ ブダペスト、ハンガリー アル・アフマディ、クウェート シャーン、リヒテンシュタイン ルクセンブルク市、ルクセンブルク キシナウ、モルドバ ラゴス、ナイジェリア ブカレスト、ルーマニア ブラチスラバ、スロバキア リュブリャナ、スロベニア イスタンブール、トルコ キエフ、ウクライナ タシュケント、ウズベキスタン
ヨーロッパ中央（ワルシャワ）	ポーランド	ワルシャワ、ポーランド
ヨーロッパ北部	フィンランド ベラルーシ	ハミナ、フィンランド ミンスク、ベラルーシ

©2025 Palo Alto Networks, Inc.

Compute ロケーション	Prisma Access場所	都市と国
	カザフスタン リトアニア ノルウェー ロシア中部 ロシア北西部	アスタナ、カザフスタン ヴィリニュス、リトアニア オスロ、ノルウェー モスクワ、ロシア サンクトペテルブルク、ロシア
ヨーロッパ北部（ストックホルム）	スウェーデン	ストックホルム、スウェーデン
ヨーロッパ北西部	英国 ガーナ	ロンドン、イギリス アクラ、ガーナ
ヨーロッパ北西部（パリ）	フランス南部	パリ、フランス
ヨーロッパ南	イタリア ヨルダン ケニア モナコ	ミラノ、イタリア アンマン、ヨルダン モンバサ、ケニア モナコ
ヨーロッパ南西部	スペイン中部 アンドラ ポルトガル スペイン東部	マドリード、スペイン アンドラ・ラ・ベリャ、アンドラ リスボン、ポルトガル バルセロナ、スペイン
ヨーロッパ西	オランダ中部 デンマーク オランダ南部	エームスハーフェン、オランダ コペンハーゲン、デンマーク ロッテルダム、オランダ
フランス北部	フランス北部	パリ、フランス
香港	香港	香港、中国
インド北部	インド北部	ニューデリー、インド
アイルランド	アイルランド	ダブリン、アイルランド

©2025 Palo Alto Networks, Inc.

Compute ロケーション	Prisma Access場所	都市と国
日本南部	日本南部	大阪、日本
中東中央（カタール）	カタール	ドーハ、カタール
中東中央（サウジアラビア）	サウジアラビア	リヤド、サウジアラビア
中東中央（UAE）	アラブ首長国連邦	アラブ首長国連邦
中東西部	イスラエル	テルアビブ、イスラエル
ナイジェリア（ラゴス）	ナイジェリア（ラゴス）	ラゴス、ナイジェリア
ニュージーランド（オークランド）	ニュージーランド（オークランド）	オークランド、ニュージーランド
南アフリカ中部	南アフリカ中部	ヨハネスブルグ、南アフリカ
南アフリカ西部	南アフリカ西部	ケープタウン、南アフリカ
南アメリカ東部	ブラジル南部 ブラジル中部 ブラジル東部 パラグアイ ベネズエラ	サンパウロ、ブラジル ブラジリア、ブラジル リオデジャネイロ、ブラジル アスンシオン、パラグアイ カラカス、ベネズエラ
南アメリカ西部	チリ アルゼンチン ボリビア ペルー ウルグアイ	サンティアゴ、チリ ブエノスアイレス、アルゼンチン ボリビア、サンタクルス・デ・ラ・シエラ リマ、ペルー モンテビデオ、ウルグアイ
南アメリカ西部（リマ）**	南アメリカ西部（リマ）**	リマ、ペルー
韓国	韓国	ソウル、韓国
スイス	スイス ウガンダ	チューリッヒ、スイス カンパラ、ウガンダ

©2025 Palo Alto Networks, Inc.

Compute ロケーション	Prisma Access場所	都市と国
台湾	台湾	彰化、台湾
米国中部	米国中部	カウンシルブラフス、アメリカ合衆国
米国中央部（シカゴ）**	米国中央部（シカゴ）**	シカゴ、アメリカ合衆国
米国中央西部	米国中央西部	ソルトレイクシティ、アメリカ
米国東部	米国東部 米国北東部 グアテマラ	アシュバーン、アメリカ合衆国 ニューヨーク市、アメリカ合衆国 グアテマラシティ、グアテマラ
米国北西部	米国北西部	ザ・ダレス、アメリカ
米国南部	米国南部 メキシコ中部 メキシコ西部	ダラス、アメリカ合衆国 メキシコシティ、メキシコ グアダラハラ、メキシコ
米国南東部	米国南東部 コロンビア コスタリカ エクアドル パナマ	モンクスコーナー、アメリカ ボゴタ、コロンビア サンホセ、コスタリカ グアヤキル、エクアドル パナマシティ、パナマ
米国南東部（マイアミ）**	米国南東部（マイアミ）**	マイアミ、アメリカ
米国南西部	米国南西部 米国西部	ロサンゼルス、アメリカ合衆国 サンフランシスコ、アメリカ合衆国

©2025 Palo Alto Networks, Inc.

シアターとロケーショングループ

シアター/ロケーショングループ	IPプールグループID
コロンビア コスタリカ エクアドル グアテマラ メキシコ中部 パナマ 米国東部 米国南東部 米国中部 コスタリカ 北中部米国 米国北東部 米国南部 米国南東部 ベネズエラ	1
カナダ東部 カナダ中部	2
アイルランド	3
フランス南部 ガーナ イギリス	4
フランス北部	5
アジア、オーストラリア、日本	6
アンドラ オーストリア ブルガリア クロアチア	7

©2025 Palo Alto Networks, Inc.

シアター/ロケーショングループ	IPプールグループID
チェコ共和国	
エジプト	
ドイツ中部	
ドイツ北部	
ドイツ南部	
ギリシャ	
ハンガリー	
イスラエル	
イタリア	
ヨルダン	
ケニア	
クウェート	
リヒテンシュタイン	
ルクセンブルク	
モルドバ	
モナコ	
ナイジェリア	
ポーランド	
ポルトガル	
ルーマニア	
スロバキア	
スロベニア	
サウジアラビア	
南アフリカ中部	
スペイン中部	
スペイン東部	
トルコ	
ウクライナ	
アラブ首長国連邦	
ウズベキスタン	

©2025 Palo Alto Networks, Inc.

シアター/ロケーショングループ	IPプールグループID
ベラルーシ フィンランド カザフスタン リトアニア ノルウェー ロシア中部 ロシア北西部 スウェーデン	8
デンマーク オランダ中部 オランダ南部	9
アフリカ、欧州、中東	10
スイス ウガンダ	11
ベルギー ラトビア セネガル	12
Brazil Central（ブラジル中部） Brazil East（ブラジル東部） ブラジル南部 Paraguay（パラグアイ） Venezuela（ベネズエラ）	13
オーストラリア東部 Australia South（オーストラリア南部） Australia Southeast（オーストラリア南東部） ニュージーランド Papua New Guinea（パプアニューギニア）	14
Cambodia（カンボジア）	15

©2025 Palo Alto Networks, Inc.

シアター/ロケーショングループ	IPプールグループID
インドネシア マレーシア Myanmar（ミャンマー） Philippines（フィリピン） シンガポール タイ ベトナム	
香港	16
台湾	17
韓国	18
Bangladesh（バングラデシュ） India North（インド北部） India South（インド南部） India West（インド西部） Pakistan West（パキスタン西部） Pakistan South（パキスタン南部） カタール	19
South Africa West（南アフリカ西部） スウェーデン South Africa West（南アフリカ西部）	20
Japan Central（日本中部） Japan South（日本南部）	21
バーレーン	22
Canada West（カナダ西武） Mexico Central（メキシコ中部） Mexico West（メキシコ西武） 米国中央西部 US Northwest（米国北西部）	23

©2025 Palo Alto Networks, Inc.

シアター/ロケーショングループ	IPプールグループID
US Southeast（米国南西部） US West（米国西部）	
Argentina（アルゼンチン） Bolivia（ボリビア） チリ Peru（ペルー） ウルグアイ	24

地域別ロケーション

所在地
アフリカ地域
Kenya（ケニア）
Nigeria（ナイジェリア）
セネガル
South Africa Central（南アフリカ中部）
South Africa West（南アフリカ西部）
アジア地域
Bangladesh（バングラデシュ）
Cambodia（カンボジア）
香港
India North（インド北部）
India South（インド南部）
India West（インド西部）
インドネシア
カザフスタン

©2025 Palo Alto Networks, Inc.

所在地
マレーシア
Myanmar（ミャンマー）
Pakistan South（パキスタン南部）
Pakistan West（パキスタン西部）
パキスタン西部（II）
Papua New Guinea（パプアニューギニア）
Philippines（フィリピン）
シンガポール
韓国
スリランカ
台湾
タイ
ベトナム
オーストラリア/ニュージーランド（ANZ）地域
オーストラリア東部
Australia South（オーストラリア南部）
Australia Southeast（オーストラリア南東部）
ニュージーランド
欧州地域
Andorra（アンドラ）
Austria（オーストリア）
Belarus（ベラルーシ）
ベルギー
ブルガリア

©2025 Palo Alto Networks, Inc.

所在地
クロアチア
チェコ共和国
デンマーク
フィンランド
France North（フランス北部）
France South（フランス南部）
Germany Central（ドイツ中部）
Germany North（ドイツ北部）
Germany South（ドイツ南部）
ガーナ
Greece（ギリシャ）
ハンガリー
アイルランド
イタリア
ラトビア
Liechtenstein（リヒテンシュタイン）
Lithuania（リトアニア）
Luxembourg（ルクセンブルク）
Moldova（モルドバ）
Monaco（モナコ）
Netherlands Central（オランダ中部）
Netherlands South（オランダ南部）
ノルウェー
ポーランド

©2025 Palo Alto Networks, Inc.

所在地
ポルトガル
ルーマニア
Russia Central（ロシア中部）
Russia Northwest（ロシア北西部）
スロバキア
スロベニア
Spain Central（スペイン中部）
Spain East（スペイン東部）
スウェーデン
スイス
ウガンダ
イギリス
ウクライナ
Uzbekistan（ウズベキスタン）
日本地域
Japan Central（日本中部）
Japan South（日本南部）
中東地域
バーレーン
エジプト
イスラエル
ヨルダン
クウェート
カタール

©2025 Palo Alto Networks, Inc.

所在地
サウジアラビア
トルコ
アラブ首長国連邦
北アメリカ地域
カナダ中部
Canada East（カナダ東部）
Canada West（カナダ西武）
Costa Rica（コスタリカ）
Mexico Central（メキシコ中部）
Mexico West（メキシコ西武）
Panama（パナマ）
US Central（米国中部）
米国中央西部
US East（米国東部）
US Northeast（米国北東部）
US Northwest（米国北西部）
US South（米国南部）
US Southeast（米国南東部）
US Southeast（米国南西部）
US West（米国西部）
南アメリカ地域
Argentina（アルゼンチン）
Bolivia（ボリビア）
Brazil Central（ブラジル中部）

©2025 Palo Alto Networks, Inc.

所在地
Brazil East（ブラジル東部）
Brazil South（ブラジル南部）
チリ
コロンビア
Ecuador（エクアドル）
Paraguay（パラグアイ）
Peru（ペルー）
ウルグアイ
Venezuela（ベネズエラ）

明示型プロキシのロケーション

Prisma Accessは明示型プロキシに対して次の場所をサポートしています。明示型プロキシは、GeoDNSを使用して、モバイル・ユーザーを最も近いPrisma Accessデプロイ先ロケーションに解決し、接続します。

- アフリカ、欧州、中東
  - ベルギー
  - フィンランド
  - France South（フランス南部）
  - Germany Central（ドイツ中部）
  - イスラエル
  - イタリア
  - Netherlands Central（オランダ中部）
  - ポーランド
  - カタール
  - サウジアラビア
  - South Africa Central（南アフリカ中部）
  - Spain Central（スペイン中部）
  - スイス
  - イギリス

©2025 Palo Alto Networks, Inc.

- アジア、オーストラリア、日本:
  - Australia South（オーストラリア南部）
  - オーストラリア南東部
  - 中国
  - 香港
  - Japan Central（日本中部）
  - Japan South（日本南部）
  - India North（インド北部）
  - India West（インド西部）
  - インドネシア
  - シンガポール
  - 韓国
  - 台湾
- 北米&南米:
  - ブラジル南部
  - チリ
  - カナダ中部
  - カナダ東部
  - US Central（米国中部）
  - US East（米国東部）
  - US Northwest（米国北西部）
  - US South（米国南部）
  - US Southeast（米国南東部）
  - US Southeast（米国南西部）
  - 米国中央西部

Colo-Connectの場所

Prisma AccessColo-Connectは以下のPrisma Accessロケーションをサポートしています。Colo-Connectをサポートするためにサービス接続を作成する際は、以下の場所にのみ作成するようにしてください。

専用インターコネクトリンクの場合、専用インターコネクト接続を作成できるロケーションのGCPリストを使用してください。

- Australia South（オーストラリア南部）
- オーストラリア南東部
- ベルギー

©2025 Palo Alto Networks, Inc.

- ブラジル南部
- カナダ中部
- カナダ東部
- チリ
- フィンランド
- France South（フランス南部）
- Germany Central（ドイツ中部）
- 香港
- India North（インド北部）
- India West（インド西部）
- インドネシア
- イタリア
- Japan Central（日本中部）
- Japan South（日本南部）
- Netherlands Central（オランダ中部）
- カタール
- サウジアラビア
- シンガポール
- South Africa Central（南アフリカ中部）
- Spain Central（スペイン中部）
- スイス
- 台湾
- イギリス
- US Central（米国中部）
- 米国中央西部
- US East（米国東部）
- US Northwest（米国北西部）
- US South（米国南部）
- US Southeast（米国南東部）
- US Southeast（米国南西部）

サポートされているStrata Logging Serviceリージョン

Prisma Accessは以下のStrata Logging Serviceリージョンをサポートしています:

- オーストラリア
- カナダ

©2025 Palo Alto Networks, Inc.

- フランス
- ドイツ
- 日本
- インド
- インドネシア
- イスラエル
- オランダ - ヨーロッパ
- カタール
- サウジアラビア
- シンガポール
- スイス
- 台湾
- 英国
- 米国 - アメリカ

リモートネットワーク - 高パフォーマンス、トラフィックレプリケーション、および安全なインバウンド アクセス ロケーション

以下の高性能リモート・ネットワーク・ロケーションがPrisma Accessではサポートされています:

- Andorra（アンドラ）
- Argentina（アルゼンチン）
- Australia East（オーストラリア東部）
- Australia South（オーストラリア南部）
- Australia Southeast（オーストラリア南東部）
- Austria（オーストリア）
- Bangladesh（バングラデシュ）
- Belarus（ベラルーシ）
- ベルギー
- Bolivia（ボリビア）
- Brazil Central（ブラジル中部）
- Brazil East（ブラジル東部）
- Brazil South（ブラジル南部）
- ブルガリア
- Cambodia（カンボジア）
- Canada Central（カナダ中部）

©2025 Palo Alto Networks, Inc.

- カナダ東部
- チリ
- コロンビア
- Costa Rica（コスタリカ）
- クロアチア
- チェコ共和国
- デンマーク
- Ecuador（エクアドル）
- エジプト
- フィンランド
- France North（フランス北部）
- France South（フランス南部）
- Germany Central（ドイツ中部）
- Germany North（ドイツ北部）
- Germany South（ドイツ南部）
- ガーナ
- Greece（ギリシャ）
- グアテマラ
- 香港
- ハンガリー
- India North（インド北部）
- India South（インド南部）
- India West（インド西部）
- インドネシア
- イスラエル
- イタリア
- Japan Central（日本中部）
- Japan South（日本南部）
- ヨルダン
- カザフスタン
- Kenya（ケニア）
- クウェート
- ラトビア
- Liechtenstein（リヒテンシュタイン）
- Lithuania（リトアニア）

©2025 Palo Alto Networks, Inc.

- Luxembourg（ルクセンブルク）
- マレーシア
- Mexico Central（メキシコ中部）
- Mexico West（メキシコ西武）
- Moldova（モルドバ）
- Monaco（モナコ）
- Myanmar（ミャンマー）
- Netherlands Central（オランダ中部）
- Netherlands South（オランダ南部）
- ニュージーランド
- Nigeria（ナイジェリア）
- ノルウェー
- Pakistan South（パキスタン南部）
- Pakistan West（パキスタン西部）
- パキスタン西部（II）
- Panama（パナマ）
- Papua New Guinea（パプアニューギニア）
- Paraguay（パラグアイ）
- Peru（ペルー）
- Philippines（フィリピン）
- ポーランド
- ポルトガル
- カタール
- ルーマニア
- Russia Central（ロシア中部）
- Russia Northwest（ロシア北西部）
- サウジアラビア
- セネガル
- シンガポール
- スロバキア
- スロベニア
- South Africa Central（南アフリカ中部）
- 韓国
- Spain Central（スペイン中部）
- Spain East（スペイン東部）

©2025 Palo Alto Networks, Inc.

- スリランカ
- スイス
- 台湾
- タイ
- トルコ
- ウガンダ
- イギリス
- ウクライナ
- ウルグアイ
- US Central（米国中部）
- 米国中央西部
- US East（米国東部）
- US Northeast（米国北東部）
- US Northwest（米国北西部）
- US South（米国南部）
- US Southeast（米国南東部）
- US Southeast（米国南西部）
- US West（米国西部）
- Uzbekistan（ウズベキスタン）
- Venezuela（ベネズエラ）
- ベトナム

Prisma Access中国のロケーション

Prisma Access中国は中国本土の以下の場所に対応しています:

- 中国北部–北京（中国北部コンピュート・ロケーションを使用）
- 中国西北部–宁夏（中国北西部のコンピュートロケーションを使用）

FedRAMP中程度および高い場所

Prisma SASE FedRAMP ドキュメントにおける FedRAMP ロケーションのリストを見つけてください。

北米地域の地図

北アメリカのPrisma Accessロケーションを選ぶ際の参考として、以下の地図を使用してください。

©2025 Palo Alto Networks, Inc.



ローカルゾーンのロケーション

次のローカルゾーンは、Prisma AccessのIPv4でサポートされています:

- 次のローカルゾーンのいずれかにデプロイするリクエストを開始するためには、*Palo Alto Networks*の担当者と連携する必要があります。
- *IPv6*はサポートされていません。

- オーストラリア西部（パース）
- ニュージーランド（オークランド）
- ナイジェリア（ラゴス）
- 南アメリカ西部（リマ）
- 米国中央部（シカゴ）
- 米国南東部（マイアミ）

©2025 Palo Alto Networks, Inc.

Prisma Accessおよび関連サービスの処理場所

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

Prisma Accessは、世界100以上のロケーションでローカルエクスペリエンスを提供し、最適化されたパフォーマンスとレイテンシに基づいて各ロケーションをセキュリティコンピューティングロケーションにマッピングします。

コンピューティング場所を特定の国に限定するという要件がある場合は、各Prisma Accessの国マッピングを参照し、Prisma Access設定時にその国に関連付けられた場所のみをデプロイします。

次の表は、Strata Logging Serviceリージョン、Strata Cloud Manager（Prisma Access (Managed by Strata Cloud Manager)用の、Prisma Access Insights、Autonomous DEM、およびSaaS Security Inline）の国別処理場所を示しています。

Strata Logging Service	Strata Cloud Manager設定	Prisma Access Insightsデータ	Autonomous DEM	SaaS Security Inline
英国	英国	英国	英国	英国
オランダ	ドイツ	オランダ	オランダ	ドイツ (EU)
ドイツ	ドイツ	ドイツ	ドイツ	ドイツ (EU)
スイス	スイス	スイス	スイス	ドイツ (EU)
フランス	ドイツ	フランス	フランス	ドイツ (EU)
シンガポール	シンガポール	シンガポール	シンガポール	シンガポール
インド	インド	インド	インド	インド
日本	日本	日本	日本	日本
カナダ	カナダ	カナダ	カナダ	米国
米国	米国	米国	米国	米国
オーストラリア	オーストラリア	オーストラリア	オーストラリア	オーストラリア
イスラエル	ドイツ	イスラエル	イスラエル	ドイツ (EU)
カタール	カタール	カタール	カタール	ドイツ (EU)

©2025 Palo Alto Networks, Inc.

Strata Logging Service	Strata Cloud Manager設定	Prisma Access Insightsデータ	Autonomous DEM	SaaS Security Inline
サウジアラビア	ドイツ	サウジアラビア	サウジアラビア	ドイツ (EU)
台湾	シンガポール	台湾	台湾	シンガポール
インドネシア	シンガポール	インドネシア	インドネシア	シンガポール

©2025 Palo Alto Networks, Inc.

Prisma Access インフラストラクチャ管理

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access(Panorama管理)	❑ Prisma Accessライセンス

Prisma Accessは共有所有権モデルを使用します。Palo Alto Networksは、基盤となっているセキュリティインフラを、安全かつ回復力があり、常に最新の状態で、必要な時に利用できるように維持管理しています。ロケーションやユーザーのオンボーディング、ポリシーのプッシュや更新、ログのクエリ、レポートの生成はお客様の組織が担当します。

Palo Alto Networksは、セキュリティインフラの次の部分を管理します。セキュリティ インフラに加え、Prisma Accessはリリースとアップグレードも管理します：

- **Prisma Access**
- **Strata Logging Service**—ログの配信機構は、当社が管理します。
- コンテンツ更新- PAN-OSの更新を含む リリースとアップグレードを管理します。モバイルユーザーに対しては、Prisma Accessではさまざまなバージョンの GlobalProtectアプリケーションが用意されており、そのリストからアクティブにするGlobalProtectアプリケーションのバージョンを選択することができます。
- 耐障害性–サービスの可用性を管理します。
- 自動スケーリング–サービス接続やリモートネットワークを追加した場合、または単一の地域内の1つまたは複数のゲートウェイにさらにモバイルユーザーがログインした場合、自動的にサービスを拡張します。
- プロビジョニング–インフラと必要なものすべてのプロビジョニングを行います。
- サービス監視–サービスのステータスを監視して、その機能を維持します。
- 位置マッピングの計算- 各Prisma Accessロケーションは、最適化されたパフォーマンスとレイテンシに基づいてセキュリティ コンピューティングの場所にマッピングされます。つまり、システム管理者によって変更されない限り、特定の国のトラフィックは定義されたコンピューティングの場所に送信されます。場所とコンピューティング場所のマッピングについては、Prisma Accessプライバシー データ シートを参照してください。

また、セキュリティインフラの次のコンポーネントの管理も、お客様の組織が行います。

- ユーザー–モバイルユーザーのオンボーディングを管理します。
- 認証–ユーザーの認証を管理します。
- モバイルデバイス管理 - **MDM**—Prisma Accessで保護されている組織のモバイル機器を、独自のMDMソフトウェアを使って管理できます。
- (Prisma Access (Managed by Panorama)のみ) **Panorama**および**Cloud Services**プラグイン–Cloud ServicesプラグインがインストールされているPanoramaについては、Cloud Servicesプラグインをサポートするバージョンの Panoramaを実行していることを確認する必要がありま

©2025 Palo Alto Networks, Inc.

す。また、新しいプラグインが利用できるようになったら、PanoramaでCloud Servicesプラグインを更新する必要があります。

- ポリシーの作成と管理–Prisma Accessで使用するポリシーを策定し、Panoramaでそれを作成します。
- ログ解析とフォレンジック–Prisma Accessがログを提供しています。お客様は、用意されている統合ツール、または他社の統合ツールを使って、解析やレポート生成を行います。
- オンプレミスセキュリティ–オンプレミスネットワークのマイクロセグメント間のオンプレミスセキュリティを提供します。一部のデプロイメント環境では、すべてのトラフィックをPrisma Accessで保護するように設定することができます。
- ネットワーク–Prisma Accessへのネットワーク接続を提供します。
- 監視–オンプレミスネットワークのステータスを監視します。
- サービス接続性–モバイルユーザー向けにPrisma Accessゲートウェイとの接続を提供します（例：ISPを提供）。また、サービス接続やリモートネットワーク接続が使用する、IPSecトンネルの終端ポイントとして使用する、オンプレミスデバイスも提供します。
- オンボーディング–モバイルユーザー、本社/データセンターサイト、支店サイトのオンボーディングを行います。
- （Prisma Access (Managed by Panorama)のみ）バックアップ- Panorama設定のバックアップを管理します。

©2025 Palo Alto Networks, Inc.

Prisma AccessAPI

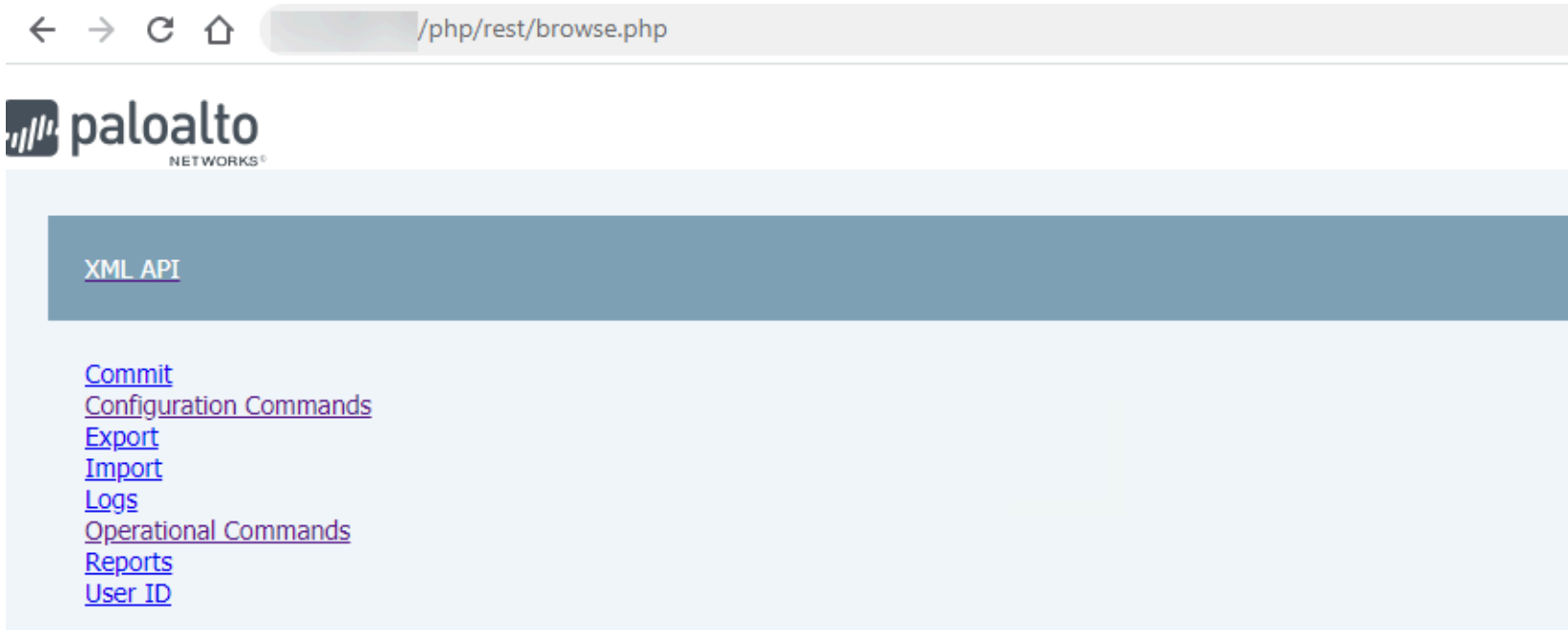
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス

Prisma Access (Managed by Strata Cloud Manager)向けAPI

Prisma Access (Managed by Strata Cloud Manager)用APIの詳細については、Palo Alto Networksの開発者向けドキュメントサイトpan.devを参照してください。 Prisma Access (Managed by Strata Cloud Manager)は、サービスのオンボーディング、設定、および運用にこれらのAPIを使用しています。

Prisma Access (Managed by Panorama)向けAPI

Panoramaで設定と管理を行うために利用できるXML APIの他に、Prisma Access固有のタスクを実行するために使用できるCloud Servicesプラグイン用のXML APIが用意されています。サードパーティサービス、アプリケーション、またはスクリプトを介してこれらのAPIを使用して、Prisma Access用の設定およびレポートタスクを自動化してください。



©2025 Palo Alto Networks, Inc.

WebブラウザとWebインターフェースを使ったPrisma Access (Managed by Panorama)APIへのアクセス

ブラウザを使ってAPIにアクセスするには、Prisma Accessを管理するPanoramaに管理者権限でログインして、URLの最後に/apiを指定してください。URLがXML APIブラウザ インターフェースに変更されます。

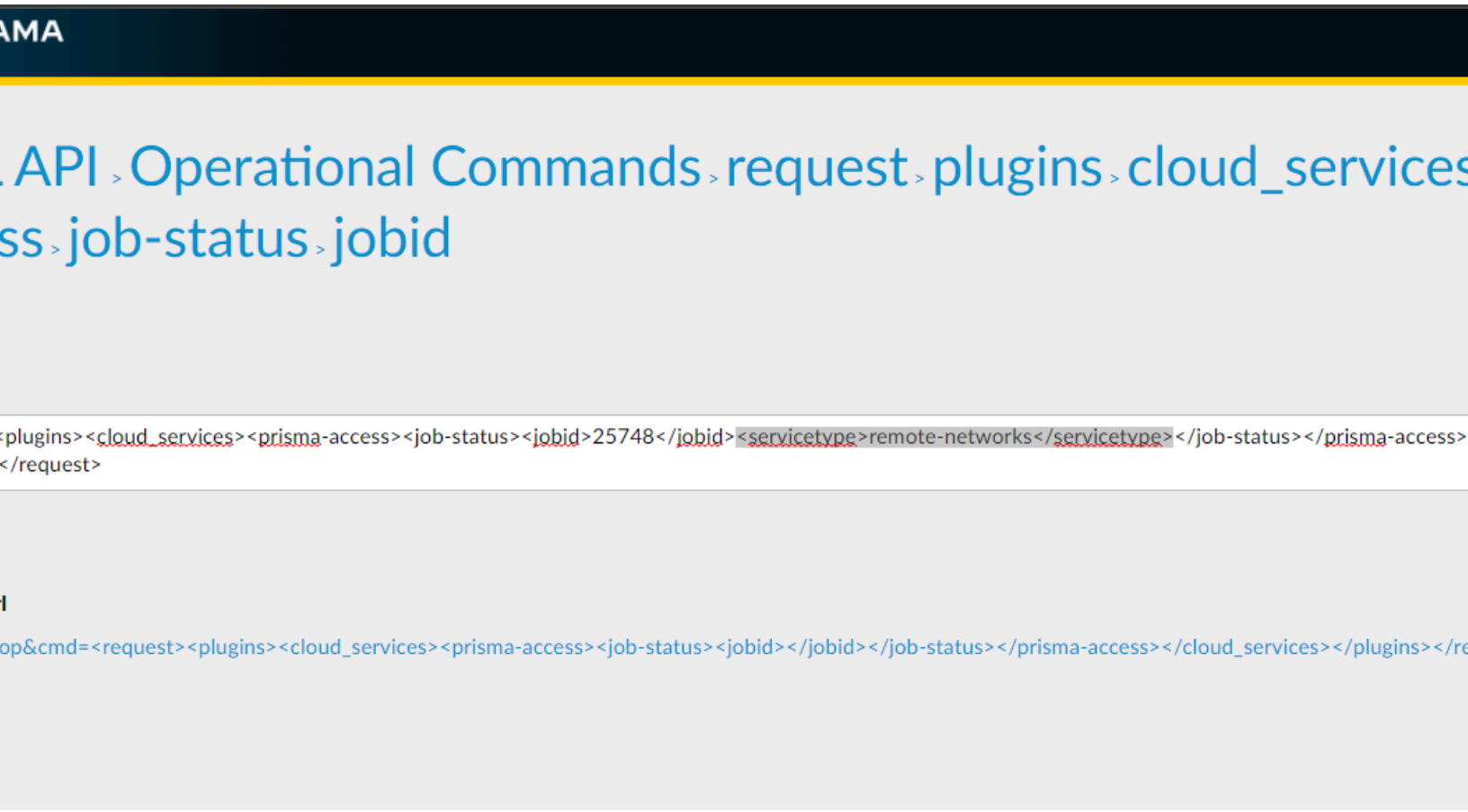
Prisma Access APIは、XMLツリー内の次のXML Path Language（XPath）ノードに存在しています:

- 設定コマンド:**XML API** > **Configuration Commands** > **devices** > **entry[@name='localhost.localdomain']** > **plugins** > **cloud_services**
- 操作コマンド:**XML API** > 操作コマンド > **request** > **plugins** > **cloud_services** > **prisma-access**

XMLツリーをナビゲートすると、Prisma Accessは**XML**領域のツリーにデータを入力します。**XML**領域に必要な値を入力し、**[Submit (送信)]** をクリックすると、XMLリクエストが処理されます。たとえば、ジョブのオンボーディング ステータスを要求するには、**XML API** > 操作コマンド > **request** > **plugins** > **cloud_services** > **prisma-access** > **job-status** > **jobid**に移動し、**jobid** フィールドにジョブIDを入力し、サービス タイプ**servicetype**領域に入力して、**[Submit (送信)]** をクリックして要求を送信します。

このXMLは、ジョブのオンボーディング ステータスのみを取得します。すべてのコミット操作のステータスを取得するには、*Prisma AccessUI* を使用します。

©2025 Palo Alto Networks, Inc.



Prisma Accessは出力をXML形式で返します。

 ©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>
```


Webインターフェース を使用してPanorama 内のAPI を見つけることもできます。

curlコマンドを使用してPanoramaマネージドAPIコマンドを取得する

APIコマンドの結果を取得するためにCLIを使用することを好む場合、Prisma Accessのパブリックアドレスとインフラストラクチャ IP アドレスを取得するために使用するAPIと組み合わせて、APIを使用することができます。これを行うには、次のコマンドを使用します。

設定コマンド:

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

操作コマンド:

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

ここで:

 ©2025 Palo Alto Networks, Inc.

- *<panorama-ip-address>*はPrisma Accessを管理するPanoramaのIPアドレスです。
- *<api-key>*は、API キーでPrisma AccessのIPアドレスを取得します (Panorama Cloud Services Configuration Service Setup Generate API Key)。 (**Panorama** > クラウド サービス > 構成 > サービス セットアップ > **API** キーの生成)。
- *<api-parameters>*と*</api-parameters>*は、リクエストされた情報をAPIから取得するために使用するAPIパラメータです。

マルチテナントデプロイメントの場合は、API情報を取得するテナントの名前をAPIに追加します。

たとえば、以下のようなパラメータを持つPrisma Accessデプロイメントがあるとします：

- **Panorama IP**アドレス:1.2.3.4
- **API**キー:12345abcde
- テナント名: tenant-1

そのテナントのアクティブなモバイル ユーザーの数を取得する場合は、次のcurlコマンドを入力します。

```
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>"
```

Prisma Access (Managed by Panorama)でCLIコマンドを使用する

Prisma Accessでは、CLIコマンドを使ってPrisma Accessのデータを取り出すことができます。CLIにアクセスするには、Prisma Accessを管理しているPanoramaのIPアドレスを使用してSSH接続を確立します。

CLI は、マルチテナント デプロイメントのテナント名の入力を除いて、PAN-OS コマンドと同じモードを使用し、同じ動作をします。テナント名は、`tenant-name` *tenant-name* コマンドを使用して入力します。たとえば、テナント名が *tenant-1*の場合、マルチテナント デプロイメントでアクティブなユーザー数を取得するには、次のコマンドを入力します。

```
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インサイトAPI

Prisma AccessInsights API を使用すると、Prisma AccessInsightsテナントにデータリソースを照会できます。APIには2つのバージョンがあります。Prisma AccessInsights 2.0と1.0の両方のAPIを使用すると、Prisma Accessネットワークデプロイメントの健全性をPrisma Accessテナントに問い合わせることができます。API呼び出しは両方のバージョンで同じですが、バージョンごとに異なるアクセス トークンが使用され、アクセス トークンを取得するメカニズムもバージョンごとに異なります。

©2025 Palo Alto Networks, Inc.

Prisma AccessInsights APIを使い始めるには、[Prisma SASEへようこそ]の開発者ガイドをご覧ください。

Prisma Access Insights APIでは、Prisma Access Insights APIに固有のコンテンツ、APIバージョン2.0、APIバージョン1.0、Prisma Access Insights APIの例、PAI FAQに関する情報を説明しています。

2.0 APIについて

Prisma Access Insights 2.0 APIは、テナントサービス グループ（TSG）識別子を使用してPalo Alto Networksによってテナントがオンボードされたprisma Access (Managed by Strata Cloud Manager)顧客を対象としています。テナントがTSG IDを使用しているかどうかを確認するには、Prisma Accessハブにアクセスし、**Prisma Access Insights**アプリケーション名をクリックして、**[Manage Apps (**アプリケーションの管理**)]**セクションを確認します。

2.0のAPIはPrisma Access (Managed by Panorama)の顧客も利用いただけます。この場合、Prisma Access (Managed by Panorama)のデプロイメントがマルチテナントであれば、スーパーテナントだけが TSG ID を持ち、サブテナントはStrata Logging Serviceテナント ID を持つヘッダに含まれます。

API 2.0のケース

スーパーテナントをTSG IDに移行した後、サブテナントを照会する場合:

ヘッダーには次の情報が必要です。`Prisma-Tenant:tsg_id:sub_tenant_id`

1.0 APIについて

Prisma Access Insights 1.0 APIは、すべてのPrisma Access (Managed by Strata Cloud Manager)シングルテナントのお客様、およびPrisma Access (Managed by Panorama)シングルテナントとマルチテナントのお客様を対象としています。

API 1.0 のケース

スーパーテナントをTSG IDに移行する前に、1.0 API を使用してサブテナント情報を照会するときに、エンドポイントにスーパーテナントIDを含めます。

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

呼び出しに次のヘッダーを含めます。`Prisma-Tenant: {tenant_id}: {sub_tenant_id}`

©2025 Palo Alto Networks, Inc.

Prisma AccessをPanoramaからStrata Cloud Managerへ移行する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス Prisma Access (Managed by Panorama)からPrisma Access (Managed by Strata Cloud Manager)への移行を開始するには、Palo Alto Networksのアカウントチームにお問い合わせください。

Panoramaによって構成が管理されている既存のPrisma Accessデプロイメントがあり、構成管理のためにStrata Cloud Managerに移行したい場合、Palo Alto Networksは、既存のPrisma Access構成をStrata Cloud Managerに移行できる製品内ワークフローを提供します。

Panoramaの代わりにStrata Cloud Managerを使ってPrisma Accessコンフィギュレーションを管理すると、以下のようなメリットがあります：

- 継続的なベストプラクティス評価
- 安全なデフォルト設定
- 機械学習（ML）ベースの構成最適化
- 合理化されたウェブセキュリティワークフロー
- ネットワークの健全性、セキュリティ、効率性を評価するのに役立つインタラクティブなビジュアル サマリー (コマンド センター)
- 複雑なタスクのための直感的なワークフロー
- シンプルで安全な管理API
- クラウドネイティブアーキテクチャは、拡張性、回復力、グローバルなリーチを提供します
- 管理するハードウェアや保守するソフトウェアは不要です

Prisma Access (Managed by Strata Cloud Manager)への移行の準備

移行を開始する前に、最低限必要なソフトウェアと、移行できるPrisma Access (Managed by Panorama)デプロイメントの種類を把握しておく必要があります。

- 移行するタイミング- データプレーンまたはインフラストラクチャのアップグレード中はアップグレードを実行しないでください。アップグレード設定をチェックして、今後データプレーンのアップグレードがあるかどうかを確認します。
- **Panorama**から**Prisma Access (Managed by Strata Cloud Manager)**への一方向の移行 —Prisma Access (Managed by Panorama)からPrisma Access (Managed by Strata Cloud Manager)デプロイメントへの移行のみ可能です。Strata Cloud Managerへの移行後、Panorama を使用してPrisma Accessデプロイメントの管理に戻ることはできません。

©2025 Palo Alto Networks, Inc.

- 最小**Panorama**バージョン- 最小Panoramaバージョン 10.0 が必要です。
- 必要な管理者ロール- 移行を開始するには、Strata Cloud Managerにスーパーユーザーとしてログインする必要があります。
- ライセンス要件–有効なPrisma Accessライセンスが必要です。
- **Cloud Identity Engine**- 移行する前に、Cloud Identity EngineのDirectory Syncコンポーネントを現在のPrisma Access (Managed by Panorama)テナントに統合しておく必要があります。
- サポートされていない機能- 移行プログラムでは以下の機能はサポートされていません。
  Prisma Access 機能:
  - マルチテナント デプロイメント
  - IoTセキュリティ
  - データフィルタリング （代替として、 エンタープライズDLPを使用）
  - SSHプロキシ
  - GlobalProtectポータルとゲートウェイの個別認証
- 構成の差分の問題- 移行中に構成の差分を実行する場合、次のオブジェクト名が表示される差分は構成に影響しないため無視してください。
  - クライアントレス VPN 暗号化設定
  - Hip プロファイルの名前変更
  - モバイル ユーザーの冗長性
  - ビデオ トラフィックの除外

Prisma Access (Managed by Panorama)デプロイメントをStrata Cloud Managerに移行する

Prisma Access (Managed by Panorama)をPrisma Access (Managed by Strata Cloud Manager)デプロイメントに移行するには、次の手順を実行します。

大まかに言うと、次のようになります。

1. 最新のコンフィギュレーションがPrisma Accessに正しくプッシュされ、最新のコンフィギュレーションが保存され、Prisma Accessを管理するPanorama から.xmlコンフィギュレーション・ファイルがエクスポートされていることを確認してください。
2. Strata Cloud Managerから移行プログラムを開始する。
3. Panorama 構成と移行されたStrata Cloud Manager構成の構成の差分（diffs）を確認します。
4. 差分を解決して移行を完了します。

©2025 Palo Alto Networks, Inc.

STEP 1 | 移行のためにPanoramaを準備します。

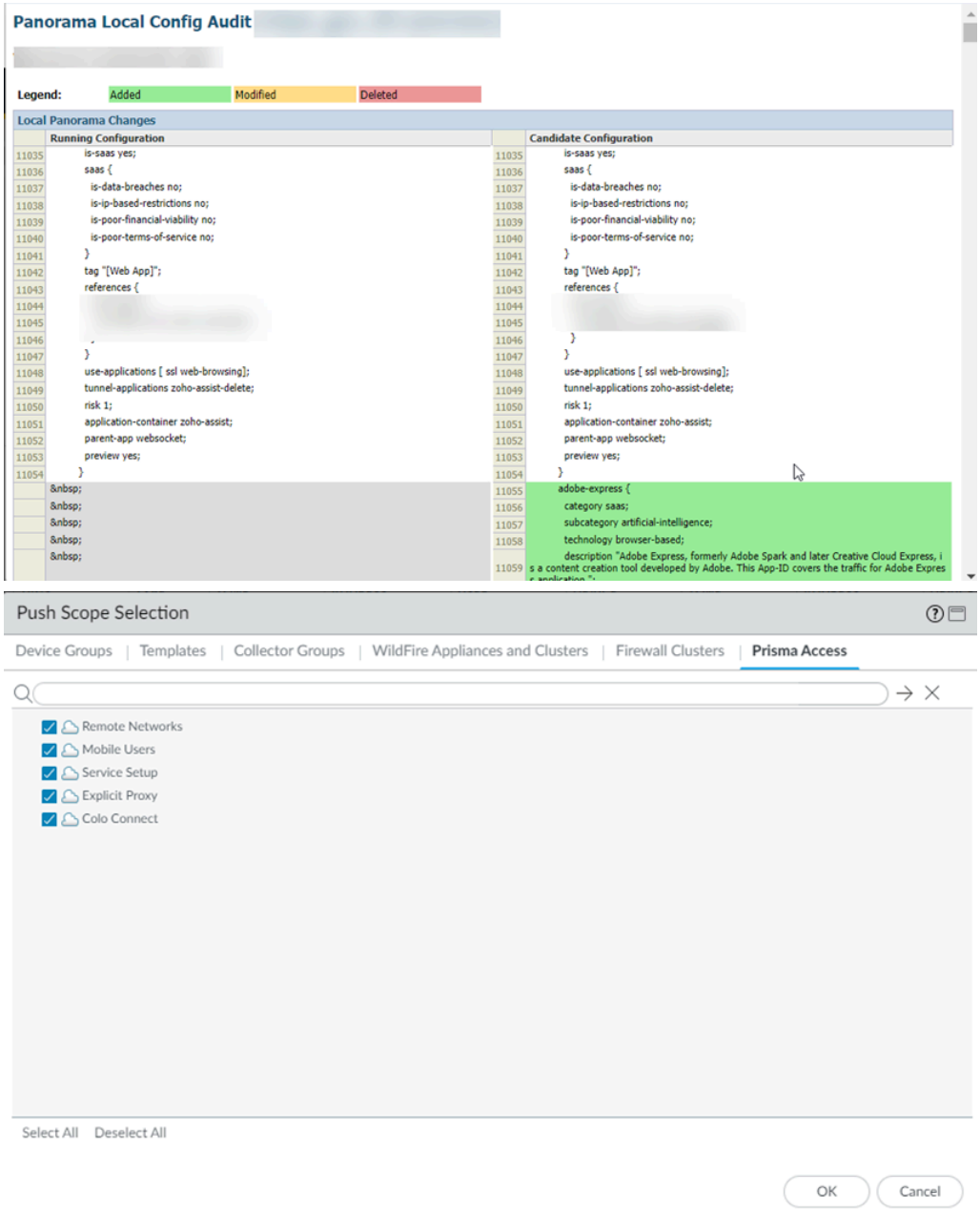
1. Prisma Accessを管理するPanoramaに、スーパーユーザーロールが割り当てられた管理者アカウントでログインします。
2. （任意）PanoramaとPrisma Access用にカスタムマスター キーを設定した場合は、そのことをメモしておいてください。

   デプロイメントでデフォルトのマスター キーを使用する場合、この手順は必要ありません。
3. 現在の Panorama設定が最新であり、PanoramaとPrisma Accessにすべての変更をコミットしてプッシュしていることを確認してください。これを行うには、**[Commit (コ**

©2025 Palo Alto Networks, Inc.

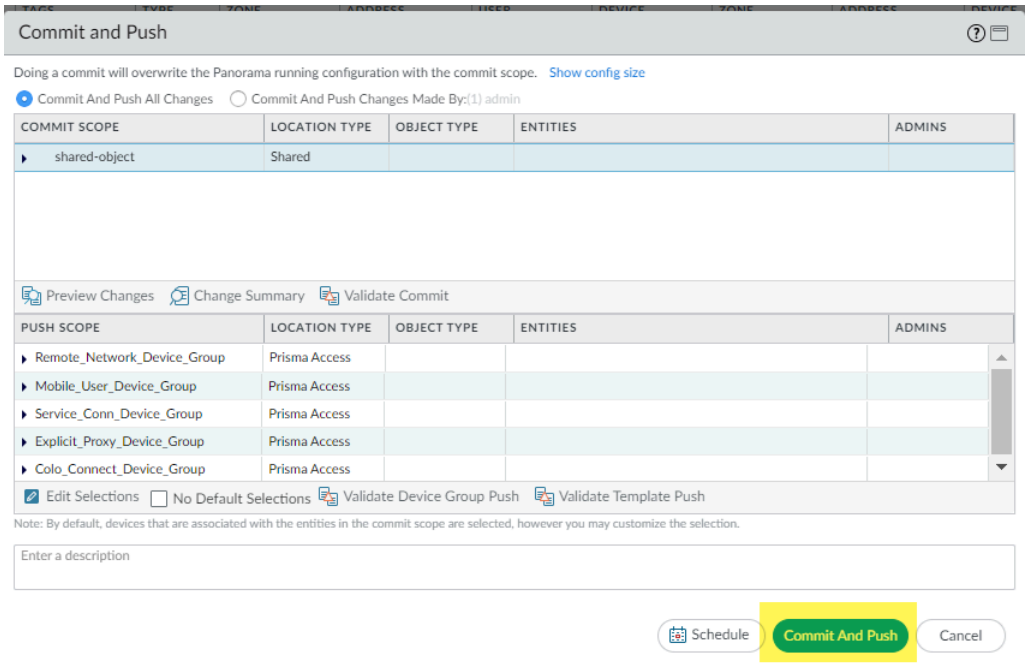
ミット)] > **[Commit & Push (コミットとプッシュ)]** と **[Preview Changes (変更のプレビュー)]**へと移動します。

4. (任意) 実行中の設定と候補の設定の差分を確認し、それらの変更をプッシュするかどうかを決定します。変更をコミットしてプッシュしたい場合は、選択範囲を編集し、プッシュスコープでプッシュしたいPrisma Accessコンポーネントを選択します。



5. (任意) 変更内容を、**Commit and Push**（コミットしてプッシュ）します。

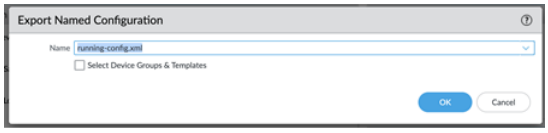
©2025 Palo Alto Networks, Inc.



6. **[Panorama]** > **[Setup (セットアップ)]** > **[Operations (オペレーション)]** に移動し、 名前付き**Panorama**構成スナップショットをエクスポートします。

   この.xmlファイルは、移行プロセス中にStrata Cloud Managerにアップロードするために必要です。テクニカルサポート ファイルや**.xml**構成ファイル以外のファイルをアップロードしないでください。

7. **running-config.xml** 構成ファイルを選択し、**[OK]** をクリックします。

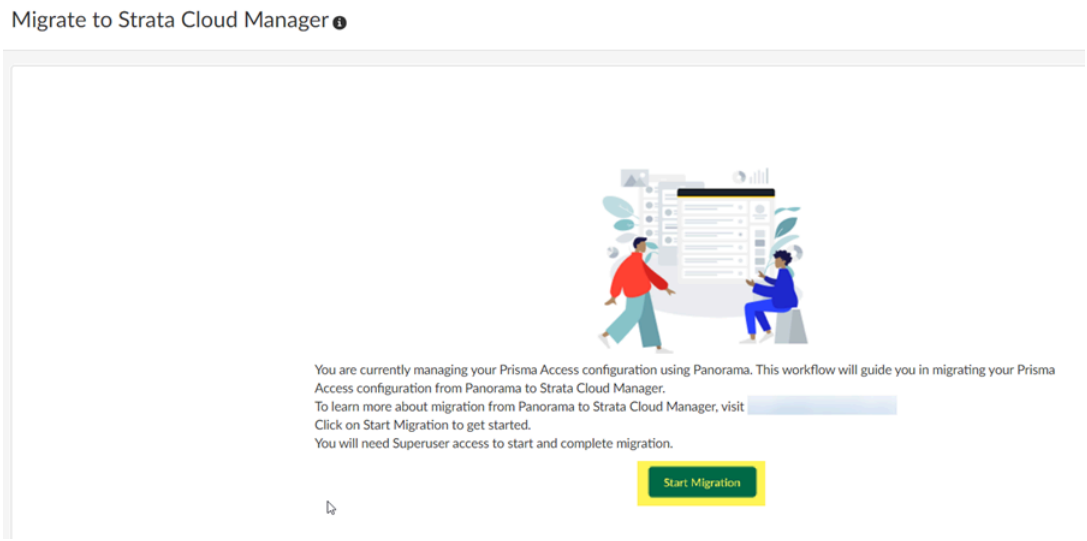


STEP 2 | スーパーユーザー ロール を持つ管理者としてStrata Cloud Managerにログインし、**[Manage (管理)]** > **[Configuration (設定)]** > **[NGFWとPrisma Access]**に移動します。

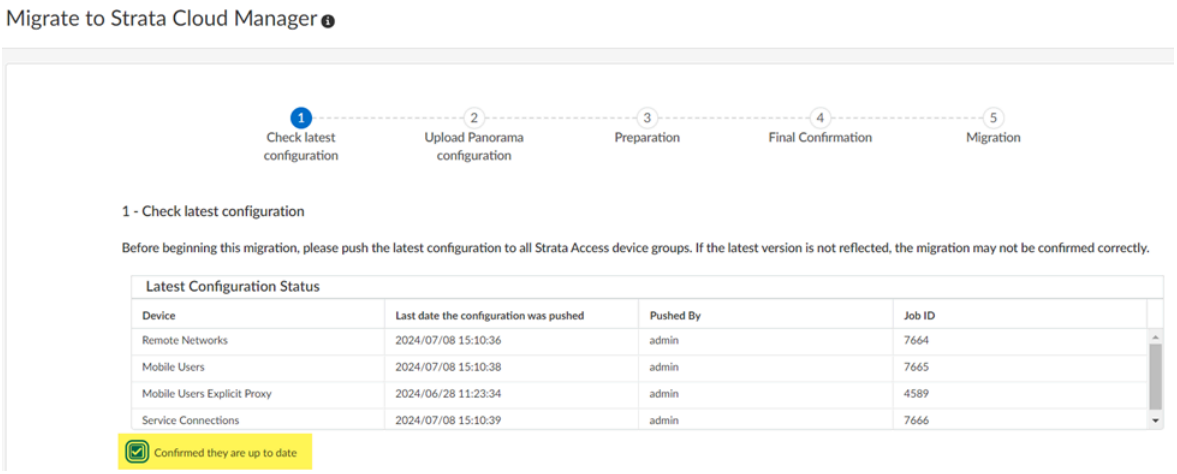
移行プログラムは、Panoramaによって管理されたデプロイメントがあることを検出します。

©2025 Palo Alto Networks, Inc.

STEP 3 | 移行を開始します。



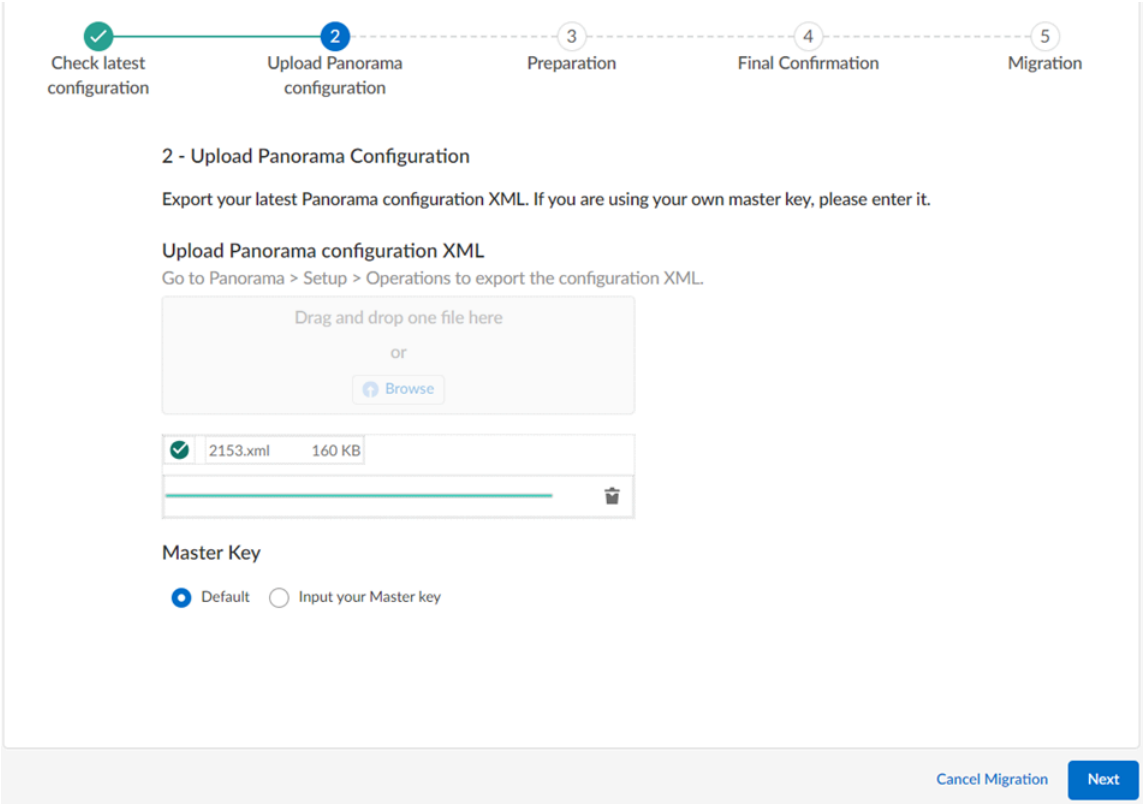
STEP 4 | 移行プログラムは、構成が最新であることを確認するように要求し、構成を最後に更新したユーザーを表示します。この構成に最新の変更が含まれていることを確認したら、**[Confirmed they are up to date (**最新であることを確認しました**)]** を選択し、**[Next (**次へ**)]**をクリックします。



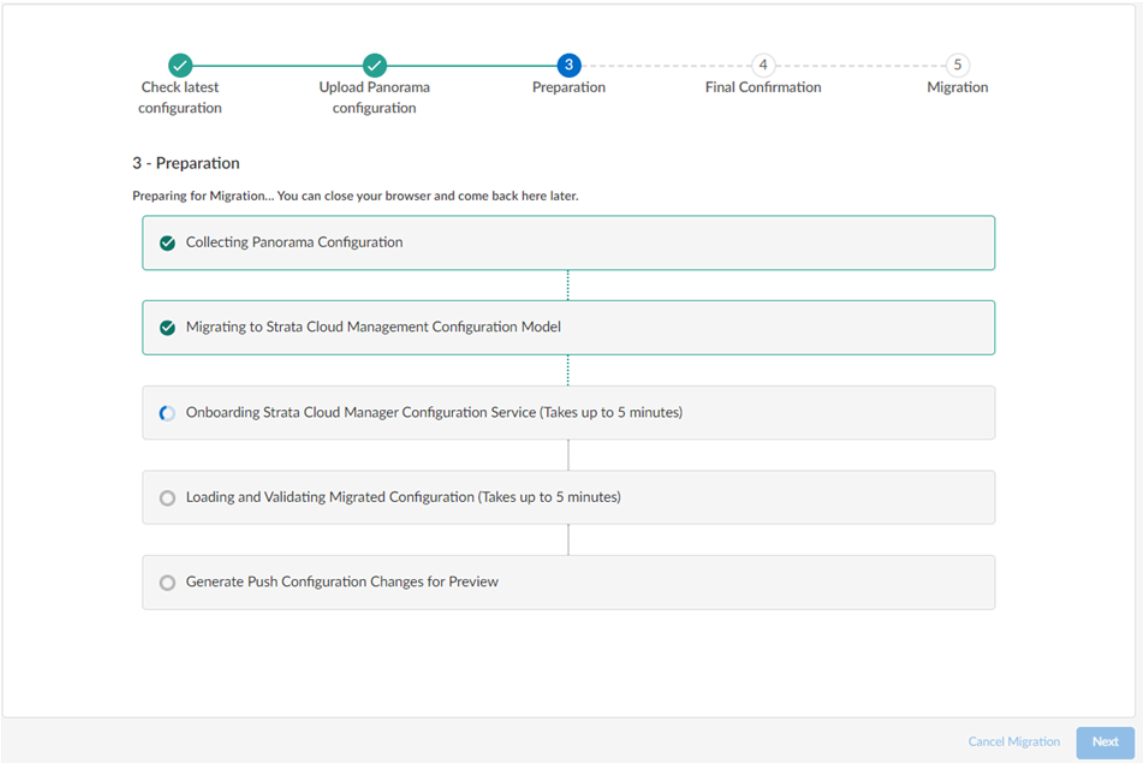
STEP 5 | 前のステップでダウンロードした Panorama 設定 .xml ファイルをドラッグ & ドロップするか、ファイルを選択します。

 ©2025 Palo Alto Networks, Inc.

STEP 6 | マスターキーを入力するか、カスタム マスターキーを作成していない場合は、 Strata Cloud Managerにデフォルト のものを使用するように要求し、[次へ]をクリックします。



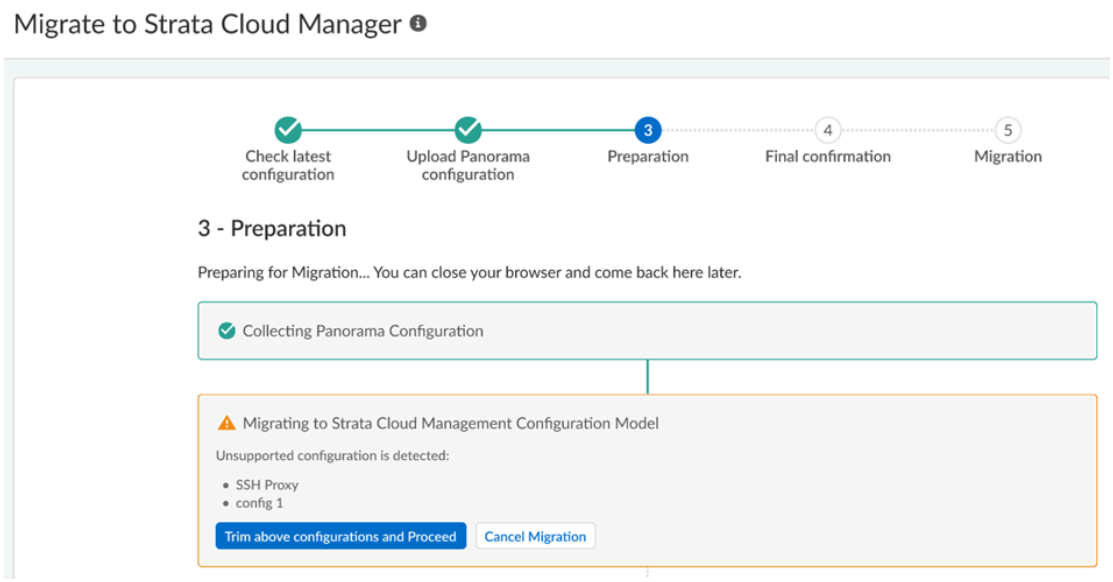
移行プログラムが始まります。



©2025 Palo Alto Networks, Inc.

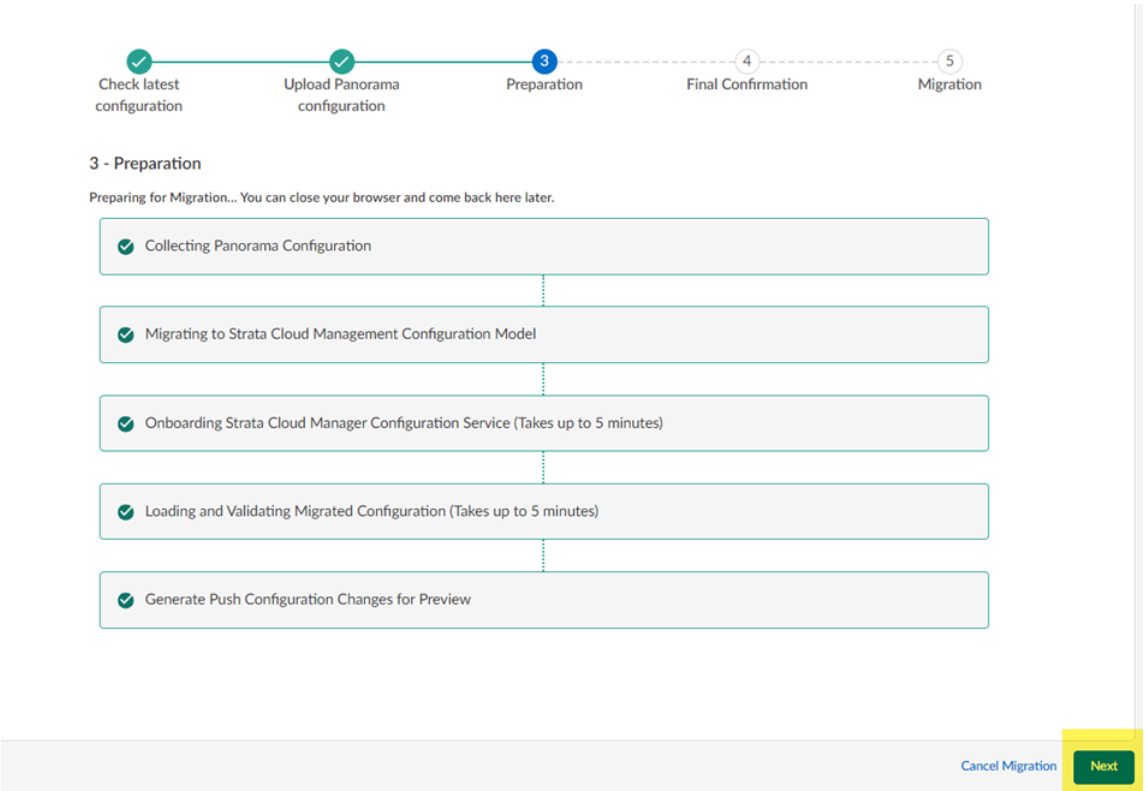
すべての手順が完了するまでお待ちください。

STEP 7 | 移行中に、プログラムが サポートされていない構成に遭遇したことを示した場合、 上記の構成をトリミングして続行する か、 移行をキャンセルすることができます。



サポートされていない構成 (マルチテナント構成など) によっては移行がキャンセルされ、移行プログラムで問題を解決できない場合があります。この場合は、 移行をキャンセルします。

STEP 8 | 移行が完了したら、[次へ]をクリックします。



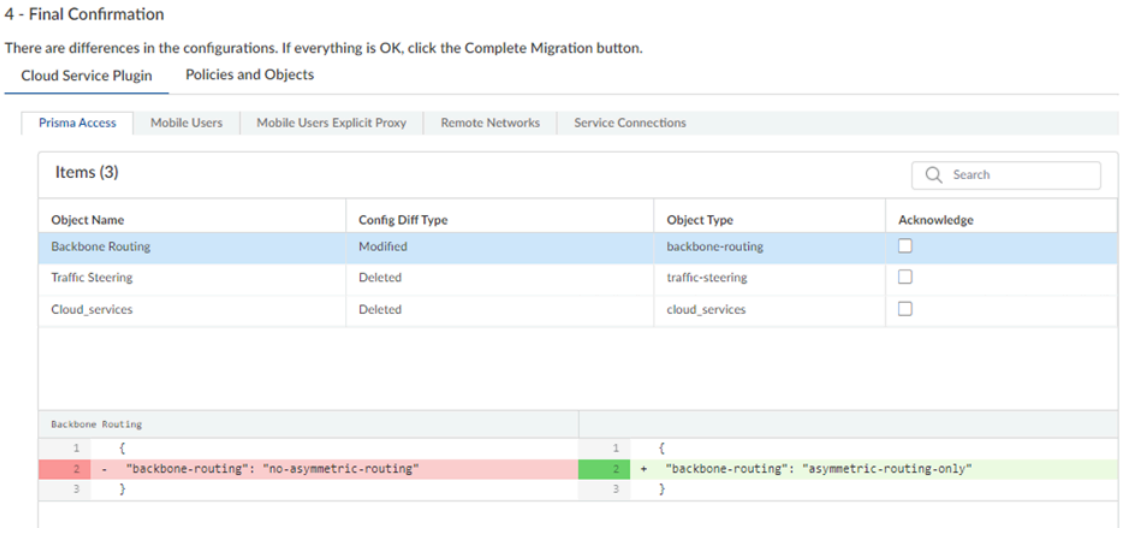
©2025 Palo Alto Networks, Inc.

STEP 9 | 移行プログラムによって変更が加えられた場合は、最終確認画面で変更内容を確認します。

移行プログラムは、PanoramaとStrata Cloud Managerの構成の違いを考慮したり、サポートされていない機能を修正するために、あなたの構成に変更を加えるかもしれません。変更が必要な場合、移行プログラムはそれらの変更を差分ビューに表示し、新しい行は緑色、削除された行は赤色で表示します。

次のオブジェクト名を示す差分は無視してください。これらは構成に影響しません。

- クライアントレス *VPN* 暗号化設定
- ヒッププロファイルの名前変更
- モバイルユーザーの冗長性
- 動画トラフィックを除外



STEP 10 | (任意) 差分に変更を加えます。

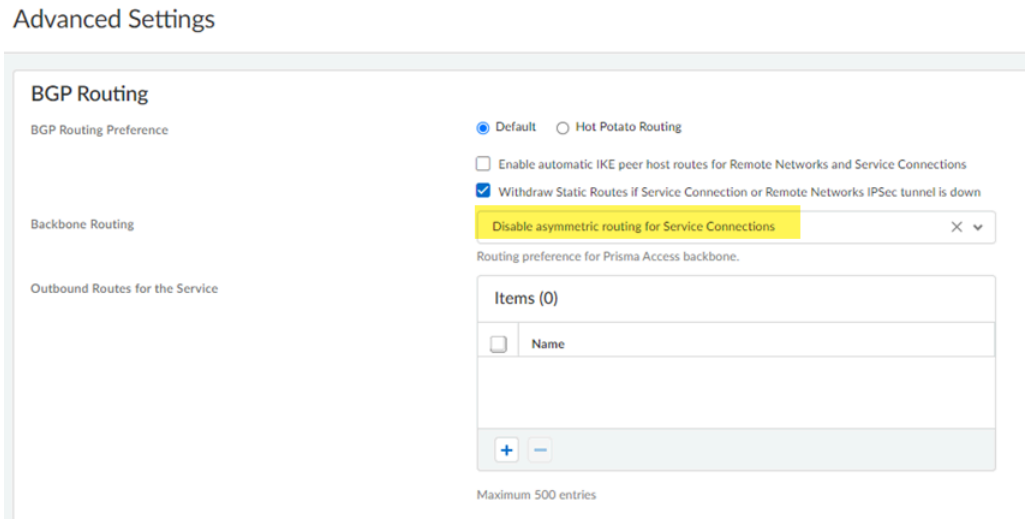
移行を完了し、変更を Strata Cloud Manager にプッシュするまで、変更は構成にコミットされません。

1. Prisma Access構成内で差分を見つけた領域に移動し、構成を変更します。

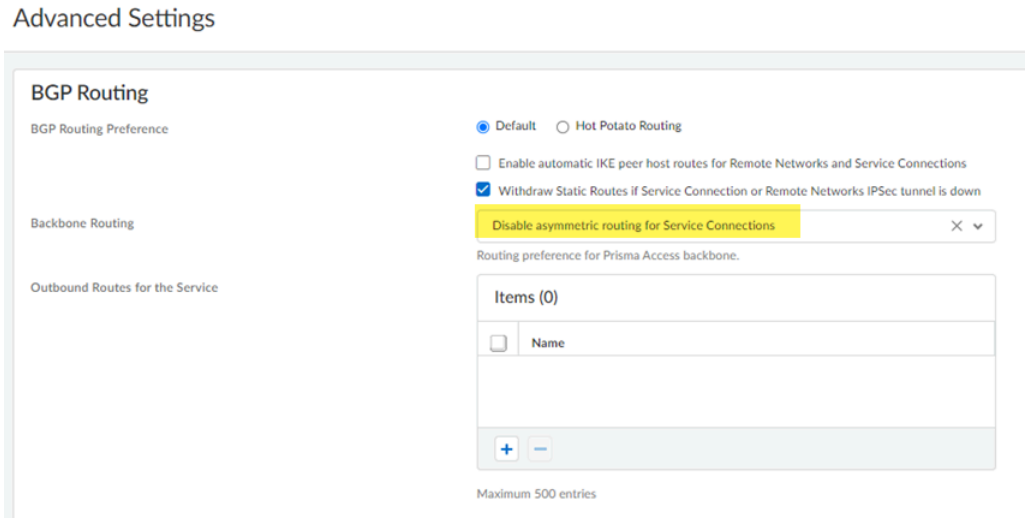
   前の手順の例では、移行プログラムによってバックボーン ルーティングが変更されました (**no-asymmetric-routing** から **asymmetric-routing-only**へ)。この設定を元の構成に戻すには、 **Workflows (ワークフロー) > Prisma Access**セットアップ > サービス接続 > 詳細設定 > に進みます。 次に、バックボーン ルーティング 構成を **[Disable**

©2025 Palo Alto Networks, Inc.

Asymmetric Routing for Service Connections (サービス接続の非対称ルーティングを無効にする**)]**に変更します。



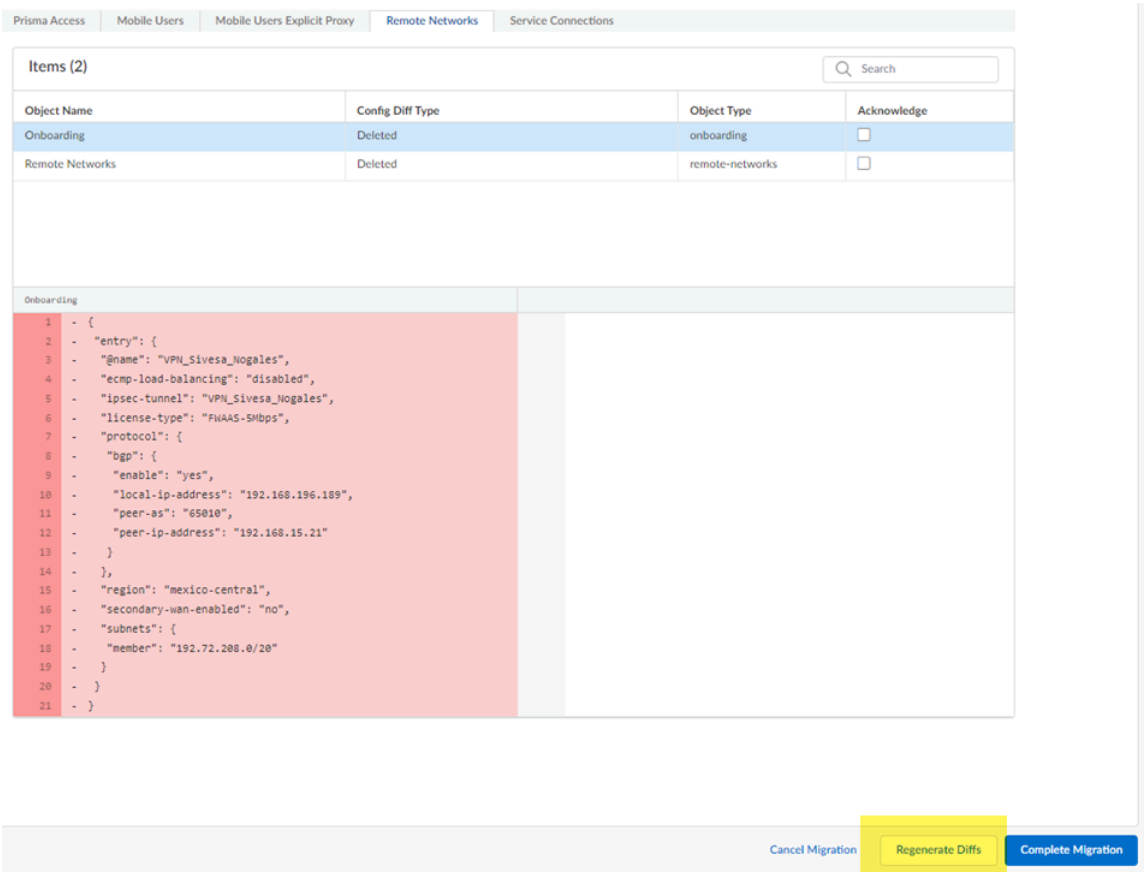
2. (任意) 変更を追跡するには、変更が完了したら変更を確認します 。
   必須ではありませんが、変更を行ったら変更内容を確認して追跡できるようにしておくと便利です。



3. 引き続き変更を確認し、変更を加えて承認します。

 ©2025 Palo Alto Networks, Inc.

STEP 11 | (任意) 構成に変更を加えた場合は、 差分を再生成して 更新された差分を表示します。

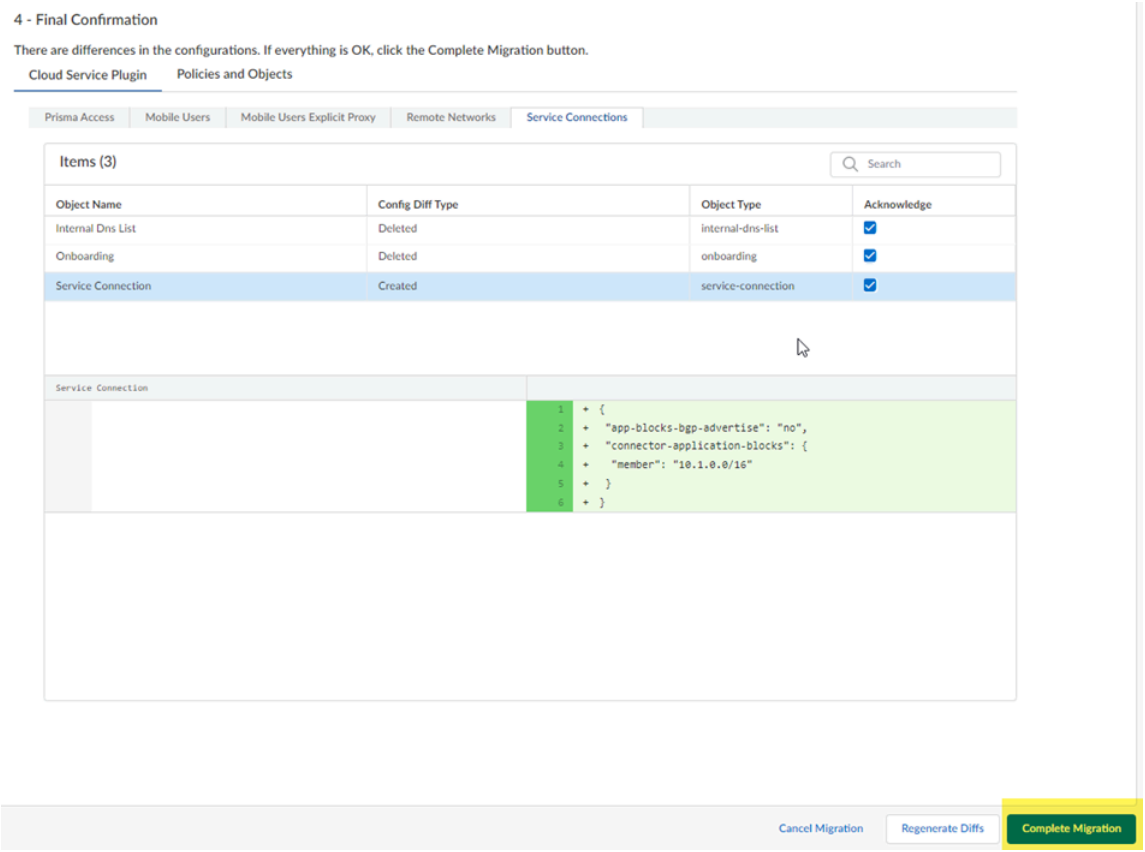


 ©2025 Palo Alto Networks, Inc.

STEP 12 | 移行を完了します。

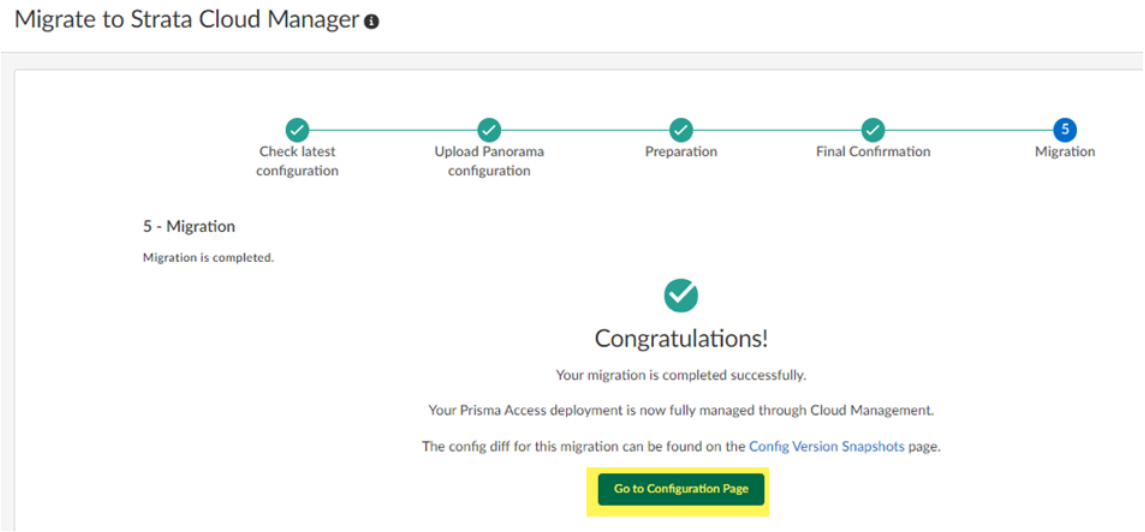
必須ではありませんが、変更を承認すること もできます。

移行を完了すると、**Panorama**管理の展開に戻ることはできず、デプロイメントでは、その管理に**Strata Cloud Manager**が永続的に使用されます。

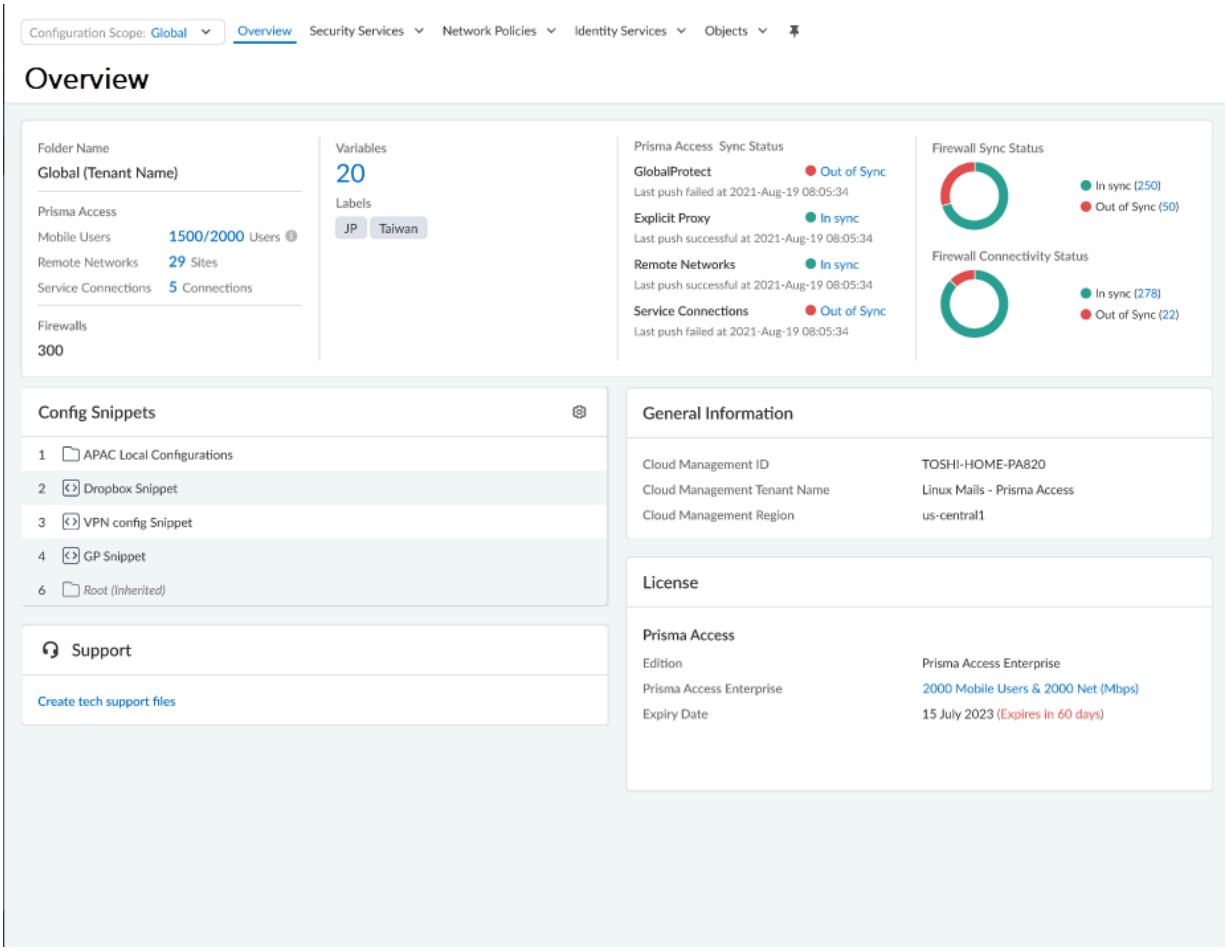


©2025 Palo Alto Networks, Inc.

STEP 13 | (任意) 移行した構成を確認するには、 構成ページに移動します 。



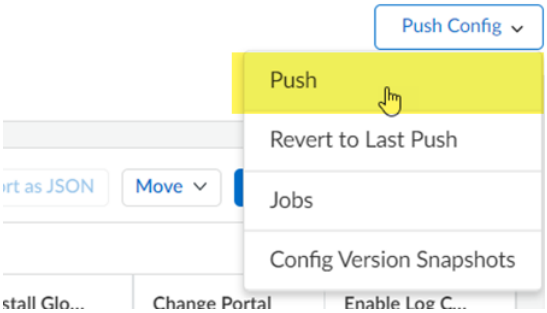
移行されたデプロイメントが表示されます。



 ©2025 Palo Alto Networks, Inc.

STEP 14 | 移行した構成の変更を適用するには、 **[Push Config (設定をプッシュ)]** > **[Push (プッシュ)]**を実施します 。

このプッシュ操作により、移行が正常に完了し、Prisma Accessが移行した構成にすべての変更を適用したことが確認されます。



STEP 15 | プッシュ操作中に受信したメッセージを書き留め、問題が見つかった場合は必要に応じて設定を変更します。

©2025 Palo Alto Networks, Inc.

Prisma Accessリリースとアップグレード

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス

Prisma Accessのリリースとアップデートにより、常に最新の状態を維持し、ユーザーを保護することができます。Prisma Accessインフラなど一部のアップデートはPalo Alto Networksが管理しており、それに対応するための詳細な通知がお客様に送信されます。その他のアップデートについては、お客様自身が確認する必要があり、できる限り早い時期に指定されているバージョンのコンテンツアップデート、ソフトウェアアップデート、およびプラグインバージョンのアップデート（必要な場合）をスケジュールする必要があります。

https://sase.status.paloaltonetworks.com/*Web*サイトにアクセスすれば、*Prisma Access*や*Strata Logging Service*を含むすべてのクラウド・サービスのステータスを、各サービスの稼働時間の履歴とともに取得することができる。またこのサイトにサインアップして、インフラ更新が計画された時の通知、および更新発生時、*Palo Alto Networks*がインシデントを作成、更新、または解決した時のリアルタイム通知に関する、メールやテキストメッセージを参照することもできます。

Prisma Access リリースタイプ

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス

Prisma Accessには、リモート ネットワークやモバイル ユーザーに最高のセキュリティを提供するための新機能や最適化を含む、メジャー リリースやインフラ メンテナンスを含むアップグレードがあります。

次のリストは、リリースの種類と、各リリースについて提供される事前通知を定義します。すべてのリリースの通知を確実に受け取るには、Prisma Accessウェブサイト(https://sase.status.paloaltonetworks.com/)で電子メールまたはテキスト通知を登録して、Strata Cloud Managerのアラートに登録してください。

- メジャー リリース- メジャー リリースには通常、重要な新機能と最適化が含まれており、このような更新はPalo Alto Networksによって設定された計画されたメンテナンス ウィンドウを使用してプッシュされます。Palo Alto Networks は、このような計画されたメンテナンス活動を、sase.status.paloaltonetworks.comを通じて電子メール通知で顧客に通知します。

  通知– Palo Alto Networksは、メジャー リリースに関して次の通知を提供します。

デプロイメント タイプ	通知期間
実稼働環境への導入	Palo Alto Networksはメジャーリリースの21日前に通知を提供します。
ラボ デプロイメント	Palo Alto Networksはメジャーリリースの7日前に通知を提供します。

スケジュールされたメジャー リリース アップグレードに加えて、*Palo Alto Networks* では、別のスケジュールに従う 緊急のスケジュールされたアップグレードを実行する必要がある場合があります。

ラボ テナントは、Prisma Accessサービス レベル アグリーメント（SLA）の対象外であり、顧客は、本番前のテストと検証の目的でのみテナントを使用するよう強く推奨されています。

©2025 Palo Alto Networks, Inc.

- インフラストラクチャのメンテナンス- 増分機能と最適化が含まれます。場合によっては、Palo Alto Networksはホットフィックスとインフラストラクチャのメンテナンスを組み合わせることがあります。

  通知– Palo Alto Networks は次の通知を提供します。

デプロイメント タイプ	通知期間
実稼働環境への導入	Palo Alto Networks は、インフラストラクチャのメンテナンスの10日前に通知を提供します。
ラボ デプロイメント	Palo Alto Networks は、インフラストラクチャのメンテナンスの7日前に通知を提供します。

  スケジュールされたメジャー リリース アップグレードに加えて、*Palo Alto Networks* では、別のスケジュールに従う 緊急のスケジュールされたアップグレードを実行する必要がある場合があります。

- クラウドサービスプラグインリリース（**Panorama**管理デプロイメントのみ） – Prisma Accessに新しいプラグインが必要な場合は、リリースの一般提供 (GA) 日にPalo Alto Networksカスタマー サポート ポータル (CSP)およびPanorama からダウンロードできるようになります。

  Prisma Accessは下位互換性とサポートされているソフトウェア バージョンを維持するために、すべてのテナントを特定の Cloud Services プラグイン バージョンに強制的にアップグレードする場合があります。このような強制活動では、プラグインのアップグレードを計画するために、**14**日前に通知 が提供されます (sase.status.paloaltonetworks.comページ経由)。このサービスでは、最新のプラグインがダウンロード可能になったらすぐにアップグレードすることを強くお勧めします。

緊急スケジュールアップグレード

Palo Alto Networksでは、ホットフィックスや緊急のバグ修正 (ゼロデイ脅威の修正やプラグインの変更など) を含む緊急のデータプレーンまたはインフラストラクチャのアップグレードを時々実行する必要があります。Palo Alto Networks は、緊急に予定されているアップグレードの48時間前に通知できるよう最善を尽くしますが、緊急に予定されているアップグレードについては、より短い通知期間が提供される場合もあります。

©2025 Palo Alto Networks, Inc.

Prisma Accessアップグレードタイプ

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス

Palo Alto Networksはクラウドベースのインフラを、お客様の手間を煩わせることなくアップグレードします。アップグレードによっては、新しいプラグインのインストールなど、何らかのアクションを実施する必要がある場合もあります。

以下のリストは、Prisma Accessのアップグレードの種類を記載したものです：

- インフラストラクチャのアップグレード – Palo Alto Networksは、基盤となるサービスバックエンド、オーケストレーション、監視インフラストラクチャを含む、Prisma Accessインフラストラクチャ(Prisma Accessコントロールプレーンとも呼ばれる)をアップグレードします。

  年に4～6回、インフラストラクチャのアップグレードを受けることが期待できます。
- データプレーンのアップグレード–Palo Alto Networksが、ネットワークおよびユーザートラフィックのトラフィック検査とセキュリティ ポリシーの適用を可能にする、Prisma Accessデータプレーンのアップグレードを行います。

  アプリケーションを使用して、データプレーンのアップグレード電子メールアラート通知にサインアップし、アップグレード設定を指定します。
- **Prisma Access定期メンテナンス** – Prisma Accessは、インフラストラクチャのホットフィックスや緊急バグ修正に関連するメンテナンスを2週間ごとに予約しています。
- (Panoramaマネージドデプロイメントのみ) クラウドサービスプラグインのアップグレード – 新しいプラグインリリースが利用可能になったら、ネットワーク管理者は管理を行うパノラマアプライアンス上のクラウドサービスプラグインをアップグレードする必要があります。Prisma Access
- (Panoramaマネージドデプロイメントのみ) **Panorama**ソフトウェアバージョンアップグレード – Prisma Accessとの互換性を維持するために、Panoramaソフトウェアのアップグレードが必要になる場合があります。

以下の表は、各リリースに含まれる内容と、弊社が提供するメンテナンス ウィンドウ、およびPrisma Accessサービスへの影響を示したものです。

アップグレードタイプ	メンテナンス期間	影響
インフラのアップグレード	2 ～ 8 時間	ネットワークトラフィックへの影響はありませんが、メンテナンス期間中はコミットを実行することができません。

©2025 Palo Alto Networks, Inc.

アップグレードタイプ	メンテナンス期間	影響
		Palo Alto Networksはビジネスへの影響を最低限に抑えられる現地時刻に、アップグレードをスケジュールします。
データプレーンのアップグレード	72時間	Palo Alto Networksは、この期間を使用して、すべての顧客のデータプレーンをアップグレードします。この期間中には、変更を行ってコミットすることができます。当社の目標はネットワークトラフィックへの影響を最低限に抑えることにありますが、場合によっては短時間の中断が発生することがあります。詳細については Prisma Accessデータプレーンのアップグレードを参照してください。 アプリを使用して、データプレーンのアップグレードの電子メールアラート通知にサインアップし、アップグレードの希望時間帯を含むアップグレード設定を指定します。
クラウド サービス プラグインのアップグレード (Panoramaマネージド デプロイメントのみ)	プラグインが利用可能になったらインストールします。	Prisma Accessは下位互換性とサポートされているソフトウェアバージョンを管理するうえで、すべてのテナントを特定のプラグインバージョンにアップグレードする必要がある場合があります。 プラグインのアップグレード中、Panoramaで設定の変更とコミットを行うことはできません。
Panoramaソフトウェアバージョンアップグレード (Panoramaマネージド デプロイメントのみ)	Prisma Accessを管理するPanoramaでアップグレードをスケジュールして実行します。	メジャーリリース後にPrisma Accessがインフラとデータプレーンをアップグレードする場合、アップグレードが前のバージョンのPanoramaと

©2025 Palo Alto Networks, Inc.

アップグレードタイプ	メンテナンス期間	影響
		互換性がない可能性があります。Prisma AccessおよびCloud Servicesの頻繁なリリースにより、Panoramaのソフトウェア互換性（サポート終了）の日付がPanoramaリリースのソフトウェア寿命の日付よりも短く、Panoramaバージョンの互換性がPrisma Accessのみに適用されます。Prisma Accessと併用する場合のPanoramaのサポート終了日などの詳細については、[Palo Alto Networks Compatibility Matrix (Palo Alto Networksの互換性マトリックス)]のPrisma AccessとPanoramaのバージョンの互換性を参照してください。

©2025 Palo Alto Networks, Inc.

Prisma Accessのソフトウェアおよびコンテンツアップデートの頻度

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス

- Strata Cloud Manager
- Panorama

Prisma Access (Managed by Strata Cloud Manager)のソフトウェアおよびコンテンツアップデートの頻度

次の表は、Prisma Accessがコンテンツやソフトウェアの更新を含むインフラストラクチャ コンポーネントを更新する方法を示しています。この表には、Prisma Accessがソフトウェアを自動的に更新するかどうかも示されています。更新が自動的に行われない場合は、それらのインフラストラクチャの更新を適用する方法を確認できます。

また、ハブからすべてのクラウドサービスのステータスを確認することもできます。

コンポーネント	スケジュールの更新	コメント
GlobalProtectアプリ	• **GlobalProtect**アプリのメジャーリリース（例：***x*.0**または**4.*x***）—Prisma Accessは、リリースの*x*.0.1バージョンが全般的に利用できるようになってから7～10日後に、最新のリリースでアプリケーションを更新します。 たとえば、アプリのリリースが 4.0 の場合、 Prisma Accessは4.0.1リリースの7日から10日後にアプリケーションを更新します。 • **GlobalProtect**アプリのマイナーリリース（例：**4.1.*x***）—Prisma Accessは当該リリースが全般的に利用できるようになってから、7～10日後にアプリケーションを最新のマイナーリリースに更新します。	クラウドは、アップグレード可能なアプリのバージョンを制御します。

©2025 Palo Alto Networks, Inc.

コンポーネント	スケジュールの更新	コメント
インフラにおけるPAN-OSソフトウェアのアップグレード–予定	Palo Alto Networks® は、Prisma Accessの新しいバージョンがリリースされると、PAN-OSインフラストラクチャをアップグレードします。Palo Alto Networksでは®、アップグレード予定日の3週間前にお知らせします。	インフラストラクチャに関するアップグレードのお知らせを電子メールまたはテキストで受け取るには、 Hubにご登録ください。
アプリケーションと脅威のアップデート	毎日24時間単位で Palo Alto Networks®は、毎月第3火曜日に新しいApp-IDをリリースします。これらの新しいApp-IDは、24時間以内に確認、導入するように計画してください。このトラフィックに与える影響を最小限に抑えるために、新しいApp-IDフィルタを使用してください。 新しいアプリID特性を使用すると、ネットワーク上の新しいアプリケーションを表示し、新しく分類されたアプリケーション アクティビティの詳細を表示できます。ここでの学習内容は、最近分類された App-ID を実施するためにセキュリティ ポリシーを更新する方法についての正しい決定を下すのに役立ちます。	
アンチウィルス保護	毎時間、当該時間の10分後	Prisma Accessは、常に最新のアンチウィルスリリースで更新されています。
WildFire	リアルタイム	Prisma Accessは、常に最新のWildFireリリースで更新されています。
GlobalProtect データファイル	毎時間	Prisma Accessは、常に最新のGlobalProtectデータファイルリリースで更新されています。
クライアントレス VPN アプリケーション シグネチャ	毎時間	Prisma Accessは、常に最新のClientless VPNアプリケーションシグネチャリリースで更新されています。

©2025 Palo Alto Networks, Inc.

Prisma Access (Managed by Panorama)のソフトウェアおよびコンテンツアップデートの頻度

最新のアプリケーションと脅威シグネチャを入手して、Palo Alto Networksが提供する脅威防御機能を活用するために、ソフトウェアおよびコンテンツのアップデートを次の表に示します。**Cloud Controlled? (**クラウドが管理しているか？**)**カラムの属性が「**No**」の場合、コンポーネントを更新するために必要なアクションを実行します。

コンポーネント	スケジュールの更新	クラウドが管理しているか？（はい/いいえ）	コメント

Prisma Accessとの互換性を維持するためのPanoramaソフトウェアのアップグレード	Prisma Accessのメジャーリリースの場合、次の使用事例においてPanoramaのバージョンをアップグレードしなければならないことがあります。
	• 必要なアップグレード–場合によっては、Prisma Accessとの互換性を維持するために、Panorama のソフトウェア バージョンをアップグレードする必要があります。
	  • メンテナンス期間–Panoramaソフトウェアのバージョンをアップグレードするために、メンテナンス期間をスケジュールする必要があります。
	  • 影響–Panoramaのバージョンをアップグレードしないと、新し
		いいえ	Panoramaバージョンが Prisma Accessと互換性がなくなる時期については、「Prisma Accessとの Panoramaソフトウェア バージョンの互換性のサポート終了 (EoS) 日」を参照してください。Prisma Accessで使用できる現在サポートされているPanoramaバージョンについては、「Prisma AccessとPanoramaバージョンの互換性」を参照してください。Panoramaの新しいバージョンへのアップグレード方法については、Panoramaのコンテンツ更新とソフトウェア更新のインストールを参照してください。

©2025 Palo Alto Networks, Inc.

コンポーネント	スケジュールの更新	クラウドが管理しているか？（はい/いいえ）	コメント
	いバージョンのプラグインを使用できません。 • 通知—Palo Alto Networksは、スケジュールされているメジャーリリースアップグレードの100日前に通知を行います。 • オプションのアップグレード—その他の事例として、Prisma Accessのメジャーリリースでサポートされている新機能を使用するために、Panoramaソフトウェアバージョンのアップグレードが必要なことがあります。 • メンテナンス期間—Panoramaソフトウェアのバージョンをアップグレードするために、メンテナンス期間をスケジュールする必要があります。 • 影響—Panoramaをアップグレードしないと、Prisma Accessがサポートしている新機		

©2025 Palo Alto Networks, Inc.

コンポーネント	スケジュールの更新	クラウドが管理しているか？（はい/いいえ）	コメント
	能を使用できません。 • 通知—Palo Alto Networksは、Prisma Access リリースタイプに定義されているスケジュールされたメジャーリリースアップグレードの21日前に、Panoramaの要件について通知します。		
Cloud Servicesプラグインのバージョン	プラグインのリリース後に利用できます。	不要	プラグインをアップグレードするための作業を実行します。Prisma Accessがプラグインのバージョンを更新するタイミングの詳細については、Prisma Access リリースタイプを参照してください。Panoramaアプライアンスでプラグインをアップグレードする方法については、「Cloud Servicesプラグインのアップグレード」を参照してください。
GlobalProtectアプリケーション	• **GlobalProtect**アプリケーションのメジャーリリース（例：**x.0**または**5.*x***）—Prisma Accessは、リリースのx.0.1バージョンが全般的に利用	あり	クラウドが、アップグレードに利用できるアプリケーションのバージョンを管理します。ただし、提供するアプリケーションの異なるバージョンを選択

©2025 Palo Alto Networks, Inc.

コンポーネント	スケジュールの更新	クラウドが管理しているか？（はい/いいえ）	コメント
	できるようになってから7～10日後に、最新のリリースでポータル上のエージェントを更新します。 たとえば、エージェントリリース5.1の場合、Prisma Accessは5.1.1のリリース後7～10日間でポータルのエージェントを更新します。 • **GlobalProtect**アプリケーションのマイナーリリース（例：**5.1.*x***）—Prisma Accessは当該リリースが全般的に利用できるようになってから、7～10日後にポータル上のエージェントを最新のインフラストラクチャ管理に更新します。		し、エンドユーザーにGlobalProtectアプリケーションのアップデートを公開する時期や方法を指定することができます。詳細はGlobalProtectアプリケーションのアップグレード を参照してください。 Prisma AccessデプロイメントでGlobalProtectアプリケーションのHotfixが必要な場合は、Palo Alto Networksテクニカルサポートにサポートケースを開いてサポートを受けてください。
アプリケーションと脅威のアップデート	毎日24時間単位で Palo Alto Networks®は、毎月第3火曜日に新しいApp-IDをリリースします。これらの新しいApp-IDは、24時間以内に確認、導入するように計画してください。 新しいアプリID特性を使用すると、ネッ	あり	

©2025 Palo Alto Networks, Inc.

コンポーネント	スケジュールの更新	クラウドが管理しているか？（はい/いいえ）	コメント
	トワーク上の新しいアプリケーションを表示し、新しく分類されたアプリケーション アクティビティの詳細を表示できます。ここでの学習内容は、最近分類された App-ID を実施するためにセキュリティ ポリシーを更新する方法についての正しい決定を下すのに役立ちます。		
アンチウィルス保護	毎時間、当該時間の10分後	あり	Prisma Accessは、常に最新のアンチウィルスリリースで更新されています。
WildFire	リアルタイム	あり	Prisma Accessは、WildFireパブリッククラウドで WildFireシグネチャが生成されるとすぐに、新しく検出されたマルウェアのWildFireシグネチャを取得できます。
GlobalProtect データファイル	毎時間	あり	Prisma Accessは、常に最新のGlobalProtectデータファイルリリースで更新されています。
Clientless VPNアプリケーション署名	毎時間	あり	Prisma Accessは、常に最新のClientless VPNアプリケーションシグネチャリリースで更新されています。

©2025 Palo Alto Networks, Inc.

Prisma Accessデータプレーンのアップグレード

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

*Prisma Access (Managed by Strata Cloud Manager)*ではユーザーの介入を必要とせずに、データプレーンのアップグレードが自動的に実行されます。

Prisma Accessはサービス上でデータプレーンのアップグレードを実行し、組織のエンドユーザー、ビジネス資産、デジタル変革を保護するための新しいセキュリティ機能と機能を提供します。Prisma Accessの新バージョンでデータプレーンのアップグレードが必要な場合、アップグレードの前に、アップグ レードプロセスの仕組みを理解し、必要な前提条件を整えておく必要があります。

データプレーンは年に 1 ～ 2 回アップグレードされる予定です。リリースによっては、必要なデータプレーン アップグレードに加えて、それを必要とするPrisma Access機能をサポートするためのオプションのデータプレーン アップグレードを提供する場合があります。

- データプレーンのアップグレードの概要
- データプレーンのアップグレード例

データプレーンのアップグレードの概要

Prisma Accessでは、お客様のデータプレーンを週末の2日間に2回に分けてアップグレードします。 Strata Cloud Managerを使用してアップグレードに関する情報をお知らせします。大まかに言えば、アップグレード プロセス中に次の手順が実行されます。

- Strata Cloud Managerからの電子メール通知は、データプレーンのアップグレード開始予定日の21日前に届きます。この電子メール通知には、フェーズ1のデータプレーン アップグレードの開始日が記載されています。

  *Strata Cloud Manager*に*21*日前の日付が表示されることがありますが、この日付は*21*日前の通知を受け取るまで確定しない可能性があります。

©2025 Palo Alto Networks, Inc.

- 電子メールでは、最初にアップグレードするロケーションと、Strata Cloud Managerを通じてアップグレードを希望する時間帯を選択し、送信するよう求められます。

  特定のテナントに対して、アップグレードする最初の場所と時間枠を複数回変更して送信できます。予定開始日の7日前に行われた最後の送信が、アップグレードのためにサービスによって選択されます。アップグレード開始日から7日間は変更できません。

  変更を加えた場合、その変更が Insights (インサイト) のアップグレード ダッシュボードに表示されるまでに最大 30 分かかることがあります。Prisma Accessが変更を処理し完了すると、アラート電子メールで通知されます。

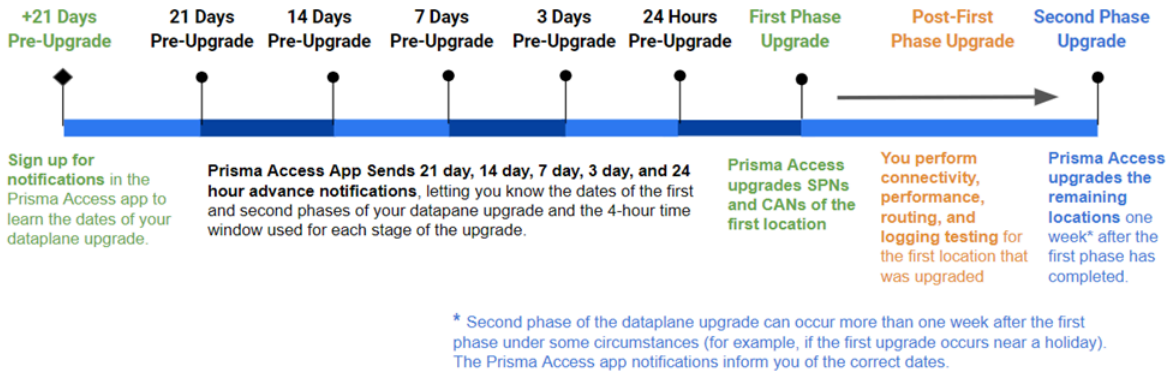
  Palo Alto Networks では、デプロイメント全体を反映する場所を選択することを強くお勧めします。たとえば、モバイル ユーザー、サービス接続、リモート ネットワーク デプロイメントがある場合は、すべてのデプロイメント タイプを含む場所を選択します。

- Prisma Accessは選択した場所または複数の場所で、それらの場所に対して選択されたローカル時間枠内にアップグレードのフェーズ1を実行します。
- 選択したアップグレード場所に、モバイル ユーザー - GlobalProtect、モバイル ユーザー - 明示型プロキシ、サービス接続、またはリモート ネットワークの組み合わせがある場合、このセクションの後半で説明するように、各デプロイメントのデータプレーンは必要なデータプレーン バージョンにアップグレードされます。
- 最初の場所でアップグレードが完了すると、Strata Cloud Managerよりメール通知が届きます。お客様はデータプレーンのアップグレード直後にサービスを監視して、新しい問題が発生しないことを確認するようお勧めします。
- 万一、新しい問題が発生した場合は、Palo Alto Networksテクニカルサポートに問題を報告してください。

  テクニカルサポートチームは問題を調査して修正措置を取ります。その際、以前のデータプレーンバージョンにロールバックさせていただく場合もあります。この決定は、テクニカルサポートケースを介してお客様に通知いたします。
- 新しい問題がない場合、または新しい問題がアップグレードとは無関係な場合、Prisma Accessは次の週末にデータプレーンのアップグレードを続行します。
- 残りの場所のアップグレードは、最初のアップグレードで選択したのと同じ時間枠 (現地時間) 内に実行されます。
- データプレーンのアップグレードが完了すると、電子メールアラートで通知されます。
- データプレーンのアップグレード後にプラグインのアップグレードが必要な場合は、データプレーンのアップグレードが完了した後に プラグインをアップグレードする ことをPalo Alto Networksは推奨します。

以下の図に、アップグレードに使用するタイムラインを示し、データプレーンのアップグレードに必要なタスク（緑色で表示）と、Prisma Accessが実行する手順を示します。

©2025 Palo Alto Networks, Inc.



次のセクションでは、データプレーンのアップグレード プロセスについて詳しく説明します。

通知にサインアップすると、 Prisma Accessはアップグレード プロセスに使用される2つの週末の日付をお知らせします。これらの通知は、アップグレードの最初のフェーズが発生する21日前、14日前、7日前、3日前、および24時間前に配信されます。IKEプロセスは、2つのフェーズで行われます。

- フェーズ1では、指定した時間枠を使用して最初の週末に選択した場所をアップグレードし、アップグレードが完了すると電子メールで通知します。最初にアップグレードする場所を選択しなかった場合、または時間帯を選択しなかった場合、Prisma Accessがあなたに代わって選択します。

  Palo Alto Networks は、*Strata Cloud Manager*で選択した*4*時間のウィンドウの間に場所のアップグレードを試みます。ただし、この時間枠の中で必要なアップグレードを完了することはベストエフォートであり、*Palo Alto Networks*はその時間枠内にロケーションがアップグレードされることを保証するものではありません。アップグレード中に問題が発生した場合、*Palo Alto Networks* は当初の*4*時間のウィンドウから*24*時間後にアップグレードを試みます。

  このため、データプレーンのアップグレードが行われる*2*つの週末のそれぞれについて、金曜日の現地時間午後*8*時から月曜日の現地時間午後*8*時までの*72*時間の変更要求ウィンドウをスケジュールする必要があります。アップグレードが完了するとメールが届きます。

Prisma Accessはアップグレードのフェーズ1中に、デプロイメントに次の変更を加えます。

デプロイメント タイプ	アップグレードされるもの
モバイル ユーザー - GlobalProtectデプロイメント:	Prisma Accessのアップグレード: • 指定したロケーションのGlobalProtectゲートウェイ (モバイル ユーザー セキュリティ処理ノード *(MU-SPN)*とも呼ばれます)。 • そのリージョンに関連付けられたGlobalProtectポータル。

©2025 Palo Alto Networks, Inc.

デプロイメント タイプ	アップグレードされるもの
モバイル ユーザー - 明示型プロキシ デプロイメント:	Prisma Accessは指定した明示型プロキシの場所の明示型プロキシ ノードをアップグレードします。
リモートネットワーク デプロイメント	Prisma Accessは、バックアップ (HA) リモート ネットワーク (リモート ネットワーク セキュリティ処理ノード *(RN-SPN)*とも呼ばれます) をアップグレードし、指定した場所のバックアップ リモート ネットワークをアクティブ ノードにします。バックアップ リモート ネットワーク接続は、すべての場所でアクティブ ノードとバックアップ ノードがアップグレードされる次の週末までアップグレードされません。 選択した場所に複数の RN-SPN がある場合、すべてのプライマリ ノードが新しいデータプレーン バージョンにアップグレードされます。
サービスコネクション	Prisma Accessは、バックアップ (HA) サービス接続 (サービス接続企業アクセス ノード (SC-CAN) とも呼ばれます) をアップグレードし、指定した場所のバックアップ サービス接続をアクティブ ノードにします。バックアップ サービス接続は、すべての場所でアクティブ ノードとバックアップ ノードがアップグレードされる次の週末までアップグレードされません。 選択した場所に複数のSC-CANがある場合、すべてのバックアップ ノードが新しいデータプレーン バージョンにアップグレードされます。
ZTNA コネクタ	ZTNAコネクタはアップグレードされません。必要に応じて ZTNA コネクタをアップグレード できます。

最初のアップグレードと 2 回目のアップグレードの間に、最初にアップグレードされた場所を監視し、接続、パフォーマンス、ルーティング、およびログのテストを行って、場所が正常にアップグレードされたことを確認します。アップグレード後にサービスに影響する障害が発生した場合は、Palo Alto Networksテクニカル サポートに サポート ケース を開いて支援を受けてください。Palo Alto Networksは、24時間以内にデータプレーンを以前のデータプレーン バージョンにロールバックすることで、問題の解決を試みます。

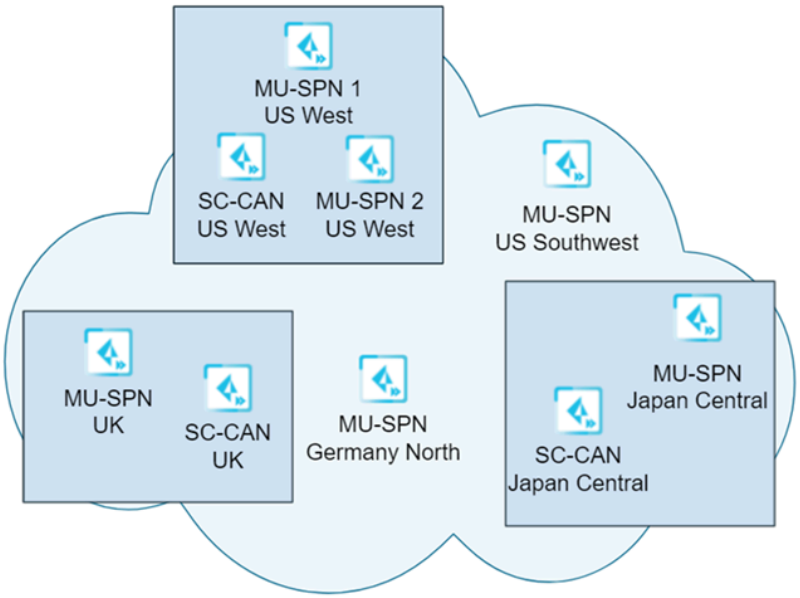
©2025 Palo Alto Networks, Inc.

- 7日後 Prisma Accessは最初の場所をアップグレードし、 Prisma Accessは最初のフェーズで選択したのと同じ時間枠を使用して、残り (フェーズ#2アップグレード) をアップグレードし、アップグレードが完了すると電子メールで通知します。

  アップグレード期間が長くなる場合があります。たとえば、フェーズ2が米国の祝日中に発生した場合、アップグレードの2 番目のフェーズは、最初のフェーズの7日後ではなく14日後に発生します。*Strata Cloud Manager*で受け取る通知には、データプレーンのアップグレードの具体的なスケジュールが表示されます。

データプレーンのアップグレード例

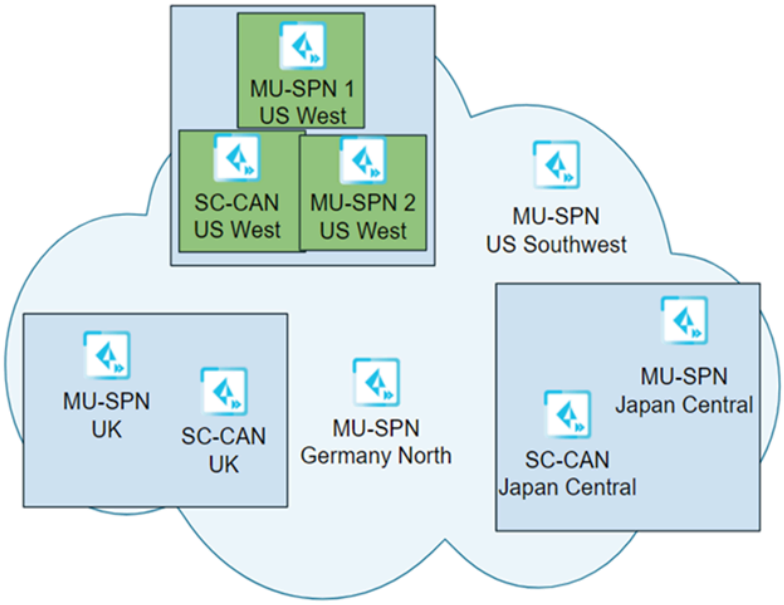
次の例は、5つのゲートウェイ (MU-SPN) と3つのSC-CANを備えたモバイル ユーザー デプロイメントのデータプレーン アップグレード手順の例を示したものです。米国西部のロケーションには、自動スケール イベントの結果として2つのMU-SPNがあります (多数のモバイル ユーザーがそのロケーションにログインした後に、追加のMU-SPNが追加されました)。



この例では、最初にアップグレードする単一の場所 (米国西部) を選択し、アップグレードのために土曜日の午前8時から正午までの4時間のアップグレード ウィンドウを要求しています。

最初のアップグレード週末（フェーズ＃1）には、米国西部のSC-CANとMU-SPNのアップグレードが午前8時から午後12時の間に行われます。土曜日の太平洋時間。

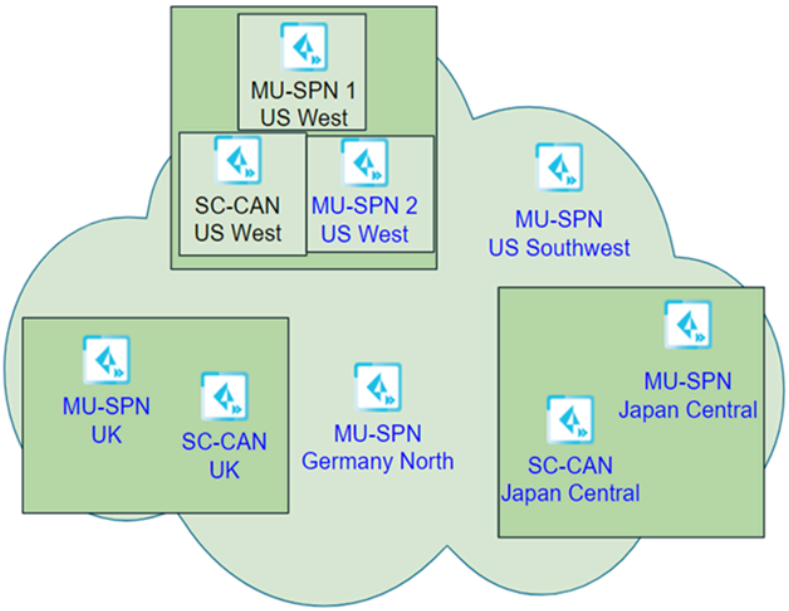
©2025 Palo Alto Networks, Inc.



最初の場所がアップグレードされてから7日後、Palo Alto Networksは、アップグレードの最初のフェーズで使用されたのと同じ4時間の時間枠 (土曜日の午前8時から午後12時) を使用して、残りのコンポーネント (フェーズ #2) をアップグレードします。

この例では、 Prisma Accessはデータプレーンをアップグレードするときに、次のタイムゾーン情報を使用します。

- 日本中央MU-SPNおよびSC-CANは、日本の現地時間を使用してアップグレードされます。
- 英国のMU-SPNとSC-CANは、英国の現地時間を使用してアップグレードされます。
- 米国南西部の MU-SPN は太平洋時間を使用してアップグレードされます。



©2025 Palo Alto Networks, Inc.

アップグレードアラートと更新情報を受け取る

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

データプレーンアップグレードのアップグレードスケジュールをお知らせし、アップグレードのご希望を選択するには、Strata Cloud Managerを使用してPrisma Access通知を購読する必要があります。 Strata Cloud Managerでは、アップグレードが行われる週末の2日間をEメールアラートでお知らせします。最初にアップグレードする場所と、アップグレードに使用する4時間の時間枠を選択します。

アップグレードの開始後、次の手順で示すようにStrata Cloud Managerを使ってアップグレードのステータスを監視することもできます。

STEP 1 | Strata Cloud Managerからのアラート通知に登録します。

STEP 2 | 今後のデータプレーンのアップグレードについて通知を確認し、次のいずれかの方法でアップグレードの設定を選択します。

- [ワークフロー] > [ソフトウェア アップグレード] > **[Prisma Access** > [アップグレード設定]を選択します。

  アップグレード ダッシュボードが表示されます。



- Strata Cloud Managerにログインし、スケジュールされたアップグレードのページ上部のバナーを表示し、[ここをクリック]を選択します。
- 予定されているアップグレードの通知をメールで確認し、メール内のハイパーリンクをクリックします。
- [ワークフロー] > [ソフトウェア アップグレード] > **[Prisma Access** > [アップグレード設定]を選択します。

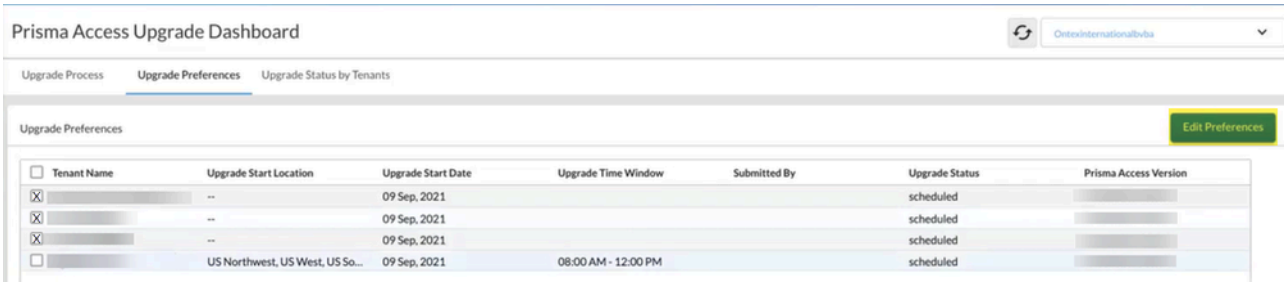
STEP 3 | (任意) アップグレード プロセスの詳細について知るには、「アップグレード プロセス」 をお読みください。

©2025 Palo Alto Networks, Inc.

STEP 4 | **Upgrade Preferences (**アップグレードのプリファレンス**)**を選択します。

マルチテナントデプロイメントの場合、すべてのテナントがこの領域に表示されます。デプロイメントのアップグレード設定をすでに選択している場合は、その選択内容がここに表示されます。

1. アップグレード設定を行うテナントを選択し、**[Edit Preferences (**プリファレンスの編集**)]**を選択します。



2. 最初にアップグレードしたい**[PreferredPrisma AccessLocations (**優先ロケーション**)]**を選択してください。

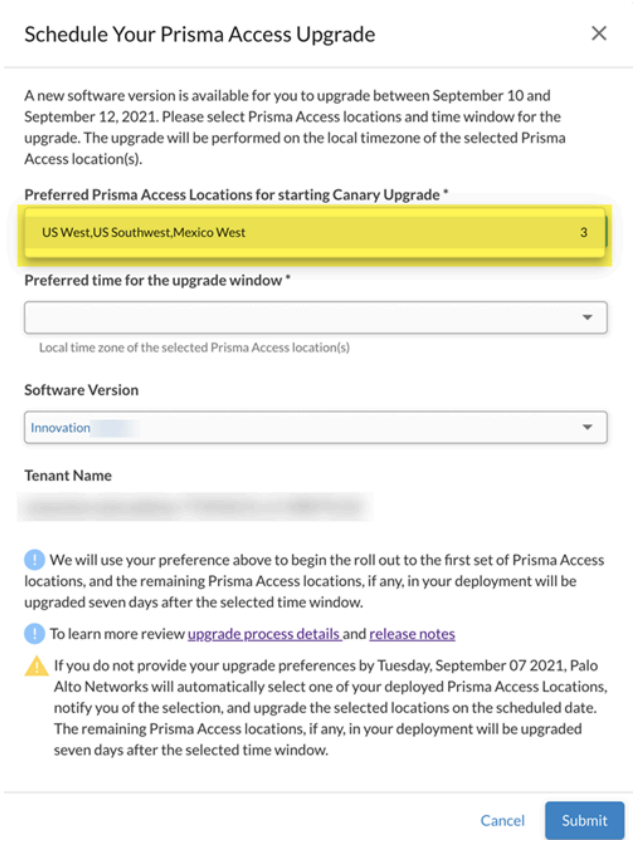
   Palo Alto Networks では、デプロイメント全体を反映する場所を選択することを強くお勧めします。たとえば、モバイル ユーザー、サービス接続、リモート ネットワーク デプロイメントがある場合は、すべてのデプロイメント タイプを含む場所を選択します。

   ドロップダウン リストの選択肢から選択します。

   - Prisma Accessにはモバイル ユーザー、リモート ネットワーク、サービス接続、またはそれらの組み合わせをデプロイした場所のみが表示されます。
   - ドロップダウン リスト内のグループは同じコンピューティング場所に属します。

   Prisma Accessが場所がアップグレードされたときに電子メールアラートでお知らせします。

©2025 Palo Alto Networks, Inc.



最初のセットの後 Prisma Access 場所が正常にアップグレードされると、 Prisma Access チームはこれらの場所を7日間監視し、その後残りのPrisma Access場所すべてをアップグレードします。1 つの場所または少数の場所を選択すると、1 週間後に残りの場所がアップグレードされる前に、これらの場所を監視する機会が得られます。

ドロップダウン リストに場所が表示されない場合は、共通の場所がデプロイされていない複数のテナントを選択したか、選択したテナントに場所がまだオンボードされていません。

3. 利用可能なオプションのリストから、 アップグレード ウィンドウの希望時間 を選択します。

   次のアップグレード時間枠から選択してください。時間枠は、アップグレードされる場所に対してローカルであり、すべて 4 時間の枠です。

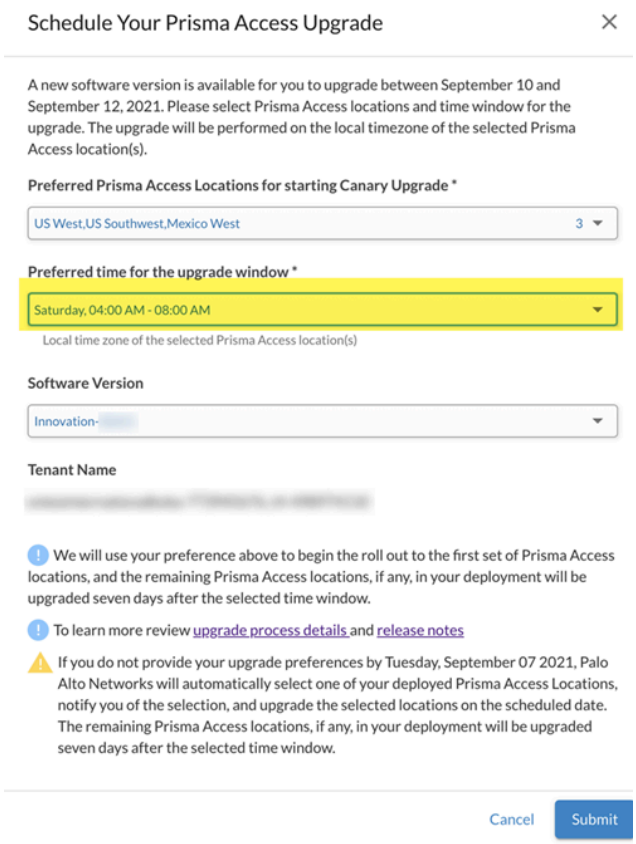
   - 金曜日 午後8時から午前12時（深夜）
   - 土曜日 午前12時（深夜）から午前4時
   - 土曜日 午前4時から午前8時まで
   - 土曜日 午前8:00～午後12:00（正午）
   - 土曜日 午後12時（正午）～午後4時
   - 土曜日 午後4時～午後8時

   Palo Alto Networksは、お客様の設定を使用して、選択した Prisma Access の場所でロールアウトを開始します。予定開始日の 7 日前に行われた最後の送信が、アップグ

©2025 Palo Alto Networks, Inc.

レード用にサービスによって選択されます。変更を加えた場合、その変更が Insights (インサイト) のアップグレード ダッシュボードに表示されるまでに最大 30 分かかることがあります。Prisma Accessが変更を処理し完了すると、アラート電子メールで通知されます。

アップグレード予定日の 7 日前までにアップグレード設定を提供しなかった場合、*Palo Alto Networks* は配備済みの*Prisma Access*ロケーションの最初のセットを自動的に選択し、その旨を通知して、選択したロケーションを予定日にアップグレードします。デプロイメントに残りの*Prisma Access*ロケーションがある場合は、選択したタイムウィンドウの 7 日後にアップグレードされます。



4. 複数のバージョンが利用可能な場合は、アップグレードする ソフトウェア バージョンを選択します。
5. 変更を**Submit**（送信）します。

©2025 Palo Alto Networks, Inc.

STEP 5 | ロールアウトが始まったら、 [ワークフロー] > [ソフトウェアアップグレード] > > **[Prisma Access]** > [テナント別のアップグレードステータス]を選択し、[場所別のアップグレードステータス]を表示します。

このページには、アップグレードされる各場所について次の情報が表示されます。

- アップグレードされるテナントの名前。
- アップグレード プロセスの開始日と終了日。
- テナントがアップグレードされるデータプレーンのバージョン。
- アップグレードの推奨時間枠。
- アップグレードされる最初の場所。
- 残りの場所がアップグレードされる日付。

さらに、アップグレードされる場所、アップグレードの開始日時、アップグレードに使用されるタイムゾーンが表に表示されます。アップグレード ステータス 列には次の情報が表示されます。

アップグレードステータス	詳説
スケジュール済み	データプレーンのアップグレードがスケジュールされました。
スタート	アップグレードが開始されました。
処理中	データプレーンのアップグレードが進行中です。
再試行中	データプレーンのアップグレードは正常に完了しませんでしたが、Prisma Accessは旧バージョンのデータプレーンを使用して運航を続けています。Prisma Accessは週末のメンテナンス・ウィンドウが切れる前にアップグレードを再試行する予定です。
成功	アップグレードは正常に完了しました。

STEP 6 | 最初のセットの場所のデータプレーンのアップグレードが完了したら、アップグレードされた場所を監視し、接続、パフォーマンス、ルーティング、およびログのテストを行って、正常にアップグレードされたことを確認します。

STEP 7 | 2番目の場所のセットのアップグレードが予定されている場合は、 **[Workflows (ワークフロー)]** > **[Software Upgrades (ソフトウェアアップグレード)]** > **Prisma Access** > **[Upgrade Status by Tenants (テナント別のアップグレードステータス)]**を選択して、それらの場所を監視し、ステータスを確認します。

Prisma Accessはデータプレーンのアップグレードが完了すると、電子メール通知が送信されます。

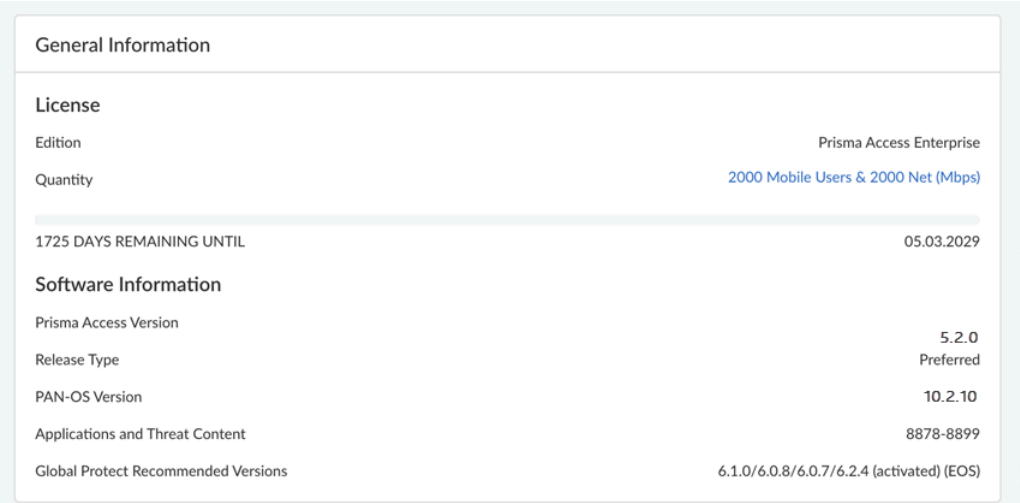
©2025 Palo Alto Networks, Inc.

Prisma Access ソフトウェアバージョンを表示する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス

Prisma Access (Managed by Strata Cloud Manager)

ソフトウェアとコンテンツのバージョン情報、**[Manage (管理)]** > **[Configuration (設定)]** > **[NGFWとPrisma Access]** > [概要] > [一般情報]でご確認いただけます。**Prisma Access**設定スコープを選択します。



一般情報ページでは、次の情報が提供されます。

エリア	詳説
テナント**ID**	Palo Alto Networksサービスのアップグレードを知るために、連絡先情報（会社名、連絡先名、メールアドレス、および電話番号）の共有を可能にします。 テナントのID。
テナント名	テナントの名前。
リージョン	テナントの地域。
Prisma Accessバージョン	現在Prisma Accessバージョン。

©2025 Palo Alto Networks, Inc.

エリア	詳説
PAN-OS バージョン	データプレーンが実行しているPAN-OSのバージョン。データプレーンは、Prisma Accessインフラストラクチャのコンポーネントであり、ネットワークとユーザート ラフィックのトラフィック検査とポリシー実施を可能にします。
リリースタイプ	実行しているリリースのタイプ (PreferredまたはInnovation)。 イノベーション リリースでは、優先リリースよりも高いPAN-OSデータプレーンが必要です。
アプリケーションと脅威コンテンツ	アプリケーションと脅威のコンテンツは、実行中のバージョンを更新します 。

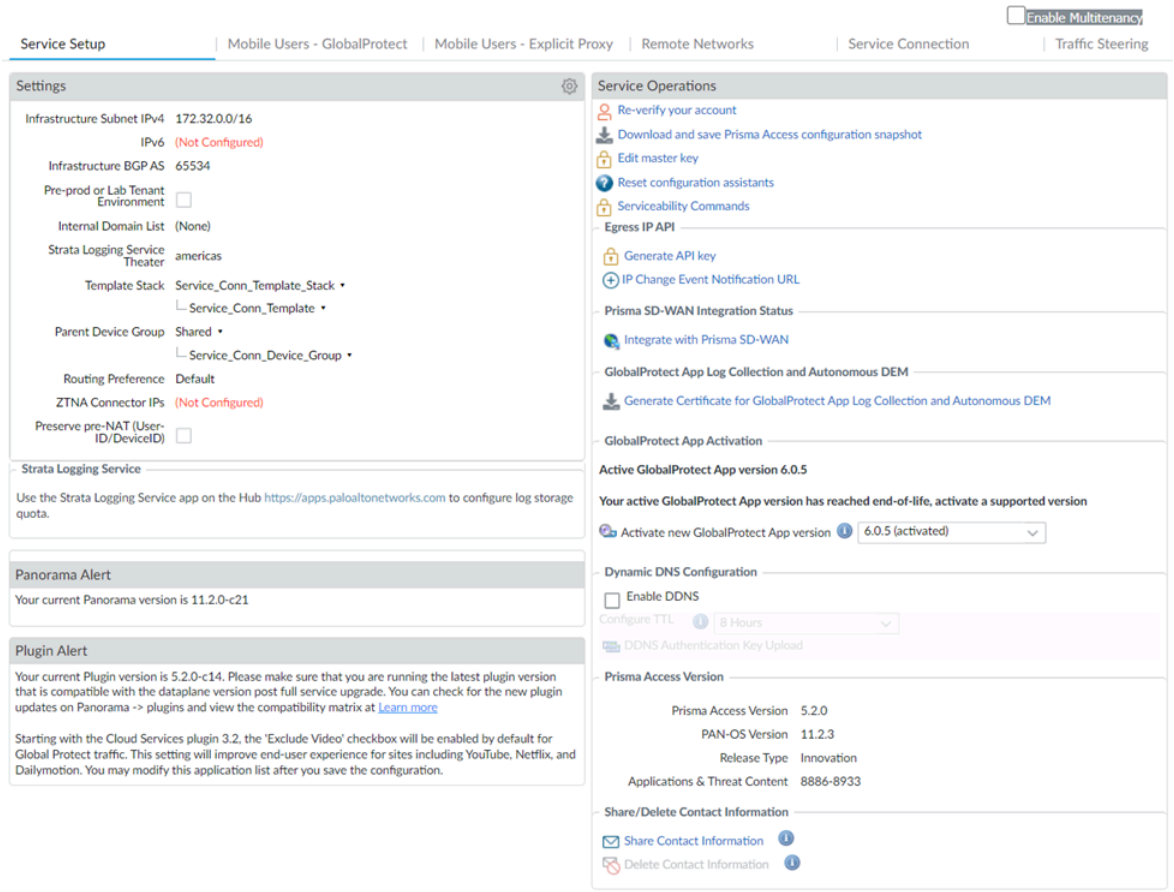
Prisma Access (Managed by Panorama)

Prisma AccessPanoramaやCloud Servicesプラグインなどの自分が管理するコンポーネント、データプレーンなどのPrisma Accessが管理するコンポーネント、およびPrisma Accessが管理するけれども自身がバージョンを指定できる（Prisma Accessポータルで提供するGlobalProtectアプリのバージョン）コンポーネントから成り立っています。サービスセットアップ（サービス設定）ページ（**[Panorama]** > **[Cloud Services (**クラウドサービス**)]** > **[Configuration (**設定**)]** > **[Service Setup (**サービスセットアップ**)]**）には、これらのコンポーネントのステータスが単一のページに表示されます。このページには、現在動作しているPanoramaおよびプラグインのバージョンが、Prisma Accessで使用するためのサポートが終了（EoS）する時期を知らせるメッセージも表示されます。お客様の組織がアップグレードを検討するために十分な時間を確保できるように、EoS日付の詳細が表示されます。

すべての日付は協定世界時（*UTC*）で表されています。

Service Setup（サービス設定）ページには、次の情報が表示されます。

©2025 Palo Alto Networks, Inc.



エリア	詳説
Panorama Alert（**Panorama**アラート）	現在実行しているPanoramaのバージョンが表示されます。**Upgrade requirements**（アップグレード要件）エリアには、Panoramaのバージョン情報、および現在互換性があるPanoramaバージョンの、Prisma Accessの管理に関するサポートが終了する日付（EoS）などが表示されます。この情報を利用して、EoSの日付が到来する前にPanoramaのアップグレードを検討してください。
Plugin Alert（プラグインアラート）	Prisma Accessを管理しているPanoramaにインストールされている、現在のCloud Servicesプラグインが表示されます。**Upgrade requirements**（アップグレード要件）エリアには、次のバージョンのプラグインが公開される日付、次のプラグインにアップグレードするまでの有効期限、および古いプラグインバージョンを使って変更とコ

©2025 Palo Alto Networks, Inc.

エリア	詳説
	ミットを行えなくなる日付が表示されます。この情報を利用して、次のCloud Servicesプラグインへのアップグレードを検討してください。
Prisma SD-WAN統合ステータス	**[Prisma SD-WAN**と統合する]を選択すると、Prisma SD-WANとPrisma Access間の機能を可能にするCloudBladeシンクライアントが有効になります。
GlobalProtectアプリケーションのログ収集と自律型**DEM**	[トラブルシューティングのためのGlobalProtectアプリケーション ログ収集]を有効にしている場合、またはモバイル ユーザーに対して 自律型デジタルエクスペリエンス管理 (ADEM) を有効にする場合は、**[GlobalProtect** アプリケーション ログ収集および **Autonomous DEM** の証明書の生成] をクリックして証明書を生成します。この証明書により、GlobalProtectアプリケーションは、Strata Logging Service（ログを収集するため）および自律型DEMと認証することができます。Prisma Access は、証明書を生成するときに、**[Shared (**共有**)]**内の **Mobile_User_Template**テンプレートの下にある Panorama[デバイス] > [証明書管理] > [証明書] > [デバイス証明書] の デバイス証明書にも証明書をダウンロードして、モバイル デバイスにプッシュします。
GlobalProtect App Activation（**GlobalProtect**アプリケーションのアクティベーション）	モバイルユーザーがPrisma Accessポータルからダウンロードできる、現在動作している（アクティブな）バージョンのGlobalProtectアプリケーション、およびアップグレードできるバージョンのGlobalProtectアプリケーションが表示されます。
ダイナミック**DNS**設定	リモート ネットワークのトラブルシューティングのためにダイナミック DNS (DDNS)が有効になっているかどうかを表示します。
Prisma Accessバージョン	現在Prisma Accessバージョン。
PAN-OS バージョン	データプレーンが実行しているPAN-OSのバージョン。データプレーンは、Prisma Accessインフラストラクチャのコンポーネ

©2025 Palo Alto Networks, Inc.

エリア	詳説
	ントであり、ネットワークとユーザート ラフィックのトラフィック検査とポリシー実施を可能にします。
リリースタイプ	実行しているリリースのタイプ (PreferredまたはInnovation)。 イノベーション リリースでは、優先リリースよりも高いPAN-OSデータプレーンが必要です。
アプリケーションと脅威コンテンツ	アプリケーションと脅威のコンテンツは、実行中のバージョンを更新します 。
Share/Delete Contact Information（連絡先情報の共有/削除）	Palo Alto Networksサービスのアップグレードを知るために、連絡先情報（会社名、連絡先名、メールアドレス、および電話番号）の共有を可能にします。 以前に入力した連絡先情報がある場合、このエリアから入力した情報を削除することができます。 連絡先情報には、次の特殊文字を使用しないでください: • "（二重引用符） • '（アポストロフィ） • <（しょうなり不等号） • >（だいなり不等号） • &（アンパサンド ）

©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

Prisma Accessセットアップ

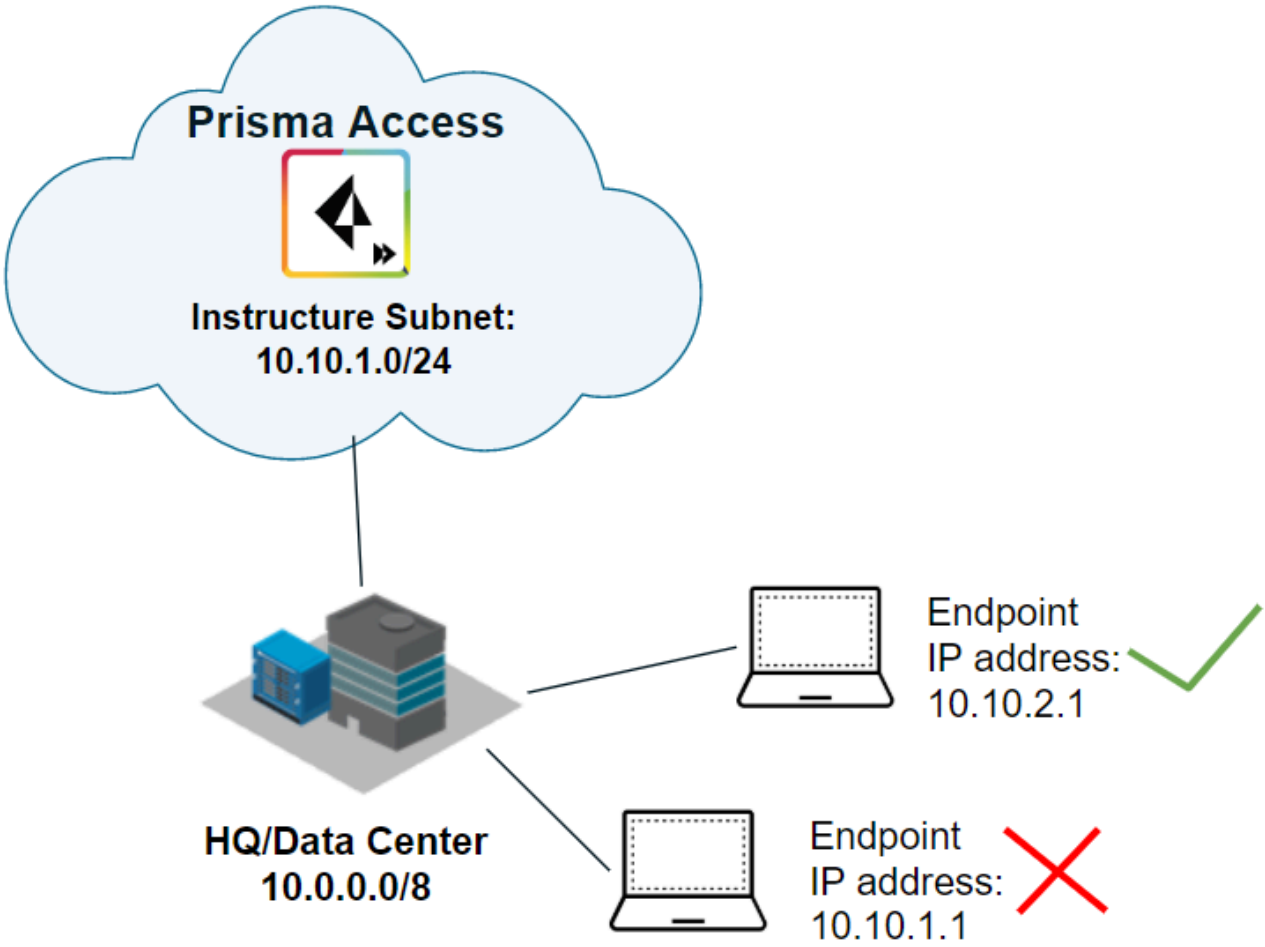
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

インフラサブネットを追加する際には、次の推奨事項と要件を使用してください。

- 組織のIPアドレスプール内の既存のスーパーネットからのインフラサブネットにPrisma Accessを割り当てることができますが、既存のネットワークないでの他の用途に対してインフラサブネットからのIPアドレスは割り当てないようにしてください。

  既存のスーパーネット10.0.0.0/8から割り当てた、Prisma Accessインフラサブネット10.10.1.0/24の例を次に示します。インフラのサブネットとして10.10.1.0/24を割り当てた後は、そのサブネットからのIPアドレスを使用することはできません。たとえば、エンドポ

イントに10.10.2.1を割り当てることはできますが、10.10.1.1はインフラサブネットの一部であるため使用できません。



- インフラサブネットに対する新しいサブネットを作成する場合、内部的に使用するその他のIPアドレスとオーバーラップしないサブネットを使用してください。
- (推奨)RFC 1918 準拠のサブネットを使用します。RFC 1918非準拠の（パブリック）IPアドレスはサポートされていますが、インターネットのパブリックIPアドレス空間と競合する可能性があるため、お勧めできません。
- 次のIPアドレスおよびサブネットと重複するサブネットは指定しないでください。Prisma AccessはこれらのIPアドレスおよびサブネットを内部使用のために予約します。
  - 169.254.0.0/16
  - 100.64.0.0/10
- このサブネットは、モバイルユーザーデプロイ環境用に割り当てる予定のIPアドレスプールとオーバーラップすることはできません。
- サービスインフラが非常に大規模になる可能性があるため、最低でも「/24」サブネットワークを指定する必要があります。

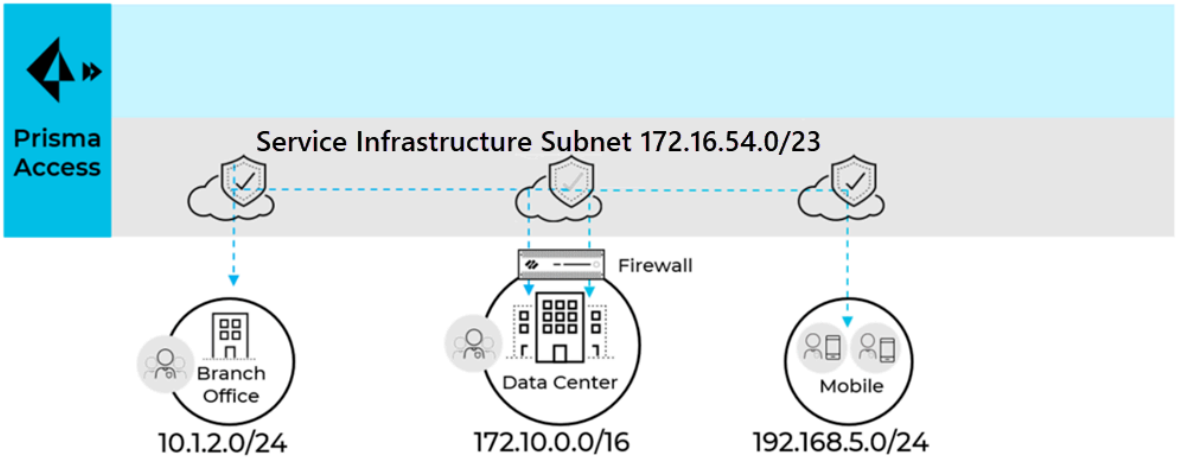
©2025 Palo Alto Networks, Inc.

Prisma Accessのセットアップ

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス

Prisma Accessを使用してリモート ネットワークとモバイル・ユーザを保護する前に、インフラストラ クチャ サブネットを構成します。 Prisma Accessは、このサブネット内のIPアドレスを使用して、リモート ネットワーク ロケーション、モバイル ユーザ、本社、およびデータ センター（該当する場合）間のネットワークを確立します。 Prisma Accessはまた、サービス接続を使用して、本社またはデータセンターの場所から内部リソースにアクセスします。

このサブネットワークは既存のネットワークの拡張となります。したがって、ネットワーク内の既存の IP サブネットと重複しないようにする必要があります。以下の例では、Prisma Accessインフラ サブネットに 172.16.54.0/23 のサブネットを使用しています。



サイト数が 50 未満、モバイル ユーザーが 2500 人未満の小規模ネットワークの場合は、/24 サブネットを検討してください。サイト数が 100 未満、モバイル ユーザーが 5000 未満の中規模ネットワークの場合は、/23 サブネットを検討してください。ほとんどの場合、/23 サブネットで十分です。サイト数が 100 を超える場合やモバイル ユーザーが 5000 人を超える場合、または将来的に増加が見込まれる場合は、Palo Alto Networks に問い合わせて、より大きなサブネット サイズが必要かどうかを評価してください。

Prisma Accessセットアップ方法を学びます。

- Strata Cloud Manager
- Panorama

Prisma Accessのセットアップ (Strata Cloud Manager)

Prisma Accessをインストール、設定するためのステップの概要を次のワークフローに示します

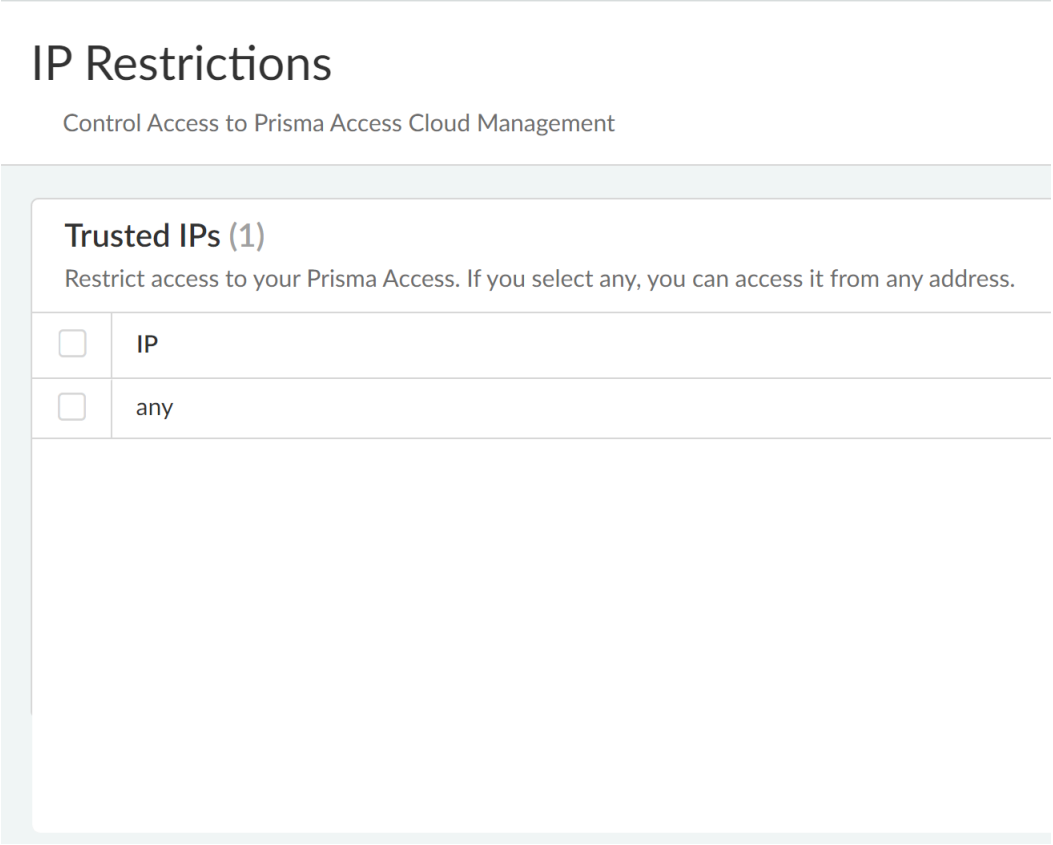
©2025 Palo Alto Networks, Inc.

STEP 1 | ハブを介してStrata Cloud Managerを起動します。

1. インターネット ブラウザを起動し、 ハブに サインインします 。
2. Strata Cloud Managerを起動します。

STEP 2 | Prisma Access (Managed by Strata Cloud Manager) 管理者向けの信頼できるIPアドレスを指定します。

Prisma Access (Managed by Strata Cloud Manager)アクセスできるのは、これらの送信元IPアドレスからログインした管理者（および認証に成功した管理者）のみです。IPアドレスはパブリックアドレスである必要があります。デフォルトでは、信頼されたアドレスは強制されません（リストは任意に設定されています ） 。開始するには、左側のナビゲーション パネルで [設定] メニューを見つけて、**[IP 制限]**をクリックします。



STEP 3 | ライセンス要件を特定し、Prisma Access コンポーネントをアクティブ化してインストールします。

STEP 4 | Prisma Accessエレメント間の通信を可能にする、サービスインフラとサービス接続を有効にします。

STEP 5 | デプロイメントの必要に応じて、GlobalProtect または Explicit Proxy を使用してモバイル ユーザーを保護します。

STEP 6 | リモートネットワーク接続を計画、作成、および設定します。

STEP 7 | （任意） 認証方法をローカル認証から、ご自分の組織の認証方法に変更します。

©2025 Palo Alto Networks, Inc.

STEP 8 | （任意） Strata Logging Serviceから外部Syslogレシーバーにログを転送します。

STEP 9 | （任意）Prisma Accessのステータスを確認します。

ハブからアプリケーション インスタンスにアクセスすることで、Prisma AccessやStrata Logging Serviceを含むすべてのクラウドサービスのステータスと、サービスの稼働時間の履歴を取得することができます。

また、電子メールまたはテキスト メッセージの通知にサインアップして、インフラストラクチャの更新が計画されているとき、更新が発生したとき、および Palo Alto Networks® がインシデントを作成、更新、または解決したときに通知を受け取ることもできます。電子メールによる更新情報にサインアップするには、 ハブ のホームページの [リソース] セクションに移動し、[サービス ステータス]を選択します。その後、クラウド サービスの特定の更新とインシデントを サブスクリプション できます。

Prisma Accessのセットアップ (Panorama)

Prisma Access (Managed by Panorama) Accessをインストール、設定するためのステップの概要を次のワークフローに示します。

単一の*Panorama*に複数の*Prisma Access*インスタンスが存在するデプロイ環境（マルチテナント）をセットアップする場合は、を参照してください。大部分の組織では、複数のテナントを作成、管理する必要はありません。

STEP 1 | Prisma Accessを管理するPanoramaアプライアンスと一緒に使用する、任意のセキュリティアプライアンスの許可リストに、次のURLとポートを追加します。

また、Panoramaアプライアンスがを使用している場合（**Panorama** > **Setup**（セットアップ） > **Service**（サービス） > **Proxy Server**（プロキシサーバー））、またはPrisma AccessでSSLフォワード プロキシを使用している場合、プロキシまたはプロキシサーバーの許可リストに、次のURLとポートを忘れずに追加してください。

- api.gpcloudservice.com （Prisma Access用）
- api.paloaltonetworks.com （Prisma Access用）
- apitrusted.paloaltonetworks.com （Prisma Access用）
- Strata Logging Serviceに必要なFQDNとポート

*Panorama*アプライアンスとインターネット間に、次世代型*Palo Alto Networks*ファイアウォールが存在している場合、ファイアウォールにセキュリティポリシールールを追加して、*Panorama*アプライアンスからインターネットへの、***paloalto-logging-service***と***paloalto-shared-services*** *App-ID*を許可する必要があります。これらのアプリケーションは、*Panorama*アプライアンスがログのクエリに使用する、*Prisma Access*と*Strata Logging Service*への、*SSL*で保護された通信を可能にします。*Panorama*アプライアンスは従来のレイヤー*4*ファイアウォールの背後にある場合、*Panorama*から発信されるポート*443*と*444*を許可して、*Panorama*からのトラフィックを許可してください。*Palo Alto Networks App-ID*を使用せずに、レイヤー*4*ポートを開くことは、セキュリティが低下するためお勧めできません。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | ネットワークの許可リストに、Panoramaが使用するポートを追加します。

STEP 3 | ライセンス要件を特定し、Prisma Access コンポーネントをアクティブ化してインストールします。

STEP 4 | 既存のPanorama設定をPrisma Accessにインポートするか、または新しいテンプレートとデバイスグループを作成して、Prisma Access設定を開始します。

セキュリティポリシー、認証ポリシー、サーバープロファイル、セキュリティプロファイル、アドレスオブジェクト、アプリケーショングループなどの環境設定をPrisma Accessにプッシュするには、Prisma Accessにプッシュしたい設定を持つ新しいテンプレートとデバイスグループを作成するか、または既存のデバイスグループとテンプレートを、サービスのオンボーディング時にPrisma Accessによって作成されたテンプレートスタックとデバイスグループ階層に追加します。

購入した内容に応じて、Prisma Accessによって次のテンプレートとデバイスグループが作成されます（たとえば、明示的プロキシライセンスを購入しない場合、明示的プロキシテンプレートとデバイスグループは表示されません）。

- テンプレート:
  - **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**
- デバイスグループ:
  - **Explicit_Proxy_Device_Group**
  - **Mobile_User_Device_Group**
  - **Remote_Network_Device_Group**
  - **Service_Conn_Device_Group**

Prisma Accessでの設定は簡単です。インターフェイスやルーティングプロトコルなどのインフラ設定を行う必要はありません。この設定は自動化され、Panoramaからサービスが自動的に作成したテンプレート、デバイスグループ内にプッシュされます。リモートネットワークにあるIPSec対応デバイスへの、IPSec VPNトンネルの作成に必要な設定など、サービスが必

©2025 Palo Alto Networks, Inc.

要とする任意のインフラ設定を行うことができます。必要に応じて、サービスのセットアップを簡素化するために、テンプレートとデバイス階層を設定に追加することができます。

サービスのセットアップを簡素化するために、Prisma Accessを使用するためのセットアップ作業を開始する前に、必要なテンプレートとデバイスグループを作成またはインポートしてください。

Prisma Access用テンプレートとデバイスグループを作成する場合、それに管理対象デバイスを割り当てる必要はありません。代わりに、Prisma Accessが作成したテンプレートスタックおよびデバイスグループ階層に、それを追加します。Prisma Accessが作成したテンプレートまたはデバイスグループを、他のテンプレートスタックやデバイスグループには追加しないでください。

STEP 5 | Strata Cloud Managerを使ってデンシメール通知に登録します。

Prisma Accessはこのアプリの通知を使用して、データプレーンのアップグレードを含むサービスに関する通知を提供します。

STEP 6 | Panoramaのデフォルトマスターキーとクラウドサービスプラグインのデフォルトマスターキーを変更します。

Palo Alto Networksは、セキュリティのベストプラクティスとして、PanoramaおよびCloud Servicesプラグインでマスターキーを変更することを推奨しており、マスターキーは毎月変更することをお勧めします。

Panorama とPrisma Accessのマスター キーは同期されないため、Palo Alto Networks では、Prisma Accessのマスター キーも同期せずに Panorama のマスター キーを自動的にローテートしないことを推奨しています。Panorama UIまたはAPIコマンドを使用して、マスターキーを変更できます。

デプロイするマスターキーを必ず追跡してください。マスターキーは回復できません。マスターキーの有効期限が切れた場合、新しいマスターキーを設定するために現在のマスターキーを入力する必要があります。現在のマスターキーが期限切れになった場合、*Panorama*アプライアンスを工場出荷時の設定にリセットする必要があります。

1. Panoramaでマスターキーを変更します。
   1. **[Panorama]** > **[Master Key and Diagnostics**（マスター キーおよび診断）**]**の順に選択します。

      現在のマスターキーを指定しないでください。
   2. **New Master Key (**新規マスター キー**)** を設定し、**Confirm New Master (**マスターキーの確認**)** を行います。

      設定したマスターキーをメモしてください。
   3. マスター キーの Lifetime (有効期間) と Time for Reminder (リマインダーの時間) を構成します。
   4. **OK** をクリックします。
2. **[Panorama]** > **[Cloud Services (**クラウドサービス**)]** > **[Configuration (**設定**)]** > **[Service Operations (**サービスオペレーション**)]** > **[Edit master key (**マスター キーの編集**)]**を選択

©2025 Palo Alto Networks, Inc.

し、Panorama用に入力したのと同じマスター キーを入力して、Prisma Accessのマスター キーを変更します。

APIコマンドを使用してマスターキーを変更することもできます。これには2つのステップが必要です。1つはPanoramaマスター キーを変更すること、もう1つはPrisma Accessマスター キーを変更することです。マスターキーを変更するには、次のAPIコマンドを使用してください:

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

STEP 7 | Prisma Accessエレメント間の通信を可能にする、サービスインフラとサービス接続を有効にします。

1. サービスインフラとサービス接続の有効化を計画します。
2. サービスインフラを有効にします。
3. 会社のリソースへのアクセスを可能にするサービス接続を作成します。

   会社のリソースへのアクセスが不要な場合でも、モバイルユーザーとリモートネットワーク間のアクセスを有効にするために、サービス接続を作成してください。

STEP 8 | Prisma Accessのモバイルユーザーデプロイメントでは、デプロイメントに応じてGlobalProtectまたは明示型プロキシを使用してモバイルユーザーを保護します。

Prisma Access (Managed by Panorama)でGlobalProtectを設定するには:

1. モバイルユーザー用のゾーンを設定するには、Mobile_User_Templateに2つのゾーン（たとえば、Mobile-UsersとInternet）を作成し、ゾーンをマッピングします。Prisma Access接続ユーザーまたは本社/支店オフィスではないゾーンは、Untrust（信頼しない）にマップする必要があります。

   Panorama > **Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Mobile Users**（モバイルユーザー）下で、InternetをUntrustに、Mobile-UsersをTrustにマップします。
2. 認証の設定

   サービスがセットアップされており、ユーザーがインターネットにアクセスできることを検証する最初のステップとして、ローカル認証を使用することをお勧めします。後ほど、ご自分の企業の認証手段に切り替えることができます。
3. デバイスグループのセキュリティポリシーを設定します。

   インターネットへのトラフィックを許可するセキュリティポリシーを作成するには、Mobile_User_Device_Groupを選択し、**Policies**（ポリシー） > **Security**（セキュリ

 ©2025 Palo Alto Networks, Inc.

ティ） > **Prerules**（プレルール） > **Add**（追加）を選択して、ルールを追加します。以下に例を示します。Mobile-Users to Internet。

4. サービスを開始するには、変更をコミットしてプッシュします。
5. **Panorama** > **Cloud Services**（クラウドサービス） > **Status**（ステータス） > **Monitor**（監視） > **Mobile Users**（モバイルユーザー）の順に選択して、**Status**（ステータス）を参照し、ポータルのFQDNにpingできることを確認します。
6. GlobalProtectアプリケーションをダウンロードしてインストールし、アプリを使用してモバイル ユーザー（ローカル ユーザ）としてポータルに接続し、インターネット上のいくつかの Web サイトをブラウズし、 Panorama 上のトラフィック ログをチェックすることで、Prisma Accessがモバイル ユーザーのインターネット トラフィッ クを保護していることを検証します。

モバイルユーザーを明示型プロキシで保護するには:

1. 明示型プロキシの設定ガイドラインを閲覧します。
2. SAML 認証の設定明示的プロキシにはSAML認証が必要です。
3. Cloud Identity Engine (クラウドIDエンジン)を使用してグループマッピングを設定します。
4. 明示型プロキシの設定を完了してください。
5. 変更をコミット、プッシュ配信します。

STEP 9 | リモートネットワーク接続を計画、作成、および設定します。

1. Prisma Accessに1つまたは複数のリモートネットワークを追加します。

   1つのロケーションをオンボーディングした後、次に一括インポート機能を使ってその他のロケーションを追加することができます。
2. リモートネットワークから本社へのトラフィックを許可するセキュリティポリシーを作成します（例：Trust to Trust）。Trust to Trust (信頼から信頼へ)。
3. サービス接続、リモートネットワーク接続、およびモバイルユーザー間の接続性を確認します。

STEP 10 | Prisma AccessのIPアドレスを取得するために使用されるAPIスクリプトを実行し、モバイルユーザーのIPアドレスを取得するためにレガシースクリプトを使用します。

企業ネットワーク/アプリケーションへのインバウンドアクセスを制限するために、組織のネットワークの許可リストに、これらのアドレスを追加します。

STEP 11 | （任意） 認証方法をローカル認証から、ご自分の組織の認証方法に変更します。

1. 組織の要件を満たす認証プロファイルを作成します（SAML、LDAP、RADIUSなど）。
2. 組織がRADIUSやActive Directoryなどのオンプレミス認証を使用している場合、Prisma Accessが内部リクエストのソースIPアドレスとして使用するIPアドレス（Prisma AccessのIPアドレスを取得する）をネットワークの許可リストに追加する、またはインフラサブネット全体（Prisma Accessはこのサブネットからループバック IPアドレスを取得します）のIPアドレスを許可します。
3. この新しい認証プロファイルを使用するには、Prisma Accessポータルとゲートウェイの認証プロファイルを更新してください。

©2025 Palo Alto Networks, Inc.

STEP 12 | （任意） Strata Logging Serviceから外部Syslogレシーバーにログを転送します。

 ©2025 Palo Alto Networks, Inc.

Prisma Accessサービスインフラの設定

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス ❑ **Pre-prod or Lab Tenant (**プレ プロまたはラボ テナント**)**に最低限必要なPrisma Accessバージョン:3.0-Preferred

Prisma Accessは、ブランチ ネットワーク、モバイル ユーザー、Prisma Accessセキュリティ インフラ、およびサービス接続を介してPrisma Accessに接続する予定の本社やデータセンター ネットワークとの間の通信のために、サブネットを使用してネットワーク バックボーンを作成します。

リモートネットワーク拠点、モバイルユーザ、およびサービス接続を介してPrisma Accessに接続する予定のHQやデータセンター間の通信を可能にするには、サービスインフラストラクチャ サブネットを設定します。 Prisma Accessはこのサブネットを使用して、支店ネットワーク、モバイル ユーザー、Prisma Accessセキュリティ インフラ、およびサービス接続を介してPrisma Accessに接続する予定の本社やデータ センター ネットワーク間の通信用ネットワーク バックボーンを作成します。

- Strata Cloud Manager
- Panorama

Prisma Accessサービスインフラの設定 (Strata Cloud Manager)

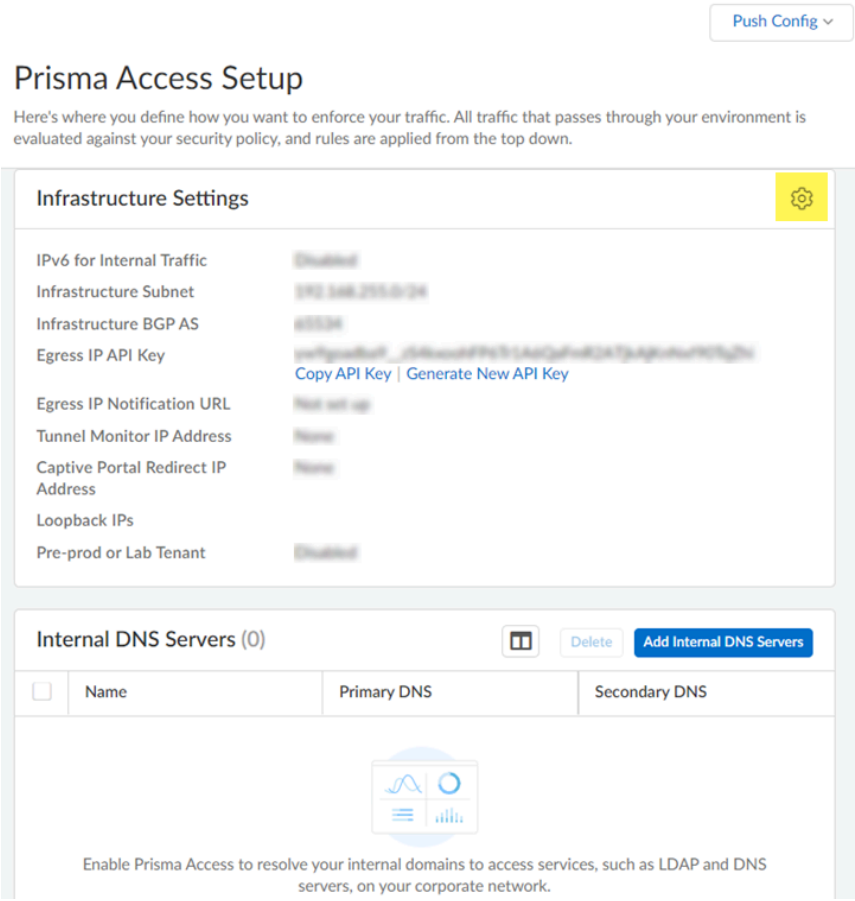
Prisma Access用のインフラストラクチャ サブネットを追加する場合は、次の推奨事項と要件に従ってください。

- ❑ RFC 1918 準拠のサブネットを使用します。RFC 1918非準拠の（パブリック）IPアドレスはサポートされていますが、インターネットのパブリックIPアドレス空間と競合する可能性があるため、お勧めできません。
- ❑ 169.254.0.0/16および100.64.0.0/10サブネット範囲と重複するサブネットは、Prisma Accessが内部使用のためにこれらのIPアドレスとサブネットを予約しているため、指定しないでください。
- ❑ このサブネット トワークは既存のネットワークの拡張であるため、企業ネットワーク内で使用する IP サブネットや、[Prisma Access for Users (ユーザー用)] または [Prisma Access for Networks (ネットワークス用)] に割り当てるIPアドレスプールと重複することはできません。
- ❑ サービス インフラストラクチャには多数の IPアドレスが必要なので、/24 サブネットワーク (例: 172.16.55.0/24) を指定する必要があります。
- ❑ リモート ネットワークまたはサービス接続にダイナミック ルーティングを使用する場合は、RFC 6996準拠のBGPプライベートAS番号も構成する必要があります。

STEP 1 | Prisma Accessを起動します。

©2025 Palo Alto Networks, Inc.

STEP 2 | **Workflows (ワークフロー) > [Prisma Accessセットアップ] > Prisma Access > [Infrastructure Settings (インフラストラクチャ設定)]**に移動し、ギアをクリックして設定を編集します。



STEP 3 | Prisma Accessが、リモート ネットワーク ロケーション、モバイル ユーザー、およびPrisma Accessオーバー サービス接続を計画している本社またはデータセンター間の通信を可能にするために使用できるインフラストラクチャ サブネットを入力します。

インフラストラクチャ サブネットには*RFC 1918*準拠のサブネットを使用します。*RFC 1918*非準拠の（パブリック）*IP*アドレスはサポートされていますが、インターネットのパブリック*IP*アドレス空間と競合する可能性があるため、お勧めできません。

STEP 4 | (任意) IPv6 を設定する場合は、**[内部トラフィック]**に**[IPv6]** を選択し、IPv6サブネットを選択します。

STEP 5 | Prisma Accessインフラ内で使用する**Infrastructure BGP AS**（インフラ**BGP AS**）を入力します。

Prisma Accessがリモート ネットワークとHQまたはデータ・センターのリソースへのルートを動的に検 出できるように、ダイナミック ルーティングを有効にしたい場合は、ボーダー ゲートウェイ プロトコル（BGP）を使用する必要があります。インフラストラクチャ **BGP AS**は、BGPがトラフィックを送信できるルートを識別する自律システム（AS）番号で

©2025 Palo Alto Networks, Inc.

す。AS 番号を指定しない場合、Prisma AccessはデフォルトのAS 番号 (65534) を使用します。

独自のAS番号を指定する場合は、RFC 6996準拠のプライベートAS番号を使用する必要があります。使用できるフォーマットは、4バイトのASプレーン [64512-65534],[4200000000-4294967294] またはASドット [0.64512-0.65534], [64086.59904-65535.65534]表記です。

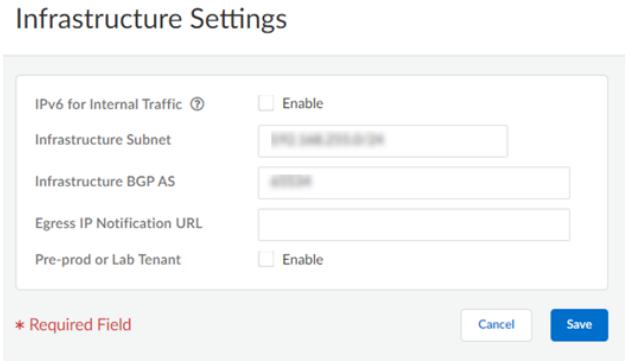
STEP 6 | 送信元IPアドレスに基づいてユーザーがアプリケーションにアクセスできるようにする場合、アプリケーション アクセス ポリシーで許可できるように、Prisma Accessからのトラフィックがソース アドレスとして使用するIPアドレスのリストを取得する必要があります。

Egress IP APIキーをコピーして、Prisma AccessEgress IP Address API(出口側IPアドレスAPI)を使用できるようにします。また、Prisma Accessを使用するIPアドレスは定期的に変更されるため（たとえば、新しい場所を追加したり、Prisma Accessが既存の場所でリソースを拡張する必要がある場合、またはインフラストラクチャをアップグレードしたりする場合）、IPアドレスがいつ変更されるかを把握しておく必要があります。これにより、ポリシールールを更新したり、**Egress IP Notification URL (**出力側**IP**通知**URL)**を定義して更新を自動化したりできます。詳細については、Prisma Access用のIPアドレスの取得を参照してください。

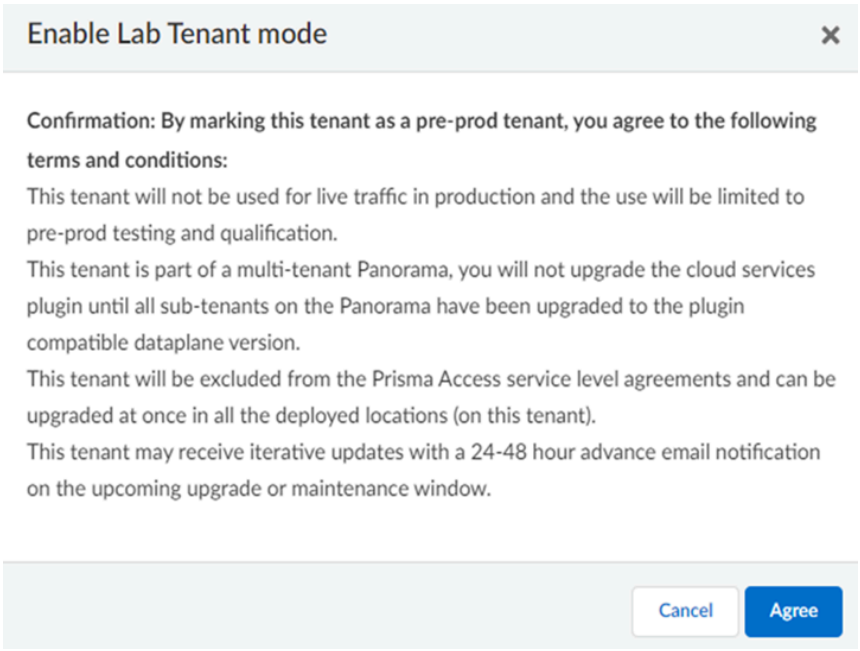
©2025 Palo Alto Networks, Inc.

STEP 7 | (任意) テナントを運用前テナントまたはラボテナントとして有効にします。

1. テナントを**Pre-Prod**または**Lab**テナントとして有効にします。



2. 確認に同意します。



テナントを運用前テナントまたはラボテナントとして有効化すると、他の実稼働テナントをアップグレードする前に、このテナントのみのアップグレードをスケジュールできます。テナントは、次回のアップグレードの24 ～ 48時間前に通知を受け取ります。運用前テナントまたはラボテナントからテナントを無効にすると、そのテナントは本番テナントと見なされます。

3. 変更を保存します。

STEP 8 | Prisma Accessが内部ドメインを解決できるようにするには、**[Add Internal DNS Servers (内部DNSサーバーの追加)]** をクリックする。

企業ネットワーク内のリソースへのアクセスを可能にするためにサービス接続を構成する予定で、内部ドメインを解決するためにPrisma Accessも必要な場合は、内部ドメインのリストを定義する必要があります。内部ドメイン リスト内のドメインに対するDNSクエリ

©2025 Palo Alto Networks, Inc.

は、Prisma Accessリモート ネットワーク ユーザーとモバイル ユーザーがリソースを 利用できるように、ローカルDNSサーバーに送信されます。

1. Prisma Accessが内部ドメイン名を解決するために使用するプライマリ**DNS** サーバとセカンダリ**DNS** サーバを入力する。
2. Prisma Accessに解決したい内部ドメイン名を追加します。

   ドメインリスト内のドメインの先頭にワイルドカード（*）を使用できます（例：*.acme.localまたは*.acme.com）。

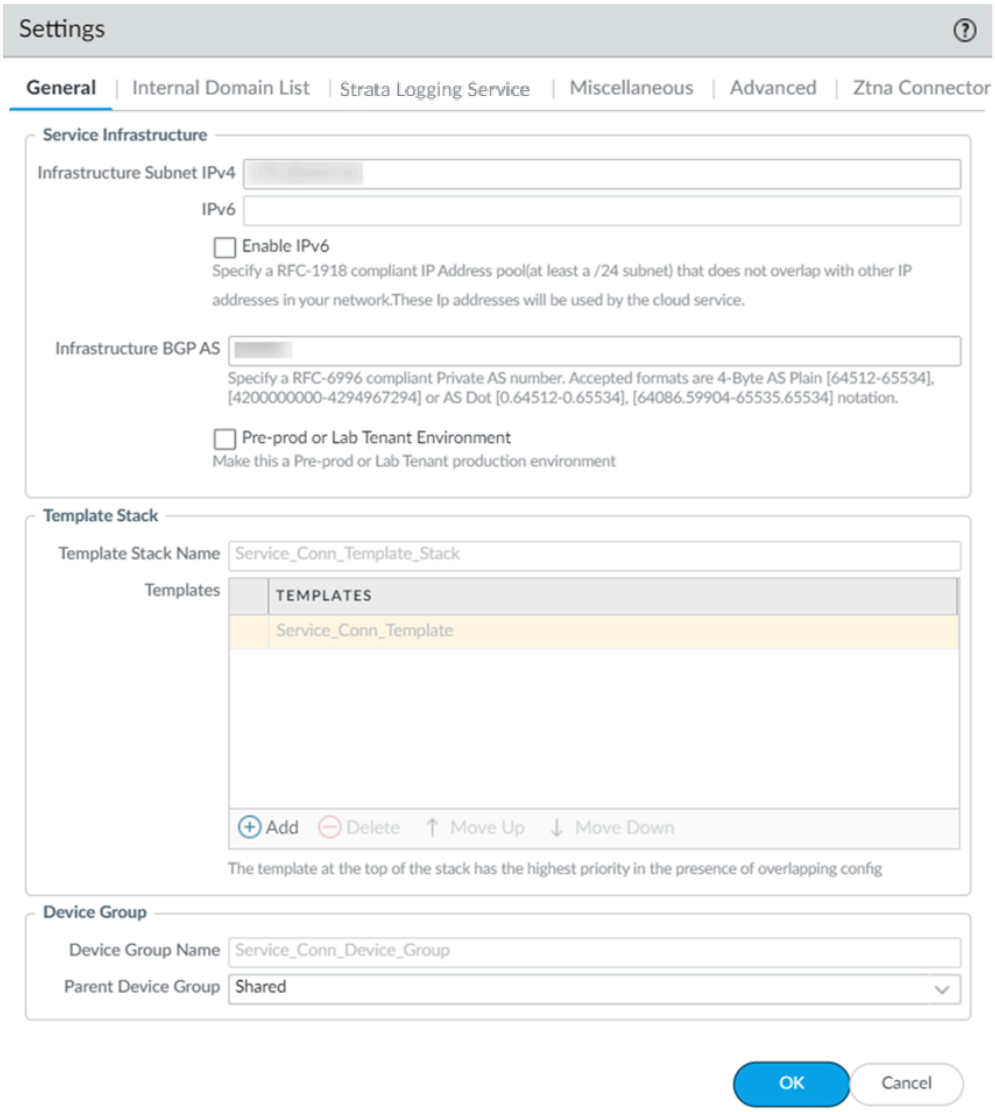
STEP 9 | **Config** をプッシュして、サービスインフラストラクチャの設定をPrisma Accessに保存します。

Prisma Accessサービスインフラの設定 (Panorama)

リモートネットワークやモバイルユーザーを保護するためのPrisma Accessの設定を開始する前に、サービス接続、リモートネットワーク、モバイルユーザー間の通信、およびサービス接続経由でPrisma Accessに接続する予定の企業ネットワークとの通信に対して、Prisma Accessネットワークバックボーンの作成に使用する、インフラサブネットを設定する必要があります。インフラのセットアップには多数のIPアドレスが必要になるため、「/24」サブネットを使用する必要があります（例：172.16.55.0/24）。必ずすべてのガイドラインと要件に従ってください。

©2025 Palo Alto Networks, Inc.

STEP 1 | **Panorama** > **Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Service Setup**（サービスのセットアップ）の順に選択し、歯車型アイコンをクリックして設定を編集します。



STEP 2 | [全般] タブで、要件を満たすインフラストラクチャサブネットを指定します (例: 172.16.55.0/24)。

STEP 3 | (任意) IPv6 を設定する場合は、[内部トラフィック]に**[IPv6]** を選択し、IPv6サブネットを選択します。

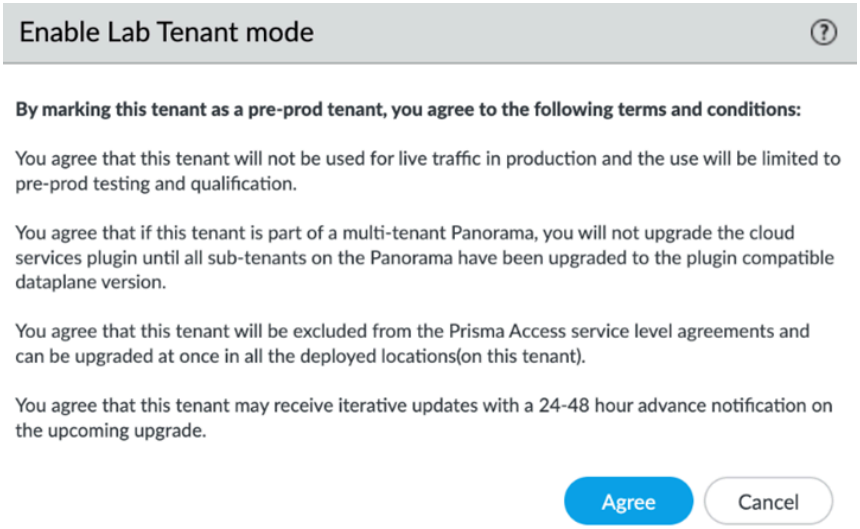
STEP 4 | （任意）Prisma AccessがBGPを使用して、リモート ネットワークおよび HQ/データセンター ロケーションのリソース へのルートを動的に検出できるようにする場合は、Prisma Accessインフラストラクチャ内で使用するインフラストラクチャ **BGP AS**を入力します。

AS番号を指定しない場合、デフォルトのAS番号65534が使用されます。

©2025 Palo Alto Networks, Inc.

STEP 5 | (任意) テナントを **Pre-prod** または **Lab** テナント環境として有効にします。

テナントを運用前テナントまたはラボテナントとして有効化すると、他の実稼働テナントをアップグレードする前に、このテナントのみのアップグレードをスケジュールできます。テナントは、次回のアップグレードの24 ～ 48時間前に通知を受け取ります。



運用前テナントまたはラボテナントからテナントを無効にすると、そのテナントは本番テナントと見なされます。

*Clean Pipe*向けの*Prisma Access*ではこの機能はサポートされていません。

STEP 6 | （任意） Prisma Accessが、企業のDNSサーバを使用して内部ドメインを解決できるようにします。

サービス接続経由で企業ネットワーク上の、LDAPサーバーなどの内部ドメインをPrisma Accessに解決させる必要がある場合に、このステップを使用します。たとえば、会社

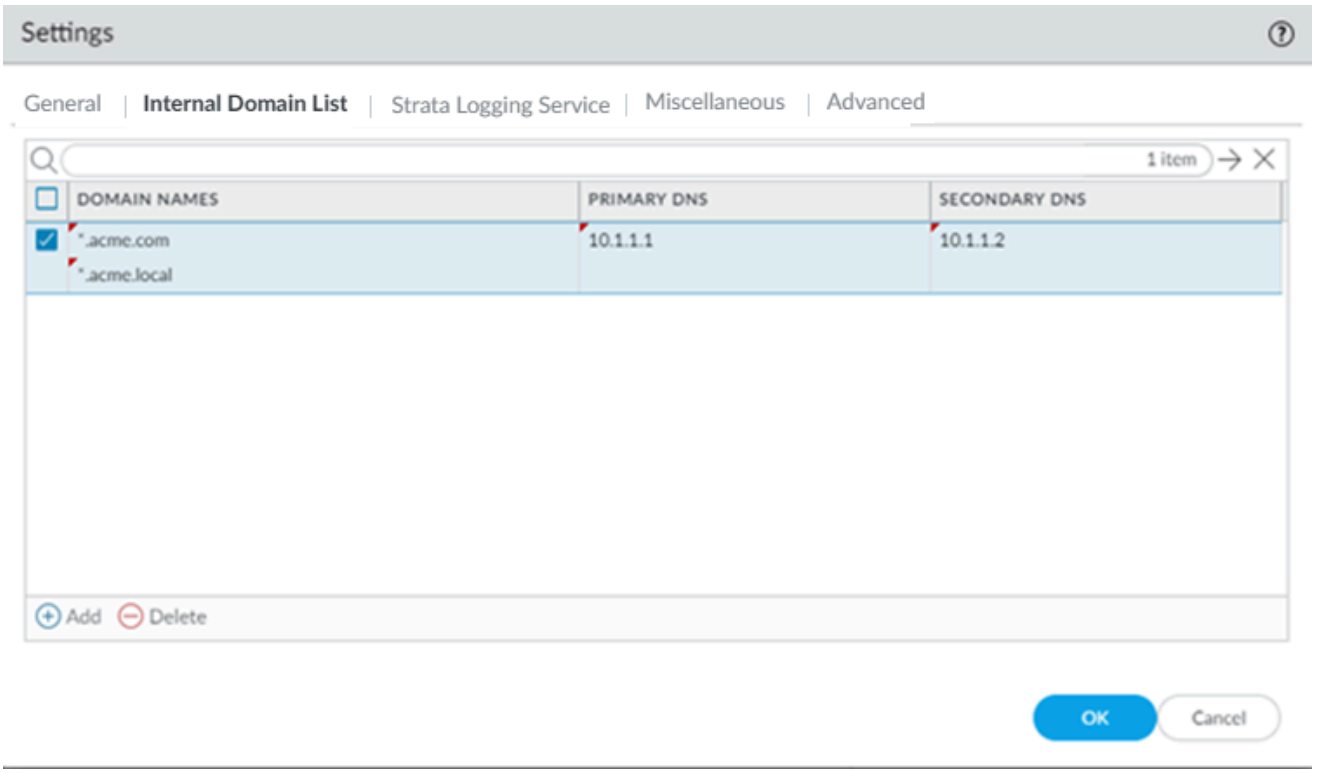
©2025 Palo Alto Networks, Inc.

のDNSサーバーを確実に利用するために、企業ドメインのDNS検索を利用したい場合は、企業ドメインと会社のDNSサーバーをここに指定します。

1. **Internal Domain List**（内部ドメインリスト）タブを選択します。
2. Prisma Accessが内部ドメイン名を解決するために使用するドメイン名、プライマリ**DNS**、およびセカンダリ**DNS**サーバーを追加します。

   ドメインリスト内のドメインの先頭にワイルドカード（*）を使用できます（例：*.acme.localまたは*.acme.com）。

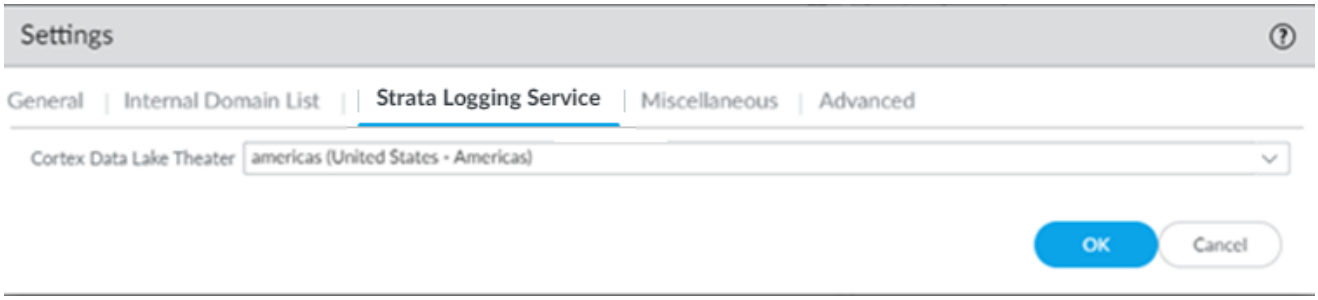
   *Prisma Access*の内部ルーティングの問題が発生する可能性があるため、*127.0.0.1*アドレスを入力しないでください。



©2025 Palo Alto Networks, Inc.

STEP 7 | Strata Logging Serviceを有効化します。

1. **Strata Logging Service**タブを選択します。
2. **Strata Logging Service Theater**を選択し、**[OK]**をクリックします。



3. 必要なログタイプを**Panorama/Strata Logging Service**に転送するログ転送プロファイルを使用して、Prisma Accessに設定をプッシュするために使用するデバイスグループを構 成します。

   新しいインストールの完了後、またはPrisma Accessテンプレート ステータスタックからPrisma Access以外のテンプレートを削除した場合、Cloud Servicesプラグインは次のログ設定（**Device**（デバイス） > **Log Settings**（ログ設定））を自動的に追加します：

   - Mobile_User_Templateには、システムログ（**system-gpcs-default**）、ユーザーIDログ（**userid-gpcs-default**）およびHIP Matchログ（**hipmatch-gpcs-default**）およびGlobalProtectログ（**gp-prismaaccess-default**）のログ設定が追加されます。
   - Remote_Network_Templateには、システムログ（**system-gpcs-default**）、ユーザーIDログ（**userid-gpcs-default**）、およびGlobalProtectログ（**gp-prismaaccess-default**）のログ設定が追加されます。
   - Service_Conn_Templateには、システムログ（**system-gpcs-default**）、およびGlobalProtectログ（**gp-prismaaccess-default**）のログ設定が追加されます。

   これらのログ設定は、システム、ユーザーID、HIPマッチ、およびGlobalProtectログを自動的にStrata Logging Serviceに転送します。

   ログ設定の変更を適用するには、次の手順を実行した後、変更内容をコミット、プッシュしてください。

   - モバイルユーザーテンプレートにログ設定を適用するには、**Panorama** > **Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Mobile Users**（モバイルユーザー）の順に選択し、歯車型アイコンをクリックして、設定を編集し、OKをクリックします。
   - リモートネットワークテンプレートにログ設定を適用するには、**Panorama** > **Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Remote Networks**（リモートネットワーク）の順に選択し、歯車型アイコンをクリックして、設定を編集し、OKをクリックします。
   - サービス接続テンプレートにログ設定を適用するには、**Panorama** > **Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Service Setup**（サービ

©2025 Palo Alto Networks, Inc.

スのセットアップ）の順に選択し、歯車型アイコンをクリックして、設定を編集し、OKをクリックします。

他のログタイプの転送を有効にする方法は、そのタイプによって異なります。ポリシー一致に基づいて生成されるログの場合は、ログ転送プロファイルを使用します。詳細については、Strata Logging Service スタートガイド を参照してください。

STEP 8 | (任意) その他の 設定を構成します。

1. (任意) URLフィルタリング構成で **[URL**に終了トークンを追加する] を選択して 、外部動的リスト (EDL) または カスタムURLカテゴリのURLに終了トークンを追加します。

   EDLまたはカスタムURLカテゴリで URL を使用し、URLに転送スラッシュ (/) を追加しない場合は、意図したよりも多くのURLが許可される可能性があります。たとえば、一致する URL として **example.com/** の代わりに **example.com** を入力すると、example.com.website.info や example.com.br にも一致します。

   URLフィルタリング設定で「**URL**に終了トークンを追加する」を選択すると、Prisma AccessはEDLまたはカスタムURLカテゴリのURLに終了トークンを設定します。**example.com**と入力すると、Prisma Accessはexample.com/ と同じように扱い、そのURLのみに一致します。

2. （任意） [サービス接続のトラフィック ログを無効にする]を選択すると、Prisma Accessデプロイメントのサービス接 続でのロギングが無効になります。

   サービス接続によってログ記録されるトラフィックフローの大半が非対称である場合、Strata Logging Serviceロギングストレージの消費を抑えるために、サービス接続のロギングを無効にする必要がある場合があります。デプロイメントにサービス接続経由の非対称フローがない場合、ログ記録を無効にする必要はありません。

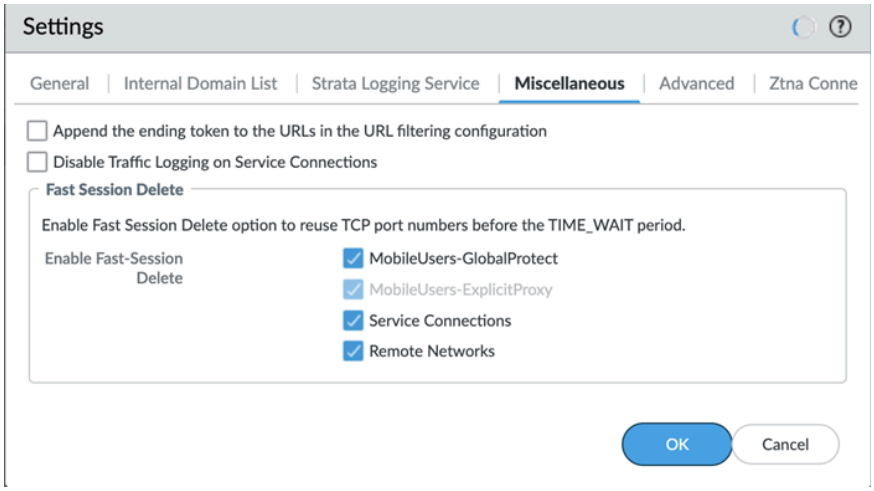
3. (任意) リモート ネットワーク、サービス接続、またはモバイル ユーザー - GlobalProtectデプロイメントに対して高速セッション削除を有効にするには、 モバイ

©2025 Palo Alto Networks, Inc.

ル ユーザー - **GlobalProtect**、 サービス接続、または リモート ネットワークのチェック ボックスをオンにします。

高速セッション削除により、Prisma AccessはTCP TIME_WAIT期間が終了する前にTCPポート番号を再利用できるため、存続期間が短い可能性があるSSL復号化セッションに役立ちます。

モバイル ユーザーの場合 - 明示型プロキシ展開では、高速セッション削除は機能の重要な部分であり、無効にすることはできません。



STEP 9 | (任意) 詳細 設定 (ルーティングの設定、サービス接続の対称ネットワーク パス オプション、HIP再配信) を構成します。

1. サービス接続で使用する、**Routing Preference**（ルーティング基本設定）を指定します。

   組織のネットワークまたはPrisma Accessネットワークで使用する、サービス接続トラフィックを処理するための、ネットワーク基本設定を指定できます。

   - **Default**（デフォルト）—Prisma Accessの内部ネットワークで、デフォルトのルーティングを使用します。
   - **Hot potato routing**（ホットポテトルーティング）—Prisma Accessは、サービス接続トラフィックを組織のWANにできる限り即座に渡します。

   *Prisma Access*サービス接続のルーティング方法を変更するには、組織のトポロジーとルーティングデバイス、および*Prisma Access*のルーティングの仕組みを完全に理解しておく必要があります。ルーティング方法をデフォルトから変更する前に、サービス接続トラフィックのルーティングをよくお読みになることをお勧めします。

2. サービス接続に使用するバックボーン ルーティングを構成します。

   デフォルトでは、 Prisma Accessバックボーンでは、サービス接続を介してデータセンターまたは本社から返されるトラフィックに対して対称ネットワーク パスが必要で

©2025 Palo Alto Networks, Inc.

す。CPEからのサービス接続にECMPまたは別の負荷分散メカニズムを使用したい場合は、Prisma Accessバックボーンを介して非対称フローを有効にできます。

- サービス接続バックボーン全体で対称フローを要求するには**no-asymmetric-routing**を選択します。
- サービス接続バックボーン全体でPrisma Accessが非対称フローを使用できるようにするには、**asymmetric-routing-only**を選択します。
- ある場所に複数のサービス接続がある場合、非対称ルーティング（**asymmetric-routing-with-load-share**）（デフォル ト設定）を選択することで、Prisma Accessデプロイメントで負荷分散を利用できる。ただし、負荷分散はベストエフォート方式で行われるため、サービス接続の1つがダウンすると負荷分散は失敗します。

3. サービス接続を使用して、モバイルユーザーとリモートネットワークのユーザーからHIP情報を再配信するPrisma Accessを使用したHIP情報の再配信。
4. Prisma AccessがGlobalProtectアプリケーションに接続された危険なデバイスを識別し、隔離するためのPrisma Access GlobalProtectのデプロイメントにおける侵害されたデバイスの識別と隔離。
5. バックアップ トンネルなしでトンネルがダウンしたときにPrisma Accessでスタティック ルートを削除する場合は、[サービス接続またはリモート ネットワーク**IPSec**トンネルがダウンしている場合はスタティック ルートを撤回する]を選択します 。

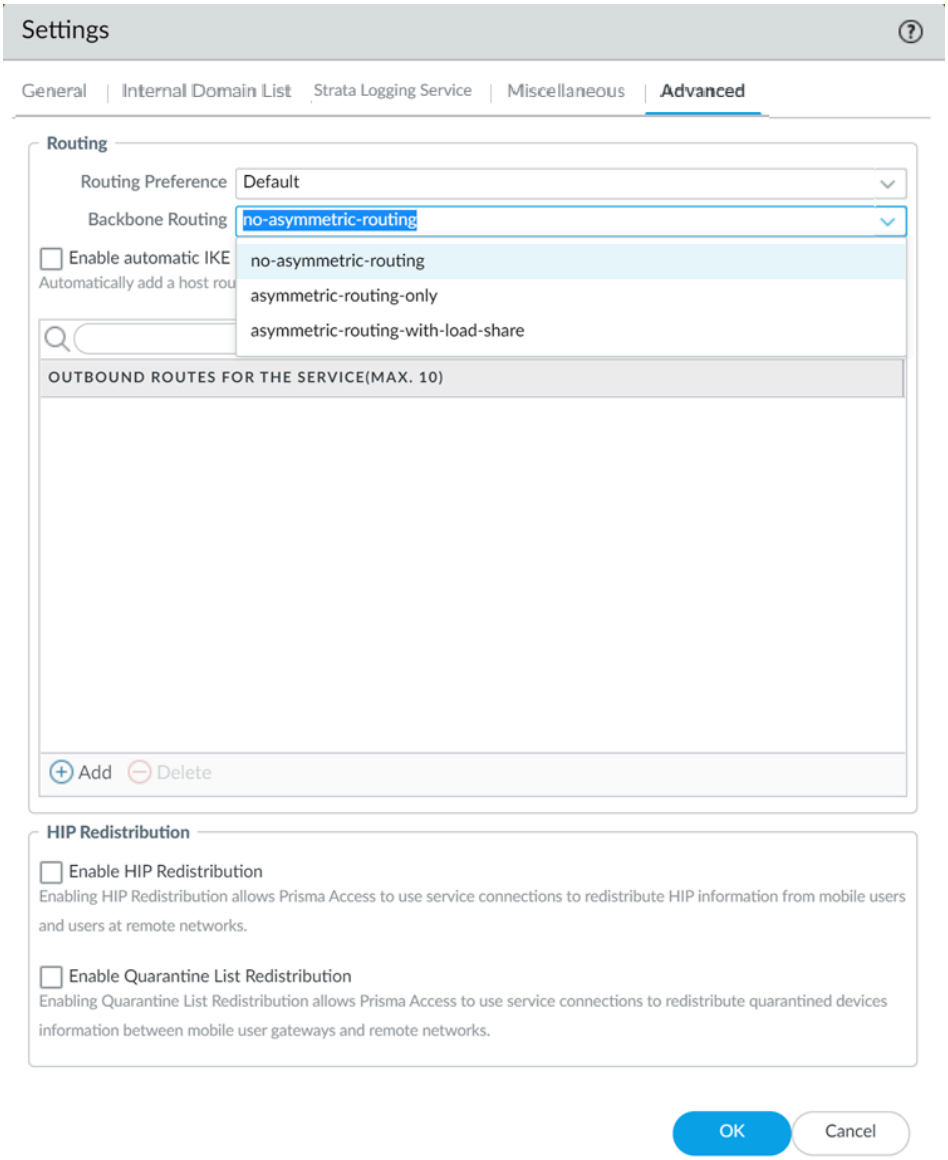
   Prisma Accessは次の状況ではルートを削除します。

   - プライマリ トンネルがダウンし、セカンダリ トンネルが存在しません。
   - プライマリ トンネルとセカンダリ トンネルが構成されているが、両方がダウンした場合。

   トンネル監視が有効になっていない場合、この変更を適用することはできません。
6. (任意) リモート ネットワークおよびサービス接続のIPSecトンネル パケットをインターネット経由で静的IKEゲートウェイにルーティングする場合は、 リモート ネットワークおよびサービス接続の自動**IKE**ピア ホスト ルートを有効にします。
7. （オプション） Prisma Accessがすべてのサービス接続とリモート・ネットワーク接続にスタティック ルートを追加するプレフィックスを10個まで追加して、サービスのア

©2025 Palo Alto Networks, Inc.

ウトバウンドルートを指定します**(Max 10)**。 その後、Prisma Accessはインターネット経由でこれらのプレフィックスにトラフィックをルーティングします。



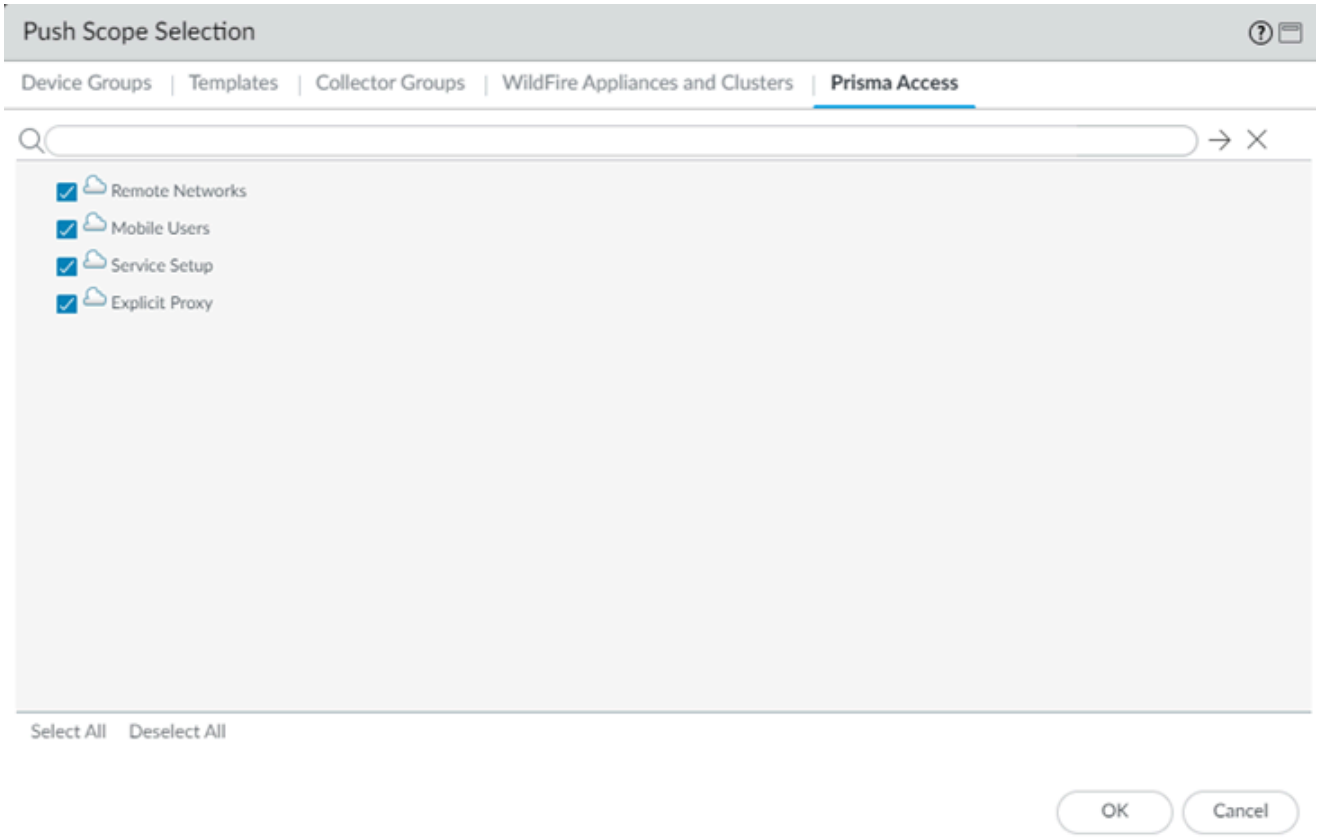
STEP 10 | **OK**をクリックして、サービスセットアップ設定を保存します。

©2025 Palo Alto Networks, Inc.

STEP 11 | Panorama にすべての変更をコミットし、その設定変更をPrisma Accessにプッシュします。

1. **Commit**（コミット） > **Commit to Panorama**（**Panorama** へのコミット）をクリックします。
2. **Commit**（コミット） > **Push to Devices**（デバイスへのプッシュ）をクリックして、**Edit Selections**（選択内容の編集）をクリックします。
3. **Prisma Access**タブで、**Service setup**が選択されていることを確認し、**OK**をクリックする。

   Prisma Accessは、コミットする必要があるコンポーネントを自動的に選択します。

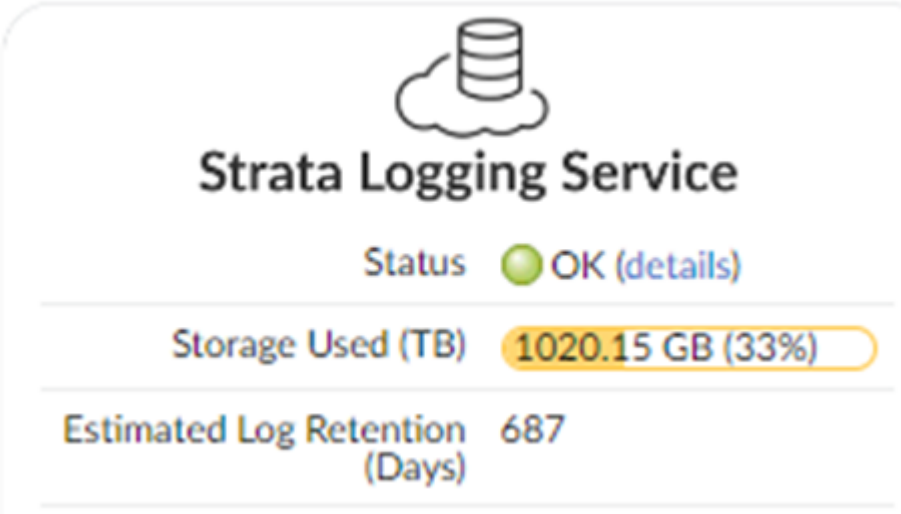


4. **Push**（プッシュ）をクリックします。

©2025 Palo Alto Networks, Inc.

STEP 12 | Prisma AccessがStrata Logging Serviceに正常に接続されていることを確認します。

1. **Panorama** > **Cloud Services** > **Status** (ステータス) > **Status** (ステータス) > **Strata Logging Service** を選択し、ステータスが **OK** であることを確認します。



ステータスが**Error**（エラー）になっている場合は、詳細リンクをクリックしてエラーを確認してください。

STEP 13 | 設定セットアップするPrisma Access:

- プライベート アプリへのアクセスを許可するサービス接続を作成します。
- ネットワーク向け設定Prisma Access
- ユーザー向け設定 Prisma Access

©2025 Palo Alto Networks, Inc.

モバイルユーザー:IPアドレス割り当て

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス

Prisma Accessデプロイメント環境をセットアップしたら、インフラを積極的にプランニングして、それに応じて必要なIPアドレスを許可リストに追加できるように、IPアドレスがどのような場合に変更されるのかを理解しておくことをお勧めします。何らかの変更を行った結果（たとえば、他のモバイルユーザーのロケーションを追加した）、またはPrisma Accessが自動的に実施する変更（たとえば、単一のPrisma Accessゲートウェイに多数のモバイルユーザーがアクセスした）ような場合に、IPアドレスの変更が行われます。

ユーザーにPrisma Accessを初めてデプロイすると、Prisma Accessは各ポータルとゲートウェイに2つのパブリック*IP*アドレスと、該当する場合はイグレス*IP*アドレスを割り当てます。これらのIPアドレスは一意であり、共有されず、Prisma Accessデプロイメント専用であり、Prisma Accessのサブスクリプションが失効して猶予期間が終了するまで、テナントに割り当てられたままとなります。

マルチテナントを設定している場合は、Prisma Accessによって各テナントに対して専用のIPアドレスが追加されます。

パブリックIPアドレスは、インターネットベースの宛先へのリクエストにPrisma Accessが使用する送信元IPアドレスであるため、SaaSアプリケーションや一般にアクセス可能なパートナーアプリケーションなどのリソースへのアクセスをユーザーに提供するためには、パブリックIPアドレスが何であるかを知り、それらをネットワーク内の許可リストに追加する必要がある場合があります。

次のイベントが発生した場合は、新しいパブリックIPアドレスをテナントに追加できます。

- 大量のモバイルユーザーが同じロケーションにアクセスした。

  多数のユーザーにサービスを提供するための容量要件に対処するために、Prisma Accessは1つまたは複数のゲートウェイを追加することができ、Prisma Accessはユーザー数の増加に対応するために1つまたは複数のゲートウェイを追加し、既存のパブリックIPアドレスの1つまたは複数を新しいゲートウェイに割り当て、使用されていたIPアドレスを置き換えるために新しいIPアドレスのセットをモバイルユーザーロケーションに追加します。
- デプロイ環境に1つ以上のロケーションが追加されました。

  さらに場所を追加すると、Prisma Accessは、追加した新しい場所ごとに、別のゲートウェイと新しいIPアドレスのセットを追加します。

Prisma Accessでは、スケーリング イベントが発生した後やロケーションを追加した後により多くのパブリックIPアドレスが使用可能になるため、IP変更イベント通知URLを追加するか、APIを使用してモバイル ユーザー アドレスを取得し、Prisma Accessインフラストラクチャ

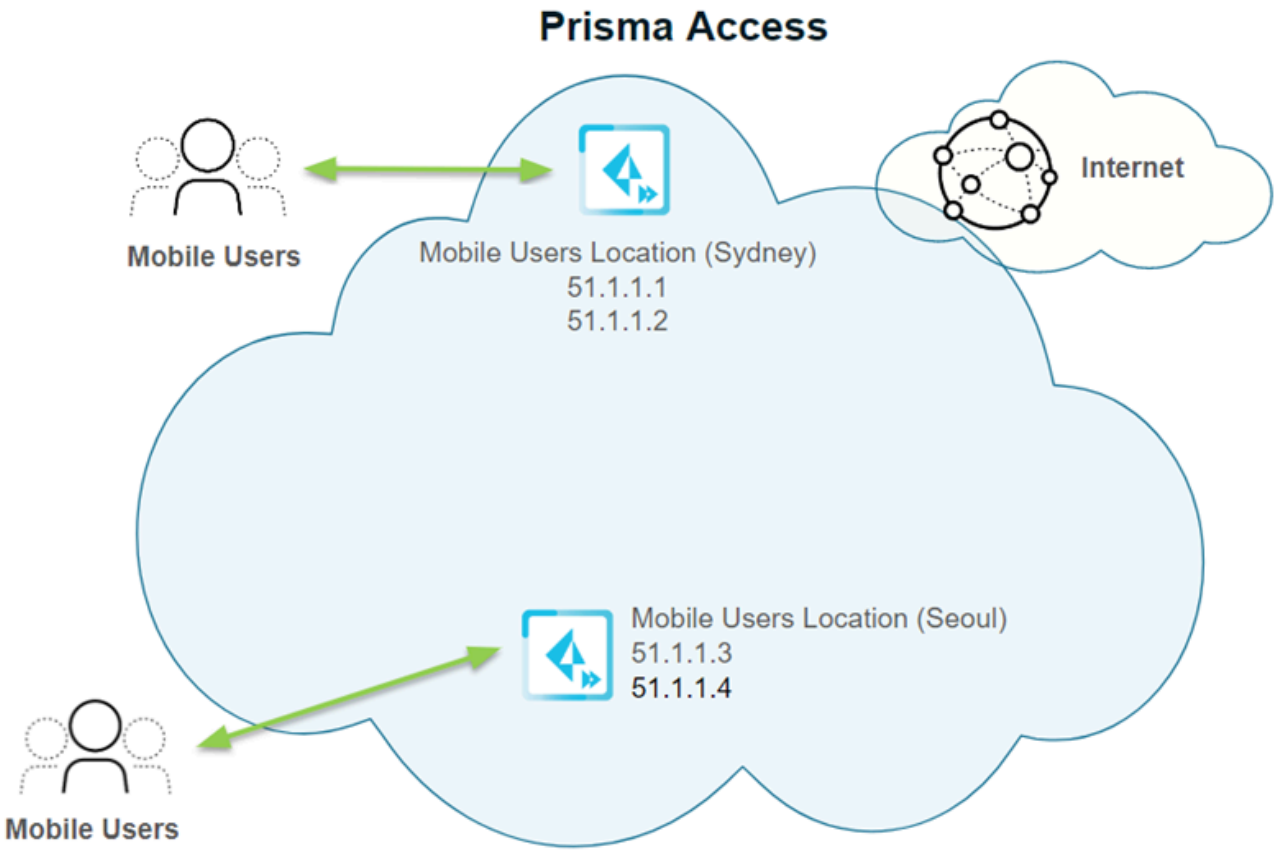
©2025 Palo Alto Networks, Inc.

内のIPアドレスの変更を通知する必要があります。次に、追加または変更されたアドレスを、許可リストに追加できます。

例:パブリックIPアドレスのスケーリングの例 (モバイル ユーザー)

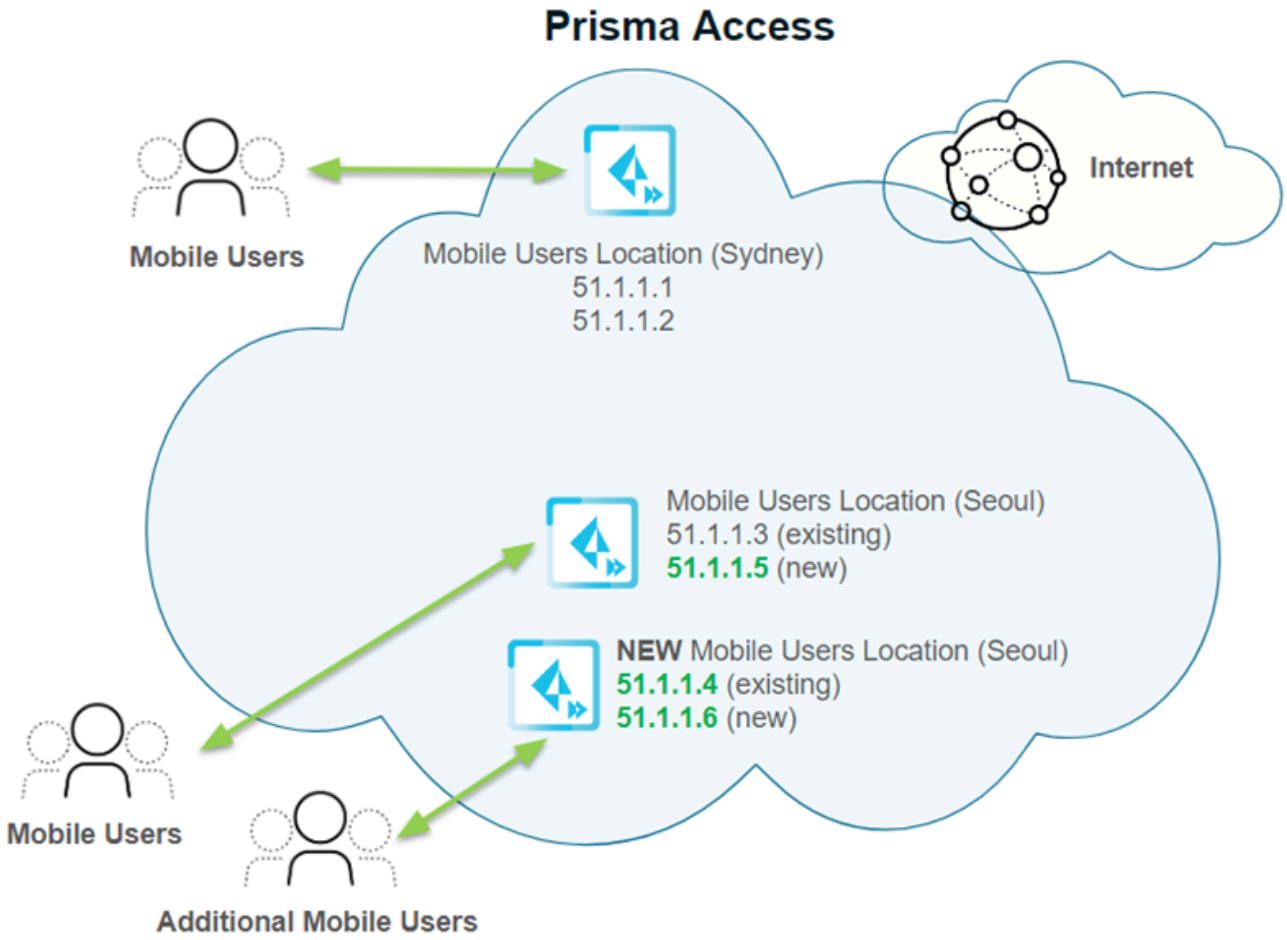
スケーリングイベント、または新しいロケーションを追加した時に、Prisma Accessが使用する、モバイルユーザーパブリックIPアドレスの割り当てプロセスの例を次に示します。

次の例では、新しいモバイルユーザーデプロイ環境向けに、2つのロケーション（SydneyとSeoul）を、Asia Pacific（アジア太平洋）地域に指定します。シドニーとソウル。各ロケーションには2つのゲートウェイIPアドレスが割り当てられます。



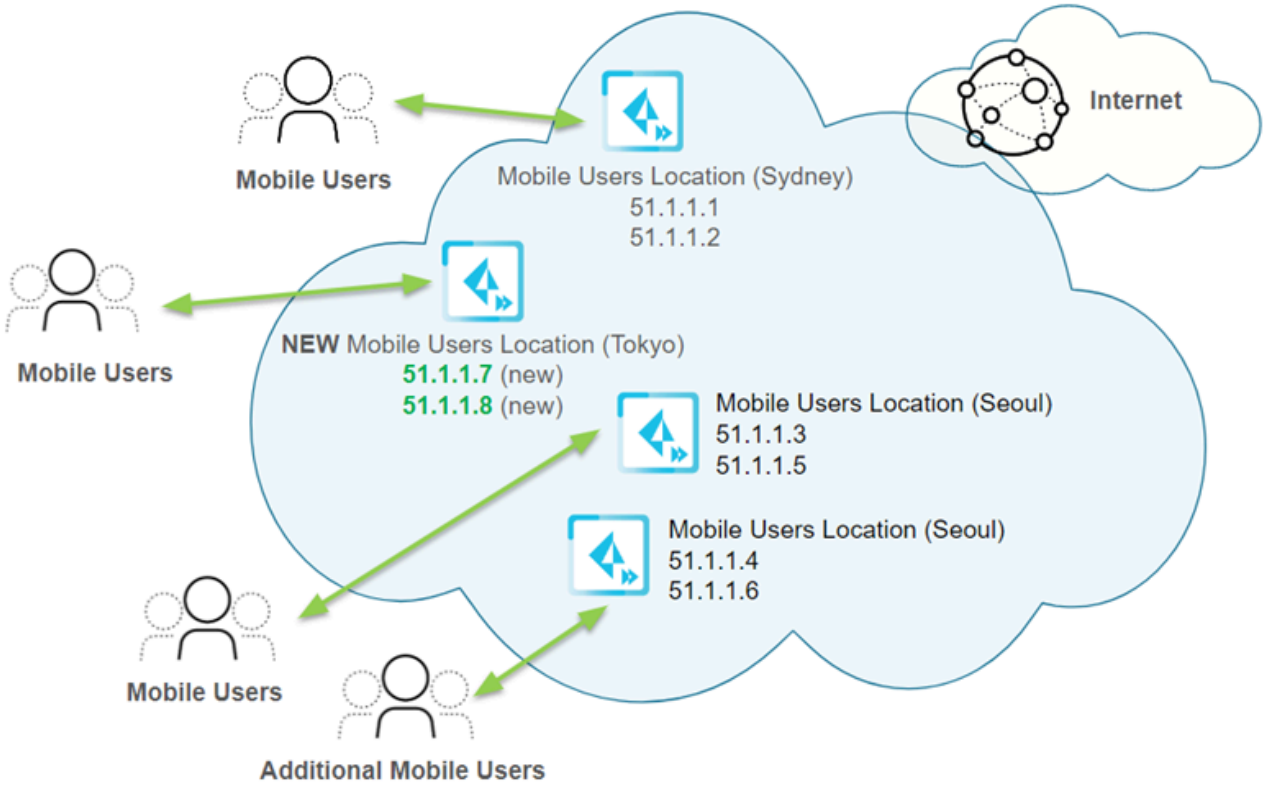
ここで、ロケーションSeoul（ソウル）に、多数のユーザーがログインしました。これらの余分なユーザーを収容するために、Prisma Accessはソウルのロケーション用に2つ目のゲートウェイを追加し、1つ目のソウルのゲートウェイからゲートウェイアドレスの1つ（51.1.1.4）を取り出し、2つ目のソウルのゲートウェイに割り当てます。次に、2つの追加IPアドレス (この例では 51.1.1.5 と 51.1.1.6) を追加し、2つのソウル ゲートウェイに追加します。

©2025 Palo Alto Networks, Inc.



次に、アジア太平洋地域に別のロケーション、東京を追加します。 Prisma Accessは新しいゲートウェイに2つの新しいIPアドレス (51.1.1.7 と 51.1.1.8) を作成します。

©2025 Palo Alto Networks, Inc.



ロケーションを追加したり、スケーリング イベントが発生するたびに、Prisma Accessが割り当てた新しいイグレスとゲートウェイのIPアドレスを取得し、ネットワーク内の許可リストに追加する必要がある。Prisma Accessは、各ロケーションのすべてのアクティブなゲートウェイのために、常に2組のIPアドレスを保持しています。

ループバックIPアドレスの割り当て (モバイル ユーザー)

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

ループバックアドレスは、Prisma Accessが内部ソースへのリクエストに使用するIPアドレスで、インフラストラクチャサブネットから割り当てられたものです。インフラストラクチャまたはデータプレーンのアップグレード中に、モバイル ユーザーのループバックIPアドレスが変更される場合があります。

インフラストラクチャまたはデータプレーンのアップグレード中、サービス接続またはリモート ネットワーク接続のループバック*IP*アドレスは変更されません。変更される可能性があるのは、モバイル ユーザーのループバック*IP*アドレスのみです。

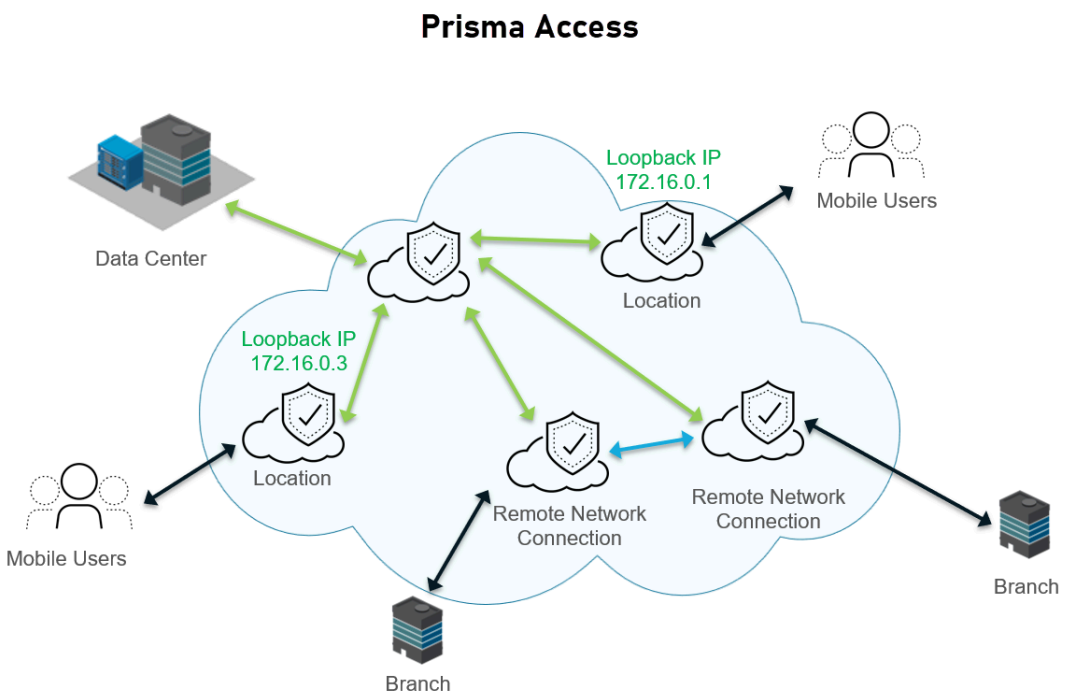
©2025 Palo Alto Networks, Inc.

Prisma Accessは、Prisma Accessインフラストラクチャを有効にするときに指定したインフラストラクチャのサブネットから、ループバックIPアドレスを割り当てます。インフラストラクチャサブネット全体を許可リストに追加し、インフラストラクチャまたはデータプレーンのアップグレード中にモバイル ユーザー ループバックIPの変更を計画する必要がなくなります。インフラストラクチャ サブネットを見つけるには、次を選択します。

- Prisma Access (Managed by Strata Cloud Manager):**[Workflows (ワークフロー)]** > **Prisma Access [Setup (セットアップ)]** > **Prisma Access** > **[Infrastructure Settings (インフラストラクチャ設定)]** と **[Infrastructure Subnet (インフラストラクチャサブネット)]**を表示します
- Prisma Access (Managed by Panorama):**[Panorama]** > **[Cloud Services (クラウド サービス)]** > **[Status (ステータス)]** > **[Network Details (ネットワーク詳細)]** > **[Service Infrastructure (サービス インフラストラクチャ)]** と進み **[Infrastructure Subnet (インフラストラクチャ サブネット)]**を表示します

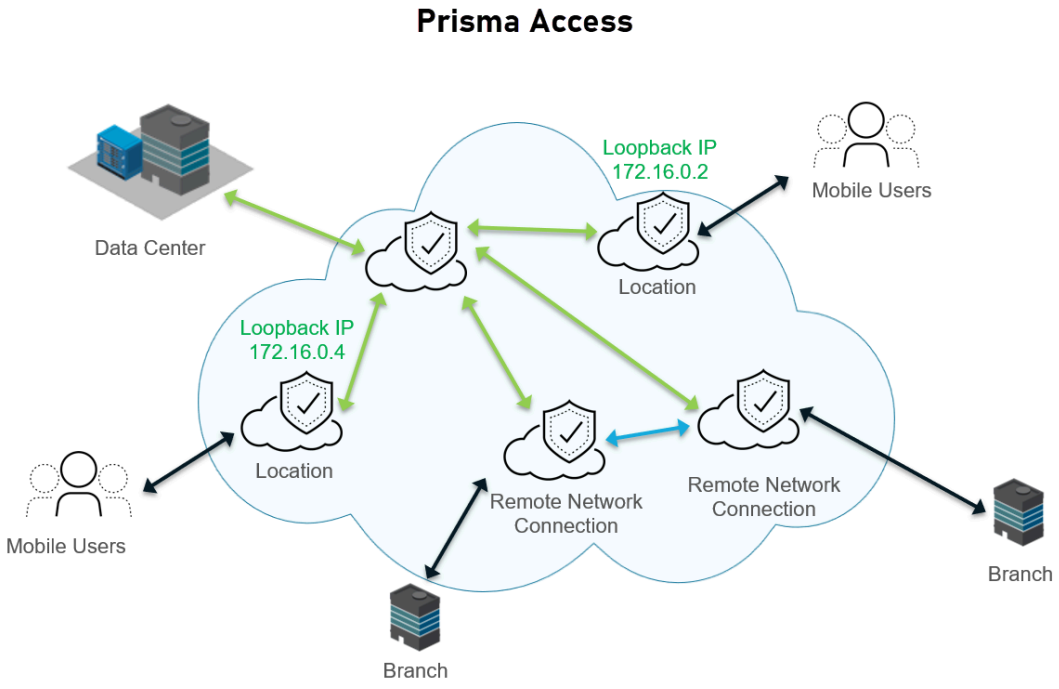
パブリックIPアドレスとループバックIPアドレスを取得するために使用されるAPIを使用して、これらのアドレスを取得します。

次の例は、インフラストラクチャサブネットが 172.16.0.0/16 であるPrisma Accessのデプロイメントを示したものです。 Prisma Accessは、インフラストラクチャサブネットからモバイルユーザー用にループバックIPアドレス172.16.0.1と172.16.0.3を割り当てています。



たとえば、Cloud Servicesプラグインの新リリースの準備などの理由で、インフラまたはデータプレーンがアップグレードされると、Prisma Accessはモバイルユーザー向けにインフラサブネットから2つの異なるIPアドレスを割り当てます（172.16.0.1は172.16.0.2に変更、172.16.0.3は172.16.0.4に変更）。

©2025 Palo Alto Networks, Inc.

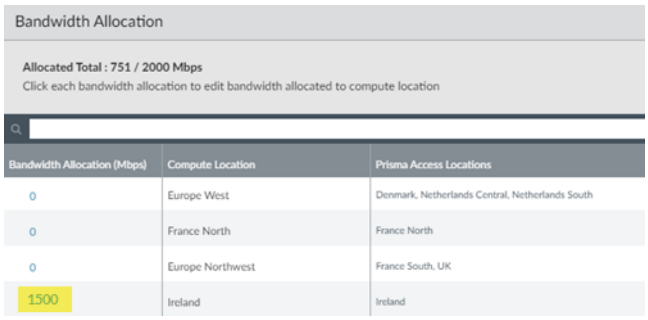


©2025 Palo Alto Networks, Inc.

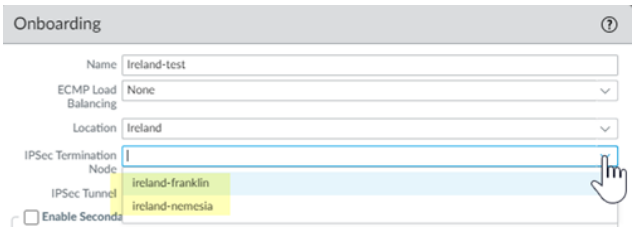
リモートネットワーク:IPSec終端ノードと サービスIPアドレス

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

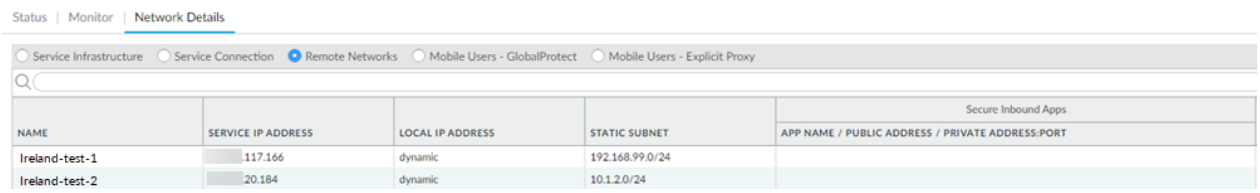
リモート ネットワークをオンボードすると、それが *IPSec* 終端ノードに関連付けされ、各IPSec終端ノードには サービス**IP**アドレス が関連付けられます。リモート ネットワーク接続用のIPSecトンネルをセットアップするときに、このアドレスをCPEのピアIPアドレスとして使用します。各終端ノードは最大1,000 Mbpsの帯域幅を提供できます。1,000 Mbpsを超える帯域幅をコンピューティング ロケーションに関連付けると、複数の サービス**IP**アドレスが提供されます。



アイルランドのコンピューティング ロケーションでリモート ネットワークをオンボードする場合、合計帯域幅が 1,000 Mbpsを超えるため、2つのIPSec終端ノードの選択肢が提供されます。



各IPSec終端ノードには **[Panorama]** > **[Cloud Services (**クラウド サービス**)]** > **[Status (**ステータス**)]** > **[Network Details (**ネットワーク詳細**)]** > **[Remote Networks (**リモート ネットワーク**)]**で確認できるように、独自のサービス**IP**アドレスがあります。



 ©2025 Palo Alto Networks, Inc.

リモートネットワーク:帯域幅割り当てに関連するIPアドレスの変更

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

このセクションは、ロケーションごとに帯域幅を割り当てるレガシーPrisma Accessデプロイメントがある場合に適用されます。新しいデプロイメントではコンピューティングロケーションごとに帯域幅を割り当てます。 Prisma AccessがこれらのIPアドレスをどのように割り当てるかについては、リモートネットワーク:IPSec終端ノードと サービスIPアドレスを参照してください。

リモートネットワーク接続用のIPアドレスは一意で共有されず、Prisma Accessデプロイメント環境専用のアドレスとなります。これらのIPアドレスは、Prisma Accessがリモートネットワークのオンボーディングの一環として作成した後は変更されず、アップグレード後もIPアドレスが維持されます。ただし、既存の接続の帯域幅を増やす場合、増加によりロケーションの帯域幅が500 Mbpsを超えると、リモートネットワークのIPアドレスが変更される可能性があるため、注意を払う必要があります。

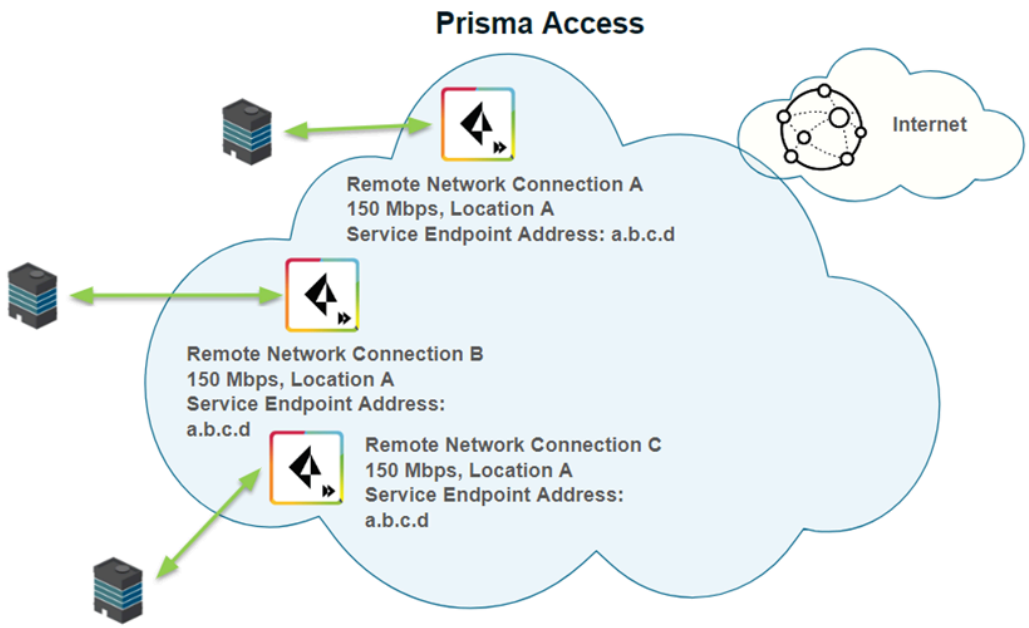
また、*Prisma Access*が新しい*Prisma Access*コンピュート リージョンを作成し、すでにオンボーディングしているロケーションでその新しいリージョンを使用する場合、出口*IP*アドレスが変更される可能性があります。

これらの帯域幅のガイドラインは、既存の接続をアップグレードする場合にのみ適用されます。単一のリモート ネットワーク接続は、1000 Mbps (プレビュー) 接続であっても、そのサイズに関係なく、常に単一の サービス**IP**アドレスを受け取ります。

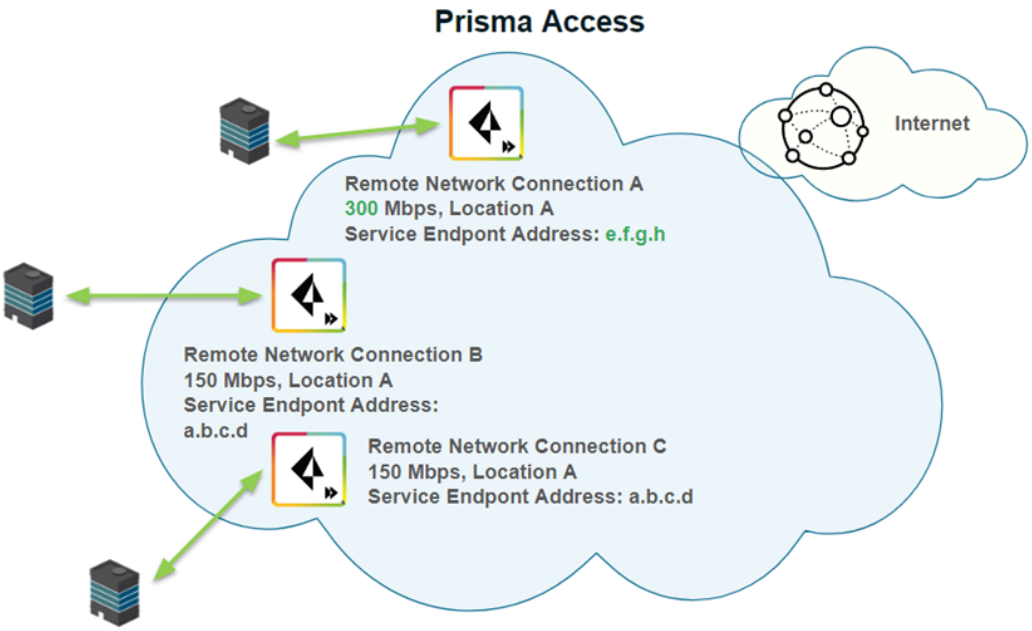
*1000 Mbps*帯域幅オプションはプレビュー モードです。プレビュー中のスループットはベストエフォート方式で配信され、実際のパフォーマンスはトラフィックの組み合わせによって異なります。

同じロケーション内にある、それぞれ帯域幅が150 Mbpsである3つのリモートネットワーク接続の例を次に示します。合計帯域幅は500 Mbpsになるので、Prisma Accessはそのロケーション内のすべての接続に対して、単一のIPアドレスを割り当てます。

©2025 Palo Alto Networks, Inc.



次の例は、リモートネットワーク接続Aの帯域幅を150 Mbpsから300 Mbpsに増やした場合を表しています。すべての接続の合計帯域幅が500Mbpsを超えているため、 Prisma Accessは追加の帯域幅を持つ接続に新しいサービスIPアドレス を割り当てます。その他のサービスIPアドレスは変更されません。



逆に、帯域幅が100 Mbpsのリモート ネットワークが4つある場合、リモート ネットワークの1つの帯域幅を100 Mbpsに増やしても、合計帯域幅が500 Mbpsになるため、そのリモート ネットワークの サービスIPアドレスは変更されません。

 ©2025 Palo Alto Networks, Inc.

リモート ネットワーク接続の帯域幅を削減しても、 サービス***IP***アドレスは変更されません。

Panoramaでサービス**IP**アドレスのを見つけるには、**Panorama** > クラウド サービス > ステータスの > **[Network Details (**ネットワーク詳細**)]**タブを選択し、 **[Remote Networks (**リモート ネットワーク**)]**のラジオ ボタンをクリックして、リモート ネットワークの サービス**IP**アドレスのを表示するか、APIスクリプトを使用します。

©2025 Palo Alto Networks, Inc.

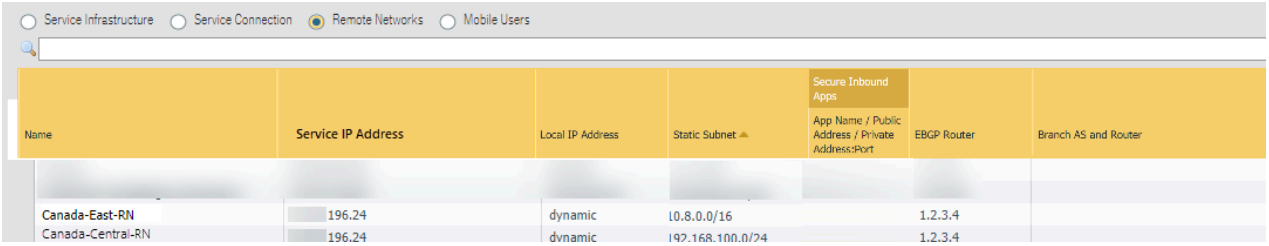
リモートネットワーク:サービスIPアドレス と出力IPアドレスの割り当て

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

Prisma Accessでは、世界的なデプロイメントに対応し、その地域に応じた体験を提供するために、100ヶ所以上ものロケーションが用意されています。2つのロケーションが同じ にマップされる場合があり、これはリモート ネットワーク接続用のIPSecトンネルを設定するときにピアIPアドレスとして使用されます。ただし、ユーザーが地域に対して正しいデフォルト言語を利用できるように、ロケーションが異なる出口IPアドレスを使用することもあります。

サービス接続では、インターネットへの出力がサポートされていないため、言語のローカリゼーションはサポートされません。 *Prisma Access*によって、サービス接続ごとに*1*つのサービス*IP*アドレス のみが割り当てられ、その*IP*アドレスは、オンボーディング時に指定した場所に対応するコンピューティング ロケーションに地理的に登録されます。

次の例では、カナダに2つのリモート ネットワーク ロケーションがデプロイされている顧客デプロイメントを示しています。カナダ中部とカナダ東部。 Prisma Accessでは、両方の場所に同じ サービスIPアドレス、 が割り当てられています。リモートネットワークトンネルを設定する場合、リモートネットワーク接続のIPSecトンネルを作成する際には、このIPアドレスをピアIPアドレスとして使用します。



ただし、カナダ東部では、カナダ中部 (英語) とは異なるデフォルト言語 (フランス語) が使用されます。このため、 Prisma Accessは異なる出力IPアドレスを割り当てます。エグレスIPアドレスに対してAPIスクリプトを実行した場合、これらの2つのロケーションの2つの異なるIPアドレスが返されます。

©2025 Palo Alto Networks, Inc.

Prisma AccessのIPアドレスを取得する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス

Prisma AccessインフラのIPアドレスを手動でネットワークの許可リストに追加している、またはエンタープライズアプリケーションへのインバウンドアクセスを制限するために自動スクリプトを使ったIPベースの制限を採用している場合、これらのアドレスがどのような役割を果たしているのか、なぜそれらを許可するのか、およびそれを取得するために実施する作業について理解しておく必要があります。

Prisma Accessは、Prisma Accessの設定を完了するまで、これらのIPアドレスを提供しません。デプロイメントが完了したら、APIスクリプトを使用してこれらのIPアドレスを取得します。APIスクリプトは、 Prisma Access UI と、取得するアドレスを指定するために作成した .txt ファイルを使用します。

Prisma Access設定が完了するまでこれらの作業を行う必要はありませんが、事前に作業の概念を理解しておけば、デプロイ完了後に何をすればいいのかを素早く判断できます。

- Strata Cloud Manager
- Panorama

Prisma AccessのIPアドレスを取得する （Strata Cloud Manager）

Prisma Access インフラストラクチャIPアドレス

各デプロイメントタイプに対してPrisma Accessが使用するIPアドレス、IPアドレスを取得するためにAPIスクリプトを実行する場合に使用するキーワード、およびそれを許可リストに追加する必要があるかどうかについての情報を、次の表に示します。

デプロイメント タイプ	IPアドレスタイプ ：	詳説
モバイルユーザー	Prisma Access ゲートウェイ (**gp_gateway**)	ゲートウェイのIPアドレスを取得します。モバイル ユーザーデプロイメントの許可リストにゲートウェイとポータルの両方のIPアドレスを追加します。 モバイルユーザーは、SaaSパブリックアプリケーションなどの内部またはインターネットリソースにアクセスするために、Prisma Accessゲートウェイに接続します。

©2025 Palo Alto Networks, Inc.

デプロイメント タイプ	IPアドレスタイプ：	詳説
	Prisma Access ポータル (**gp_portal**)	ポータルのIPアドレスを取得します。モバイル ユーザーデプロイメントの許可リストにゲートウェイとポータルの両方のIPアドレスを追加します。 モバイルユーザーは、初期設定とゲートウェイのロケーションを取得するために、Prisma Accessポータルにログインします。
	ループバックIPアドレス	このアドレスは、Prisma Accessが内部ソースに対して行われるリクエスト向けに使用するソースIPアドレスで、インフラサブネットから割り当てられます。Prisma Accessを、RADIUSやActive Directory (アクティブディレクトリ - AD)認証などの、内部リソースにアクセスさせるには、ループバックIPアドレスを許可リストに追加します。 モバイルユーザーのループバックIPアドレスは変更される可能性があるため、ネットワーク内のインフラサブネット全体のIPアドレスを許可することをお勧めします。
モバイルユーザー - 明示型プロキシ	認証キャッシュ サービス (ACS)	明示型プロキシユーザの認証状態を保存するPrisma Accessサービスのアドレス。 このアドレスは、モバイル ユーザー (明示型プロキシ) のデプロイメントにのみ使用されます。
	TCP (ネットワーク) ロードバランサー。	Prisma Accessが明示型プロキシ ネットワーク ロードバランサに使用するアドレス。 このアドレスは、モバイル ユーザー (明示型プロキシ) のデプロイメントにのみ使用されます。
リモートネットワーク	リモートネットワークのIPアドレス（**remote_network**）	Prisma AccessがPrisma Accessリモートネットワーク接続用に割り当てるサービスIPアドレスと、Prisma Accessがリモート ネットワーク・ユーザーがその地域の正しいデフォルト言語を取得できるよ

©2025 Palo Alto Networks, Inc.

デプロイメント タイプ	IPアドレスタイプ：	詳説
		うにするために使用する出口IPアドレスが含まれます。Prisma Accessがインターネットリソースにアクセスできるように、これらのアドレスをネットワークの許可リストに追加してください。
	ループバックIPアドレス	Prisma Accessが内部ソースに対して行われるリクエスト向けに使用するソースIPアドレスで、インフラサブネットから割り当てられます。Prisma Accessを、RADIUSやActive Directory認証などの、内部リソースにアクセスさせるには、ループバックIPアドレスを許可リストに追加します。

IPアドレスを取得するために使用するAPIスクリプトを実行します

Prisma Accessがインフラで使用するIPアドレスを取得するには、以下の手順に従ってください。

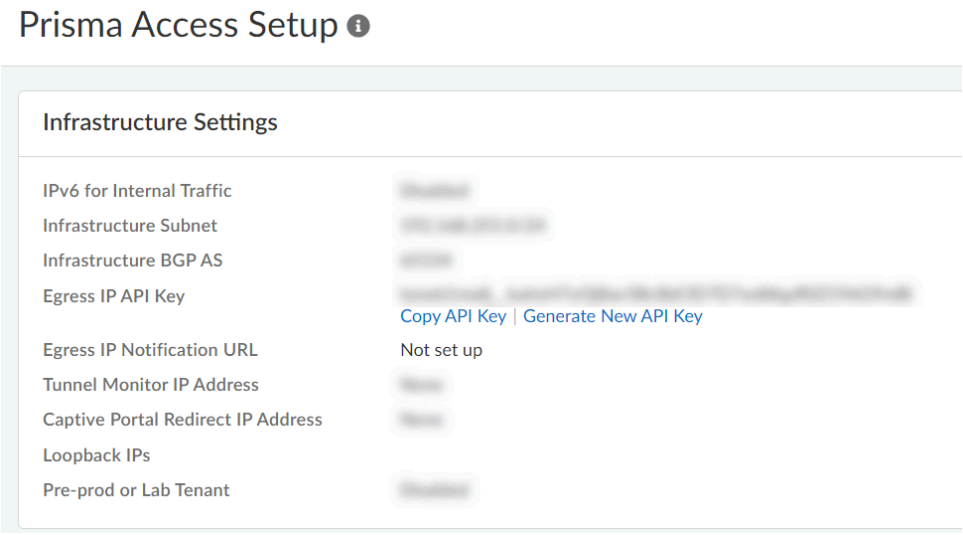
このコマンドは、ループバックアドレスを取得しません。ループバック*IP*アドレスを取得するには、ループバックAPIコマンドを使用してください。

©2025 Palo Alto Networks, Inc.

STEP 1 | API鍵を入手します。

Prisma Accessの認証を受け、APIコマンドを使ってIPアドレスリストを取得するには、このキーが必要になります。

1. Prisma Access (Managed by Strata Cloud Manager)へと進み、**[Workflows (ワークフロー)]** > **[Prisma Accessセットアップ]** > **Prisma Access** > **[Infrastructure Settings (インフラストラクチャ設定)]** を選択します。
2. 新しい **API** キーの生成を選択します。



すでにAPI鍵を生成している場合は、Current Key（現在の鍵）が表示されます。鍵をまだ生成していない、または監査や鍵のローテーションのコンプライアンス基準を満たすために、既存の鍵を置換したい場合は、**Generate New API Key**（新しい**API**鍵の生成）をクリックして新しい鍵を生成します。

STEP 2 | .txtファイルを作成し、ファイルにAPIコマンドオプションを記入します。

APIコマンドを使用するには、2つの手順が必要になります。まず、.txtファイルを作成して、取得するIPアドレスに対するパラメータを指定し、コマンドを実行する場所からアクセス可能なフォルダにファイルを保存します。次に、APIを実行して、作成した.txtファイルの名前と場所をコマンドに指定します。

.txtファイルに、次のキーワードと引数を指定します。このトピックの例ではファイル名として**options.txt**を使用していますが、コマンドに指定できる限り任意のファイル名を使用することができます。

引数	可能な選択肢（キーワード）	コメント
serviceType	**all** **remote_network** **gp_gateway** **gp_portal** **swg_proxy**	**all**– すべてのサービスタイプ（デプロイ環境に応じてリモートネットワーク、モバイルユーザー（ゲートウェイとポータルの両方）、およびClean Pipe）に対して、許可リストに追加する必要があるIPアドレスを取得します。

©2025 Palo Alto Networks, Inc.

引数	可能な選択肢（キーワード）	コメント
	rbi	**remote_network**—リモートネットワークデプロイ環境で許可リストに追加する必要があるIPアドレスを取得します。 **gp_gateway**—モバイルユーザーデプロイ環境向けに、許可リストに追加する必要がある、ゲートウェイIPアドレスを取得します。 **gp_portal** —モバイルユーザーデプロイ環境向けの許可リストに追加する必要がある、ポータルIPアドレスを取得します。 **swg_proxy**—デプロイされた各明示的プロキシの場所、認証キャッシュ サービス (ACS)、およびネットワーク ロード バランサの出力IPアドレスを取得します。 **rbi**— SaaSアプリケーションに接続するために 、リモート ブラウザ分離 (RBI) デプロイメントの許可リストに追加する必要がある出力IPアドレスを取得します。
addrType	**all** **active** **service_ip** **auth_cache_service** **network_load_balancer**	**all** (全て) または **active** (アクティブ)— 許可リストに追加する必要があるすべてのIPアドレスを取得します。 このAPIは、ループバックIPアドレスを取得しません。ループバックIPアドレスを取得するには、従来のAPI コマンドを使用します。 **service_ip**— リモート ネットワーク接続用のIPSec トンネルを設定するときにピアIPアドレスとして使用する サービス**IP**アドレスを取得します。 **auth_cache_service**—明示型プロキシACSのIPアドレスを取得します (モバイル ユーザー - 明示型プロキシデプロイメントにのみ適用)。 **network_load_balancer**—明示型プロキシ ネットワーク ロード バランサのIPアドレスを取得します (モバイル ユーザー (明示型プロキシ デプロイメント) にのみ適用されます)。
アクションタイプ	**pre_allocate**	モバイルユーザー展開のみ-**actionType** が **pre_allocate** の場合、IPアドレスまたはサブネットを取得できます。 Prisma Access モバイル ユーザーデプロイメント用の

©2025 Palo Alto Networks, Inc.

引数	可能な選択肢（キーワード）	コメント
		ゲートウェイとポータル。事前に割り当てられたゲートウェイIPアドレスを取得するには、**serviceType** を **gp_gateway** にしてこれを使用し、事前に割り当てられたゲートウェイIPアドレスを取得するには、**serviceType** を **gp_portal** にしてこれを使用します。 事前に割り当てられたIPアドレスを取得すると、モバイル ユーザーの場所をオンボードする前に、ゲートウェイとポータルのIPアドレスを組織の許可リストに追加できます。これにより、場所をオンボードした直後にモバイル ユーザーが外部のSaaSアプリにアクセスできるようになります。
location	**all** **deployed**	**all**—すべてのロケーションからIPアドレスを取得します。モバイルユーザーデプロイ環境の場合、オンボーディング時に追加したロケーションと追加しなかったロケーションの両方のロケーションのIPアドレスを取得します。 **deployed**—モバイルユーザーのオンボーディング時に追加したすべてのロケーションのIPアドレスを取得します。 このキーワードはモバイル ユーザーのデプロイメントにのみ適用されます。 Prisma Access モバイル ユーザーのオンボーディング中にその場所を選択しなかった場合でも、プロビジョニング中にすべてのモバイル ユーザーの場所にIPアドレスを関連付けます。**all**を指定した場合、このAPIコマンドはデプロイ環境に対して選択しなかったロケーションも含めて、すべてのモバイルユーザーロケーションのIPアドレスを取得します。**deployed**を指定した場合、オンボーディング時に選択したロケーションのIPアドレスのみが取得されます。

.txtファイルにオプションを、次の形式で指定します。

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


©2025 Palo Alto Networks, Inc.

STEP 3 | IPアドレスを取得するには、次のコマンドを入力します:

- Prisma Access 2.1 で導入された新しい API を使用するには、次のコマンドを入力します。

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

2023 年 5 月現在、一部のクラウド管理デプロイメントでは https://api.prod6.datapath.prismaaccess.com/getPrismaAccessIP/v2 が使用されます (URL では prodではなく prod6 に注意してください)。

- レガシー API を使用するには、次のコマンドを入力します。このコマンドは、2022 年 5 月に廃止される予定のレガシー API エンドポイントを使用します。

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

ここで、*option.txt* は前の手順で作成した .txt ファイルであり、*Current-API-Key*はPrisma AccessAPI キーです。

たとえば、.txtファイル名が**option.txt**で、APIキーが**12345abcde**の場合、次のAPIコマンドを使ってすべてのロケーションのパブリックIPアドレスを取得します：

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

API コマンドは大量の情報を返すことができます。出力を読みやすくするために、*Python* がインストールされている場合は、*CURL*コマンドの最後に | *python -m json.tool* を追加できます。

API コマンドは次の形式でアドレスを返します。

```
{ "result": [ { "address_details": [ { "address":"1.2.3.4" "allow_listed": false "addressType": "address-type" "serviceType": "service-type" } ], "addresses": [ "1.2.3.4" ] "zone": "zone-name", "zone_subnet": [zone-subnet ] }, "status": "success"
```

ここで:

- **address_details** は、 各場所の住所の詳細を表示します。
  - **serviceType**はIPアドレスのタイプ（リモートネットワーク（**remote_network**）、Prisma Accessゲートウェイ（**gp_gateway**）、 Prisma Access ポータル (**gp_portal**)、クリーン パイプ (**clean_pipe**)、 またはリモート ブラウザー分離 (**rbi**)。
  - **addressType** は、 addrType キーワードで指定されたアドレスのタイプ (モバイル ユーザーの場所にIPアドレスを事前割り当てする場合は、**active** または **pre-allocated** の いずれか) を指定します。

 ©2025 Palo Alto Networks, Inc.

- **address** は、 許可リストに追加する必要があるIPアドレスを示します。

  APIが複数のIPアドレスを返す場合、 Prisma Accessアドレス フィールドにIPアドレスを要約します。
- アドレスには、 許可リストに追加する必要がある場所のすべてのIPアドレスが一覧表示されます。
- ゾーン は Prisma AccessIPアドレスに関連付けられた場所。
- **zone_subnet**は 、モバイル ユーザー ゲートウェイおよびポータルのサブネットです。Prisma Access は、モバイル ユーザーの場所にIPアドレスを事前割り当てする場合にもこのサブネットを提供します。

.txtファイル内のオプションに何か問題があった場合は、次のようなエラーが返されます:

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

STEP 4 | 取得したIPアドレスを使って、オンプレミスサーバーまたはSaaSアプリケーションポリシールールの許可リストを更新します。

APIコマンドの例

APIコマンドの.txtファイルにキーワードと引数を入力する場合、次の例を利用してください。コマンドの出力を変更するには、.txtファイル内のオプションを変更します。コマンド自体は変更しません。

これらのIPアドレスの取得	.txtファイルにこれらのパラメータを指定	コメント
モバイルユーザーのIPアドレス		
すべてのモバイルユーザーのIPアドレス	`{ "serviceType": "gp_gateway", "addrType": "all", "location": "all" }`	*addrType* が *all* の場合、 Prisma Access すべてのモバイル ユーザー ゲートウェイIPアドレスを取得します。 すべて の 場所 とは、 Prisma Access オンボードされていない場所も含め、利用可能なすべての場所のIPアドレスを取得します。Prisma Access オンボードされていない場所のIPアドレスを予約して、オンボードする前にこれらのIPアドレスを許可リストに追加できるようにします。
オンボードされたモバイルユーザー	`{ "serviceType": "gp_gateway", "addrType": "al`	*location*タイプに*deployed*を指定すると、モバイルユーザーのオン

©2025 Palo Alto Networks, Inc.

これらのIPアドレスの取得	.txtファイルにこれらのパラメータを指定	コメント
の場所のIPアドレス	`l", "location": "deployed" }`	ボーディング時に選択したロケーションのIPアドレスのみがPrisma Accessによって取得されます。
オンボーディングされたモバイルユーザーロケーションのすべてのアクティブなIPアドレス	`{ "serviceType": "gp_gateway", "addrType": "active", "location": "deployed" }`	*addrType* が *active* の場合、Prisma Access オンボードした場所のIPアドレスのみを取得します。
リモートネットワークのIPアドレス		
すべてのリモートネットワークのIPアドレスを取得します	`{ "serviceType": "remote_network", "addrType": "all", "location": "all" }`	このコマンドは、オンボーディングしたリモートネットワークのパブリックIPアドレスと出口IPアドレスを取得します。デプロイされた場所 を使用しないでください。*addrType*に*active*を指定することは可能ですが、この場合*addrType*に*all*を指定したのと同じアドレスが取得されます。
明示型プロキシIPアドレス		
デプロイされたロケーションのACSIPアドレスを取得する	`{ "serviceType": "swg_proxy", "location": "deployed", "addrType": "auth_cache_service" }`	このコマンドは、明示型プロキシデプロイメントのACSIPアドレスを取得します。*addrType* に *all* を入力すると、すべてのアドレスタイプ (ACS およびネットワークロード バランサのIPアドレス) が取得されます。
リモートブラウザ分離IPアドレス		
デプロイされたロケーションのリモート ブラウザ分離 (RBI)IPアドレスを取得します。	`{ "serviceType": "rbi", "location": "all", "addrType": "all" }`	このコマンドは、デプロイされた各RBIロケーション出口IPアドレスを取得します。これらのIPアドレスを許可リストに追加して、SaaS アプリケーションに接続できます。

©2025 Palo Alto Networks, Inc.

IPアドレスおよびループバックアドレスの取得に使われる従来のスクリプト

Prisma Accessとともに使われる、古いAPIスクリプトで利用できるキーワードとパラメータ、およびデプロイメントタイプに応じて使用するAPIに関する情報と推奨事項を次の表に示します。

これらの古いコマンドは、パブリック*IP*アドレスおよび出口*IP*アドレスの2種類のIPアドレスを取得します。許可リストに追加するために必要なすべてのIPアドレスを取得するために、2種類の古いAPIコマンドが用意されています。

- パブリック*IP*アドレスは、Prisma Accessがインターネットベースのソースに対して行われたリクエスト向けに使用するソースIPアドレスです。Prisma Accessを、SaaSアプリケーションやパブリックにアクセス可能なパートナーアプリケーションなどの、インターネットリソースにアクセスさせるには、パブリックIPアドレスを許可リストに設定します。

  モバイルユーザー、リモートネットワーク、Clean Pipeデプロイはパブリックアドレスを使用します。

- 出口*IP*アドレスは、Prisma Accessがインターネットへの出口トラフィックに使用するIPアドレスで、Prisma Accessがインターネットリソースにアクセスできるように、それらのアドレスを許可リストにも追加する必要があります。

  さまざまな目的で使用されますが、Prisma Accessはユーザーが、Prisma Accessロケーションから目的の言語のWebページを受け取れるようにするために、出口IPアドレスを使用します。すべてのロケーションがパブリックIPアドレスを保有していますが、エグレスIPアドレスは持っていないロケーションも存在しています。次のロケーションは、出口IPアドレスを使用しません：

  - バーレーン
  - ベルギー
  - France North（フランス北部）
  - France South（フランス南部）
  - 香港
  - アイルランド
  - 韓国
  - 台湾
  - 英国

  モバイルユーザー、リモートネットワーク、Clean Pipeのデプロイはエグレスアドレスを使用します。

モバイルユーザーデプロイ環境で使用されるコマンド	
コマンド名	コメント
get_egress_ip_all=yesコマンド `curl -k -H header-api-key:`現在の*API*キー`"https://api.gpcloudservice.com/`	Prisma Accessを、SaaSアプリケーションやパブリックにアクセス可能なパートナーアプリケーションなどの、インターネットリソースにアクセスさせるために許可リストに追加する、すべてのIPアドレスを取得します。このコマンドには、以下の制約があります。

©2025 Palo Alto Networks, Inc.

モバイルユーザーデプロイ環境で使用されるコマンド	
コマンド名	コメント
`getAddrList/latest?get_egress_ip_all=yes`	• このコマンドは、大量のアドレスを取得する可能性があります（200件以上）。ご自分の企業が、大量な数のアドレスを許可リストに追加できない場合は、*gpcs_gp_gw*および*gpcs_gp_portal*キーワードを使って現在使用しているIPアドレスのみを取得できます。ただし、この場合ロケーションを追加するたびにコマンドを実行する必要があります。また、スケーリングイベントが発生した場合、新しいIPアドレスを許可リストに追加する必要があります。 • Prisma Accessは、これらのIPアドレスに対応しているロケーションを表示しません。そのため、このコマンドで返されたすべてのIPアドレスを許可リストに追加することをお勧めします。 • このコマンドで、ループバックアドレス取得されません。
gpcs_gp_gwおよび**gpcs_gp_portal**キーワード `curl -k -H header-api-key:`*Current-API-Key*`"https://api.gpcloudservice.com/getAddrList/latest?fwType=gpcs_gp_gw | gpcs_gp_portal&addrType=public_ip | egress_ip_list | loopback_ip"`	デプロイ環境で許可リストに追加できるIPアドレス数が制限されている場合に、このコマンドを使用します。このコマンドで返されたすべてのIPアドレスを、ネットワークの許可リストに追加します。このコマンドでは、ループバックIPアドレスを取得することもできます。

リモートネットワークデプロイ環境で使用されるコマンド	
コマンド名	コメント
gpcs_remote_networkキーワード `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"`	リモートネットワークデプロイ環境で許可リストに追加する必要があるIPアドレスを検索する場合に、このコマンドを使用します。 このコマンドを使って、リモートネットワークデプロイ環境の出口IPアドレスを検索することもできます。出口IPアドレスは、状況によって異なる場合があります。

©2025 Palo Alto Networks, Inc.

Clean Pipeデプロイ環境で使用されるコマンド	
コマンド名	コメント
gpcs_clean_pipeキーワード `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"`	Clean Pipeデプロイ環境で許可リストに追加する必要があるIPアドレスを検索する場合に、このコマンドを使用します。

モバイルユーザーデプロイ環境のパブリック/エグレス**IP**アドレスの取得

このレガシー スクリプトは、 新しいAPIスクリプトに置き換えられました。Palo Alto Networksでは、ループバック アドレスを除くすべてのIPアドレスを取得するには、新しいスクリプトを使用することをお勧めします。

モバイルユーザーにSaaSまたはパブリックアプリケーションへのアクセスを許可するためにパブリックIPアドレスを許可リストに追加する場合は、 Prisma Accessはゲートウェイとポータルの IPアドレスごとに2つのIPアドレスが提供されるため、スケーリングやその他のイベント中に1つのIPアドレスを使用できます。IPアドレスセットをそれが使用される前に許可リストに設定し、スケーリングイベント中にSaaS/パブリックアプリケーションにアクセスできるようにして、モバイルユーザーに関する問題を防止することができます。

これらの新しいアドレスを取得するには、次の作業を実施します。

STEP 1 | APIキーを取得するには、**[Workflows (ワークフロー)]** > **[Prisma Accessのセットアップ]** > **Prisma Access** > **[Infrastructure Settings (インフラストラクチャの設定)]** > **[Generate New API Key (新しいAPIキーの生成)]**を選択します。

Prisma Accessの認証を受け、以下に記載しているURLコマンドを使ってIPアドレスリストを取得するには、この鍵が必要になります。Panorama管理者またはSuperuserのみが、このAPI鍵を生成または利用できます。

STEP 2 | モバイルユーザーのパブリックIPアドレスを取得するには、次のいずれかのコマンドを入力します：

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

ここでの*Current-API-Key* はPrisma Access API キーです。

たとえば、API鍵が**12345abcde**の場合、次のAPIコマンドを使ってすべてのロケーションのパブリックIPアドレスを取得します：

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


©2025 Palo Alto Networks, Inc.

パブリック、ループバック、エグレスIPアドレスの取得

パブリック、ループバック、出口IPアドレスを取得するには、次の作業を行ってください。

STEP 1 | Prisma AccessのパブリックIPアドレス、ループバックIPアドレス、またはその両方を取得します。

API キーと API エンドポイント URL を手動で、または自動化スクリプトで使用します:

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

ここで、現在の API キーを自分の API キーに置き換え、次のキーワードと引数のいずれかまたは両方を使用する必要があります。

キーワードの	説明
fwType キーワード	
gpcs_gp_gw	取得 Prisma Access ゲートウェイIPアドレス（モバイルユーザーデプロイメント用）
。**gpcs_gp_portal**	は取得します Prisma Access ポータルIPアドレス（モバイルユーザー展開用）
。**gpcs_remote_network**	は取得します Prisma Access リモートネットワークIPアドレス（リモートネットワーク展開用）
。**gpcs_clean_pipe**	は取得します Prisma Access クリーンパイプIPアドレス。addrType
キーワード	
パブリック**IP**	Prisma Access がインターネット ベースのソースへのリクエストに使用するソースIPアドレスを取得します。 モバイルユーザーロケーションの場合、Prisma Accessにはロケーション別にIPアドレスが表示されます。リモートネットワークの場合、 Prisma Access リモート ネットワーク名別にIPアドレスを一覧表示します。
出力**IP**リスト	IPアドレスを取得します Prisma Access インターネットへの追加の送信トラフィックのためにパブリックIPアドレスを使用します。 モバイルユーザーロケーションの場合、Prisma Accessにはロケーション別にIPアドレスが表示されます。リモート・ネットワークの場合、Prisma Accessはリモート ネットワーク名でIPアドレスをリストします。

©2025 Palo Alto Networks, Inc.

キーワードの	説明
loopback_ip	内部ソースに対するリクエスト（たとえば、RADIUSまたはActive Directoryサーバー）のために使用され、インフラサブネットから割り当てられる、ソースIPアドレスを取得します。

キーワードを指定しない場合は、 Prisma Accessはすべてのアドレスを取得します。

たとえば、すべてのリモート ネットワークのパブリックIPアドレスのリストを手動で取得するには、次の cURL コマンドを試すことができます:

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

または、次の例のようにpythonスクリプトを使ってすべてのIPアドレスのリストを取得できます：

```
  #!/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 | 取得したIPアドレスを使って、オンプレミスサーバーまたはSaaSアプリケーションポリシールールの許可リストを更新します。

モバイルユーザーの場所にIPアドレスを事前割り当てする

Prisma Access モバイル ユーザー - GlobalProtectデプロイメントではゲートウェイとポータルのIPアドレスを使用し、モバイル ユーザー - 明示型プロキシ デプロイメントでは認証キャッシュ サービス (ACS) とネットワーク ロード バランサのIPアドレスを使用します。モバイル ユーザー: GlobalProtectIPアドレスは 出力*IP*アドレスと呼ばれます。ロケーションをオンボードする前にモバイルユーザーのIPアドレスを事前に割り当てる必要がある場合（たとえば、組織がモバイルユーザーに外部SaaSアプリケーションへのアクセスを許可するためにモバイルユーザー–GlobalProtectデプロイメントのIPアドレスを許可リストに追加する必要がある場合）、APIスクリプトを実行して 、 オンボードする前に、事前にこれらのPrisma AccessIPアドレスを場所に割り当てておきます。その後、場所をオンボードする前に、その場所の出力IPアドレスを組織の許可リストに追加できます。

API 応答には、要求された場所の出力IPアドレスのパブリック IP プール サブネットも含まれます。追加した場所の出力IPアドレスは、このサブネットの一部になります。サブネットを許可リ

 ©2025 Palo Alto Networks, Inc.

ストに追加すると、許可リストをさらに変更することなく、将来的に場所を追加できるようになります。

Prisma Accessは、API スクリプトを使用して要求しない限り、IPアドレスとサブネットを事前に割り当てません。事前割り当てスクリプトを実行すると、有効期間は 90 日間になります。これらの IP アドレスとサブネットは一意であり、共有されず、有効期間中はPrisma Accessデプロイメント専用となります。有効期間が終了する前にロケーションをオンボードする必要があります。そうしないと、アドレスが失われます。有効期間をいつでも確認するには、API スクリプトを実行します。

Palo Alto Networks では、後でオンボードする場所に対してのみIPアドレスを事前に割り当てることをお勧めします。

IPアドレスを事前に割り当てるには、次のタスクを完了します。

STEP 1 | Prisma AccessAPI キーを取得します。

STEP 2 | .txt ファイルを作成し、作成した .txt ファイルで次のオプションを指定して、モバイルユーザーの出力IPアドレスを事前に割り当てます。

.txtファイルに次のテキストを入力します。

- モバイル ユーザー - **GlobalProtect**デプロイメント:

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

- モバイル ユーザー - 明示型プロキシ デプロイメント:

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

場所 は Prisma AccessIPアドレスを事前に割り当てる場所です。

最大12個のエントリを入力します。12個以上の場所を入力すると、Prisma Accessが事前に割り当てられたIPアドレスを取得するときにタイムアウトエラーが発生する可能性があります。

STEP 3 | このCURL コマンドを入力します。

©2025 Palo Alto Networks, Inc.

STEP 4 | .txt ファイルを再度開き、既存の情報を削除して編集することで、有効期間を含め、要求した IPアドレスとサブネットを取得します。

- モバイル ユーザー - **GlobalProtect**デプロイメント:
  - 事前に割り当てられたすべてのIPアドレスを取得するようにPrisma Accessに要求するには、.txt ファイルに以下のテキストを入力します。

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

  - 指定された場所のPrisma Accessゲートウェイ用に事前に割り当てられたすべての IP アドレスを取得するようPrisma Accessに要求するには、.txt ファイルに同じ情報を入力するが、.txt ファイルの「`all`」を「`gp_gateway`」に置き換えます。
  - 指定された場所のPrisma Accessポータル用に事前に割り当てられたすべての IP アドレスを取得するようPrisma Accessに要求するには、.txt ファイルに同じ情報を入力するが、.txt ファイルの「`all`」を「`gp_portal`」に置き換えます。
- モバイル ユーザー - 明示型プロキシ デプロイメント:

  Prisma Accessに、明示型プロキシデプロイメントの許可リストに追加する必要があるすべての IP アドレスを事前に割り当てるよう要求するには、.txt ファイルに以下のテキストを入力する。

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

Palo Alto Networks では、許可リストに追加するために必要なすべての事前割り当て済み出力 IPアドレスを取得できるように、 すべて 入力することをお勧めします。



モバイル ユーザー *(GlobalProtect*デプロイメント*)* の場合、*API*コマンドは大量の情報を返すことがあります。出力を読みやすくするために、*Python* がインストールされている場合は、*CURL*コマンドの最後に `| python -m json.tool` を追加できます。

STEP 5 | 事前に割り当てられたアドレスを取得するには、このCURLコマンドを再入力します。

Prisma Accessは次の形式で情報を返します。

```
    "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-
```

 ©2025 Palo Alto Networks, Inc.

```
address2", "service_type":"gp_gateway", "addressType":"pre-
allocated", "validity_period_remaining" :"90 days" } , },
```

ここで、変数は次のAPIコマンド出力を表します。

変数	説明
prisma-access-zone1	事前に割り当てられた IP アドレスが取得されたPrisma Accessのロケーション。
ip-address1 と *ip-address2*	Prisma Accessが指定された場所に事前に割り当てた出口IPアドレス。 Prisma Accessは各場所に対して2つのIPアドレスを取得します。これらのIPアドレスの両方を許可リストに追加する必要があります。
subnet-and-mask1 と *subnet-and-mask2*	Prisma Accessがお使いのデプロイメントの出口IPアドレス用に事前に割り当て、予約したサブネット。
サービスタイプ	事前に割り当てられた出力IPアドレスのタイプ（`gp_portal` または Prisma Access ポータルまたは `gp_gateway`Prisma Access ゲートウェイ）。
有効期間	事前に割り当てられた IPアドレスが有効な残り時間（日数）。 IPアドレスの有効期間が終了する前に、モバイル ユーザーの位置情報をオンボードします。事前に割り当てられた IPアドレスの有効期限が切れた場合は、API スクリプトを再実行して、事前に割り当てられた別の IPアドレスのセットを取得できます。

次のいずれかの条件を満たす場所に対して IPアドレスを事前割り当てしようとすると、エラーが発生する可能性があります。

- すでにその場所をオンボードしています。
- オンボードした後、場所を削除しました。

  この場合、.txt ファイルに次のテキストを入力して、その場所のモバイル ユーザー - GlobalProtect IPアドレスを取得します。

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


©2025 Palo Alto Networks, Inc.

- ライセンスで許可されているモバイル ユーザーの場所の最大数に達したため、これ以上場所を追加することはできません。
- 入力されたロケーション名が誤っています。
- **gp_gateway**以外の **serviceType** を入力しました。
- **pre_allocate**以外の **actionType** を入力しました。

Prisma AccessIPアドレス変更通知をセットアップする

サービス接続、リモートネットワーク接続、およびモバイルユーザーの、リモートネットワークおよびループバックIPアドレス変更に対する、パブリックIPアドレス変更の通知を受けるために、変更のアラートを受け取るURLを指定することができます。Prisma AccessはHTTP POSTリクエストを使って通知を送信します。POSTリクエストには、次の通知データがJSONフォーマットで含まれています：

```
 {"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"}
```

通知を受け取ったら、2ステップの作業を行う必要があります。まず手動で、またはプログラムを使って、IP またはループバックアドレスを取得する必要があります。次に、ユーザーがサービスを利用できないような事態を回避するために、適切な許可リスト内のIPアドレスを更新する必要があります。



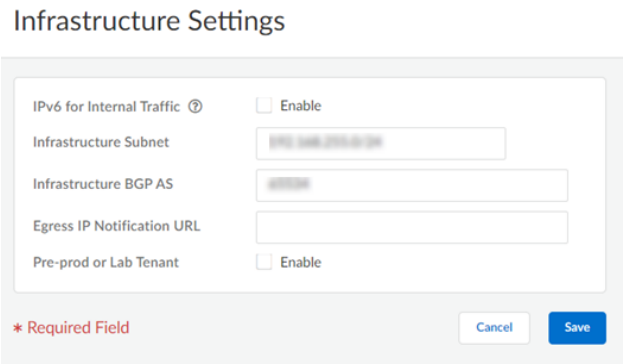
この通知は、*Prisma Access*によって新しい*IP*アドレスがアクティブになる数秒前に送信されます。新しい*IP*アドレスの取得とネットワーク内の許可リストへの追加の両方に、自動スクリプトを使用することをお勧めします。

IP通知URLを追加するには、次の作業を行ってください。

STEP 1 | **[Workflows (ワークフロー)] > [Prisma Accessセットアップ] > Prisma Access > [Infrastructure Settings (インフラストラクチャ設定)]**へ移動します。

©2025 Palo Alto Networks, Inc.

STEP 2 | Prisma Accessインフラストラクチャの**IP**アドレスの変更を通知できるように、**Egress IP Notification URL (**出口**IP**通知**URL)**を追加する。



変更通知をリッスンしているHTTPまたはHTTPS WebサービスにIPアドレスまたはFQDNを指定できます。 Prisma Accessでは、これらの通知は、パブリックIPアドレスを使用してインターネットから送信します。

通知URLを有効にするために構成をプッシュする必要はありません。

Prisma AccessのIPアドレスを取得する （Panorama）

Prisma AccessインフラのIPアドレスを手動でネットワークの許可リストに追加している、またはエンタープライズアプリケーションへのインバウンドアクセスを制限するために自動スクリプトを使ったIPベースの制限を採用している場合、これらのアドレスがどのような役割を果たしているのか、なぜそれらを許可するのか、およびそれを取得するために実施する作業について理解しておく必要があります。

Prisma Accessは、Prisma Accessの設定を完了するまで、これらのIPアドレスを提供しません。デプロイメントが完了したら、APIスクリプトを使用してこれらのIPアドレスを取得します。APIスクリプトは、 Prisma AccessUI と、取得するアドレスを指定するために作成した .txt ファイルを使用します。

*Mobile User-GlobalProtect*をデプロイメントしている場合、この*API*の代わりに*Prisma AccessUI*を使用してパブリック*IP*アドレスの割り当てを管理し、*Prisma Access*が*IP*アドレスを解放する前に*IP*アドレスが許可リストに追加されていることを確認することができます。このようにして、 *Prisma Access*は許可リストに登録された*IP*アドレスのみをプロビジョニングします。

以下の表では、Prisma Accessが各デプロイメントタイプで使用するIPアドレスのリストと、IPアドレスを取得するAPIスクリプトを実行するときに使用するキーワードを示し、組織の許可リストに追加する必要があるかどうかを説明します。

デプロイメント タイプ	IPアドレスタイプ：	詳説
モバイルユーザー — **(GlobalProtect)**	Prisma Access ゲートウェイ **(gp_gateway)**	ゲートウェイIPアドレス。モバイル ユーザーデプロイメントの許可リストにゲートウェイとポータルの両方のIPアド

©2025 Palo Alto Networks, Inc.

デプロイメント タイプ	IPアドレスタイプ：	詳説
		レスを追加する必要があります。 モバイルユーザーは、SaaSパブリックアプリケーションなどの内部またはインターネットリソースにアクセスするために、Prisma Accessゲートウェイに接続します。 モバイル ユーザーの場合、Prisma Accessは初期デプロイメント時に、デプロイする場所ごとに2つのIPアドレスを割り当てます。
	Prisma Access ポータル (**gp_portal**)	ポータルのIPアドレス。モバイル ユーザーデプロイメントの許可リストにゲートウェイとポータルの両方のIPアドレスを追加する必要があります。 モバイルユーザーは、初期設定とゲートウェイのロケーションを取得するために、Prisma Accessポータルにログインします。
	ループバックIPアドレス	Prisma Accessが内部ソースへのリクエストに使用するソースIPアドレスで、Prisma Accessサービスインフラの設定 (Panorama)から割り当てられます。Prisma Accessを、RADIUSやActive Directory (アクティブディレクトリ - AD)認証などの、内部リソースにアクセスさせるには、ループバックIPアドレスを許可リストに追加します。 ループバックIPアドレスは変更される可能性があるため、Palo Alto Networksでは、ネットワーク内のインフラストラクチャ サブネッ

©2025 Palo Alto Networks, Inc.

デプロイメント タイプ	IPアドレスタイプ：	詳細
		ト全体のすべてのIPアドレスを許可することをお勧めします。インフラサブネットを探すには、**Panorama** > **Cloud Services**（クラウドサービス） > **Status**（ステータス） > **Network Details**（ネットワーク詳細） > **Service Infrastructure**（インフラ）の順に選択します。サブネットは、**Infrastructure Subnet**（インフラサブネット）エリアに表示されます。 ループバックIPアドレスを取得するには、従来のAPI スクリプトを使用します。
モバイルユーザー - 明示型プロキシ	認証キャッシュ サービス (ACS)	明示型プロキシユーザの認証状態を保存するPrisma Accessサービスのアドレス。 このアドレスは、 モバイルユーザーの明示型プロキシにのみ使用されます。
	TCP (ネットワーク) ロードバランサー。	Prisma Accessが明示型プロキシ ネットワーク ロードバランサに使用するアドレス。 このアドレスは、 モバイルユーザーの明示型プロキシにのみ使用されます。
リモートネットワーク	リモートネットワークのIPアドレス（**remote_network**）	Prisma AccessがPrisma Accessリモートネットワーク接続に割り当てるサービスIPアドレスと、Prisma Accessがリモートネットワークユーザーがその地域の正しいデフォルト言語を取得できるようにするために使用するリモートネットワーク:サービスIPアドレス と出力IPアドレスの割り当て。Prisma Accessがインターネットリソースにアクセスできるよう

©2025 Palo Alto Networks, Inc.

デプロイメント タイプ	IPアドレスタイプ：	詳説
		に、これらのアドレスをネットワークの許可リストに追加してください。
	ループバックIPアドレス	Prisma Accessが内部ソースへのリクエストに使用するソースIPアドレスで、Prisma Accessサービスインフラの設定 (Panorama)から割り当てられます。Prisma Accessを、RADIUSやActive Directory (アクティブディレクトリ - AD)認証などの、内部リソースにアクセスさせるには、ループバックIPアドレスを許可リストに追加します。ループバックIPアドレスを取得するには、従来のAPIスクリプトを使用します。
Clean Pipe	Clean PipeのIPアドレス（**clean_pipe**）	これらのIPアドレスを許可リストに追加して、Clean Pipeサービスがインターネット リソースにアクセスできるようにします。
	ループバックIPアドレス	Prisma Accessが内部ソースへのリクエストに使用するソースIPアドレスで、Prisma Accessサービスインフラの設定 (Panorama)から割り当てられます。Prisma Accessを、RADIUSやActive Directory (アクティブディレクトリ - AD)認証などの、内部リソースにアクセスさせるには、ループバックIPアドレスを許可リストに追加します。ループバックIPアドレスを取得するには、従来のAPIスクリプトを使用します。

©2025 Palo Alto Networks, Inc.

IPアドレスを取得するために使用するPrisma AccessAPIスクリプトを実行します

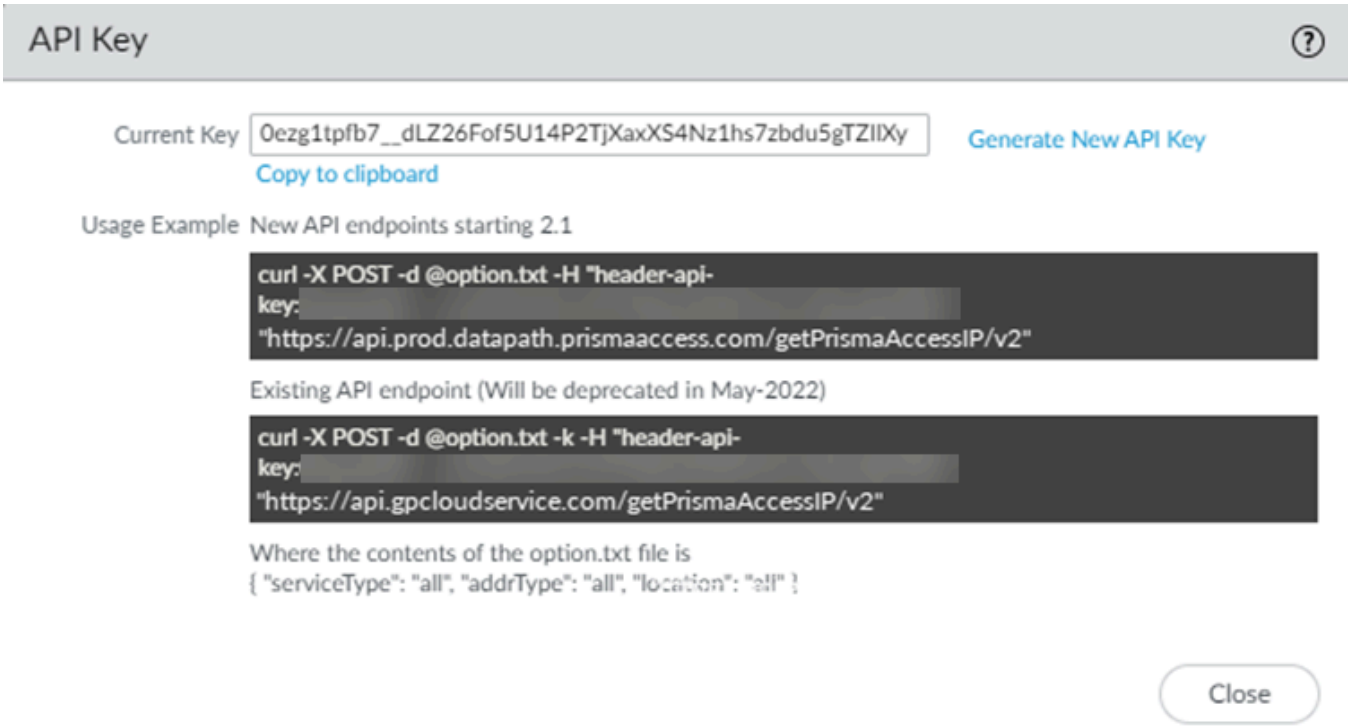
Prisma Accessはインフラストラクチャ内で使用されるパブリック IP アドレスとプライベート IP アドレスを取得するために使用できる API スクリプトを提供します。組織のネットワーク内の許可リストにパブリックIPアドレスを追加する必要がある場合は、次の手順に従って、APIスクリプトでこれらのIPアドレスを取得します。

このコマンドは、ループバックアドレスを取得しません。ループバック*IP*アドレスを取得するには、ループバックAPIを使用してください。

STEP 1 | API鍵を入手します。

Prisma Accessの認証を受け、APIコマンドを使ってIPアドレスリストを取得するには、このキーが必要になります。Panorama管理者またはSuperuserのみが、このAPI鍵を生成または利用できます。

1. **[Panorama] > [Cloud Services**（クラウドサービス）**] > [Configuration**（設定）**] > [Service Setup**（サービスのセットアップ）**]**を選択します。
2. **Generate API Key**（**API**鍵の生成）を選択します。



すでにAPI鍵を生成している場合は、**Current Key**（現在の鍵）が表示されます。鍵をまだ生成していない、または監査や鍵のローテーションのコンプライアンス基準を満たすために、既存の鍵を置換したい場合は、**Generate New API Key**（新しい**API**鍵の生成）をクリックして新しい鍵を生成します。

STEP 2 | .txtファイルを作成し、ファイルにAPIコマンドオプションを記入します。

APIコマンドを使用するには、2つの手順が必要になります。まず、.txtファイルを作成して、取得するIPアドレスに対するパラメータを指定し、コマンドを実行する場所からアクセス可

 ©2025 Palo Alto Networks, Inc.

能なフォルダにファイルを保存します。次に、APIを実行して、作成した.txtファイルの名前と場所をコマンドに指定します。

.txtファイルに、次のキーワードと引数を指定します。例については、Prisma AccessIPアドレスを取得するためのAPI例を参照してください。このドキュメントの例ではファイル名として**options.txt**を使用していますが、コマンドに指定できる限り任意のファイル名を使用することができます。

引数	可能な選択肢（キーワード）	コメント
serviceType	**all** **remote_network** **gp_gateway** **gp_portal** **clean_pipe** **swg_proxy** **rbi**	**all**– すべてのサービスタイプ（デプロイ環境に応じてリモートネットワーク、モバイルユーザー（ゲートウェイとポータルの両方）、およびClean Pipe）に対して、許可リストに追加する必要があるIPアドレスを取得します。 **remote_network**–リモートネットワークデプロイ環境で許可リストに追加する必要があるIPアドレスを取得します。 **gp_gateway**–モバイルユーザーデプロイ環境向けに、許可リストに追加する必要がある、Mobile Users–GlobalProtectゲートウェイIPアドレスを取得します。 **gp_portal**–モバイルユーザーデプロイ環境向けに、許可リストに追加する必要がある、Mobile Users–GlobalProtectポータルIPアドレスを取得します。 **clean_pipe**–Clean Pipeデプロイ環境向けの許可リストに追加する必要がある、IPアドレスを取得します。 **swg_proxy**–デプロイされた各明示型プロキシの場所、認証キャッシュ サービス (ACS)、およびネットワーク ロード バランサの出力IPアドレスを取得します。

©2025 Palo Alto Networks, Inc.

引数	可能な選択肢（キーワード）	コメント
		rbi— SaaSアプリケーションに接続するために 、リモートブラウザ分離 (RBI) デプロイメントの許可リストに追加する必要がある出力IPアドレスを取得します。
addrType	**all** **active** **service_ip** **auth_cache_service** **network_load_balancer**	**all** (全て) または **active** (アクティブ)— 許可リストに追加する必要があるすべてのIPアドレスを取得します。 このAPIは、ループバックIPアドレスを取得しません。ループバックIPアドレスを取得するには、従来のAPIを使用します。 **service_ip**— リモート ネットワーク接続用の IPSec トンネルを設定するときにピアIPアドレスとして使用する サービスIPアドレスを取得します。 **auth_cache_service**—明示型プロキシACSのIPアドレスを取得します (明示型プロキシデプロイメントにのみ適用されます)。 **network_load_balancer**—明示型プロキシ ネットワーク ロード バランサのIPアドレスを取得します (明示型プロキシのデプロイメントにのみ適用されます)。
アクションタイプ	**pre_allocate**	モバイルユーザー展開のみ-**actionType** が **pre_allocate** の場合、IPアドレスまたはサブネットを取得できます。Prisma Access モバイル ユーザーデプロイメント用のゲートウェイとポータル。事前に割り当てられたゲートウェイIPアドレスを取得するには、**serviceType**を**gp_gateway**に

 ©2025 Palo Alto Networks, Inc.

引数	可能な選択肢（キーワード）	コメント
		してこれを使用し、事前に割り当てられたポータルIPアドレスを取得するには、**serviceType**を**gp_portal**にしてこれを使用します。 事前に割り当てられたIPアドレスを取得すると、モバイル ユーザーの場所をオンボードする前に、ゲートウェイとポータルのIPアドレスを組織の許可リストに追加できます。これにより、場所をオンボードした直後にモバイルユーザーが外部のSaaSアプリにアクセスできるようになります。
location	**all** **deployed**	**all**—すべてのロケーションからIPアドレスを取得します。モバイルユーザーデプロイ環境の場合、オンボーディング時に追加したロケーションと追加しなかったロケーションの両方のロケーションのIPアドレスを取得します。 **deployed**—モバイルユーザーのオンボーディング時に追加したすべてのロケーションのIPアドレスを取得します。 このキーワードはモバイルユーザーのデプロイメントにのみ適用されます。 Prisma Accessは、モバイル ユーザーのオンボーディング中にその場所を選択しなかった場合でも、プロビジョニング中にすべてのモバイル ユーザーの場所にIPアドレスを関連付けます。**all**を指定した場合、このAPIコマンドはデプロイ環境に対して選択しなかったロケーションも含めて、すべてのモバイルユーザーロケーションのIPアドレスを取得し

©2025 Palo Alto Networks, Inc.

引数	可能な選択肢（キーワード）	コメント
		ます。**deployed**を指定した場合、オンボーディング時に選択したロケーションのIPアドレスのみが取得されます。

.txtファイルにオプションを、次の形式で指定します。

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

STEP 3 | IPアドレスを取得するには、次のコマンドを入力します:

- Prisma Access 2.1で導入された新しいAPIを使用するには、次のコマンドを入力します。

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

  2023 年 5 月現在、一部のPanorama管理デプロイメントでは https://api.prod6.datapath.prismaaccess.com/getPrismaAccessIP/v2 が使用されます (URL では prodではなく prod6 に注意してください)。

- レガシー API を使用するには、次のコマンドを入力します。このコマンドは、2022 年 5 月に廃止される予定のレガシー API エンドポイントを使用します。

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

ここで、*option.txt* は前の手順で作成した .txt ファイルであり、*Current-API-Key*はPrisma AccessAPI キーです。

たとえば、.txtファイル名が**option.txt**で、APIキーが**12345abcde**の場合、次のAPIコマンドを使ってすべてのロケーションのパブリックIPアドレスを取得します：

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

API コマンドは大量の情報を返すことができます。出力を読みやすくするために、Python がインストールされている場合は、CURLコマンドの最後に | python -m json.tool を追加できます。

API コマンドは次の形式でアドレスを返します。

```
{ "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"
```

ここで:

- **address_details** は、 各場所の住所の詳細を表示します。
  - **serviceType**はIPアドレスのタイプ（リモートネットワーク（**remote_network**）、Prisma Accessゲートウェイ（**gp_gateway**）、 Prisma Access ポータル (**gp_portal**)、クリーン パイプ (**clean_pipe**)、 またはリモート ブラウザー分離 (**rbi**)。
  - **addressType** は、 addrType キーワードで指定されたアドレスのタイプ (モバイル ユーザーの場所にIPアドレスを事前割り当てする場合は、**active** または **pre-allocated** の いずれか) を指定します。
  - **address** は、 許可リストに追加する必要があるIPアドレスを示します。

    APIが複数のIPアドレスを返す場合、 Prisma Accessアドレス フィールドにIPアドレスを要約します。
- アドレスには、 許可リストに追加する必要がある場所のすべてのIPアドレスが一覧表示されます。
- ゾーン は Prisma AccessIPアドレスに関連付けられた場所。
- **zone_subnet**は 、モバイル ユーザー ゲートウェイおよびポータルのサブネットです。Prisma Access は、モバイル ユーザーの場所にIPアドレスを事前割り当てする場合にもこのサブネットを提供します。

.txtファイル内のオプションに何か問題があった場合は、次のようなエラーが返されます:

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

STEP 4 | 取得したIPアドレスを使って、オンプレミスサーバーまたはSaaSアプリケーションポリシールールの許可リストを更新します。

モバイルユーザー向けのIP最適化：GlobalProtectとのデプロイメント

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	• Prisma Accessライセンス • Prisma Access バージョン 5.0 以降、

IPアドレス最適化は、デプロイメント環境におけるIPアドレスの全体的な数を削減するアーキテクチャ上の拡張機能のセットです。これにより、許可リスティング ワークフローが簡素化され

 ©2025 Palo Alto Networks, Inc.

ると同時に、耐障害性が向上し、Prisma Accessテナントの迅速なオンボーディングが可能になります。

- モバイルユーザー向けのよりシンプルなパブリック**IP**アドレス許可リスト**—GlobalProtect**デプロイメント Prisma Access —場所を追加したり、既存のPrisma Accessロケーションでスケーリングイベントが発生したりすると、新しいIPアドレスがモバイルユーザーセキュリティ処理ノード（MU-SPN）に割り当てられる場合があります。SaaSアプリケーションや企業ファイアウォールの妨害を避けるために、Prisma Accessが割り当てる新しいイグレスIPアドレスとゲートウェイIPアドレスを取得し、ネットワーク内の許可リストに追加することがベストプラクティスとされています。その結果、多数のIPアドレスを管理している状況が発生する可能性があります。IP最適化により、管理する必要のあるIPアドレスの数が減ります。
- **Prisma Access**テナントのオンボーディングの迅速化 — IP最適化がなければ、Prisma Accessとプライベート ネットワークにまたがる各デバイスに固有のプライベートIPアドレスを割り当てる必要があり、限られた企業内のルーティング可能なIPアドレス スペースから大規模なIPブロックを割り当てる必要があります。IP最適化では、Prisma Accessがデフォルトで共有アドレス空間からアドレスを割り当て、NATプライベート アプリケーショントラフィックを実施することができます。

*IP*最適化は、*Prisma AccessGlobalProtect*の新規デプロイメント環境のみを対象としています。既存の*GlobalProtect*デプロイメントは、既存のマルチテナント環境から作成した新しいテナントを含め、対象外です。さらに、オンプレミスのゲートウェイとポータルを使用していた *GlobalProtect*デプロイメントを*Prisma Access*に移行する場合、この機能を有効にする前に、すべてのユーザーが*GlobalProtect*アプリケーションのバージョン *6.1.4* 以降、*6.2.3* 以降、または *6.3.0* 以降を実行していることを確認してください。

*IP*最適化に関する次の追加要件をメモしておいてください。

- *IP*最適化には、モバイルユーザー最適化には*Prisma Access 5.0*以降、が必要で、*GlobalProtect*を初めてセットアップするときに有効にすることができます。
- *GlobalProtect*を初めてセットアップすると、*Prisma Access IP*最適化を有効にするかどうかを尋ねられます。
- *IP*最適化デプロイメントでは、パブリック (外部) アプリへのアクセスに *IPv6*はサポートされていません。プライベートアプリアクセスはサポートされています。新しい*Prisma Access*デプロイメント環境で*IPv6*を有効にするには、*Palo Alto Networks*のアカウントチームに連絡してください。弊社担当者がリクエストに対応するための*TAC*ケースを作成します。
- Prisma Access IPアドレスを取得するAPIは、*IP*最適化が有効になっていても、通常通り機能し続けます。

 ©2025 Palo Alto Networks, Inc.

Prisma AccessIPアドレスを取得するためのAPI例

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

インフラストラクチャIPアドレスを取得するAPIコマンドの.txtファイルにキーワードと引数を入力する場合は、次の例を使用します。コマンドの出力を変更するには、.txtファイル内のオプションを変更します。コマンド自体は変更しません。

これらのIPアドレスの取得	.txtファイルにこれらのパラメータを指定	コメント
モバイルユーザーのIPアドレス		
すべてのモバイルユーザーのIPアドレス	`{ "serviceType": "gp_gateway", "addrType": "all", "location": "all" }`	*addrTyp* が*all* の場合、 Prisma Accessは選択した場所のすべてのIPアドレスを取得します GlobalProtectモバイルユーザーの設定 (Panorama)。 すべてのロケーション とは、 Prisma Accessはオンボードされていない場所も含め、利用可能なすべての場所のIPアドレスを取得することを意味します。 Prisma Accessはオンボードされていない場所のIPアドレスを予約して、オンボードする前にこれらのIPアドレスを許可リストに追加できるようにします。

オンボードされたモバイルユーザーの場所のIPアドレス	`{ "serviceType": "gp_gateway", "addrType": "all", "location": "deployed" }`
	または
	`{ "serviceType": "gp_gateway", "addrTy`
		ロケーションタイプが*[デプロイ済み]* の場合、Prisma Accessはオンボードした場所のIPアドレスのみを取得します。
		これらのゲートウェイIPアドレスを取得するには、*addrType*として*all*または*active*を使用します。

©2025 Palo Alto Networks, Inc.

これらのIPアドレスの取得	.txtファイルにこれらのパラメータを指定	コメント
	`pe": "active", "location": "deployed" }`	
リモートネットワークのIPアドレス		
すべてのリモートネットワークのIPアドレスを取得します	`{ "serviceType": "remote_network", "addrType": "all", "location": "all" }`	このコマンドは、オンボーディングしたリモートネットワークのパブリックIPアドレスと出口IPアドレスを取得します。デプロイされたロケーション を使用しないでください。*addrType*に*active*を指定することは可能ですが、この場合*addrType*に*all*を指定したのと同じアドレスが取得されます。
Clean PipeのIPアドレス		
すべてのClean Pipe IPアドレスを取得します	`{ "serviceType": "clean_pipe", "addrType": "all", "location": "all" }`	このコマンドは、オンボーディングしたClean Pipeのパブリックアドレスと出口IPアドレスを取得します。デプロイされたロケーション を使用しないでください。*addrType*に*active*を指定することは可能ですが、この場合*addrType*に*all*を指定したのと同じアドレスが取得されます。
明示型プロキシIPアドレス		
デプロイされたロケーションのACS IPアドレスを取得する	`{ "serviceType": "swg_proxy", "location": "all", "addrType": "all" }`	このコマンドは、デプロイメントされた各明示的プロキシの場所、認証キャッシュサービス (ACS)、およびネットワーク ロード バランサ (明示的プロキシのデプロイメントにのみ関連) の出口IPアドレスを取得します。
リモートブラウザ分離IPアドレス		

©2025 Palo Alto Networks, Inc.

これらのIPアドレスの取得	.txtファイルにこれらのパラメータを指定	コメント
デプロイされたロケーションのリモート ブラウザ分離 (RBI)IPアドレスを取得します。	<pre>{ "serviceType": "rbi", "location": "all", "addrType": "all" }</pre>	このコマンドは、デプロイされた各RBIロケーション出口IPアドレスを取得します。これらのIPアドレスを許可リストに追加して、SaaS アプリケーションに接続できます。

©2025 Palo Alto Networks, Inc.

Prisma AccessIPアドレスが変更されたら通知を受け取る

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

サービス接続、リモートネットワーク接続、およびモバイルユーザーの、リモートネットワークおよびループバックIPアドレス変更に対する、パブリックIPアドレス変更の通知を受けるために、変更のアラートを受け取るURLを指定することができます。通知の送信には、HTTP POSTリクエストが使用されます。POSTリクエストには、次の通知データがJSONフォーマットで含まれています：

```
 {"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"}
```

通知を受け取ったら、2ステップの作業を行う必要があります。まず手動で、またはプログラムを使って、IP またはループバックアドレスを取得する必要があります。次に、ユーザーがサービスを利用できないような事態を回避するために、適切な許可リスト内のIPアドレスを更新する必要があります。

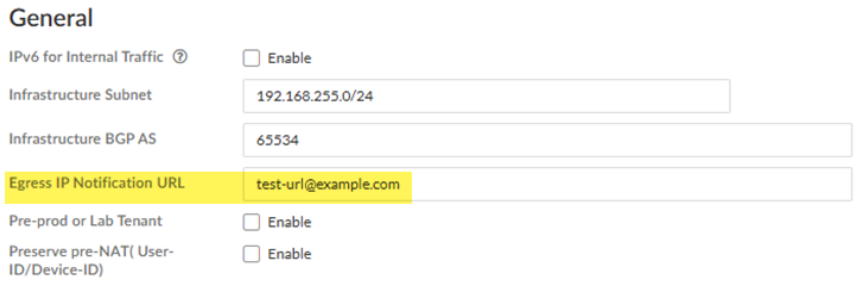
この通知は、*Prisma Access*によって新しい*IP*アドレスがアクティブになる数秒前に送信されます。新しい*IP*アドレスの取得とネットワーク内の許可リストへの追加の両方に、自動スクリプトを使用することをお勧めします。

IPアドレス通知URLを追加するには、次のタスクを完了します。

- Prisma Access (Managed by Strata Cloud Manager)デプロイメントの場合、 [ワークフロー] > **[Prisma Access** セットアップ] > **[Prisma Access]** > [インフラストラクチャ設定]に移動し、歯車をクリックして設定を編集し、IPアドレスの変更を通知できる **[Egress IP Notification URL**

©2025 Palo Alto Networks, Inc.

(出力IP通知URL)] を追加します。ここでは、Prisma Accessインフラストラクチャの IPアドレスの変更を通知することができます。



- Prisma Access (Managed by Panorama)デプロイメントの場合、**[Panorama]** > **[Cloud Services]** > **[Configuration (設定)]** > **[Service Setup (サービスセットアップ)]** に移動し、**IP**変更イベント通知**URL**を追加して、IPアドレスの変更を通知できるようにします。 ここでは、Prisma AccessインフラストラクチャのIPアドレスの変更を通知することができ、**OK**を押します。



変更通知をリッスンしているHTTPまたはHTTPS Webサービスに IPアドレスまたはFQDNを指定できます。 Prisma Accessでは、これらの通知は、パブリックIPアドレスを使用してインターネットから送信します。

通知URLを有効にするために変更をコミットする必要はありません。

©2025 Palo Alto Networks, Inc.

レガシースクリプトを使用してIPアドレスを取得する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

このセクションで説明するコマンドは、*Prisma Access 1.5* 以降の新しい*API*スクリプトに取って代わられているが、ループバックアドレスを取得する必要がある場合や、スクリプトやその他の自動化ツールで使用するデプロイメントでは、まだサポートされています。

Prisma Accessとともに使われる、古いAPIスクリプトで利用できるキーワードとパラメータ、およびデプロイメントタイプに応じて使用するAPIに関する情報と推奨事項を次の表に示します。

これらのレガシーコマンドはパブリック*IP*アドレスとイグレス*IP*アドレスも取得しますが、Palo Alto Networksでは、これらのコマンドを取得するには新しいAPIスクリプトを使用し、ループバックIPアドレスを取得するにはレガシーAPIのみを使用することを推奨しています。

- パブリック*IP*アドレスは、Prisma Accessがインターネットベースのソースに対して行われたリクエスト向けに使用する送信元IPアドレスです。Prisma Accessを、SaaSアプリケーションやパブリックにアクセス可能なパートナーアプリケーションなどの、インターネットリソースにアクセスさせるには、パブリックIPアドレスを許可リストに設定します。

  モバイルユーザー、リモートネットワーク、Clean Pipeデプロイはパブリックアドレスを使用します。
- 出口*IP*アドレスは、Prisma Accessがインターネットへの出口トラフィックに使用するIPアドレスで、Prisma Accessがインターネットリソースにアクセスできるように、それらのアドレスを許可リストにも追加する必要があります。

  さまざまな目的で使用されますが、Prisma Accessはユーザーが、Prisma Accessロケーションから目的の言語のWebページを受け取れるようにするために、出口IPアドレスを使用します。すべてのロケーションがパブリックIPアドレスを保有していますが、エグレスIPアドレスは持っていないロケーションも存在しています。次のロケーションは、エグレスIPアドレスを使用しません：

  - Prisma Accessリリース1.4より前に追加したロケーション。
  - バーレーン
  - ベルギー
  - France North（フランス北部）
  - France South（フランス南部）
  - 香港
  - アイルランド
  - 韓国
  - 台湾

©2025 Palo Alto Networks, Inc.

- 英国

モバイルユーザー、リモートネットワーク、Clean Pipeのデプロイはエグレスipアドレスを使用します。

モバイルユーザーデプロイ環境で使用されるコマンド	
コマンド名	コメント
get_egress_ip_all=yesコマンド `curl -H header-api-key:`*Current-API-Key*`"https://api.prod.datapath.prismaaccess.com/getAddrList/latest?get_egress_ip_all=yes`	Prisma Accessを、SaaSアプリケーションやパブリックにアクセス可能なパートナーアプリケーションなどの、インターネットリソースにアクセスさせるために許可リストに追加する、すべてのIPアドレスを取得します。このコマンドには、以下の制約があります。 • このコマンドは、大量のアドレスを取得する可能性があります（200件以上）。ご自分の企業が、大量な数のアドレスを許可リストに追加できない場合は、*gpcs_gp_gw*および*gpcs_gp_portal*キーワードを使って現在使用しているIPアドレスのみを取得できます。ただし、この場合ロケーションを追加するたびにコマンドを実行する必要があります。また、スケーリングイベントが発生した場合、新しいIPアドレスを許可リストに追加する必要があります。 • Prisma Accessは、これらのIPアドレスに対応しているロケーションを表示しません。そのため、このコマンドで返されたすべてのIPアドレスを許可リストに追加することをお勧めします。 • このコマンドで、ループバックアドレス取得されません。
gpcs_gp_gwおよび**gpcs_gp_portal**キーワード `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"`	デプロイ環境で許可リストに追加できるIPアドレス数が制限されている場合に、このコマンドを使用します。このコマンドで返されたすべてのIPアドレスを、ネットワークの許可リストに追加する必要があります。このコマンドでは、ループバックIPアドレスを取得することもできます。

©2025 Palo Alto Networks, Inc.

リモートネットワークデプロイ環境で使用されるコマンド	
コマンド名	コメント
gpcs_remote_networkキーワード `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"`	リモートネットワークデプロイメント環境で許可リストに追加する必要があるIPアドレスを検索する場合に、このコマンドを使用します。 このコマンドを使って、リモートネットワークデプロイ環境のエグレスIPアドレスを検索することもできます。エグレスIPアドレスは、状況によって異なる場合があります。

Clean Pipeデプロイメント環境で使用されるコマンド	
コマンド名	コメント
gpcs_clean_pipeキーワード `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"`	Clean Pipeデプロイ環境で許可リストに追加する必要があるIPアドレスを検索する場合に、このコマンドを使用します。

モバイルユーザーのIPアドレスを取得する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	☐ Prisma Accessのライセンス

このレガシースクリプトは、*Prisma Access 1.5*で新しい*API*スクリプトに差し替えられました。*Palo Alto Networks*では、ループバック アドレスを除くすべての *IP* アドレスを取得するために、 新しいスクリプト を使用することをお勧めします。

モバイルユーザーにSaaSまたはパブリックアプリケーションへのアクセスを許可するためにパブリックIPアドレスを許可リストに追加する場合は、 Prisma Accessはゲートウェイとポータルの IPアドレスごとに2つのIPアドレスが提供されるため、スケーリングやその他のイベント中に1つのIPアドレスを使用できます。IPアドレスセットをそれが使用される前に許可リストに設定し、スケーリングイベント中にSaaS/パブリックアプリケーションにアクセスできるようにして、モバイルユーザーに関する問題を防止することができます。

これらの新しいアドレスを取得するには、次の作業を実施します。

©2025 Palo Alto Networks, Inc.

STEP 1 | **Panorama > Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Service Setup**（サービス設定）を選択した後、**Generate API Key**（APIキーの生成）を選択して、API キーを入手します。

Prisma Accessの認証を受け、以下に記載しているcURLコマンドを使ってIPアドレスリストを取得するには、この鍵が必要になります。Panorama管理者またはSuperuserのみが、このAPI鍵を生成または利用できます。

STEP 2 | モバイルユーザーのパブリックIPアドレスを取得するには、次のいずれかのコマンドを入力します：

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

ここでの*Current-API-Key* はPrisma Access API キーです。

たとえば、API鍵が**12345abcde**の場合、次のAPIコマンドを使ってすべてのロケーションのパブリックIPアドレスを取得します：

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

Prisma Accessが1セットのパブリックIPアドレスを使用するたびに、別のIPアドレスが割り当てられます。Prisma Accessが追加されたパブリックIPアドレスセットを使用したと考えられる場合（たとえば、単一のロケーションに大量のモバイルユーザーがアクセスした）、このAPIコマンドを再度実行して、新しいパブリックIPアドレスセットを探すことができます。アップレード後は、すべてのIPアドレスが変更されずに残ります。

パブリック、ループバック、出口IPアドレスの取得

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

この古いスクリプトは*Prisma Access1.5*で新しいスクリプトに差し替えられました。*Palo Alto Networks*では、ループバック アドレスを除くすべての*IP*アドレスを取得するために、 新しいスクリプトを使用することをお勧めします。

パブリック、ループバック、出口IPアドレスを取得するには、次の作業を行ってください。

STEP 1 | API鍵を取得して、**IP Change Event Notification URL**（**IP**変更イベント通知**URL**）を追加します。ここから、Prisma Accessインフラ内のIPアドレスの変更通知を受け取ることができます。

詳細は Prisma AccessIPアドレスが変更されたら通知を受け取る を参照してください。

©2025 Palo Alto Networks, Inc.

STEP 2 | Prisma AccessのパブリックIPアドレス、ループバックIPアドレス、またはその両方を取得します。

API キーと API エンドポイント URL を手動で、または自動化スクリプトで使用します:

```
 header-api-key:現在の API キー "https://
api.prod.datapath.prismaaccess.com/getAddrList/latest?
fwType=$fwType&addrType=$addrType"
```

ここで、現在のAPIキーを自分のAPIキーに置き換え、次のキーワードと引数のいずれかまたは両方を使用する必要があります。

キーワード	の説明
fwType キーワード	
gpcs_gp_gw	取得 Prisma Access ゲートウェイIPアドレス（モバイルユーザーデプロイメント用）。gpcs_gp_portal
は	取得します Prisma Access ポータルIPアドレス（モバイルユーザーデプロイメント用）。gpcs_remote_network
は	取得します Prisma Access リモートネットワークIPアドレス（リモートネットワークデプロイメント用）
。**gpcs_clean_pipe**	は取得します Prisma Access クリーンパイプIPアドレス。addrType
キーワード	
パブリック**IP**	Prisma Access がインターネット ベースのソースへのリクエストに使用する送信元IPアドレスを取得します。 モバイルユーザーの場所については、 Prisma AccessIP アドレスを場所別にリストします。リモートネットワークの場合、 Prisma Accessはリモート ネットワーク名別に IP アドレスを一覧表示します。
egress_ip_list	IPアドレスを取得します Prisma Access インターネットへの追加の送信トラフィックのためにパブリック IP アドレスを使用します。 モバイルユーザーの場所については、 Prisma AccessはIP アドレスを場所別にリストしま

©2025 Palo Alto Networks, Inc.

キーワード	の説明
	す。リモートネットワークの場合、 Prisma Accessはリモート ネットワーク名別にIPアドレスを一覧表示します。
loopback_ip	内部ソース (RADIUSまたはActive Directoryサーバーなど) への要求に対してPrisma Accessによって使用される送信元IPアドレスを取得します。このアドレスはインフラストラクチャ サブネットから割り当てられます。

キーワードを指定しない場合は、 Prisma Accessはすべての IP アドレスを取得します。

たとえば、すべてのリモート ネットワークのパブリック IP アドレスのリストを手動で取得するには、次の Curl コマンドを試すことができます:

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

または、次の例のようにpythonスクリプトを使ってすべてのIPアドレスのリストを取得できます：

```
  #!/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
 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)
```

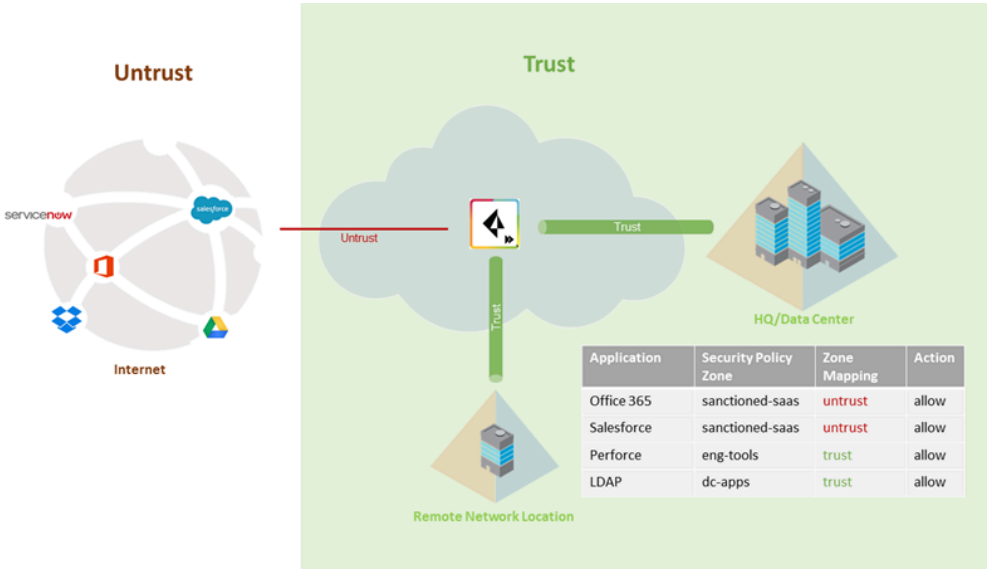
STEP 3 | 取得したIPアドレスを使って、オンプレミスサーバーまたはSaaSアプリケーションポリシールールの許可リストを更新します。

©2025 Palo Alto Networks, Inc.

Prisma Access ゾーン

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス

ファイアウォールで、ゾーンはインターフェイスと関連付けられます。しかし、Prisma Accessでは、ネットワークインフラは自動的にセットアップされます。つまり、インターフェイスを設定してそれを作成したゾーンと関連付ける手間が不要になります。ただし、一貫したセキュリティポリシー適用を可能にするためには、ゾーンマッピングを作成して、Prisma Accessにゾーンを内部の（信頼する）インターフェイスに関連付けるか、または外部（信頼しない）インターフェイスに関連付けるかを指示する必要があります。そうすることで、セキュリティポリシールールが正しく適用されます。デフォルトでは、Prisma Accessにプッシュされるゾーンはすべて信頼しない（Untrust）ものと設定されます。認可したSaaSアプリケーションも含めて、インターネット宛てのトラフィックに関連するゾーンは信頼しない（Untrust）設定にする必要があります。ただし、内部ネットワークまたはデータセンター内のアプリケーションへのアクセスを可能にするゾーンはすべて、信頼する（Trust）にマップする必要があります。下の例ですべての認可されたSaaSアプリケーション（この場合Office 365とSalesforce）は、sanctioned-saasゾーンにセグメント化されており、これらのアプリケーションの使用とポリシー適用が有効になっています。Prisma Accessによるsanctioned-saasゾーンと外部に直面しているインターフェイスの関連付けを有効にするには、このゾーンを信頼しない（Untrust）ものとしてマップする必要があります。eng-toolsおよびdc-appsゾーンは、企業オフィス内のアプリケーションへのアクセスを提供しているので、信頼するゾーンにする必要があります。



Prisma Accessは3 つのゾーン (信頼ゾーン、非信頼ゾーン、クライアントレス VPN) をサポートし、それらを自動的に設定することでポリシーの作成を簡素化します。

©2025 Palo Alto Networks, Inc.

ゾーン	詳説
Trust	企業ネットワーク内のすべての信頼済みおよびオンボー IPアドレス、サービス接続、またはモバイル ユーザーを含むゾーン。
Untrust	企業ネットワーク外のすべての信頼されていないIPアドレス、サービス接続、またはモバイル ユーザー。デフォルトでは、信頼されていないIPアドレスまたはモバイル ユーザーは、本質的に信頼されません。
クライアントレス VPN	HTML、HTML5、および JavaScript テクノロジを使用する一般的なエンタープライズ Web アプリケーションへの安全なリモートアクセスを提供します。ユーザーはGlobalProtectソフトウェアをインストールすることなく、SSL対応のWebブラウザから安全なアクセスを利用できます。これは、パートナーや契約業者をアプリケーションにアクセスできるようにしたり、個人デバイスなどの管理対象外のアセットを安全に利用できるようにしたりしなければならない状況に便利です。 クライアントレス *VPN* のゾーンはデフォルトでトラストゾーンにマッピングされます。この設定は変更できません。

inter-fw (インターFW)のゾーンを表示するPrisma Accessログは、Prisma Accessインフラストラクチャ内の通信に使用されるログです。

ゾーンを作成するときは、次の名前をゾーンに使用しないでください。これらは内部ゾーンに使用される名前です。

- 信頼できる
- 信頼できない
- inter-fw(インターFW)
- リモート ネットワークに使用する任意の名前（リモート ネットワーク名はStrata Logging Serviceログのソースゾーンとして使用）

*inter-fw*のゾーンを表示する*Prisma Access*ログは、*Prisma Access*インフラストラクチャ内の通信に使用されるログである。

©2025 Palo Alto Networks, Inc.

Prisma Access向けDNS

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス

Prisma Accessでは、組織内部のドメインと外部のドメインの両方のドメインを解決する、DNSサーバーを指定することができます。LDAPやDNSサーバーのような企業ネットワーク上のサービスへのアクセスを提供する場合、特に本社やデータセンターでこの種のリソースへのアクセスを提供するサービス接続を設定する場合は、このようにしてください。 Prisma Accessは、モバイルユーザーのGlobal Protectとリモート ネットワークのデプロイメントのためのDNS解決をサポートしています。内部ドメイン リスト内のドメインに対するDNSクエリは、Prisma Accessリモート ネットワーク ユーザーとモバイル ユーザーがリソースを 利用できるように、ローカルDNSサーバーに送信されます。

たとえば、会社のDNSサーバーを確実に利用するために、企業ドメインのDNSルックアップを利用したい場合は、企業ドメインと会社のDNSサーバーをここに指定します。エンドポイントが**DNS**プロキシ**IP**アドレスを使用するようにするには、**[Workflow (ワークフロー)]** > **[Prisma Access**セットアップ**]** > **[Prisma Access]** > **[Prisma Access DNS Proxy IP Address]**に示されているIPアドレス経由でDNSを解決するように設定する必要があります。

- Strata Cloud Manager
- Panorama

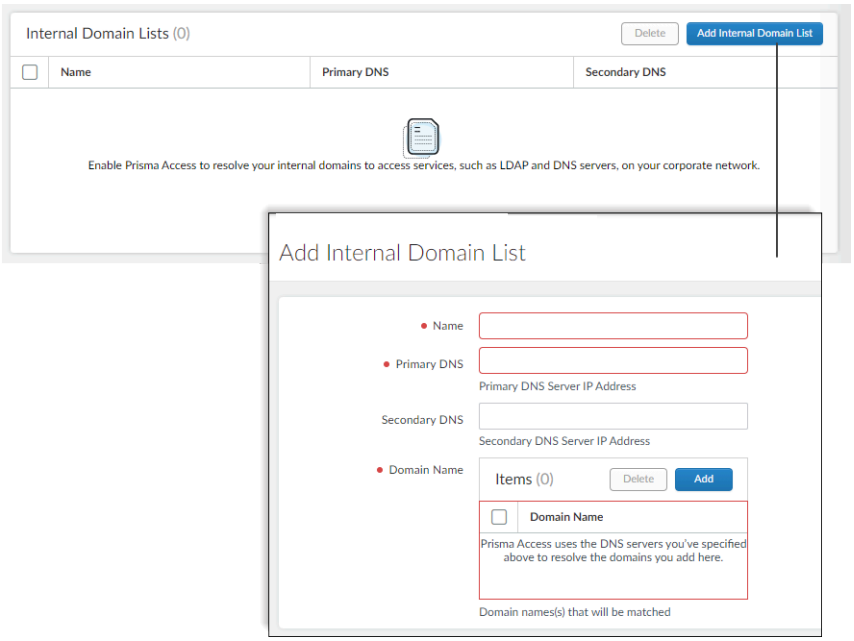
Prisma Access向けDNS （Strata Cloud Manager）

ここでは、内部ドメインを解決するためにPrisma Accessを設定する方法と、モバイル・ユーザーのデプロイメントやリモート ネットワーク サイトのためにDNS設定をカスタマイズする方法（内部ドメインとパブリック ドメインの両方を解決する）を紹介します。

©2025 Palo Alto Networks, Inc.

これにより、すべてのトラフィックに適用される内部ドメイン リストがセットアップされます。

1. **[Workflows (ワークフロー)] > [Prisma Accessセットアップ] > Prisma Access**および**[Add Internal DNS Servers (内部DNSサーバーの追加)]**を追加します。



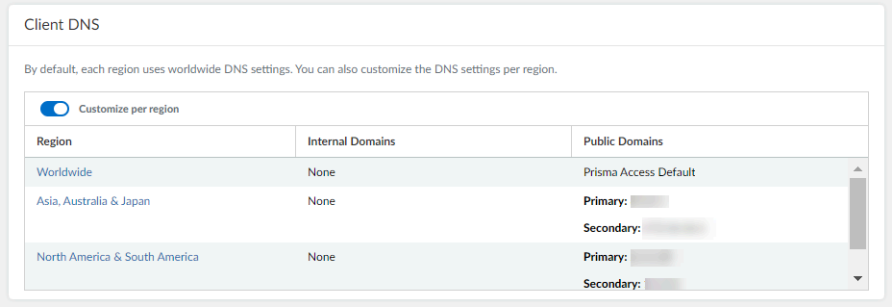
2. Prisma Accessが内部ドメイン名を解決するために使用するプライマリDNSサーバーとセカンダリDNSサーバーを入力します。
3. 解決のためにこれらのDNSサーバーに送信する内部ドメイン名を追加します。

   ドメインリスト内のドメインの先頭にワイルドカード（*）を使用できます（例：*.acme.localまたは*.acme.com）。

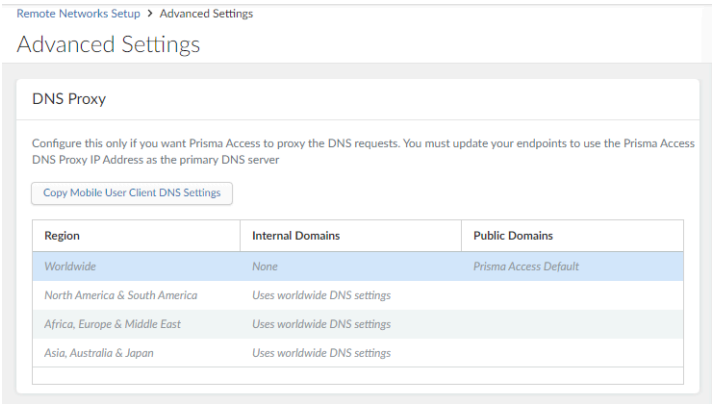
©2025 Palo Alto Networks, Inc.

特定のモバイル ユーザーのデプロイメントまたはリモート ネットワーク サイトにのみ適用される内部ドメイン リストを追加します。

1. DNSセキュリティの設定:
   - モバイルユーザー- **[Workflows (ワークフロー)]** > **[Prisma Accessセットアップ]** > **[GlobalProtect]** > **[Infrastructure Settings (インフラストラクチャ設定)]** へと進み、**[クライアントDNS]**を見つけます。



   - **[リモートネットワーク]**- **[Workflows (ワークフロー)]** > **[Prisma Accessセットアップ]** > **[Remote Networks (リモート ネットワーク)]** > **[Advanced Settings (詳細設定)]**へ移動して、**[DNS Proxy]**を見つけます。



2. Worldwide (全世界領域) のデフォルト（Prisma AccessのデフォルトDNSサーバー）を使用するか、地域に応じて設定をカスタマイズする。どちらの場合も、地域を選択して、その地域の DNS設定を調整およびカスタマイズします。
3. 内部ドメインの解決にこれらの**DNS**設定を使用するオプションをチェックし、任意でパブリックドメインの解決にも内部**DNS**サーバーを使用します。このオプションを選択しないと、Prisma Accessはクラウドのデフォルト DNSサーバーを使用してパブリック ドメインの要求を解決します。
4. モバイル ユーザーIPアドレス プール内のすべてのアドレスからDNSサーバーへのトラフィックを許可します。

   Prisma AccessのDNSプロキシは、指定したDNSサーバーに要求を送信します。DNS要求の送信元アドレスは、リージョンに割り当てたIPプールの最初のIPアドレスです。DNS要求がサーバーに確実に到達できるようにするには、モバイル ユーザーIPアドレス プール内のすべてのアドレスからDNSサーバーへのトラフィックを許可する必要があります。

©2025 Palo Alto Networks, Inc.

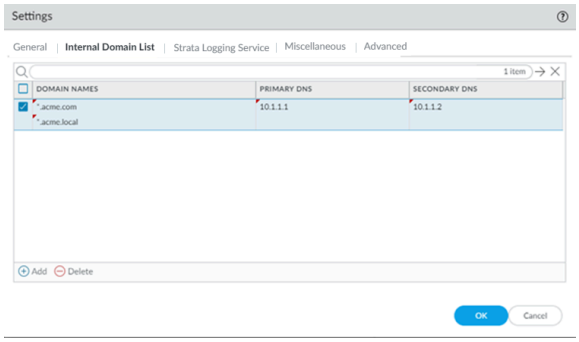
Prisma Access向けDNS （Panorama）

内部ドメインを解決するためにPrisma Accessをセットアップします。

これにより、すべてのトラフィックに適用される内部ドメイン リストがセットアップされます。

1. **Panorama** > **Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Service Setup**（サービスのセットアップ）の順に選択し、歯車型アイコンをクリックして設定を編集します。
2. **Internal Domain List**（内部ドメインリスト）タブを選択します。
3. Prisma Accessが内部ドメイン名を解決するために使用するドメイン名、プライマリDNS、およびセカンダリDNSサーバを追加します。

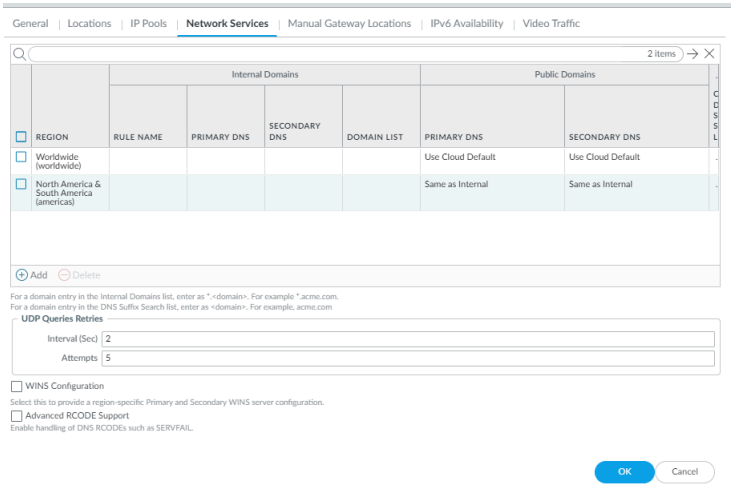
   ドメインリスト内のドメインの先頭にワイルドカード（*）を使用できます（例：*.acme.localまたは*.acme.com）。



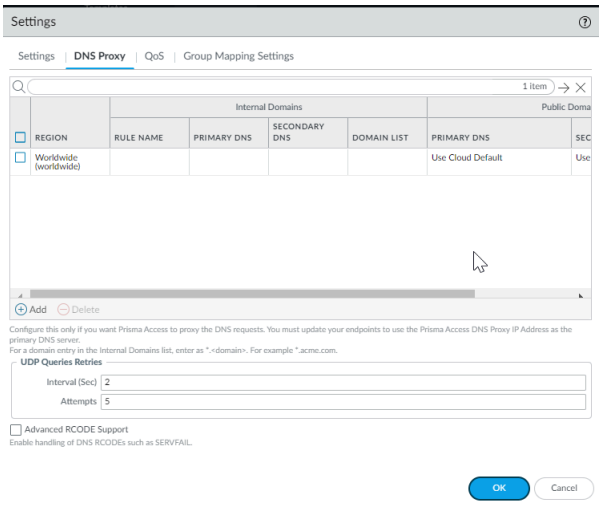
©2025 Palo Alto Networks, Inc.

特定のモバイル ユーザーのデプロイメントまたはリモート ネットワーク サイトにのみ適用される内部ドメイン リストを追加します。

1. DNSセキュリティの設定:
   - モバイルユーザー – **[Panorama]** > **[Cloud Services (クラウドサービス)]** > **[Configuration (設定)]** > **[モバイルユーザー - GlobalProtect]**に移動し、外部ゲートウェイを選択し、**[ネットワークサービス]** をクリックします。



   - リモートネットワーク – **Panorama** > **[Cloud Services (クラウドサービス)]** > **[Configuration (設定)]** > **[リモートネットワーク]** > **[設定]** > **[DNSプロキシ]**に移動します。



2. Worldwide (全世界領域) のデフォルト（Prisma AccessのデフォルトDNSサーバー）を使用するか、地域に応じて設定をカスタマイズする。どちらの場合も、地域を選択して、その地域の DNS設定を調整およびカスタマイズします。
3. 内部ドメイン のDNS 設定を構成するルールを1つ以上追加します。
   - ルールの一意のルール名を入力します。

©2025 Palo Alto Networks, Inc.

- 内部DNSサーバーに、指定したドメインのみを解決させる場合は、Domain List（ドメインリスト）に解決するドメインを入力します。ドメインの前にアスタリスクを指定します (例:*.acme.com)。最大 1,024 のドメインエントリを指定できます。

  Prisma Accessには、クラウドのデフォルトサーバーを使用して*.amazonaws.com ドメインを解決するルールが事前定義されています。内部 DNS サーバーに、より限定的な*.amazonaws.com ドメイン (*.s3.amazonaws.com など) を解決させたい場合は、ドメインリストに URL を入力します。Prisma Accessはリスト内のドメイン名を長いものから短いものの順に評価し、次に上からブームの順に評価します。

- 内部ドメインにアクセスできるカスタムDNSサーバーがある場合は、プライマリDNSサーバーとセカンダリDNSサーバーのIPアドレスを指定するか、[Use Cloud Default (クラウドデフォルトを使用)]を選択してデフォルトのPrisma AccessDNSサーバーを使用します。

4. パブリックドメイン のDNS 設定を指定します。

   - **Use Cloud Default (**クラウドのデフォルトを使用**)** – デフォルトのPrisma Access DNSサーバーを使用します。
   - **Same as Internal Domains (**内部ドメインと同じ**)**-内部ドメインの解決に使用するのと同じサーバーを使用する。このオプション#onを選択すると、パブリックドメインの解決に使用されるDNSサーバーは、[内部ドメイン]セクションの最初のルールに設定されたサーバーと同じになります。
   - **Custom DNS server (**カスタム**DNS**サーバー**)**- パブリック (外部) ドメインにアクセスできるDNSサーバーがある場合は、そのフィールドにプライマリDNSサーバー アドレスを入力します。

5. (任意) DNSサフィックスを追加して、解決できない非修飾ホスト名が入力されたときにクライアントがローカルで使用する必要があるサフィックスを指定できます (例:acme.local)。Prisma Access管理者ガイド (Panorama Managed) では、ドメインサフィックス (たとえば acme.com) の前にワイルドカード (*) 文字を入力しないでください。複数のサフィックスを追加できます。
6. モバイル ユーザーIPアドレス プール内のすべてのアドレスからDNSサーバーへのトラフィックを許可します。

   Prisma AccessのDNSプロキシは、指定したDNSサーバーに要求を送信します。DNS要求の送信元アドレスは、リージョンに割り当てたIPプールの最初のIPアドレスです。DNS要求がサーバーに確実に到達できるようにするには、モバイル ユーザーIPアドレス プール内のすべてのアドレスからDNSサーバーへのトラフィックを許可する必要があります。

©2025 Palo Alto Networks, Inc.

Prisma Accessの高可用性 (HA)

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

Panoramaアプライアンスを高可用性（HA）構成でデプロイすると、システム/ネットワーク障害時の冗長性を提供しており、Prisma Accessへの継続的な接続性を確保できます。HA構成で、片方のPanoramaアプライアンスがアクティブプライマリに、もう一方がパッシブセカンダリになります。フェイルオーバー発生時には、セカンダリピアがアクティブになり、お客様のPrisma Access管理の役割を引き継ぎます。

HAセットアップを簡素化するには、Prisma Access およびStrata Logging Service認証コードとコンポーネントを購入し、クラウド サービス プラグインをインストールするプライマリ Panorama アプライアンスのシリアルナンバーを認証コードに関連付けた後、Panorama Managed Prisma Accessをアクティベートしてインストールする前に、Panorama アプライアンスを HA に設定します。この手順を使って、すでにプラグインがインストールされている、既存のPanoramaアプライアンスを設定することもできます。

新しいPanoramaアプライアンスのペアを用意して始める場合でも、すでにスタンドアロンのPanoramaアプライアンスをセットアップしており、ライセンス設定とインストール作業を完了している場合でも、HAを有効にする前に前提条件を忘れずに確認してください。

- カスタマーサポートポータル（CSP）で、PanoramaアプライアンスHAピアを、同じ顧客アカウントを使って登録する必要があります。
- Panoramaアプライアンスのピアは、同じフォームファクタ（同じモデルのハードウェアアプライアンス、または同一の仮想アプライアンス）および同じバージョンのOSを持ち、同じセットのライセンスを保持している必要があります。Prisma AccessとStrata Logging Serviceにはプレミアムサポートライセンスが必要です。
- プライマリPanoramaアプライアンスのシリアルナンバーは、Prisma AccessおよびStrata Logging Service認証コードと関連付け られています。スタンドアロンのPanoramaアプライアンスにプラグインをインストール、セットアップした場合、そのPanoramaアプライアンスをプライマリピアとして使用してください。そのスタンドアロンピアをセカンダリPanoramaアプライアンスとして割り当てる必要がある場合、作業を続行する前に、プライマリPanoramaアプライアンスピアにライセンスを移転するためのアシスタンスとサポートを、Palo Alto Networksに依頼してください。

*Panorama*ペアの*HA*を無効にし、単一の*Panorama*が*Prisma Access*を管理する構成に戻した場合、*Prisma Access*コンポーネント のステータスを取得する際にエラーが発生しないように、アカウントを再確認する必要があります。

PanoramaアプライアンスをHA構成でセットアップするには、次の手順を実行します。

STEP 1 | Panorama での HA のセットアップを行います。

プライマリPanoramaアプライアンスを**Primary**（プライマリ）に、セカンダリPanoramaアプライアンスを**Secondary**（セカンダリ）に設定し、プライマリPanoramaアプライアンスのシ

©2025 Palo Alto Networks, Inc.

リアルナンバーが、Prisma AccessおよびStrata Logging Service認証コードと結びつけられていることを確認してください。

STEP 2 | プライマリ（アクティブ）およびセカンダリ（パッシブ）Panoramaアプライアンスが同期されており、それらの間のHAリンク状態がアップになっていることを確認します。

1. プライマリPanoramaアプライアンスで、**Dashboard**（ダッシュボード）にアクセスし、**Widgets**（ウィジット） > **System**（システム） > **High Availability**（高可用性）の順に選択して、HAウィジットを表示します。
2. **Sync to peer**（ピアと同期）を行い、**Yes**（はい）をクリックして、**Running Config**（実行中の設定）で **Synchronized**（同期済み）が表示されるまで待ちます。
3. **Local**（ローカル）ピアが**active**（アクティブ）であることを確認します。
4. パッシブPanoramaアプライアンスで、**Dashboard**（ダッシュボード）にアクセスし、**Widgets**（ウィジット） > **System**（システム） > **High Availability**（高可用性）の順に選択して、HAウィジットを表示します。
5. **Running Config**（実行中の設定）で **Synchronized**（同期済み）が表示されることを確認します。
6. **Local**（ローカル）ピアが**passive**（パッシブ）であることを確認します。

STEP 3 | プライマリPanoramaアプライアンスに、Prisma Accessコンポーネントをインストールします。

1. プライマリPanorama アプライアンスにログインし、**Panorama** > **Licenses**（ライセンス）の順に選択します。
2. **Retrieve license keys from license server**（ライセンスサーバーからライセンスキーを取得）をクリックします。
3. Panorama Managed Prisma Access をアクティブ化してインストールし、ワンタイム パスワード (OTP) を生成してアカウントを確認します。

STEP 4 | HAが有効になっていることを確認します。

1. プライマリPanoramaアプライアンスで、CLIにアクセスして、次の運用コマンドを入力します。

   ```
   tail follow yes mp-log plugin_cloud_services.log
   ```

2. ログ出力内で次のテキストを探します。ここでXは、プライマリPanoramaアプライアンスのシリアル番号、Yはセカンダリ Panoramaアプライアンスのシリアル番号を表しています。

   ```
   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
   ```


©2025 Palo Alto Networks, Inc.

```
 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. Customer Support Portal（CSP）（カスタマーサポートポータル）にログインして、**Assets**（アセット） > **Cloud Services**（クラウドサービス）の順に選択して、両方のPanoramaピアがPrisma AccessおよびStrata Logging Serviceライセンスに結びつけられていることを確認します。
4. プライマリおよびセカンダリPanoramaアプライアンスの、フィールドを確認します。

   Palo Alto NetworksがPrisma Accessライセンスを自動的にセカンダリPanoramaアプライアンスに関連付けるため、Auth Code（認証コード）、Model Name（モデル名）、License Description（ライセンスの説明）、およびExpiration Date（有効期限）フィールドが、プライマリPanoramaアプライアンスとセカンダリPanoramaアプライアンスの両方で同じになっていなければなりません。

STEP 5 | セカンダリ Panorama アプライアンスにログインし、Panorama Managed Prisma Access をアクティブ化してインストールします。

Customer Support Portal（CSP）（カスタマーサポートポータル）にログインしてOTPを生成する場合、セカンダリPanoramaアプライアンスのシリアル番号を指定していることを確認してください。

STEP 6 | プライマリおよびセカンダリPanoramaアプライアンスの変更内容をコミットします。

1. 変更内容を、**Commit**（コミット） > **Commit and Push**（コミットしてプッシュ）します。
2. **OK**、**Push**（プッシュ）の順にクリックします。

STEP 7 | プライマリPanoramaアプライアンスとセカンダリPanoramaアプライアンスが、引き続き同期状態になっていることを確認します。

©2025 Palo Alto Networks, Inc.

事前定義済みテンプレート:サービス接続またはリモートネットワークのオンボード

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

Prisma Accessには、一般的なIPSecおよびSD-WANデバイスに対する事前定義されたIPSecテンプレートが用意されています。これらのプロファイルを利用すれば、当該デバイスを使って接続を終端しているサービス接続やリモートネットワーク接続のオンボーディングを素早く簡単に行えます。

共通テンプレートを共有すると、共通に共有される暗号、事前共有鍵、ピア識別子を使用して、同じタイプの複数のリモート接続をオンボードすることもできます。

- 事前定義済みテンプレート:サービス接続またはリモートネットワークのオンボード
- 共通のSD-WANデバイスに対してサポートされているIKEおよびIPSec暗号プロファイル

Prisma Accessには、オンプレミスデバイスとPrisma Access間のIPSecトンネルのセットアトップに使用できる、次の事前定義テンプレートが用意されています。

- IPSec Tunnels（**Network** > **IPSec Tunnels**）（Remote_Network_TemplateおよびService_Conn_Template下）。
- IKE Gateways（**Network** > **Network Profiles** > **IKE Gateways**）（Remote_Network_TemplateおよびService_Conn_Template下）。
- IPSec Crypto Profiles（**Network** > **Network Profiles** > **IPSec Crypto**）（Remote_Network_TemplateおよびService_Conn_Template下）。
- IKE Crypto Profiles（**Network** > **Network Profiles** > **IKE Crypto**）（Remote_Network_TemplateおよびService_Conn_Template下）。

現在のところ、次のベンダー用のテンプレートが用意されています。

次のテンプレートの他に、ここに記載されていない任意のオンプレミスデバイスに使用できる*Generic*（汎用）テンプレートも用意されています。

- Ciscoアプライアンス：
  - Cisco統合サービス ルータ (ISR)
  - Cisco適応型セキュリティ アプライアンス (ASA)
- Citrix
- Prisma SD-WAN(旧 CloudGenix)
- Riverbed
- Silver Peak

©2025 Palo Alto Networks, Inc.

Prisma Accessが提供するテンプレートを使って、サービス接続またはリモートネットワーク接続をオンボーディングするには、次の作業を行います。

STEP 1 | Panoramaにテンプレートが表示されるように、Panoramaで設定作業を行います。

Cloud Servicesプラグインのアップグレード時に、新しいテンプレートが自動表示されることはありません。テンプレートを表示するには、アップグレードした後にこのステップを実行してください。新規インストールの場合、初回のセットアップの一環としてこの初期設定が行われるため、このステップを実施する必要はありません。

これらのテンプレートを削除した後、もう一度使用する必要がある場合も、このステップを実行してください。

- サービス接続の場合、**Panorama** > **Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Service Setup**（サービスのセットアップ）の順に選択して、**Settings**（設定）エリアの歯車型アイコンをクリックして**Settings**を開き、**OK**をクリックします。
- リモートネットワーク接続の場合、**Panorama** > **Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Remote Networks**（リモートネットワーク）の順に選択して、**Settings**（設定）エリアの歯車型アイコンをクリックして**Settings**を開き、**OK**をクリックします。

STEP 2 | **Network**（ネットワーク）を選択し、次に適切な**Template**（テンプレート）を選択します（リモートネットワーク接続を作成する場合は**Remote_Network_Template**、サービス接続を作成する場合は**Service_Conn_Template**）。

STEP 3 | サービス接続またはネットワーク接続の終端となるデバイスのタイプを判断し、そのデバイスで使用するテンプレートを探します。

ご利用の*SD-WAN*または*IPSec*デバイスがリストに記載されていない場合は、汎用プロファイルをご利用ください。

STEP 4 | **Network**（ネットワーク） > **Network Profiles**（ネットワークプロファイル） > **IKE Gateways**（**IKE**ゲートウェイ）を選択し、ご利用のデバイスのIKEゲートウェイプロファイルに次の変更を行います：

IPSec暗号およびIKE暗号プロファイルは変更せずに利用できますが、IKEゲートウェイプロファイルはネットワーク設定と合致するように変更を加える必要があります。

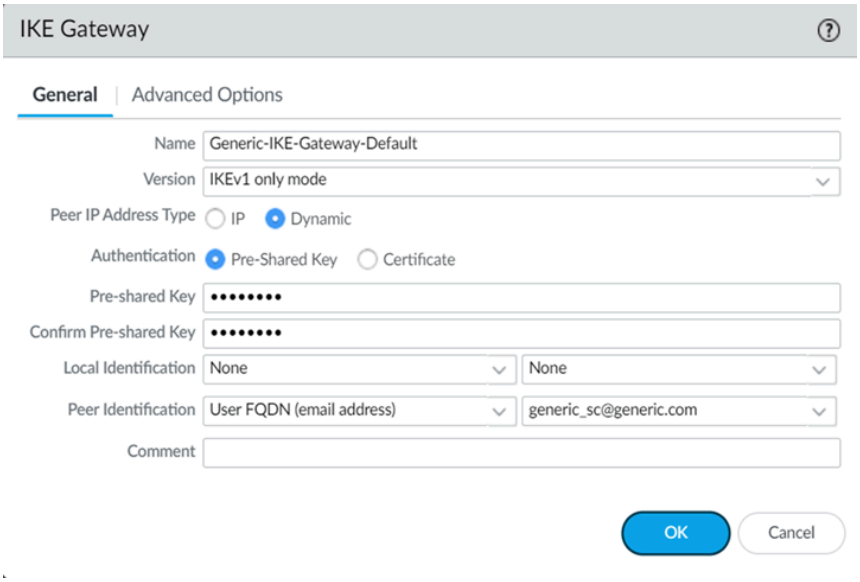
- （任意）Prisma AccessとのIPSecトンネルのセットアップに使用するオンプレミスデバイスのパブリックIPアドレスが分かっている場合、**Peer IP Address Type**（ピア**IP**アドレス

 ©2025 Palo Alto Networks, Inc.

タイプ）で**IP**を指定し、IPSecトンネルの**Peer Address**（ピアアドレス）を入力して、スタティックIPアドレスを設定します。

- IPSecトンネルに事前共有鍵を使用する場合、**Pre-shared Key**（事前共有鍵）を指定します。
- **IP Address**（**IP**アドレス）または**User FQDN**（ユーザー**FQDN**）の**Peer Identification**（ピア**ID**）を指定します。

  IPSecトンネルのもう一方の側の終端に使用するデバイスの設定は、ここで指定した設定と同じにする必要があります。



STEP 5 | サービス接続またはリモートネットワーク接続のオンボーディングを行い、IPSecトンネルのもう一方の側にあるデバイスと一致する**IPSec tunnel**設定を指定します。

©2025 Palo Alto Networks, Inc.

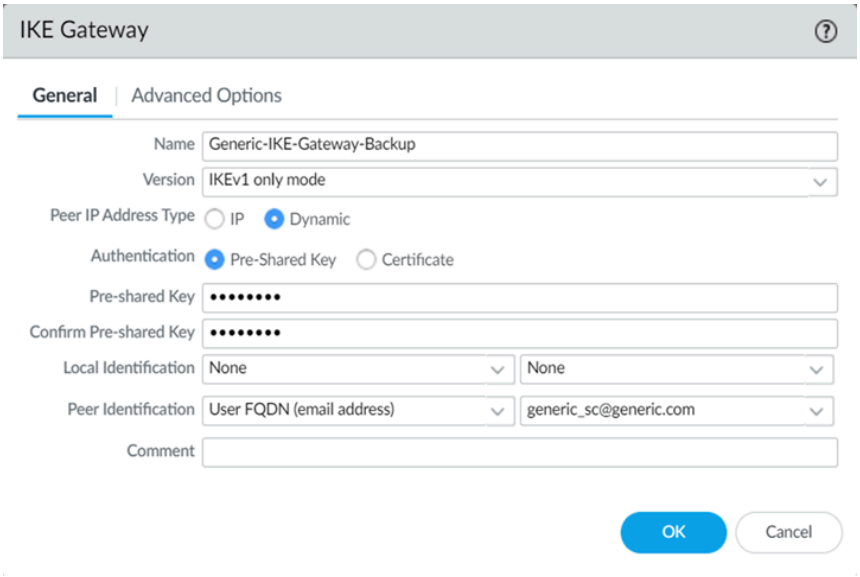
STEP 6 | （オプション）サービス接続またはリモートネットワーク接続のバックアップトンネル（セカンダリWAN）を追加する必要がある場合、次の設定作業を行います。

セカンダリ WAN の設定は、次の展開ではサポートされていません。

- セカンダリ WAN がプライマリ IPsec トンネルを使用してアクティブ/アクティブモードに設定されている場合。
- 顧客宅内機器 (CPE) が、プライマリおよびセカンダリIPsecトンネルを使用する等コストマルチパス (ECMP) 構成で設定されている場合。

1. バックアップトンネル用の新しいIKEゲートウェイを作成し、複製する事前定義テンプレートから設定をコピーします。

   汎用ネットワークデバイスのバックアップトンネル設定を作成する例を次に示します。

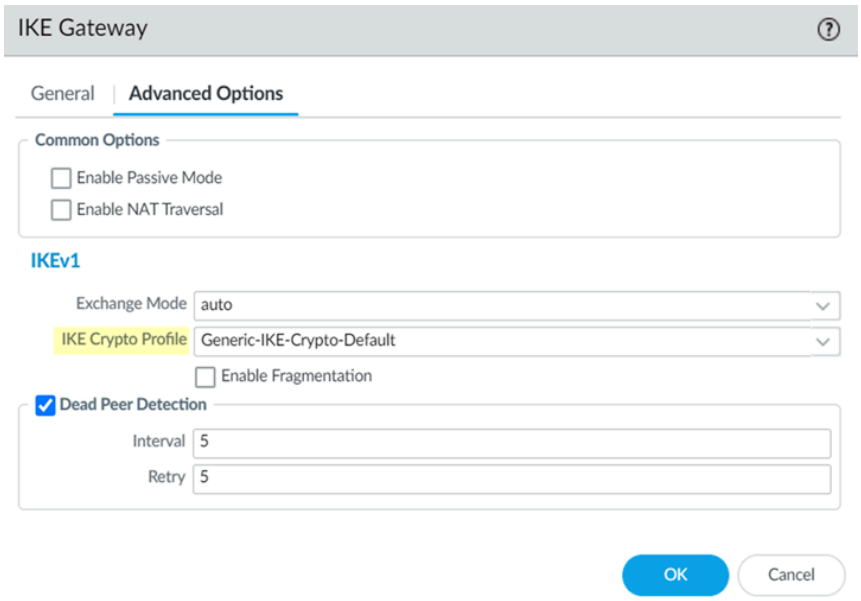


2. **Advanced Options**（詳細オプション）で、使用する事前定義テンプレートの**IKE Crypto Profile**（**IKE**暗号プロファイル）を指定します。

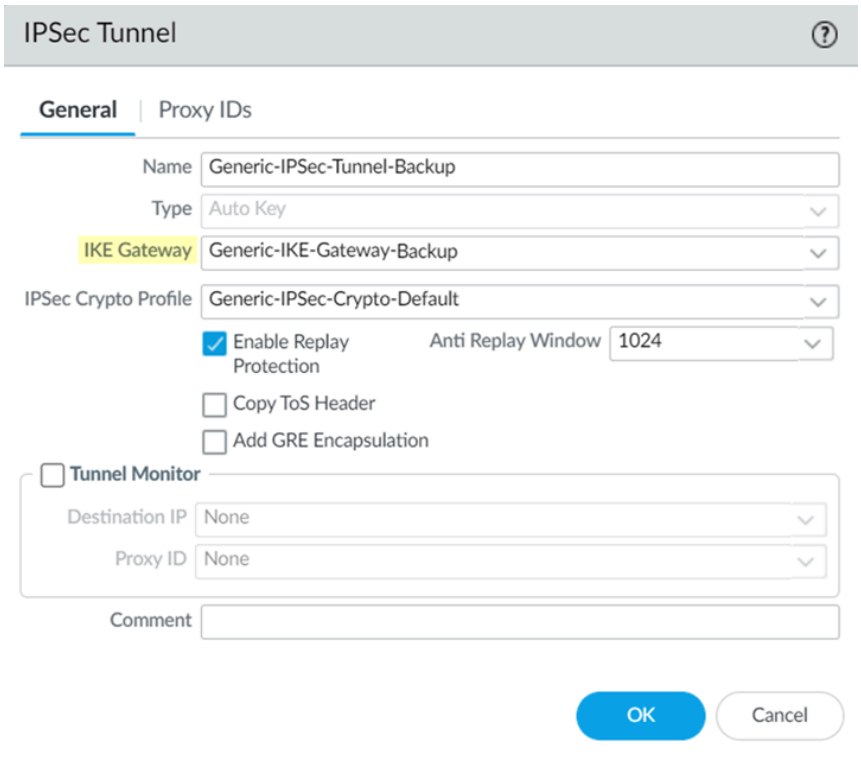
   IPSecトンネルには、CBC暗号の代わりにGCM暗号を使用することをお勧めします。

   Prisma SD-WANをオンボードする場合は、**[Enable Passive Mode (**パッシブ モードを有効にする**)]**を選択します。

©2025 Palo Alto Networks, Inc.

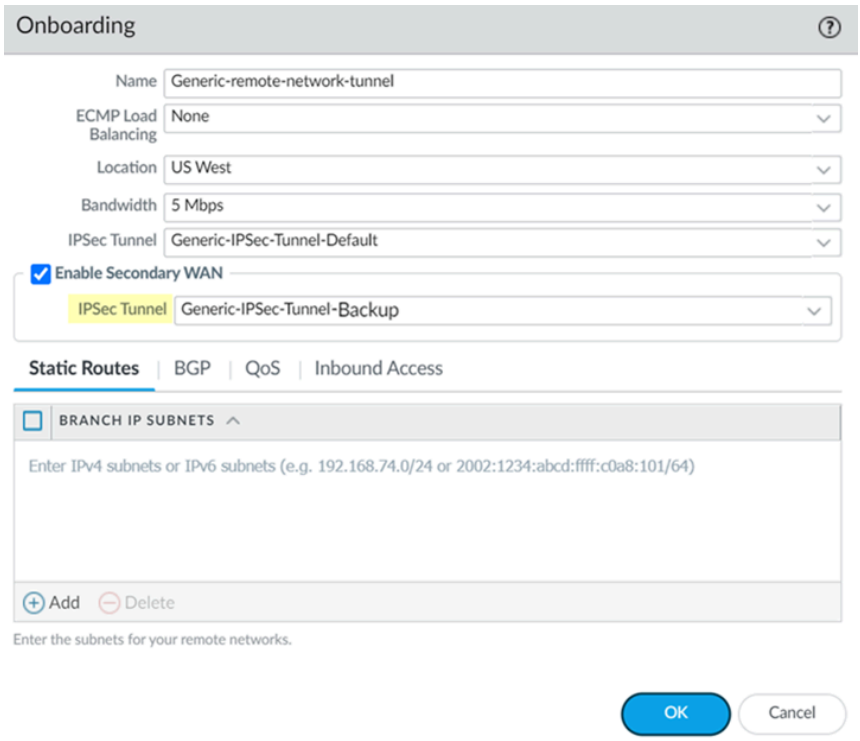


3. 新しいIPSecトンネルを作成し、作成した新しいIKEゲートウェイを指定して、それ以外の設定はすべてデフォルトテンプレートからコピーします。



4. サービス接続またはリモートネットワーク接続のオンボーディングを行う場合、**Enable Secondary WAN**（セカンダリ**WAN**を有効にする）を選択して、バックアップWAN用に作成したトンネルを指定します。

 ©2025 Palo Alto Networks, Inc.



STEP 7 | IPSecトンネルのもう一方の側を終端するために使用するデバイスの、暗号、事前共有鍵、およびピアIDを一致させて、サービス接続またはリモートネットワーク接続の設定を完了します。

STEP 8 | （任意）同じタイプのネットワークデバイスを使用する複数のリモートネットワーク接続をオンボーディングする必要がある場合は、リモートネットワークの設定を**Export**（エクスポート）して、設定を編集してから、その設定を**Import**（インポート）します。

共通のSD-WANデバイスに対してサポートされているIKEおよびIPSec暗号プロファイル

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

このセクションは、さまざまな共通するSD-WANデバイスに対して、サポートされている暗号プロファイルを説明しています。SD-WANデバイスの設定を行う場合、これらのプロファイルをガイドラインとして、Prisma Accessでリモートネットワークの設定をどのように行えるのかを理解してください。

- Aruba SD-WAN対応IKEおよびIPSec暗号プロファイル
- Aryaka SD-WAN対応IKEおよびIPSec暗号プロファイル

©2025 Palo Alto Networks, Inc.

- Citrix SD-WAN対応IKEおよびIPSec暗号プロファイル
- Prisma SD-WAN デバイスは IKE および IPSec 暗号化プロファイルをサポートしています
- Nuage Networks SD-WAN対応IKEおよびIPSec暗号プロファイル
- Riverbed SteelConnect SD-WAN対応IKEおよびIPSec暗号プロファイル
- Silver Peak SD-WAN対応IKEおよびIPSec暗号プロファイル
- Viptela SD-WAN対応IKEおよびIPSec暗号プロファイル

©2025 Palo Alto Networks, Inc.

Prisma Accessサービス接続

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

サービス接続 (企業アクセス ノード (CAN) とも呼ばれる) を使用すると、モバイル ユーザーとリモート ネットワークのユーザーはプライベート アプリやリソースにアクセスでき、モバイル ユーザーとリモート ネットワークは相互に通信できるようになります。

サービス接続に加えて、Palo Alto Networksはプライベート アプリにアクセスするために使用できるその他のサービスも提供しています。

- ZTNA コネクター Zero Trust Network Access (ZTNA) コネクタを使用すると、Prisma Accessを組織のプライベート アプリに簡単かつ安全に接続できます。ZTNA コネクタは、自動化されたセキュア トンネルを使用して、モバイル ユーザーとブランチ ロケーションのユーザーにプライベート アプリへのアクセスを提供します。また、Cloud Identity Engineを使用して、ZTNAが保護する プライベート アプリを自動的に検出する こともできます。
- Prisma Access Colo-Connect—Colo-Connectを使用すると、広帯域幅のサービス接続を提供できるクラウドインターコネクトを使用して、Prisma Accessを使用してプライベートアプリケーションを保護することができます。

Palo Alto Networksでは、Prisma Accessデプロイメント時に必ずサービス接続を作成することを推奨しています。すべてのサービス接続には次の特性があります。

- サービス接続は、本社またはデータセンターのリソースへのアクセスを可能にします。

  たとえば、セキュリティ ポリシーが、Active Directoryのようなオンプレミス認証サービスを使ったユーザー認証を要求している場合、サービスが存在している企業ロケーションにアクセスするためにPrisma Accessを有効にする（また、サービスがアクセスに使用できるサービスアカウントを設定する）必要があります。同様に、リモートネットワークおよびモバイルユーザーがアクセスする必要がある企業リソースがある場合、対応する企業ネットワークにアクセスするためにPrisma Accessを有効にする必要があります。

  このような理由でサービス接続を作成する場合、それを実装する前にサービス接続の計画を策定する必要があります。
- サービス接続により、リモートネットワークとモバイルユーザーは相互に通信できます。

  本社またはデータセンターにアクセスする必要がない場合でも、リモートネットワークロケーションへのアクセスをモバイルユーザーに許可しなければならない場合もあります。このような場合、プレースホルダ値を使ってサービス接続を作成することができます。リモートネットワーク接続はすべてメッシュ化されていますが、モバイルユーザーはハブアンドスポークネットワーク内のサービス接続を使って、リモートネットワークに接続するため、これが必要になります。そのような理由で、既存のサービス接続が理想的な地理的ロケーションにない場合、プレースホルダー値でサービス接続を作成することもあります。

- サービス接続では、インターネットへの出力がサポートされていないため、言語のローカリゼーションはサポートされません。 Prisma Accessによって、サービス接続ごとに1つのサービスIPアドレス のみが割り当てられ、そのIPアドレスは、オンボーディング時に指定した場所に対応するコンピューティング場所に地理的に登録されます。

サービス接続の数は、お持ちのPrisma Accessライセンスによって異なります。

- ZTNAまたはEnterpriseライセンスをお持ちの場合、サービス接続の数はライセンス エディションによって異なります。ローカル エディションをお持ちの場合は、最大2つのサービス接続を構成できます。ワールドワイド エディションをお持ちの場合は、最大5つのサービス接続を構成できます。
  - ZTNA Connectorを使用すると、Prisma Accessを組織のプライベートアプリに接続できます。ZTNA コネクタは、自動化されたセキュア トンネルを使用して、モバイル ユーザーとブランチ ロケーションのユーザーにプライベート アプリへのアクセスを提供します。詳細については、Prisma Access ZTNAコネクタを参照してください。
- 複数のテナントを管理し 、ZTNAまたはEnterpriseライセンスを所有している場合、テナントあたりのサービス接続数は、テナントごとに割り当てるユニット数と所有するライセンスの種類によって異なります。
  - グローバル ライセンスがあり、テナントに少なくとも1,000ユニットを割り当てている場合は、そのテナントに最大5つのサービス接続を割り当てることができます。
  - グローバル ライセンスがあり、テナントに200 ～ 999ユニットを割り当てる場合、そのテナントに最大2つのサービス接続を割り当てることができます (ローカルデプロイメントの接続数と同じ)。
  - ローカル ライセンスをお持ちの場合は、最小の200を超えて割り当てるユニット数に関係なく、テナントごとに最大2つのサービス接続を割り当てることができます。

  グローバル ライセンスとローカル ライセンスの両方で、さらに必要な場合はサービス接続用の追加ライセンスを購入できます。高度なデプロイメントにおけるサービス接続については、Prisma Accessサービス接続の高度なデプロイメント:を参照してください。

サービス接続の構成を開始する前に、 まず収集する必要がある情報を確認してください。

©2025 Palo Alto Networks, Inc.

サービス接続を計画します

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

Prisma Accessが以下のタスクを実行できるように、サービス接続を作成する：

- 本社またはデータセンター内のリソースへのアクセスを許可します。

  リモート・ネットワークやモバイル・ユーザーがアクセスする必要がある企業リソース がある場合は、Prisma Accessを有効にして、対応する企業ネットワークにアクセスできるようにする 必要があります。
- リモート ネットワークとモバイル ユーザーが相互に通信できるようにします。

  Prisma Accessユーザーが本社やデータセンターに接続する必要がない場合でも、モバイル ユーザーがリモート ネットワーク・サイトにアクセスできるようにする必要があるかもしれない。すべてのリモート ネットワーク サイトは完全にメッシュ化されていますが、モバイル ユーザー インフラストラクチャは完全にメッシュ化されていないため、このユース ケースではサービス接続が必要です。サービス接続を最小限に構成することで、モバイル ユーザーがブランチ ネットワークにアクセスするために必要なハブ アンド スポーク ネットワークが確立されます。

  ネットワーク効率を向上させるには、サービス接続をリモート ネットワークまたはモバイル ユーザーが最も頻繁にアクセスするネットワークの近くに配置します。

本社またはデータセンター情報を収集する

サービス接続の構成を開始する前に、Prisma Accessに接続させたい各本部またはデータセンターについて、以下の情報を収集してください。

モバイル ユーザーがリモート ネットワークの場所にアクセスできるようにするためだけにサービス接続を作成する場合は、この情報を収集する必要はありません。

Prisma Access (Managed by Strata Cloud Manager)と**Prisma Access (Managed by Panorama)**のサービス接続向け：

- ❑ 企業サイトでのIPSec対応のファイアウォール、ルーター、またはSD-WANデバイス接続。
- ❑ Prisma Accessから企業ネットワーク上の IPSec 対応デバイスへのプライマリ VPN トンネルを終端するための IPSec 設定。
- ❑ Prisma Accessから企業ネットワーク上のIPSec対応デバイスへのセカンダリVPNトンネルを終了するためのIPSec 設定。

  IPSecトンネル、トンネル監視、およびIPSec暗号プロファイル構成を含む既存のテンプレートがある場合は、そのテンプレートをテンプレート スタックに追加して、IPSecトンネルの

©2025 Palo Alto Networks, Inc.

作成プロセスを簡素化できます。または、自動的に作成されるService_Conn_Templateを編集し、企業サイトに戻る IPSec トンネルを作成するために必要なIPSec構成を作成することもできます。 また、Prisma Accessより一般的に使用されるネットワーク デバイス用の定義済みIPSecテンプレートのセットと、定義済みテンプレートに含まれていないデバイス用の汎用テンプレートも提供されます。

- サイトのIPサブネットワークのリスト。
- Prisma Accessが解決できなければならない内部ドメインのリスト。
- Prisma Accessが IPSec トンネル監視のためにICMP ping要求を送信できる、ネットワークのサイトにある企業アクセス ノードのIPアドレス。

  このアドレスが、Prisma Accessインフラのサブネット全体から ICMP で到達可能であることを確認する。
- サービス インフラストラクチャ サブネットのネットワーク到達性設定。

  本社またはデータセンターから、サービスインフラ全体のサブネットに到達できるようにする。Prisma Accessは、このサブネットからのすべての制御プレーン トラフィックにIPアドレスを使用する。

Prisma AccessPanoramaサービス接続専用：

この情報は、***Prisma Access (Managed by Panorama)***でサービス接続を計画する場合にのみ必要です。

- アクセスに必要な場合、認証用のサービス アカウント。
- サービス接続で使用するルーティング タイプ (静的または動的 (BGP))。

  Prisma Access (Managed by Panorama)がユーザーを必要なリソースにルーティングできるように、リソースへのルートを指定する必要があります。この作業には、次の1つまたは複数の方法を利用できます。

  - ユーザーにアクセスさせる各サブネットワークまたは特定のリソースへの、スタティックルートを定義する。
  - サービス接続ロケーションとPrisma Access間にBGPを設定します。
  - 両方の方法を組み合わせて使用する。

©2025 Palo Alto Networks, Inc.

Prisma Accessでサービス接続を設定する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス

Prisma Accessが以下のタスクを実行できるように、サービス接続を作成する：

- 本社またはデータセンター内のリソースへのアクセスを許可します。

  リモート・ネットワークやモバイル・ユーザーがアクセスする必要がある企業リソー スがある場合は、Prisma Accessを有効にして、対応する企業ネットワークにアクセスできるようにする 必要があります。サービス接続の構成を開始する前に、Prisma Accessに接続させたい各本部またはデータ センターについて、以下の情報を収集してください。

  - 企業サイトでのIPSec対応のファイアウォール、ルーター、またはSD-WANデバイス接続。
  - Prisma Accessから企業ネットワーク上の IPSec 対応デバイスへのプライマリ VPN トンネルを終端するための IPSec 設定。
  - Prisma Accessから企業ネットワーク上のIPSec対応デバイスへのセカンダリVPNトンネルを終了するためのIPSec 設定。

    IPSecトンネル、トンネル監視、およびIPSec暗号プロファイル構成を含む既存のテンプレートがある場合は、そのテンプレートをテンプレート スタックに追加して、IPSecトンネルの作成プロセスを簡素化できます。または、自動的に作成されるService_Conn_Templateを編集し、企業サイトに戻る IPSec トンネルを作成するために必要なIPSec構成を作成することもできます。 また、Prisma Accessより一般的に使用されるネットワーク デバイス用の定義済みIPSecテンプレートのセットと、定義済みテンプレートに含まれていないデバイス用の汎用テンプレートも提供されます。
  - サイトのIPサブネットワークのリスト。
  - Prisma Accessが解決できなければならない内部ドメインのリスト。
  - Prisma Accessが IPSec トンネル監視のためにICMP ping要求を送信できる、ネット ワークのサイトにある企業アクセス ノードのIPアドレス。

    このアドレスが、Prisma Accessインフラのサブネット全体から ICMP で到達可能であることを確認する。
  - サービス インフラストラクチャ サブネットのネットワーク到達性設定。

    本社またはデータセンターから、サービスインフラ全体のサブネットに到達できるようにする。Prisma Accessは、このサブネットからのすべての制御プレーン トラフィックにIPアドレスを使用する。
  - （Prisma Access (Managed by Panorama) のみ) アクセスに必要な場合は、認証用のサービスアカウント。

©2025 Palo Alto Networks, Inc.

- （Prisma Access (Managed by Panorama)のみ) サービス接続で使用するルーティングタイプ（スタティックまたはダイナミック（BGP））。
- (Prisma Access (Managed by Panorama)のみ) ユーザーを必要なリソースにルーティングできるように、リソースへのルートを指定する必要があります。この作業には、次の1つまたは複数の方法を利用できます。
  - ユーザーにアクセスさせる各サブネットワークまたは特定のリソースへの、スタティックルートを定義する。
  - サービス接続ロケーションとPrisma Access間にBGPを設定するPrisma Access。
  - 両方の方法を組み合わせて使用する
- リモート ネットワークとモバイル ユーザーが相互に通信できるようにします。

  Prisma Accessユーザーが本社やデータセンターに接続する必要がない場合でも、モバイル ユーザーがリモート ネットワーク・サイトにアクセスできるようにする必要があるかもしれない。すべてのリモート ネットワーク サイトは完全にメッシュ化されていますが、モバイル ユーザー インフラストラクチャは完全にメッシュ化されていないため、このユース ケースではサービス接続が必要です。サービス接続を最小限に構成することで、モバイル ユーザーがブランチ ネットワークにアクセスするために必要なハブ アンド スポーク ネットワークが確立されます。

  ネットワーク効率を向上させるには、サービス接続をリモート ネットワークまたはモバイル ユーザーが最も頻繁にアクセスするネットワークの近くに配置します。

- Strata Cloud Manager
- Panorama

Prisma Accessでサービス接続を設定する （Strata Cloud Manager）

Prisma Access (Managed by Strata Cloud Manager)のサービス接続を構成して、プライベート アプリまたは内部企業リソースへのアクセスを許可するには、以下の手順を実行します。

STEP 1 | **[Workflows (**ワークフロー**)]** > **Prisma Access [Setup (**セットアップ**)]** > **[Service Connections (**サービスコネクション**)]**を選択し、次に**[Add Service Connection (**サービス接続を追加**)]**を選択します。

STEP 2 | サービス接続にわかりやすい名前を付けます。

STEP 3 | 本社またはデータセンターがある**Prisma Access**ロケーションを選択します。

STEP 4 | (任意) モバイル ユーザーのソースNATを有効にします (GlobalProtect IPプール アドレス、インフラストラクチャ サブネット内のIPアドレス、またはその両方)。

Prisma AccessGlobalProtectモバイルユーザーとデータセンターのプライベートアプリケーションおよびリソース間のNATトラフィックに使用される1つまたは複数のサービス接続でサブネットを指定することができます。

- データ トラフィック ソース**NAT**- モバイル ユーザIPアドレス プール アドレスに対してNATを実行し、それらのアドレスがデータ センターにアドバタイズされないようにし、

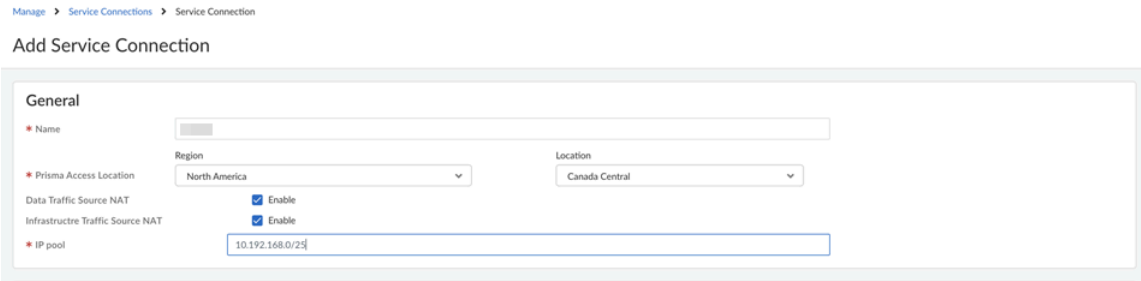
 ©2025 Palo Alto Networks, Inc.

サービス接続で指定したサブネットのみがデータ センターでアドバタイズされ、ルーティングされるようにします。

- インフラストラクチャ トラフィック ソース**NAT**- インフラストラクチャ サブネットのアドレスに対してNATを実行し、それらのアドレスがデータ センターにアドバタイズされないようにし、サービス接続で指定したサブネットのみがデータ センターでアドバタイズされ、ルーティングされるようにします。
- ユーザー**ID**–選択すると、Prisma Accessはこのサービス接続をID再ディストリビューションに使用します。

  ユーザー***ID***の再ディストリビューション管理- 特に大規模な*Prisma Access*のデプロイメントでは、ユーザー*ID*の再ディストリビューションに対してきめ細かい制御が必要になる場合があります。ユーザー*ID*再ディストリビューション管理を使用すると、 ユーザー ***ID***列のチェック マークを削除して特定のサービス接続のデフォルトの*ID*再ディストリビューション動作を手動で無効にし、*ID*再ディストリビューションに使用する特定のサービス接続を選択できます。ほとんどの構成ではこれを行う必要はありません。この機能を有効にするには、*Palo Alto Networks*サポートにお問い合わせください。

- ソース**NAT**プール- モバイル ユーザーのIPアドレス プール、インフラストラクチャ サブネット、またはその両方でNATを実行するために使用されるIPアドレス プールを指定します。
  - プライベート IP (RFC 1918) サブネットまたはルーティング ドメインでルーティング可能な適切なサブネットを使用します。
  - サブネットが、モバイル ユーザー - GlobalProtect IPアドレス プール、インフラストラクチャ サブネット、またはこのテナントに使用されるその他のソースNATアドレスと重複していないことを確認します。
  - /25 から /32 までのサブネットを入力します。



 ©2025 Palo Alto Networks, Inc.

STEP 5 | **IPSec** トンネルを選択します。プライマリまたはセカンダリIPSecトンネルをまだ設定していない場合は、**[設定]** を選択して、以下の手順に従います。

1. トンネルにわかりやすい名前を付けます。
2. IPSecデバイスと、Prisma Accessとのトンネルを確立するために使用するHQまたはデータセンター の**[Branch Device Type (ブランチ デバイス タイプ)]**を選択する。
3. ［**Branch Device IP Address**］ で、トンネルエンドポイントを識別するスタティック **IP** アドレスまたはダイナミック IP アドレスのいずれかを選択します。

   ブランチデバイスの**IP**アドレスをダイナミックに設定する場合は、HQまたはデータセンターのIKE ID（**IKE**ローカル**ID**）または Prisma Access (**IKE** ピア識別) により、IPSec ピアが認証できるようになります。

   サービス接続が完全に展開されるまでは、Prisma Access IKE ID（**IKE** ピア **ID**）に使用する値がないため、通常は、Prisma AccessIKE ID ではなく HQ/データセンター（**IKE** ローカル **ID**）に IKE ID を設定します。

STEP 6 | トンネルモニタリングをオンにする。

Prisma Accessがトンネルが稼働しているかどうかを判断するために、HQまたはデータセンターネットワーク上のトンネル監視先の宛先**IP**アドレスを入力し、支店のIPSecデバイスがポリシーベースを使用している場合は、関連するプロキシ**ID**を入力します。

入力したトンネル監視 IP アドレスは自動的にブランチ サブネットワークのリストに追加されます。

STEP 7 | トンネル設定を保存します。

STEP 8 | ルーティングとサービス品質設定を追加または調整するには、 **[ワークフロー] > [Prisma Accessセットアップ] > [サービス接続]** へと進み、 サービス接続を追加します。ルーティングまたは**QoS**設定のセットアップまたは編集を行います。

STEP 9 | スタティック ルートを設定します。

1. 本社またはデータ センターとの間でトラフィックをルーティングするためのスタティック ルートの場合は、ブランチで保護するIPサブネットまたはIPアドレスを追加します 。

   HQまたはデータ センター ネットワーク上のIPサブネットに変更を加えた場合は、スタティック ルートを手動で更新する必要があります。

STEP 10 | ダイナミック ルーティングを構成します。

1. HQまたはデータセンターのサブネットをアドバタイズするためのダイナミック ルーティングの場合は、 ダイナミック ルーティング用に**BGP**を有効にします。
2. (任意)**MRAI**タイマー 値を選択します。

   BGPルーティングでは、ネットワーク内のBGPルーティング収束を調整するために使用できる 最小ルート広告間隔 *(MRAI)*と呼ばれるタイマーが提供されます。MRAIは宛先ごとに更新のレートを制限するように機能し、BGPルータは同じプレフィックスのアドバタイズメントを送信する前に、少なくとも設定されたMRAI時間待機します。数値が小さいほど収束時間は速くなりますが、ネットワーク内に作成される広告は多くなりま

 ©2025 Palo Alto Networks, Inc.

す。数値が大きいほど、送信できる広告の数は減りますが、ルーティングの収束も遅くなる可能性があります。ルーティング収束の高速化と広告の削減の間の最適なバランスを実現するために、ネットワークに配置する数を決定します。

MRAIの範囲を1 ～ 600秒に設定します。デフォルト値は30秒です。

3. 顧客構内装置（CPE）へのBGPを介したモバイル ユーザIPサブネットのアドバタイズ数を減らすには、**[Summarize Mobile User Routes before advertising**（アドバタイズ前にモバイルユーザールートを要約する）**]**を選択して、アドバタイズする前にサブネットを要約するようにPrisma Accessを指定します。

   デフォルトでPrisma Accessは、モバイルユーザーのIPアドレスプールを、/24サブネットのブロックでアドバタイズします。それを要約すると、Prisma Accessによって指定したサブネットに基づいてプールがアドバタイズされます。たとえば、Prisma Accessは、パブリックユーザーのモバイルIPプールを、アドバタイズ前に10.8.1.0/24、10.8.2.0/24、10.8.3.0/24などのサブネットに分割するのではなく、/20のサブネットを使用して10.8.0.0/20のプールをアドバタイズします。これらのアドバタイズを要約することで、CPEルーティングテーブルに保存されるルート数を削減できる可能性があります。たとえば、限定された数のルートを受け付けるクラウドVPNゲートウェイ（仮想プライベートゲートウェイ（VGW）またはトランジットゲートウェイ（TGW））で、IPプールの要約を使用することができます。

4. （任意） Prisma AccesseBGPを使用してリモート ネットワークのデフォルト ルート アドバタイズメントを開始するには、**[Advertise the Default Route (**デフォルト ルートのアドバタイズ**)]**を選択します。ネットワークに、BGPがアドバタイズしている他のデフォルトルートが存在していないことを確認してください。そうしないと、ネットワークにルーティング上の問題が発生する可能性があります。

5. (任意) セカンダリWANを設定していて、セカンダリ (バックアップ) BGPピアのピア アドレスを変更する必要がある場合は、**[Use different BGP Peer for Secondary Tunnel (**セカンダリ トンネルに別の**BGP**ピアを使用する**)]** を選択し、一意のピアを入力し、必要に応じてセカンダリWANのローカルIPアドレスを入力します。

6. サービス接続から顧客宅内機器 (CPE) の eBGP ピアからの送信プレフィックスにコミュニティを追加するには、**[Add no-export community]** を**[Enabled Out]**に設定します。この機能はデフォルトでは 無効になっています。

   [Enabled In]または**[Enabled Both]**はサポートされていないため、選択しないでください。

7. （任意） Prisma AccessがHQまたはデータセンターにルートを転送しないようにするには、**[Do Not Export Routes (**ルートをエクスポートしない**)]**を選択します。

   デフォルトで、Prisma Accessは、ローカルルート、および他のサービス接続、リモートネットワーク、およびモバイルユーザーサブネットから受信するすべてのプレフィックスを含め、すべてのBGPルーティング情報をアドバタイズします。Prisma AccessによるBGPアドバタイズメントの送信を防止しながら、受信したBGP情報を使って、他のBGPネイバーからルートを学習するには、このチェックボックスを選択します。

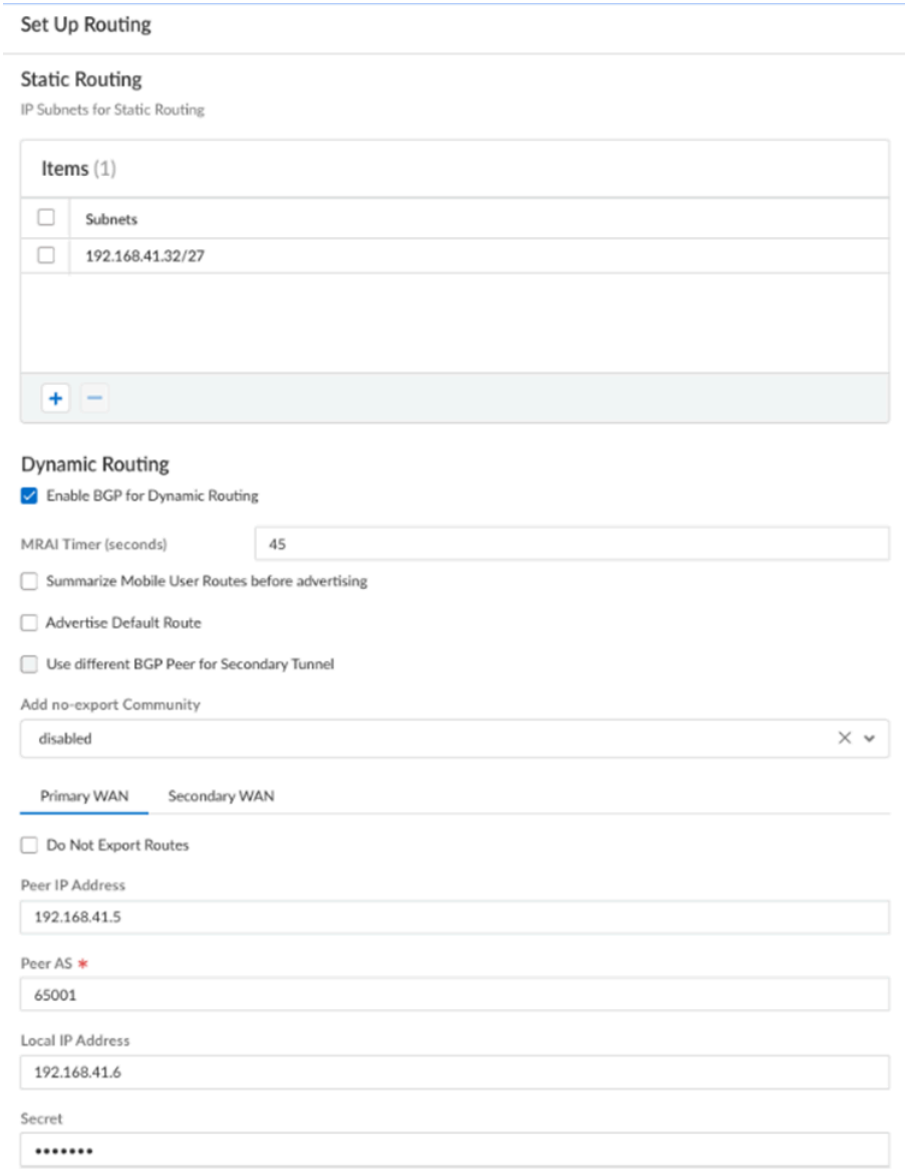
   Prisma AccessはBGPアドバタイズを送信しないため、このオプションを選択した場合は、Prisma Accessに戻るルートを確立するために、オンプレミス機器にスタティック ルートを設定する必要があります。

©2025 Palo Alto Networks, Inc.

8. HQまたはデータセンター ネットワーク上のeBGPルーターのルーターIDとして割り当てられた ピア**IP**アドレス を入力します。
9. ネットワークの自律システム (AS) である **Peer AS**を入力します。

   RFC 6996準拠のBGPプライベートAS番号を使用します。
10. が**BGP**のローカル**IP**アドレスとして使用するローカルIPアドレスPrisma Accessを入力します。

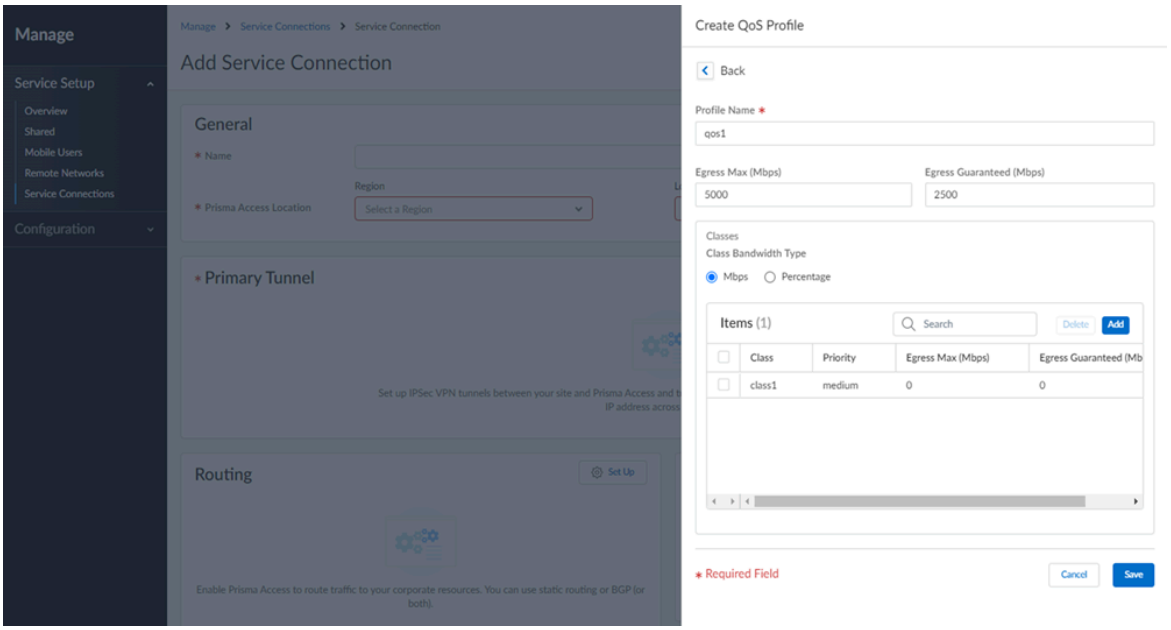
    ローカル アドレスは、BGPピアリングを成功させるためにHQまたはデータ センター デバイスで必要な場合にのみ必要です。指定するIPアドレスは、インフラサブネットまたはリモートネットワーク内のサブネットのIPアドレスと、競合またはオーバーラップしていないことを確認してください。
11. BGP ピア通信を認証するためのシークレットパスワードを入力します。
12. [シークレットの確認]を選択します。



 ©2025 Palo Alto Networks, Inc.

STEP 11 | （任意） QoSを設定します。

始めに、QoS Profileを追加して、HQまたはデータセンターとPrisma Access間のトラフィックを形成するQoSクラスを定義します。次に、QoSポリシー ルールを作成し、そのルールにプロファイルを追加して、一致するHQまたはデータ センターのトラフィックにQoSを適用します。



1. **QoS**プロファイルの名前を入力します。
2. **[Create New**（新規作成）**]**を選択します。
3. HQまたはデータ センター サービス接続から送信されるトラフィックの最大スループット (Mbps 単位) を**Egress Max**として設定します。

   本社またはデータセンターの最大ライセンス帯域幅までの値を指定できます。
4. 保証された帯域幅を **Egress Guaranteed**(Mbps 単位) として設定します。

   Egress Guaranteed [最低保証帯域 出力側]の値を超えるトラフィックは、ベスト エフォートで、保証されません。保証されているが使用されていない帯域幅は、すべてのトラフィックで引き続き利用可能です。
5. 各QoSクラス を定義し、ポリシー ルールに添付します。

   QoSクラスにより、QoSポリシールールにマッチしたトラフィックの優先度と帯域幅が決まります。単一のQoSプロファイルには、定義可能なQoSクラスが8つあります。特

 ©2025 Palo Alto Networks, Inc.

に設定しない限り、QoS クラスに一致しないトラフィックには class 4 が割り当てられます。

6. QoSクラスの優先度を設定します。

   優先度には、リアルタイム、高、中、低があります。

7. 出力最大 値を設定します。

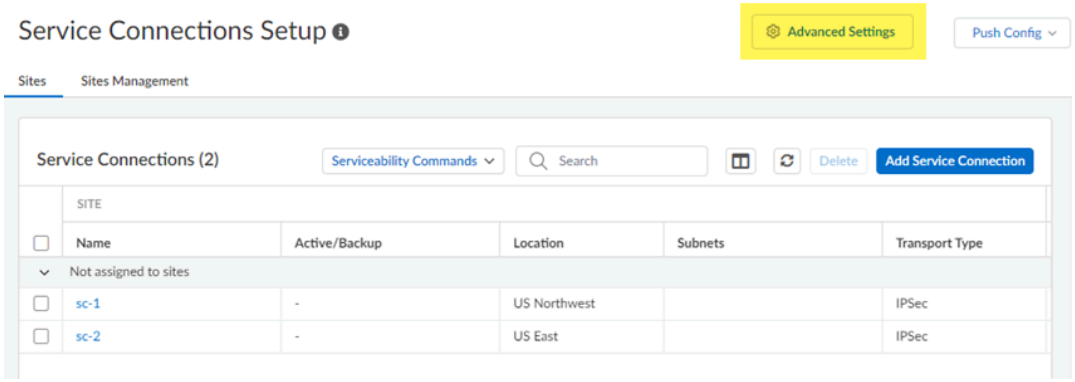
   QoSクラスの出力最大値、または複数のQoSクラスの出力最大値の組み合わせは、QoSプロファイルの出力最大値を超えてはなりません。

8. 出力保証値を設定します。

   QoSクラスに割り当てられた保証帯域幅はそのクラス用に予約されず、未使用の帯域幅はすべてのトラフィックで使用可能になります。出力保証値を超えるクラスのトラフィックはベストエフォートですが、保証されません。

©2025 Palo Alto Networks, Inc.

STEP 12 | サービス接続の詳細設定を構成します。



1. サービス接続で使用する、**BGP Routing Preference**（**BGP**ルーティング基本設定）を指定します。

   組織のネットワークまたはPrisma Accessネットワークで使用する、サービス接続トラフィックを処理するための、ネットワーク基本設定を指定できます。

   - **Default**（デフォルト）—Prisma Accessの内部ネットワークで、デフォルトのルーティングを使用します。
   - **Hot potato routing**（ホットポテトルーティング）—Prisma Accessは、サービス接続トラフィックを組織のWANにできる限り即座に渡します。

   *Prisma Access*サービス接続のルーティング方法を変更するには、組織のトポロジーとルーティングデバイス、および*Prisma Access*のルーティングの仕組みを完全に理解しておく必要があります。ルーティング方法をデフォルトから変更する前に、サービス接続トラフィックのルーティングをよくお読みになることをお勧めします。

2. バックアップ トンネルなしでトンネルがダウンしたときにPrisma Accessでスタティック ルートを削除する場合は、[サービス接続またはリモート ネットワーク**IPSec**トンネルがダウンしている場合はスタティック ルートを撤回する]を選択します 。

   Prisma Accessは次の状況ではルートを削除します。

   - プライマリ トンネルがダウンし、セカンダリ トンネルが存在しません。
   - プライマリ トンネルとセカンダリ トンネルが構成されているが、両方がダウンした場合。

   トンネル監視が有効になっていない場合、この変更を適用することはできません。

3. サービス接続に使用するバックボーン ルーティングを構成します。

   デフォルトでは、 Prisma Accessバックボーンでは、サービス接続を介してデータ センターまたは本社から返されるトラフィックに対して対称ネットワーク パスが必要で

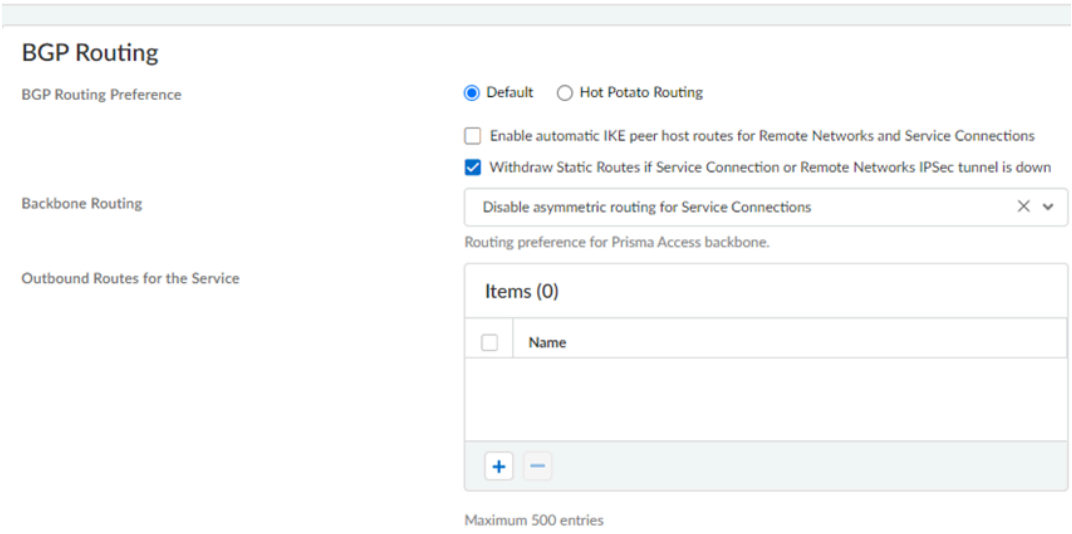
 ©2025 Palo Alto Networks, Inc.

す。CPEからのサービス接続にECMPまたは別の負荷分散メカニズムを使用したい場合は、Prisma Accessバックボーンを介して非対称フローを有効にできます。

- サービス接続バックボーン全体で対称フローを要求するには、[サービス接続の非対称ルーティングを無効にする] を選択します。
- Prisma Access がサービス接続バックボーン全体で非対称フローを使用できるようにするには、**[Allow asymmetric routing for Service Connections (**サービス接続の非対称ルーティングを許可する)]を選択します。
- 1つの場所に複数のサービス接続がある場合、[サービス接続全体で非対称ルーティングと負荷分散を許可する](デフォルト設定)を選択することで、Prisma Accessデプロイメントで負荷 分散を利用できます。ただし、負荷分散はベストエフォート方式で行われるため、サービス接続の1つがダウンすると負荷分散は失敗します。

  [サービス接続間で非対称ルーティングと負荷分散を許可する]を選択すると、Prisma Accessは GlobalProtectポータルとゲートウェイおよびサービス接続間のネットワーク冗長性を有効にします。この機能により、モバイル ユーザー データプレーンと異なるコンピューティング場所のサービス接続の間に冗長ネットワーク パスが提供されます。冗長性を有効にすると、ユーザーはデータ センターまたは本社のサービス接続の背後にあるリソースに、より回復力のあるアクセスを提供できます。モバイル ユーザーがリモート ネットワークのリソースにアクセスするにはサービス接続が必要であるため、ユーザーはリモート ネットワークの場所にあるリソースにアクセスする際の回復力も向上します。

4. （オプション） Prisma Accessがすべてのサービス接続とリモート・ネットワーク接続にスタティック ルートを追加するプレフィックスを 500 個まで追加して、サービスのアウトバウンドルートを指定します。 その後、Prisma Accessはインターネット経由でこれらのプレフィックスにトラフィックをルーティングします。



その他のIKEオプション

Prisma Accessは、選択した IPSecデバイス・タイプに基づいて、HQ/DCのデバイスとPrisma Accessとの間の IKE フェーズ1鍵交換プロセスに推奨される暗号のセットと鍵の有効期間を提供します。推奨設定を使用することも、環境に応じて設定をカスタマイズすることもできます。

 ©2025 Palo Alto Networks, Inc.

IKEネゴシエーションに使用するIPSecデバイスと Prisma Access の **IKE** プロトコル バージョンを選択します。

[IKEv1 Only Mode]を選択すると、Prisma AccessはネゴシエーションにIKEv1プロトコルのみを使用できます。**[IKEv1 Only Mode]**を選択すると、Prisma AccessはネゴシエーションにIKEv1プロトコルのみを使用できます。**IKEv2**優先モードを選択した場合、Prisma AccessIPSec デバイスもIKEv2をサポートしている場合にのみ、IKEv2 プロトコルを使用します。IPSecデバイスがIKEv2をサポートしていない場合、Prisma AccessはIKEv1プロトコルの使用に戻ります。

IKEv1 暗号プロファイル を追加して、IKE フェーズ 1 のキー交換プロセスに使用される暗号化および認証アルゴリズムを定義する IKE 暗号設定をカスタマイズします。

Prisma Accessは、このトンネルの確立に使用されているブランチ デバイス タイプに基づいて、デフォルトの IKE 暗号プロファイルを自動的に使用します。

- 暗号化- IKE SA ネゴシエーションで使用される暗号化アルゴリズムを指定します。

  Prisma Accessは、次の暗号化アルゴリズムをサポートしています。3des (168 ビット)、aes-128-cbc (128 ビット)、aes-192-cbc (192 ビット)、aes-256-cbc (256 ビット)、およびDES (56 ビット)。null (暗号化なし) を選択することもできます。
- 認証- IKE SA ネゴシエーションで使用される認証アルゴリズムを指定します。

  Prisma Accessは、sha1 (160 ビット)、sha256 (256 ビット)、sha384 (384 ビット)、sha512 (512 ビット)、および md5 (128 ビット) の認証アルゴリズムをサポートします。null (認証なし) を選択することもできます。
- **DH** グループ—IKE SA ネゴシエーションで IKE の対称キーを生成するために使用される Diffie-Hellman (DH) グループを指定します。Diffie-Hellman アルゴリズムは、一方の秘密鍵ともう一方の公開鍵を使用して共有のシークレットを作成します。これは、両方の VPN トンネル ピアによって共有される暗号化鍵です。

  Prisma Accessは次のDHグループをサポートします。グループ 1 (768 ビット)、グループ 2 (1024 ビット-デフォルト）、グループ 5 (1536 ビット)、グループ 14 (2048 ビット)、グループ 19 (256 ビット楕円曲線グループ)、グループ 20 (384 ビット楕円曲線グループ)です。セキュリティを最強にするには、最も大きい番号のグループを選択します。
- ライフタイム- IKE フェーズ 1 キーが有効である単位と時間を指定します (デフォルト 8 時間)。IKEv1 の場合、security association (SA) は、鍵の有効期限が切れる前にアクティブに鍵更新されません。IKEv1 フェーズ 1 の鍵更新は、SA の有効期限が切れた場合にのみトリガーされます。IKEv2 の場合、キーの有効期限が切れる前に SA の鍵更新する必要があります。SA の有効期限が切れたときに鍵更新すされない場合、SA は新しいフェーズ 1 鍵を開始する必要があります。
- **IKEv2 Authentication Multiple**—認証カウントを決定するために、Key Lifetime (キーの有効期間) で乗算される値を指定します（範囲は0 ～ 50、デフォルトは0）。認証カウントは、セキュリティ処理ノードが IKEv2 IKE SA 鍵更新を実行できる回数であり、この回数だけ実行した後は、IKEv2 再認証をやり直す必要があります。デフォルト値の0は、再認証機能が無効になります。

©2025 Palo Alto Networks, Inc.

IKE パッシブ モード を有効にして、Prisma Accessが IKE 接続にのみ応答し、IKE 接続を開始しないようにします。

IKE NAT トラバーサルは デフォルトでオンになっています。

これは、IKE および UDP プロトコルに UDP カプセル化が使用され、IPSec VPNトンネルのエンドポイント間にあるネットワークアドレス変換（NAT）デバイスを通過できることを意味します。

その他のIPSecオプション

Prisma Accessは、選択したIPSecデバイス タイプに基づいて、セキュリティ・アソシエーション（SA）のIKE フェーズ2において、IPSecデバイスと Prisma Access 間のIPSecトンネル内のデータを保護するために推奨されるIPSecプロトコルと鍵の有効期間設定のセットを提供します。推奨設定を使用することも、環境に応じて設定をカスタマイズすることもできます。

IPSec暗号プロファイル をカスタマイズして、Auto Key IKE が IKE フェーズ 2 中に IKE SA のキーを自動的に生成するときに、トンネル内でデータを保護する方法を定義します。

Prisma Accessは 、ブランチ デバイス タイプ ベンダーに基づいてデフォルトのIPSec暗号プロファイルを自動的に構成します。デフォルトのプロファイルを使用することも、カスタムプロファイルを作成することもできます。

- **IPSec** プロトコル- VPN トンネルを通過するデータを保護します。Encapsulating Security Payload (**ESP**) プロトコルは、データの暗号化、ソースの認証、およびデータ整合性の検証を行います。Authentication Header (**AH**) プロトコルは、ソースの認証とデータ整合性の検証を行います。

  IPSec プロトコルとして **ESP** を使用する場合は、IPSec SA ネゴシエーションで使用される暗号化 アルゴリズムも指定します。

  Prisma Accessは、次の暗号化アルゴリズムをサポートしています: aes-256-gcm (256 ビット)、aes-256-cbc (256 ビット)、aes-192-cbc (192 ビット)、aes-128-gcm (128 ビット)、aes- 128-cbc (128 ビット)、3des (168 ビット)、および DES (56 ビット)。null (暗号化なし) を選択することもできます。

認証- IPSec SA ネゴシエーションで使用される認証アルゴリズムを指定します。

Prisma Accessは、sha1 (160 ビット)、sha256 (256 ビット)、sha384 (384 ビット)、sha512 (512 ビット)、および md5 (128 ビット) の認証アルゴリズムをサポートします。IPSec プロトコルがESPの場合は、[none (なし)] (認証なし) を選択することもできます。

DH グループ-IPSec security association (Security Associations - SA) ネゴシエーションで IKE の Diffie-Hellman (DH) グループを指定します。

Prisma Accessは次のDHグループをサポートします。グループ 1 (768 ビット)、グループ 2 (1024 ビット-デフォルト）、グループ 5 (1536 ビット)、グループ 14 (2048 ビット)、グループ 19 (256 ビット楕円曲線グループ)、グループ 20 (384 ビット楕円曲線グループ)です。セキュリティを最強にするには、最も大きい番号のグループを選択します。Prisma Accessが IKE フェーズ 1 中に作成するキーを更新したくない場合は、**no-pfs**(完全転送秘密なし) を選択

©2025 Palo Alto Networks, Inc.

します。このオプションを選択すると、Prisma AccessはIPSec SAネゴシエーションに現在のキーを再利用します。

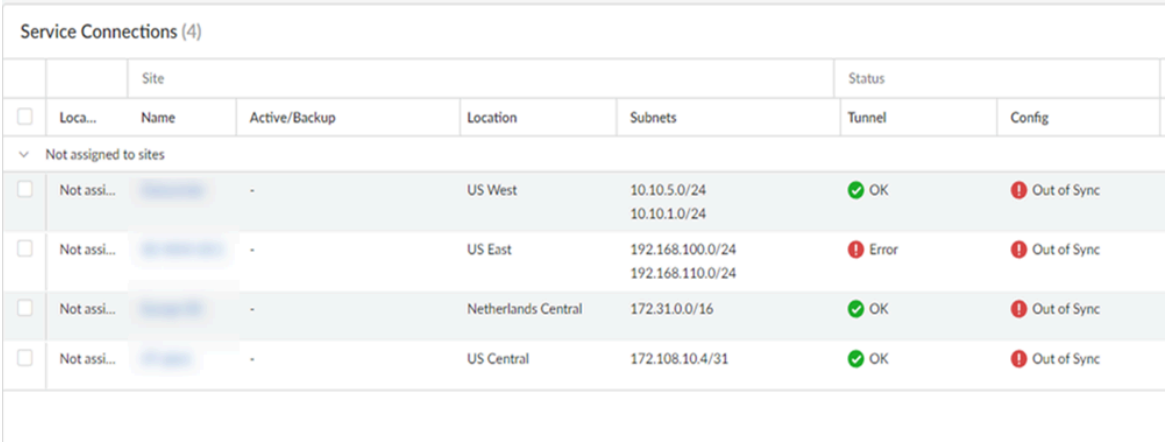
ライフタイム- ネゴシエートされたキーが有効である単位と時間を指定します (デフォルトは1時間)。

ライフサイズ- キーが暗号化に使用できるデータの単位と量を指定します。

サービス接続のステータスを確認します。

サービス接続が正常に設定されたことを確認するには、**[ワークフロー] > [Prisma Accessセットアップ] > [サービス接続]**を選択し、 **[ステータス]** が **OK**であることを確認します。

ステータスが**OK**になっていない場合は、Statusアイコン上にカーソルを移動して、エラーがあるかどうかを確認してください。



サイト 領域では、オンボードされたすべてのサービス接続とそのステータスおよびその他の詳細を表示できます。

サイト

- 名前- サービス接続の名前。
- アクティブ/バックアップ- サービス接続のアクティブな場所とバックアップの場所。
- サブネット- サービス接続に割り当てられたインフラストラクチャ サブネット。

ステータス

- **Tunnel**（トンネル）–Prisma Accessとサービス接続間の接続の運用ステータス。
- **Config**（設定）–サービスへの設定の最後のプッシュのステータス。ローカル設定とクラウド内の設定が一致する場合、Config Statusは**In sync**（同期）になります。ローカルで変更を行ったけれども、まだクラウドに設定をプッシュしていない場合、ステータス**Out of sync**（非同期）が表示される可能性があります。ステータスインジケータ上にカーソルを移動すると、詳細情報が表示されます。設定をPrisma Accessにコミットしてプッシュすると、Config Statusが**In sync**になります。

Prisma Access

- **Location**（ロケーション）–サービス接続がデプロイされたロケーション。

©2025 Palo Alto Networks, Inc.

- サービスIP- サービス接続のIPアドレス。
- EBGP ルーター- サービス接続におけるEBGPルーターのIPアドレス。

リンク

- BGP IPv4– サービス接続におけるBGP IPv4ルーティングのステータス。
- BGP IPv6– サービス接続におけるBGP IPv6ルーティングのステータス。
- IPSecトンネル- サービス接続のIPSecトンネル。最初に確立する IPSec トンネルが (プライマリ) トンネルになります。2番目のIPSecトンネルを確立した場合、それは (セカンダリ) トンネルになります。
- ピアIPアドレス- サービス接続のゲートウェイIPアドレス。

Prisma Accessでサービス接続を設定する （Panorama）

Prisma Access Panoramaのサービス接続を構成して、プライベート アプリまたは内部企業リソースへのアクセスを許可するには、以下の手順を実行します。

サービス接続のオンボードと構成には*CLI*を使用しないでください。サービス接続をオンボードするために*CLI*を使用する必要がある場合は、*Palo Alto Networks*チームにお問い合わせください。

STEP 1 | **Panorama** > **Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Service Connection**（サービス接続）を選択します。

STEP 2 | いずれかの企業ネットワークサイトに新しいサービス接続を**Add**（追加）します。

STEP 3 | 企業サイトの **Name**（名前）を指定します。

STEP 4 | サイトの場所から、もっとも近い**Location**（ロケーション）を選択します。

Prisma Accessロケーションのリストはこのセクションを参照してください。

2 つのアスタリスクで示される場所は、 ローカル ゾーンです。このような立地は、コンピュート、ストレージ、データベース、インフラストラクチャー サービスを人口や産業の中心地の近くに配置することになりますが、いくつかの制限もあります。ローカル ゾーンを追加するには、Palo Alto Networksの担当者にお問い合わせください。

STEP 5 | 企業のロケーションにある、ファイアウォール、ルーター、またはSD-WANデバイスにアクセスするための**IPSec Tunnel**（**IPSec**トンネル）を選択、または新たに追加します。

- 既存の **IPSec**トンネル 構成を使用している場合は、ドロップダウンから選択します。各サービス接続用に作成しているトンネルは、Prisma Accessを企業の各ロケーションにあるIPSec対応デバイスに接続するものであることに注意してください。IKEゲートウェイ設定のピアアドレスは、各トンネルに対して一意でなければなりません。ただ

©2025 Palo Alto Networks, Inc.

し、Crypto（暗号）プロファイルなど、他の一般的な一部の設定エレメントの再使用は可能です。

> 選択する*IPSec*トンネルは、*Auto Key*（自動鍵）交換と*IPv4*のみを使用する必要があります。さらに、*IPSec* トンネル、*IKE* ゲートウェイ、および暗号プロファイル名が *31* 文字以下であることを確認してください。

- 新しい IPSec トンネル構成を作成する には:

  [新しい **IPSec** トンネル]をクリックし、 名前 を付けて、[IKE ゲートウェイ]、[IPSec 暗号化プロファイル]、および [トンネル監視] 設定を構成します。

- 本社またはデータセンターのIPSec対応デバイスがポリシーベースのVPNを使用している場合:

  Proxy IDs（プロキシ**ID**）タブで、Prisma Accessがローカルデバイスとの**IPSec**トンネルを正常に確立できるように、ローカルIPSecデバイスに設定されているプロキシIDと一致するプロキシIDを**Add**（追加）します。

- 返信攻撃を検出して無効化するには:

  リプレイ保護を有効にするをそのままにします。

- 元のToS情報を保存するには:

  カプセル化されたパケットの内部IPヘッダーから外部IPヘッダーにTOS（Type of Service）フィールドをコピーするには、**Copy TOS Header**（**TOS**ヘッダーのコピー）を選択します。

- サービス接続のトンネル監視を有効にするには:

  Tunnel Monitor (トンネル モニター**)**を選択します。

  - **Destination IP**（宛先**IP**）アドレスを入力します。

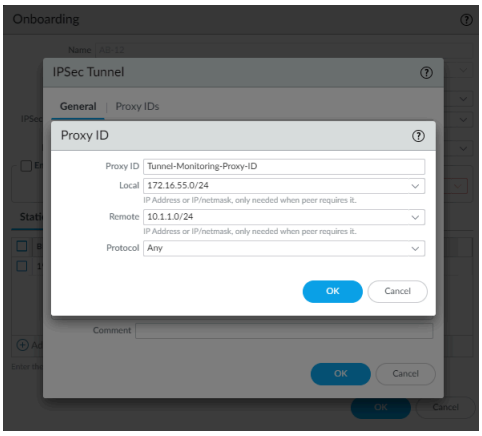
    Prisma AccessがIPSecトンネル監視のために、ICMP pingリクエストを送信できる、本社またはデータセンターサイトのIPアドレスを指定します。このアドレスが、Prisma Accessインフラのサブネット全体から、ICMPで到達可能であることを確認してください。

  - 複数のプロキシIDを使用するピアデバイスでトンネル監視をしようする場合、**Proxy ID**（プロキシ**ID**）を指定するか、またはインフラサブネットから本社またはデータセ

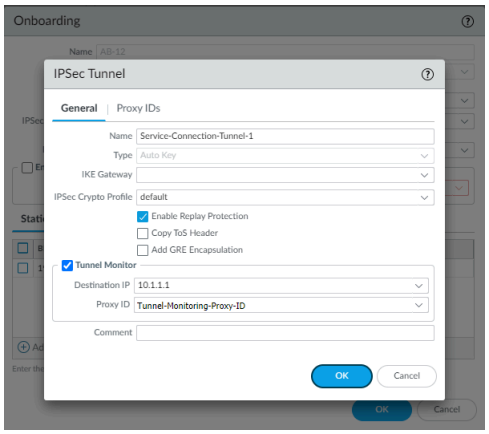
©2025 Palo Alto Networks, Inc.

ンターサイトへのアクセスを可能にする、**New Proxy ID**（新しいプロキシ**ID**）を追加します。

サービスインフラサブネット（この例では172.16.55.0/24）を**Local**（ローカル）IPサブネットに、本社/データセンターのサブネット（この例では10.1.1.0/24）を**Remote**（リモート）サブネットにしているプロキシIDの例を次に示します。



次の図は、作成したプロキシIDを**Proxy ID**（プロキシ**ID**）フィールドに指定することで、そのプロキシIDをトンネル監視に適用した例です。



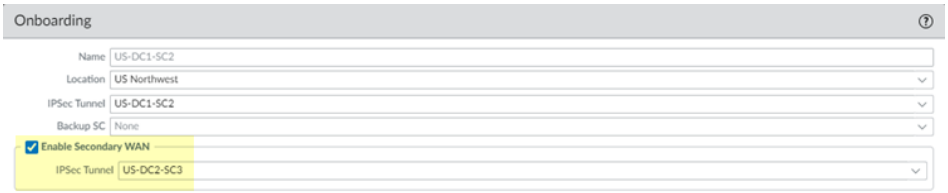
トンネル監視が機能するには、*CPE* 上でトンネルモニタリング *IP* アドレスへのスタティックルートを構成する必要があります。データセンター/本社から*Prisma Access*へのトンネル監視に使用する宛先*IP*アドレスを探すには、***Panorama*** > ***Cloud Services***（クラウドサービス） > ***Status***（ステータス） > ***Network Details***（ネットワーク詳細）を選択して、 *Service Infrastructure*（サービス インフラストラクチャ）をクリックして、***Tunnel Monitor IP Address***（トンネル監視***IP***アドレス）を参照します。

STEP 6 | BGPおよびホットポテトルーティングデプロイ環境のみ—優先するバックアップ（**Backup SC**）として使用するサービス接続を選択します。

すでに追加したサービス接続を選択することができます。 Prisma Accessは、リンク障害が発生した場合、選択した**Backup SC**を優先サービス接続として使用します。バックアップサービス接続を選択することで、3つ以上のサービス接続をオンボーディングしている場

 ©2025 Palo Alto Networks, Inc.

合の、非対称ルーティングの問題を防止することができます。この選択肢は、Hot potato routing（ホットポテトルーティング）モードでのみ利用できます。



STEP 7 | このロケーションにセカンダリWANリンクがある場合、**Enable Secondary WAN**（セカンダリ**WAN**を有効にする）を選択してから、プライマリIPSecトンネルのセットアップ時と同様の方法で、**IPSec Tunnel**（**IPSec**トンネル）を選択または設定します。

プライマリWANリンクが停止した場合、Prisma Accessは機能停止を検出して、セカンダリWANリンク経由で本社のデータセンターへのトンネルを確立します。プライマリWANリンクが復旧すると、リンクがプライマリリンクに切り替えられます。

セカンダリWANの設定は、次のデプロイメントではサポートされていません。

- セカンダリWANがプライマリ IPsec トンネルを使用してアクティブ/アクティブモードに設定されている場合。
- 顧客宅内機器 (CPE) が、プライマリおよびセカンダリIPsecトンネルを使用する等コストマルチパス (ECMP) 構成で設定されている場合。

スタティックルートを使用する場合、トンネルのフェイルオーバー時間は検出時から15秒未満になりますが、ご利用のWANプロバイダによって異なります。

BGPルーティングを設定し、トンネル監視を有効にしている場合、セキュリティパラメータインデックス（SPI）が失敗していると判断するまでの、デフォルトのホールドタイムがもっとも短いのが、Tunnel Monitorです。これは、連続した15秒間のトンネル障害を検出すると、ピアへのすべてのルートを削除します。このように、Tunnel MonitorがBGPルートの動作を判断します。トンネルモニタリングを設定しない場合、ホールドタイマーはルートを削除する前にトンネルがダウンしている時間を決定します。 Prisma Accessは、RFC 4271で定義されているデフォルトのBGP HoldTime値90秒を使用します。これは、Prisma Accessが非アクティブなSPIのルートを削除するまでの最大待機時間です。ピアBGPデバイスに短いホールドタイムが設定されている場合、BGPホールドタイマーはより小さい方の値を使用します。

セカンダリトンネルが正常にインストールされた場合、プライマリトンネルが復旧するまでの間、セカンダリルートが優先されます。プライマリとセカンダリの両方が機能している場合は、プライマリルートが優先されます。

セカンダリ（バックアップ）接続に別の*BGP*ピアを使用する場合、*Prisma Access*は *CPE* によってアドバタイズされたマルチエグジットディスクリミネーター（*MED*）属性を尊重しません。この注意事項は、リモートネットワーク接続またはサービス接続のいずれかで複数の *BGP* ピアを使用する場合に適用されます。

©2025 Palo Alto Networks, Inc.

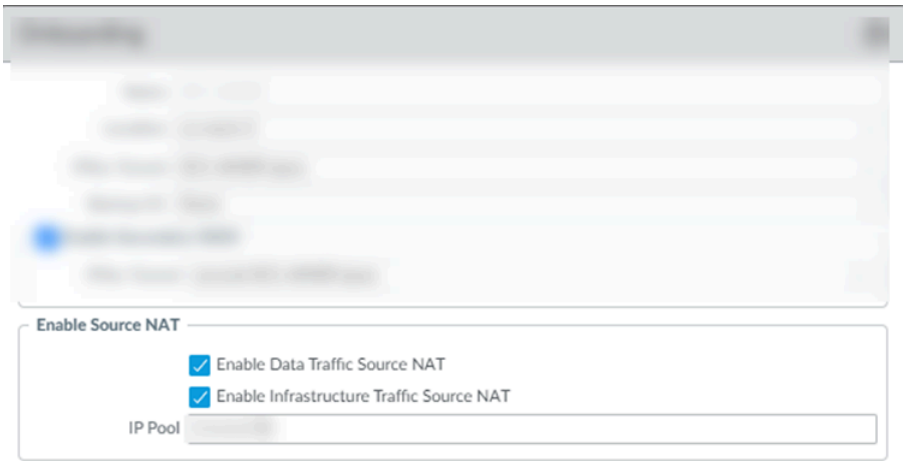
STEP 8 | (任意) モバイル ユーザーのソースNATを有効にします (GlobalProtect IPプール アドレス、インフラストラクチャ サブネット内のIPアドレス、またはその両方)。

Prisma AccessGlobalProtectモバイルユーザーとデータセンターのプライベートアプリケーションおよびリソース間のNATトラフィックに使用される1つまたは複数のサービス接続でサブネットを指定することができます。

- データ トラフィック ソース**NAT**を有効にする- モバイル ユーザIPアドレス プール アドレスに対してNATを実行し、それらのアドレスがデータ センターにアドバタイズされないようにし、サービス接続で指定したサブネットのみがデータ センターでアドバタイズされ、ルーティングされるようにします。
- インフラストラクチャ トラフィック ソース**NAT**を有効にする- インフラストラクチャ サブネットのアドレスに対して NAT を実行し、それらのアドレスがデータ センターにアドバタイズされないようにし、サービス接続で指定したサブネットのみがデータ センターでアドバタイズされ、ルーティングされるようにします。
- ユーザー**ID**–選択すると、Prisma Accessはこのサービス接続をID再ディストリビューションに使用します。

  ユーザー*ID*の再ディストリビューション管理- 特に大規模な*Prisma Access*のデプロイメントでは、ユーザー*ID*の再ディストリビューションに対してきめ細かい制御が必要になる場合があります。ユーザー*ID*再ディストリビューション管理を使用すると、 ユーザー ***ID***列のチェック マークを削除して特定のサービス接続のデフォルトの*ID*再ディストリビューション動作を手動で無効にし、*ID*再ディストリビューションに使用する特定のサービス接続を選択できます。ほとんどの構成ではこれを行う必要はありません。この機能を有効にするには、*Palo Alto Networks*サポートにお問い合わせください。
- **IP**プール- モバイル ユーザーのIPアドレス プール、インフラストラクチャ サブネット、またはその両方でNATを実行するために使用されるIPアドレス プールを指定します。

  プライベート IP (RFC 1918) サブネットまたはルーティング ドメイン内でルーティング可能で、モバイル ユーザー - GlobalProtect IPアドレス プールまたはインフラストラクチャ サブネットと重複しない適切なサブネットを使用します。/25 から /32 までのサブネットを入力します。



 ©2025 Palo Alto Networks, Inc.

STEP 9 | ユーザーがアクセスする必要がある、企業サイトのサブネットワークまたは個別のIPアドレスへのルーティングを有効にします。

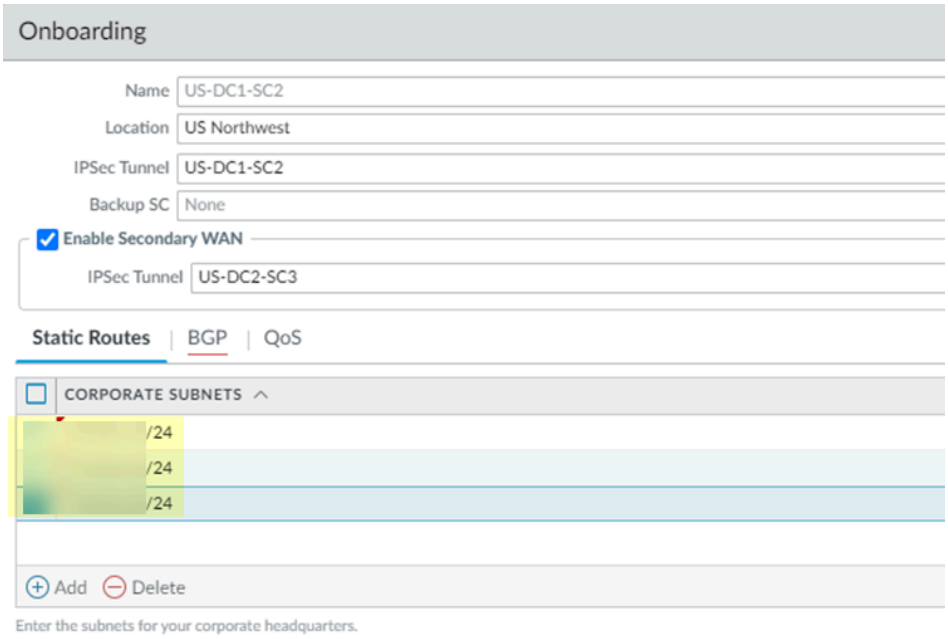
Prisma Accessはこの情報を使って、適切なサイトにリクエストをルーティングします。各サイトのネットワークは相互にオーバーラップすることはできません。また、サービスインフラ用またはユーザー用のPrisma AccessIPプール用に指定した各IPアドレスプールをオーバーラップさせることもできません。**Static Routes**（スタティックルート）、**BGP**、または両方の組み合わせを設定することができます。

Static Routes（スタティックルート）を設定するには：

1. **Static Routes**（スタティックルート）タブで**Add**（追加）をクリックして、リモートユーザーがアクセスする必要があるサブネットワークアドレス（例：172.168.10.0/24）、またはDNSサーバーなどのリソースの個別のIPアドレス（例：10.32.5.1/32）を入力します。

 ©2025 Palo Alto Networks, Inc.

2. Prisma Accessがこの場所でアクセスを必要とするすべてのサブネットまたは IP アドレスについて、これを繰り返します。



BGPを設定する場合:

1. **BGP**タブで、 **Enable**を選択します。

   BGPを有効にすると、Prisma Accessインフラストラクチャとe**BGP**接続を終了する顧客構内装置(CPE)間で発生する可能性のある余分なホップに対応するため、Prisma Accessでは外部BGP(eBGP)のTTL(time-to-live)値を8に設定します。

   *Prisma Access*は、サービス接続またはリモートネットワーク接続の *BGP* デフォルトルート広告を受け入れません。

2. (任意) 次の選択肢から選択します。

   - 顧客宅内機器 (CPE) の eBGP ピアからの送信プレフィックスに企業アクセス ノード (サービス接続) の **no-export** コミュニティを追加するには、**[Add no-export community]** を **[Enabled Out]**に設定します。この機能はデフォルトでは 無効になっています 。

     ホットポテト ルーティング モードではこの機能を使用しないでください。

   - Prisma AccessBGPピアが、組織のネットワークにルートを転送することを防止します。**Prisma Access Routes**をアドバタイズしないでください。

     デフォルトで、Prisma Accessは、ローカルルート、および他のサービス接続、リモートネットワーク、およびモバイルユーザーサブネットから受信するすべてのプレフィックスを含め、すべてのBGPルーティング情報をアドバタイズします。Prisma AccessがBGPアドバタイズメントを送信しないようにしても、他の BGP ネイバーからルート

©2025 Palo Alto Networks, Inc.

を学習するために受信した BGP 情報を使用する場合は、このチェックボックスをオンにします。

> このオプションを選択した場合、*Prisma Access*は*BGP*アドバタイズメントを送信しないため、オンプレミス機器にスタティック・ルートを設定し、*Prisma Access*に戻るルートを確立する必要があります。

- BGPから顧客構内設備（CPE）にアドバタイズされるモバイルユーザーIPサブネット数を減らすには、**Summarize Mobile User Routes before advertising**（アドバタイズ前にモバイルユーザールートを要約する）を選択して、サブネットをアドバタイズする前に要約するように指定します。

  デフォルトでは、Prisma Accessは/24サブネットのブロックでモバイル ユーザーのIPアドレス プールをアドバタイズします。それらを要約した場合、Prisma Accessは指定したサブネットに基づいてプールをアドバタイズします。たとえば、Prisma Accessは、パブリックユーザーのモバイルIPプールを、アドバタイズ前に10.8.1.0/24、10.8.2.0/24、10.8.3.0/24などのサブネットに分割するのではなく、/20のサブネットを使用して10.8.0.0/20のプールをアドバタイズします。これらのアドバタイズを要約することで、CPEルーティングテーブルに保存されるルート数を削減できる可能性があります。たとえば、限られた数のルートを受け入れることができるクラウド VPN ゲートウェイ (仮想プライベート ゲートウェイ (VGW) またはトランジット ゲートウェイ (TGW)) で IP プールの集約を使用できます。

  > ホットポテトルーティングを有効にしてルート集約を有効にすると、*Prisma Access*は非対称ルーティングを引き起こす可能性のある *AS-PATH* を先頭に追加しなくなります。ホットポテトルーティングでルート要約を有効にする前に、データセンターまたは本社からのリターントラフィックの、対称的なリターンが保証されていることを確認してください。

3. (任意)**MRAI**タイマー値を選択します。

   BGPルーティングでは、ネットワーク内のBGPルーティング収束を調整するために使用できる 最小ルート広告間隔 *(MRAI)*と呼ばれるタイマーが提供されます。MRAIは宛先ごとに更新のレートを制限するように機能し、BGPルータは同じプレフィックスのアドバタイズメントを送信する前に、少なくとも設定されたMRAI時間待機します。数値が小さいほど収束時間は速くなりますが、ネットワーク内に作成される広告は多くなります。数値が大きいほど、送信できる広告の数は減りますが、ルーティングの収束も遅くなる可能性があります。ルーティング収束の高速化と広告の削減の間の最適なバランスを実現するために、ネットワークに配置する数を決定します。

   MRAI の範囲を1 ～ 600秒に設定します。デフォルト値は30秒です。
4. このサービス接続を**Peer Address**（ピアアドレス）として設定するデータセンター/本社ネットワーク上の、eBGPルーターのルーターID として割り当てるIPアドレスを入力します。
5. **Peer AS**を入力します。これは、データセンター/本社ネットワークのファイアウォール仮想ルーターまたはBGPルーターが所属している自律型システム（AS）です。
6. (任意) Prisma AccessがBGPのローカルIPアドレスとして使用するアドレスを入力する。

   Local Addressの指定は、接続のもう一方の側にあるデバイス（Amazon Web Service（AWS） Virtual Private Gatewayなど）が、BGPピアリングを正常に行うために、特定の

 ©2025 Palo Alto Networks, Inc.

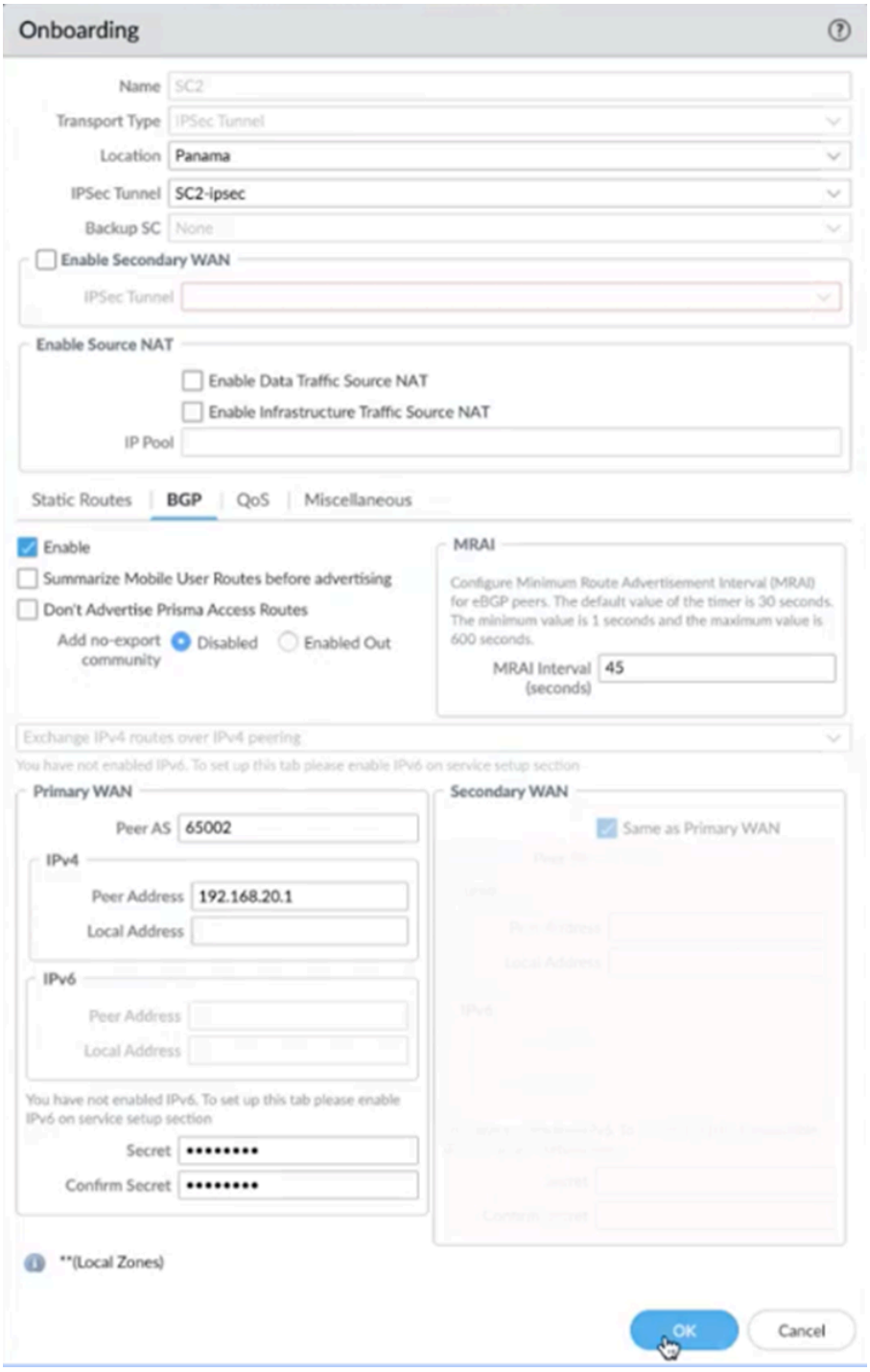
ローカルIPアドレスを必要としている場合などに役立ちます。指定するアドレスが、インフラストラクチャ サブネットまたはサービス接続のサブネット内の IP アドレスと競合または重複していないことを確認してください。

*CPE*上で*BGP* ローカル アドレスへのスタティック ルートを設定する必要があります。

サービス接続にIPV6サポートを使用する場合は、**IPv4**アドレスだけでなく **IPv6**アドレスも構成できます。また、IPv6アドレッシングを使用する前に、Prisma AccessインフラでIPv6ネットワークをグローバルに有効にする必要があります。

©2025 Palo Alto Networks, Inc.

7. （任意） BGPピア通信の認証のために、**Secret**（シークレット）にパスフレーズを入力して、その内容を確認します。



STEP 10 | （任意）**Secondary WAN**（セカンダリ**WAN**）を設定しており、セカンダリ（バックアップ）BGPピアの**Peer Address**（ピアアドレス）または**Local Address**（ローカルアドレス）を変更する必要がある場合、**Same as Primary WAN**（プライマリ**WAN**と同じ）の選択

©2025 Palo Alto Networks, Inc.

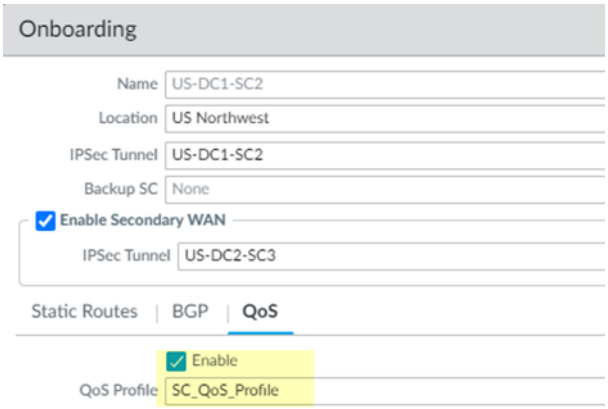
を解除して一意のピアを入力します。また、必要に応じてセカンダリWANのローカルIPアドレスを入力します。

一部のデプロイ環境では（例:AWS VPNゲートウェイを持つピアにBGPを使用している）、プライマリWANとセカンダリWANのBGPピアが異なっていることがあります。そのような場合、セカンダリWANに対して、別のBGPピアを設定することができます。

セカンダリ*WAN*を使用する *BGP*導入の場合、*Prisma Access*はプライマリおよびセカンダリトンネルの両方を***UP***状態に設定するが、ネットワーク トラフィックについては通常の*BGP*アクティブ バックアップ動作に従います。*Prisma Access*はプライマリ トンネルをアクティブに設定し、そのトンネルを介してのみトラフィックを送受信します。プライマリ トンネルに障害が発生した場合、*Prisma Access*は*BGP*ルールを使用して障害を検出し、セカンダリ トンネルをアクティブに設定し、セカンダリ トンネルのみを使用してトラフィックを送受信します。

STEP 11 | (任意)必要に応じて、サービス接続の**Quality of Service**（サービス品質）を有効にして、QoSプロファイルを指定するか、または**New QoS Profile**（新しい**QoS**プロファイル）を追加します。

リモートネットワークおよびサービス接続へのQoSトラフィックをシェーピングするために、QoS プロファイルを作成して、PAN-OSセキュリティポリシーでマークしたトラフィック、オンプレミスデバイスでマークしたトラフィック、またはPAN-OSがマークしたトラフィックとオンプレミスがマークしたトラフィックの両方に対して、それらのプロファイルを適用することができます。詳細は リモートネットワークのQoS を参照してください。



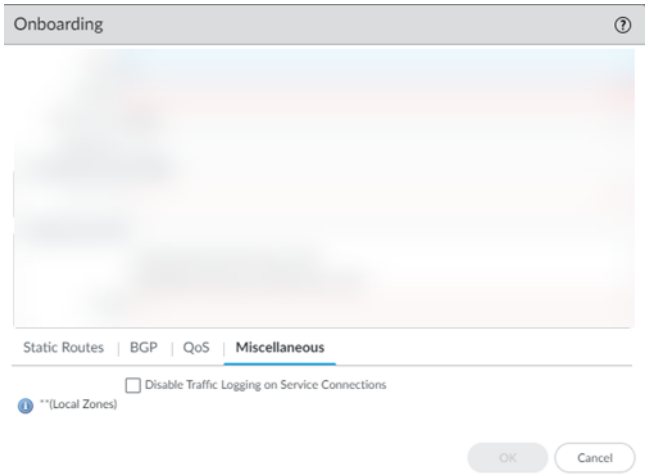
STEP 12 | (任意) その他の 設定を構成します。

1. （任意） [サービス接続のトラフィック ロギングを無効にする]を選択すると、Prisma Accessデプロイメントのサービス接 続でのロギングが無効になります。

   サービス接続によってログ記録されるトラフィックフローの大半が非対称である場合、Strata Logging Serviceロギングストレージの消費を抑えるために、サービス接続の

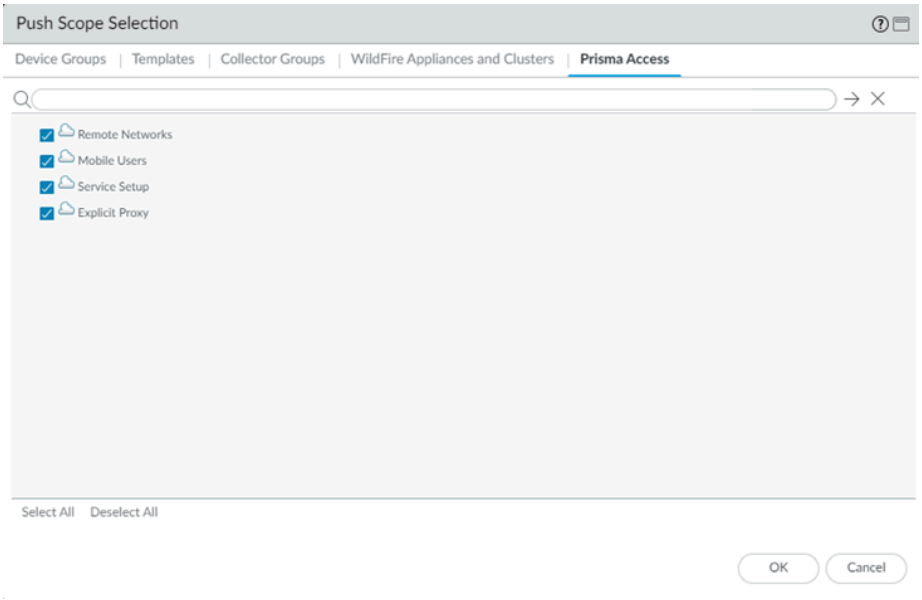
 ©2025 Palo Alto Networks, Inc.

ロギングを無効にする必要がある場合があります。デプロイメントにサービス接続経由の非対称フローがない場合、ログ記録を無効にする必要はありません。



STEP 13 | Panoramaに変更をコミットし、その設定変更をPrisma Accessにプッシュします。

1. **Commit**（コミット） > **Commit and Push**（コミットしてプッシュ）をクリックします。
2. [選択内容を編集]をクリックし、**[Prisma Access]**タブで**[Push Scope (**スコープをプッシュ**)]**に**[Service Setup (**サービスのセットアップ**)]**が選択されていることを確認し、**[OK]**をクリックする。



3. **[Commit and Push (**コミットしてプッシュ**)]** をクリックします。

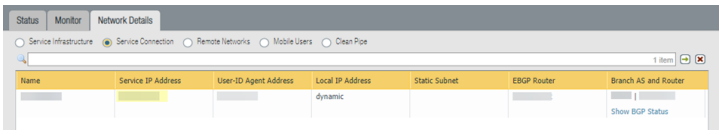
STEP 14 | 他のサービス接続を追加するには、ステップ2～ステップ11を繰り返します。

©2025 Palo Alto Networks, Inc.

STEP 15 | 企業ネットワーク上のIPSec対応デバイスからPrisma Accessへの、IPSecトンネルを1つまたは複数設定します。

1. Prisma Access内のトンネルのIPアドレスを判断するには、**Panorama > Cloud Services**（クラウドサービス） **> Status**（ステータス） **> Network Details**（ネットワーク詳細） の順に選択して、 **Service Connection**（サービス接続） ラジオボタンをクリックして、サイトの **Service IP Address**（サービス**IP**アドレス）を記録します。

   サービス**IP**アドレスは、IPSec対応デバイスからサービス接続へのトンネルを作成する際に接続する必要がある、パブリックに面しているアドレスです。



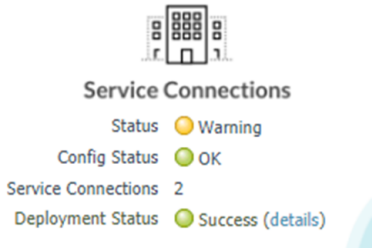
2. 企業所在地にあるIPSec対応デバイスで、 Prisma Access内のサービス**IP**アドレス に接続するIPSecトンネルを構成し、そのデバイス上で変更をコミットして、 トンネルを確立できるようにします。

サービス接続のステータスを確認します。

サービス接続が正常にセットアップされたことを検証するには、**Panorama > Cloud Services**（クラウドサービス） **> Status**（ステータス） **> Status**（ステータス）の順に選択して、Status（ステータス）が**OK**になっていることを確認してください。

モバイル ユーザーとリモート ネットワークのユーザー間の通信を可能にするためにプレースホルダー値を使用してサービス接続を作成した場合、サービス接続の状態を確認する必要はありません。

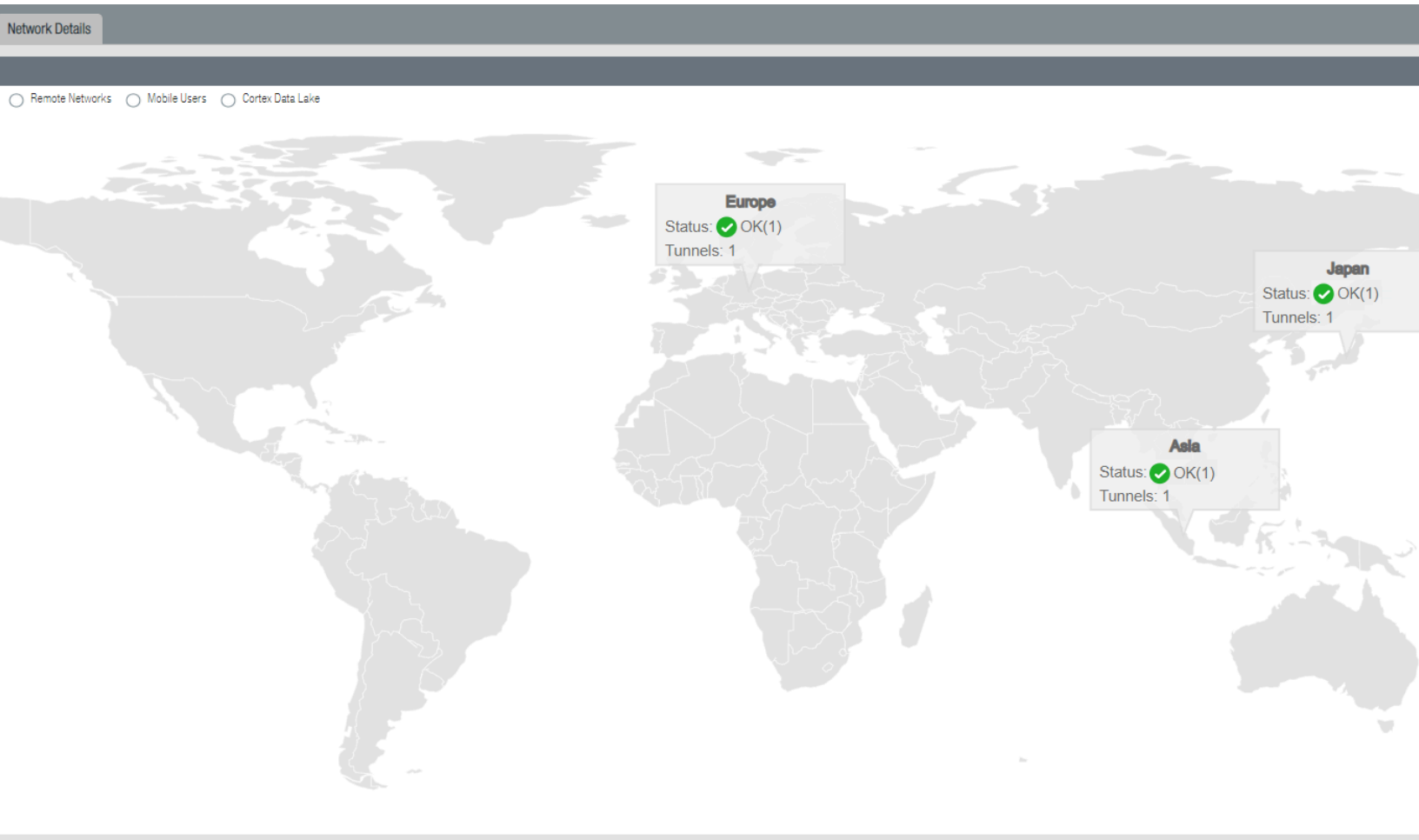
Deployment Status（デプロイステータス）では、オンボーディングおよびデプロイジョブのステータスを参照することができます。また、完了したジョブのステータスに関する詳細情報も参照することができます。



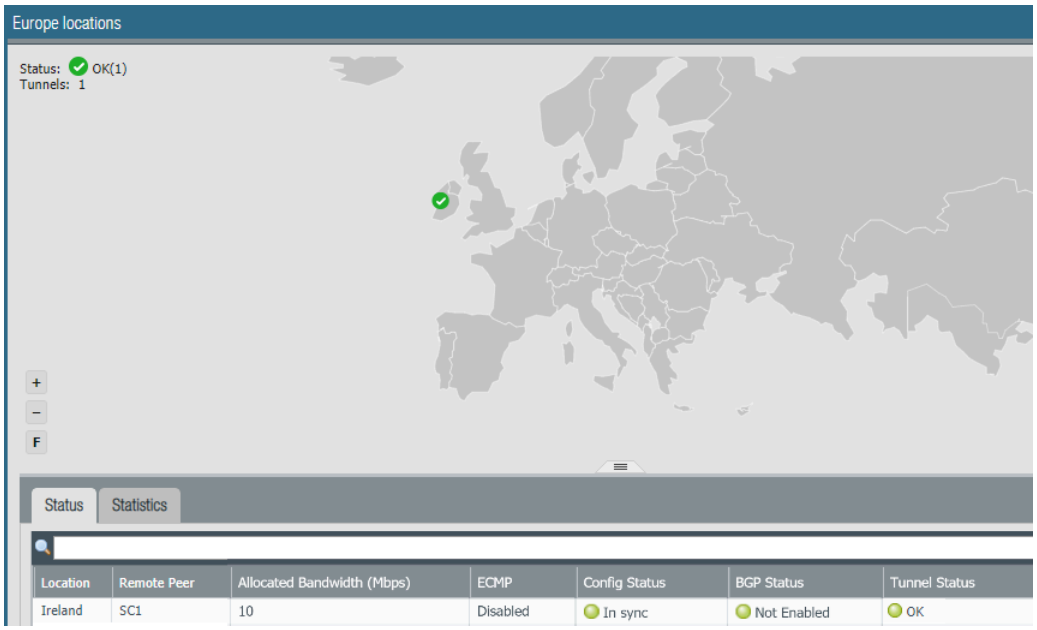
ステータスが**OK**になっていない場合は、Statusアイコン上にカーソルを移動して、エラーがあるかどうかを確認してください。

サービス接続のグラフィカル表示とステータス詳細を参照するには、**Monitor**（監視）タブで**Service Connection**（サービス接続）を選択します。

 ©2025 Palo Alto Networks, Inc.



地域を選択すると、その地域の詳細情報が表示されます。



マップの下にあるタブをクリックすると、サービス接続に関するその他の情報が表示されます。

©2025 Palo Alto Networks, Inc.

Status（ステータス）タブ：

- **Location**（ロケーション）–サービス接続がデプロイされたロケーション。
- **Remote Peer**（リモートピア）–このサービスインフラが、IPSecトンネルをセットアップしている、企業のロケーション。
- **Allocated Bandwidth**（割当たられている帯域幅）–割り当てられたサービス接続数に300 Mbpsを乗じた値。

  この数値は、利用可能なサービス接続帯域幅を表しているものではありません。

  各サービス接続は約*1Gbps* のスループットを提供しますが、実際のスループットは次のようないくつかの要因に依存します。

  - トラフィックミックス（例:フレームサイズ）
  - サービス接続と本社またはデータセンター間のレイテンシとパケットロス
  - サービスプロバイダのパフォーマンス制限
  - 顧客の終端デバイスのパフォーマンス制限
  - その他の顧客データセントートラフィック

- **ECMP**–このサービス接続に対してECMP（Equal Cost Multipath）を設定している場合。サービス接続ではECMPが使用されないため、このステータスは**Disabled**（無効）になります。
- **Config Status**（設定ステータス）–サービスへの設定の最後のプッシュのステータス。ローカル設定とクラウド内の設定が一致する場合、Config Statusは**In sync**（同期）になります。ローカルで変更を行ったけれども、まだクラウドに設定をプッシュしていない場合、ステータス**Out of sync**（非同期）が表示される可能性があります。ステータスインジケータ上にカーソルを移動すると、詳細情報が表示されます。設定をPrisma Accessにコミットしてプッシュすると、Config Statusが**In sync**になります。
- **BGP Status**（**BGP**ステータス）–企業/本社のロケーションのファイアウォールまたはルーターとサービス接続が確立されているPrisma Access間のBGP状態に関する情報が表示されます。一時的にステータスが各種BGP状態（**Idle**、**Active**、**Open send**、**Open pend**、**Open confirm**）に切り替わることがありますが、一般的にBGPステータスには次のような項目が表示されます。

  - **Connect**（接続）–データセンター/本社のルーターが、Prisma AccessとのBGPピアリレーションシップの確立を試みています。
  - **Established**（確立済み）–BGPピアリレーションシップが確立されています。

  このフィールドには、BGP接続がエラー状態にあるかどうかも表示されます。

  - **Warning**（警告）–8分間以上に渡ってBGPステータスの更新がありません。ファイアウォールが機能停止している可能性があります。
  - **Error**（エラー）–BGPステータスが不明です。

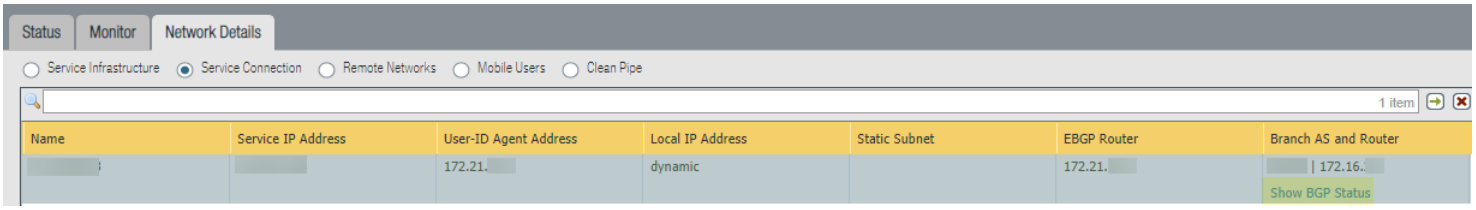
- **Tunnel Status**（トンネル ステータス）–Prisma Accessとサービス接続間の接続の運用ステータス。

©2025 Palo Alto Networks, Inc.

Statistics（統計）タブ：

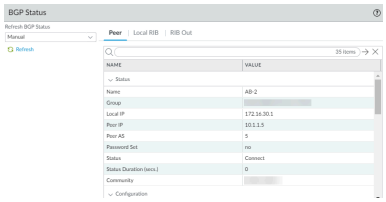
- **Location**（ロケーション）–サービス接続がデプロイされたロケーション。
- **Remote Peer**（リモートピア）–このサービス接続が、IPSecトンネルをセットアップしている、企業のロケーション。
- **Ingress Bandwidth (Mbps)**（着信帯域幅）–本社/データセンターのロケーションからPrisma Accessへの帯域幅。
- **Ingress Peak Bandwidth (Mbps)**（着信ピーク帯域幅）–本社/データセンターのロケーションからクラウドサービスへのピーク負荷。
- **Egress Bandwidth (Mbps)**（発信帯域幅）–Prisma Accessから本社/データセンターのロケーションへの帯域幅。
- **Egress Peak Bandwidth (Mbps)**（発信ピーク帯域幅）–Prisma Accessから本社/データセンターのロケーションへのピーク負荷。
- **QoS**–このボタンを選択すると、クラスあたりの破棄パケット数を含めた、リアルタイムの、および過去のQoS統計情報を表したグラフが表示されます。このグラフには、QoSが有効になっているサービス接続またはリモートネットワーク接続のみが表示されます。

BGPを設定した場合、**Panorama** > **Cloud Services**（クラウドサービス） > **Status**（ステータス） > **Network Details**（ネットワーク詳細） > **Service Connection**（サービス接続） > **Show BGP Status**（**BGP**ステータスの表示）の順に選択して、そのステータスを確認することができます。



BGP Status（BGPステータス）ダイアログが表示されます。このタブには、次の情報が表示されます。

- **Peer**（ピア）–ステータス、ルート数合計、設定、およびランタイム統計とカウンタを含む、BGPピアのルーティング情報。ルート数合計は**bgpAfiIpv4-unicast Counters**エリアの、**Incoming Total**（着信合計）および**Outgoing Total**（発信合計）フィールドに表示されます。

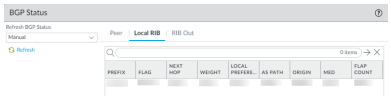


- ローカル**RIB**- Prisma Accessがローカルで使用する BGP ルート。Prisma Accessは、隣接するネットワーキングデバイスから送信された情報を保管する、BGP RIB-Inテーブルからこの情報を選択し、ローカルBGPインポートポリシーおよびルーティング決定を適用し、ルーティング情報ベース（RIB）にローカルのRIB情報を保管します。

  最初の256件のエントリのみが表示されることに注意してください。その他のエントリを表示するには、Filter（フィルタ）フィールドにサブネットまたはIPアドレスを入力して、Apply

 ©2025 Palo Alto Networks, Inc.

Filter（フィルタの適用）をクリックします。最大256件の、ルーティングエントリのサブセットが表示されます。



- **RIB Out**—BGP更新メッセージを利用して、Prisma Accessがピアにアドバタイズするルーティング情報。

©2025 Palo Alto Networks, Inc.

サービス接続を使用してモバイル ユーザーとリモート ネットワーク間のアクセスを有効にする

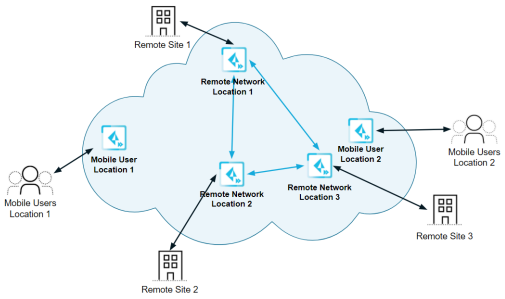
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ サイト間およびユーザー間アクセス用のネット相互接続を含むPrisma Accessライセンス

モバイルユーザーおよびリモートネットワークを接続するサービス接続を設定するには、次の値を使ってサービス接続を**Add**（追加）します。

- モバイルユーザーに近い**Region**（地域）を選択します。
- プレースホルダ値を使って、**IPSec Tunnel**（**IPSec**トンネル）および**IKE Gateway**（**IKE**ゲートウェイ）を**Add**（追加）します。
- プレースホルダ**Corporate Subnets**（企業サブネット）を追加します。

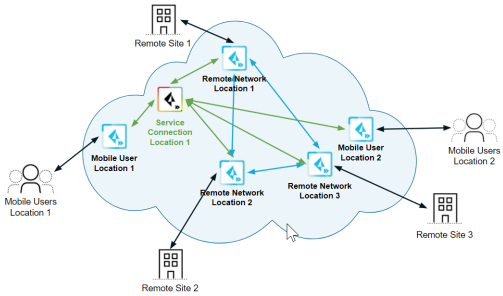
  Prisma Accessはこのトンネルを使ってトラフィックをルーティングしないため、他の設定されたサブネットと競合/オーバーラップしない任意の値が有効とみなされます。

異なる地理的エリアにモバイルユーザー達が存在し、リモートネットワークがあるPrisma Accessデプロイメント環境の例を次に示します。リモートネットワーク接続は、Prisma Accessインフラ内のメッシュネットワークで接続されていますが、モバイルユーザーはリモートネットワークに接続できません。また、異なる地理的エリアにいるモバイルユーザーは、サービス接続なしでは相互に接続できません。

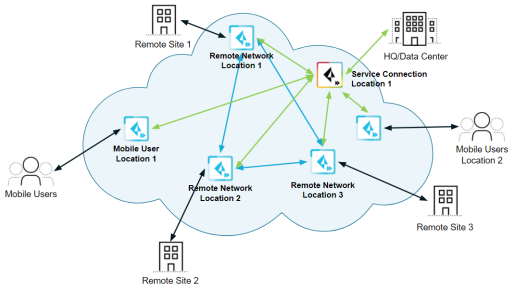


サービス接続の追加後は、サービス接続がモバイルユーザーとリモートネットワークをハブアンドスポークネットワーク内で接続します。

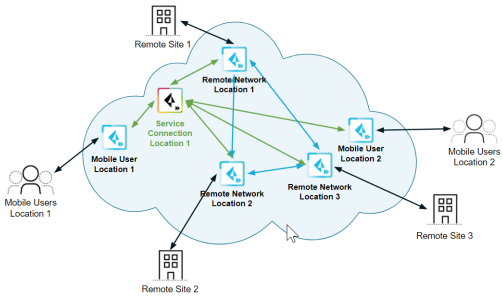
©2025 Palo Alto Networks, Inc.



サービス接続がモバイルユーザーから遠方にあるような場合も、このタイプのサービス接続が役立ちます。このタイプのネットワークデプロイメントの例を、次の図に示します。



モバイルユーザーにより近い場所に2番目のサービス接続を追加することで、モバイルユーザーとリモートネットワーク間のより効率的なネットワークを実現できます。



 ©2025 Palo Alto Networks, Inc.

サービス接続のダイナミック ルーティングに関する考慮事項

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

仕組み - サービス接続トラフィックのルーティング

Prisma AccessはダイナミックルーティングにBGPを使用しており、BGPパス選択を使ってルーティングテーブルにルートをインストールします。Prisma Accessは、サービス接続を使用して本社またはデータセンターにトラフィックをルーティング するとき、そのトラフィックを効果的に誘導するルーティング方法を使用します。 Prisma Accessは、大半のネットワーク デプロイメントに適合するように設計されたデフォルトのルーティング モデルを 使用するが、すべての組織のネットワークが同じとは限りません。幅広いデプロイメントに対応するために、Prisma Accessではサービス接続のルーティングについて他のモードを選択することも可能です。以下のセクションでは、Prisma Accessが使用するBGPルーティング方法と、Prisma Accessのデフォルトのサービス接続ルーティン グ方法を変更する前に組織のネットワークで考慮する必要がある要因について説明します。

*Prisma Access*サービス接続のルーティング方法を変更するには、組織のトポロジーとルーティングデバイス、および*Prisma Access*のルーティングの仕組みをこのセクションで説明している通りに完全に理解しておく必要があります。ルーティング方法をデフォルト設定から変更する前に、このセクションを入念に読んでおくことをお勧めします。

Prisma Accessは、スタティック ルーティングと、サービスとリモート ネットワーク接続のためのBGPを使用したダイナミック ルーティングをサポートしています。このセクションでは、Prisma AccessのデプロイメントにBGPルーティングを使用することを前提としています。BGPルーティングを選択すると、組織ネットワークはPrisma AccessからBGP情報を学習します。

サービス接続のルーティングモード

Prisma Accessでは、次のルーティング手法を選択できます。

- デフォルトルーティング - これはPrisma Accessが使用する現在のルーティングモデルです。

  Prisma AccessがBGP属性を調整せずにBGPベストパス選択メカニズムを使用したい場合は、このルーティン グモードを使用する。このモードでPrisma Accessは、カスタマ構内設備（CPE）がアドバタイズする任意の属性を使用します。

©2025 Palo Alto Networks, Inc.

- Hot Potatoルーティング—Prisma Accessは、できる限り早く組織ネットワークにトラフィックを渡します。

  組織ネットワークに、大部分のルーティング決定を行わせたい場合に、このルーティング手法を使用します。

Prisma Access デフォルトルーティング

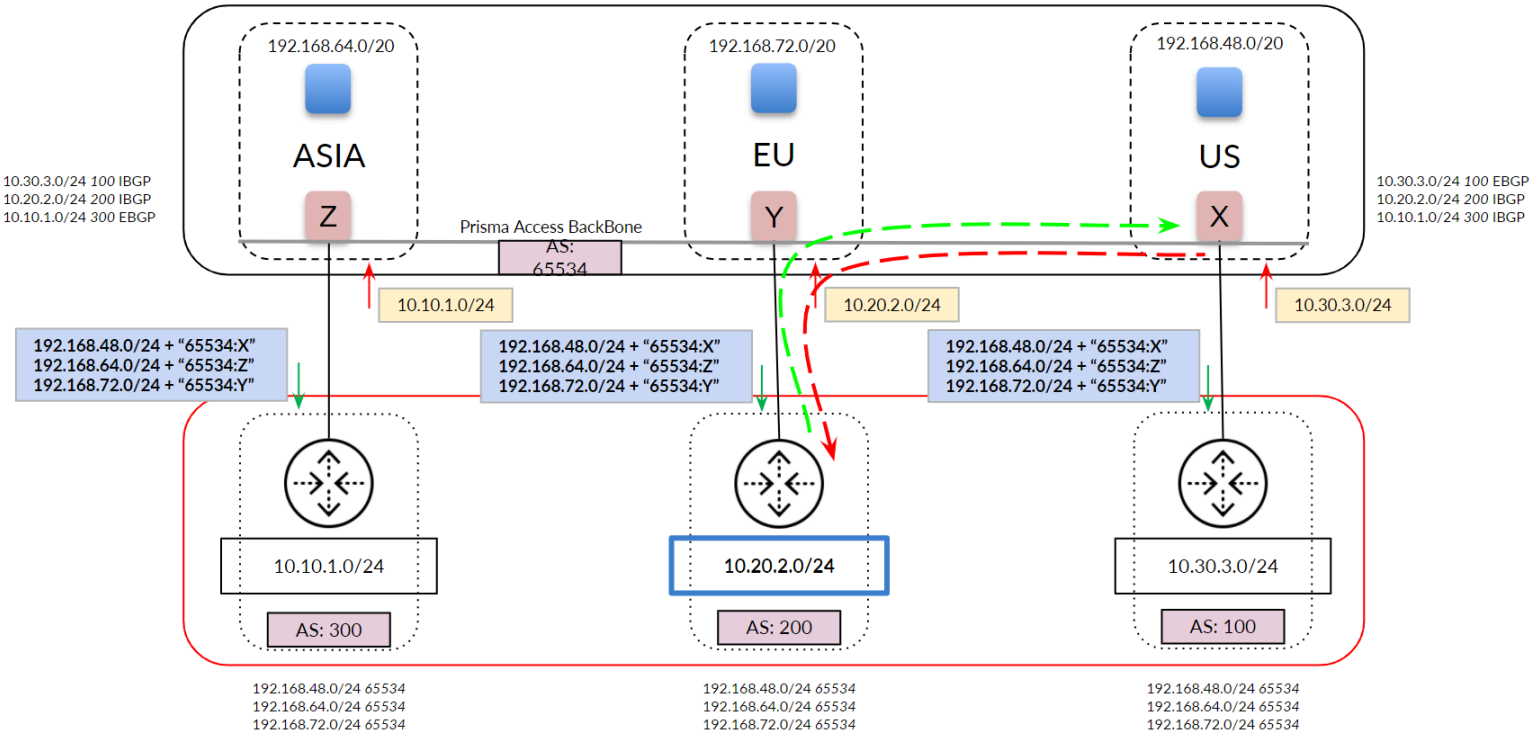
デフォルトのルーティングモードで、Prisma Accessがサービス接続トラフィックをルーティングする例を次の図に示します。組織ネットワークには、3つのデータセンター内に3つの個別のネットワークが存在しており、ネットワークに接続するバックボーンは存在していません。図の下部に示されているように、デフォルトのルーティングモードで、モバイルユーザープールは3つのネットワークに均等にアドバタイズされます。

Prisma Accessがモバイル ユーザー ルートをアドバタイズする場合、その前にアドバタイズすることに注意してください。プレフィックスがゲートウェイによって消費されると、/20 モバイル ユーザー サブネットが /24 のチャンクでアドバタイズされます。

Prisma AccessがBGPルートアドバタイズを使用する仕組みについて書き留めてください:

- Prisma Accessは、モバイルユーザーがアドバタイズしたルートのデフォルトBGP属性を調整しません（Prisma Accessは、ルートアドバタイズにAS番号を追加します）。
- Prisma Accessは、モバイル ユーザー ルートを広告し、サービス接続を通じて広告するルートに BGP コ ミュニティ値を追加します。次の図は、3つのサービス接続と3つの異なるIPアドレス ブロックが指定されたモバイル ユーザーのデプロイメントを示しています。アジア、オーストラリア、日本 地域では`192.168.64.0/20`、 アフリカ、ヨーロッパ、中東 地域では`192.168.72.0/20`、 北米および南米 地域では `192.168.48.0/20` です。 Prisma Accessはこれらのルートを/24のブロックに分割し、 Prisma AccessのAS 番号**65534**で配信しますが、配信にはBGPコミュニティ値も追加されます (アジアの場合は**Z**、EU の場合は **Y**、米国の場合は **X**)。これらのルートは、図の中央に表示されています。このようにすることで、Prisma Accessが同じAS番号を割り当てる場合でも、サービス接続を区別することができます。

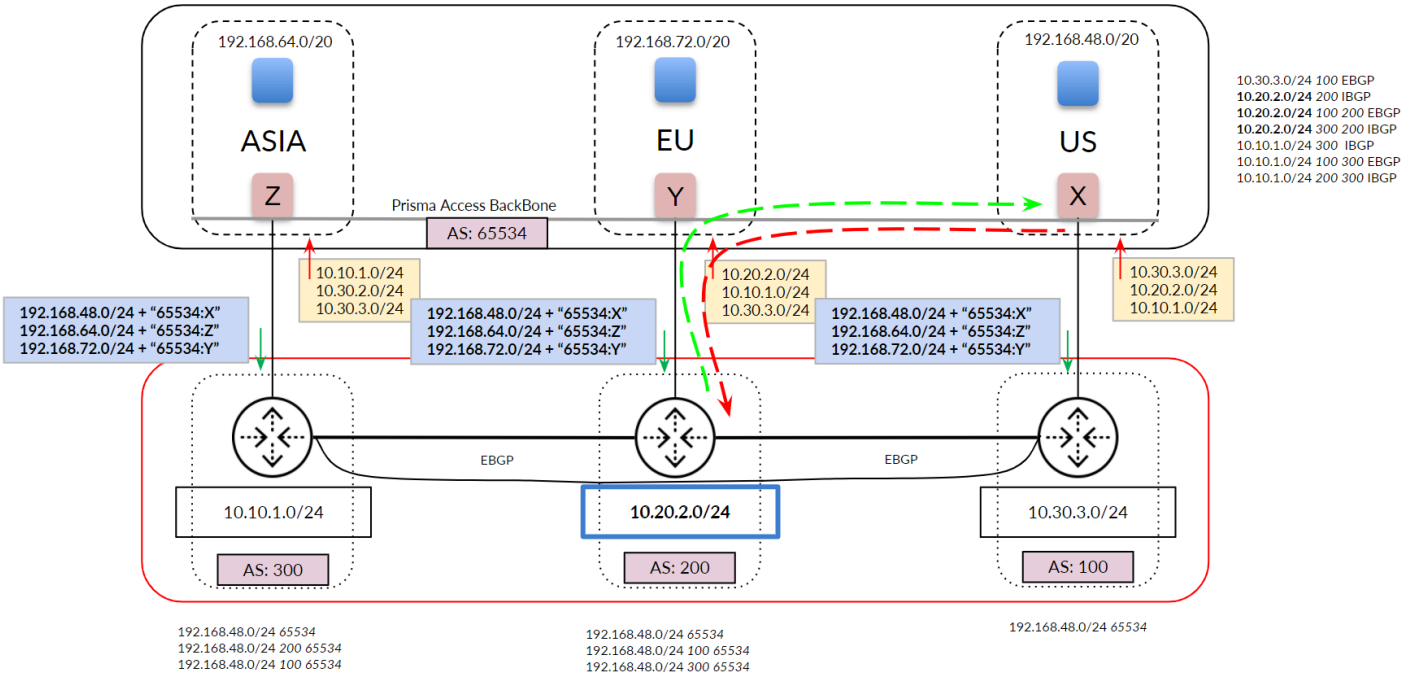
©2025 Palo Alto Networks, Inc.



フルメッシュeBGPバックボーンを持つ、一般的なネットワークを次の図に示します。この図は、Prisma Accessが右上にある組織ネットワークから学習したルートを表しています。Prisma Accessのバックボーン（iBGP）および組織のバックボーン（eBGP）を介してPrisma Accessが学習した、追加のルートに注意してください。

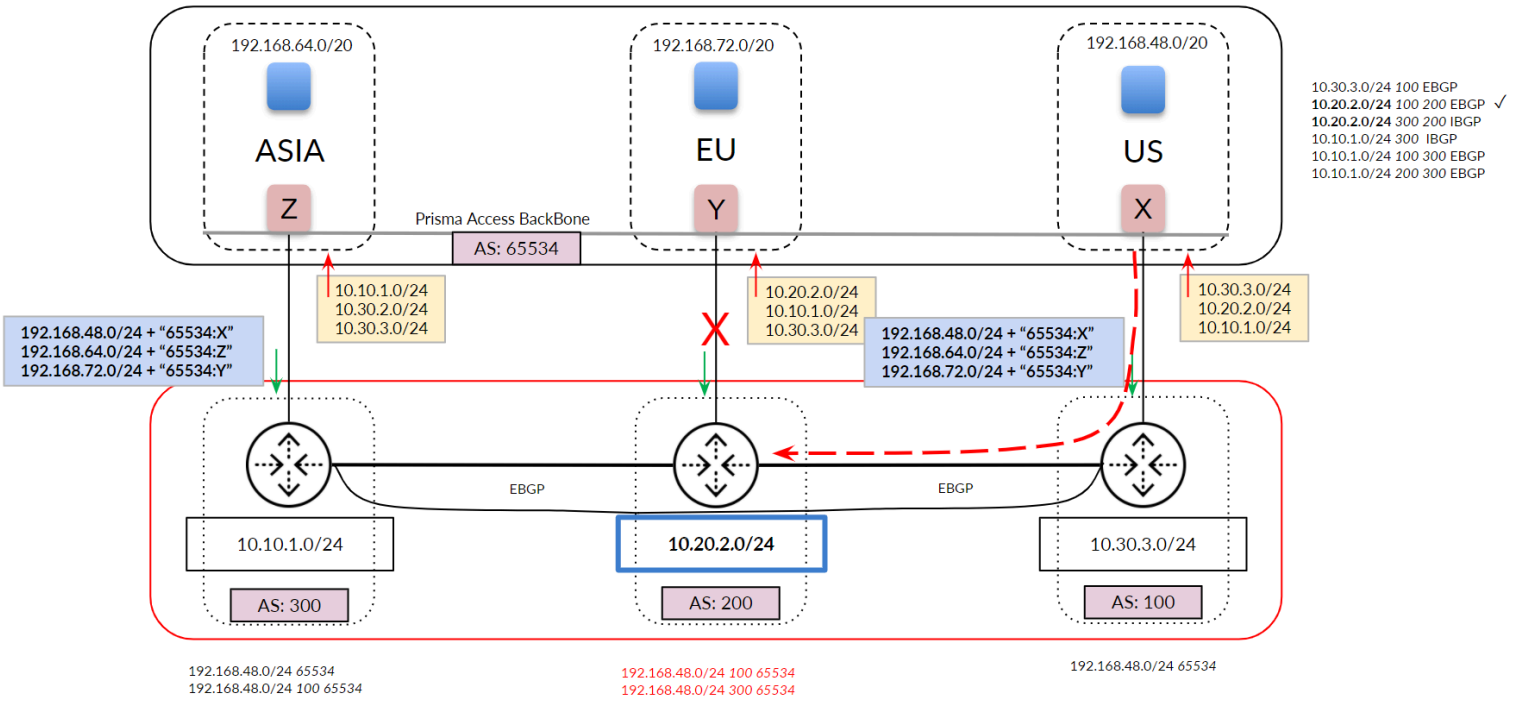
North America & South America（北米と南米）リージョン（図のUS）のモバイルユーザーと組織の**Africa, Europe & Middle East**（アフリカ、欧州、中東）リージョン（図のEU）のデータセンター間のトラフィックに対して、Prisma AccessはAS-PATHが短いルートを優先するため、EUサービス接続経由のパスが選択されます。

©2025 Palo Alto Networks, Inc.



フルメッシュeBGPバックボーンを持つデプロイ環境の場合、顧客のデータセンターのISP/CPE障害により、Prisma Accessが特定のデータセンターに到達できないと、非対称が発生する可能性があります。EUサービス接続へのリンクがダウンした場合に、何が起きるのかを次の図に示します。ネットワークはリンク障害を検出して、AS 200用の新しいルートテーブルを作成します。USサービス接続からAS 200へのトラフィックは、AS 200とAS 100間のバックボーンに対するeBGPルートの方が、サービス接続EUおよびUS間のiBGPルートよりも好ましいため、AS 200はAS 100経由のルートを使用します。ただし、オンプレミスCPEがWriterトラフィックに対してどちらかのパスを選択する可能性があるため（赤で表示）、リターントラフィックで同じパスが使用されることは保証されません。

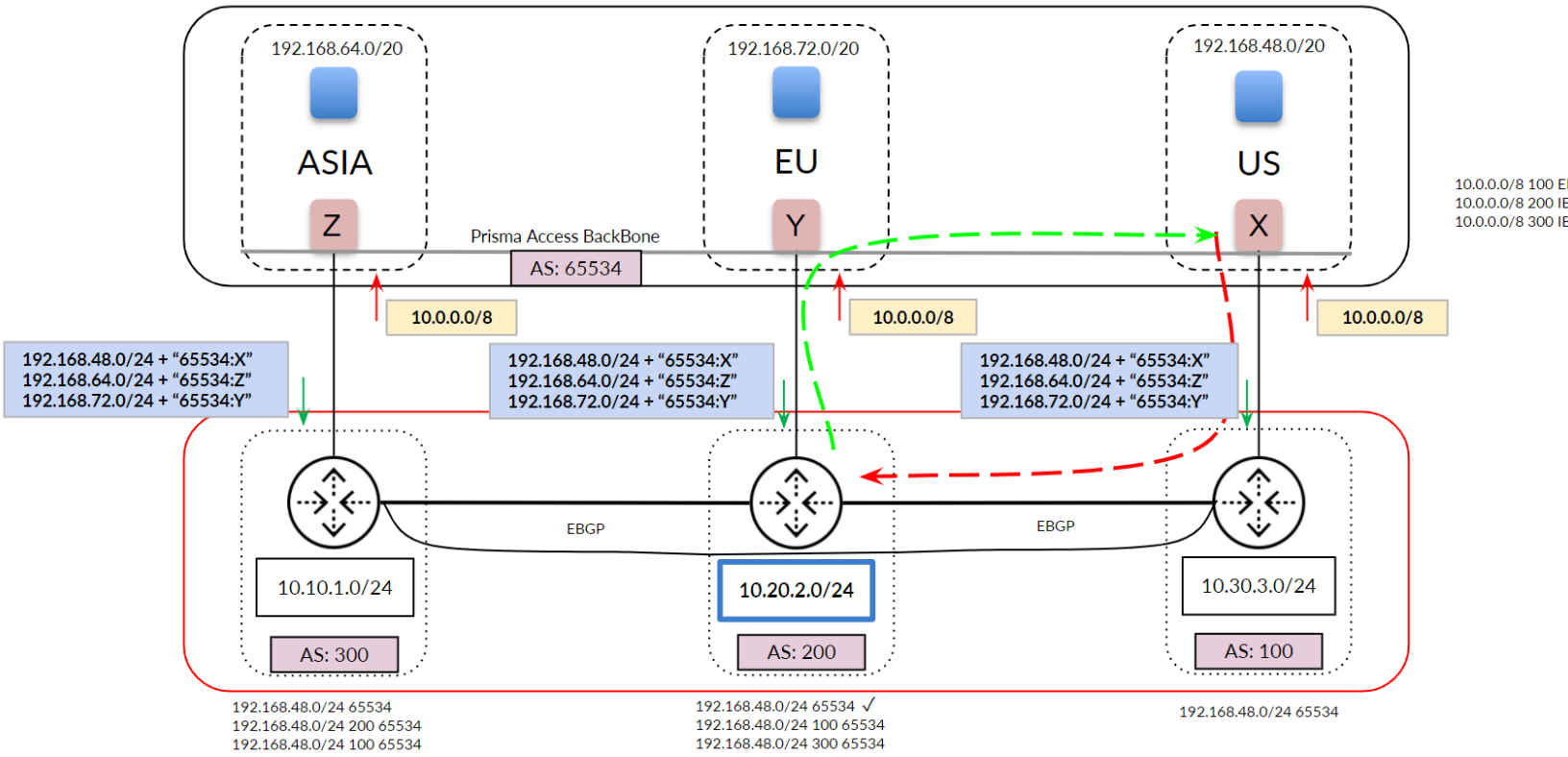
©2025 Palo Alto Networks, Inc.



前の例では、ルートが集約されていないネットワークを表していました（Prisma AccessにBGPルートアドバタイズを送信する前に、ルートの要約を実施していない）。次の例は、ルートをPrisma Accessに送信する前に、10.0.0.0/8で要約するネットワークを表しています。デフォルトのルーティングを選択した場合、Prisma Accessが要約されたルートから正しいリターンパスを判断できないため、この設定では非対称ルーティングの問題が発生する可能性があります。

*Prisma Access*デプロイ環境にリモートネットワークが存在している場合、サービス接続でルート要約を使用することはお勧めできません。サービス接続でのルート要約は、モバイルユーザーデプロイ環境専用です。

©2025 Palo Alto Networks, Inc.



モバイル ユーザー向けにルート集約を使用する場合は、Prisma Accessがトラフィックをできるだけ早く組織のネットワークに渡す、デフォルト ルーティングではなくホット ポテト ルーティングを有効にすることを強くお勧めします。さらに、各サービス接続で決定論的なルーティング動作を実現するには、次のセクションで説明するようにバックアップ **SC**を選択することをお勧めします。

ホットポテトルーティング

Hot Potato Routing（ホットポテトルーティング）を選択すると、Prisma Accessは内部ネットワークからサービス接続/データセンターに向けたトラフィックを、できる限り早く送信します。

ホットポテトルーティングで、Prisma Accessはゲートウェイから送信されるBGPプレフィックスアドバタイズの先頭にASパス（AS-PATH）を追加します。この先頭への追加は、プレフィックスが組織のオンプレミスCPEへのサービス接続からアドバタイズされるときに実行されます。Prisma AccessはAS-PATHを先頭に追加して、CPEがプライマリ トンネルとセカンダリ トンネルに適切な優先順位を与えるようにします。これにより、プライマリ トンネルがダウンした場合に、CPEがセカンダリ トンネルをバックアップとして選択できるようになります。

セカンダリ（バックアップ）BGPピアに対して異なるIPアドレスを指定した場合、次の表に示すようにトンネルのタイプに基づいて、より多くの付加が行われます。

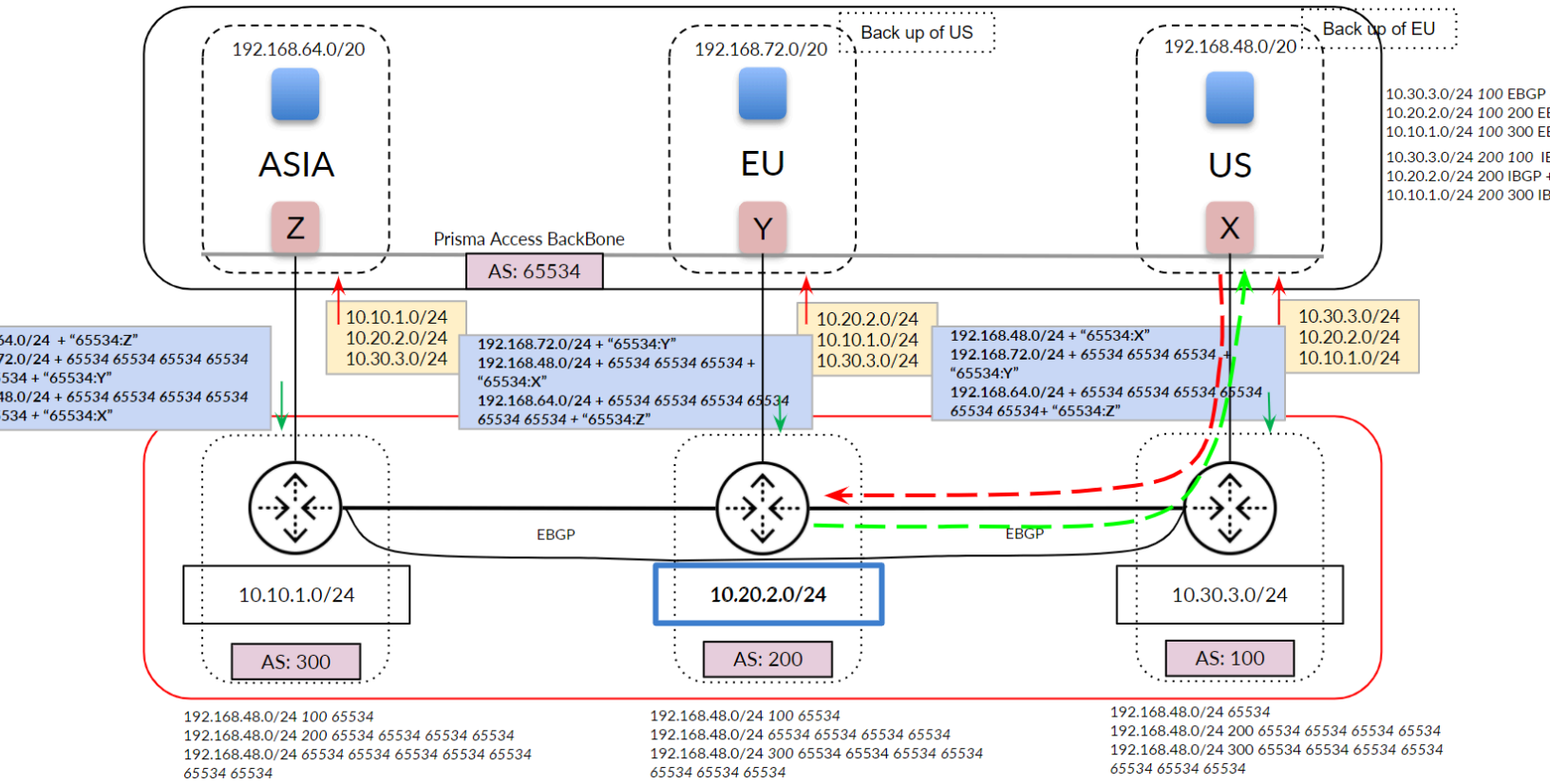
©2025 Palo Alto Networks, Inc.

プレフィックスタイプ	サービス接続トンネルタイプ	AS-PATH付加数	CPEで見られるAS-PATH合計
プライマリサービス接続からのゲートウェイプレフィックス	同じBGPピアIPアドレスを持つプライマリまたはセカンダリトンネル	0	1
バックアップサービス接続からのゲートウェイプレフィックス	同じBGPピアIPアドレスを持つプライマリまたはセカンダリトンネル	3	4
その他のすべてのサービス接続からのゲートウェイプレフィックス	同じBGPピアIPアドレスを持つプライマリまたはセカンダリトンネル	6	7
プライマリサービス接続からのゲートウェイプレフィックス	異なるBGPピアIPアドレスを持つセカンダリトンネル	1	2
バックアップサービス接続からのゲートウェイプレフィックス	異なるBGPピアIPアドレスを持つセカンダリトンネル	4	5
その他のすべてのサービス接続からのゲートウェイプレフィックス	異なるBGPピアIPアドレスを持つセカンダリトンネル	7	8

バックアップ サービス接続を指定し、サービス接続リンクに障害が発生したときにPrisma Accessがそのサービス接続をバックアップとして使用するようにします。

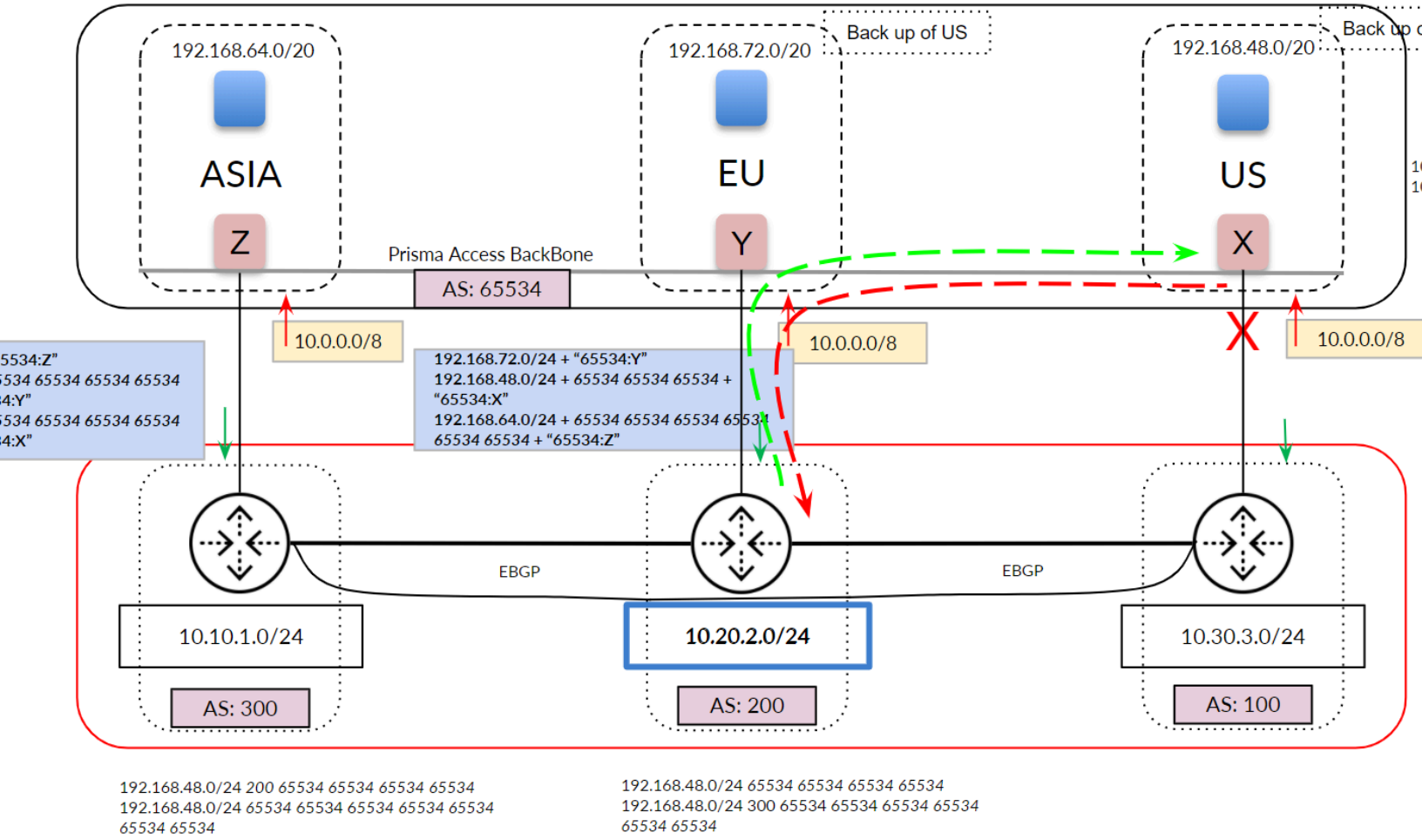
USサービス接続とAS 200間のホットポテトルーティング設定を次の図に示します。ここで、EUサービス接続はUS接続の**Backup Service Connection (**バックアップ サービス接続**)**として設定されています。Prisma Accessはホットポテトルーティングを使用して、USサービス接続経由でトラフィックをもっとも近い出口パスから送信します。戻りトラフィックはAS100を通る同じパスをたどります。これは、このパスの方が米国のモバイル ユーザー プールへのAS-PATHが短いためです。 Prisma Accessは、 トンネルがプライマリ トンネルであるか、バックアップ トンネルであるか、あるいはプライマリにもバックアップにも使用されていないかに応じて、プレフィックス アドバタイズメントの先頭にAS-PATHを追加します。

©2025 Palo Alto Networks, Inc.



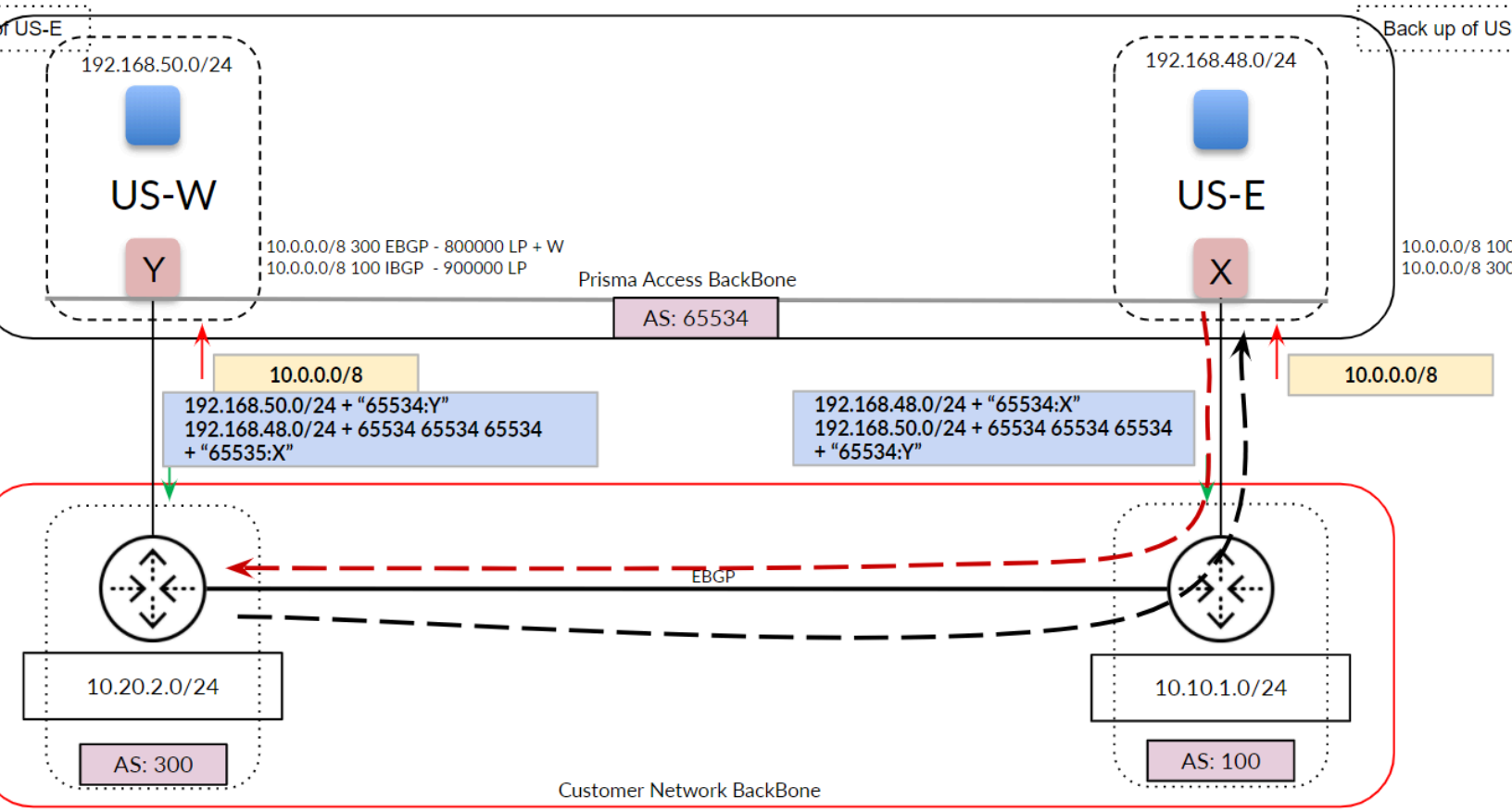
バックアップサービス接続を設定しているため、USサービス接続へのリンクがダウンした場合、ホットポテトルーティングは、EUサービス接続経由のもっとも短いルートを使ってトラフィックを送信します。このルーティングの例は、ルート集約を使用しているネットワークにも適用されます。

 ©2025 Palo Alto Networks, Inc.



単一のリージョン内の複数のサービス接続に対して、バックアップサービス接続を使用することも可能です。North America（北米）リージョンに2つのサービス接続を持つ、Prisma Accessデプロイメント環境を次の図に示します。この場合、対称ルーティングを確実にするために、US-Wサービス接続にUS-Eのバックアップ サービス接続を指定し、その逆も同様にします。

©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

Prisma Access ZTNAコネクタ

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ ZTNA コネクタ アドオン ライセンス アドオン ライセンスを含む Essential ライセンスには、8つのZTNAコネクタ、100個のFQDN、および4つのIPサブネット機能が含まれます。 アドオン ライセンスを含む Advanced ライセンスには、40個の ZTNA コネクタ、300個のFQDN、および 1024 個のIPサブネット機能が含まれます。 アドオン ライセンスを含むプレミアム ライセンスには、200個のZTNAコネクタ、4000個のFQDN、および1024個のIPサブネット機能が含まれます。 ❑ ZTNAコネクタアドオンライセンスを購入しない場合は、 Prisma Accessライセンスには、4 つのコネクタ、40 個の FQDN、および 4 つの IP サブネットが含まれます。この機能は、ご使用の環境で ZTNA コネクタを試す目的で提供されています。

Zero Trust Network Access（ZTNA）コネクタを使用すると、Prisma Accessを組織のプライベート・アプリに簡単かつ安全に接続できます。ZTNA コネクタは、自動化されたセキュア トンネルを使用して、モバイル ユーザーとブランチ ロケーションのユーザーにプライベート アプリへのアクセスを提供します。ZTNA コネクタはトンネルを自動的に設定するため、プライベート アプリが配置されているデータ センターや本社、パブリック クラウドの場所、パートナー ネットワークへの IPSec トンネルやルーティングを手動で設定する必要はありません。

デプロイしたZTNAコネクタVMは、最も近いPrisma Accessロケーションを特定することで、可能な限り最適なレイテンシが保証されるほか、帯域幅アクセスをコネクタあたり最大 2 Gbps、コネクタ グループあたり最大 8 Gbps まで拡張できます。

デフォルトではPrisma Accessはすべてのアクセスを拒否するので、管理者は特許取得済みのユーザー ID、アプリ ID、デバイス ID 構造に基づくポリシー ルールを使用してリソースへのアクセスを明示的に許可する必要があります。これにより、攻撃対象領域とセキュリティ リスクを軽減できます。接続が許可されると、当社はその接続の信頼性を継続的に検証し、セキュリティの脅威を継続的に検査し、データ漏洩を継続的に検査します。さらに、Prisma AccessZTNA Connectorを使用すると、アプリケーションのプライベートIPアドレスは公開されません。

ZTNA コネクタ コンポーネント

- コネクター–コネクタとはPrisma Accessへのトンネルを構築する仮想マシンのことを指します。ZTNAコネクタは、IPSec および IKE 設定を指定する必要なくトンネル管理を自動化します。コネクタは、クラウド サービス (Amazon Web Services (AWS)、Google Cloud Platform (GCP)、Microsoft Azure)、仮想サーバー (VMware ESXi)、またはカーネルベースの仮想マシン (KVM) にオンボードした VM にオンボードします。Palo Alto Networks では、Prisma Access にオンボードされたアプリケーションと同じサブネットに VM をデプロイメント開することをお勧めします。コネクタからアプリケーションへのルートがある限り、別のサブネットを提供することもできます。

  コネクタVMをデプロイした後、 Prisma AccessはVM のバージョンをアップグレードするオプションの提供など、VM を管理します。ZTNA Connector VMをインストールすると、最も近いPrisma Accessロケーションを検出し、Prisma Accessへの安全なIPSecトンネルを開始します。

- コネクタ グループ– コネクタ グループは、コネクタとアプリの論理的なグループです。コネクタ グループに複数のコネクタを追加することで、グループ内のアプリにトンネルの冗長性と帯域幅の増加が提供されます。各コネクタ グループは最大 の4つのコネクタをサポートします。

  異なるコネクタを使用して特定のアプリへのアクセスを提供する場合は、コネクタを別々のグループに配置します。

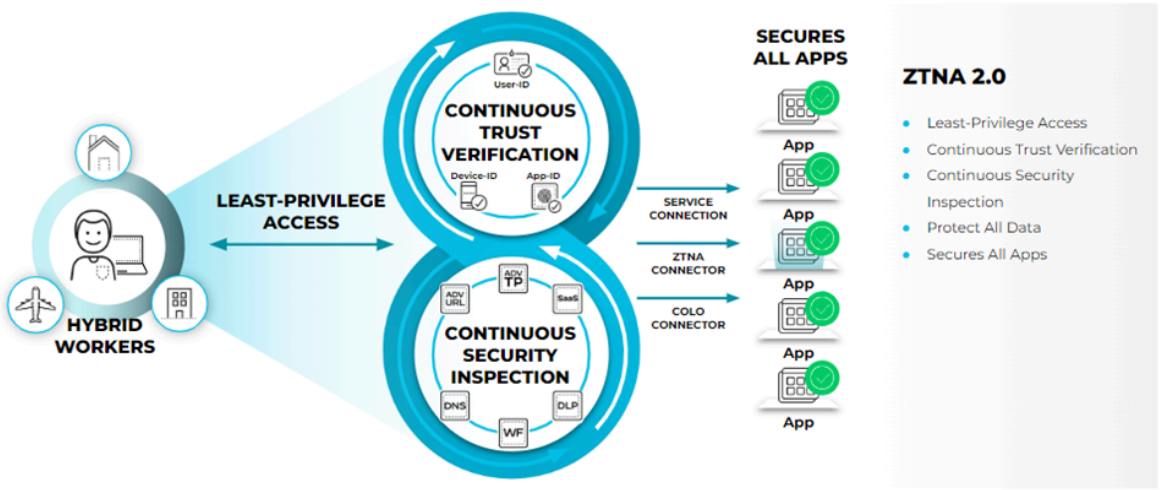
- ターゲット- ZTNA コネクタが Prisma Access にオンボードするプライベート アプリ。FQDN (**FQDN** ターゲット)、ワイルドカード (ワイルドカード ターゲット)、 またはアプリが配置されている IP アドレスやサブネットを使用して、アクセスを提供する特定のアプリを定義できます。または、CIE に接続された IdP からアプリを取得して、ZTNA コネクタでアプリを自動的に検出することもできます。

©2025 Palo Alto Networks, Inc.

ZTNAコネクタの使用例

次のシナリオで ZTNA コネクタを使用します。

- プライベート アプリへの接続- プライベート アプリに接続するすべてのクライアント開始トラフィックに ZTNA コネクタを使用します。



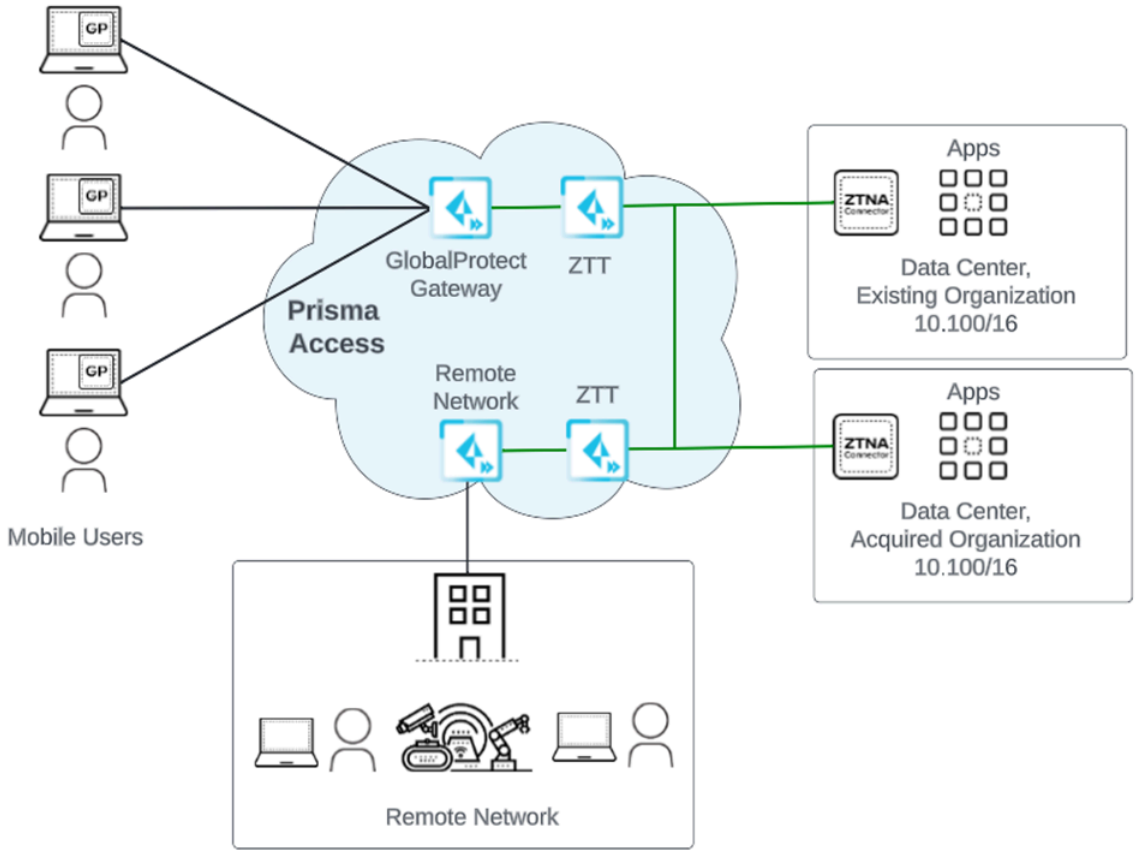
- 重複したプライベート ネットワーク- 別の組織を買収または合併した大企業のネットワーク管理者の場合、2 つのネットワークが重複するアドレス範囲 (たとえば、RFC 1918 プライベート ネットワーク アドレス空間) を使用している可能性があります。重複したネットワークでホストされているアプリへのアクセスをユーザーに提供するには、ルーティングと NAT の構成が面倒になる可能性があります。ZTNA コネクタを使用すると、IP ルーティングを構成することなく、FQDN、FQDN ワイルドカード、IP サブネットを使用してアプリに接続できるため、重複したネットワークでのアプリ アクセスが簡素化されます。

  ZTNA コネクタは、ZTNA コネクタ トンネル ターミネータ (ZTT) を使用して、ユーザーにプライベート アプリへの安全なアクセスを提供します。

  コンピューティング リージョンで ZTNA コネクタをアクティブ化すると、ZTT ノードが自動的にオンボードされます。ZTNA コネクタは、ZTT を使用して IPSec トンネルを自動的に形成します。リージョン内のすべてのコネクタが削除された後も、リージョン内の ZTT ノードは 24 時間アクティブなままになります。同じリージョン内のすべてのコネクタが削除されて

©2025 Palo Alto Networks, Inc.

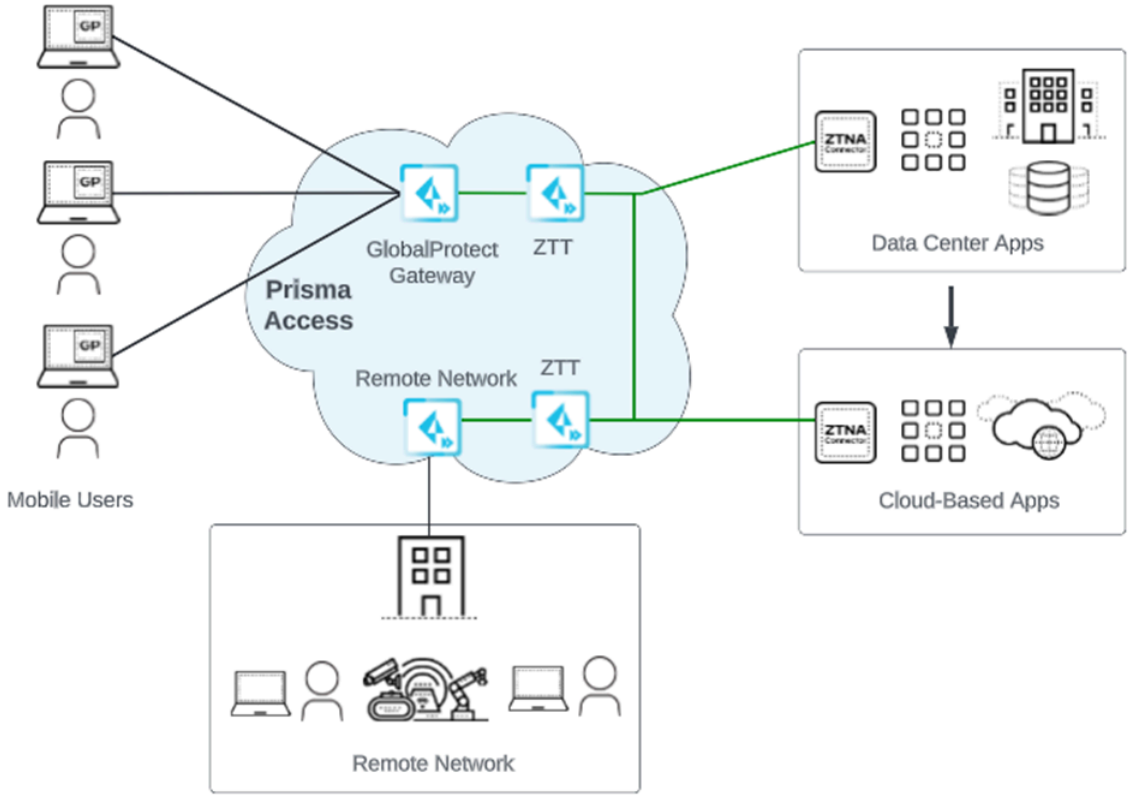
から 24 時間以内に新しいコネクタがデプロイされると、既存の ZTT が再利用されます。24 時間後に新しい ZTNA コネクタがアクティブ化されると、新しい ZTT が作成されます。



- データ センターからクラウドへの移行- 組織がオンプレミスのアプリをクラウドに移行する場合 (「リフト アンド シフト」を使用して既存のオンプレミス アプリケーションを移行するか、クラウド ネイティブ アプリを開発するかのいずれか)、AWS、GCP、Azure、またはその他のクラウド プロバイダーのクラウド VPC でアプリをホストできます。数百または数千の

 ©2025 Palo Alto Networks, Inc.

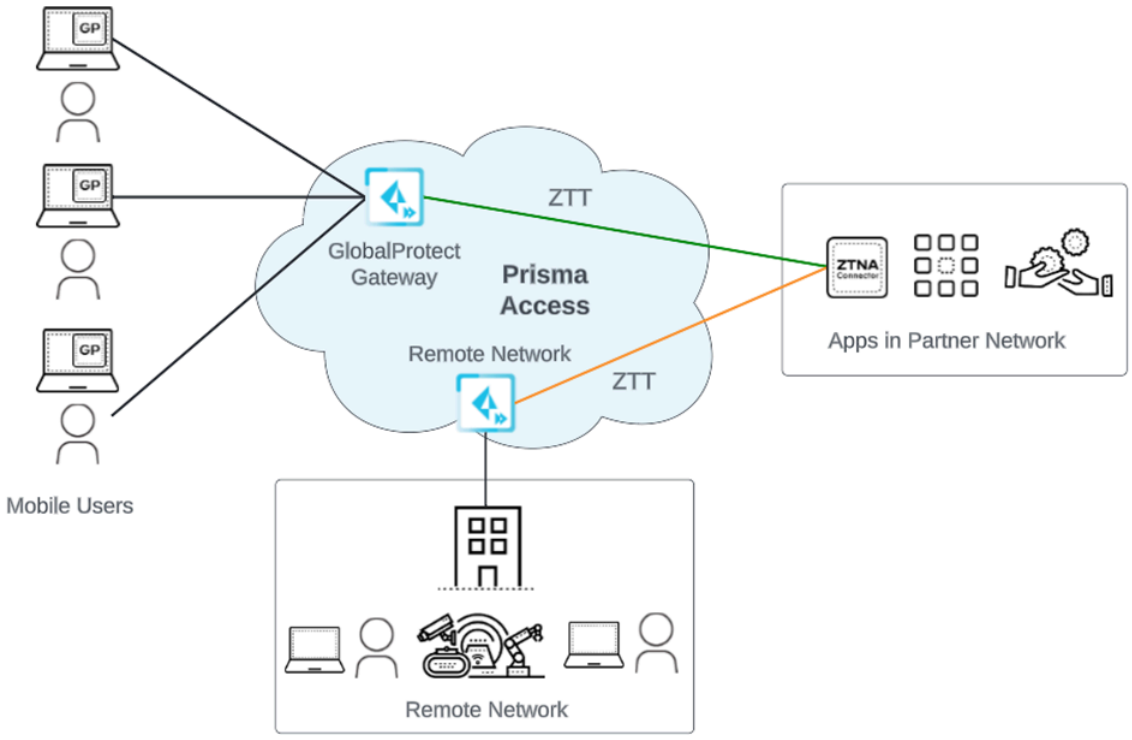
VPC がある場合、ZTNA コネクタを使用すると、クラウド配信のアプリ アクセスを提供するプロセスを加速できます。



- ビジネス パートナー ネットワーク内のアプリケーションへのアクセス- 一部の組織は、ビジネス パートナーのネットワークでホストされているアプリケーションにアクセスします。サービス接続を使用してこれらのアプリを接続するには、手動ルーティングと NAT 構成が必

 ©2025 Palo Alto Networks, Inc.

要です。ZTNA コネクタを使用すると、手動で IP ルーティング構成を実行せずにこれらのアプリに接続できます。



©2025 Palo Alto Networks, Inc.

サービス接続と ZTNA コネクタでサポートされているユースケース

ZTNA コネクタはサービス接続の代替ではありません。サービス接続を補完したり共存したりできるため、プライベート アプリを柔軟に保護できます。すでにサービス接続をデプロイしている場合は、別のアプリケーション アクセス モデルに移行する場合を除き、引き続き使用できます。次の表は、サービス接続または ZTNA コネクタのサポート対象およびサポート対象外のユースケースを示しています。チェックマークはユースケースがサポートされていることを示し、ダッシュ (–) はサポートされていないことを示します。

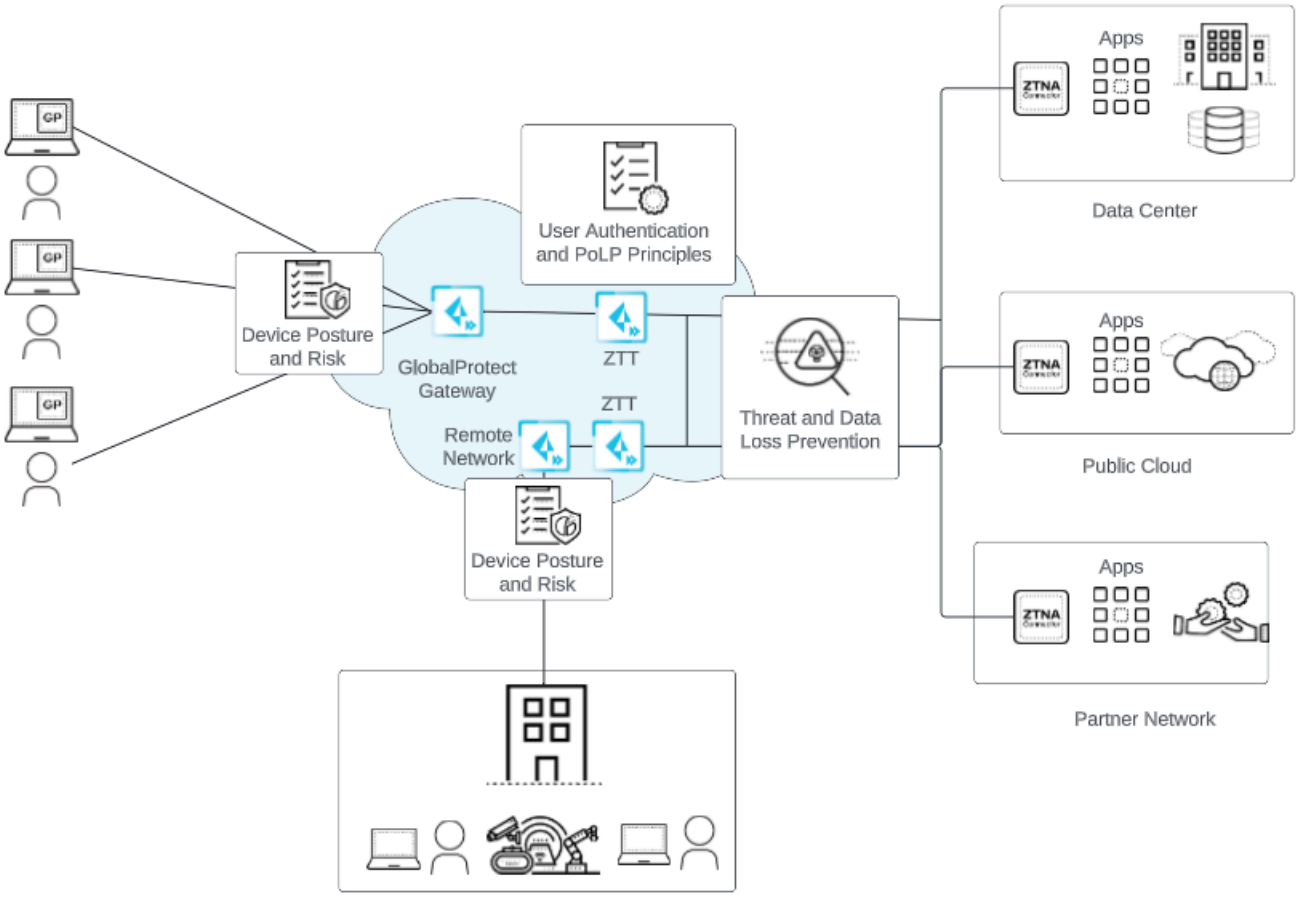
ユース ケース	ZTNA コネクタのサポート	サービス接続/サイト
重複ネットワーク内のアプリケーションへのアクセス	√	–
クライアントが開始したアプリケーション トラフィックのすべてのポートとプロトコルへのアクセス	√	√
Prisma Accessへの自動トンネル確立	√	–
自動Prisma Accessロケーション検出	√	–
最大10Gbpsのスループットを実現するPrisma Accessロケーションの自動スケーリング	√	–
IP アドレスとサブネットを使用したプライベート アプリへのアクセス	√	√
管理対象デバイス (GlobalProtect モバイル ユーザーまたはリモート ネットワーク) に到達するサーバー開始トラフィック (リモート ヘルプ デスクなど)。	–	√
固有のクライアント IP アドレスを必要とするアプリケーションまたはサービス	√	√
動的ポートを使用したアプリケーションへのアクセス（FTP アクティブ モードや VoIP など）	–	√
ユーザーIDに基づくポリシールールが適用されるオンプレミスの次世代ファイアウォールを使用したハイブリッドデプロイメント	√	√

©2025 Palo Alto Networks, Inc.

ZTNA コネクタ 2.0 の原則

ZTNA Connectorは、以下のZTNA Connector 2.0の原則を使用して、プライベートアプリをPrisma Accessに接続することができます：

- デバイスのポスチャとリスク- Prisma Access のユーザー ID に基づくポリシー ルールを使用して、ユーザーとデバイス (モバイル ユーザーと IoT デバイスの両方) のポスチャを定義し、プライベート アプリへの不正アクセスを防ぐことができます。ZTNA Connector とPrisma Accessの間で共通のポリシー・ルールを作成することもできます。
- ユーザー認証と最小権限アクセス- ユーザーまたはグループに基づくユーザー認証とポリシー ルールを使用して、最小権限の原則 (PoLP) を実装し、ユーザーに必要なアプリへのアクセスを提供しながら、必要のないアプリへのアクセスをブロックできます。
- 脅威とデータ損失の防止—Prisma AccessZTNA コネクタは、高度な脅威防止、高度な URL フィルタリング、SaaS セキュリティ、高度な WildFire、エンタープライズ DLP などの高度なセキュリティ機能を使用して、プライベート アプリとアプリ データのセキュリティを確保します。



©2025 Palo Alto Networks, Inc.

ZTNA コネクタの要件とガイドライン

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ ZTNA コネクタ アドオン ライセンス アドオン ライセンスを含む Essential ライセンスには、8つのZTNAコネクタ、100個のFQDN、および4つのIPサブネット機能が含まれます。 アドオン ライセンスを含む Advanced ライセンスには、40個の ZTNA コネクタ、300個のFQDN、および 1024 個のIPサブネット機能が含まれます。 アドオン ライセンスを含むプレミアム ライセンスには、200個のZTNAコネクタ、4000個のFQDN、および1024個のIPサブネット機能が含まれます。 ❑ ZTNAコネクタアドオンライセンスを購入しない場合は、 Prisma Accessライセンスには、4 つのコネクタ、40 個の FQDN、および 4 つの IP サブネットが含まれます。この機能は、ご使用の環境で ZTNA コネクタを試す目的で提供されています。

ZTNA コネクタを構成する前に、コネクタの要件と制限、およびデプロイメント時に従う必要があるガイドラインを理解していることを確認してください。

サポートされているPrisma Accessバージョンと要件

- Prisma Access 互換性のある SaaS エージェントを備えた 4.0 バージョン。

  Innovationリリースを含む、4.0 より前の Prisma Access リリースを、最小バージョン 4.0 にアップグレードします。

  FQDNワイルドカードやIPサブネットを使用してアプリにアクセスする場合は、Prisma Accessバージョン5.0以上が必要です。加えて、 Prisma Access5.0 では、ダンプ概要、パケット キャプチャ、およびテクニカル サポート 診断ツールの使用が可能になります。
- 5.0 の機能を使用するには、 コネクタのバージョンを少なくとも 6-2-2-ztna-connector-b1 にアップグレードする 必要があります。
- Prisma Access (Managed by Panorama)の場合、クラウド サービス プラグインのバージョンを最低バージョン 4.0 にアップグレードします。最新の機能を利用するには、最新のクラウド サービス プラグインにアップグレードしてください。

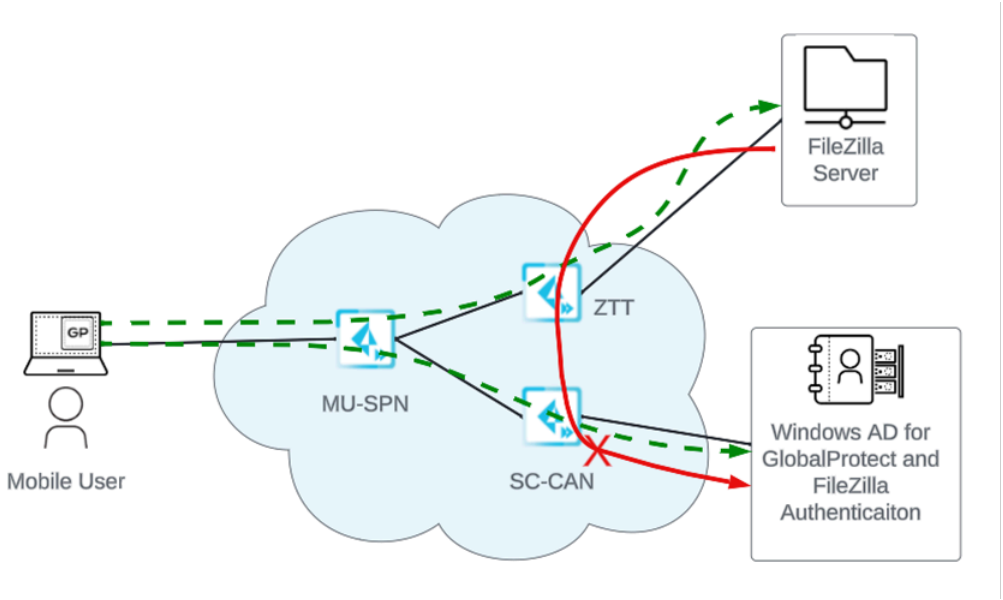
©2025 Palo Alto Networks, Inc.

アプリサポート

ZTNA コネクタは、次の例外を除き、すべてのプライベート アプリ トラフィックへのアクセスを提供します。

- ZTNA コネクタは以下をサポートしていません。
  - データ センターから発信されるトラフィック (SCCM やリモート ヘルプ デスクのトラフィックなど)。
  - ユーザーIDの再配信。
  - ポート ホッピングを実行するアプリケーション (VoIP やアクティブ モード FTP など)。
  - アクティブ モード FTP や SIP などのアプリケーション レベル ゲートウェイ (ALG) アプリ。
  - アプリケーションの Windows 統合認証 (NTLM や Kerberos など) は、データ センターのドメイン コントローラーとリソースを IPアドレス サブネットとしてオンボードする場合にのみサポートされます。SAML、OAuth、LDAP がサポートされています。
  - サービス接続の背後にあるアプリと ZTNA コネクタの背後にあるアプリ間の通信。

    たとえば、サービス接続の背後で Windows Active Directory (AD) サーバーをホストし (AD サーバーは ZTNA コネクタの背後ではサポートされていないため)、ZTNA コネクタの背後で FTP (Filezilla) サーバーをホストします。FTPサーバーがWindows ADサーバーに対する認証を必要とする場合、認証に失敗する。これは、サービス接続企業アクセス ノード（SC-CAN）とZTNAコネクタ トンネル ターミネータ（ZTT）の間のバックボーンとしてPrisma Accessを使用できないためです。



機能の制限

ZTNAコネクタのデプロイメントをセットアップおよび構成するときは、次の制限に注意してください。

©2025 Palo Alto Networks, Inc.

- 特殊文字は使用しないでください。 ZTNA オブジェクト名に、< >! @ # $ % ^ & および中国語、日本語、韓国語の文字を使用しないでください。
- 次の機能は、デフォルトの Prisma Access デプロイメントではサポートされていません。これらを有効にするには、Palo Alto Networks チームに問い合わせてください。
  - ZTNAコネクタを使用したPrisma AccessAAインフラストラクチャIPアドレスのRFC 6598アドレスの使用
- コネクタ グループのガイドライン- コネクタ グループを追加するときは、次の推奨事項に従います。
  - 単一のコネクタ グループ内のすべてのアプリは、DNS 解決に同じ DNS サーバーを使用する必要があります。
  - データ センターまたは本社からアプリにアクセスする場合、コネクタ グループ内のすべてのアプリは同じデータ センターまたは本社からのものである必要があります。
  - 1 つのコネクタ グループ内の 2 つ以上のリージョンにコネクタを追加しないでください。コネクタ グループ内のすべてのコネクタは同じリージョンに存在する必要があります。
  - Prisma Access 5.01 以降では、FQDN ターゲットまたはワイルドカード ターゲットごとに最大 4 つのコネクタ グループを指定できます (リリース 5.0 以前では、FQDN ターゲットまたはワイルドカード ターゲットごとに 1 つのコネクタ グループがサポートされていました)。FQDN ターゲットまたはワイルドカード ターゲットごとにコネクタ グループを割り当てる場合は、リージョンごとに 4 つ以上のコネクタに同じアプリを割り当てないようにしてください。

    たとえば、同じアプリ (FQDN ターゲットまたはワイルドカード ターゲットのいずれか) を 4 つのコネクタ グループに割り当て、各グループに 1 つのコネクタがあり、すべてのコネクタが同じリージョンにあるとします。1 つのリージョンでアプリごとに 4 つ以上のコネクタを割り当てていないため、この構成は許容されます。

    ただし、同じアプリ (FQDN ターゲットまたはワイルドカード ターゲットのいずれか) を 3 つのコネクタ グループに割り当て、各グループに 2 つのコネクタがあり、すべてのコネクタが同じリージョンにある場合、1 つのリージョンで同じアプリに 6 つのコネクタを割り当てることになるため、これは無効な構成になります。
- AWS ベースのコネクタやAzure ベースのコネクタなどの一部の ZTNA コネクタは自動スケーリングをサポートしています。自動スケーリングでは、AWS または Azure がコネクタ上のネットワーク帯域幅の使用状況を監視し、容量を自動的に調整してアプリのパフォーマンスを維持します。コネクタのネットワーク帯域幅の使用率が低下すると、AWS または Azure は自動スケールインをトリガーします。ZTNA コネクタでスケールインが発生すると、スケールイン対象としてマークされた ZTNA コネクタによって処理される既存の長期セッションは途中で終了します。この動作は、スケールイン後に開始された新しいトラフィック セッションには影響しません。SSH や RDP などの長時間セッションの場合、ZTNA コネクタはスケールイン中にセッションを終了するため、そのセッションに再接続する必要があります。

スケールとスループットの考慮

ZTNA コネクタは次の最大値をサポートします。

- すべてのコネクタ グループにわたるテナントあたり 4,096 個のアプリケーション

 ©2025 Palo Alto Networks, Inc.

- テナントあたり 200 個のコネクタ
- コネクタ グループあたり 512 個のアプリケーション
- コネクタグループあたり 4 つのコネクタ
- コネクタあたり 200,000 同時セッション

  各コネクタは *200,000* の同時接続をサポートできます。コネクタ グループには最大 *4* つのコネクタを含めることができ、コネクタ グループごとに最大 *800,000* の同時接続が可能です。
- 26 のコンピューティング領域
- コネクタあたり1Gbpsのスループット、Prisma Accessコンピュート ロケーションあたり最大10Gbps

サポートされているアプリケーションホスティング環境

指定された最小要件を満たす次のデータセンター環境に ZTNA コネクタ VM をデプロイできます。

クラウド プロバイダ	インスタンスサイズ	CPUサイズ	メモリー容量	ディスクサイズ
Amazon AWS	リージョンごとの m5.xlarge	4 vCPUs	16 GB	40 GB
Google Cloud Platform（GCP）	リージョンごとのn2-standard-4	4 vCPUs	16 GB	40 GB
Microsoft Azure	リージョンごとのStandard_D4_v3	4 vCPUs	16 GB	40 GB
KVM	qcowイメージを使用	4 vCPUs	16 GB	40 GB
Hyper-V	VHDイメージを使用	4 vCPUs	VM あたり 8 GB のメモリ	40 GB
VMware ESXi	OVAイメージを使用vSphere上および直接的なESXi ホスト上でのサポート	VM あたり 4 つの vCPU	VM あたり 8 GB のメモリ	40 GB ディスク (シック プロビジョニング)

VMware ESXi の場合、コネクタ VM では vMotion、VM スナップショット、または移行はサポートされません。

KVM の場合、ライブ マイグレーションとスナップショットはコネクタ VM ではサポートされません。

©2025 Palo Alto Networks, Inc.

VM をホストし、インターネットに接続できることを確認するのはお客様の責任です。

AWS、GCP、Azure には、それぞれのマーケットプレイスで入手できる ZTNA コネクタがあります。VMware ESXi Open Virtualization Application (OVA) ファイルと KVM qcow ファイルは、Palo Alto カスタマー サポート ポータルからダウンロードできます。

ネットワーク要件

以下のネットワーク要件により、ZTNAコネクタとの接続が可能になります。 Prisma Access:

- ZTNAコネクタを有効にした後 Prisma Accessリモート ネットワーク と モバイル ユーザー用に設定された DNS ルール (GlobalProtect) を使用して、DNS 要求の DNS プロキシを設定します 。
- ヘッダーを含む UDP ペイロード サイズは、ZTNA アプリケーション サーバーへのパス上の MTU サイズ 1,300 バイトを超えてはなりません。Palo Alto Networks では、パケットをこの MTU サイズ以下に維持することを推奨しています。
- ZTNA トンネル ターミネータ (ZTT) への IPSec および IKE 接続用に、WAN インターフェイス (ポート 1) IPアドレスからのアウトバウンドUDP ポート 4500 および UDP 500 を許可します。アウトバウンドUDP ポート 500 および 4500 接続の有効化を単一の IPアドレスに制限する場合は、ZTNA コネクタの **PA** サービス **IP** アドレス ([ワークフロー] > **[ZTNA** コネクタ] > [コネクタ]) に対して有効にします。



- ZTNA コネクタがインターネット インターフェイスにパブリック IPアドレスを使用する場合は、IP/50 カプセル化セキュリティ ペイロード (ESP) を許可する必要があります。
- WAN インターフェイス (ポート 1) IPアドレスから ZTNA コネクタ コントローラへのアウトバウンドTCP ポート 443 の HTTPS 接続を許可します。
- ZTNA コネクタは、IPSec トンネルの Prisma Access ZTT 側と ZTNA コネクタ側の両方を自動構成します。IKE と ESP の両方の DH グループ/暗号化/ハッシュに設定されているアルゴリズムは、ecp384/aes256/sha512 です。
- ZTNA コネクタが作成し、プライベート アプリにアクセスするために使用する IPSec トンネルを終了しないでください。
- (モバイル ユーザー - GlobalProtectデプロイメントのみ) ZTNA Connector でアプリケーションを初めてオンボードするときは、モバイル ユーザーが更新された DNS サーバー構成を受信できるように、GlobalProtectアプリケーションを更新する必要があります。ZTNA コネクタからアプリケーションを削除した場合は、モバイル ユーザーが更新された DNS サーバー構成を受信できるように、GlobalProtectアプリケーションを更新する必要があります。
- ZTNA コネクタとプライベート アプリの間にファイアウォールがある場合は、ファイアウォールで ZTNA コネクタからアプリへのアクセスを許可する必要があります (つまり、プラ

 ©2025 Palo Alto Networks, Inc.

イベート アプリのアプリ サーバーの解決済み IPアドレス、プロトコル、およびポートへのアクセスを許可する必要があります)。

さらに、アプリケーション ターゲットのヘルス プローブ用に構成したプロトコル (TCP または ICMP) をアプリに許可する必要があります。コネクタ アプリケーションは、アプリケーション サーバーをプローブして、アプリケーションへのアクセスを提供できるかどうかを判断します。 アプリケーション ターゲットのプローブ タイプ を **tcp ping**、**icmp ping**、または **none**(プローブなし) に設定できます。**tcp ping** を指定する場合、ファイアウォールはアプリへの TCP アクセスを許可する必要があります。icmp**ping** を指定する場合、ファイアウォールはアプリの ICMP エコー要求と応答を許可する必要があります。

- ping および traceroute 診断ツールを使用する前に、データ センターで ICMP が許可されていることを確認してください。一部のクラウド環境では、セキュリティ上の懸念から ICMP が許可されていません。この場合、これらのツールはアクティビティを表示しません。traceroute

  診断ツールはランダムな UDP ポートも使用するため、traceroute ツールが機能するには、すべての UDP および ICMP エラー応答を許可する必要があります。

- ZTNA コネクタがアプリの FQDN を解決できるようにローカル インターフェイスで DNS エントリが設定されていること、および ZTNA コネクタが UDP ポート 53 (DNS 解決に使用されるポート) で DNS サーバーにアクセスできることを確認してください。

- (ZTNA コネクタ バージョン 5.0 以降) ZTNA コネクタがデータセンターへのアプリケーション プローブを実行できるように、ネットワークでセキュリティ ルールが設定されていることを確認します。ZTNA コネクタは、データセンター インターフェイス IPアドレスを、アプリケーション サーバーへのアプリケーション プローブの送信元 IPアドレスとして使用します。アプリケーション プロービングが成功すると、アプリケーション ステータスは 「アップ」になり 、ZTNA コネクタへのユーザー セッションには、送信元 IPアドレスと同じデータセンター インターフェイス IPアドレスが設定されます。アプリケーションのプローブが失敗した場合、アプリケーションのステータスは 「ダウン」になります。この場合、ping および tcp ping 診断ツールを 使用して、アプリケーションへの接続をテストできます。

- ネットワーク内でRFC 6598共有アドレスを使用する場合、ZTNA ConnectorがPrisma Accessとコネクタ間、Prisma Accessとプライベートアプリ間のルーティングに使用できるIPアドレスのブロックを指定する必要があります。

©2025 Palo Alto Networks, Inc.

- 組織の許可リストに追加するIPアドレスとFQDNのリストを制限する必要がある場合は、ZTNA コネクタで許可する IPアドレスと FQDNのリストにあるものを追加します。

  たとえば、米国で ZTNA コネクタを設定する場合は、次の URL を組織の許可リストに追加します:

  - 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 (NTP 用)
  - 0.cloudgenix.pool.ntp.org (NTP 用)
  - 1.cloudgenix.pool.ntp.org (NTP 用)
  - 2.cloudgenix.pool.ntp.org (NTP 用)
  - 3.cloudgenix.pool.ntp.org (NTP 用)

  以前の *FQDN* の *DNS* 解決を *IPv4* 解決に制限します。*ZTNA* コネクタは、*IPv6* を使用したコントローラ *FQDN* への接続の確立をサポートしていません。
- コントローラへのセッションの SSL 復号化を無効にします。

ZTNA コネクタで許可する IPアドレスと FQDN

ZTNA コネクタがスムーズに機能するように、次の URL と IPアドレスを許可リストに追加します。

サービス名	ポート	方向	ソースインターフェイスインターネットプロトコル	宛先とIPアドレス
Prisma Accessにアクセス するZTNAコネクタ	443	アウトバウンド	ZTNA コネクタ WAN ポート	https://controller.cgnx.net アドレス:52.8.93.87 アドレス:52.8.25.40 https://locator.cgnx.net アドレス:13.56.217.238 アドレス:13.56.201.169 hood: 52.40.98.31 34.218.98.185 sugarloaf: 18.200.102.82

©2025 Palo Alto Networks, Inc.

サービス名	ポート	方向	ソースインターフェイスインターネットプロトコル	宛先とIPアドレス
				18.200.135.33 faber: 18.139.242.53 54.255.61.109 https://vmfg.cgnx.net アドレス:52.53.122.104 アドレス:52.53.102.7 https://controller.elcapitan.cgnx.net アドレス:52.8.93.87 アドレス:52.8.25.40 https://vmfg.elcapitan.cgnx.net アドレス:52.53.122.104 アドレス:52.53.102.7 https://controller.hood.cgnx.net アドレス:52.32.167.5 アドレス:54.70.168.33 https://vmfg.hood.cgnx.net アドレス:50.112.136.184 アドレス:34.210.34.87 https://controller.sugarloaf.cgnx.net アドレス:108.128.176.192 アドレス:18.200.144.58 https://vmfg.sugarloaf.cgnx.net アドレス:99.81.179.99 アドレス:99.80.52.255 https://sdwan-stats-hood-us.cgnx.net https://sdwan-stats-elcapitan-us.cgnx.net

©2025 Palo Alto Networks, Inc.

サービス名	ポート	方向	ソースインターフェイスインターネットプロトコル	宛先とIPアドレス
				https://sdwan-stats-hood-jp.cgnx.net https://sdwan-stats-elcapitan-jp.cgnx.net https://sdwan-stats-hood-sg.cgnx.net 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 アドレス:13.41.243.90 アドレス:18.171.17.23 https://vmfg.bowfell.cgnx.net アドレス:52.56.35.36 アドレス:52.56.224.242 https://controller.faber.cgnx.net アドレス:52.74.47.220

©2025 Palo Alto Networks, Inc.

サービス名	ポート	方向	ソースインターフェイスインターネットプロトコル	宛先とIPアドレス
				アドレス:13.251.109.27 https://vmfg.faber.cgnx.net アドレス:18.142.153.59 アドレス:52.74.58.219 h ttps://controller.townsend.cgnx.net アドレス:13.55.31.41 アドレス:3.106.168.215 https://vmfg.townsend.cgnx.net アドレス:52.64.177.240 アドレス: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	アウトバウンド	ZTNAコネクタWANおよびLANポート	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	アウトバウンド	ZTNAコネクタWANおよびLANポート	顧客またはプロバイダーのDNSサーバー

証明書の管理

安全な通信セッションにおける当事者間の信頼を確保するために、Prisma Accessはデジタル証明書を使用します。各証明書には、平文を暗号化したり、暗号化テキストを復号化したりするための暗号化キーが含まれています。また、発行者の ID を認証するためのデジタル署名も含まれています。発行者は、認証する側の信頼された認証局（CA）のリストに記載されている必要

©2025 Palo Alto Networks, Inc.

があります。必要に応じて、認証する側は発行者が証明書を無効化していないことを検証します。Prisma Accessは証明書を使用して、復号化や認証などの機能を保護し、ネットワークに接続するすべてのクライアント、サーバー、ユーザー、デバイス間の通信を保護します。

ZTNAコネクタにオンボードされたアプリケーションの場合は、証明書を設定し、証明局を追加し、Prisma Access証明書管理を使用して証明書チェックを定義します。

©2025 Palo Alto Networks, Inc.

ZTNA コネクタを有効にする

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ ZTNA コネクタ アドオン ライセンス アドオン ライセンスを含む Essential ライセンスには、8つのZTNAコネクタ、100個のFQDN、および4つのIPサブネット機能が含まれます。 アドオン ライセンスを含む Advanced ライセンスには、40個の ZTNA コネクタ、300個のFQDN、および 1024 個のIPサブネット機能が含まれます。 アドオン ライセンスを含むプレミアム ライセンスには、200個のZTNAコネクタ、4000個のFQDN、および1024個のIPサブネット機能が含まれます。 ❑ ZTNAコネクタアドオンライセンスを購入しない場合は、 Prisma Accessライセンスには、4 つのコネクタ、40 個の FQDN、および 4 つの IP サブネットが含まれます。この機能は、ご使用の環境で ZTNA コネクタを試す目的で提供されています。

ZTNA Connectorをセットアップする前に、Prisma Access内でZTNA Connectorを有効にする必要があります。ZTNA Connectorを有効にする前に、次の操作を行います。

- ZTNA コネクタの要件とガイドラインをレビューします。
- アプリケーションIPおよびコネクタIPアドレスブロックを特定します。オンボーディングするコネクタとプライベート アプリケーションにトラフィックをルーティングするために、内部でPrisma Access内で使用するための別のアドレス プールを予約する必要があります。Prisma Accessは、ZTNA ConnectorにオンボードするアプリケーションのFQDNを、アプリケーションIPアドレス ブロックのIPアドレスに解決します。同様に、Prisma Accessはコネクター IPアドレスブロックを使用して、リモートネットワークまたはモバイルユーザーから適切なZTNAコネクターにトラフィックをルーティングします。

  アドレスプール用に少なくとも/16のサブネットを確保する必要があります。RFC 1918またはRFC 6598アドレスを使用します。ZTNA Connectorのセットアップ時に、RFC 6598の代わりにRFC 1918アドレスプールを指定できます。ただし、RFC 1918を指定した後、アドレスプールタイプをRFC 6598に戻すことはできません。
- Strata Cloud Manager
- Panorama

©2025 Palo Alto Networks, Inc.

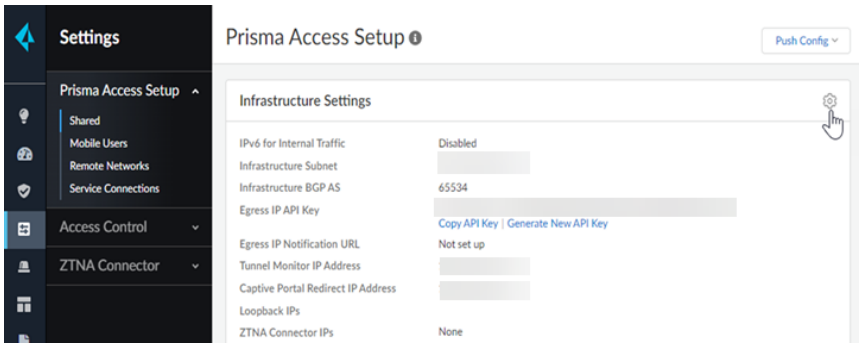
ZTNAコネクタを有効にする（Strata Cloud Manager）

Cloud Managed Prisma AccessでZTNAコネクタを有効にするには、次のワークフローを使用します。

STEP 1 | Prisma Accessが内部で使用するIPアドレスブロックを構成して、ZTNA Connectorと搭載するプライベートアプリにトラフィックをルーティングする。

コネクタとアプリケーションには個別のIPアドレス ブロックを定義する必要があり、ブロックは相互に重複できず、Prisma Accessインフラストラクチャ サブネットやGlobalProtect IPアドレス プールとも重複できません。

- **[Workflows (ワークフロー)]** > **[Prisma Accessセットアップ]** > **Prisma Access** > **[Infrastructure Settings (インフラストラクチャ設定)]**を選択します。



- **ZTNA** コネクタ アプリケーション **IP** ブロックを追加します。

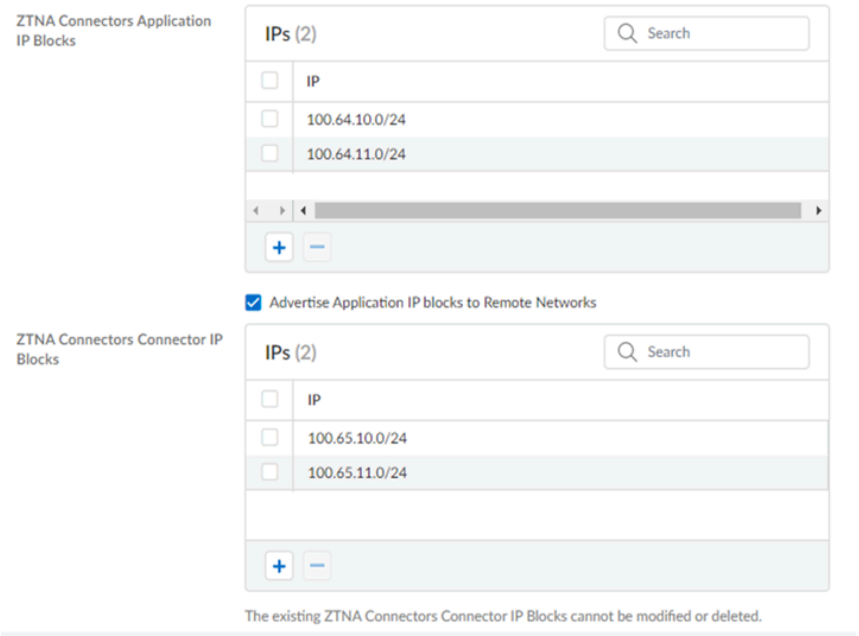
  はデプロイメントに応じて、単一のアプリケーションIPブロックまたは複数のブロックを追加できます。例えば、100.64.10.0/24 and 100.64.11.0/24を入力します。アプリケー

©2025 Palo Alto Networks, Inc.

ション **IP** ブロックをリモート ネットワークにアドバタイズして、 リモート ネットワーク アクセスを提供することもできます。

- Prisma Accessが内部的に使用して、モバイル ユーザー、リモート ネットワーク、およびデータ センター内のコネクタ VM 間でトラフィックをルーティングする **ZTNA** コネクタ・コネクタ **IP** ブロックを追加します。

  デプロイメントに応じて、単一のコネクタIPブロックまたは複数のブロックを追加できます。たとえば、100.65.10.0/24 と 100.65.11.0/24 と入力します。

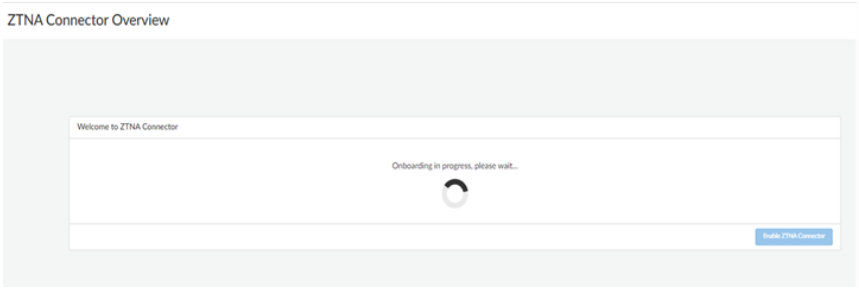


- [保存] をクリックしてIPアドレス ブロックの設定を保存し、[コミット] をクリック して設定をプッシュします。

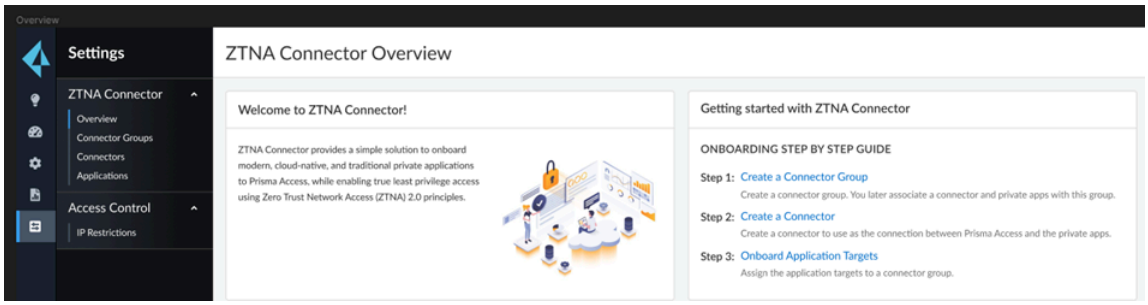
 ©2025 Palo Alto Networks, Inc.

STEP 2 | Strata Cloud ManagerからのZTNAコネクタを起動します。

- [ワークフロー] > **[ZTNA** コネクタ]を選択します。
- Prisma AccessはZTNAコネクタのインフラストラクチャのセットアップを開始します。接続と登録には数分かかる場合があります。



- オンボーディングが完了すると、ZTNAコネクタの概要が表示されます。



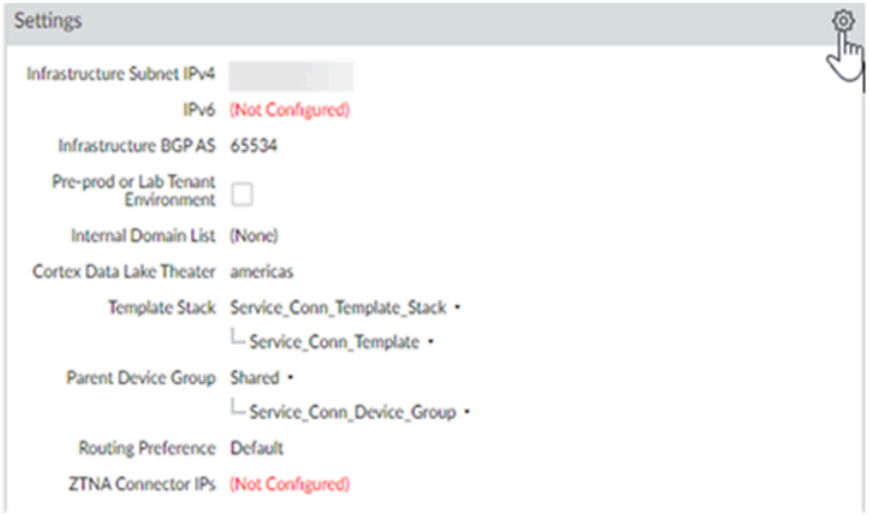
ZTNAコネクタを有効にする（Panorama）

Prisma Access (Managed by Panorama)でZTNA Connectorを有効にするには、次のワークフローを使用します。

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Prisma Accessが内部で使用するIPアドレスブロックを構成して、ZTNA Connectorと搭載するプライベートアプリにトラフィックをルーティングします。

- **Panorama** > **Cloud Services** (クラウドサービス) > **Configuration** (構成) > **Service Setup** (サービス セットアップ) を選択し、 設定を編集します 。



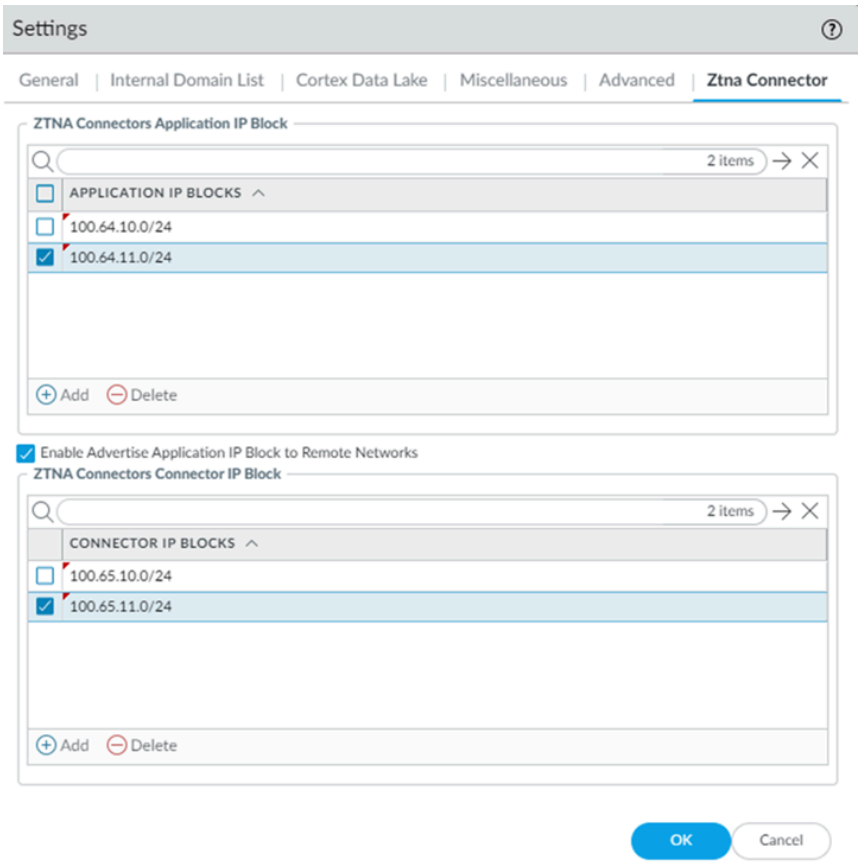
- **ZTNA**コネクタ タブで、アプリケーション**IP**ブロックを追加します 。

  デプロイメントに応じて、単一のアプリケーションIPブロックまたは複数のブロックを追加できます。たとえば、100.64.10.0/24 と 100.64.11.0/24 の場合。リモート ネットワークへのアプリケーション**IP**ブロックのアドバタイズを有効にすることもできます。

- Prisma Accessがモバイル ユーザー、リモート ネットワーク、およびデータセンター内のコネクタVM間でトラフィックをルーティングするために内部的に使用するコネクタ**IP**ブロックを設定します。

  デプロイメントに応じて、単一のコネクタIPブロックまたは複数のブロックを追加できます。たとえば、100.65.10.0/24 と 100.65.11.0/24 と入力します。

©2025 Palo Alto Networks, Inc.

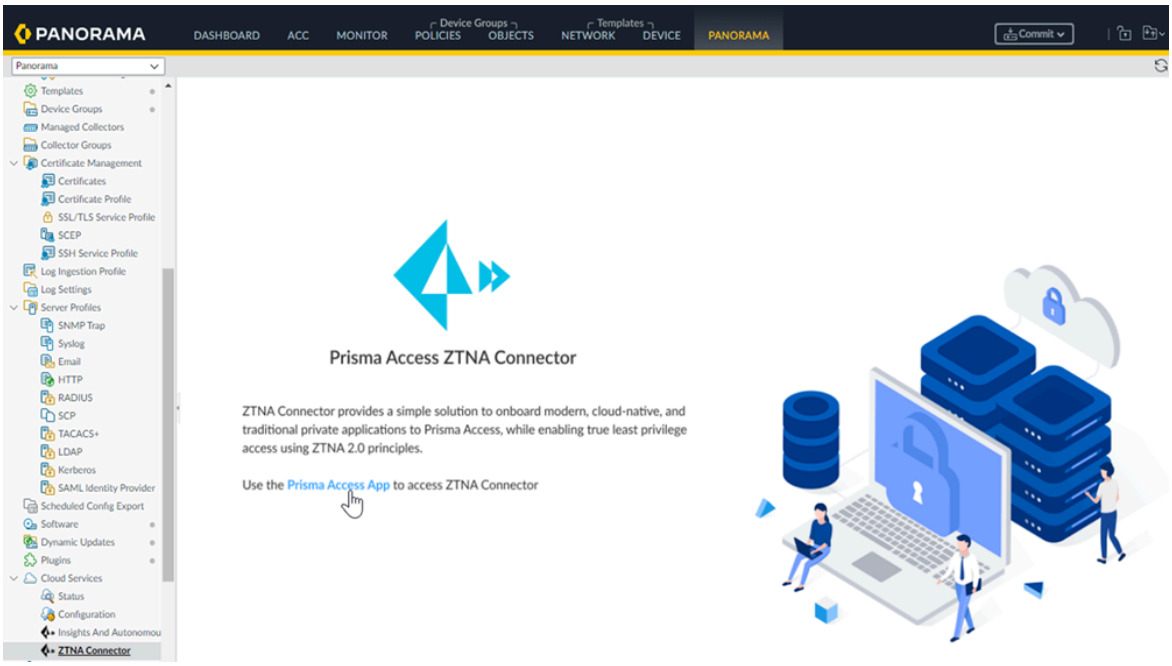


- **[OK]**をクリックしてIPアドレス ブロックの設定を保存し、**[コミット]** をクリック して設定をプッシュします。

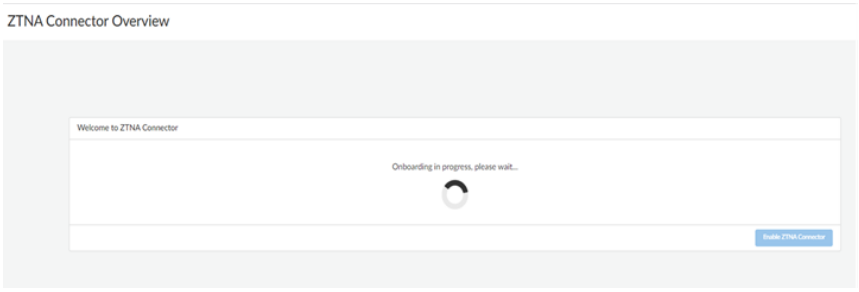
©2025 Palo Alto Networks, Inc.

STEP 2 | Panoramaのクラウド サービス プラグインからZTNAコネクタを起動します。

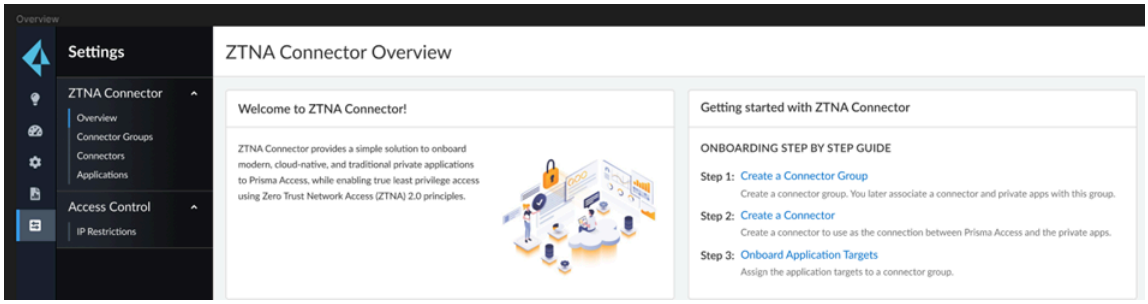
- **[Panorama]** > **[Cloud Services]** > **[ZTNA Connector]**を選択します。
- Strata Cloud Managerをクリックすると、ハブのStrata Cloud Managerで ZTNA Connectorが起動します。



- Strata Cloud Managerから、**[Settings (設定)]** > **[ZTNA Connector]**を選択します。
- Prisma AccessはZTNAコネクタのインフラストラクチャのセットアップを開始します。接続と登録には数分かかる場合があります。



- オンボーディングが完了すると、ZTNAコネクタの概要が表示されます。



 ©2025 Palo Alto Networks, Inc.

ZTNAコネクタの設定

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ ZTNA コネクタ アドオン ライセンス アドオン ライセンスを含む Essential ライセンスには、8つのZTNAコネクタ、100個のFQDN、および4つのIPサブネット機能が含まれます。 アドオン ライセンスを含む Advanced ライセンスには、40個の ZTNA コネクタ、300個のFQDN、および 1024 個のIPサブネット機能が含まれます。 アドオン ライセンスを含むプレミアム ライセンスには、200個のZTNAコネクタ、4000個のFQDN、および1024個のIPサブネット機能が含まれます。 ❑ ZTNAコネクタアドオンライセンスを購入しない場合は、 Prisma Accessライセンスには、4 つのコネクタ、40 個の FQDN、および 4 つの IP サブネットが含まれます。この機能は、ご使用の環境で ZTNA コネクタを試す目的で提供されています。

ZTNA コネクタを有効にするの後、ZTNA Connectorコンポーネントのセットアップを開始できます：

©2025 Palo Alto Networks, Inc.

STEP 1 | アプリケーション IP アドレスブロックとコネクタ IP アドレスブロックを特定し、Prisma AccessでIP アドレスブロックを追加します。

*IP*アドレスブロックについては、次の推奨事項を参照してください。

- アプリケーションごとに個別の*IP*アドレスを割り当てます。
- 各コネクタに最低 */27 IP* アドレスブロック *(1* コネクタあたり最低*32*個の*IP*アドレス*)* を割り当てます。
- 各コネクタグループに一意の*IP*アドレスを割り当てます。

必要に応じて、さらにコネクタまたはアプリケーションブロックを追加して対応できます。

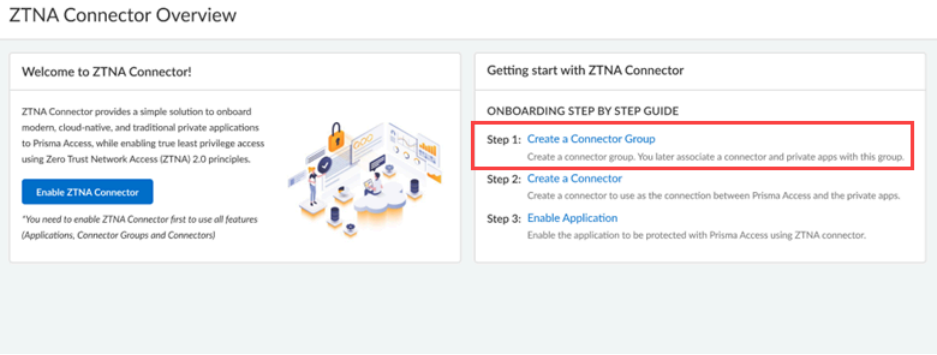
ネットワーク内でRFC 6598アドレスを使用する場合、オンボーディングするコネクタとプライ ベート アプリケーションにトラフィックをルーティングするために、内部的にPrisma Access内で使用するために別のRFC 6598 IPアドレス プールを予約する必要があります。

STEP 2 | コネクタグループを作成します。

コネクタグループは、コネクタとアプリケーションを論理的にグループ化したものです。アプリケーションとコネクタをグループ化するには、さまざまな方法があります。コネクタを地理的に異なる場所にグループ化して冗長化できます。または、同じデータセンターに複数のコネクタを作成してスループットを向上させることもできます。ポリシー管理を簡素化するために、同じユーザーグループが使用するアプリケーションをグループ化したい場合があります。最初にコネクタグループを作成し、次にコネクタとアプリケーションをグループに追加します。

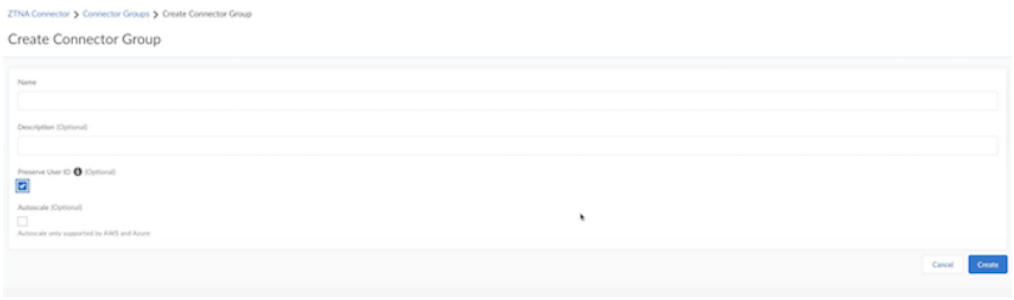
必要に応じてこの手順を繰り返して、コネクタとアプリケーションをグループ化するために必要なすべてのコネクタグループを作成します。

1. [ワークフロー] > [**ZTNA**コネクタ]を選択し、[概要] または[コネクタグループ]を選択します。そして、[コネクタグループを作成]を選択します。



 ©2025 Palo Alto Networks, Inc.

2. コネクタグループに名前を付け、[ユーザー ID を保存]を有効にし、オプションでその説明を入力します。



3. (任意) データセンターがAzureまたはAWSにあり、自動スケーリング機能を使用する場合は、**[Autoscale]** を選択します。この機能を有効にしている場合は、コネクタを作成する必要はありません。
4. コネクタグループを作成します。

©2025 Palo Alto Networks, Inc.

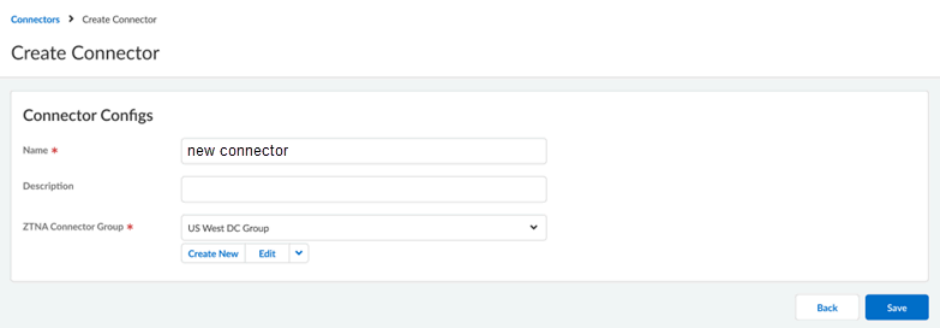
STEP 3 | 自動スケーリングされていないコネクタグループを選択した場合にのみ、コネクタを作成してコネクタグループに追加します。

コネクタを作成し、コネクタグループに追加します。

コネクタは、Prisma Accessに接続するデータセンターで実行されている仮想マシンを表します。Prisma Access内でコネクタを作成し、提供されたシークレット／キーを使用して、データセンター内の対応するコネクタVMにオンボードする必要があります。

必要に応じてこの手順を繰り返し、データ・センター・アプリケーションをPrisma Accessに接続するために必要な数のコネクタを作成します。

- [ワークフロー] > [**ZTNA**コネクタ]を選択し、[概要] または[コネクタ]を選択します。そして、[コネクタを作成]を選択します。
- コネクタの**Name**（名前）を入力します。



- (Optional) コネクタに 説明 を追加します。
- コネクタを追加するコネクタグループを選択します。

ルーティングを簡素化し、データセンターのサーバーにすばやくアクセスするために、*Palo Alto Networks*はコネクタとサーバーを同じサブネットに配置することを推奨しています。

- コネクタを作成します。

ZTNA コネクタを最新の状態に保つには、ソフトウェアバージョンを更新できます。***ZTNA Connector*** > ***Connector Groups***のアイコンには、コネクタの状態とアップグレードが可能かどうかが表示されます。

©2025 Palo Alto Networks, Inc.

STEP 4 | コネクタの設定に使用するキーとシークレットを取得します。

KeyとSecretの値は、後のステップで VM を設定するときに使用します。

1. Autoscaleコネクタグループ – 以下の手順に従ってください。
   1. ワークフロー > **ZTNA** > コネクタコネクタグループに移動します。
   2. Auto Scale コネクタグループのアクション領域で [トークンのコピー] を選択し、次に [キー] と [シークレット] の値をコピーします。

      キーとシークレットを使用して、作成したクラウドインスタンスまたは VM をコネクタに関連付けます。
2. 非自動スケーリングコネクタグループ – 以下の手順に従ってください。
   - ワークフロー > **ZTNA**コネクタ > コネクタを選択します。
   - デプロイするコネクタを選択します。
   - アクション領域で [トークンのコピー] を選択し、次に [キー] と [シークレット] の値をコピーします。

     キーとシークレットを使用して、作成したクラウドインスタンスまたは VM をコネクタに関連付けます。

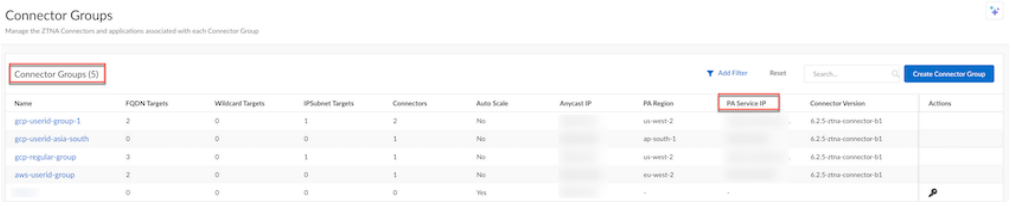


STEP 5 | ZTNA コネクタ仮想マシンをデータセンターにデプロイします。

STEP 6 | (オプション) ワークフロー > **ZTNA** > コネクタグループを選択し、コネクタグループの **PA** サービス **IP** アドレスを書き留めて、この IP アドレスを組織の許可リストに追加します。

コネクタグループに***PA*** サービス ***IP*** が表示されるのは、コネクタをオンボードした後だけです。

必要に応じて、このIPアドレスを許可リストに追加して、ネットワークがZTNAコネクタトラフィックを送受信できるようにします。



STEP 7 | ターゲットをコネクタグループに追加します。

ZTNA Connector VMを介してデータセンターのプライベートアプリにアクセスするためのターゲットを設定します。FQDNワイルドカード、FQDN、またはIPサブネットに基づいてターゲットを追加できます。ZTNA Connector は、モバイルユーザーと支社のユーザー

 ©2025 Palo Alto Networks, Inc.

がPrisma Accessを介して安全にアプリにアクセスするために必要なネットワークとDNSの設定を行います。

1. ワークフロー > **ZTNA**コネクタ > アプリケーションターゲットを選択します。
2. 作成するターゲットのタイプを選択します。

   コミットレスアプリオンボーディングの強化により、アプリケーションのオンボーディングは*1*分未満で完了し、アプリケーションにすばやくアクセスできるようになりました。この機能により、より多くのアプリケーションをオンボードすることもできます。

   制限事項*:*

   - 複数のアプリケーションターゲット *(*ポート*/*プロトコルが異なる*)* に同じ*FQDN*を追加することはできません。
   - ワイルドカードターゲットを追加または削除すると、*MU*または*RN*でコミットが行われ、*DNS*プロキシ転送ルールが追加または削除されます。ただし、ワイルドカードに一致する *FQDN*を後でワイルドカードアプリケーションから検出する場合、追加のコミットを必要としないため、アプリケーションをすばやくオンボーディングしてすぐにアクセスできるようになります。

   コミットレス アプリのオンボーディング機能を有効にするには、*Prisma Access*データプレーンをバージョン *11.2.3* 以降に更新する。

- ワイルドカードターゲット – ターゲットにはワイルドカード (*.example.com など) を使用します。ユーザーがワイルドカードと一致するサイトにアクセスすると、モバイルユーザーとリモートネットワークユーザーがそれらのアプリに ZTNA Connector からアクセスできるように自動的にオンボーディングされます。たとえば、ワイルドカードが*.example.comの場合、ユーザーがapp1.example.comのアプリにアクセスすると、ZTNA Connectorは特定のFQDN、プロトコル、およびポートを使用してその子アプリをオンボーディングするための構成を自動的に作成します。

  さらに、ユーザーがワイルドカードに基づくアプリ **(**たとえば、***.example.com** ワイルドカードに基づく **app1.example.com)** にアクセスすると、そのアプリが検出され、自動的に **FQDN** ターゲットとして登録されます。

  1. 「ワイルドカードターゲット」と「ワイルドカードターゲットの作成」に移動します。
  2. テンプレートの一意の名前を入力します。
  3. ターゲットに関連付けるコネクタグループを入力します。

     グループは**FQDN/**ワイルドカードの一種でなければなりません。

     Prisma Access5.0.1以降では、ワイルドカードターゲットとFQDNターゲットの両方に複数のコネクタグループを選択できます。ワイルドカードまたはFQDNターゲット

 ©2025 Palo Alto Networks, Inc.

ごとに最大4つのコネクタグループを選択できます。ターゲットごとに複数のコネクタグループを選択する場合は、ガイドラインを使用してください。

4. ターゲットで使用するワイルドカードを入力します。

   .example.com または.my.example.com の形式で入力します (UI ではワイルドカードの前にアスタリスクが暗黙的に追加されます)。*.*、example.*.com、または*.comのワイルドカードを指定して、すべてのサイトを許可しないでください。

5. プロトコル (**tcp**、**udp**、または両方) を選択します。
6. (任意) GlobalProtect ユーザーから ZTNA コネクタデータセンターへの ICMP プロトコルを有効にするには、「**ICMP** プロトコルを許可する」を選択します。
7. アプリに使用するポートを選択します。

   1 つのポートを入力するか、複数のポートをカンマで区切って入力するか、ダッシュを使用してポートの範囲を入力するか、または両方を入力します。 カンマの後にスペースを追加しないでください。[任意]のポート を選択して指定した任意のポートと一致させるか、[一致]を選択して一致する 1 つまたは複数のポートを入力します。

   [プロトコル] で両方を選択した場合は、[**TCP**ポート] と [**UDP**ポート] にポートを追加する必要があります。

   [詳細設定] の [**TCP**ポート] フィールドに範囲を入力すると、**icmp ping**が実行され、[プローブタイプなし] がアクティブになります。

8. 選択したプロトコルに応じて、プローブタイプとして**[TCP ping]**、**[icmp ping]**、または**[なし]**を入力します。

   [tcp ping] を選択した場合は、プローブポートを選択し、1 つのポートを入力します。ポートは、ポートとプロトコルの領域に入力したポートの範囲内にある必要はありません。ZTNAコネクタは、プローブポートからFQDNの解決済みIPアドレスにtcp pingを実行して、アプリの到達可能性を判断します。ping が成功すると、アプリは**Up**状態と見なされます。

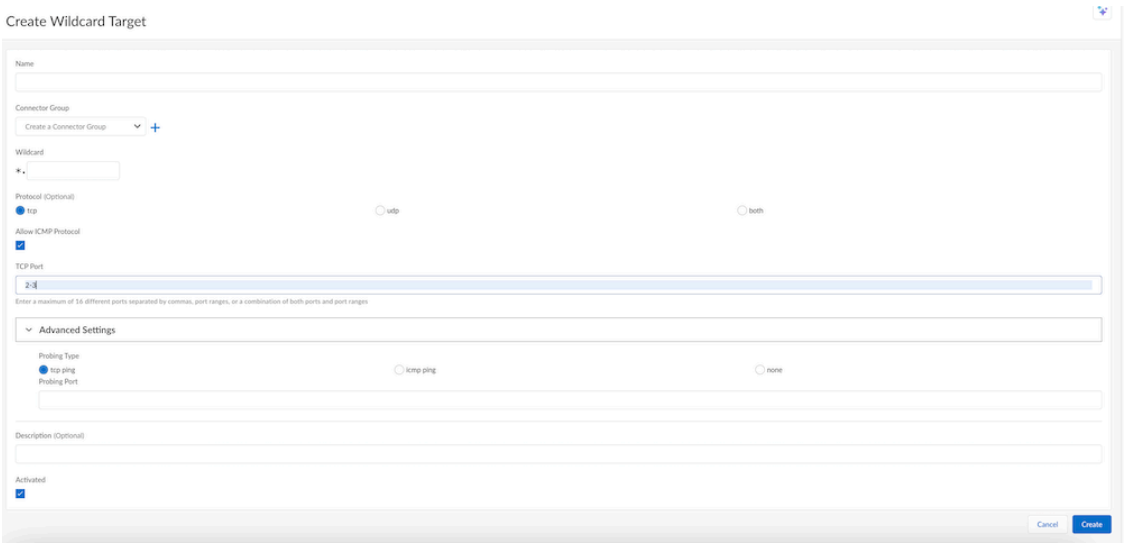
   アプリケーションのオンボーディング中に追加したプローブポートを編集することもできます。プローブポートが更新されると、ZTNA Connectorは更新されたポートでTCPプローブアプリケーションを起動し、それに応じてアプリケーションのステータスが更新されます。

   icmp ping を選択すると、ZTNA コネクタは FQDN の解決済み IP アドレスに対して ICMP ping を実行します。ICMP ping への応答が受信された場合、アプリは**up**と見なされます。

   「なし」を選択した場合、プローブは実行されず、アプリケーションは常に「**Up**」としてマークされます。

 ©2025 Palo Alto Networks, Inc.

9. [アクティベート] を選択し、ターゲットを作成します。



- **FQDN** ターゲット – 単一の FQDN のターゲットを作成するには、FQDN ターゲットを作成します。

  *Prisma Access5.0*以降、 *5.0*以降の*ZTNA*コネクタバージョンのコネクタグループでは、アプリケーション*FQDN*が複数のプライベート*IP*アドレスに解決されると、*ZTNA*コネクタはアプリケーションプローブを実行して解決されたすべての*IP*アドレスのステータスを判断し、アプリケーションステータスが「*Up*」の複数の解決済み*IP*アドレスへの*FQDN*アクセスを負荷分散します。

  FQDN ターゲットを作成するには、「**FQDN** ターゲット」と「**FQDN** ターゲットの作成」を参照してください。FQDNターゲットは、FQDNワイルドカードを作成するのと同じように、FQDNワイルドカードを1つのFQDNに置き換えて作成します。

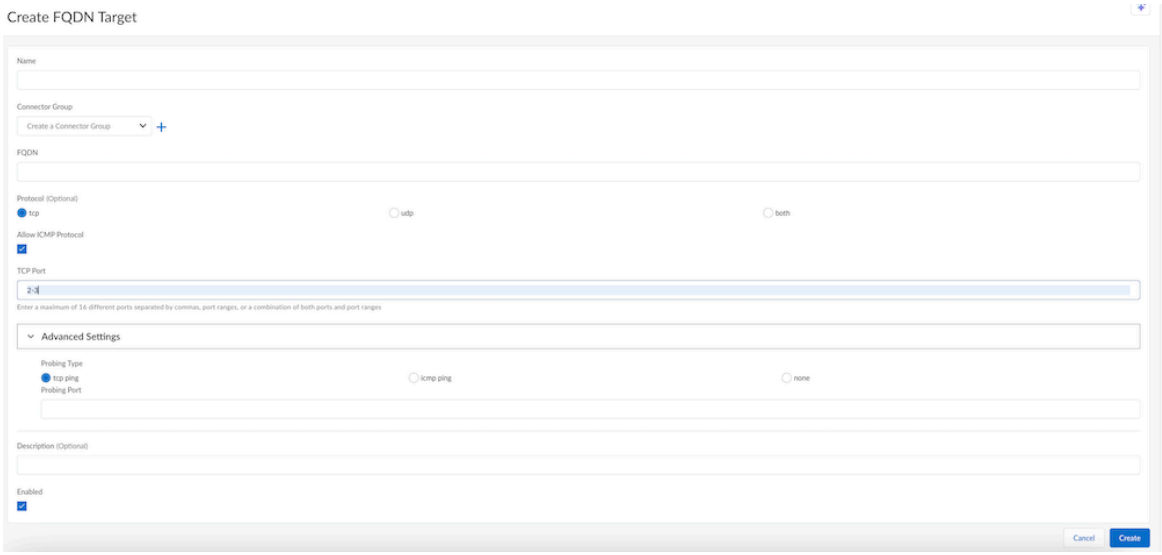
  Prisma Access5.0.1以降、FQDNターゲットおよびワイルドカードターゲットごとに複数のコネクタグループを選択できます。FQDNまたはワイルドカードターゲットごとに最大4つのコネクタグループを選択できます。ターゲットごとに複数のコネクタグループを設定する場合は、ガイドラインを使用してください。

  ワイルドカードターゲットの結果として検出されたアプリケーションもここに表示されます。ユーザーがワイルドカードと一致するサイトにアクセスすると、モバイルユーザーとリモートネットワークユーザーがそれらのアプリに ZTNA Connector からアクセスできるように自動的にオンボーディングされます。たとえば、ワイルドカードとして*.example.comを指定すると、ユーザーがapp1.example.comのアプリにアクセスすると、ZTNAコネクタはそのアプリをFQDNターゲットのリストに自動的に追加します。

  親ワイルドカードターゲットから FQDN アプリケーションが検出されても、ワイルドカードターゲットへの変更は、検出されたアプリケーションでは更新されません。また、同じ発見された FQDN は再発見されません。検出された FQDN アプリケーション

 ©2025 Palo Alto Networks, Inc.

の特性を更新する必要がある場合は、次の手順を使用して検出されたアプリケーションを手動で更新します。



- **IP**サブネット – IPサブネットベースのターゲットを作成して、FQDNではなくIPサブネットに基づいてアプリを検索します。

  1. **[IP**サブネット**]**と**[**サブネットルールの作成**]**に移動します。
  2. ターゲットの一意の名前を入力します。
  3. ターゲットに関連付けるコネクタグループを入力します。

     グループは **IP**サブネットの一種である必要があります。
  4. グループ内のコネクタが IP ルーティングアクセスを提供するデータセンターの **IP**サブネットを指定します。

     グループ内のすべてのコネクタは、指定されたIPサブネットへのルーティングアクセスを提供します。10.1.1.1/32形式の単一のIPアドレス、1つのサブネット、またはカ

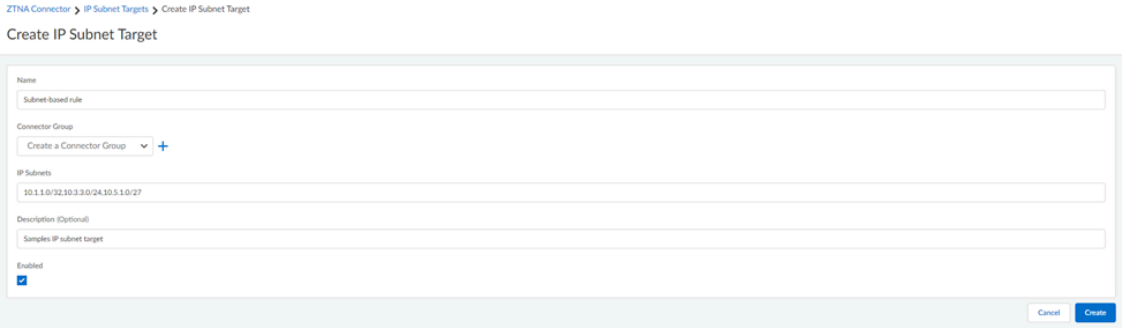
©2025 Palo Alto Networks, Inc.

ンマで区切られた複数のサブネットを選択できます。最大16個のサブネットを入力します。

IPサブネットはテナントのIPファブリック内でルーティング可能である必要があり、IPサブネットはテナント内の次のような他のIPサブネットと重複することはできません。

- Panoramaでユーザーが設定したスタティック ルート、ブランチからリモートネットワークにアドバタイズされたルート、データセンターからサービス接続にアドバタイズされたルートなど、その他のIPルーティング可能なサブネット。
- ZTNA FQDN アプリケーション IP サブネット
- ZTNA コネクタ IP サブネット
- インフラストラクチャサブネット IPアドレス
- モバイルユーザー—GlobalProtect IPアドレスプール

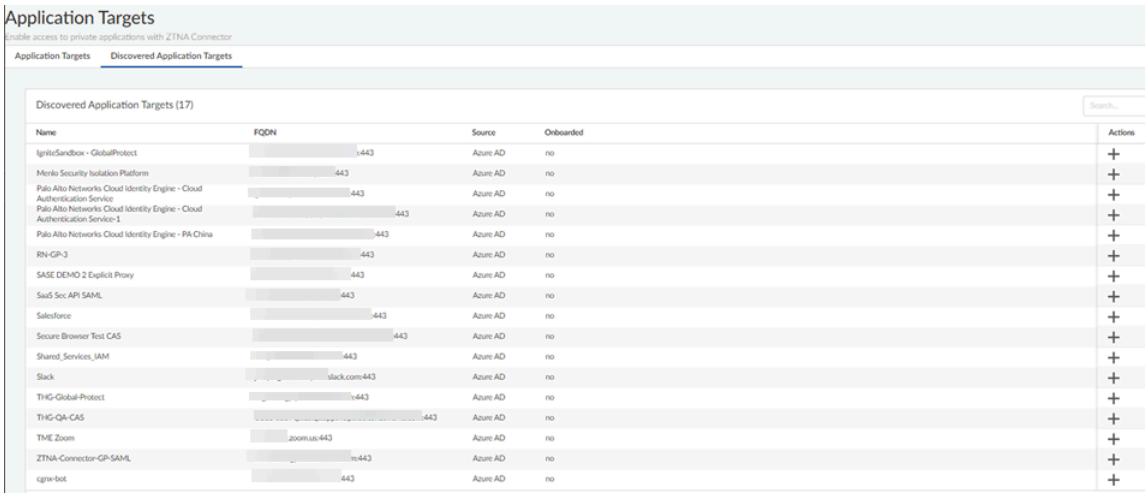
5. 有効化を選択してターゲットを作成します。



©2025 Palo Alto Networks, Inc.

STEP 8 | ZTNA Connector によって自動検出されたアプリケーションをコネクタグループに追加します。

1. Cloud Identity Engineを使用してアプリケーションの自動検出を設定する
2. **[ワークフロー] > [ZTNAコネクタ] > [アプリケーションターゲット] > [Discovered Application Targets (発見されたアプリケーション ターゲット)]**を選択します。



3. アクションの下の [+] をクリックして、アプリケーションをコネクタグループに追加します。
4. アプリケーションに一意の名前を付けます。
5. アプリに関連付ける **ZTNA** コネクタグループを選択します。
6. プローブタイプ（**TCP ping**、**icmp ping**、またはなし）を入力します。
   - **tcp ping** を選択した場合は、プローブポートも選択します。ポートは、ポートとプロトコルの領域に入力したポートの範囲内にある必要はありません。プローブタイプに**tcp ping**を選択した場合、Palo Alto Networksはプローブポートにも同じポートを使用することを推奨しています。

     ZTNAコネクタは、プローブポートからFQDNの解決済みIPアドレスにtcp pingを実行して、アプリの到達可能性を判断します。ping が成功すると、アプリは **Up** 状態と見なされます。
   - アプリケーションのオンボーディング中に追加したプローブポートを編集することもできます。プローブポートが更新されると、ZTNA Connectorは更新されたポートでTCPプローブアプリケーションを起動し、それに応じてアプリケーションのステータスが更新されます。
   - **icmp ping** を選択すると、ZTNA コネクタは FQDN に ICMP ping を実行します。ICMP pingへの応答を受信すると、ZTNA コネクタはアプリケーションのステータスを**Up**に設定します。
   - **[none (なし)]**を選択した場合、プローブは実行されず、アプリケーションは常に**Up**としてマークされます。
7. **Enabled**（有効）を選択します。
8. アプリケーションターゲットを作成します。

©2025 Palo Alto Networks, Inc.

STEP 9 | セキュリティポリシールールを作成して、ユーザーがコネクタ内のアプリにアクセスできるようにします。

STEP 10 | (任意) ZTNA コネクタを表示および監視して、ZTNA コネクタとコネクタグループのパフォーマンスを確認します。

STEP 11 | (任意) ZTNA Connectorを使用してプライベートアプリにアクセスする際に問題が発生した場合は、ping、traceroute、および nslookup 診断ツールを使用してアプリの到達可能性を確認してください。

ZTNAコネクタのアップグレード

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ ZTNA コネクタ アドオン ライセンス アドオン ライセンスを含む Essential ライセンスには、8つのZTNAコネクタ、100個のFQDN、および4つのIPサブネット機能が含まれます。 アドオン ライセンスを含む Advanced ライセンスには、40個の ZTNA コネクタ、300個のFQDN、および 1024 個のIPサブネット機能が含まれます。 アドオン ライセンスを含むプレミアム ライセンスには、200個のZTNAコネクタ、4000個のFQDN、および1024個のIPサブネット機能が含まれます。 ❑ ZTNAコネクタアドオンライセンスを購入しない場合は、 Prisma Accessライセンスには、4 つのコネクタ、40 個の FQDN、および 4 つの IP サブネットが含まれます。この機能は、ご使用の環境で ZTNA コネクタを試す目的で提供されています。

ZTNAコネクタを最新の状態に保つには、ソフトウェア バージョンを更新します。新しい機能をサポートするためにコネクタをアップグレードする必要がある場合もあります。

新しいZTNAコネクタ バージョンがリリースされると、デプロイメント内のコネクタがチェックされ、リリースされたバージョンが既存のバージョンよりも新しい場合、またはグループ内のすべてのコネクタが同じバージョンではない場合は、コネクタ グループ領域のアイコンに更新が利用可能であることが示されます。コネクタを更新することを選択した場合は、グループ全体をまとめてアップグレードするオプションが提供されます。グループをアップグレードすると、そのグループ内のすべてのコネクタが同時に自動的にアップグレードされます。個々のコネクタをアップグレードすることはできません。

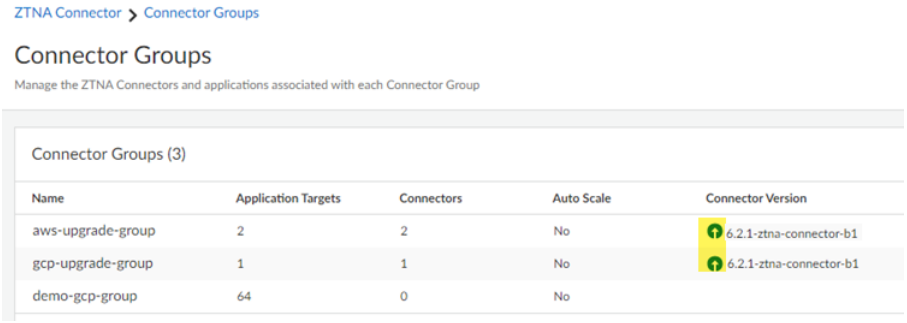
 ©2025 Palo Alto Networks, Inc.

*ZTNA*コネクタのアップグレードには約 *8* ～ *10* 分かかり、このプロセス中にコネクタが再起動されます。*Palo Alto Networks*では、ダウンタイム中または予定されたネットワーク停止中にコネクタのアップグレードをスケジュールすることをお勧めします。

STEP 1 | **[ZTNA**コネクタ**]** > **[**コネクタ グループ**]**に移動します。緑色の矢印はアップグレードが利用可能であることを示します。

テナントで利用可能な最新のイメージ バージョンにのみアップグレードできます。

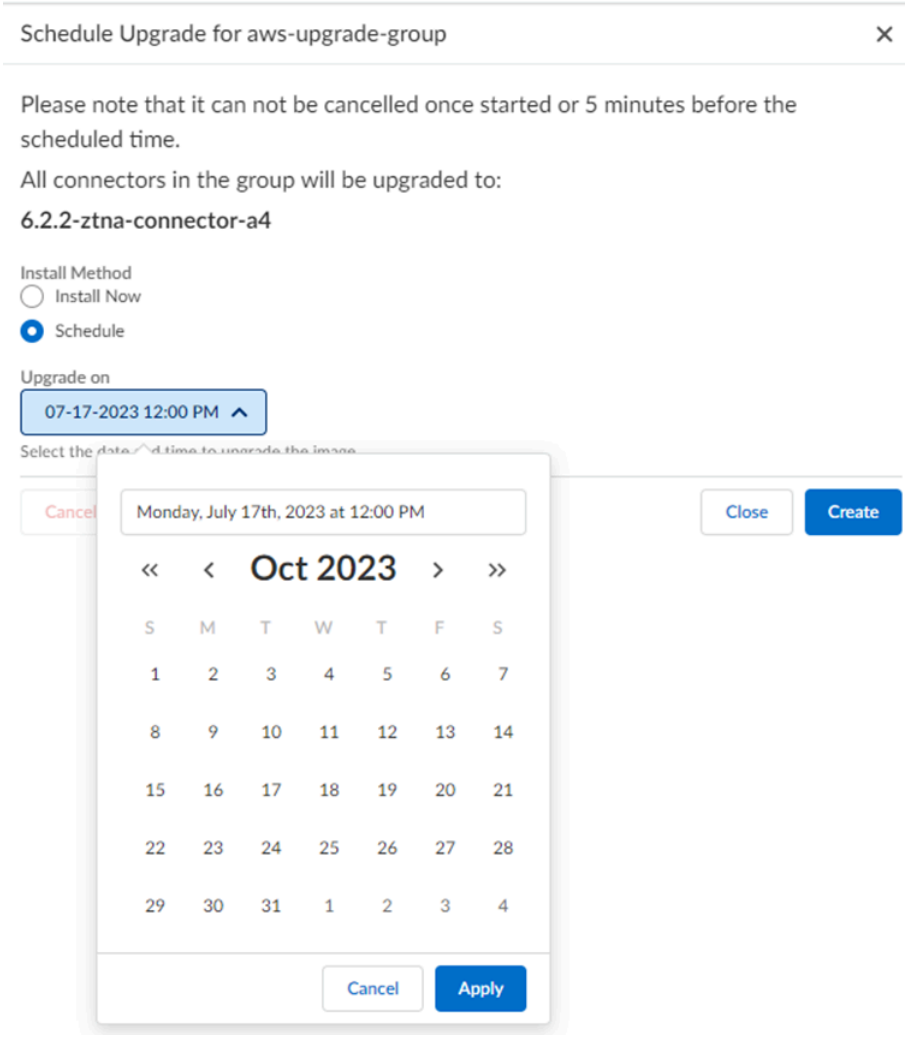
STEP 2 | コネクタ グループの横にある緑色の矢印をクリックします。



 ©2025 Palo Alto Networks, Inc.

STEP 3 | **[Install Now (今すぐインストール)]**を選択してコネクタ グループをアップグレードするか、[スケジュール]を選択してアップグレードの日時を指定します。表示される時間は、ZTNA UIを使用する管理者のローカル タイム ゾーンです。

スケジュールされたアップグレードは、開始の**5**分前までキャンセル できます。



STEP 4 | コネクタ バージョンの下にあるアイコンを表示して、コネクタのステータスを確認します。

Icon（アイコン）	詳説
	アップグレードが利用可能です。
	アップグレードが予定されています。

©2025 Palo Alto Networks, Inc.

Icon（アイコン）	詳説
	アップグレードが開始され、進行中です。
アイコンなし（コネクタバージョンのみが表示されます） 6.1.1-ztna-connector-a8	アップグレードは成功しました。
	すべてのコネクタがアップグレードされたわけではありません。
	アップグレードに失敗しました

ZTNAコネクタ診断ツール

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ ZTNA コネクタ アドオン ライセンス アドオン ライセンスを含む Essential ライセンスには、8つのZTNAコネクタ、100個のFQDN、および4つのIPサブネット機能が含まれます。 アドオン ライセンスを含む Advanced ライセンスには、40個の ZTNA コネクタ、300個のFQDN、および 1024 個のIPサブネット機能が含まれます。 アドオン ライセンスを含むプレミアム ライセンスには、200個のZTNAコネクタ、4000個のFQDN、および1024個のIPサブネット機能が含まれます。 ❑ ZTNAコネクタアドオンライセンスを購入しない場合は、 Prisma Accessライセンスには、4 つのコネクタ、40 個の FQDN、および 4 つの IP サブネットが含まれます。この機能は、ご使用の環境で ZTNA コネクタを試す目的で提供されています。

ZTNAコネクタを使用してプライベート アプリにアクセスする際に問題が発生した場合は、次のネットワーク ツールを使用して、ZTNA コネクタ UI からテストを実行し、問題を特定できます。

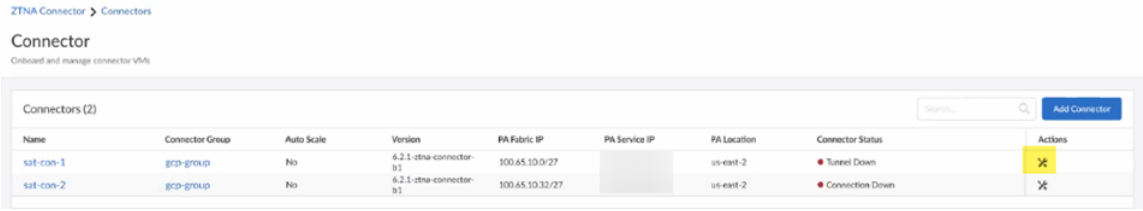
©2025 Palo Alto Networks, Inc.

- ping
- TCP Ping
- トレースルート
- nslookup
- dumpの概要
- また、パケット キャプチャを取得してZTNA コネクタの問題の原因を特定することもできます。

*ping*および*traceroute*ツールを使用する前に、ネットワークで *ICMP* が許可されていることを確認してください。一部のクラウド環境では、セキュリティ上の懸念から*ICMP*が禁止されており、これらのツールではアクティビティが表示されません。

STEP 1 | ワークフロー > **ZTNA**コネクタ > コネクタに移動します。

STEP 2 | コネクタの **[アクション]** > **[Diagnostics (診断)]** を選択します。



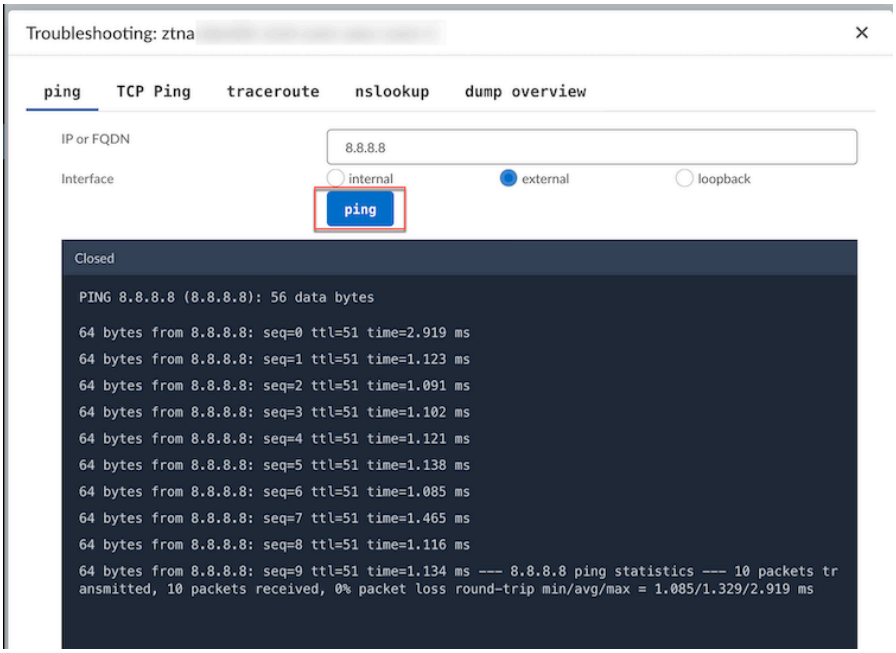
©2025 Palo Alto Networks, Inc.

STEP 3 | ping、TCP Ping、traceroute、または nslookup 診断ツールを実行します。

- **ping**:
  1. アクセスしようとしているアプリケーションの**IP**または**FQDN**を選択します。
  2. pingをテストする インターフェース を選択します。

     VMを2アームデプロイメントで構成した 場合は、VMのLAN側 (ポート 2) を確認するには内部を選択し、WAN側 (ポート 1) を確認するには外部を選択します。

     ワンアームデプロイメントの場合、WAN側とLAN側の両方がポート 1 にマップされるため、 内部 または 外部のいずれかを選択します。
  3. **ping**を選択します。

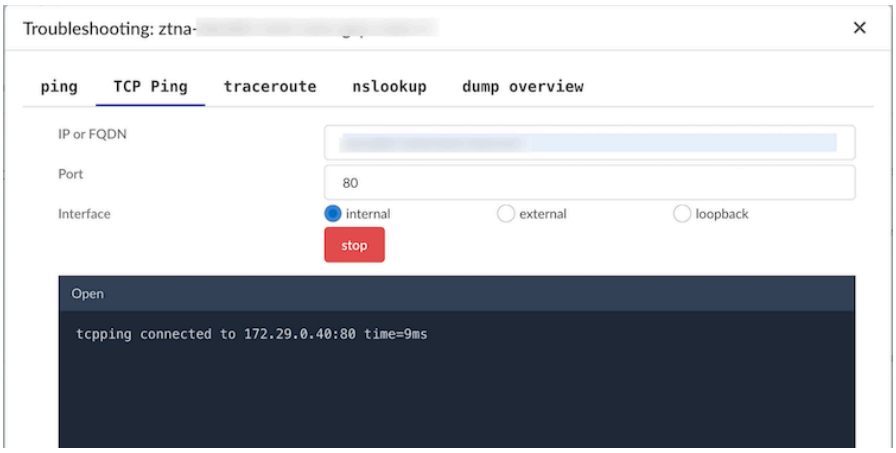
     ping出力が表示されます。
  4. テストを終了するには、[停止] をクリックします。
- **TCP ping**:

  コネクタを *ZTNA* コネクタ *6.2.5-b1* バージョンにアップグレードします。コネクタがこのバージョンで最新でない場合は、 *Strata Cloud ManagerUI* は診断ツールとして ***TCP Ping***を提供しません。

  1. アクセスしようとしているアプリケーションの **IP**または**FQDN**を選択します。
  2. pingをテストするインターフェースを選択します。

     VMを2アームデプロイメントで構成した 場合は、VMのLAN側 (ポート 2) を確認するには内部を選択し、WAN側 (ポート 1) を確認するには外部を選択します。
  3. **TCP Ping**を選択します。

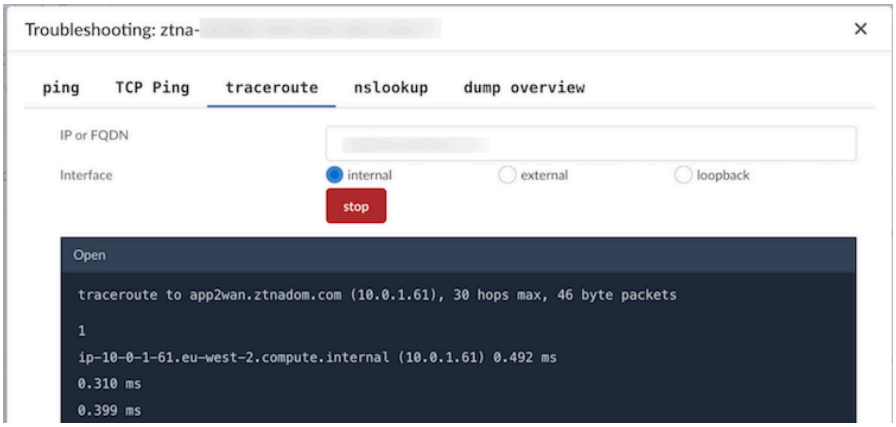
©2025 Palo Alto Networks, Inc.



4. テストを終了するには、[停止] をクリックします。

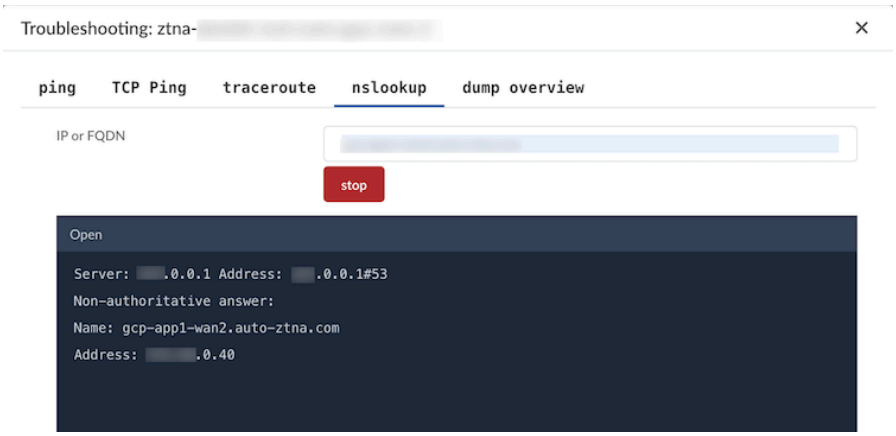
- **traceroute**:
  1. アクセスしようとしているアプリケーションの**IP**または**FQDN**を選択します。
  2. pingをテストする インターフェース を選択します。

     VMを2アームデプロイメントで構成した 場合は、VMのLAN側 (ポート 2) を確認するには内部を選択し、WAN側 (ポート 1) を確認するには外部を選択します。
  3. **traceroute**を選択します。
  4. テストを終了するには、[停止] をクリックします。



- **nslookup**:
  1. アクセスしようとしているアプリケーションの**IP**または**FQDN**を選択します。
  2. **nslookup**を選択します。
  3. テストを終了するには、[停止] をクリックします。

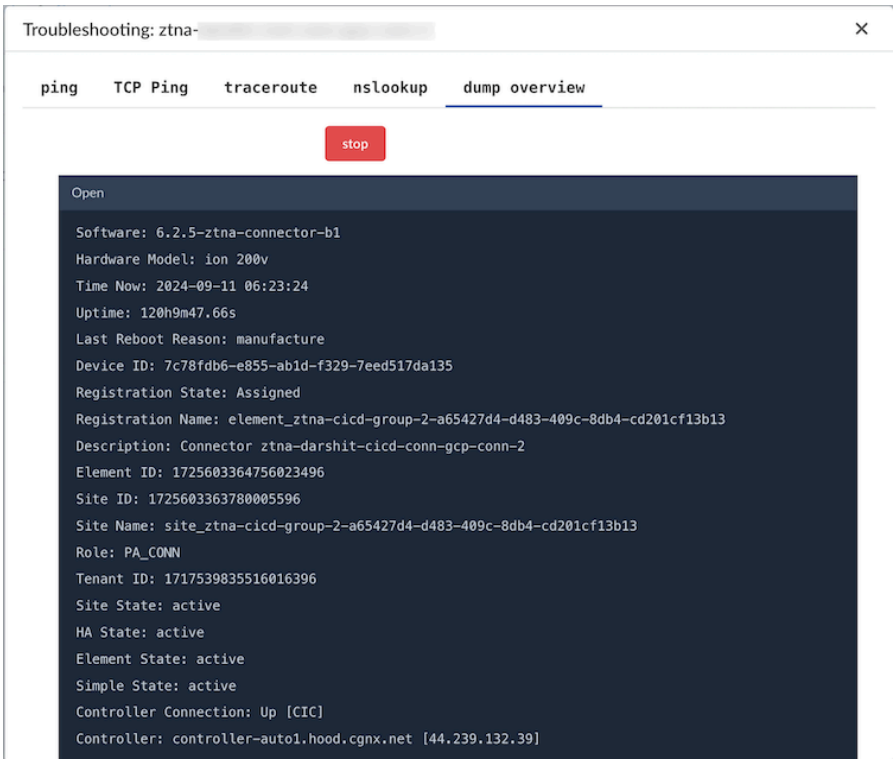
 ©2025 Palo Alto Networks, Inc.



- **dump**の概要:

  1. システムdumpをダウンロードするには [開始]をクリックし、ダウンロードを停止するには [停止] をクリックします。

     dumpの概要には、PANWのトラブルシューティングに必要なソフトウェア バージョン、インターフェースと接続の状態、およびコネクタの識別情報が表示されます。



パケット キャプチャ (pcap) の実行

ネットワーク レベルのトラブルシューティングのためにパケット キャプチャ (pcap) が必要な場合は、特定のコネクタからネットワーク データをキャプチャするパケット キャプチャを実行できます。特定のIPアドレスまたはプロトコル (TCP など) に基づいてパケットをキャプチャすることもできます。

パケット キャプチャは、次のユース ケースで役立ちます。

 ©2025 Palo Alto Networks, Inc.

- トンネルが立ち上がらない場合。コネクタとZTT間のIKEネゴシエーションをキャプチャすると、問題を特定するのに役立ちます。この場合は、 インターネット インターフェースを選択し、サービス接続の IP アドレスを送信元または宛先インターフェイスとして使用します。
- アプリがダウンした場合は、サーバーIPアドレスとデータ センター インターフェースのポートを使用してtcpdumpを取得することで、アプリのプローブを確認できます。
- エンドツーエンドのデータプレーンが機能していないが、トンネルは機能しており、アプリは起動している場合。このユースケースでは、アプリのファブリックIPアドレス宛てのIPSecトンネル上のユーザー トラフィックのtcpdumpを取得すると便利です。

STEP 1 | ワークフロー > **ZTNA**コネクタ > コネクタに移動します。

STEP 2 | トラブルシューティングするコネクタの パケット キャプチャ (虫眼鏡) を選択します。



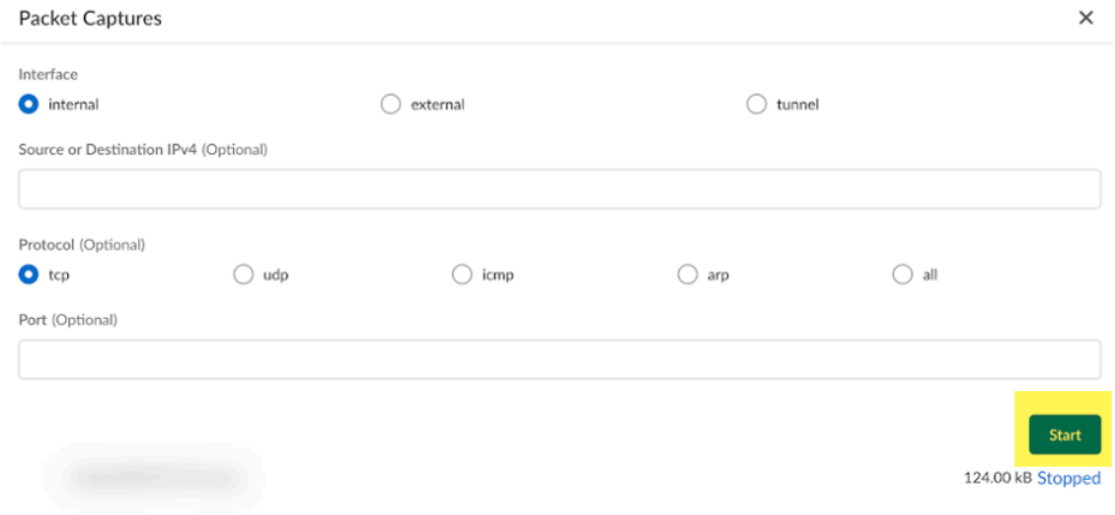
STEP 3 | パケットをキャプチャするインターフェース (内部、 外部、または トンネル)を選択します。

STEP 4 | (任意) パケットをキャプチャする 送信元または宛先 **IPv4** アドレスを指定します。
このオプションを指定すると、このIPアドレスからのパケットのみがキャプチャされます。

STEP 5 | (任意) キャプチャするパケットのタイプを選択します。
キャプチャする特定のプロトコルのパケット (**tcp**、**udp**、**icmp**、または **arp**) を選択するか、すべて を選択してすべてのパケットをキャプチャすることができます。

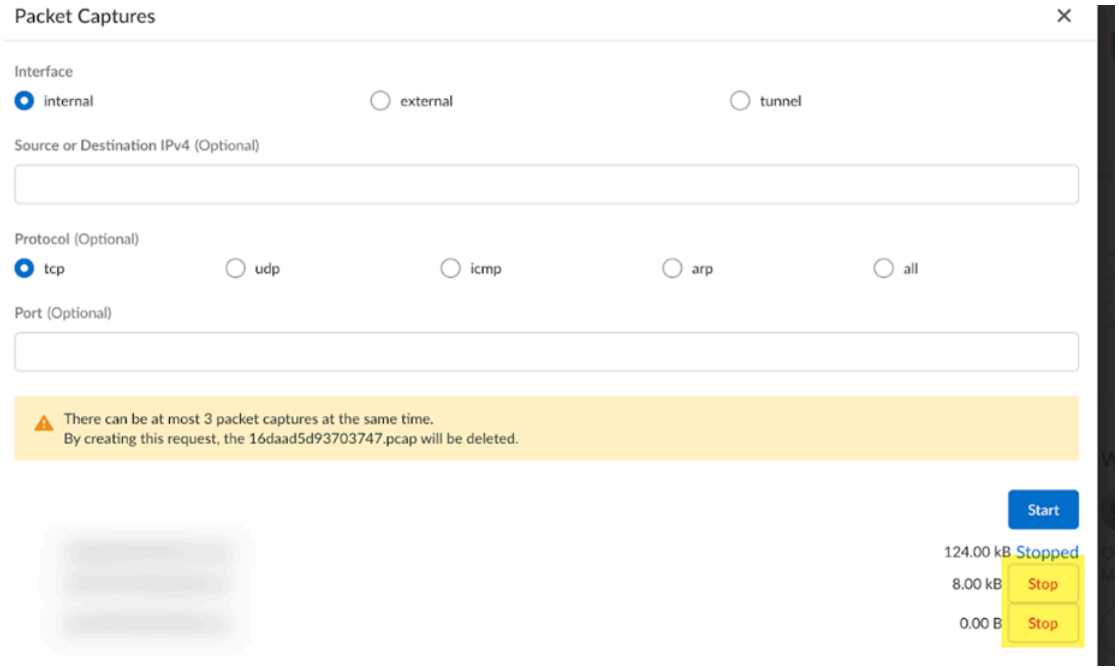
STEP 6 | (任意) パケットをキャプチャする ポート を選択します。
このオプションを指定すると、このポートからのパケットのみがキャプチャされます。

STEP 7 | パケットキャプチャを開始します 。



 ©2025 Palo Alto Networks, Inc.

STEP 8 | パケットキャプチャを停止するには、[停止]をクリックします。



- パケット キャプチャの最大ファイル サイズは5 MBです。最大サイズに達する前にキャプチャを停止しないと、ファイルは上書きされます。
- コネクタでは同時に最大3つのパケット キャプチャが許可されます。4番目のセッションが開始されると、実行中の最初のセッションは終了します。

テクニカル サポートファイルの収集

テクニカル サポート ファイルには、デバイス設定、システム情報、およびいくつかのログ (トラフィックではない) が含まれています。Palo Alto Networksでは、ZTNA Connectorの問題のトラブルシューティングを支援するために、テクニカル サポート ファイルのアップロードをリクエストする場合があります。

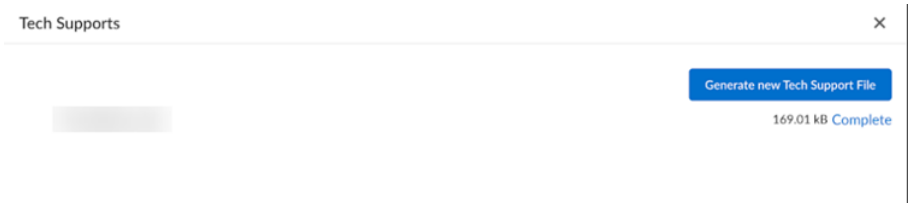
STEP 1 | ワークフロー > **ZTNA**コネクタ > コネクタに移動します。

STEP 2 | トラブルシューティングするコネクタの テクニカル サポート (手) を選択します。



 ©2025 Palo Alto Networks, Inc.

STEP 3 | 新しいテクニカル サポート ファイルを生成します。



STEP 4 | テクニカル サポート ファイルをローカルにダウンロードするには、[完了] を選択します。

©2025 Palo Alto Networks, Inc.

コネクタIPブロックの削除

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ ZTNA コネクタ アドオン ライセンス アドオン ライセンスを含む Essential ライセンスには、8つのZTNAコネクタ、100個のFQDN、および4つのIPサブネット機能が含まれます。 アドオン ライセンスを含む Advanced ライセンスには、40個の ZTNA コネクタ、300個のFQDN、および 1024 個のIPサブネット機能が含まれます。 アドオン ライセンスを含むプレミアム ライセンスには、200個のZTNAコネクタ、4000個のFQDN、および1024個のIPサブネット機能が含まれます。 ❑ ZTNAコネクタアドオンライセンスを購入しない場合は、 Prisma Accessライセンスには、4 つのコネクタ、40 個の FQDN、および 4 つの IP サブネットが含まれます。この機能は、ご使用の環境で ZTNA コネクタを試す目的で提供されています。

ZTNA コネクタを有効にするを行い、Prisma Accessがモバイル ユーザー、リモート ネットワーク、データセンター内のコネクタ VM 間のトラフィックをルーティングするために内部で使用する必要なコネクタIPブロックを追加します。以前は、コネクタIPブロックを作成した後に変更することはできませんでした。しかしコネクタIPブロックを削除または更新できるようになりました。ブロックを削除または更新するには、記載されている手順に従ってください。

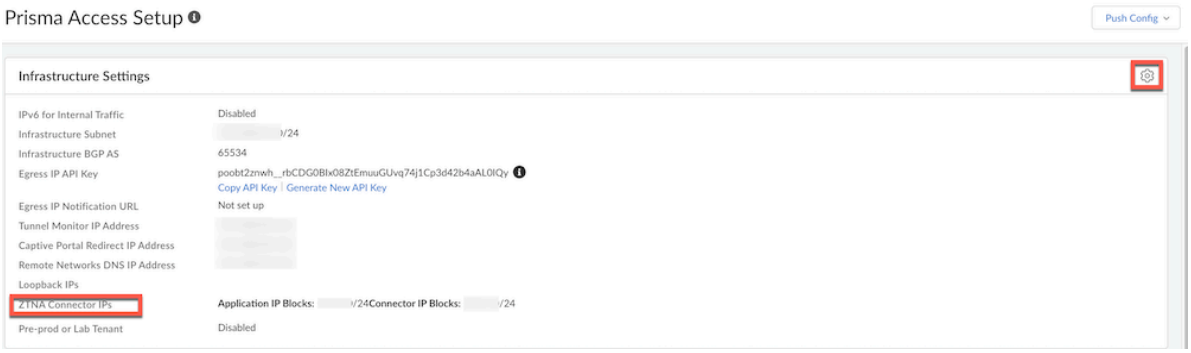
- Panorama
- Strata Cloud Manager

コネクタIPブロックの削除 (クラウド管理)

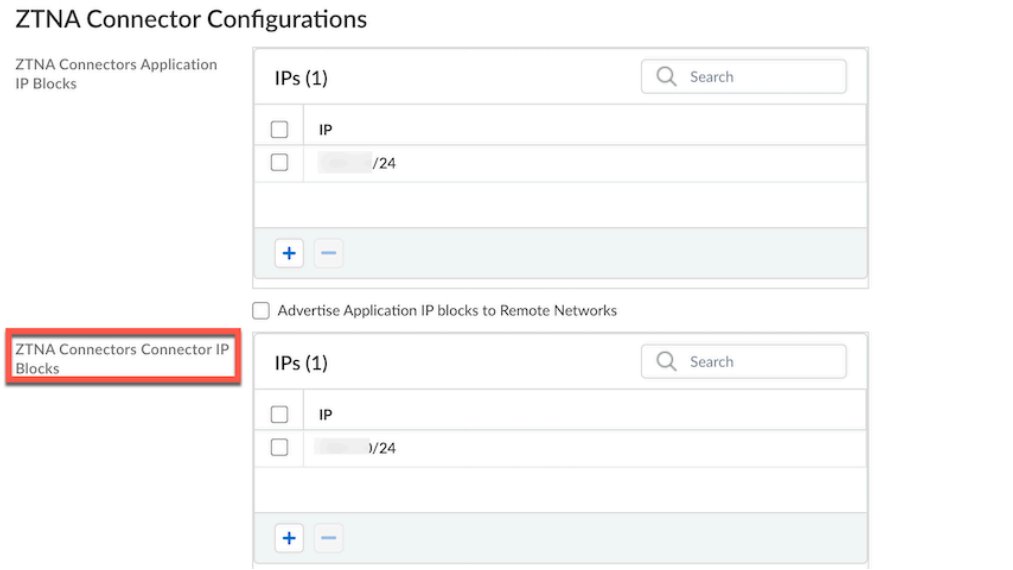
コネクタIPブロックを削除するには、次の手順を実行します。

©2025 Palo Alto Networks, Inc.

STEP 1 | [ワークフロー] > **[Prisma Access** セットアップ] > **[Prisma Access** > [インフラストラクチャ設定]に移動し、歯車をクリックして [設定]を編集します。



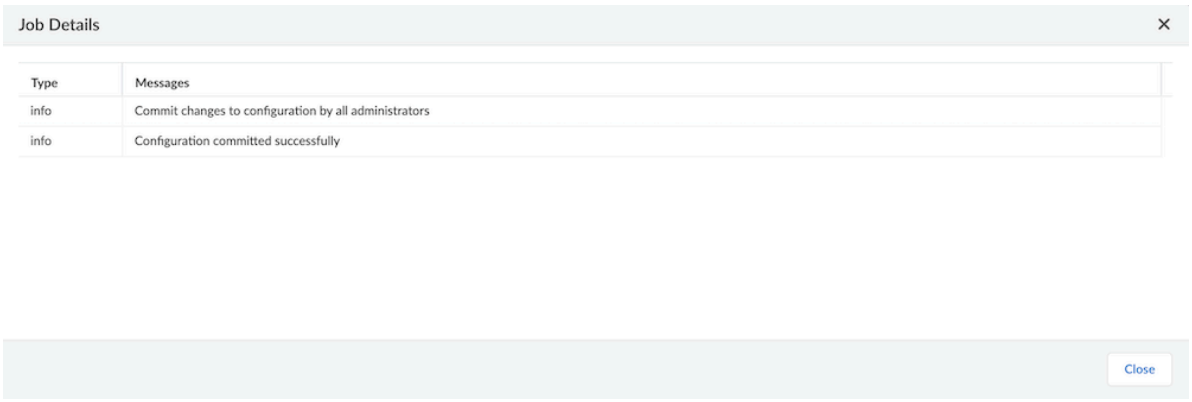
STEP 2 | **ZTNA** コネクタ構成 > **ZTNA** コネクタ コネクタ**IP**ブロックから、削除するコネクタ ブロックの横にあるチェック ボックスをオンにして、 保存をクリックします。



 ©2025 Palo Alto Networks, Inc.

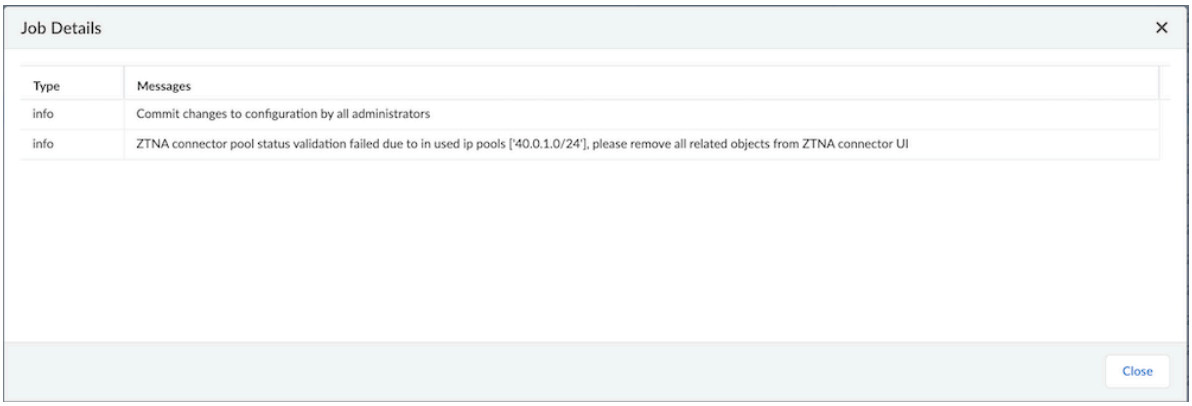
STEP 3 | 設定変更をコミットしてプッシュします。

コミットが成功するとメッセージが表示されます。



コネクタ、アプリケーション、ワイルドカード、コネクタ グループなどの ZTNA コネクタ オブジェクトを作成している場合、最初に ZTNA コネクタ オブジェクトを削除せずに コネクタ **IP** ブロック を削除しようとすると、コミットとプッシュは失敗します。

この場合は、ZTNA コネクタ オブジェクトを削除し、必要な コネクタ**IP**ブロックを削除してから、 コミットします。最初のコミットは失敗しますが、2番目のコミットは成功します。

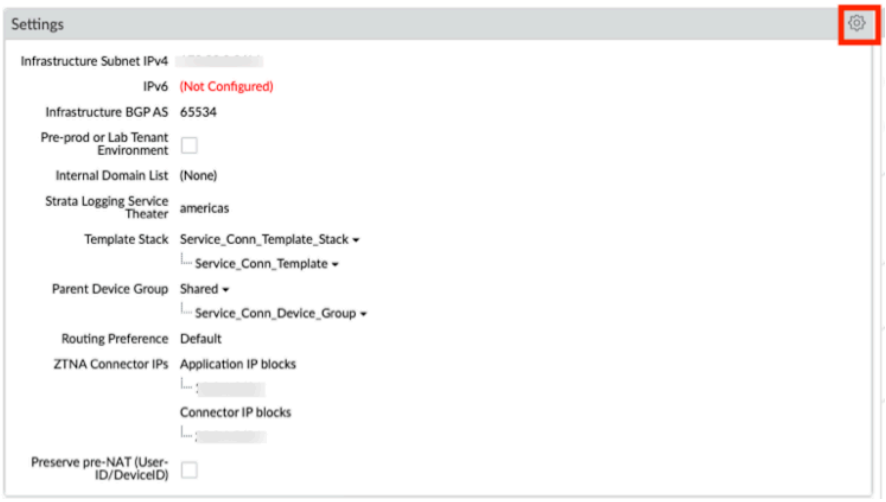


コネクタIPブロックの削除 (Panorama)

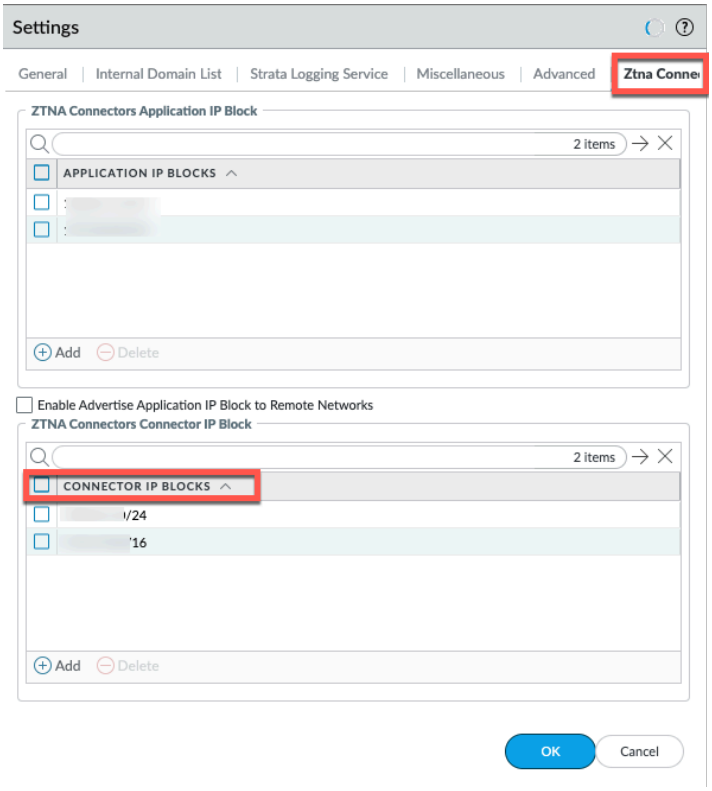
コネクタIPブロックを削除するには、次の手順を実行します。

©2025 Palo Alto Networks, Inc.

STEP 1 | **[Panorama] > [Cloud Services（クラウドサービス）] > [Configuration（設定）] > [Service Setup（サービスのセットアップ）]**の順に移動し、歯車型アイコンをクリックして**[設定]**を編集します。



STEP 2 | **[ZTNA**コネクタ**]**を有効にします。

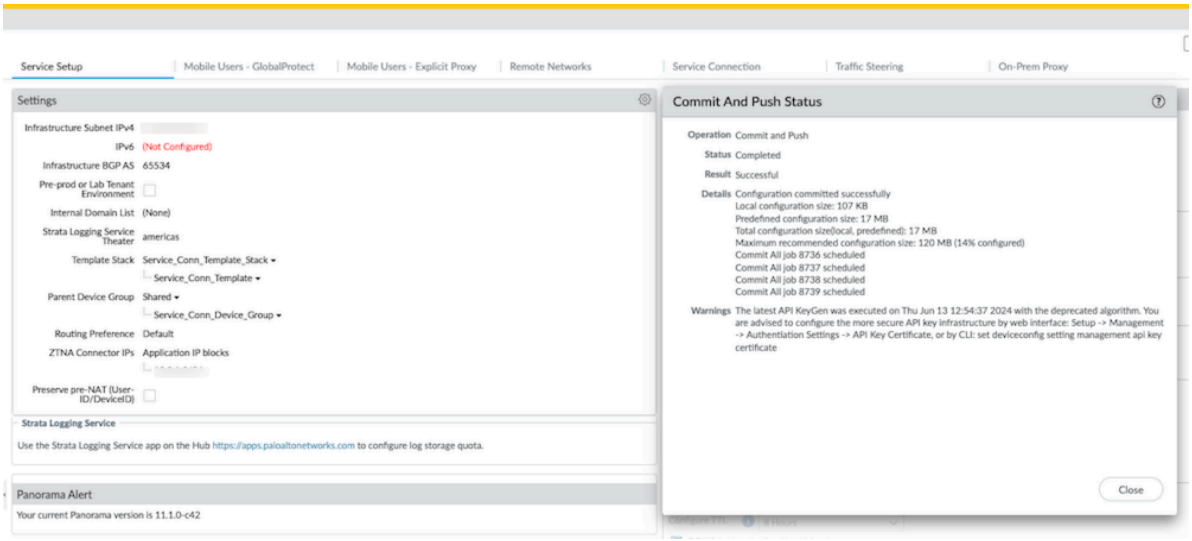


STEP 3 | 削除したいコネクターブロックの隣にあるチェック ボックスを選択し、**[OK]**をクリックして設定を保存します。

©2025 Palo Alto Networks, Inc.

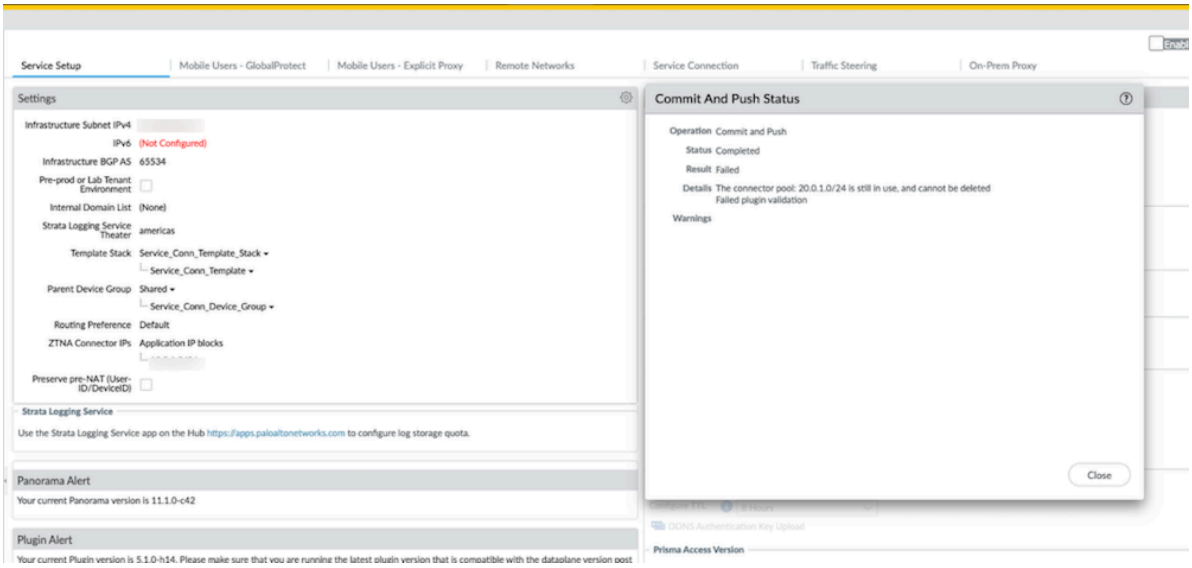
STEP 4 | 設定変更をコミットして設定変更をプッシュします。

コミットが通過すると、メッセージが表示されます。



以前にコネクタ、アプリケーション、ワイルドカード、コネクタグループなどのZTNAコネクタオブジェクトを作成しており、ZTNAコネクタオブジェクトを削除せずにコネクタ**IP**ブロックを削除しようとすると、コミットとプッシュに失敗します。

この場合、ZTNAコネクタオブジェクトを削除し、必要なコネクタ**IP**ブロックを削除してから、コミットして2回プッシュします。最初のコミットは失敗しますが、2回目は成功します。



 ©2025 Palo Alto Networks, Inc.

Cloud Identity Engineを使用してアプリケーションの自動検出を設定する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ ZTNA コネクタ アドオン ライセンス アドオン ライセンスを含む Essential ライセンスには、8つのZTNAコネクタ、100個のFQDN、および4つのIPサブネット機能が含まれます。 アドオン ライセンスを含む Advanced ライセンスには、40個の ZTNA コネクタ、300個のFQDN、および 1024 個のIPサブネット機能が含まれます。 アドオン ライセンスを含むプレミアム ライセンスには、200個のZTNAコネクタ、4000個のFQDN、および1024個のIPサブネット機能が含まれます。 ❑ ZTNAコネクタアドオンライセンスを購入しない場合は、 Prisma Accessライセンスには、4 つのコネクタ、40 個の FQDN、および 4 つの IP サブネットが含まれます。この機能は、ご使用の環境で ZTNA コネクタを試す目的で提供されています。

ZTNA コネクタが Azure Active Directory または Okta Directory で定義されているアプリケーションを自動検出するには、以下を構成する必要があります。

❑ ハブでCloud Identity Engine をアクティベートし 、最初のテナントを作成します。

Azureまたは Oktaでクラウドベースのディレクトリを構成するときは、**[Collect enterprise applications (**エンタープライズ アプリケーションの収集**)]** を選択する必要があります。

❑ Cloud Identity Engine がアクセスする ディレクトリ のタイプを選択します。

❑ Azure Active Directory(Azure AD) や Okta Directory などのクラウドベースのディレクトリを構成して、Cloud Identity Engine と通信します。

次の IdP は、アプリケーション検出での使用がサポートされています。

- Azure AD
- Okta

©2025 Palo Alto Networks, Inc.

プライベート アプリケーション ターゲットの検出

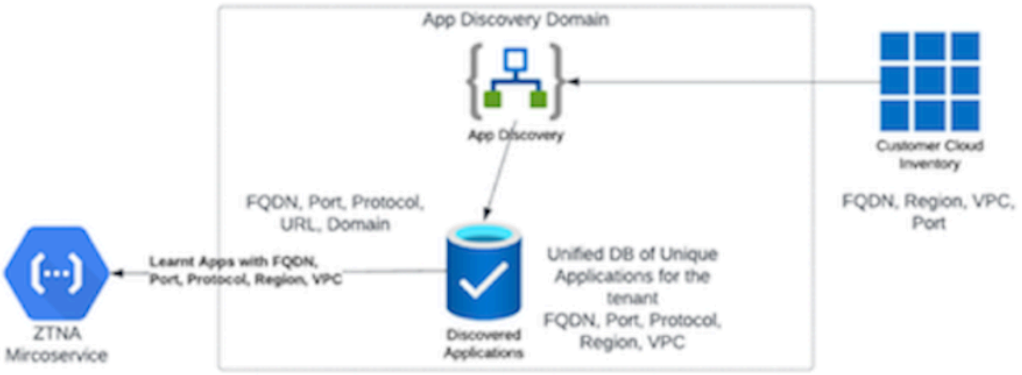
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ ZTNA コネクタ アドオン ライセンス アドオン ライセンスを含む Essential ライセンスには、8つのZTNAコネクタ、100個のFQDN、および4つのIPサブネット機能が含まれます。 アドオン ライセンスを含む Advanced ライセンスには、40個の ZTNA コネクタ、300個のFQDN、および 1024 個のIPサブネット機能が含まれます。 アドオン ライセンスを含むプレミアム ライセンスには、200個のZTNAコネクタ、4000個のFQDN、および1024個のIPサブネット機能が含まれます。 ❑ ZTNAコネクタアドオンライセンスを購入しない場合は、 Prisma Accessライセンスには、4 つのコネクタ、40 個の FQDN、および 4 つの IP サブネットが含まれます。この機能は、ご使用の環境で ZTNA コネクタを試す目的で提供されています。

最新のネットワーキング インフラストラクチャでは、何千ものプライベートアプリケーションがオンプレミスとマルチクラウドデータセンターにデプロイされています。ネットワーキングチームは、ネットワーク内またはネットワーク内の特定のサブネット内で実行されているアプリケーションを認識していないため、アプリケーションの可視性が失われます。

アプリケーションへの安全なアクセスを提供するには、FQDN、ポート、アプリケーションを手動で入力し、このアプリケーションが他のアプリケーションに依存していることを確認する必要があります。

プライベート アプリケーション ターゲット検出は、クラウド環境でホストされているアプリケーションを検出する方法を提供し、それらのアプリケーションをZTNAコネクタ ソリューションにオンボーディングできるようにします。また、クラウド プロバイダー ネットワークに接続し、検出を行い、データベースに保存します。また、検出されたアプリケーションを取得するためのさまざまなサービスへのAPIも提供します。ユーザーがZTNAコネクタではなくサービス接続のみを持っている場合は、アプリケーション ターゲットのみが検出されます。

©2025 Palo Alto Networks, Inc.



プライベート アプリケーション ターゲットの検出では、次のものが識別されます。

- FQDN
- アプリケーションのポート
- アプリケーションのプロトコル

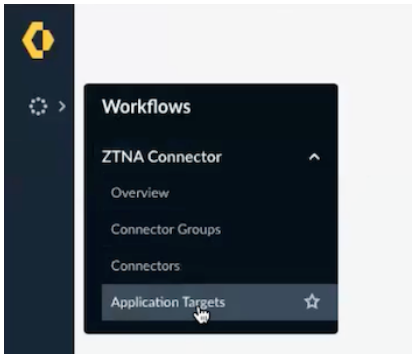
プライベート アプリケーション ディスカバリー機能を有効にする前に、必ずクラウド アイデンティティ エンジン（*CIE*）を有効にしてください。

AWSにクラウド アカウントと IAM ロールを追加し、ターゲット アプリケーションを検出するには、次の手順を実行します。

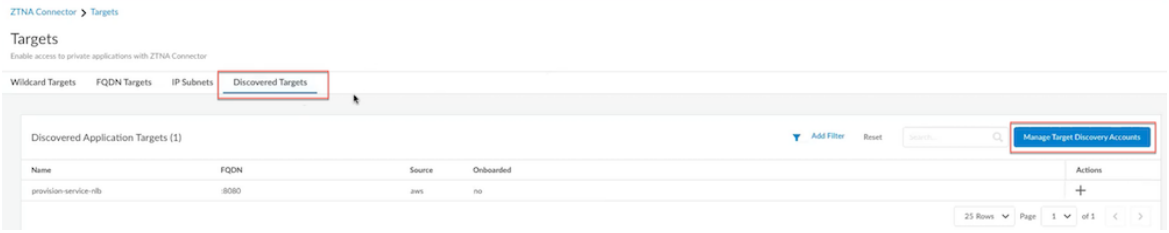
©2025 Palo Alto Networks, Inc.

STEP 1 | CloudFormation テンプレート (CFT) を取得して、クラウド アカウントを追加します。

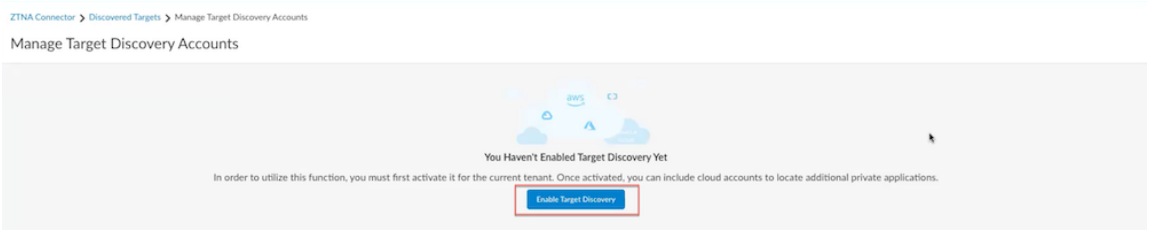
1. **[Application Targets (アプリケーションターゲット)]([Workflows (ワークフロー)] > [ZTNA Connector (ZTNAコネクタ)] > [Application Targets (アプリケーション ターゲット)])**に移動します。



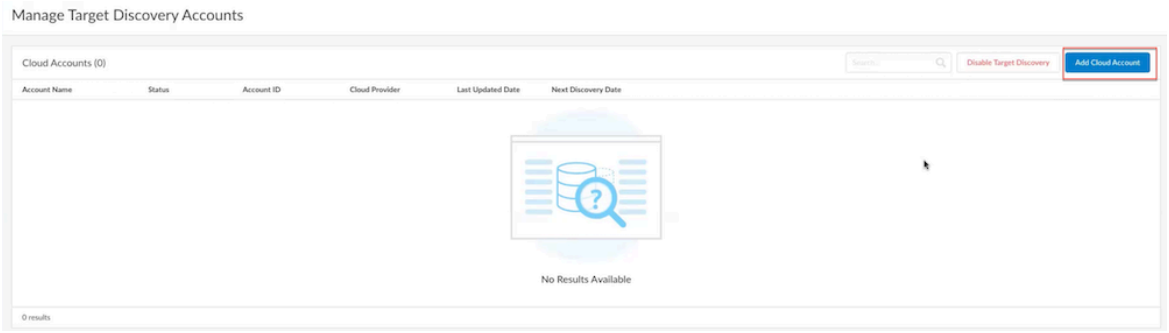
2. **[Application Targets**（アプリケーションターゲット）]ページで、**[Discovered Targets**（検出されたターゲット）]を選択し、**[Manage Target Discovery Accounts**（ターゲット検出アカウントの管理）]を選択します。



3. **[Enable Target Discovery (**ターゲット検出を有効**)]** を選択し、**[Enable (**有効**)]**を選択します。



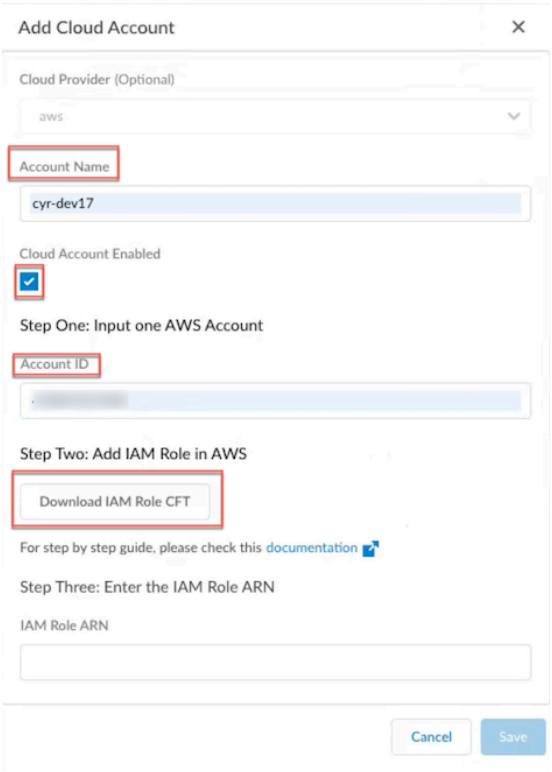
4. **[Manage Target Discovery Accounts (Target Discovery** アカウントの管理**)]** ページで、**[Add Cloud Account (**クラウドアカウントを追加**)]**を選択します。



5. **[Account Name**（アカウント名）]を追加し、**[Cloud Account Enabled**（クラウドアカウント有効）]のチェック ボックスをクリックします。AWS [Account ID (アカウン

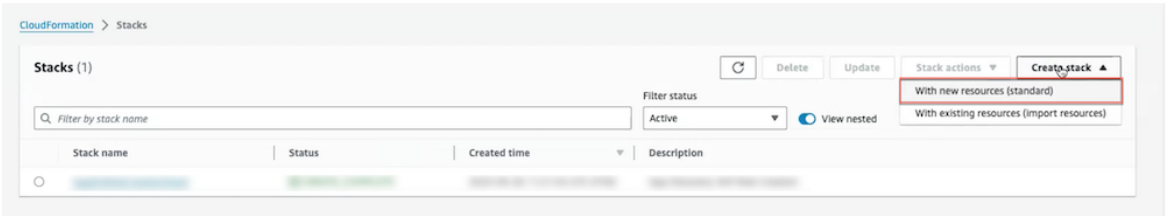
 ©2025 Palo Alto Networks, Inc.

トID)]を追加し、[Download IAM Role CFT (IAMロールCFTのダウンロード)] をクリックしてファイルをダウンロードします。



STEP 2 | AWSでIAM ロールを作成します。

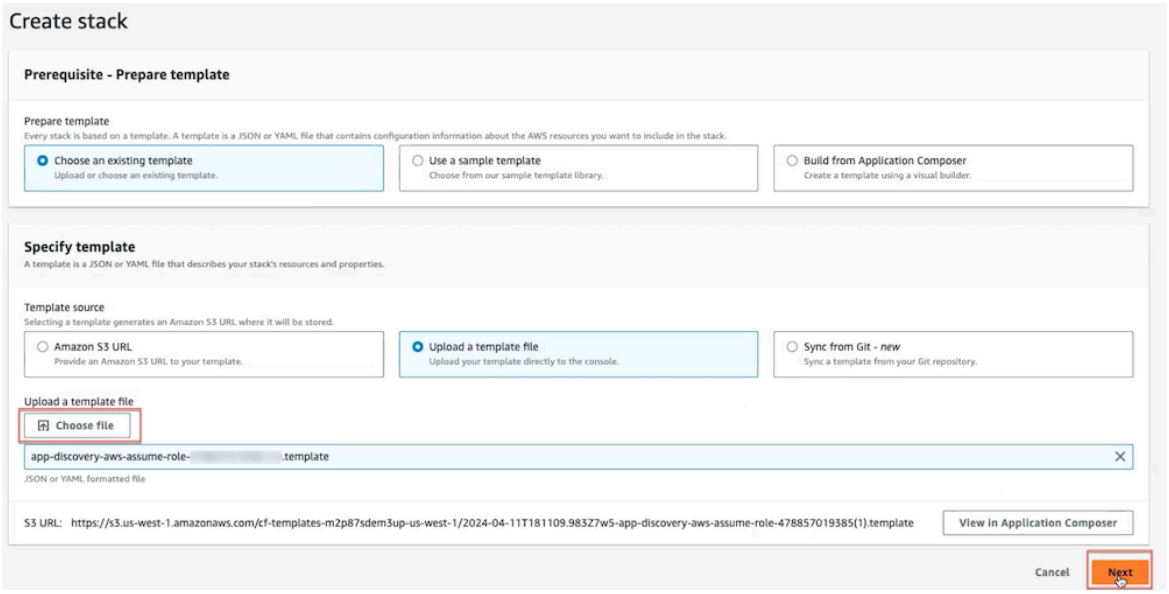
1. AWSアプリケーションに移動し、アカウントを選択しサインインします。
2. **[CloudFormation]** > [スタック] > [スタックの作成] > [新しいリソース**(標準)]**に移動し、スタックを作成します。



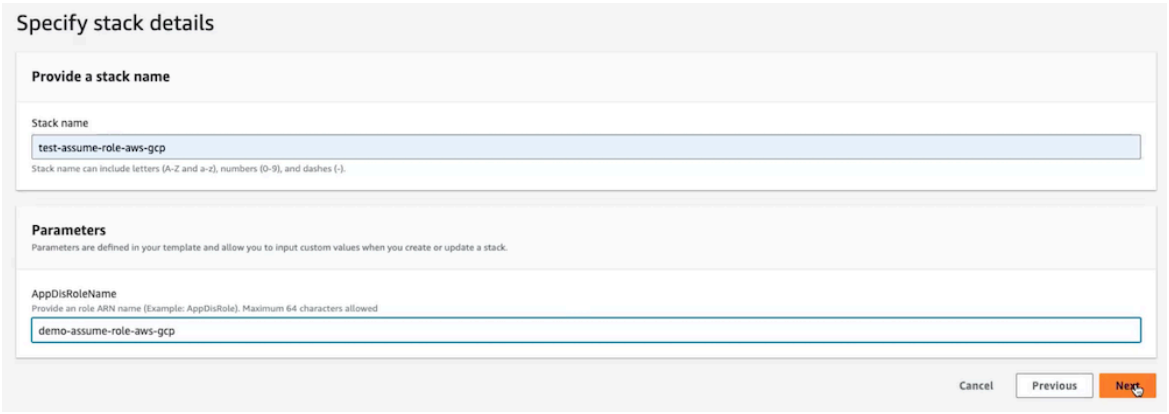
3. **[Create stack (**スタックの作成**)]** ページで、**[Prerequisite-Prepare template (**前提条件-テンプレートの準備**)]**の**[Choose an existing template (**既存のテンプレートを選択する**)]**を選択します。[テンプレートの指定]で、[テンプレートファイルのアップロード]を選択

 ©2025 Palo Alto Networks, Inc.

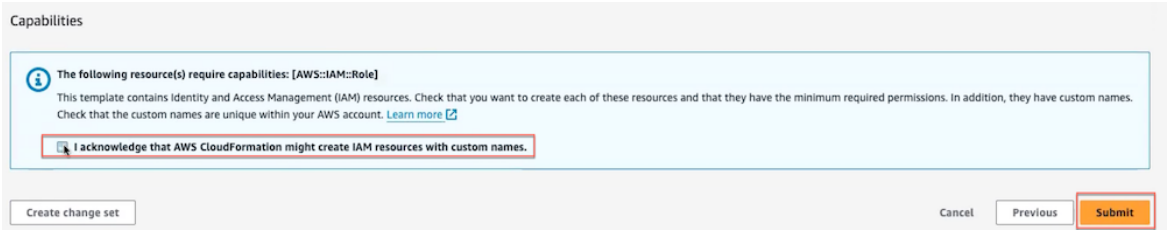
します。ステップ1で以前にダウンロードしたファイルをアップロードし、 [次へ]を選択します。



4. スタック名、**AppDisRoleName**を追加し、[次へ]を選択します。

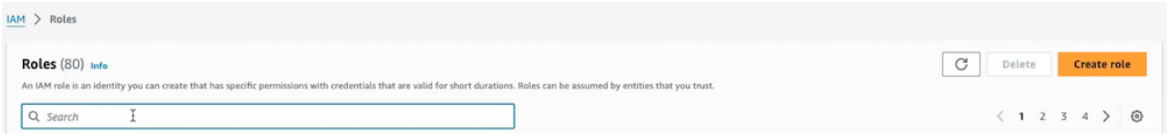


5. スタックオプションの設定 ページで、更新を行わず、 [次へ]を選択します。
6. 変更内容を確認します。カスタム名を持つIAMリソースの作成を承認するために、**[Capabilities (機能)]**の下にあるチェック ボックスを選択し、**[Submit (送信)]**を選択します。

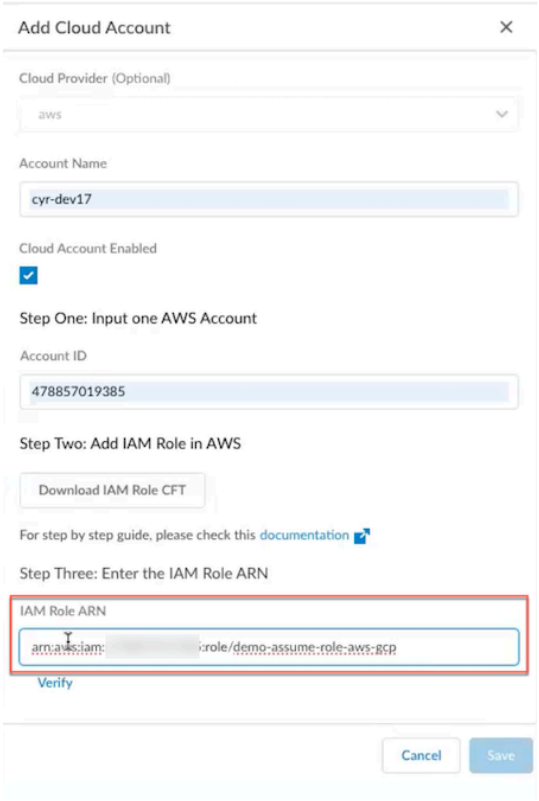


7. **IAM** > ロールに移動し、定義したロール名を検索します。ロール名を選択し、ロールの**ARN**をコピーします。

©2025 Palo Alto Networks, Inc.



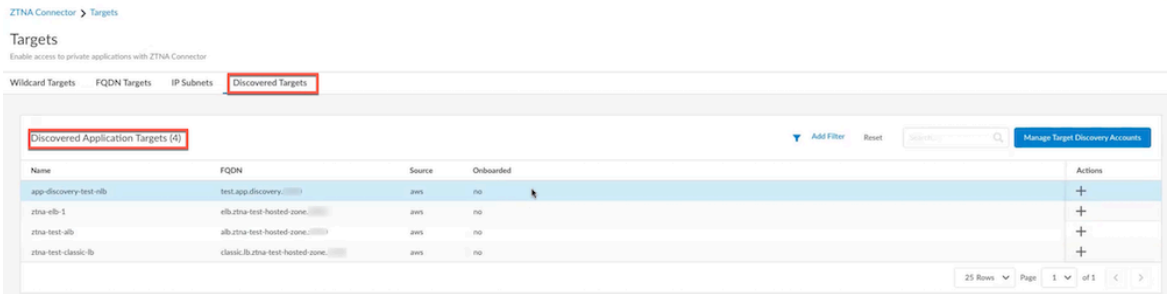
STEP 3 | **IAMロールARN**テキストフィールドにARNを貼り付け、**Verify (**検証)を選択します。ARNが検証されたら、 保存を選択します。



> ***IAM*ロール*ARN*** テキストフィールドに間違った *ARN* を追加した場合、検証は失敗し、エラーメッセージが表示されます。

アカウントを追加すると、ステータス、アカウント ID、その他の詳細を確認できます。検出の更新期間は24時間です。同じテナントに複数のアカウントを追加することもできます。

STEP 4 | 検出されたアプリを識別するには、**[Discovered Targets (**検出されたターゲット**)]**を選択します。検出されたアプリケーションのリストは、**[Discovered Application Targets (**検出されたアプリケーションターゲット**)]**の下にあります。

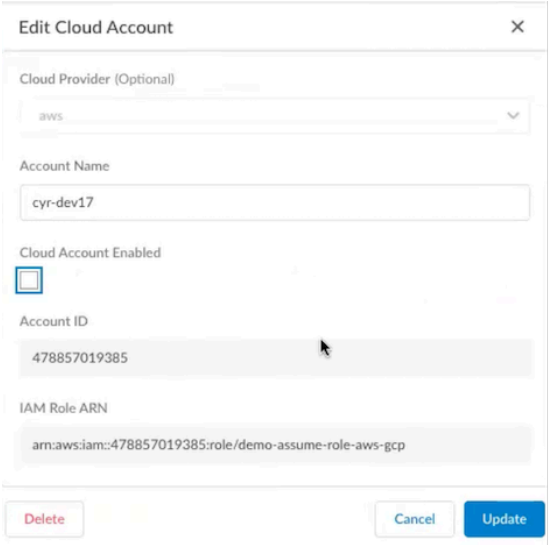


 ©2025 Palo Alto Networks, Inc.

STEP 5 | (任意) クラウドアカウントを削除します。

クラウドアカウントを削除し、ターゲット検出を無効にせずに新しいアカウントを追加するには、次の手順に従います。ただし、ターゲット検出機能を無効にする場合は、これらの手順が必須です。

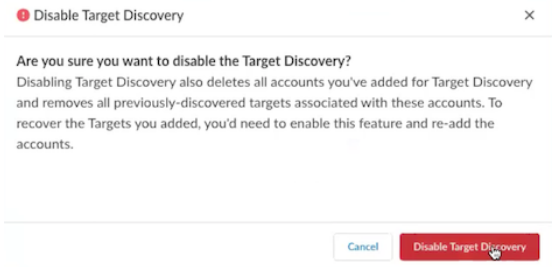
1. **[Target Discovery**アカウントの管理]で、 削除したい[アカウント名]をクリックします。
2. **[Cloud Account Enabled (**クラウドアカウントを有効)]を無効にし、[更新]を選択します。アカウントが更新されたら、 [削除]を選択します。アカウントが削除されます。



STEP 6 | (任意) ターゲット検出を無効にします。

ターゲット検出を無効にする前に、すべてのクラウド アカウントが削除されていることを確認してください。

1. [ターゲット検出の無効化]を選択し、 [ターゲット検出の無効化]を選択します。



 ©2025 Palo Alto Networks, Inc.

ZTNAコネクタ対応アプリのセキュリティ ポリシー

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ ZTNA コネクタ アドオン ライセンス アドオン ライセンスを含む Essential ライセンスには、8つのZTNAコネクタ、100個のFQDN、および4つのIPサブネット機能が含まれます。 アドオン ライセンスを含む Advanced ライセンスには、40個の ZTNA コネクタ、300個のFQDN、および 1024 個のIPサブネット機能が含まれます。 アドオン ライセンスを含むプレミアム ライセンスには、200個のZTNAコネクタ、4000個のFQDN、および1024個のIPサブネット機能が含まれます。 ❑ ZTNAコネクタアドオンライセンスを購入しない場合は、 Prisma Accessライセンスには、4 つのコネクタ、40 個の FQDN、および 4 つの IP サブネットが含まれます。この機能は、ご使用の環境で ZTNA コネクタを試す目的で提供されています。

ZTNA Connectorはポリシーを強制するのではなく、既存のPrisma Accessセキュリティ ポリシーをシームレスに拡張し、Prisma Accessを有効にするアプリケーションに適用します。つまり、すべてのアプリケーションとデータセンターで共通のポリシーを使用でき、ZTNA Connectorにオンボードされたアプリごとにセキュリティ ポリシーを個別に作成する必要がありません。

ただし、ZTNA コネクタのセットアップの一環として、セキュリティ ポリシーが次の点に該当することを確認する必要があります。

Prisma Accessと**ZTNA**コネクタ間のトラフィックを許可する

このため、ZTNAコネクタがPrisma Accessに接続できることを確認するために、ZTNA コネクタの要件とガイドラインに従ってください。

ユーザーは**ZTNA**コネクタの背後にあるアプリケーションにアクセスできます

ユーザーがZTNA Connectorアプリにアクセスできるようにするには、Prisma Accessを管理するために使用しているインターフェースについて、以下の手順に従ってください。

- Strata Cloud Manager
- Panorama

©2025 Palo Alto Networks, Inc.

ZTNAコネクタ対応アプリのセキュリティポリシー（Strata Cloud Manager）

ZTNA コネクタにアプリをオンボードした後、それらのアプリへのアクセスを許可および制御するためのポリシー ルールを設定する必要があります。ポリシーを作成して適用する手順は、アプリが ワイルドカード、IP サブネット、または FQDNで定義されているかどうかによって異なります。

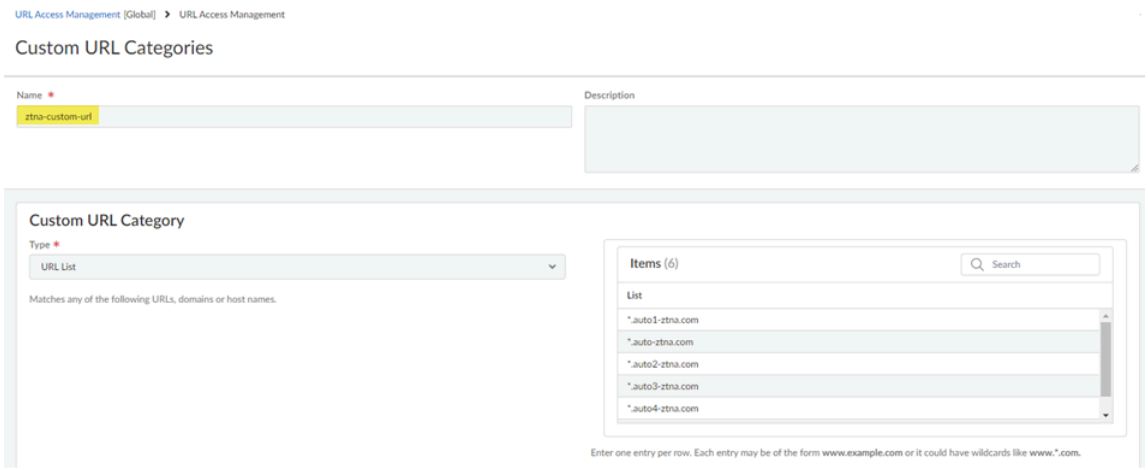
ワイルドカードベースのアプリのセキュリティポリシー

ワイルドカードベースのアプリ (**([設定] > [ZTNA コネクタ] > [アプリケーション ターゲット] > [ワイルドカード ターゲット])** では、カスタム URL カテゴリを作成する必要があります。ただし、このタイプのカテゴリでは、HTTP および HTTPS トラフィックに対してのみポリシーが適用され、その他のトラフィック (SSH など) は許可されません。このため、ZTNA コネクタ アプリケーション IP ブロックへのトラフィックを許可して、すべてのアプリへのアクセスを一時的に許可する必要があります。

ZTNA コネクタがワイルドカードに基づく FQDN を学習した後、アプリケーション IP ブロック トラフィックを許可するポリシーを無効にし、学習した FQDN に基づいてポリシー適用を適用できます。

STEP 1 | カスタム URL カテゴリを作成し、ワイルドカード URL をカテゴリに追加します。

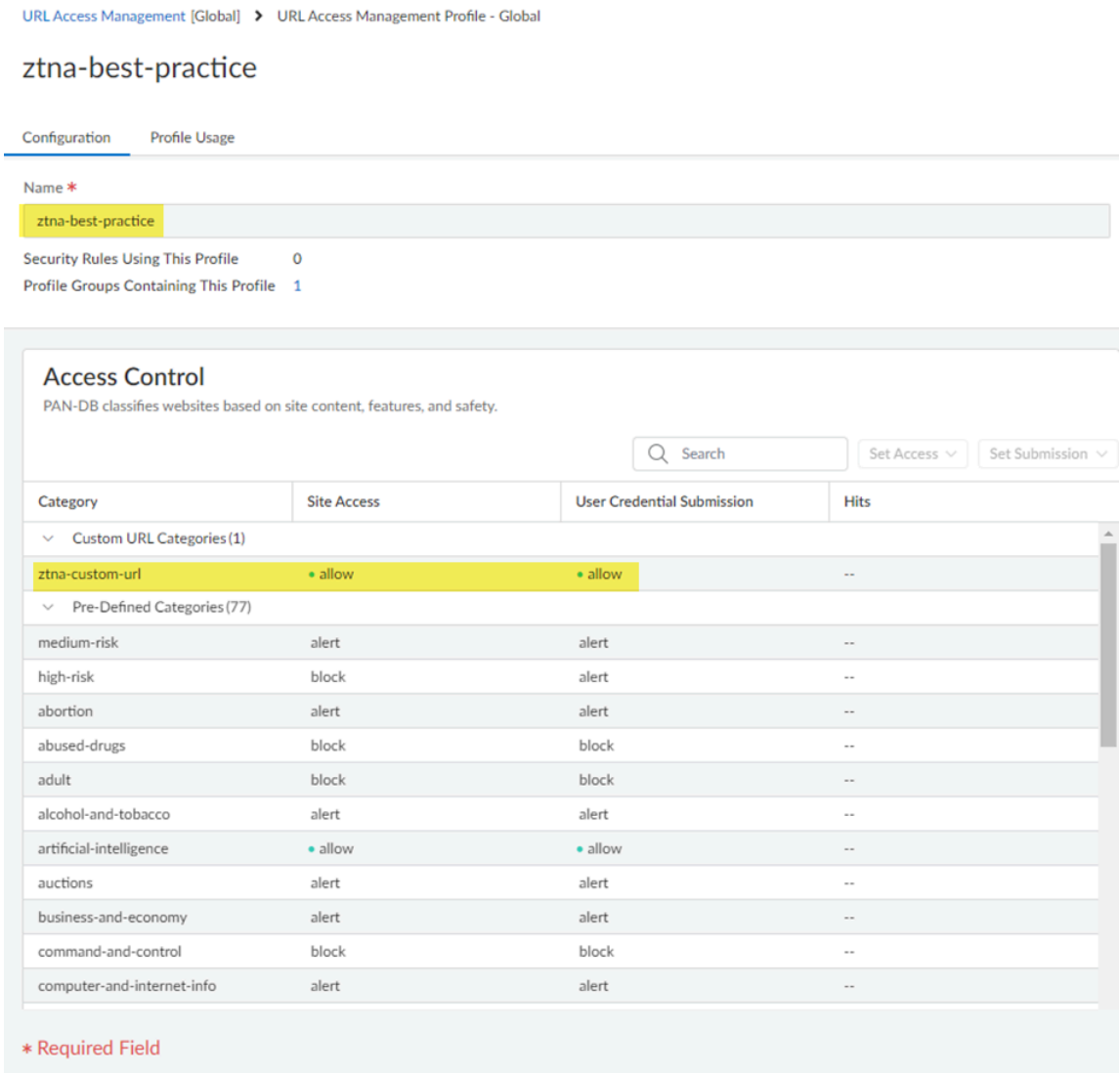
1. **[Manage (管理)] > [Configuration (設定)] > [NGFW and Prisma Access] > [Security Services (セキュリティサービス)] > [URL Access Management (URLアクセス管理)]**を順に移動します。
2. [カスタムURLカテゴリ]で**[Add Category (カテゴリを追加)]**します。
3. カスタム URL カテゴリにわかりやすい 名前 を付け、**URL** リストの タイプ を選択します。
4. ZTNA コネクタで作成したワイルドカード URL を アイテムに追加します。
5. 変更を保存します。



©2025 Palo Alto Networks, Inc.

STEP 2 | URL アクセス管理プロファイルを作成し、作成したカスタム URL カテゴリを追加します。

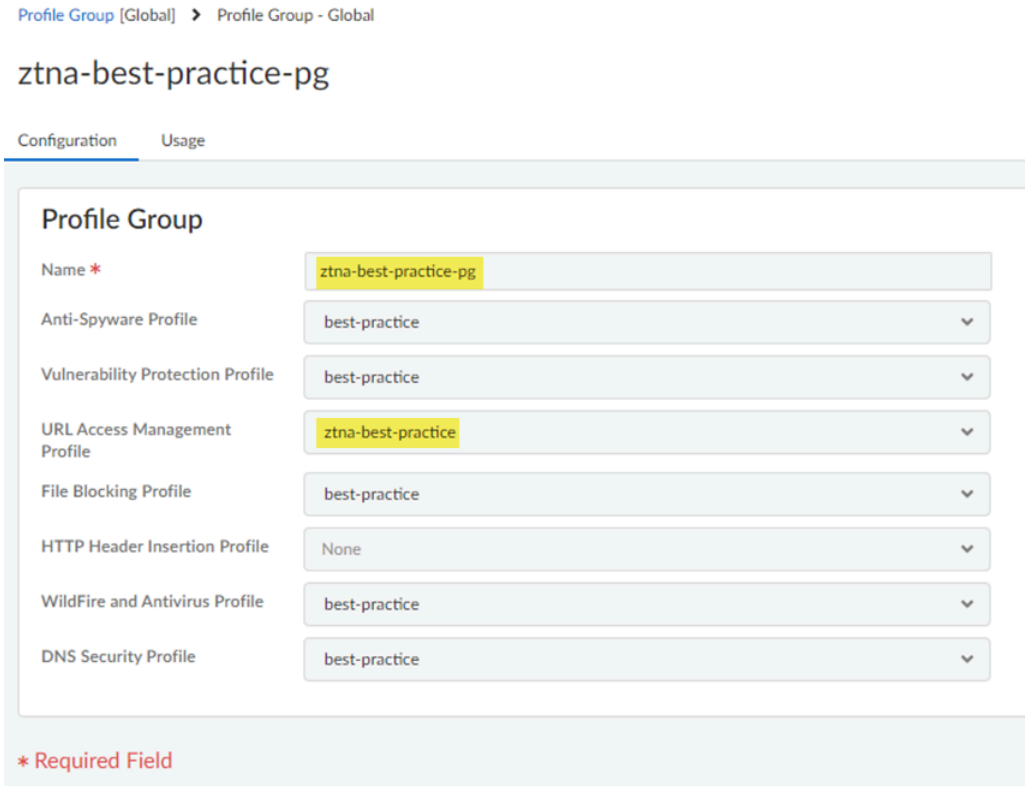
1. **URL** アクセス管理 領域にまだいる状態で、**URL** アクセス管理プロファイルを選択します。
2. 変更する既存のプロファイルを選択するか、［**Add Profile (**プロファイルの追加**)]**をクリックします。
3. 作成したカスタム URL カテゴリをプロファイルに追加します。
4. 次のパラメータを選択します。
   - サイトアクセス:Allow [許可]
   - ユーザー資格情報の送信:Allow [許可]
5. 変更を保存します。



©2025 Palo Alto Networks, Inc.

STEP 3 | プロファイル グループを作成し、URL アクセス管理プロファイルをグループに添付します。

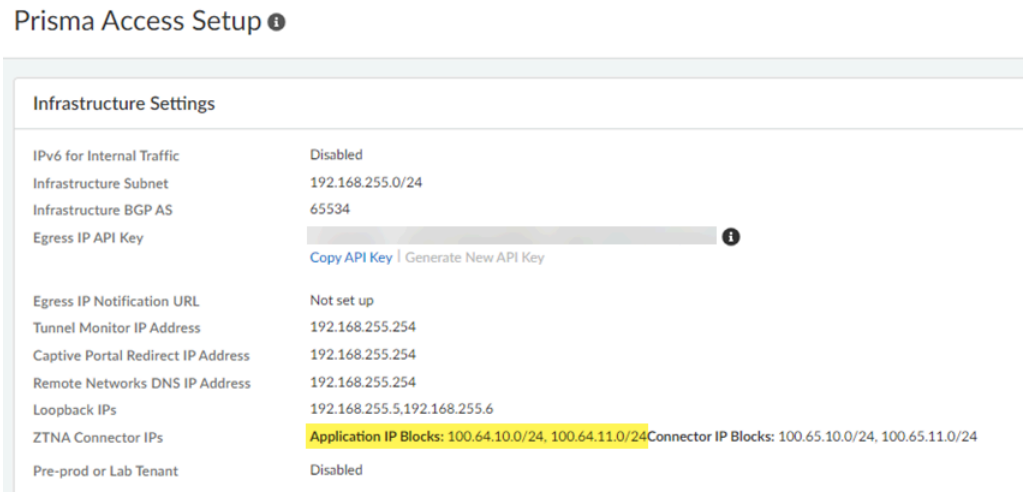
1. **[Configuration (設定)]** > **[NGFWとPrisma Access]** > **[Security Services (セキュリティサービス)]** > **[Profile Groups (プロファイルグループ)]**に移動します。
2. 作成した URL アクセス管理プロファイルを指定して、プロファイル グループを追加します 。



©2025 Palo Alto Networks, Inc.

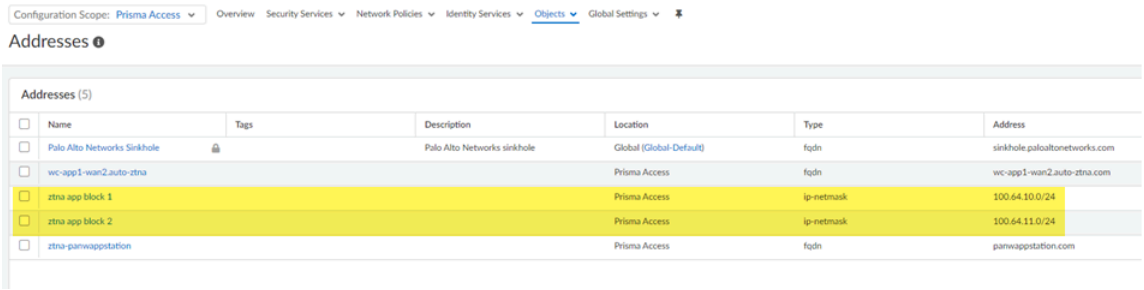
STEP 4 | ZTNA コネクタ アプリケーション IP ブロックのプロファイル グループと IP アドレスを許可するポリシーを作成します。

1. [ワークフロー] > [**Prisma Access** セットアップ] > [**Prisma Access**] > [**Prisma Access** セットアップ] に移動し、[ZTNA コネクタ IP] の下の [アプリケーション **IP** ブロック] をメモします。

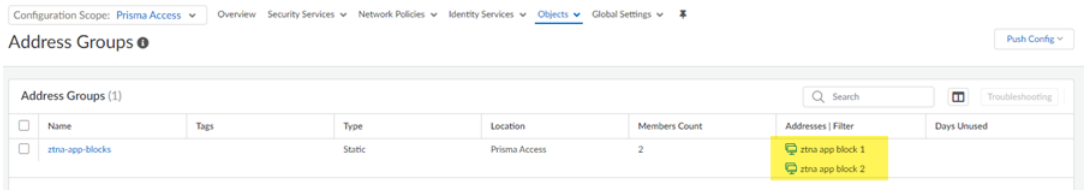


2. [構成の > 管理] > [**NGFW** および **Prisma Access** > オブジェクト] > [アドレス] > [アドレス] に移動し、取得した IP アドレスに基づいてアドレス オブジェクト を追加します 。

   IP サブネット ベースのアプリがある場合は、それらのサブネットのアドレス オブジェクトも作成します。



3. [構成の > 管理 > [**NGFW** および **Prisma Access** > オブジェクト] > [アドレス] > [アドレス グループ] に移動し、作成したアドレス オブジェクトをアドレス グループに 追加します 。



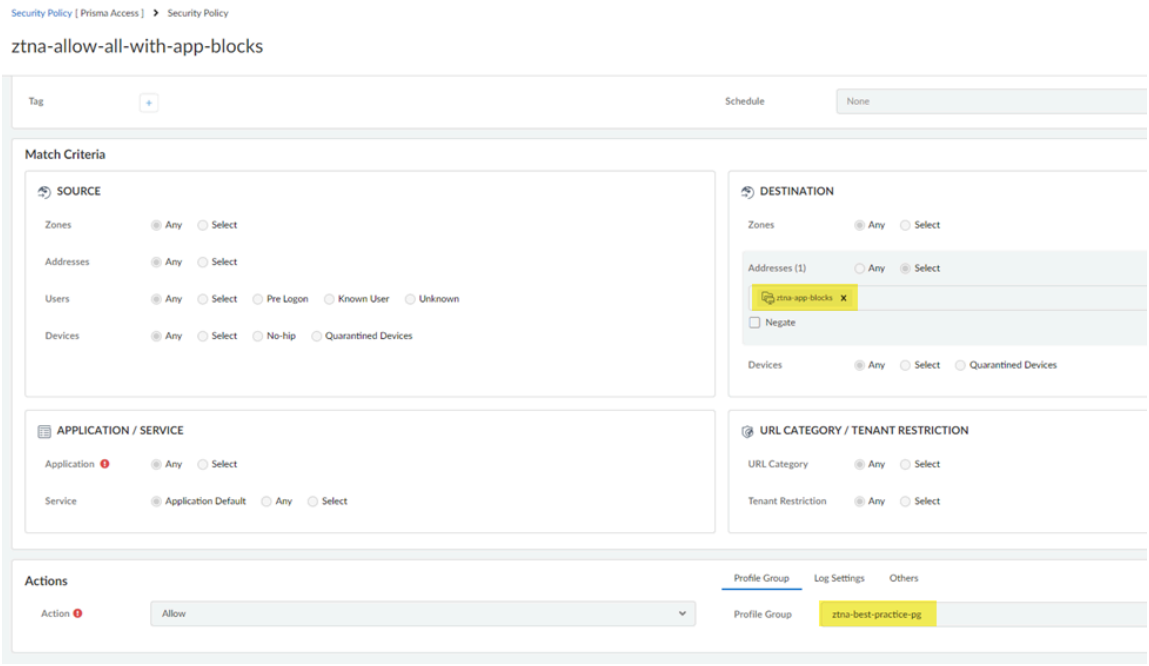
4. [構成の > 管理] > [**NGFW** および **Prisma Access** > セキュリティ サービス] > [セキュリティ ポリシー] > [事前ルール] に移動し、前の手順で作成した アドレス グループ と プ

©2025 Palo Alto Networks, Inc.

ロファイル グループ を指定して、すべてのアプリケーション IP アドレス ブロックへのアクセスを許可するセキュリティ ポリシーを 追加します。

このセキュリティ ポリシーを追加すると、ZTNA コネクタがワイルドカードに基づいてアプリを検出する間、ワイルドカード ベースのアプリ トラフィックからのすべてのトラフィックを通過できるようになります。アプリケーション IP ブロックを許可するルールがないと、ユーザーはワイルドカードベースのアプリにアクセスできません。

ZTNA コネクタがワイルドカードベースのアプリを検出するまで、このポリシーをそのままにしておくことができます。次に、このポリシーを無効にして、検出されたアプリごとにセキュリティ ポリシー ルールを追加することを選択できます。



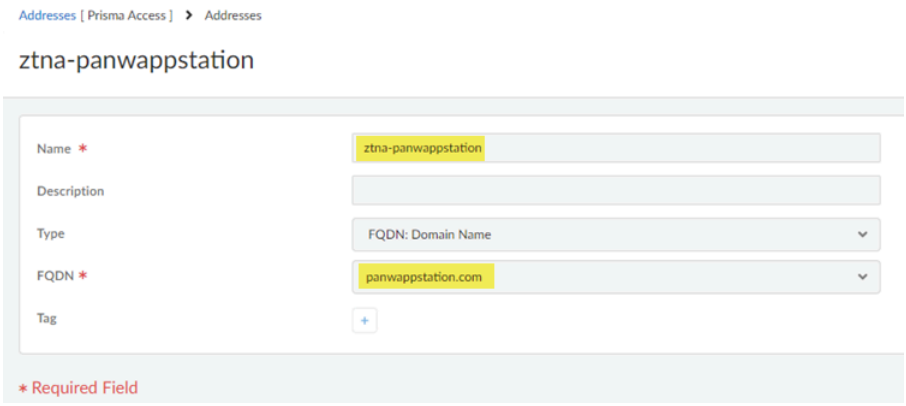
©2025 Palo Alto Networks, Inc.

STEP 5 | ZTNA コネクタがワイルドカードに基づいてアプリを検出したら、FQDN を使用して追加したアプリのセキュリティ ポリシーを構成します。

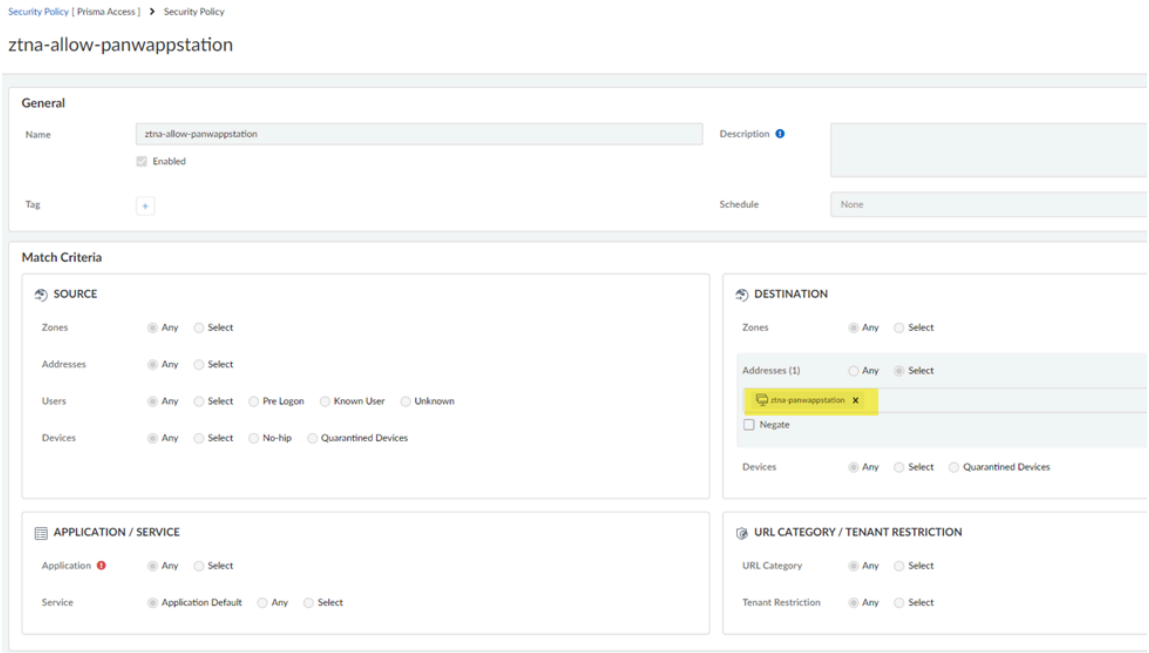
1. [ワークフロー] > **[ZTNA** コネクタ] > [アプリケーション ターゲット] > **[FQDN** ターゲット] に移動し、アプリで使用される FQDN をメモします。
2. FQDN のアドレス オブジェクトを作成します ([構成の > 管理] > **[NGFW** および **Prisma Access** > オブジェクト] > [アドレス] > [アドレス])。

   Prisma Access の 構成範囲を選択します。
3. **FQDN** タイプのアドレス オブジェクトを追加します：**Domain Name**と入力し、検出されたアプリケーションの**FQDN**を入力する。

   FQDN ターゲットの FQDN を入力します。



4. [構成の > 管理] > **[NGFW** および **Prisma Access** > セキュリティ サービス] > [セキュリティ ポリシー > 事前ルール] に移動し、検出されたアプリへのアクセスを許可するセキュリティ ポリシーを追加します 。



 ©2025 Palo Alto Networks, Inc.

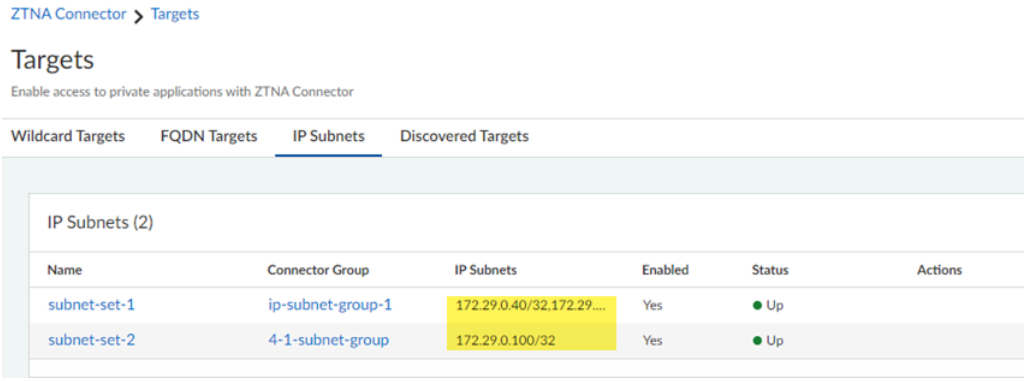
STEP 6 | 設定の変更を保存してプッシュするには、 **[Push Config (設定をプッシュ)]**をクリックします 。

STEP 7 | (任意) FQDN に基づいてセキュリティ ポリシーを作成した後、IP アプリケーション ブロックに基づくポリシーを削除します。

IP サブネットベースのアプリのセキュリティ ポリシー

IP サブネットに基づいて ZTNA コネクタ アプリケーション ターゲットを作成した場合 (**[設定] > [ZTNA コネクタ] > [コネクタ] > [アプリケーション ターゲット] > [IP サブネット]**)、次の手順を実行してアプリへのアクセスを許可します。

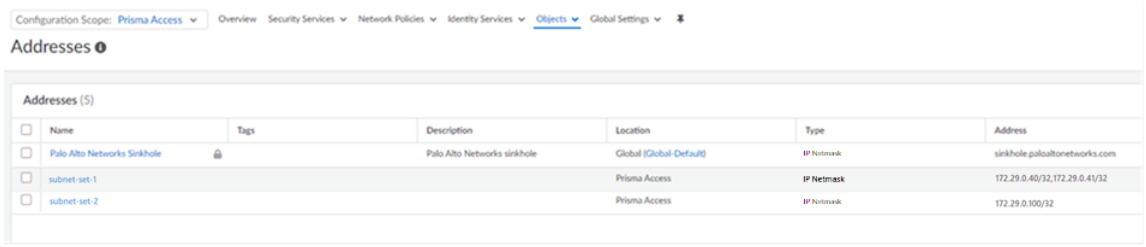
STEP 1 | **[ワークフロー] > > [ZTNA コネクタ] > [アプリケーション ターゲット] > [IP サブネット]** に移動し、アプリで使用される IP サブネットをメモします。



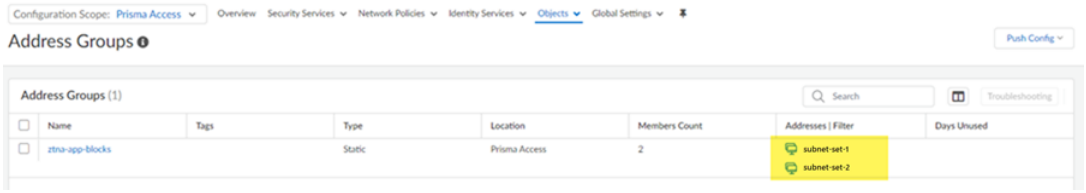
©2025 Palo Alto Networks, Inc.

STEP 2 | アプリに使用される IP サブネットの IP アドレスを許可するポリシーを作成します。

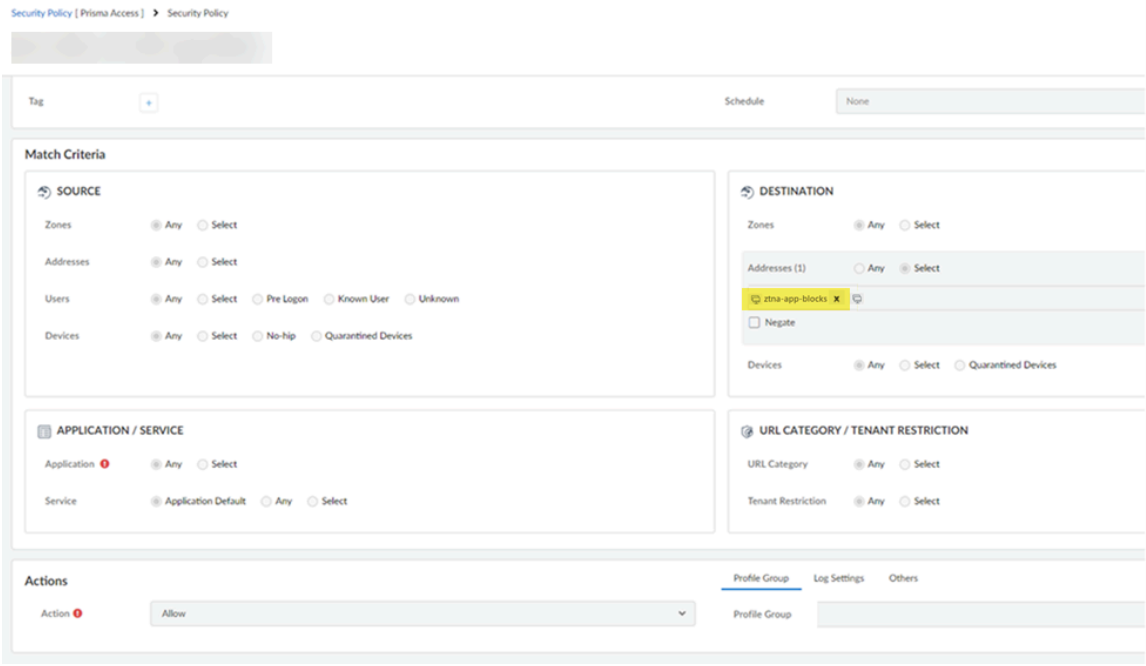
1. [構成 > 管理] > [**NGFW** および **Prisma Access** > オブジェクト] > [アドレス] > [アドレス] に移動し、取得した IP アドレスに基づいてアドレス オブジェクト を追加します 。



2. [構成 > 管理] > [**NGFW** および **Prisma Access** > オブジェクト] > [アドレス] > [アドレス グループ] に移動し、作成したアドレスをアドレス グループに 追加します 。



3. [構成 > 管理] > [**NGFW** および **Prisma Access**] > [セキュリティ サービス] > [セキュリティ ポリシー > の事前ルール] に移動し、前の手順で作成した アドレス を指定し て 、アプリの IP サブネットへのアクセスを許可するセキュリティ ポリシーを追加します。



STEP 3 | 設定の変更を保存してプッシュするには、 **[Push Config (設定をプッシュ)]**をクリックします 。

 ©2025 Palo Alto Networks, Inc.

FQDN ベースのアプリのセキュリティ ポリシー

FQDN に基づいてターゲットを追加した場合 ([設定] > [**ZTNA** コネクタ] > [コネクタ] > [アプリケーション ターゲット] > [**FQDN** ターゲット)、次の手順を実行して、アプリへのアクセスを許可するアドレス オブジェクトとセキュリティ ポリシーを作成します。

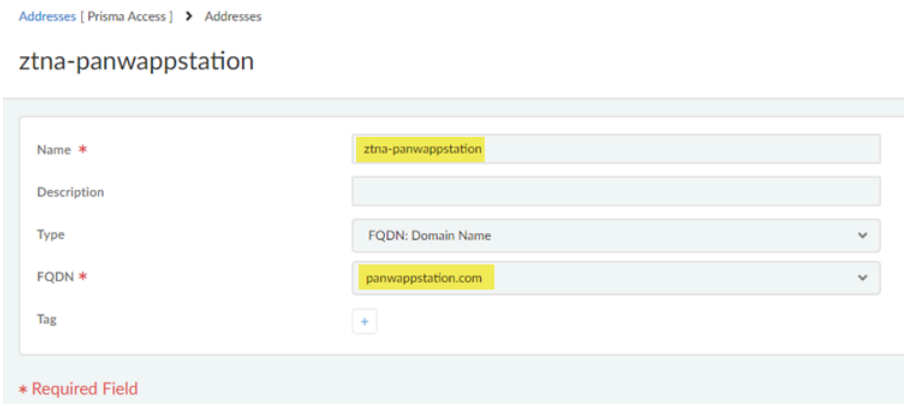
©2025 Palo Alto Networks, Inc.

STEP 1 | FQDN を使用して追加したアプリのセキュリティ ポリシーを構成します。

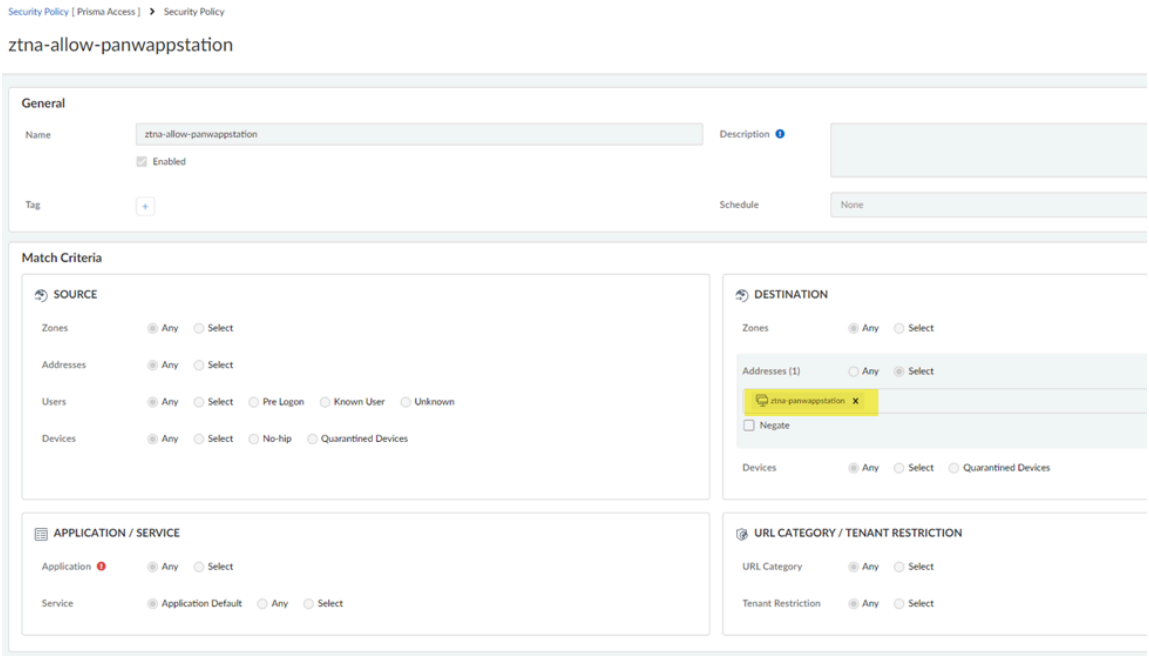
1. [ワークフロー] > **[ZTNA** コネクタ] > [アプリケーション ターゲット] > **[FQDN** ターゲット] に移動し、アプリで使用される FQDN をメモします。
2. FQDN のアドレス オブジェクトを作成します ([構成の > 管理] > **[NGFW** および **Prisma Access** > オブジェクト] > [アドレス] > [アドレス])。

   Prisma Access の 構成範囲を選択します。
3. **FQDN** タイプ のアドレス オブジェクトを追加します：**Domain Name**と入力し、検出されたアプリケーションの**FQDN**を入力する。

   検出されたすべてのアプリの FQDN を入力します。



4. 任意: **[構成の > 管理] > [NGFW** および **Prisma Access]** > [セキュリティ サービス] > [セキュリティ ポリシー > 事前ルール] に移動し、検出されたアプリへのアクセスを許可するセキュリティ ポリシーを追加します 。



STEP 2 | 設定の変更を保存してプッシュするには、 **[Push Config (**設定をプッシュ**)]**をクリックします 。

©2025 Palo Alto Networks, Inc.

ZTNAコネクタ対応アプリのセキュリティポリシー（Panorama）

ZTNA コネクタにアプリをオンボードした後、それらのアプリへのアクセスを許可および制御するためのポリシー ルールを設定する必要があります。ポリシーを作成して適用する手順は、アプリが ワイルドカード、IP サブネット、または FQDNで定義されているかどうかによって異なります。

ワイルドカードベースのアプリのセキュリティポリシー

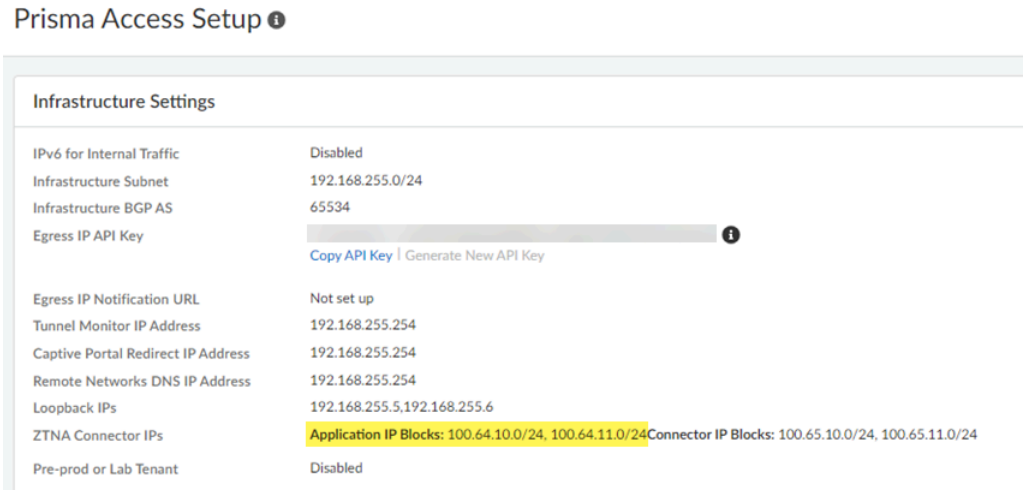
ワイルドカードベースのアプリ (([設定] > [**ZTNA** コネクタ] > [アプリケーション ターゲット] > [ワイルドカード ターゲット]) では、カスタム URL カテゴリを作成する必要があります。ただし、このタイプのカテゴリでは、HTTP および HTTPS トラフィックに対してのみポリシーが適用され、その他のトラフィック (SSH など) は許可されません。このため、ZTNA コネクタ アプリケーション IP ブロックへのトラフィックを許可して、すべてのアプリへのアクセスを一時的に許可する必要があります。

ZTNA コネクタがワイルドカードに基づく FQDN を学習した後、アプリケーション IP ブロック トラフィックを許可するポリシーを無効にし、学習した FQDN に基づいてポリシー適用を適用できます。

©2025 Palo Alto Networks, Inc.

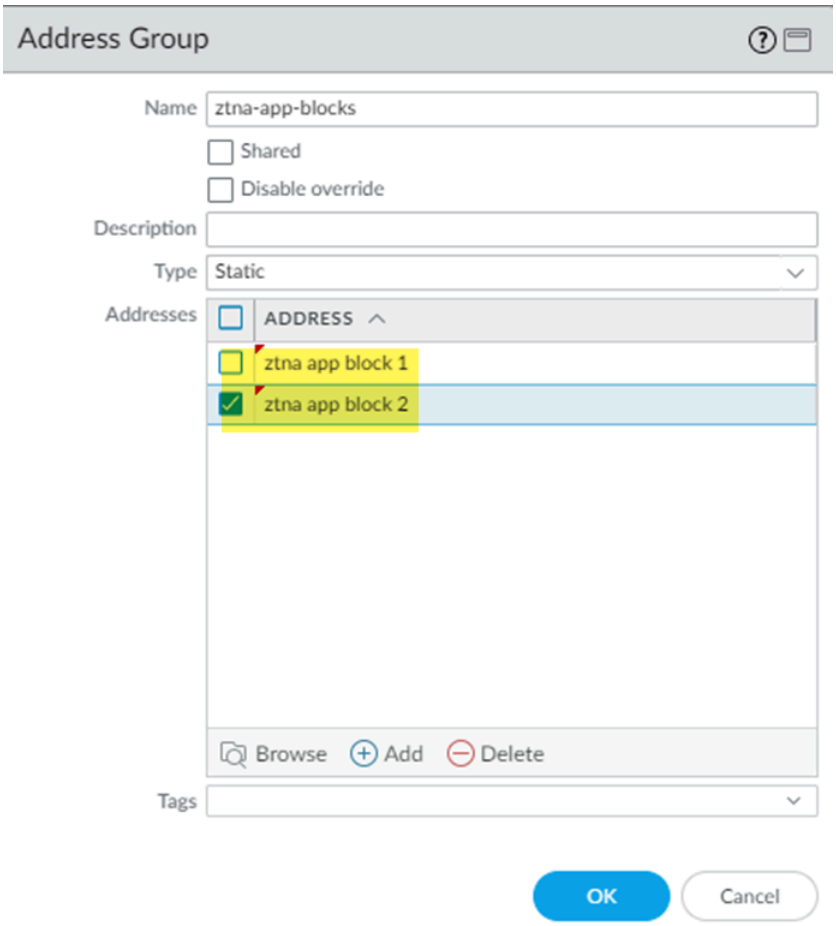
STEP 1 | ZTNA コネクタ アプリケーション IP ブロックの IP アドレスを許可するポリシーを作成します。

1. ZTNA Connector UIから、[ワークフロー] > **[Prisma Access** セットアップ] > **[Prisma Access]** > **[Prisma Access** セットアップ] に移動し、[ZTNA コネクタ IP] の下の **[**アプリケーション **IP** ブロック**]** をメモします。



2. [オブジェクト > アドレス] に移動し、取得した IP アドレスに基づいてアドレス オブジェクトを追加します 。
3. [オブジェクト] > [アドレス グループ] に移動し、作成したアドレス オブジェクトをアドレス グループに 追加します 。

©2025 Palo Alto Networks, Inc.



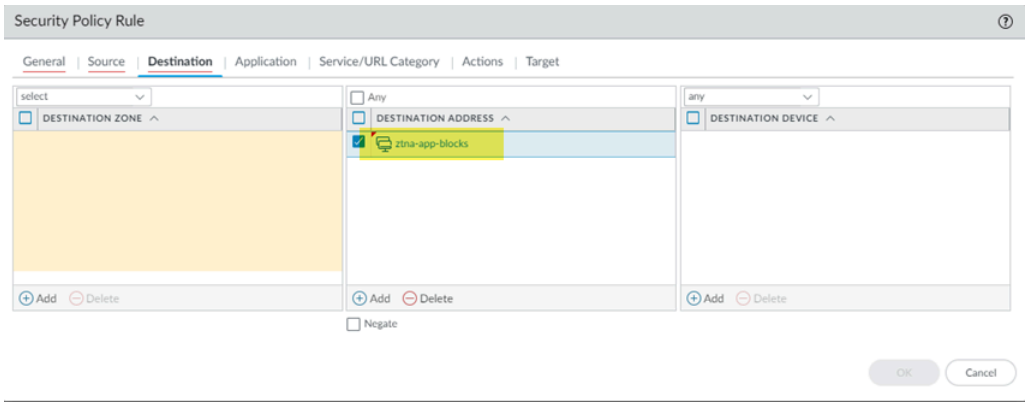
4. [ポリシー] > [セキュリティ] > [事前ルール] に移動し、前の手順で作成した アドレス グループ を指定して、すべてのアプリケーション IP アドレス ブロックへのアクセスを許可するセキュリティ ポリシーを追加します 。

   このセキュリティ ポリシーを追加すると、ZTNA コネクタがワイルドカードに基づいてアプリを検出する間、ワイルドカード ベースのアプリ トラフィックからのすべての

©2025 Palo Alto Networks, Inc.

トラフィックを通過できるようになります。アプリケーション IP ブロックを許可するルールがないと、ユーザーはワイルドカードベースのアプリにアクセスできません。

ZTNA コネクタがワイルドカードベースのアプリを検出するまで、このポリシーをそのままにしておくことができます。次に、このポリシーを無効にして、検出されたアプリごとにセキュリティ ポリシー ルールを追加することを選択できます。



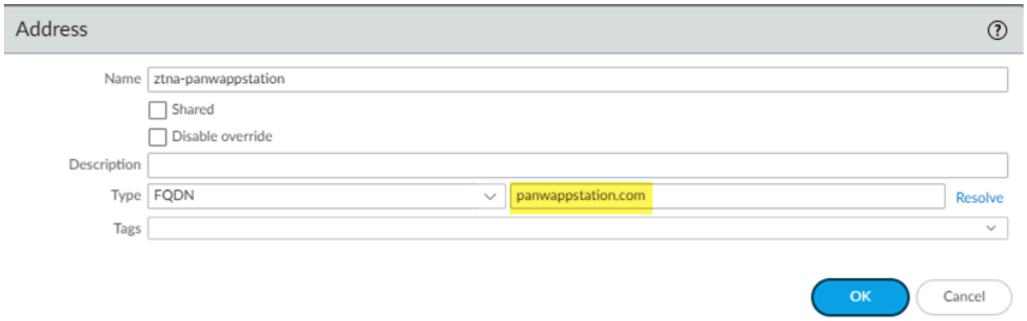
©2025 Palo Alto Networks, Inc.

STEP 2 | ZTNA コネクタがワイルドカードに基づいてアプリを検出したら、FQDN を使用して追加したアプリのセキュリティ ポリシーを構成します。

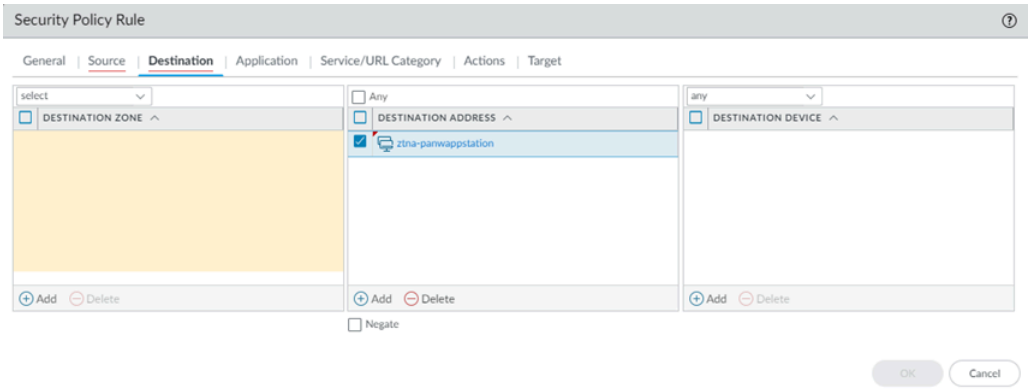
1. [ワークフロー] > **[ZTNA** コネクタ] > [アプリケーション ターゲット] > **[FQDN** ターゲット] に移動し、アプリで使用される FQDN をメモします。
2. FQDNのアドレス オブジェクト (オブジェクト > アドレス) を作成します。

   モバイル ユーザーまたはブランチ サイトのユーザーのどちらが ZTNA コネクタの背後にあるプライベート アプリにアクセスするかに応じて、**Mobile_User_Device_Group** または **Remote_Network_Device_Group**のいずれかを選択します。
3. **FQDN**タイプ のアドレス オブジェクトを追加し 、検出されたアプリケーションの **FQDN** を入力します。

   FQDN ターゲットの FQDN を入力します。



4. [ポリシー] > [セキュリティ] > [事前ルール]に移動し、検出されたアプリへのアクセスを許可するセキュリティ ポリシーを追加します 。



STEP 3 | 変更を **Commit and Push**（コミットしてプッシュ）します。

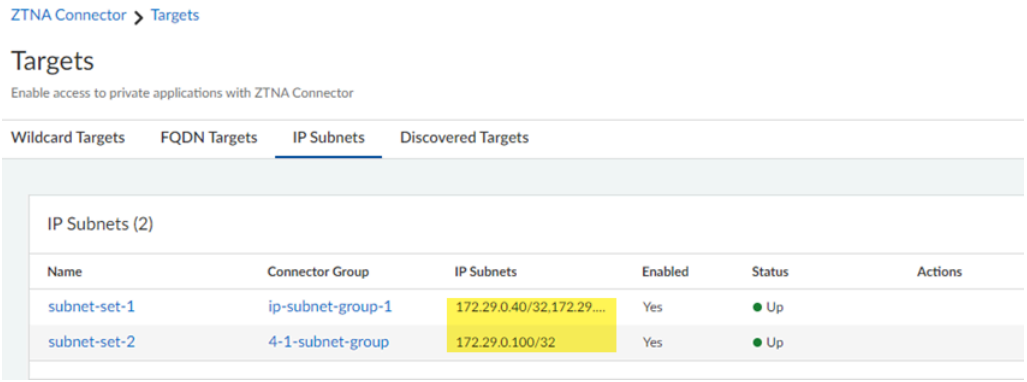
STEP 4 | (任意) FQDN に基づいてセキュリティ ポリシーを作成した後、IP アプリケーション ブロックに基づくポリシーを削除します。

IP サブネットベースのアプリのセキュリティ ポリシー

IP サブネットに基づいて ZTNA コネクタ アプリケーション ターゲットを作成した場合 ([設定] > **[ZTNA** コネクタ] > [コネクタ] > [アプリケーション ターゲット] > **[IP** サブネット])、次の手順を実行してアプリへのアクセスを許可します。

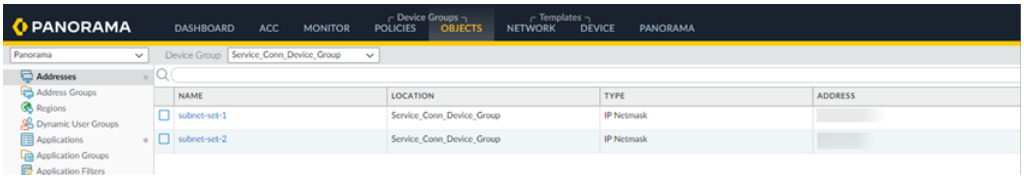
©2025 Palo Alto Networks, Inc.

STEP 1 | [ワークフロー] > > **[ZTNA** コネクタ] > [アプリケーション ターゲット] > **[IP** サブネット] に移動し、アプリで使用される IP サブネットをメモします。

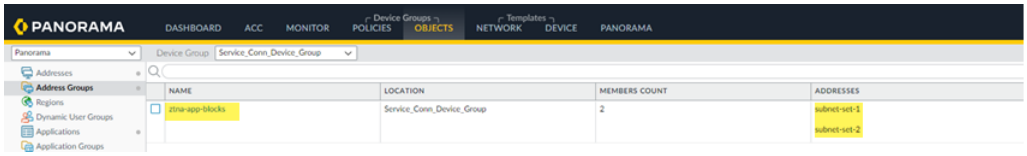


STEP 2 | アプリに使用される IP サブネットの IP アドレスを許可するポリシーを作成します。

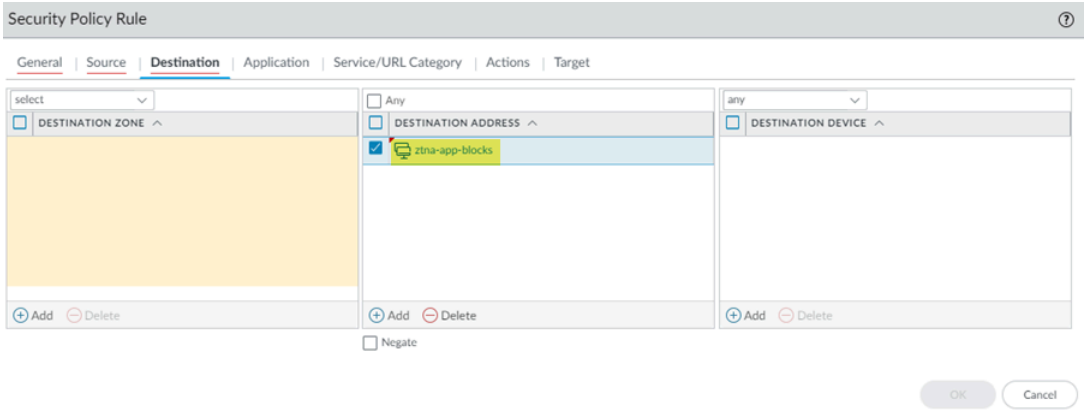
1. [構成 > 管理] > **[NGFW** および **Prisma Access** > オブジェクト] > [アドレス] > [アドレス] に移動し、取得した IP アドレスに基づいてアドレス オブジェクト を追加します 。



2. [オブジェクト] > [アドレス グループ] に移動し、作成したアドレスをアドレス グループに 追加します 。



3. [ポリシー] > [セキュリティ] > [事前ルール]に移動し、前の手順で作成した アドレス を指定して、アプリの IP サブネットへのアクセスを許可するセキュリティ ポリシーを追加します 。



STEP 3 | 設定の変更を保存してプッシュするには、 **[Push Config (**設定をプッシュ**)]**をクリックします 。

©2025 Palo Alto Networks, Inc.

FQDN ベースのアプリのセキュリティ ポリシー

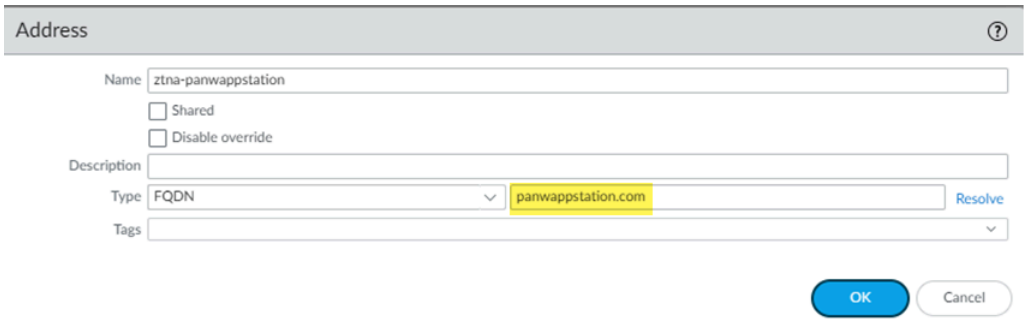
FQDN に基づいてターゲットを追加した場合 ([設定] > **[ZTNA** コネクタ] > [コネクタ] > [アプリケーション ターゲット] > **[FQDN** ターゲット)、次の手順を実行して、アプリへのアクセスを許可するアドレス オブジェクトとセキュリティ ポリシーを作成します。

STEP 1 | FQDN を使用して追加したアプリのセキュリティ ポリシーを構成します。

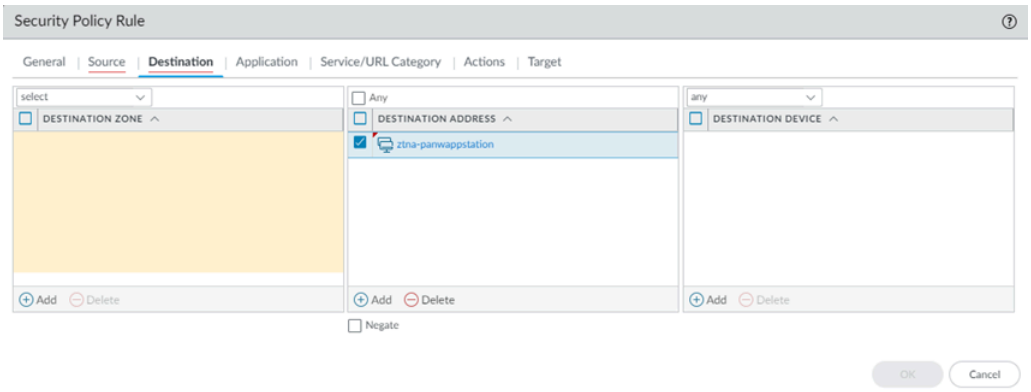
1. [ワークフロー] > **[ZTNA** コネクタ] > [アプリケーション ターゲット] > **[FQDN** ターゲット] に移動し、アプリで使用される FQDN をメモします。
2. FQDNのアドレス オブジェクト (オブジェクト > アドレス) を作成します。

   モバイル ユーザーまたはブランチ サイトのユーザーのどちらが ZTNA コネクタの背後にあるプライベート アプリにアクセスするかに応じて、**Mobile_User_Device_Group** または **Remote_Network_Device_Group**のいずれかを選択します。
3. **FQDN**タイプ のアドレス オブジェクトを追加し 、検出されたアプリケーションの **FQDN** を入力します。

   検出されたすべてのアプリの FQDN を入力します。



4. 任意: [構成の > 管理] > **[NGFW** および **Prisma Access]** > [セキュリティ サービス] > [セキュリティ ポリシー > 事前ルール] に移動し、検出されたアプリへのアクセスを許可するセキュリティ ポリシーを追加します 。



STEP 2 | 設定の変更を保存してプッシュするには、 **[Push Config (**設定をプッシュ**)]**をクリックします 。

©2025 Palo Alto Networks, Inc.

データセンターにZTNAコネクタVMを導入する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ ZTNA コネクタ アドオン ライセンス アドオン ライセンスを含む Essential ライセンスには、8つのZTNAコネクタ、100個のFQDN、および4つのIPサブネット機能が含まれます。 アドオン ライセンスを含む Advanced ライセンスには、40個の ZTNA コネクタ、300個のFQDN、および 1024 個のIPサブネット機能が含まれます。 アドオン ライセンスを含むプレミアム ライセンスには、200個のZTNAコネクタ、4000個のFQDN、および1024個のIPサブネット機能が含まれます。 ❑ ZTNAコネクタアドオンライセンスを購入しない場合は、 Prisma Accessライセンスには、4 つのコネクタ、40 個の FQDN、および 4 つの IP サブネットが含まれます。この機能は、ご使用の環境で ZTNA コネクタを試す目的で提供されています。

Prisma Access内でConnector(コネクタ)グループ、コネクタ、およびアプリケーションターゲットを構成した後、データセンタにConnector VMをデプロイする必要があります。コネクタのオンボーディングを簡素化するために、各データセンター環境のデプロイメント テンプレートが、Palo Alto Networksカスタマー サポート ポータルまたはクラウド プロバイダー マーケットプレイスから入手できます。使用するテンプレートは、ワンアームデプロイメントを使用するか、ツーアームデプロイメントを使用するかによって異なります。

サポートされているZTNAコネクタのデプロイメント

ZTNA コネクタはクラウド内のPrisma Accessパブリック IPアドレスへの接続を開始するため、イングレス(入口側)ファイアウォールのセキュリティ ルールを定義する必要はありません。ただし、ZTNA Connectorが接続を開始するため、ZTNA Connectorのクラウドコントローラへのアクセスと Prisma Accessデータプレーンへの IPSec接続を許可するためのイグレスルールを追加する必要があります。ZTNA Connectorは、クラウドの Prisma Accessパブリック IPアドレスへの接続を開始します。このため、ZTNA Connector が Prisma Accessへの IPSecトンネルを作成できるように、以下のイグレスルールが必要とされます。

©2025 Palo Alto Networks, Inc.

- インターネット接続- HTTPS (TCP 443) および IKE/IPSec (UDP 500 および 4500) の出力を許可します
- データ センター向け- 出力アプリケーション ポートを許可します。

  たとえば、出力アプリケーション ポートHTTP (80) とHTTPS (443) を許可します。これらの例のポートはTCPポートです。データ センターで別のポートが使用されている場合は、代わりにそれらのポートを許可します。

コネクタVM は、次のデプロイメント トポロジでデプロイできます。

ワンアーム デプロイメント



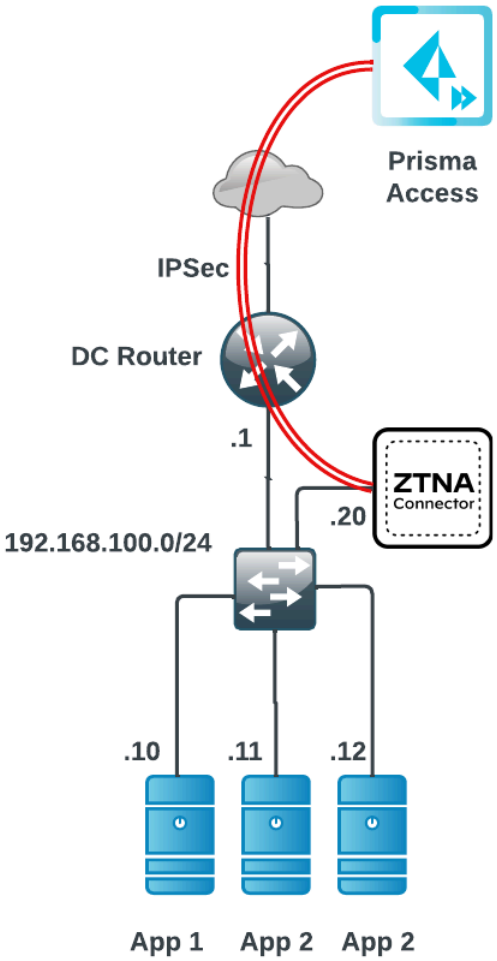
ワンアーム デプロイメントは、*AWS*、*Azure*、*GCP*などのクラウド ネイティブ環境でのみサポートされます。*ESXi*、カーネルベース仮想マシン（*KVM*）、*Microsoft Hyper-V*などのオンプレミスのデプロイメントには、*2*アームデプロイメントを使用します。

このデプロイメントでは、ZTNAコネクタはプライベートなデータセンター サブネット上にあり、データセンター ルーターを介してインターネットにアクセスできます。アプリケー

©2025 Palo Alto Networks, Inc.

ションへのアクセスは、同じサブネット上でローカルに行うことも、データセンター ルーターを介して行うこともできます。

次の図は、ワンアーム デプロイメントを使用したZTNAコネクタ ネットワーク デプロイメントの例を示しています。



©2025 Palo Alto Networks, Inc.

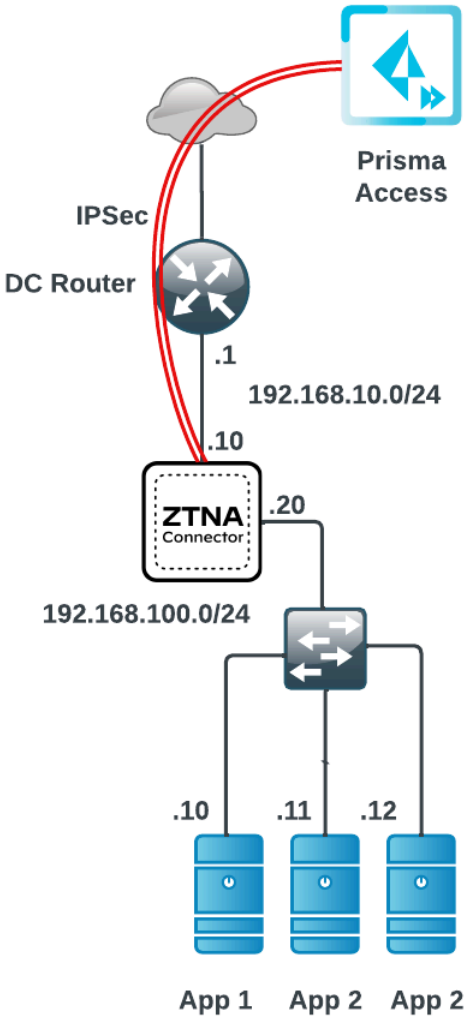
2アーム デプロイメント

入口と出口のセキュリティ ルールをより細かく制御したい場合、またはオンプレミスのVMデプロイメントがある場合は、1つのインターフェイスがインターネットに面し、もう1つがデータ センターに面する 2 アーム デプロイメントを使用できます。

2アーム コネクタでIPアドレスを設定する場合は、VMの電源をオンにする前に、ZTNAコネクタのIPアドレス割り当てが正しく設定されていることを確認してください。たとえば、次のサンプル図では、192.168.10.10 および192.168.10.20のIPアドレスが使用されています。これらのサンプル アドレスに基づいて、ZTNAコネクタのポートを192.168.10.10および192.168.100.20に設定してください。そうしないと、Prisma AccessはZTNAコネクタを介してデータ センター内のアプリにアクセスできません。192.168.10.10および192.168.100.20はサンプルのIPアドレスであり、デプロイメントを機能させるためにこれらのIPアドレスを使用する必要はありません。

次の図は、2アーム デプロイメントを使用したZTNAコネクタ ネットワーク デプロイメントの例を示しています。

©2025 Palo Alto Networks, Inc.

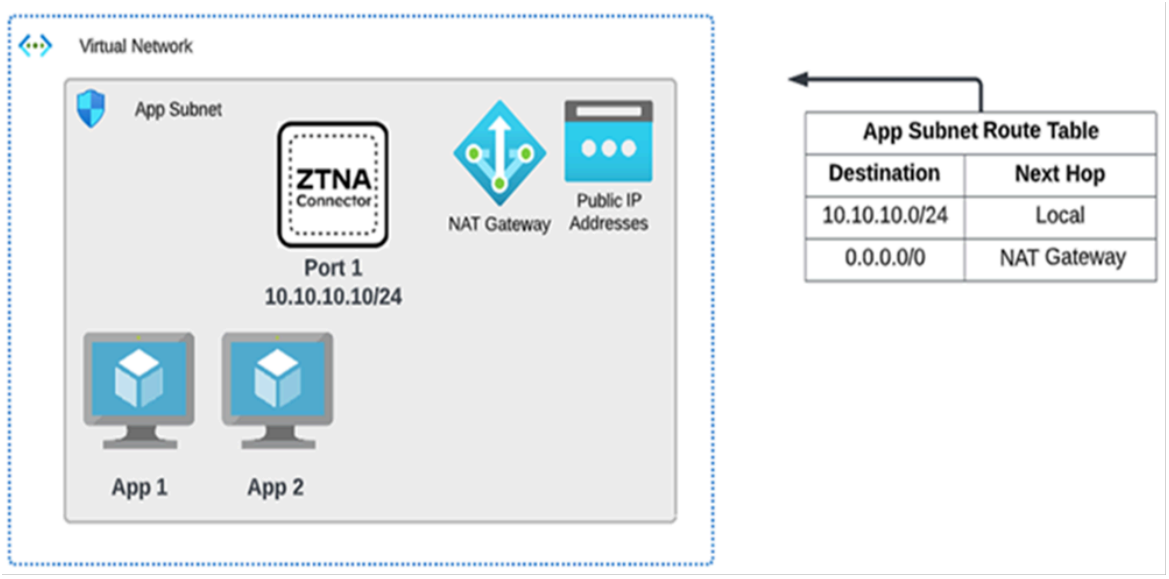


ZTNAコネクタがサポートするMicrosoft Azureのデプロイメント

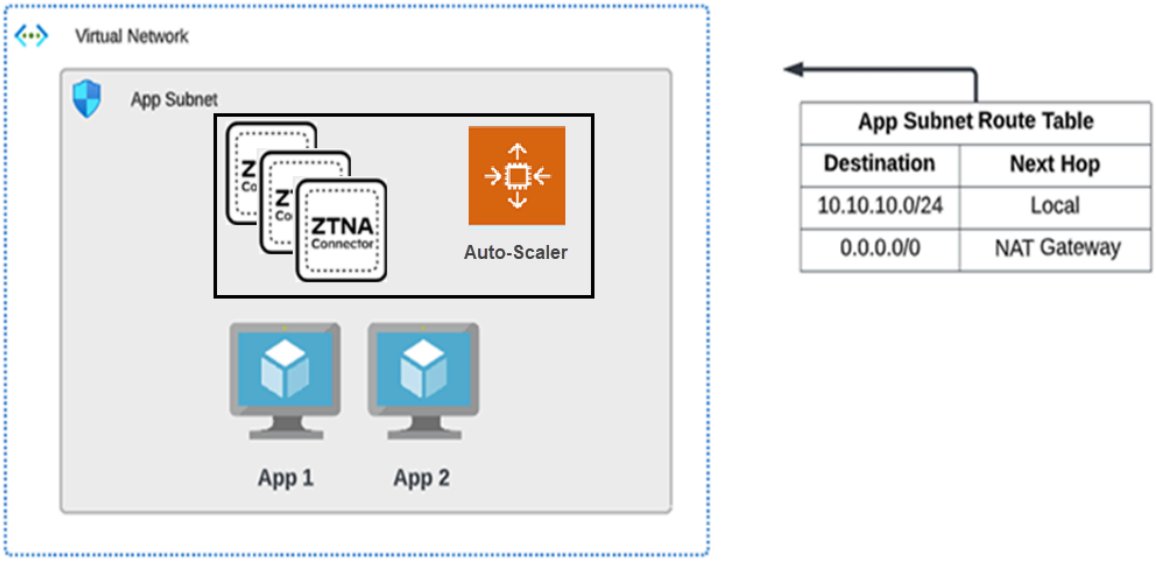
Microsoft AzureのPrisma AccessZTNAコネクタ ネットワーク デプロイメントでは、2つのデプロイメントと、各デプロイメントに対応するテンプレートがサポートされます。

次の図は、NATゲートウェイを使用した1アームモードを使用したAzureでのPrisma AccessZTNAコネクタのデプロイメント例を示しています。

©2025 Palo Alto Networks, Inc.

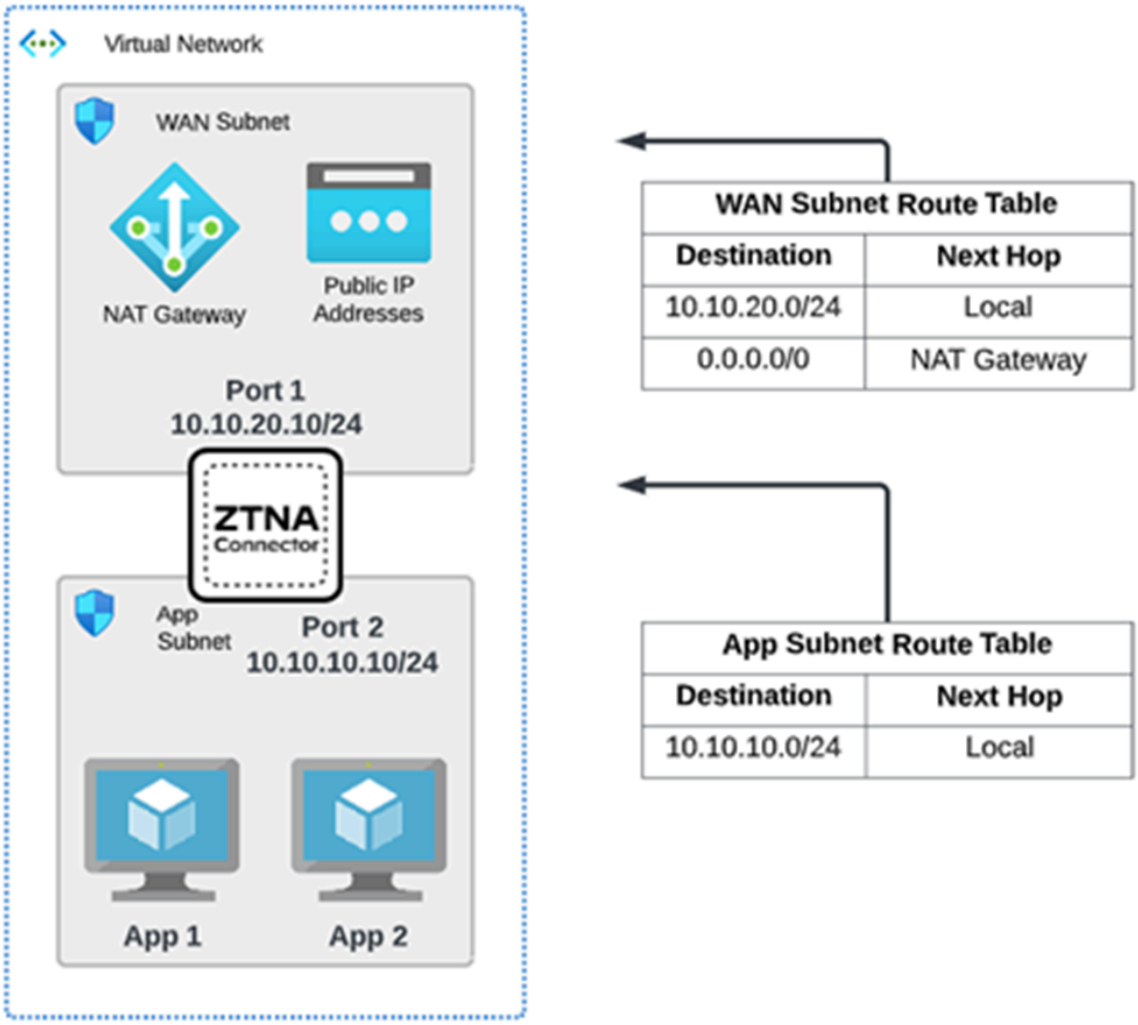


次の図は、NATゲートウェイを使用したワンアーム自動スケーリングを使用したAWSでのZTNAコネクタのデプロイメントのサンプルを示しています。



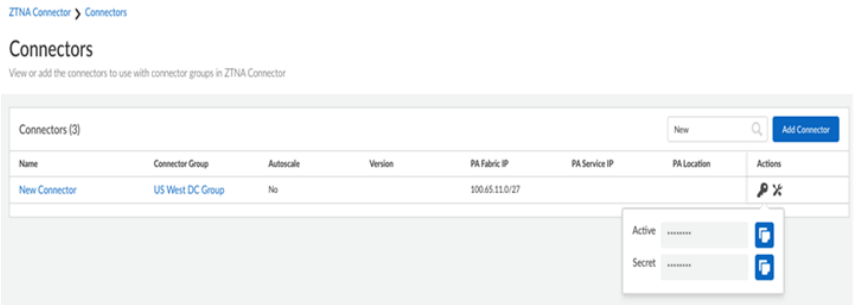
次の図は、NATゲートウェイを使用した2アームモードを使用したAzureでのPrisma AccessZTNAコネクタのデプロイメント例を示しています。

©2025 Palo Alto Networks, Inc.



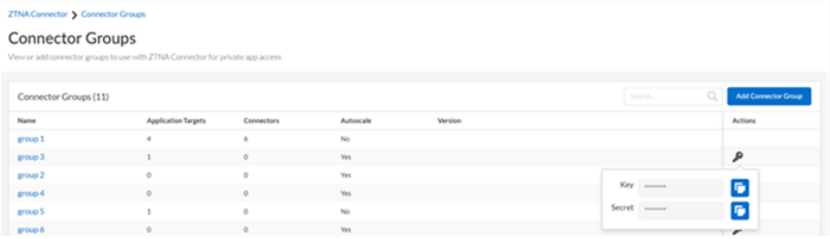
Microsoft AzureにZTNAコネクタをオンボードする

- Microsoft Azureで ZTNA コネクタを使用するために 構成する必要がある要件とガイドラインおよび FQDN とポートを確認します。
- Prisma SASEプラットフォームで、コネクタ キーとシークレットの値を取得してコピーします。ワークフロー > **ZTNA**コネクタ > コネクタで、この VM に関連付けるためにPrisma Accessで作成したコネクタ・オブジェクトを見つけ、「**Copy Token**」を選択し、次に**Key(**キー**)**と**Secret(**シークレット**)**の値をコピーします。



 ©2025 Palo Alto Networks, Inc.

- **Prisma AccessZTNA Connector 1-Arm Auto-Scaling**のデプロイメントでは、Connector Group(コネクタグループ)キーとシークレット値を取得してコピーする必要があります：ワークフロー > **ZTNA**コネクタ > コネクタグループで、このVMに関連付けるためにPrisma Accessで作成したコネクタ・オブジェクトを見つけ、「**Copy Token**」を選択し、次に**Key(**キー**)**と**Secret(**シークレット**)**をコピーします。



すべての前提条件を満たしたら、以下の手順に従ってMicrosoft AzureにZTNAコネクタをオンボードします。

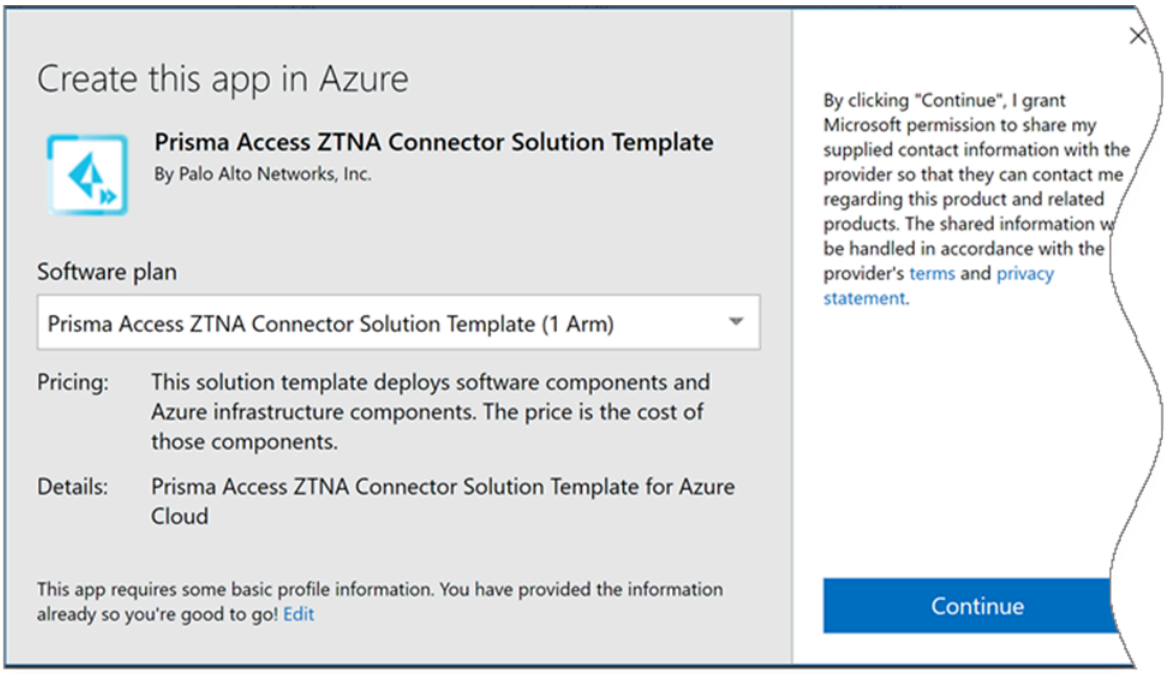
STEP 1 | Azure Marketplaceにログインして、**Prisma AccessZTNA**コネクタを検索します。

STEP 2 | **Get it now**（今すぐ入手）をクリックします。



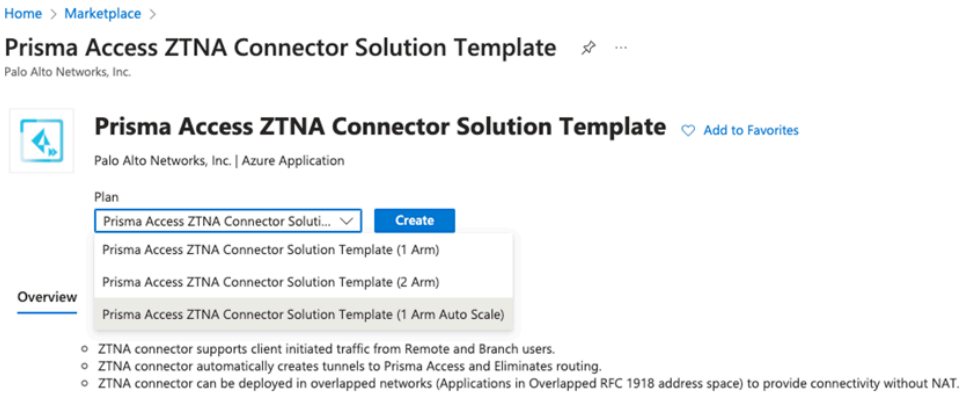
 ©2025 Palo Alto Networks, Inc.

STEP 3 | 作成プロセスを続行します 。



STEP 4 | ソフトウェア プランを選択し、Azureでこのアプリケーションを作成します 。

- Prisma Access ZTNA コネクタ ソリューション テンプレート (1 アーム)
- Microsoft Azureで自動スケーリングを使用してZTNA Connector 1-Armをデプロイする
- Prisma Access ZTNA コネクタ ソリューション テンプレート (2 アーム)



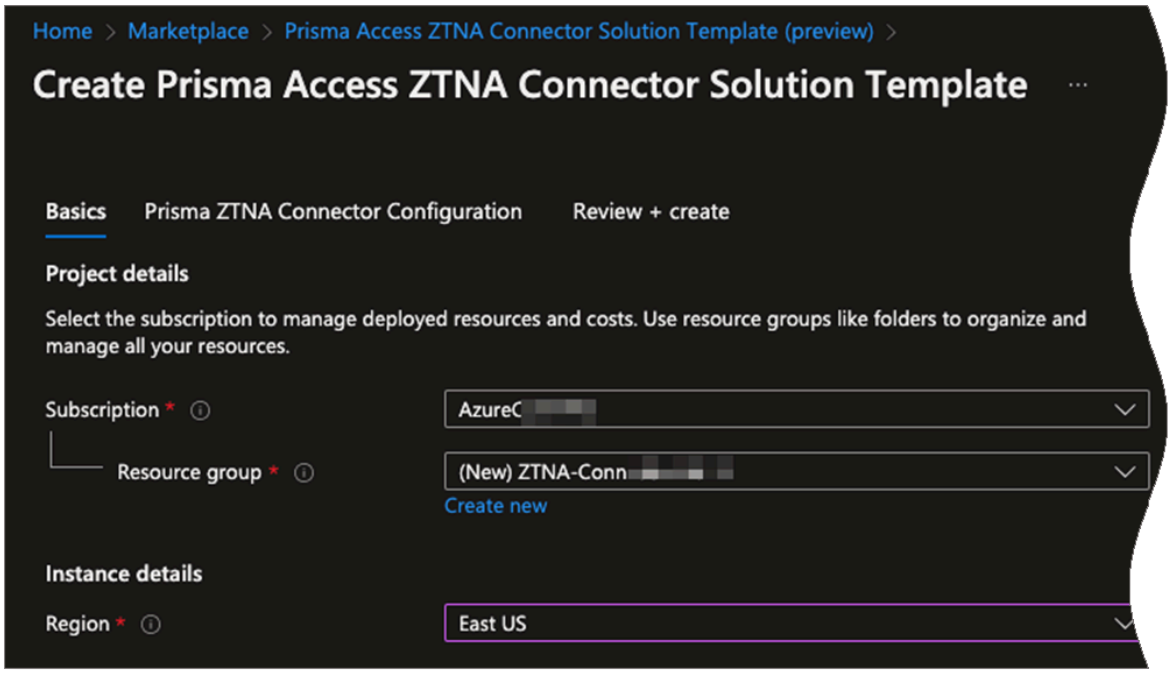
Microsoft AzureにZTNA Connector 1-Armをデプロイする

1-Arm ZTNA ConnectorをMicrosoft Azureにデプロイするには、次の手順に従います。

 ©2025 Palo Alto Networks, Inc.

STEP 1 | **[Basics (基本)]** タブで次の設定を行います。

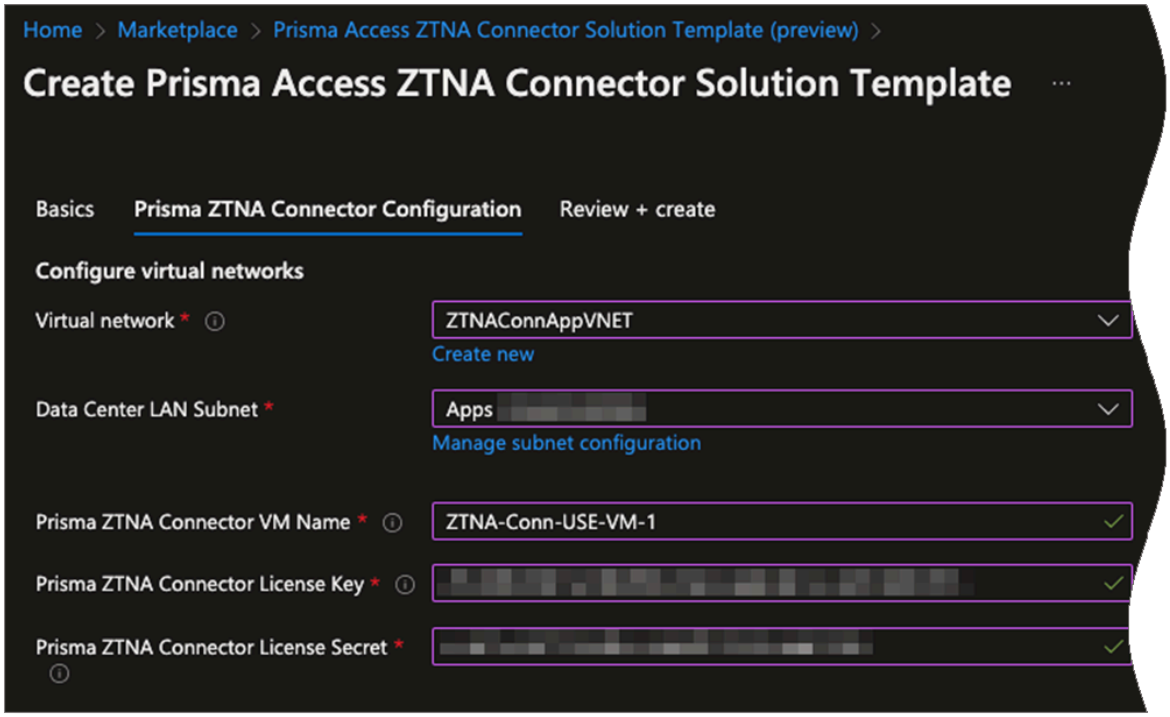
- デプロイされたリソースを管理するには、Azureサブスクリプションを選択します。
- 既存の リソース グループを選択するか、 新規作成します。
- お客様のロケーションに関連するAzureリージョンを選択します
- **NEXT (次へ)** をクリックします。**Prisma ZTNA**コネクタ設定。



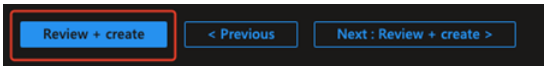
 ©2025 Palo Alto Networks, Inc.

STEP 2 | **[Prisma ZTNA** コネクタ設定] タブで仮想ネットワークを構成します。

- 新しい仮想ネットワークを作成するか、既存の仮想ネットワークを選択します。
- このコネクタにオンボードするアプリケーションをプロビジョニングした データセンター**LAN**サブネットを選択します。
- **Prisma ZTNA**コネクタ**VM**名を入力します。
- Prisma SASE ポータルから取得した**Prisma ZTNA** コネクタ ライセンス キー と**Prisma ZTNA** コネクタ ライセンス シークレットの値を入力します。



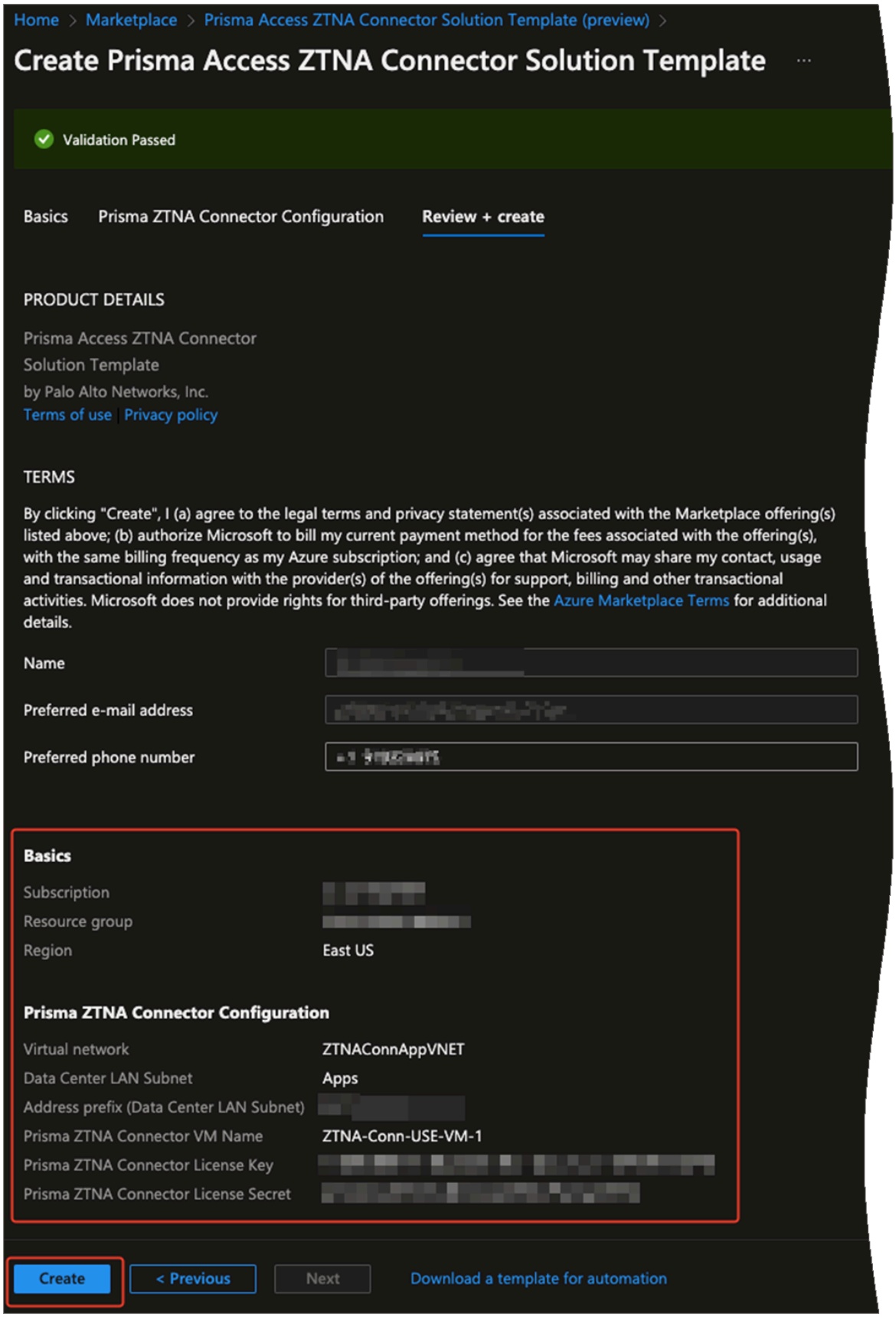
- 管理対象 Prisma ZTNA コネクタの構成を確認するには、**[Review + create (**確認 **+** 作成**)]**をクリックします 。



©2025 Palo Alto Networks, Inc.

STEP 3 | 指定した詳細を確認し、**[Create (作成)]** をクリックして仮想マシンのデプロイメントを開始します。

©2025 Palo Alto Networks, Inc.



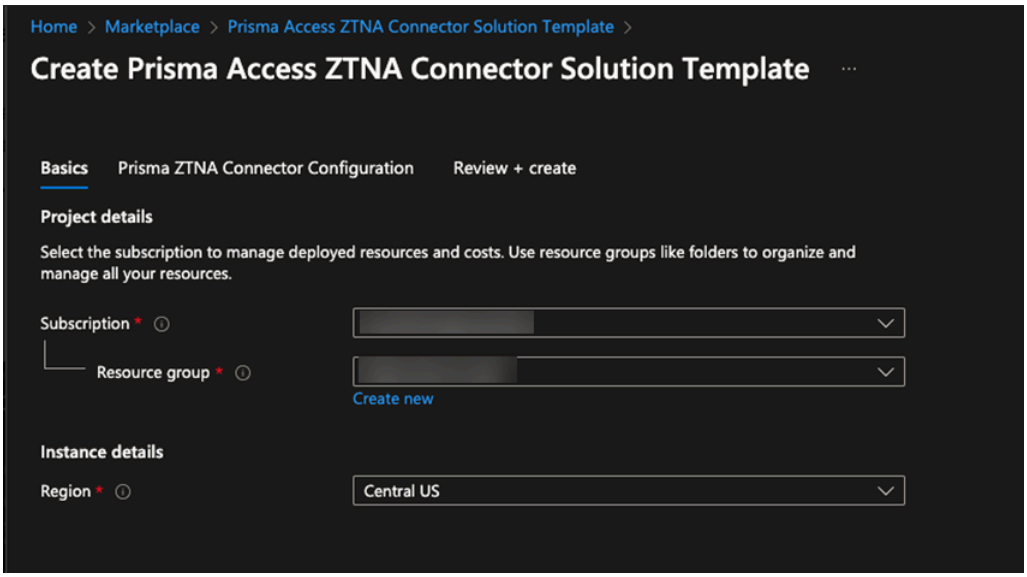
©2025 Palo Alto Networks, Inc.

STEP 4 | デプロイメントが完了したら、**[Go to resource**（リソースに移動）**]**を選択して記入します。

Microsoft Azureで自動スケーリングを使用して**ZTNA Connector 1-Arm**をデプロイする

STEP 1 | **[Basics (基本)]** タブで次の設定を行います。

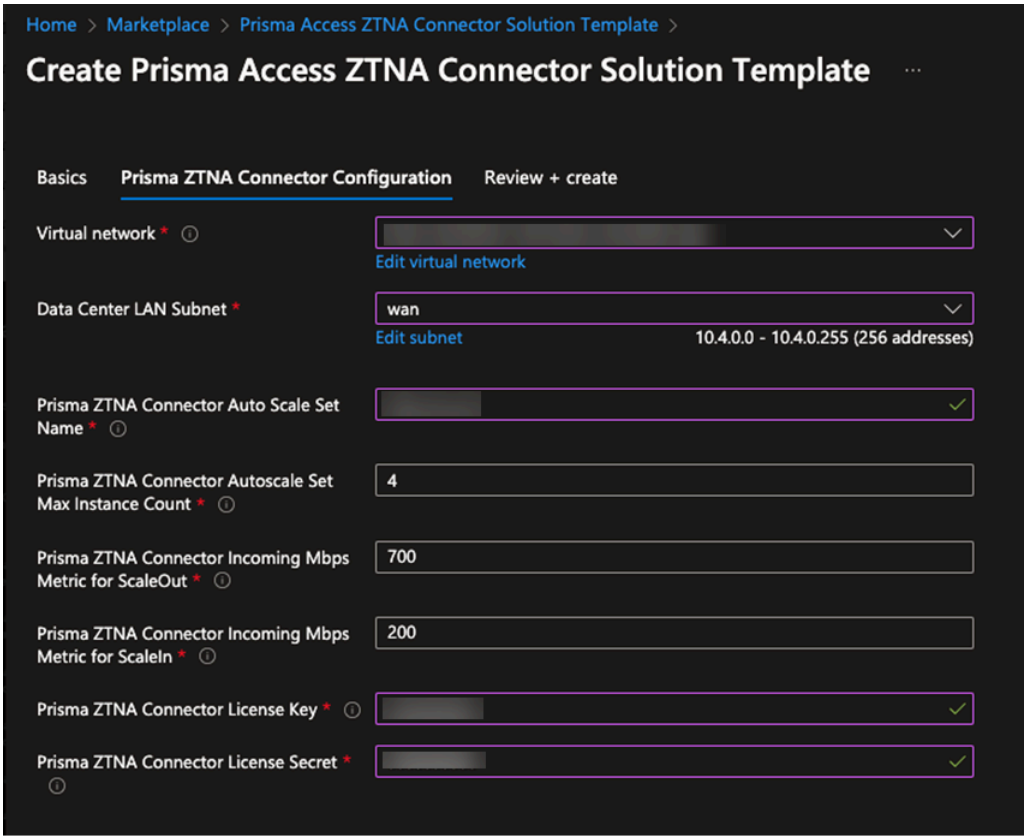
- デプロイされたリソースを管理するには、Azureサブスクリプションを選択します。
- 既存の リソース グループを選択するか、 新規作成します。
- お客様のロケーションに関連するAzureリージョンを選択します
- **NEXT (次へ)** をクリックします。**Prisma ZTNA**コネクタ設定。



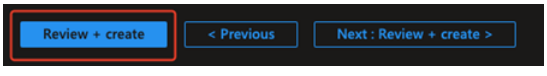
©2025 Palo Alto Networks, Inc.

STEP 2 | **Next(次へ)**で仮想ネットワークを設定する：**Prisma ZTNA**コネクタ設定タブ：

- 新しい仮想ネットワークを作成するか、既存の仮想ネットワークを選択します。
- このコネクタにオンボードするアプリケーションをプロビジョニングした データセンター**LAN**サブネットを選択します。
- **Prisma ZTNA**コネクタの自動スケール セット名を入力し、Azureで作成されたスケールセットの名前を指定します。
- **Prisma ZTNA**コネクタの自動スケール設定最大インスタンス数を入力します。コネクタ グループで許可される ZTNA コネクタの最大数は4です。
- **ScaleOut**の**Prisma ZTNA**コネクタ受信**Mbps**メトリックを入力します。100 ～ 1000 の範囲の値を入力します。
- **ScaleIn**の**Prisma ZTNA**コネクタ受信**Mbps**メトリックを入力します。1 ～ 500 の範囲の値を入力します。
- コネクタを搭載するコネクタグループのPrisma SASEポータルから取得した**Prisma ZTNA**コネクタライセンスキーと**Prisma ZTNA**コネクタライセンスシークレットの値を入力します。

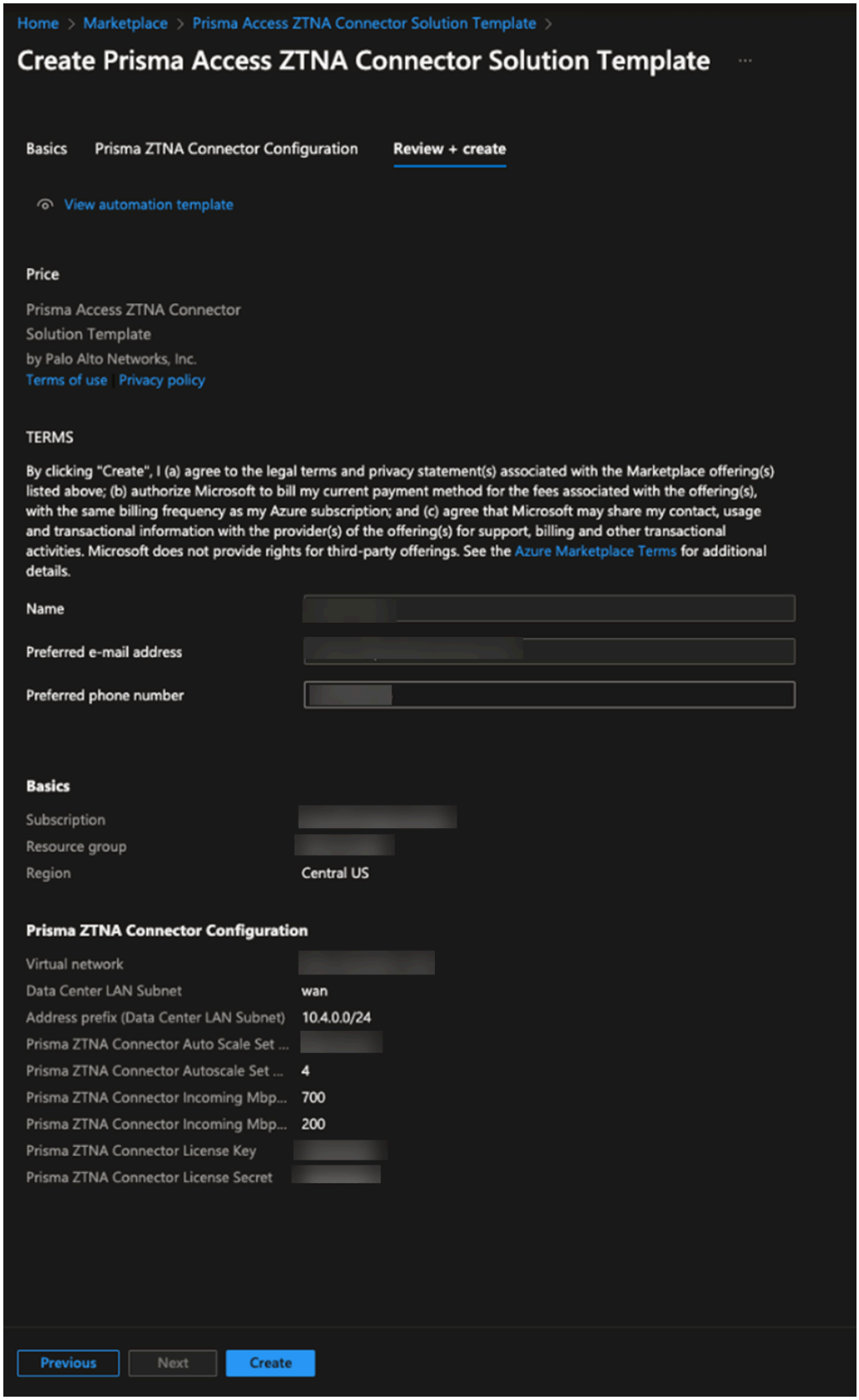


- 管理対象 Prisma ZTNA コネクタの構成を確認するには、**[Review + create (確認 + 作成)]**をクリックします 。



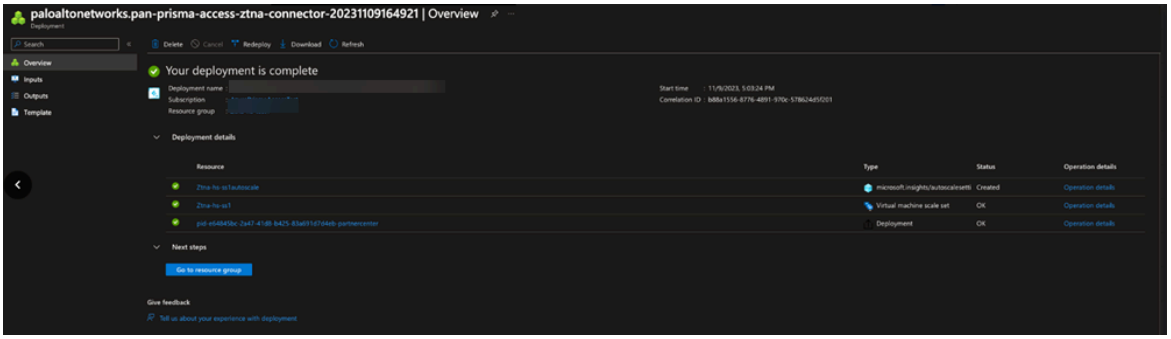
 ©2025 Palo Alto Networks, Inc.

STEP 3 | 指定した詳細を確認し、**[Create (作成)]** をクリックして仮想マシンのデプロイメントを開始します。



 ©2025 Palo Alto Networks, Inc.

STEP 4 | デプロイメントが完了したら、**[Go to resource group**（リソースグループに移動）**]**を選択して記入します。

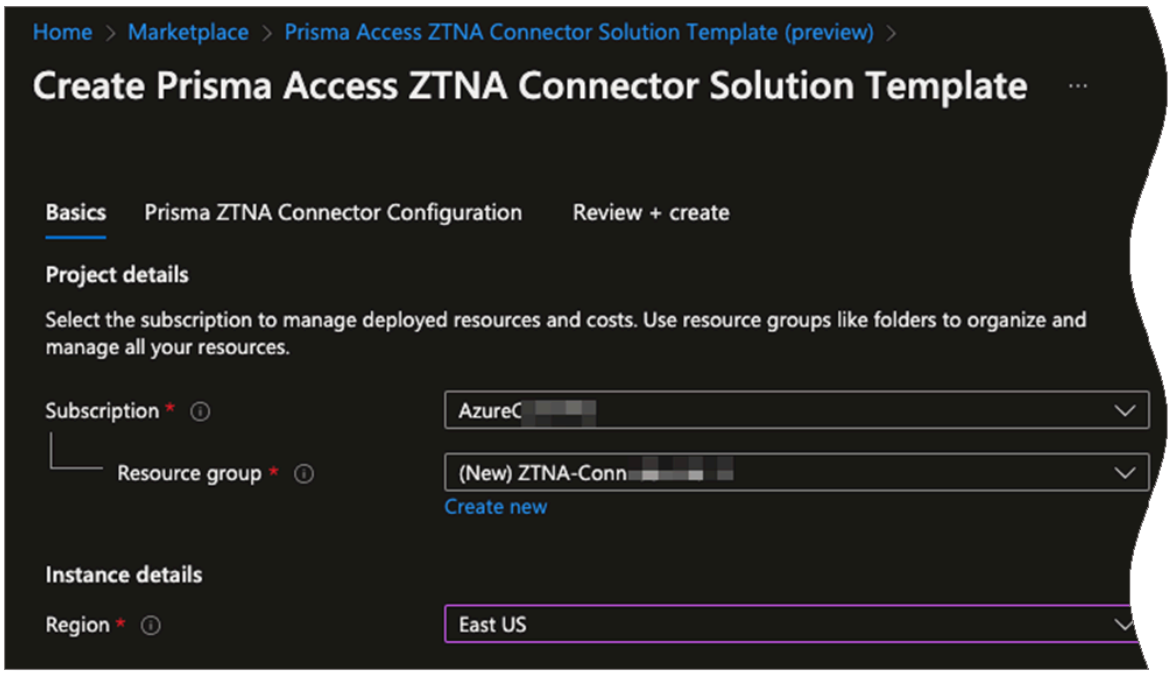


Microsoft AzureにZTNA Connector 2-Armをデプロイする

2-Arm ZTNA ConnectorをMicrosoft Azureにデプロイするには、次の手順に従います。

STEP 1 | **[Basics (基本)]** タブで次の設定を行います。

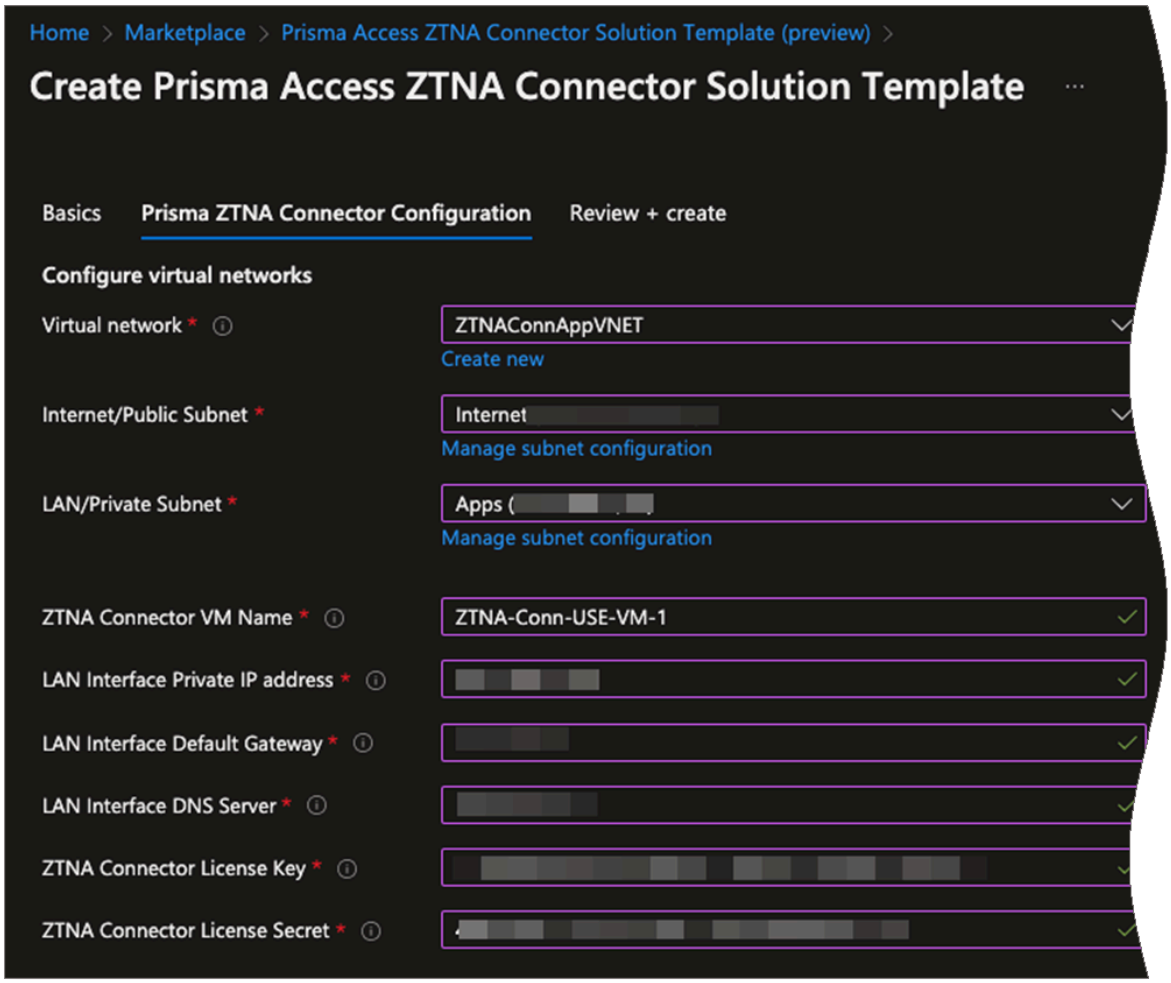
- デプロイされたリソースを管理するには、Azureサブスクリプションを選択します。
- 既存の リソース グループを選択するか、 新規作成します。
- お客様のロケーションに関連するAzureリージョンを選択します
- **NEXT (次へ)** をクリックします。**Prisma ZTNA**コネクタ設定。



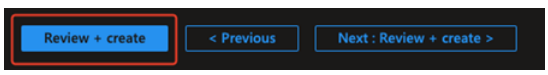
©2025 Palo Alto Networks, Inc.

STEP 2 | **Next(次へ)**で仮想ネットワークを設定する：**Prisma ZTNA**コネクタ設定タブ：

- 仮想ネットワーク を新しく作成するか、既存の仮想ネットワークを使用します。
- IPSecへのWAN接続用のインターネット/パブリック サブネットを選択します。インターネット接続には、サブネットをNATゲートウェイに関連付ける必要があります。
- このコネクタにオンボードするアプリケーションをプロビジョニングした データセンター**LAN**サブネットを選択します。
- **Prisma ZTNA**コネクタ**VM**名を入力します。
- **LAN** インターフェイスのプライベート **IP**アドレスを入力します。
- **LAN** インターフェースのデフォルト ゲートウェイのIPアドレスを入力します。
- **LAN** インターフェース**DNS**サーバーのIPアドレスを入力します。
- Prisma SASE ポータルから取得した**Prisma ZTNA** コネクタ ライセンス キー と**Prisma ZTNA** コネクタ ライセンス シークレットの値を入力します。



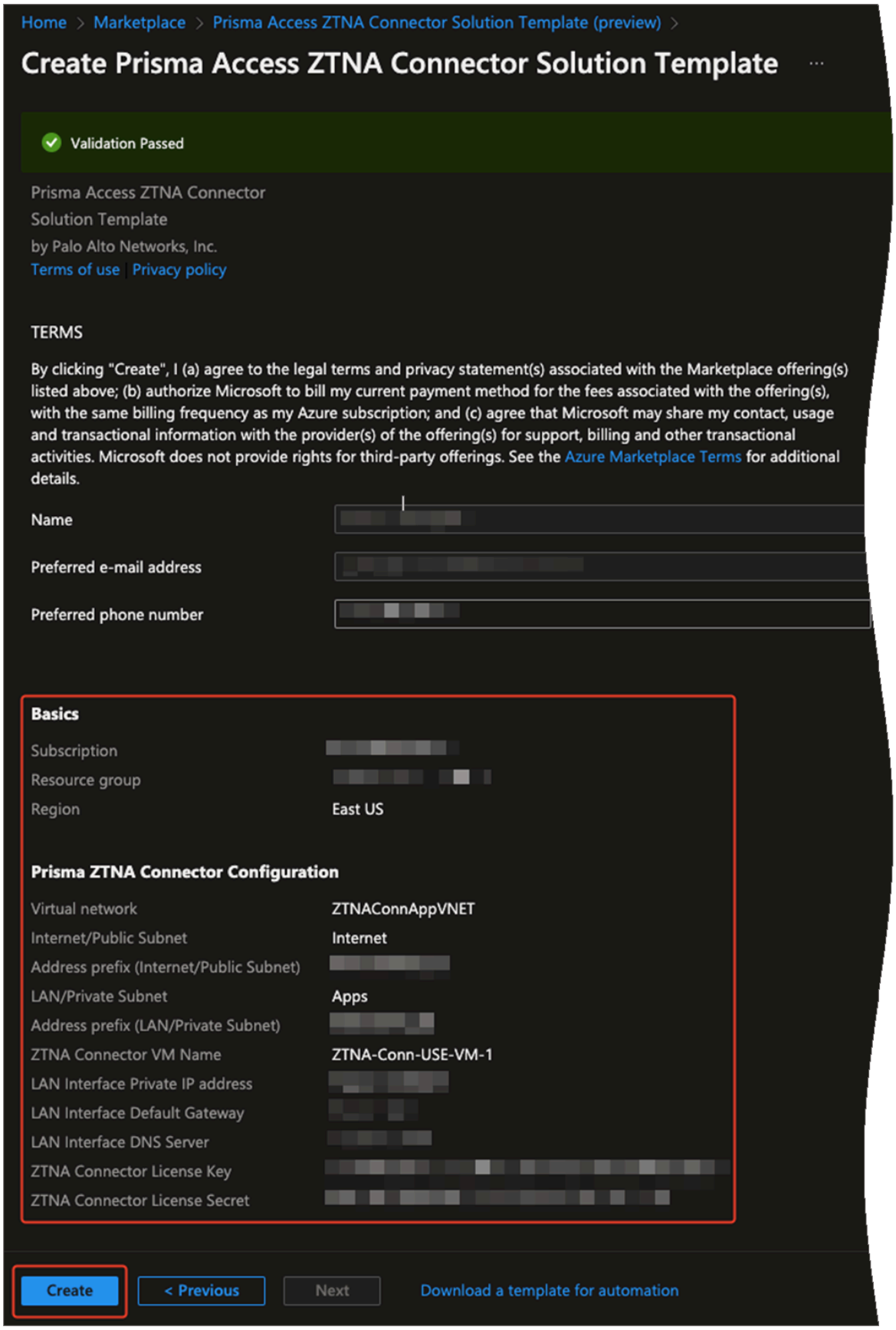
- 管理対象 Prisma ZTNA コネクタの構成を確認するには、**[Review + create (確認 + 作成)]**をクリックします 。



 ©2025 Palo Alto Networks, Inc.

STEP 3 | 指定した詳細を確認し、**[Create (作成)]** をクリックして仮想マシンのデプロイメントを開始します。

©2025 Palo Alto Networks, Inc.



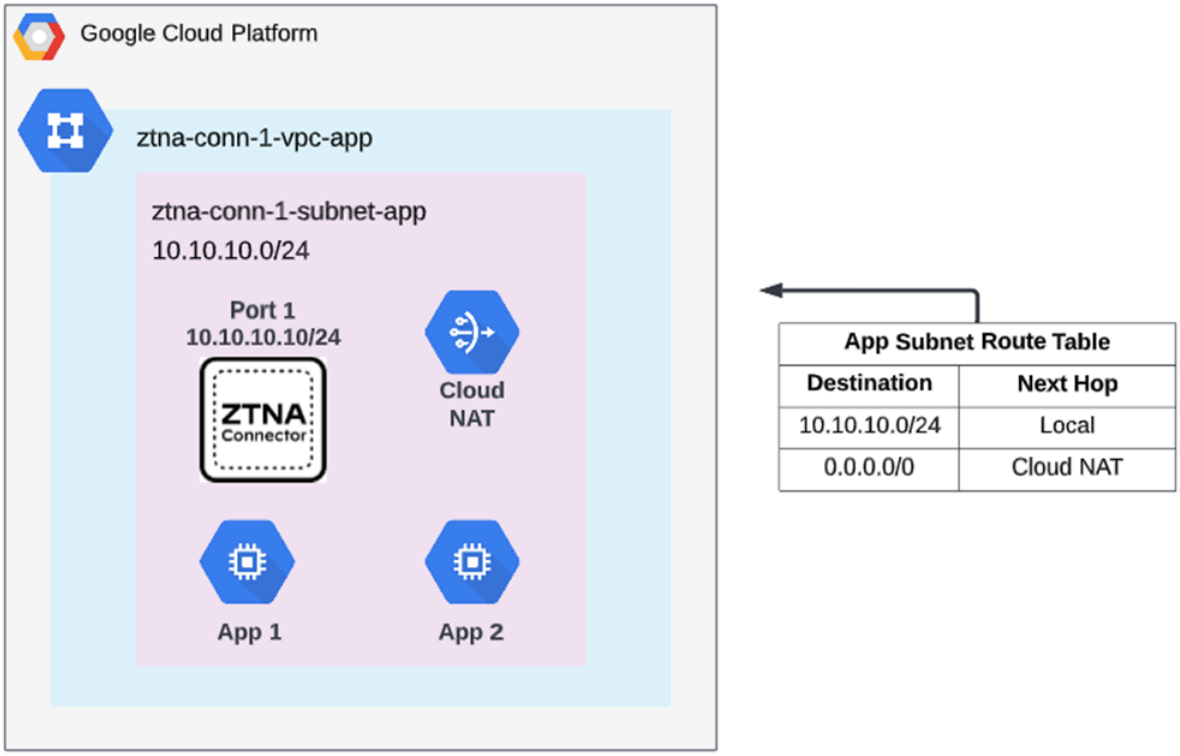
©2025 Palo Alto Networks, Inc.

STEP 4 | デプロイメントが完了したら、**[Go to resource**（リソースに移動）**]**を選択して記入します。

ZTNAコネクタでサポートされるGoogle Cloud Platformのデプロイメント

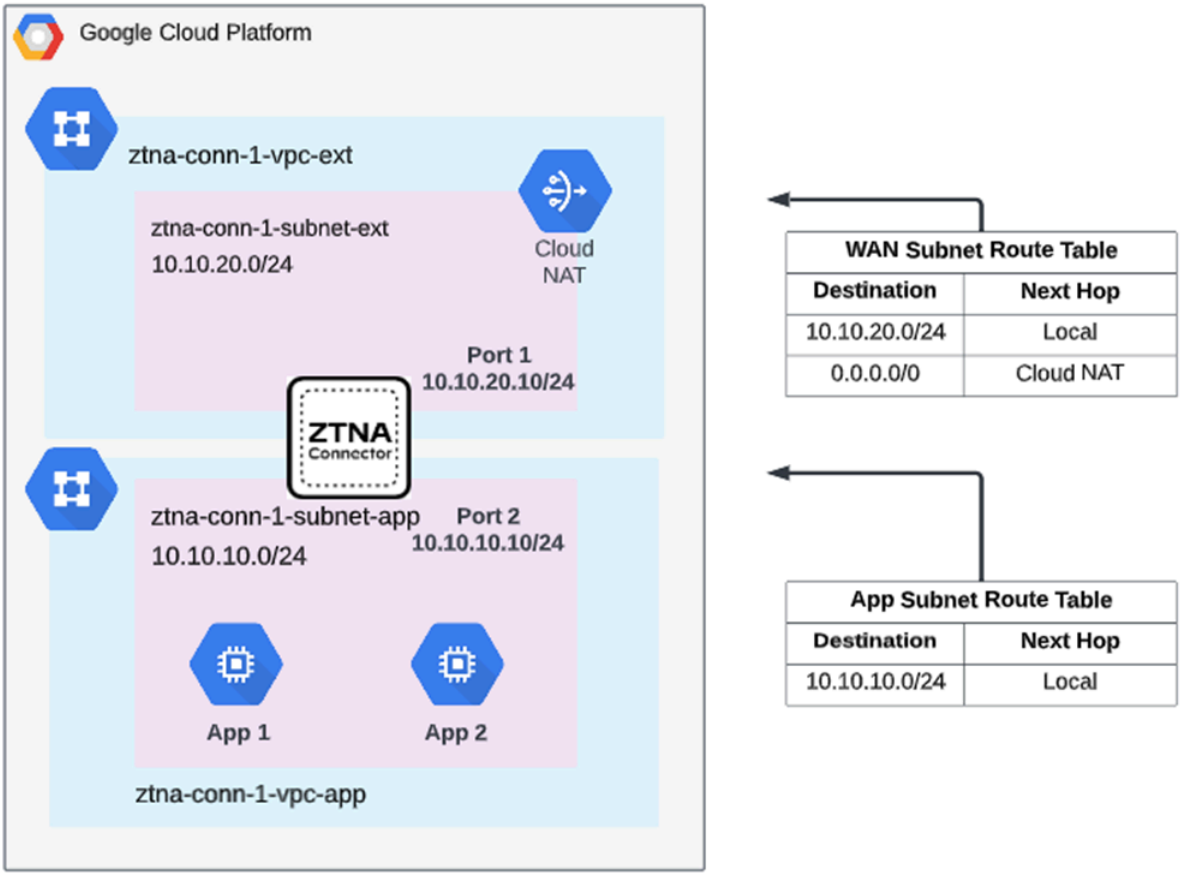
Prisma Access Google Cloud Platform (GCP) の ZTNAコネクタ ネットワーク デプロイメントでは、2つのデプロイメントと、各デプロイメントに対応するテンプレートがサポートされます。

次の図はサンプルを示しています Prisma Access NATゲートウェイを使用したワンアーム モードを使用したGCPでのZTNAコネクタのデプロイメント。



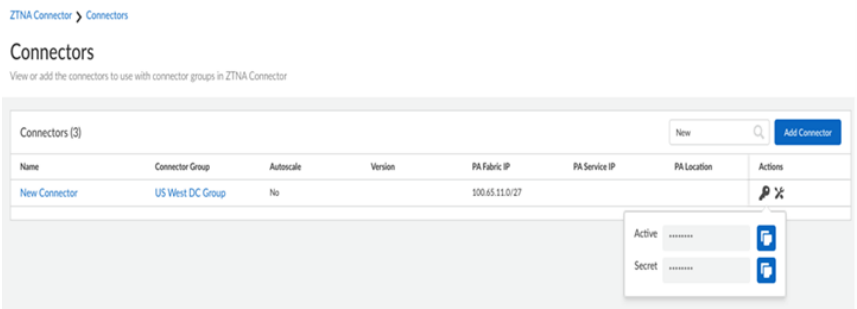
次の図は、NATゲートウェイを使用した2アームモードを使用したGCPでのPrisma AccessZTNAコネクタのデプロイメント例を示しています。

©2025 Palo Alto Networks, Inc.



Googleクラウドプラットフォームに**ZTNA**コネクタをオンボードする

- Google Cloud Platform (GCP)でPrisma AccessZTNAコネクタを使用するために 構成する必要がある要件とガイドライン および FQDN とポートを確認します。
- Prisma SASEポータルで、コネクタ キーとシークレットの値を取得してコピーします。ワークフロー > **ZTNA**コネクタ > コネクタで、この VM に関連付けるためにPrisma Accessで作成したコネクタ・オブジェクトを見つけ、「**Copy Token**」を選択し、次に**Key(**キー**)**と**Secret(**シークレット**)**の値をコピーします。



すべての前提条件を満たしたら、以下の手順に従ってGCPにPrisma AccessZTNAコネクタをオンボードします。

STEP 1 | GCP Marketplaceに移動して、**Prisma AccessZTNA**コネクタを検索します。

©2025 Palo Alto Networks, Inc.

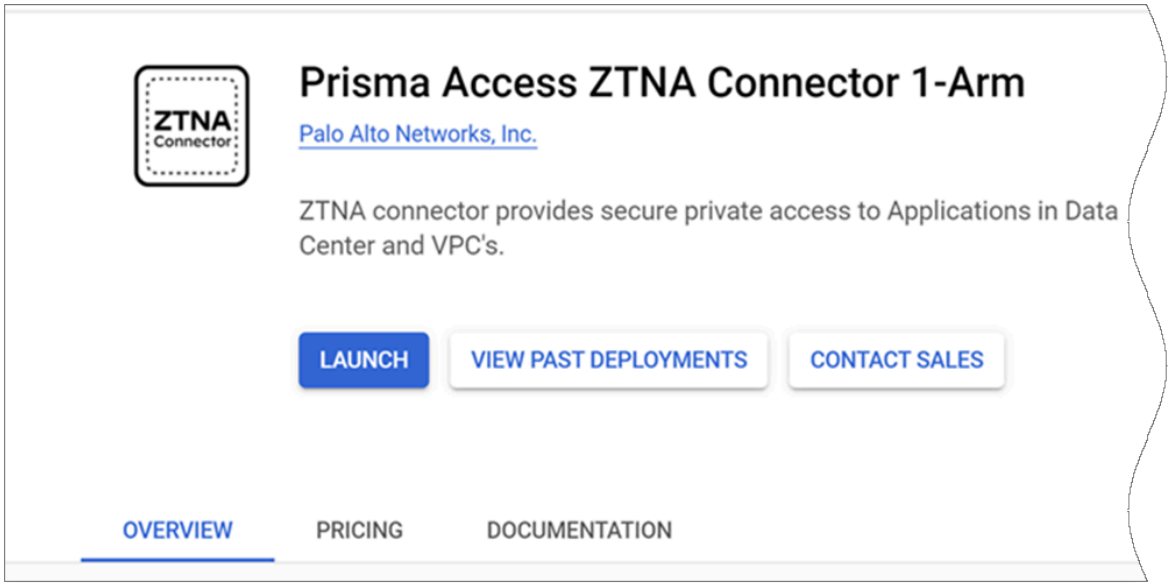
STEP 2 | 要件に最適なソフトウェア プランを選択してください。

- Prisma AccessZTNA Connector 1-Arm
- Prisma Access ZTNA Connector 2-Arm

GCP にZTNA Connector 1-Armをデプロイする

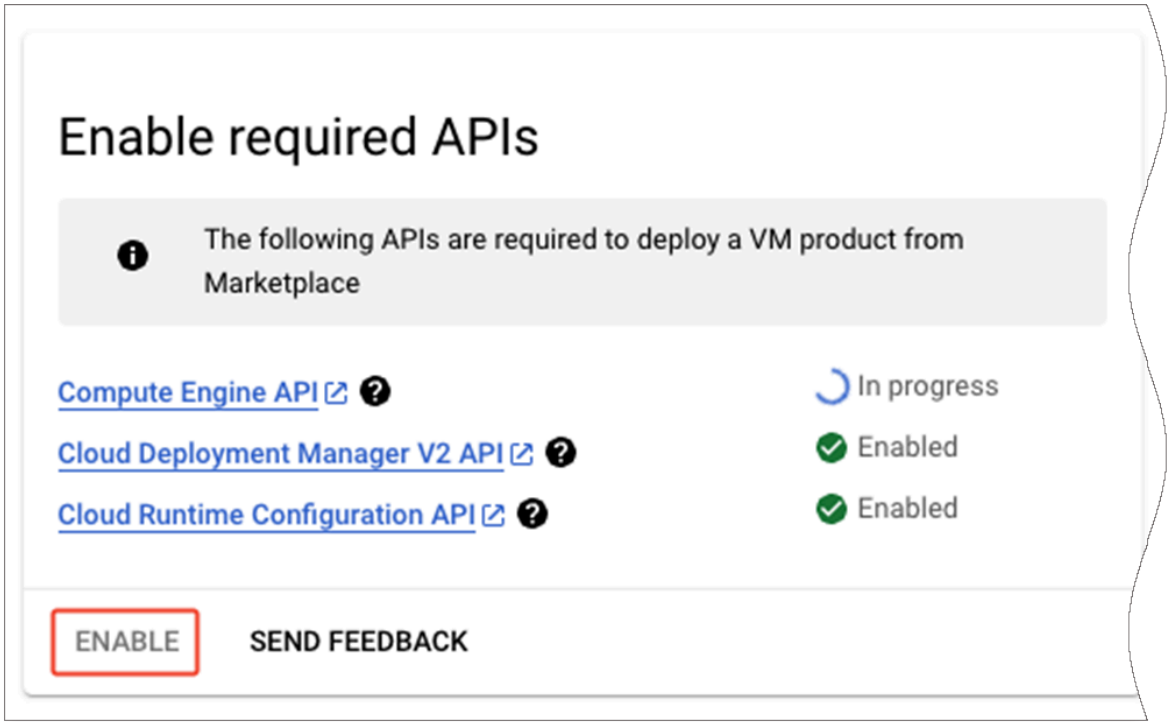
GCPに ZTNA Connector 1-Armをデプロイするには、次の手順に従います。

STEP 1 | 起動して ZTNA Connector 1-Arm を設定します。



©2025 Palo Alto Networks, Inc.

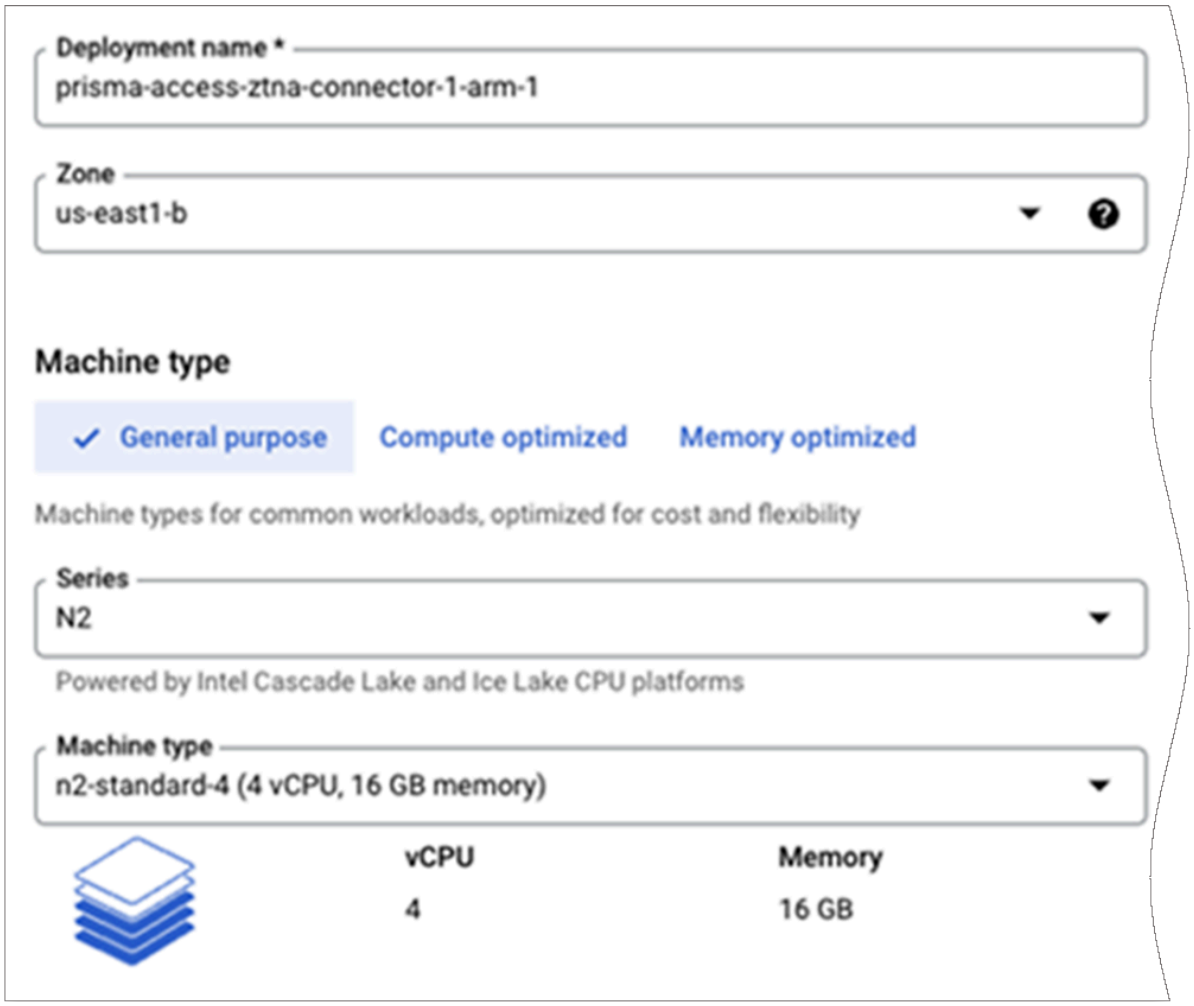
STEP 2 | (任意) マーケットプレイスから仮想マシンをデプロイするために必要なGCP APIを有効にします。



©2025 Palo Alto Networks, Inc.

STEP 3 | 以下の設定を行います。

- 仮想マシンを識別できるデプロイメント名を入力します。
- このコネクタのアプリケーションがデプロイされているゾーンを選択します。
- マシンタイプのデフォルト値を使用してください。このコネクタの認定マシンタイプは**n2-standard-4**です。

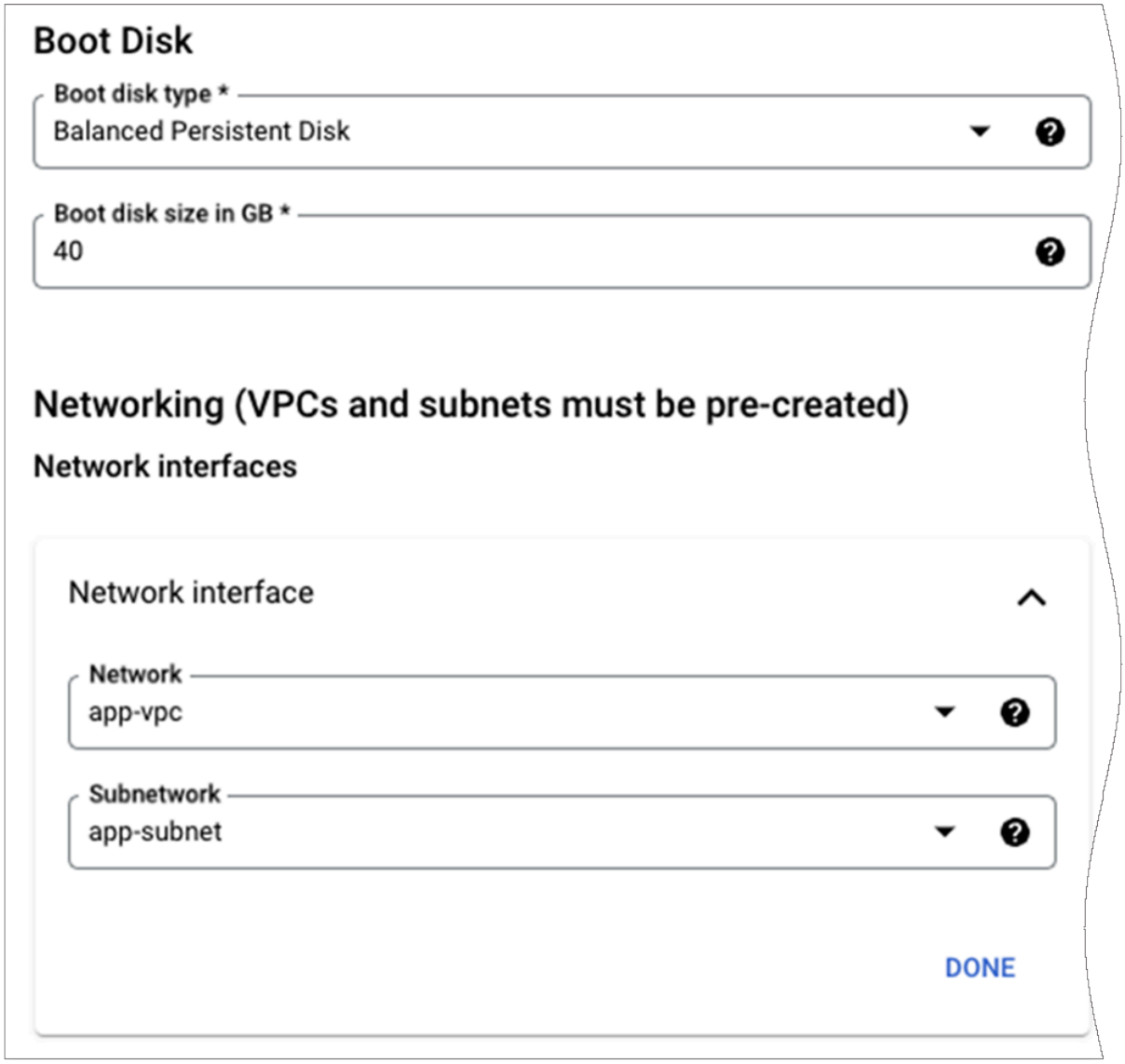


- Prisma SASE ポータルから取得した**Prisma ZTNA** コネクタ ライセンス キー と**Prisma ZTNA** コネクタ ライセンス シークレットの値を入力します。



 ©2025 Palo Alto Networks, Inc.

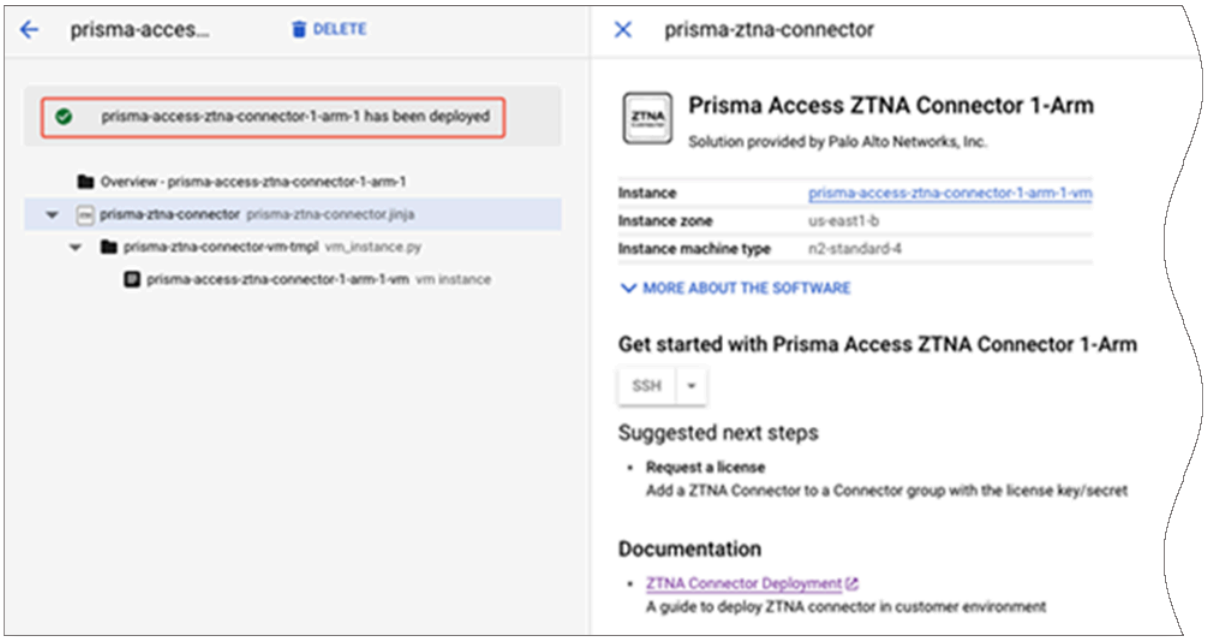
- ブートディスクセクションで以下を設定します。
  - デフォルトのブートディスクタイプを使用してください。
  - ブートディスクサイズ **(GB)** として **40 GB** を選択します。
- [ネットワーク **(VPC** とサブネットは事前に作成しておく必要があります**)]** セクションをデプロイし、ネットワークインターフェイスの詳細]を選択します。
  - 作成したサブネットを含むネットワークを選択します。
  - 使用する仮想マシンのサブネットワークを選択します。



STEP 4 | **Done (**完了**)**をクリックします。

©2025 Palo Alto Networks, Inc.

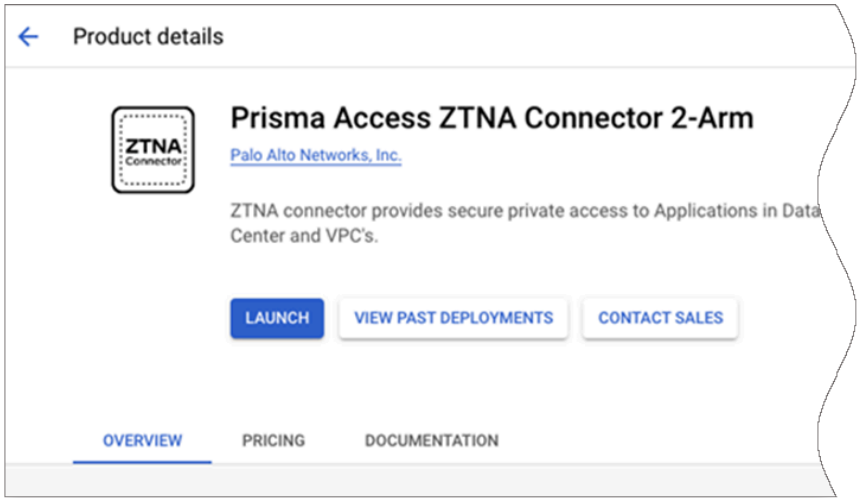
STEP 5 | **Deploy(デプロイ)** をクリックしてオンボーディングプロセスを完了します。



GCP にZTNA Connector 2-Armをデプロイする

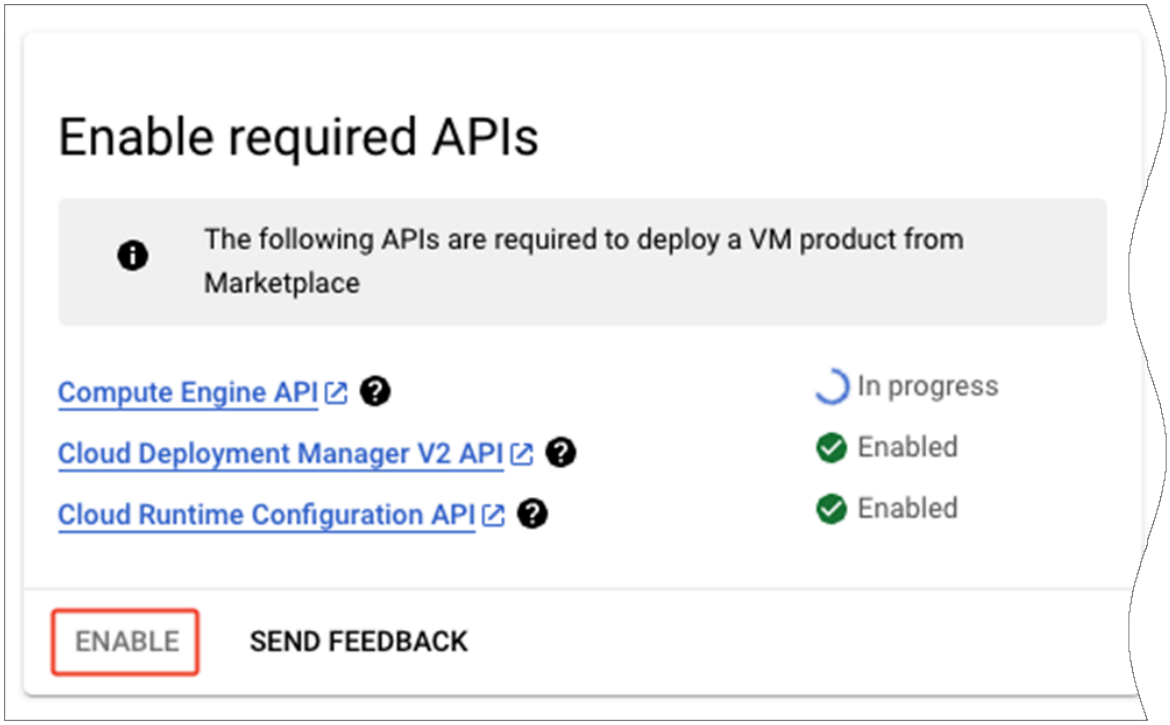
GCPに ZTNA Connectorをデプロイするには、次の手順に従います。

STEP 1 | 起動して設定します。



 ©2025 Palo Alto Networks, Inc.

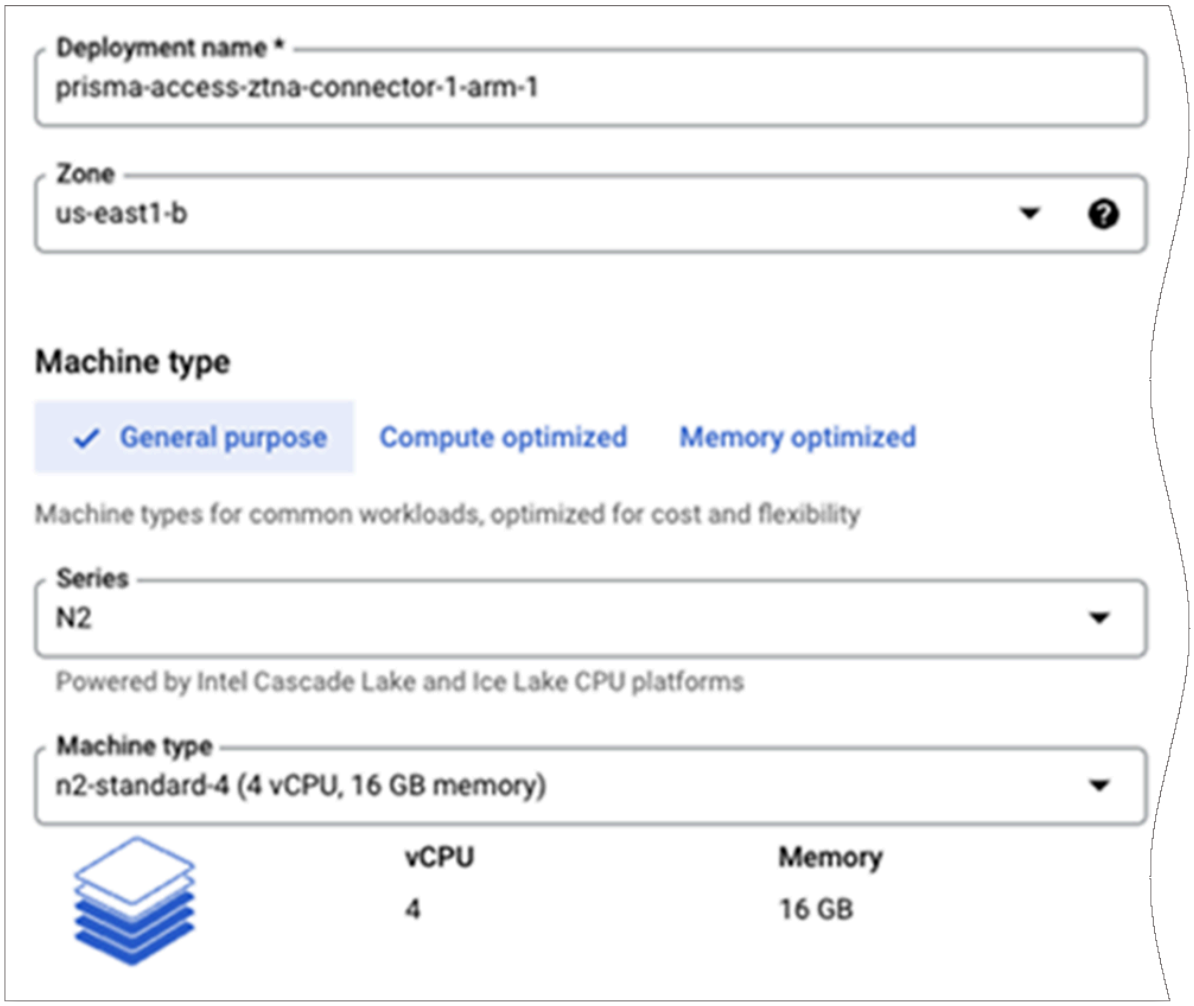
STEP 2 | (任意) マーケットプレイスから仮想マシンをデプロイするために必要なAPIを有効にします。



©2025 Palo Alto Networks, Inc.

STEP 3 | 以下の設定を行います。

- 仮想マシンを識別できるデプロイメント名を入力します。
- このコネクタのアプリケーションがデプロイされているゾーンを選択します。
- マシンタイプのデフォルト値を使用してください。このコネクタの認定マシンタイプは**n2-standard-4**です。

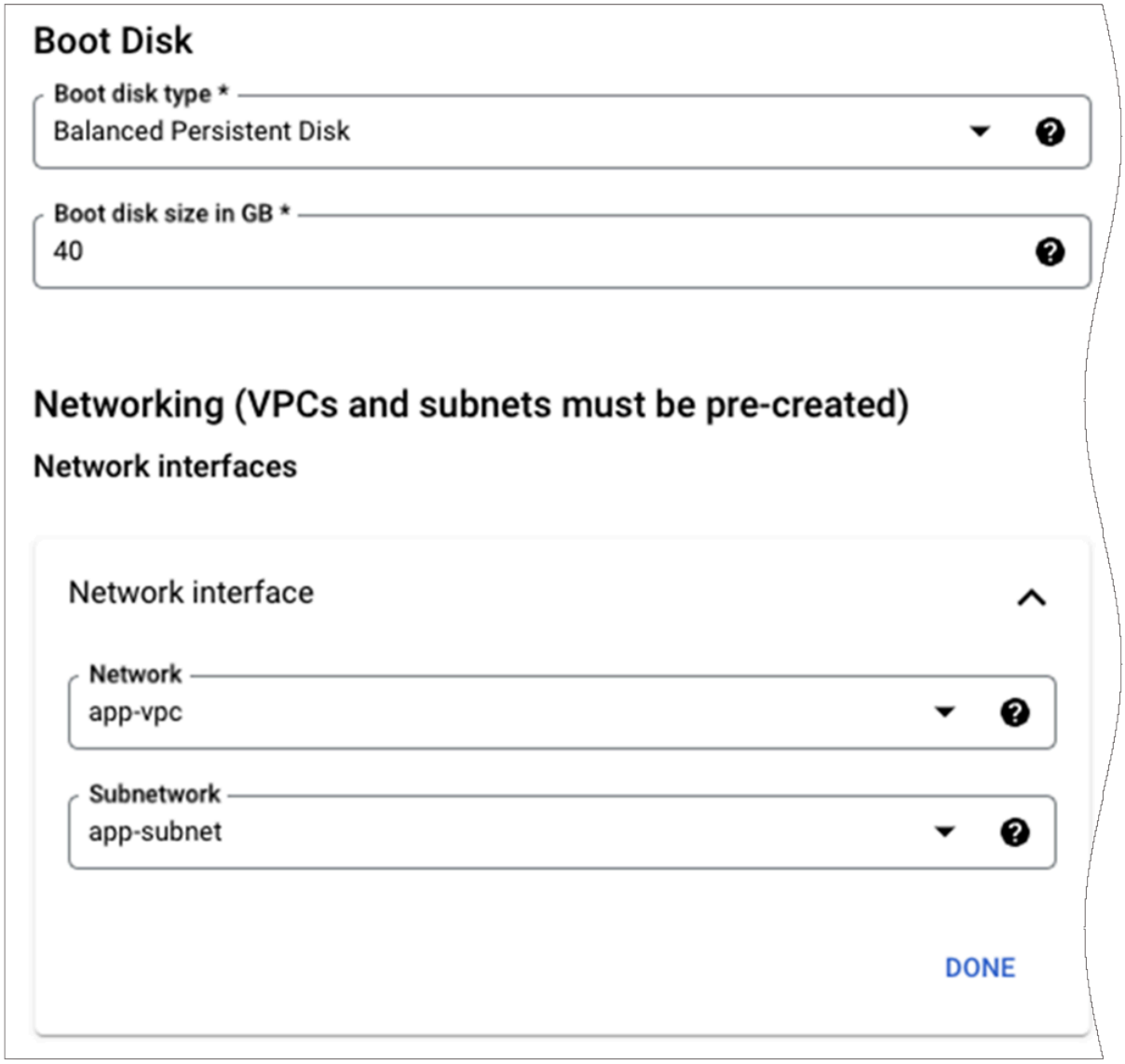


- Prisma SASE ポータルから取得した**Prisma ZTNA** コネクタ ライセンス キー と**Prisma ZTNA** コネクタ ライセンス シークレットの値を入力します。



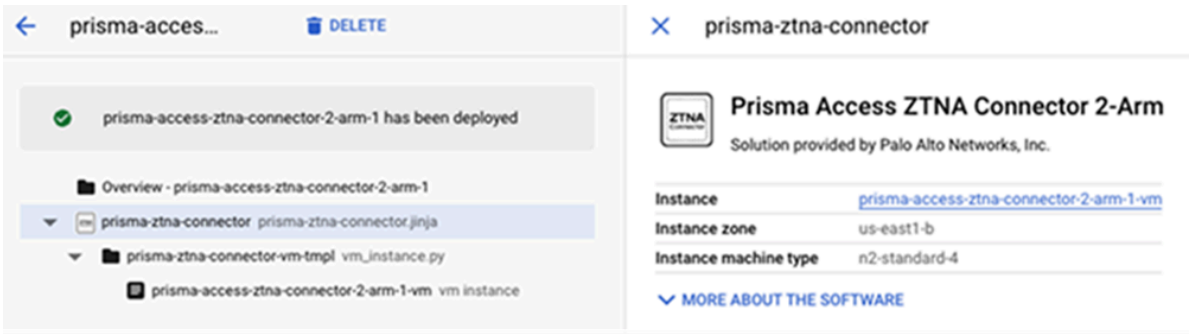
 ©2025 Palo Alto Networks, Inc.

- ブートディスクセクションで:
  - デフォルトのブートディスクタイプを使用してください。
  - ブートディスクサイズ **(GB)** として **40 GB** を選択します。
- [ネットワーク **(VPC** とサブネットは事前に作成しておく必要があります**)**] セクションをデプロイし、ネットワークインターフェイスの詳細]を選択します。
  - 作成したサブネットを含むネットワークを選択します。
  - 使用する仮想マシンのサブネットワークを選択します。



 ©2025 Palo Alto Networks, Inc.

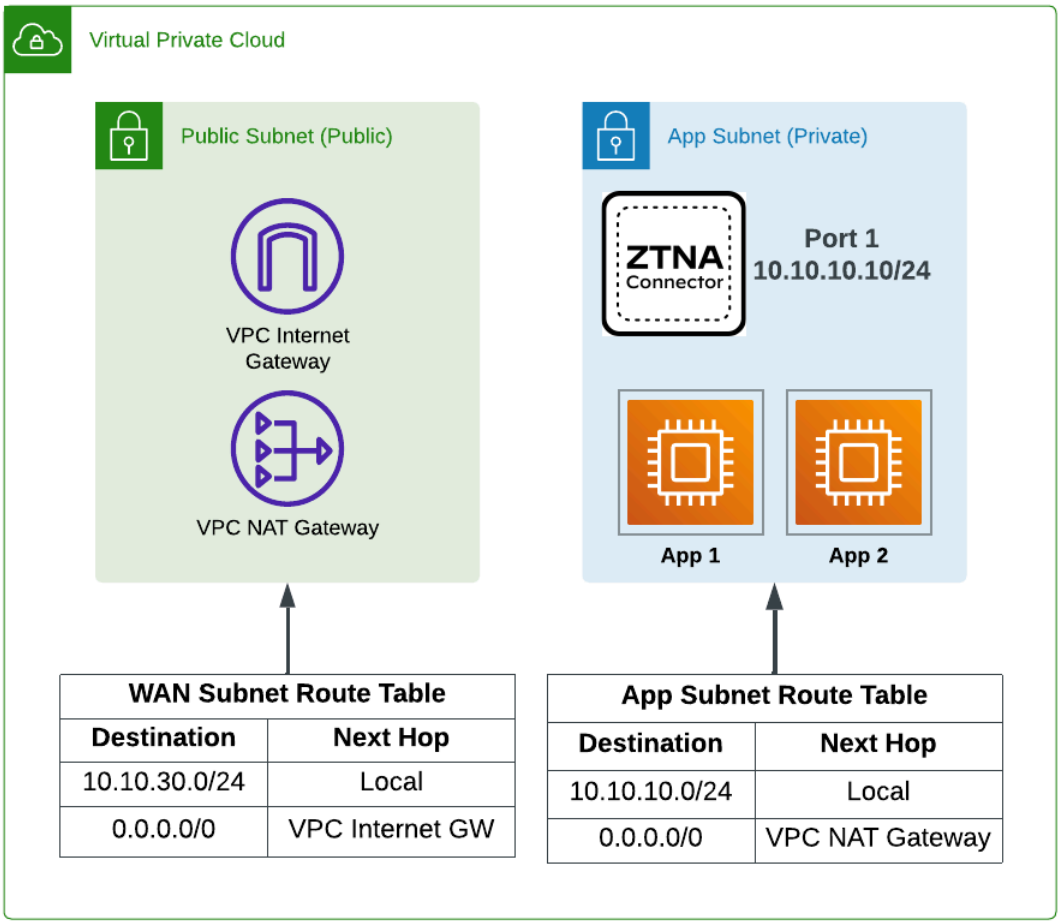
STEP 4 | **Deploy(デプロイ)** をクリックしてオンボーディングプロセスを完了します。



ZTNAコネクタでサポートされるAmazon Web Servicesデプロイメント

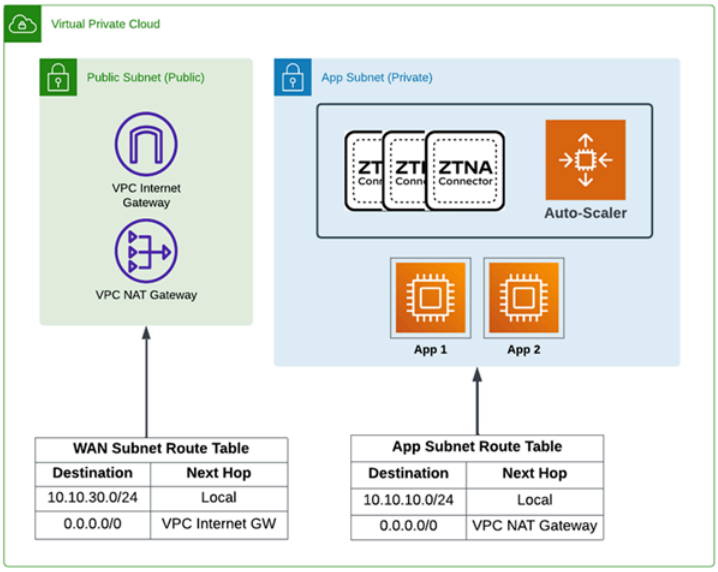
Prisma Access Amazon Web Services (AWS) のZTNAコネクタ ネットワーク デプロイメントでは、3つのデプロイメントと、各デプロイメントに対応するテンプレートがサポートされます。

次の図はサンプルを示しています Prisma Access NATゲートウェイを使用したワンアーム モードを使用したAWSでのZTNAコネクタのデプロイメント。

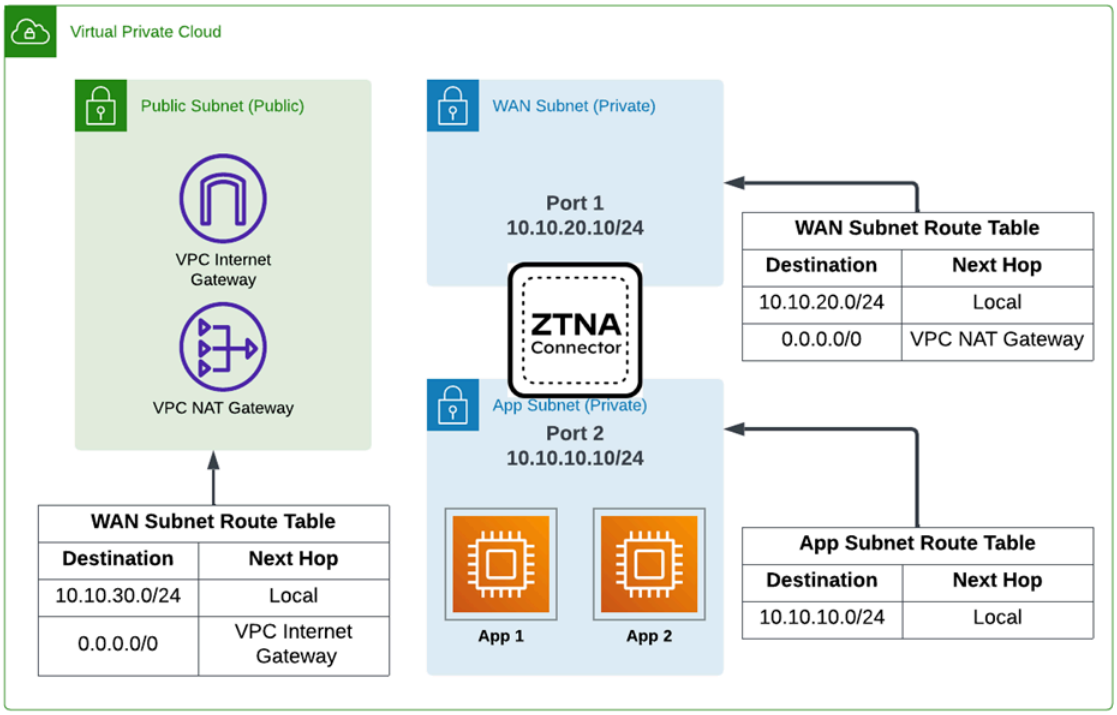


©2025 Palo Alto Networks, Inc.

次の図は、NATゲートウェイを使用したワンアーム自動スケーリングを使用したAWSでのZTNAコネクタのデプロイメントのサンプルを示しています。



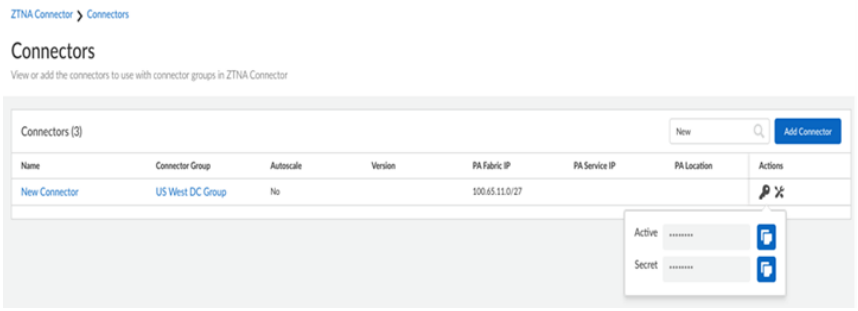
次の図は、NATゲートウェイを使用した2アームモードを使用したAWSでのZTNAコネクタのデプロイメント例を示しています。



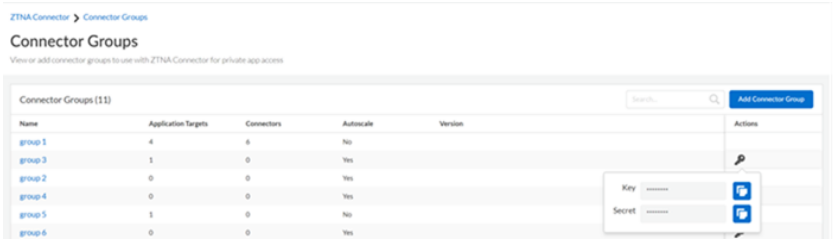
©2025 Palo Alto Networks, Inc.

Amazon Web ServicesにZTNAコネクタをオンボードする

- Amazon Web Services (AWS) で ZTNA コネクタを使用するために 構成する必要がある要件とガイドライン および FQDN とポートを確認します。
- Prisma SASEプラットフォームで、コネクタ キーとシークレットの値を取得してコピーします。ワークフロー > **ZTNA**コネクタ > コネクタで、この VM に関連付けるためにPrisma Accessで作成したコネクタ・オブジェクトを見つけ、「**Copy Token**」を選択し、次に**Key(**キー**)**と**Secret(**シークレット**)**の値をコピーします。



- **Prisma AccessZTNA Connector 1-Arm Auto-Scaling**のデプロイメントでは、Connector Group(コネクタグループ)キーとシークレット値を取得してコピーする必要があります：ワークフロー > **ZTNA**コネクタ > コネクタグループで、このVMに関連付けるためにPrisma Accessで作成したコネクタ・オブジェクトを見つけ、「**Copy Token**」を選択し、次に**Key(**キー**)**と**Secret(**シークレット**)**をコピーします。



すべての前提条件を満たしたら、以下の手順に従ってAWSにPrisma AccessZTNA Connectorをオンボードします。

STEP 1 | AWS Marketplaceにアクセスし、**Prisma Access ZTNA Connector**を検索します。

STEP 2 | 要件に最適なソフトウェア プランを選択してください。

- Prisma AccessZTNA Connector 1-Arm
- Prisma AccessZTNA Connector 1-Arm自動スケーリング
- Prisma Access ZTNA Connector 2-Arm

AWSにZTNA Connector 1-Armをデプロイする

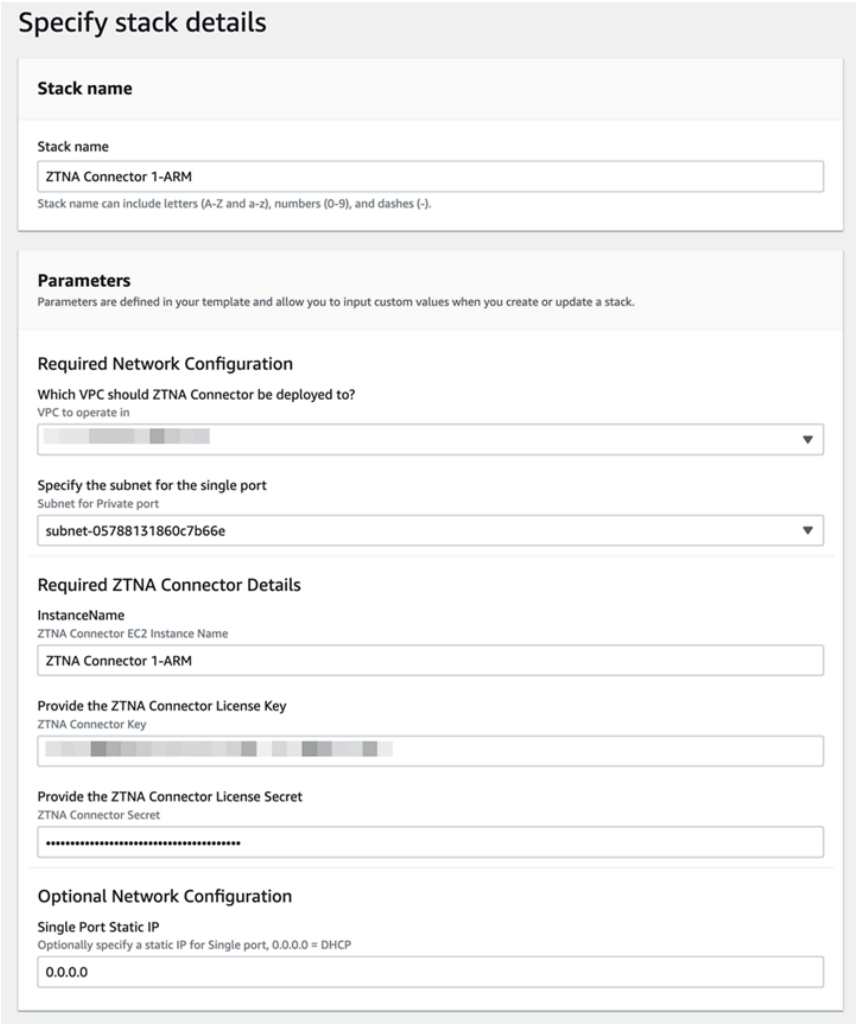
AWSにZTNA Connector 1-Armをデプロイするには、次の手順に従います。

STEP 1 | **Prisma AccessZTNA Connector 1-Arm** クラウド形成テンプレートを選択します。

©2025 Palo Alto Networks, Inc.

STEP 2 | スタックの詳細の指定 ページで以下を設定します。

- スタックを識別するための スタック名 を入力します。
- [パラメータ] セクションで、スタック テンプレートで定義されているパラメータを指定します。
  - **ZTNA** コネクタをどの **VPC** にデプロイするかを選択します。
  - このコネクタにオンボードするアプリケーションをプロビジョニングした単一ポートのサブネットを指定します。このサブネットからNATゲートウェイ経由でインターネットにアクセスする必要があります。
- Prisma SASE ポータルから取得した Prisma**ZTNA** コネクタ ライセンス キー と Prisma**ZTNA** コネクタ ライセンス シークレットの値を入力します。



AWSで自動スケーリングを使用して**ZTNA Connector 1-Arm**をデプロイする

AWSで自動スケーリングを備えたZTNA Connector 1-Armをデプロイするには、次の手順に従います。

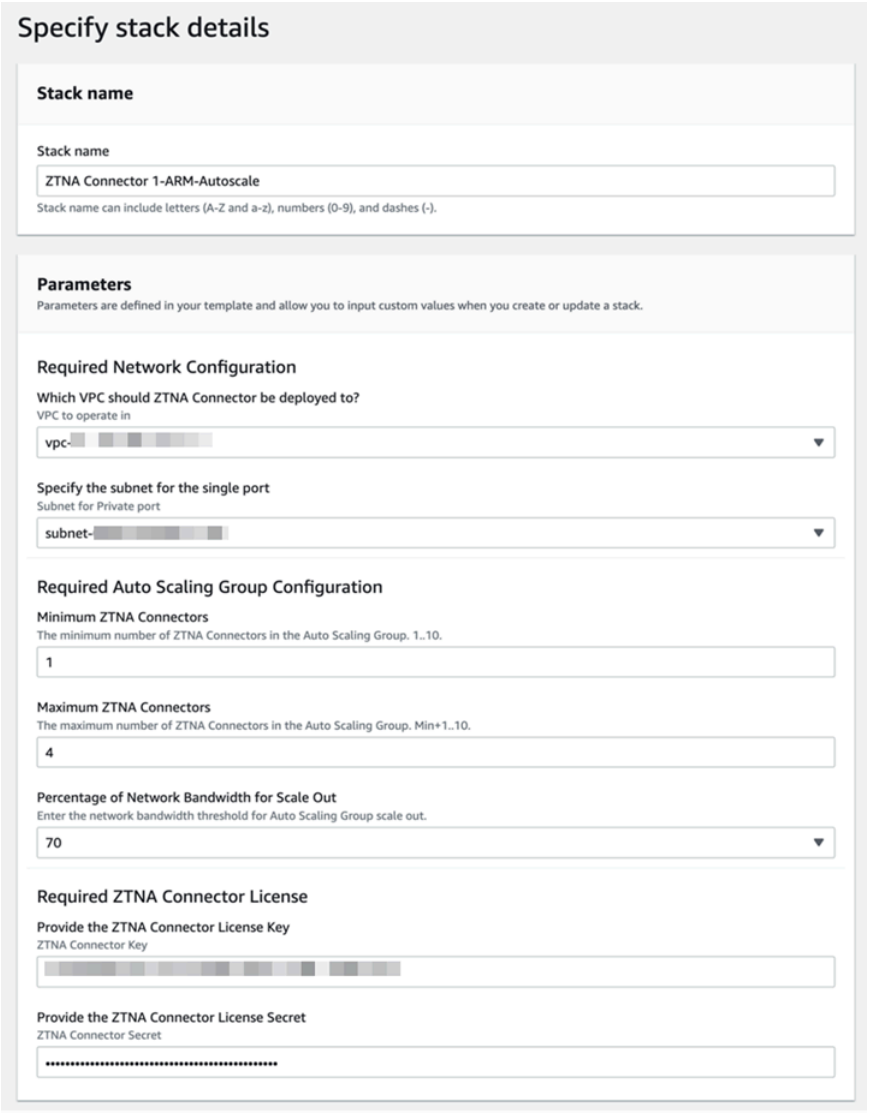
STEP 1 | **Prisma AccessZTNA Connector 1-Arm**自動スケーリングクラウド形成テンプレートを選択します。

©2025 Palo Alto Networks, Inc.

STEP 2 | スタックの詳細の指定ページで次のパラメータを設定します。

- デプロイメントの一意のスタック名を入力します。
- [パラメータ] セクションで、スタック テンプレートで定義されているパラメータを指定します。
  - **ZTNA** コネクタをどの **VPC** にデプロイするかを選択します。
  - このコネクタにオンボードするアプリケーションをプロビジョニングした単一ポートのサブネットを指定します。このサブネットからNATゲートウェイ経由でインターネットにアクセスする必要があります。
- 必要な自動スケーリング グループ設定にて:
  - 自動スケーリング グループに必要な最小**ZTNA**コネクタ数 を入力します。
  - 自動スケーリング グループに必要な 最大**ZTNA**コネクタ数 を入力します。コネクタ グループで許可される ZTNA コネクタの最大数は4です。
  - スケールアウトのネットワーク帯域幅の割合を設定します。デフォルトおよび推奨値は70%です。
- Prisma SASE ポータルから 取得した**ZTNA** コネクタ ライセンス キー と **ZTNA** コネクタ ライセンス シークレットの 値を入力します。

©2025 Palo Alto Networks, Inc.



AWSにZTNA Connector 2-Armをデプロイする

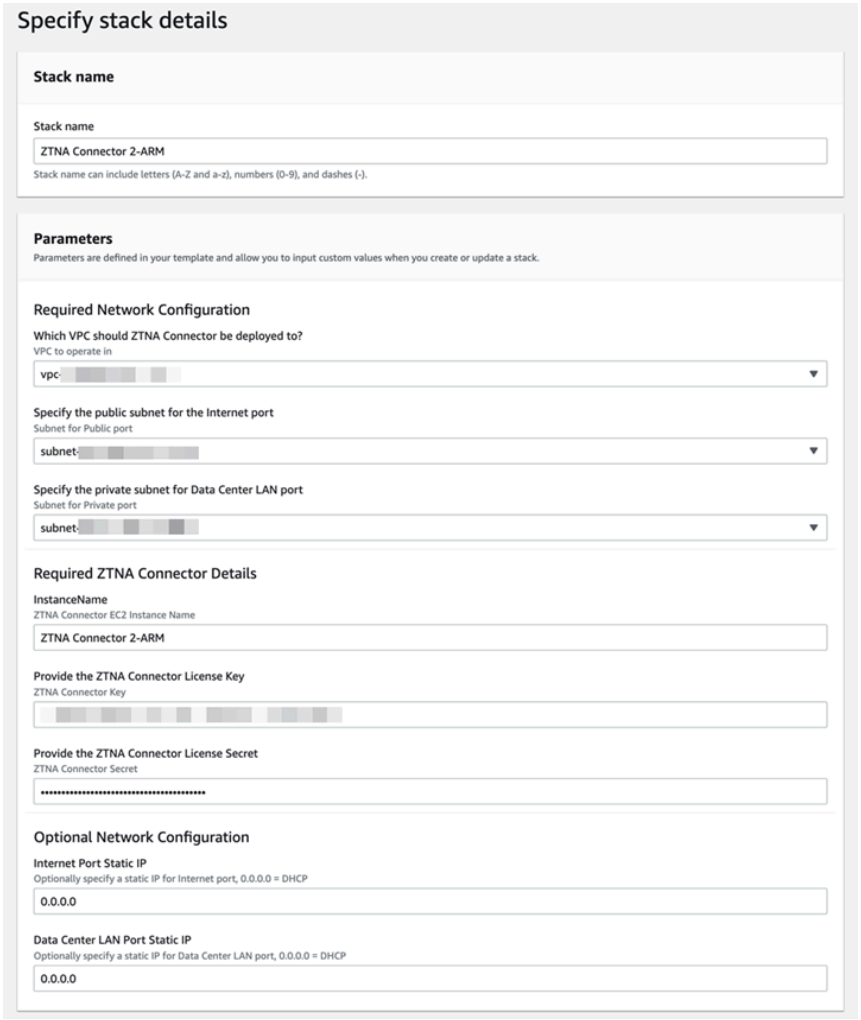
AWS に ZTNA Connector 2-Armをデプロイするには、次の手順に従います。

STEP 1 | Prisma AccessZTNA Connector 1-Armデプロイメント クラウド形成テンプレートを選択します。

©2025 Palo Alto Networks, Inc.

STEP 2 | スタックの詳細の指定 ページで、次の操作を行います。

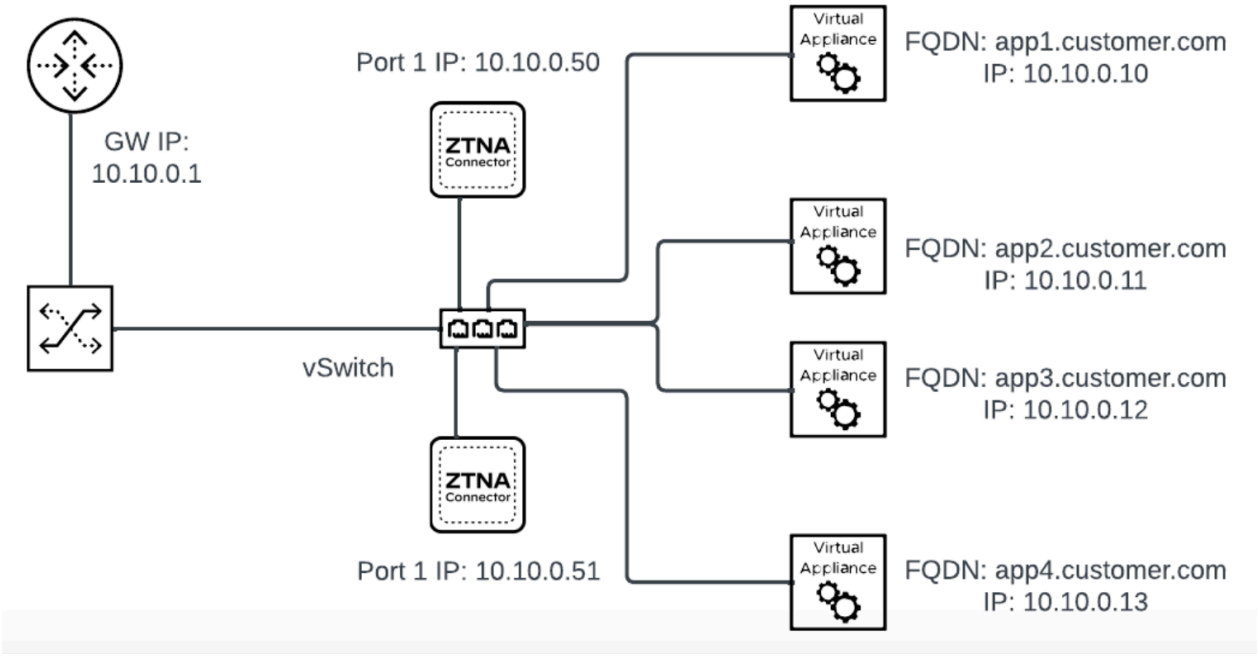
- デプロイメントの スタック名 を入力します。
- [パラメータ] セクションで、スタック テンプレートで定義されているパラメータを指定します。
  - **ZTNA** コネクタをどの **VPC** にデプロイするかを選択します。
  - IPSec への WAN 接続用のインターネット ポートのパブリック サブネットを指定します 。このサブネットは、インターネット接続のためにNATゲートウェイに関連付ける必要があります。
  - このコネクタにオンボードするアプリケーションをプロビジョニングしたデータセンター**LAN**ポートのプライベートサブネットを指定します。。
- インスタンス名を入力してください
- Prisma SASE ポータルから取得した Prisma**ZTNA** コネクタ ライセンス キー と Prisma**ZTNA** コネクタ ライセンス シークレットの値を入力します。



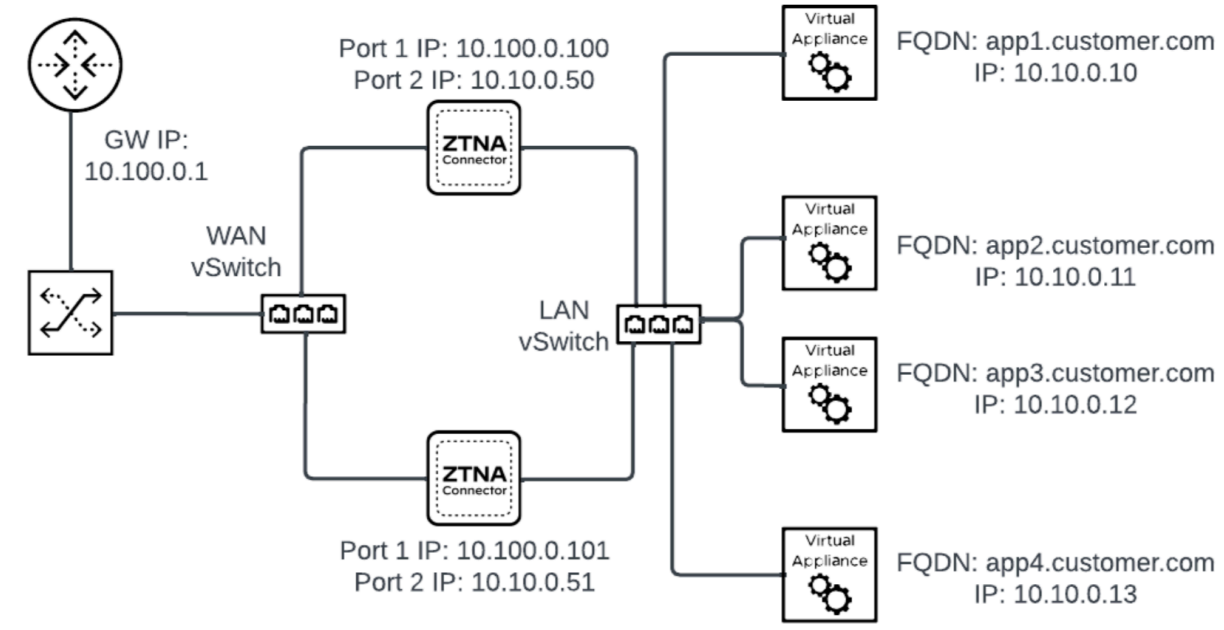
 ©2025 Palo Alto Networks, Inc.

Prisma Access ZTNAコネクタがサポートするVMware ESXiのデプロイメント

次の図は、NATゲートウェイを備えたワンアーム モードでVMware ESXiを使用するZTNAコネクタ ネットワーク デプロイメントの例を示したものです。



次の図は、NATゲートウェイを備えた2アーム モードでVMware ESXiを使用するZTNAコネクタ ネットワーク デプロイメントの例を示したものです。



©2025 Palo Alto Networks, Inc.

VMware ESXiにZTNAコネクタをオンボードする

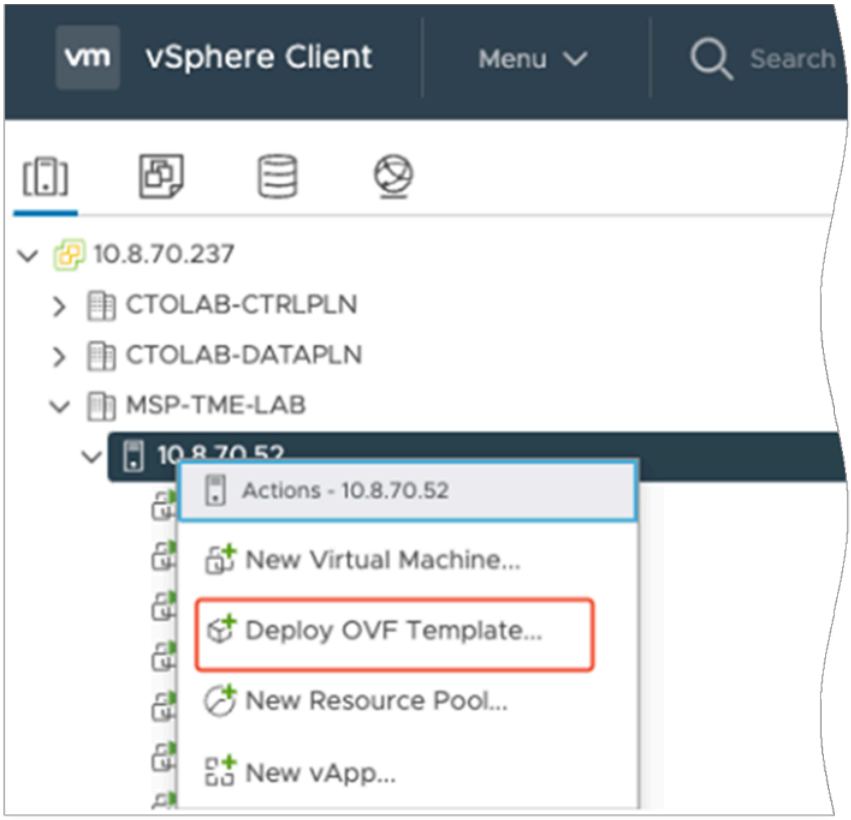
VMware ESXiにZTNAコネクタをオンボードするには、次の手順を実行します。開始する前に、ZTNA全般、特にVMware ESXiデプロイメントの要件とガイドラインを必ず確認してください。

始める前に、Microsoft Azureで ZTNAコネクタを使用するために構成する必要がある要件とガイドライン および FQDN とポートを確認します。

STEP 1 | カスタマーサポートポータル（CSP） の **[アップデート] > [ソフトウェアアップデート] > Prisma Access ZTNA Connector for Hyper-V (VMware ESXi用のZTNAコネクタ)**からZTNAコネクタVMware ESXiイメージをダウンロードします。

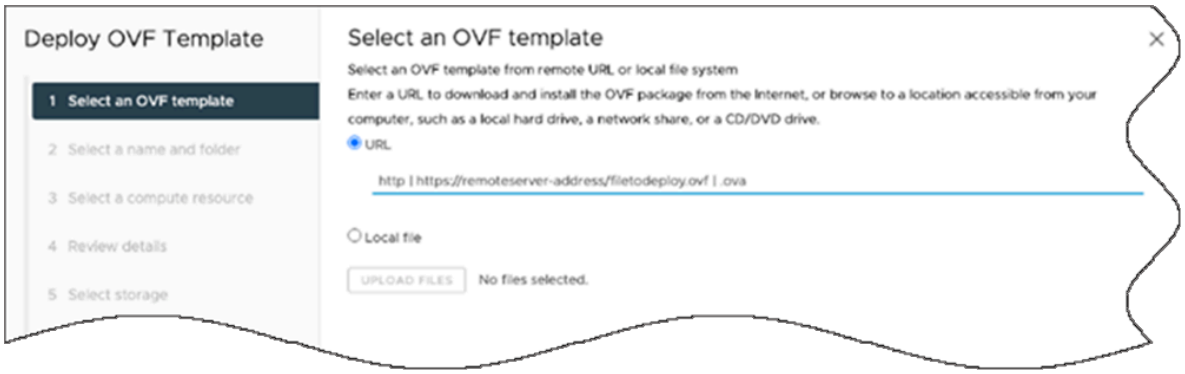
片側デプロイメントの場合は*1 NIC*バージョン ファイルをダウンロードし、両側デプロイメントの場合は*2 NIC*バージョン ファイルをダウンロードします。

STEP 2 | VMware vCenterを開き、ホストを選択して右クリックし、**[OVF**テンプレートのデプロイ]を選択します。

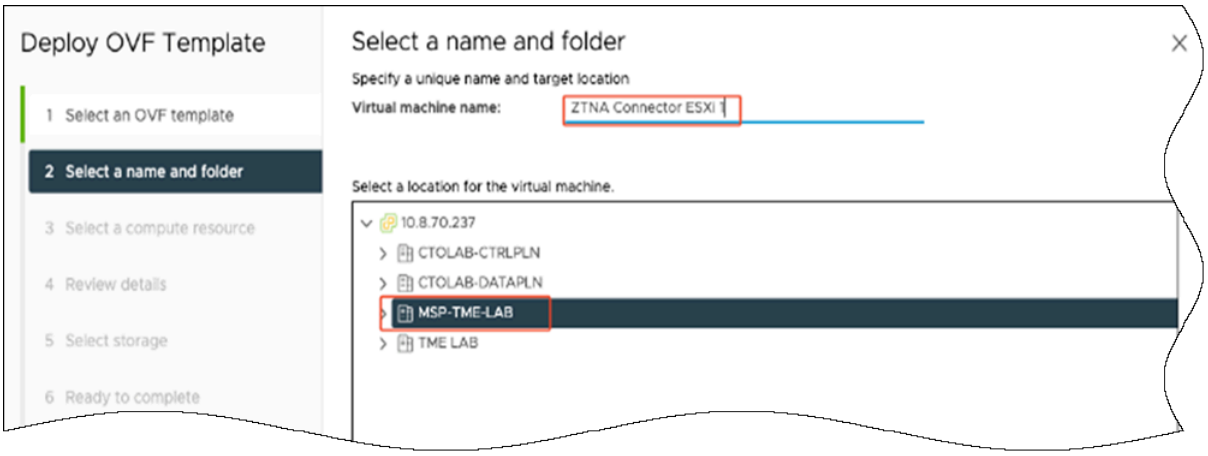


©2025 Palo Alto Networks, Inc.

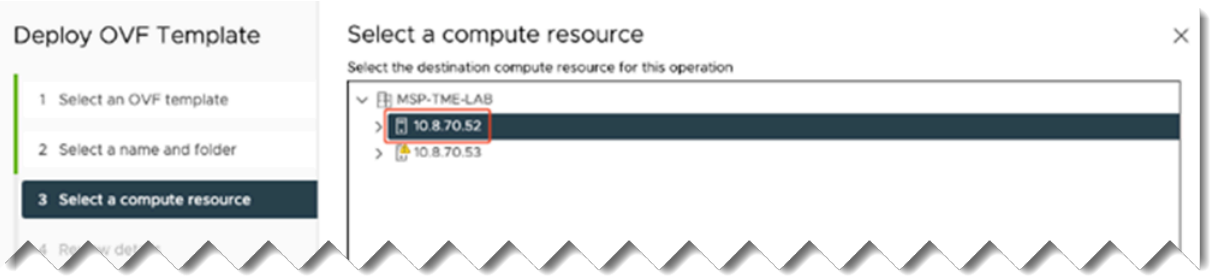
STEP 3 | コネクタOVAから場所 (URL またはローカル ファイル) を選択し、[次へ]を選択します。



STEP 4 | 仮想マシン (VM) の名前とVMの場所を入力します。

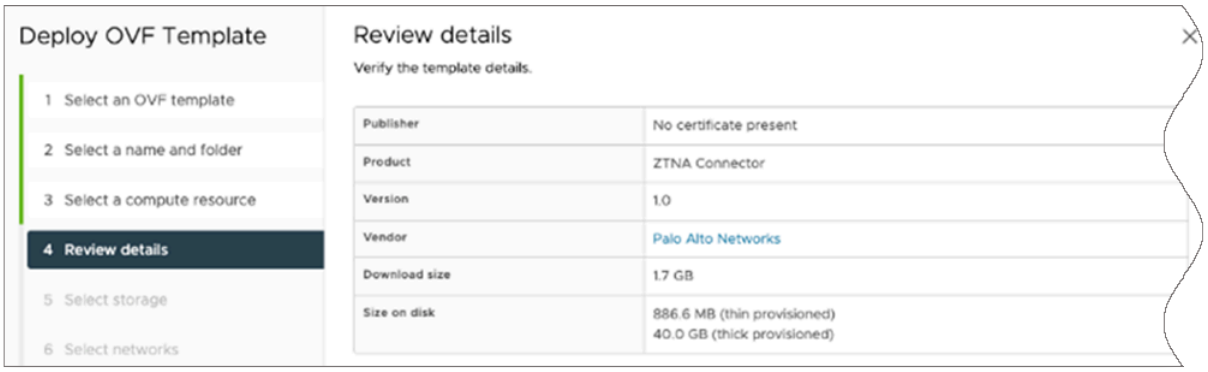


STEP 5 | VMのコンピューティング リソースを選択します。

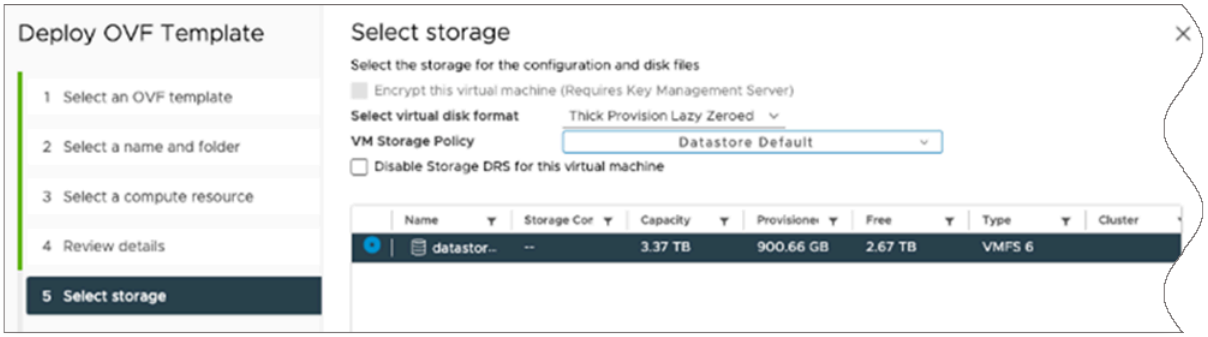


©2025 Palo Alto Networks, Inc.

STEP 6 | テンプレートの詳細を確認し、[次へ]を選択します。



STEP 7 | 仮想ディスク形式として **[Thick Provision Lazy Zeroed]** を選択し、ZTNAコネクタVMに適切なデータストアを選択します。



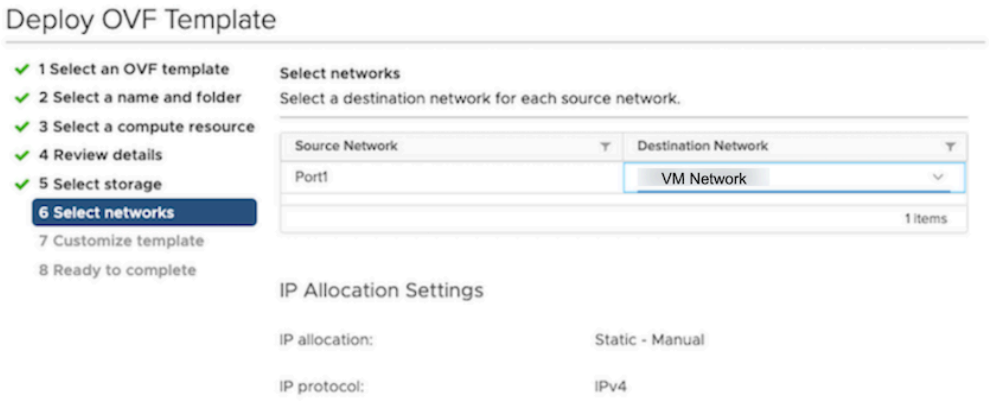
任意 仮想ディスク形式に**Thin Provision (**シン プロビジョニング**)**を選択し、ZTNAコネクタVMに適切なデータストアを選択します。この場合、要件に応じて、サーバーはホストに必要なスペースのみを割り当てます。



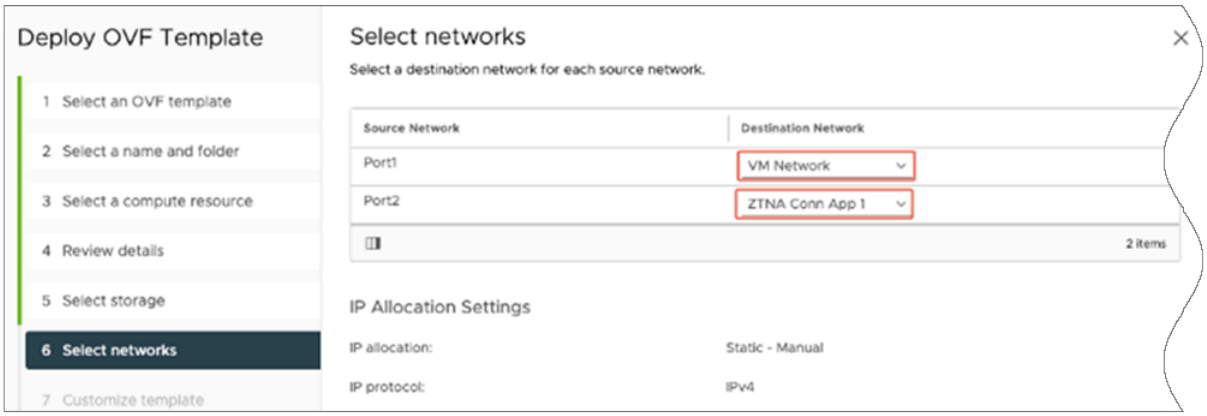
©2025 Palo Alto Networks, Inc.

STEP 8 | OVA構成テンプレートを使用して作成したインターフェースのネットワーク (ポート 1 およびポート 2) を選択します。

1. one-arm connector (ワンアーム コネクタ)をデプロイする場合、ポート **1**はWANおよびLANアプリケーション サーバーにアクセスできるネットワークです。ポート **1**のWAN/LAN ネットワークを選択します。



2. 2 アーム コネクタをデプロイする場合は、 ポート**1** にインターネット接続ポートを選択し、ポート **2**にアプリ サーバー接続ネットワークを選択します。
   - ポート1は、Prisma AccessへのIPSec接続用のWAN側ポートです。
   - ポート 2はアプリ用ポートです。



STEP 9 | まだ行っていない場合は、 ワークフロー > **ZTNA**コネクタ > コネクタに移動し、Prisma Accessで作成したコネクタオブジェクトを見つけます。 このVM に関連付けるトーク

 ©2025 Palo Alto Networks, Inc.

ンを選択し、[アクション]タブ (キー アイコン) から [トークンのコピー] を選択して、キーとシークレットの値をコピーします。



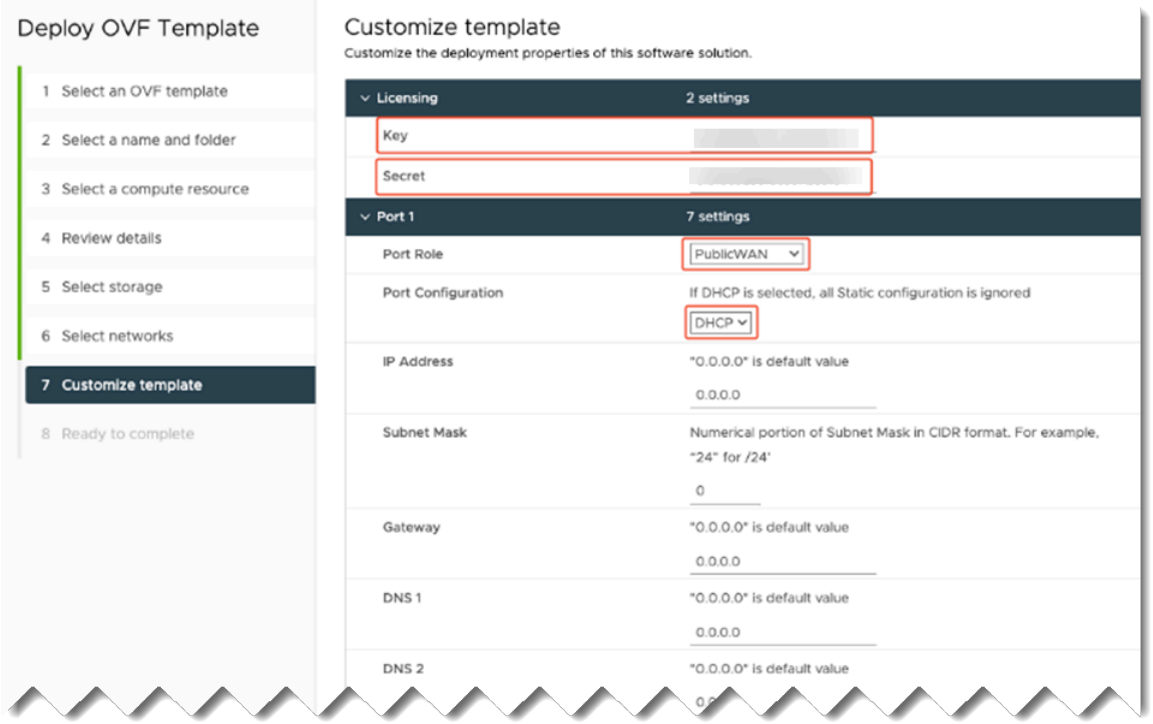
©2025 Palo Alto Networks, Inc.

STEP 10 | テンプレートのカスタマイズ 画面で、次の構成変更を行います。

- ライセンス領域 - Prisma SASEポータルから取得したキーとシークレットの値を入力します。
- ポート**1**（Prisma Accessポート側) 領域 - 次の変更を行います。
  - ロール- パブリック WAN。
  - ポート構成-**DHCP** または**Static**のいずれか。

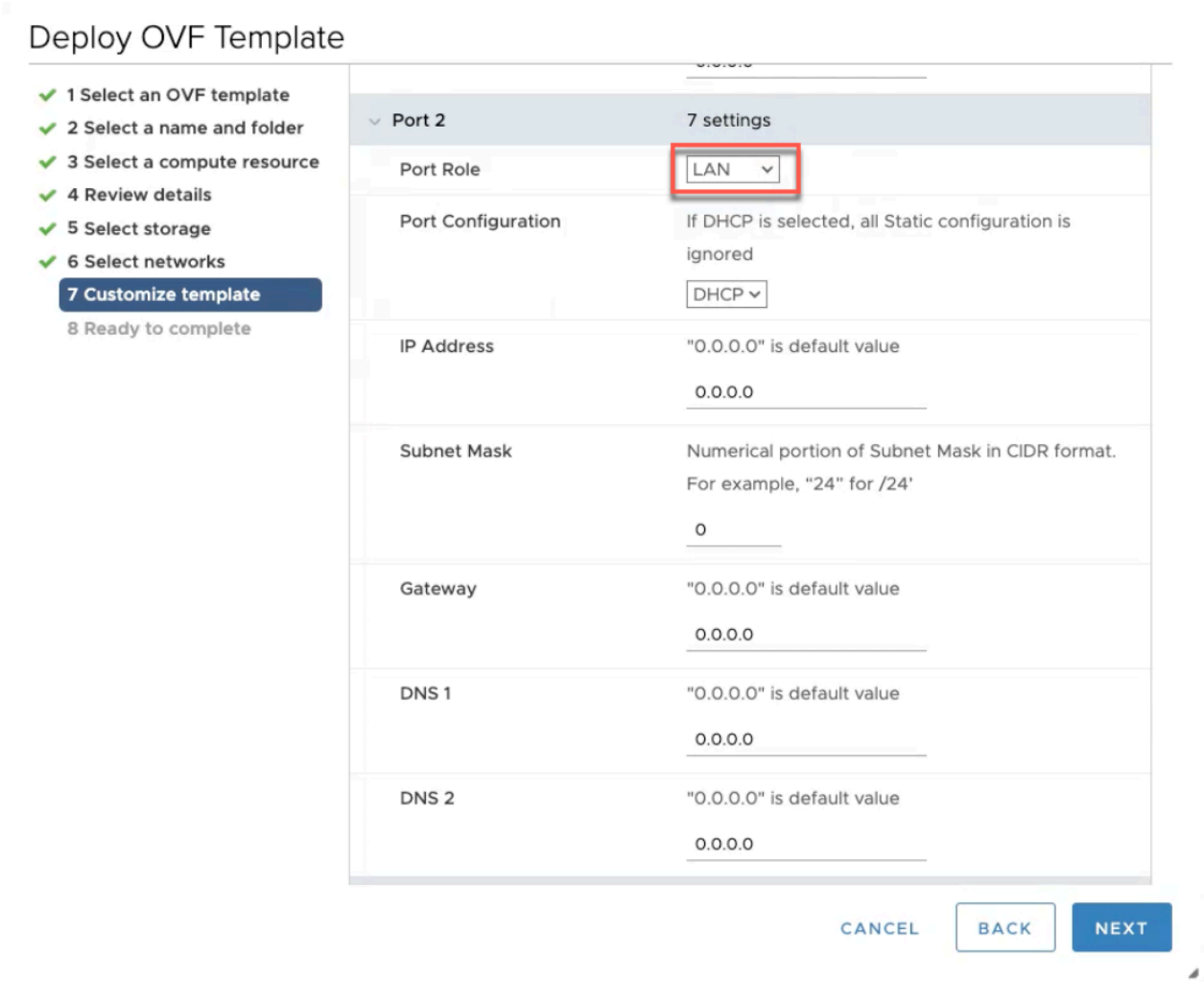
    Staticを選択した場合は、IPアドレス、サブネット マスク、ゲートウェイ、および1つまたは2つのDNSサーバー値を入力します。DHCP

    を使用する場合は、次のスクリーンショットに示すように、フィールドをデフォルトのゼロのままにします。



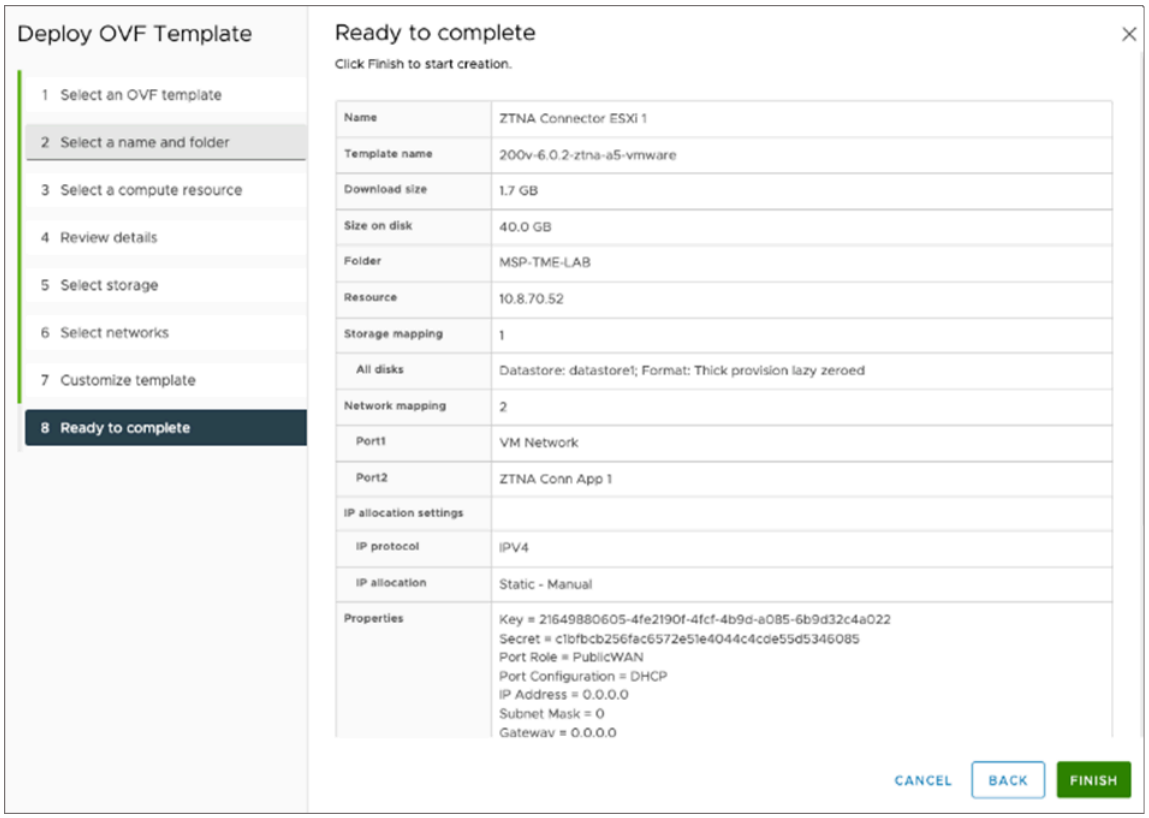
- Two-Arm ESXiデプロイメントのみ Two-Armデプロイメントの場合は、手順10でポート**1**に適用したのと同じルールを使用してポート**2**LAN IPインターフェースを構成します。

©2025 Palo Alto Networks, Inc.



©2025 Palo Alto Networks, Inc.

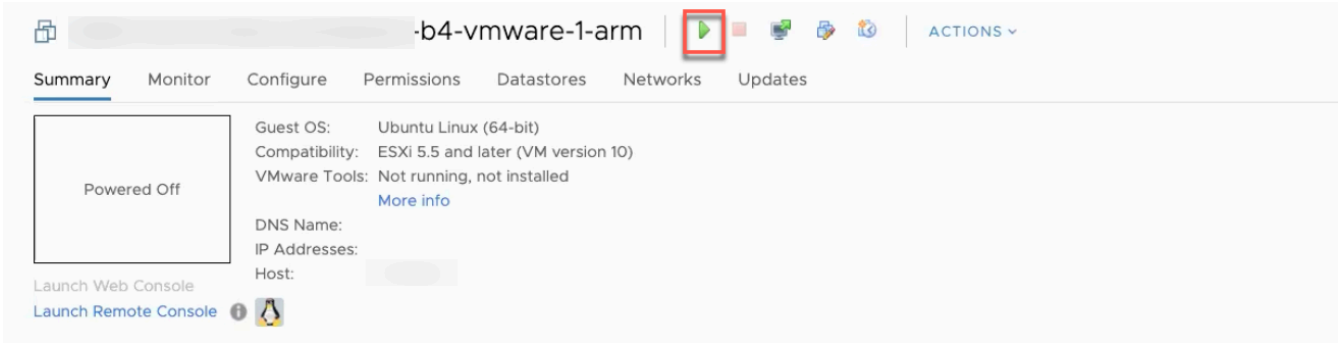
STEP 11 | 概要を確認して、**[Finish (完了)]**を選択します。



©2025 Palo Alto Networks, Inc.

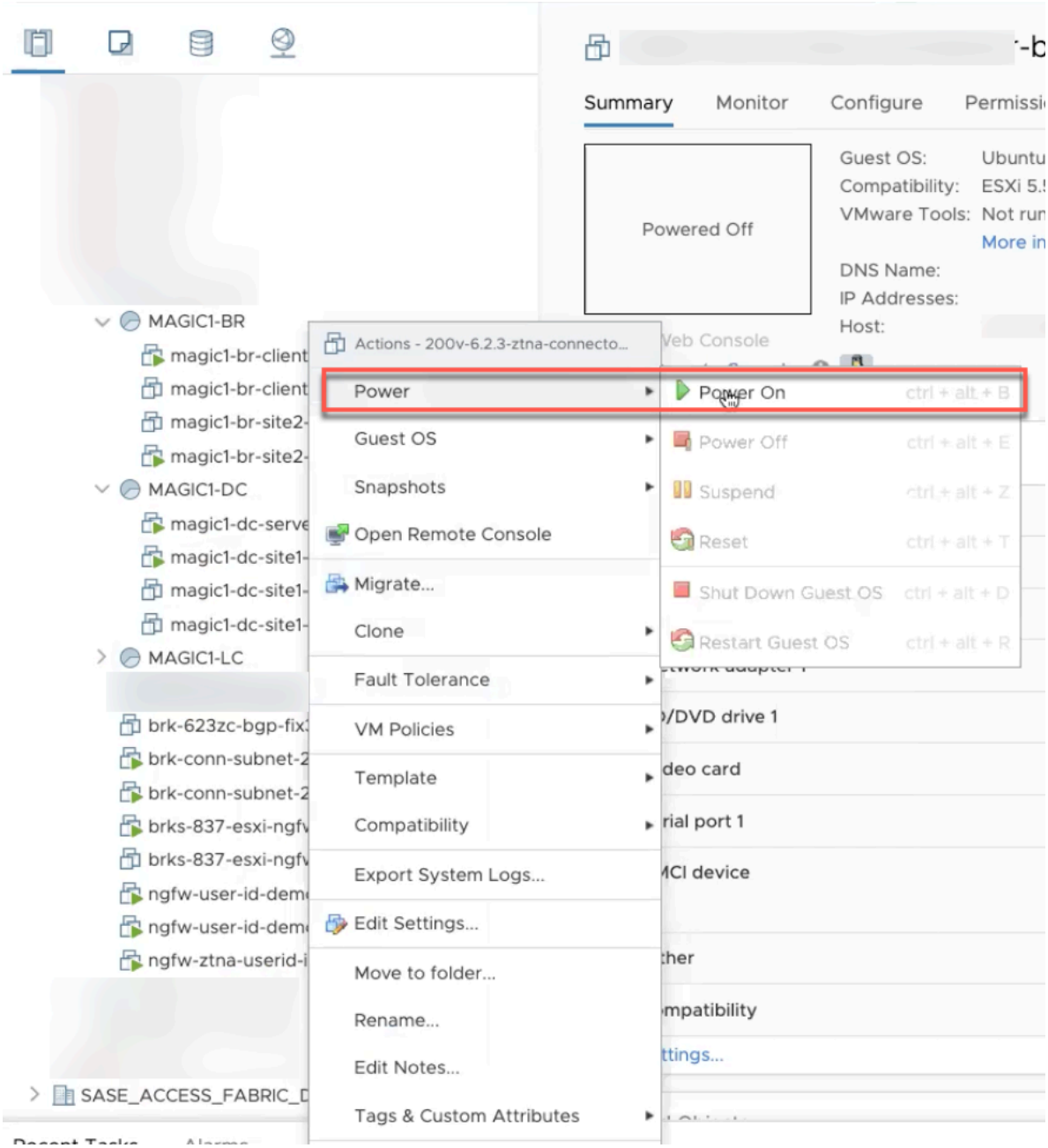
STEP 12 | 次のいずれかの方法を使用してVMの電源をオンにします。

- 仮想サーバーを起動するには、**[Power On (電源オン)]** を選択します。



- インターフェースを右クリックし、**[Power On (電源オン)]([Power (電源) > Power On (電源オン)])** を選択します。

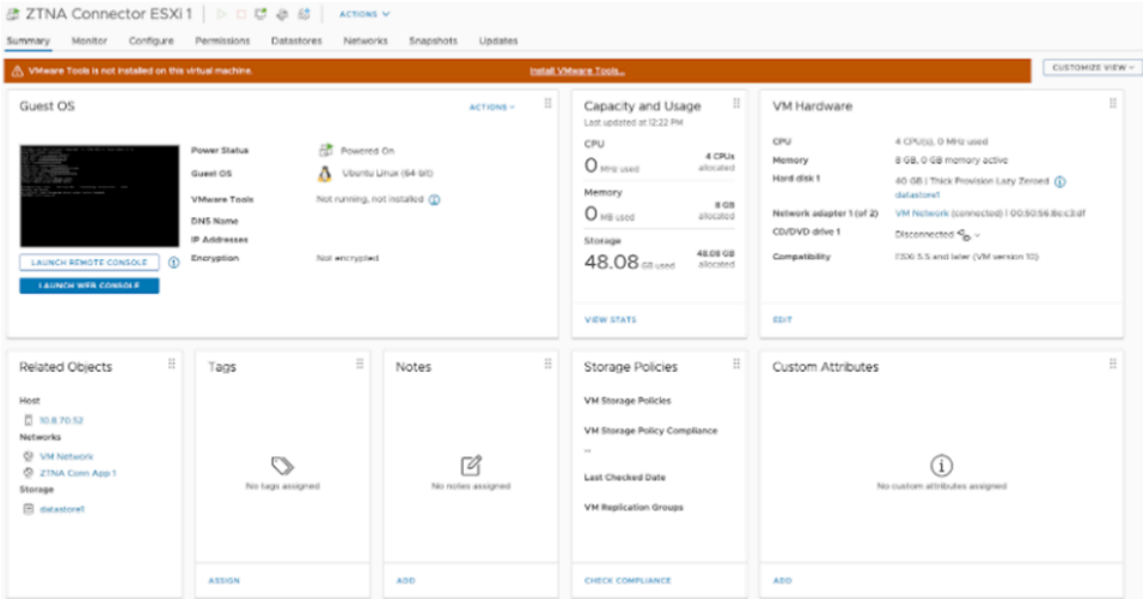
©2025 Palo Alto Networks, Inc.



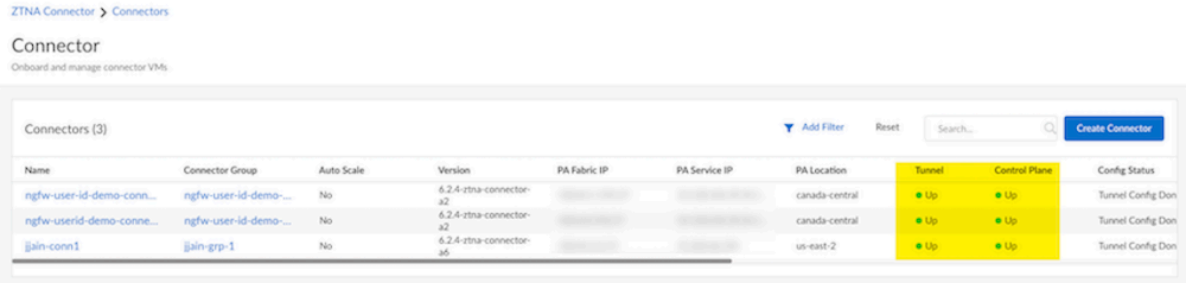
 ©2025 Palo Alto Networks, Inc.

STEP 13 | VMをデプロイした後、起動していることを確認します。

ESXi仮想サーバーが起動したら、 Prisma AccessはZTNAコネクタとして使用するデバイスの構成を完了します。



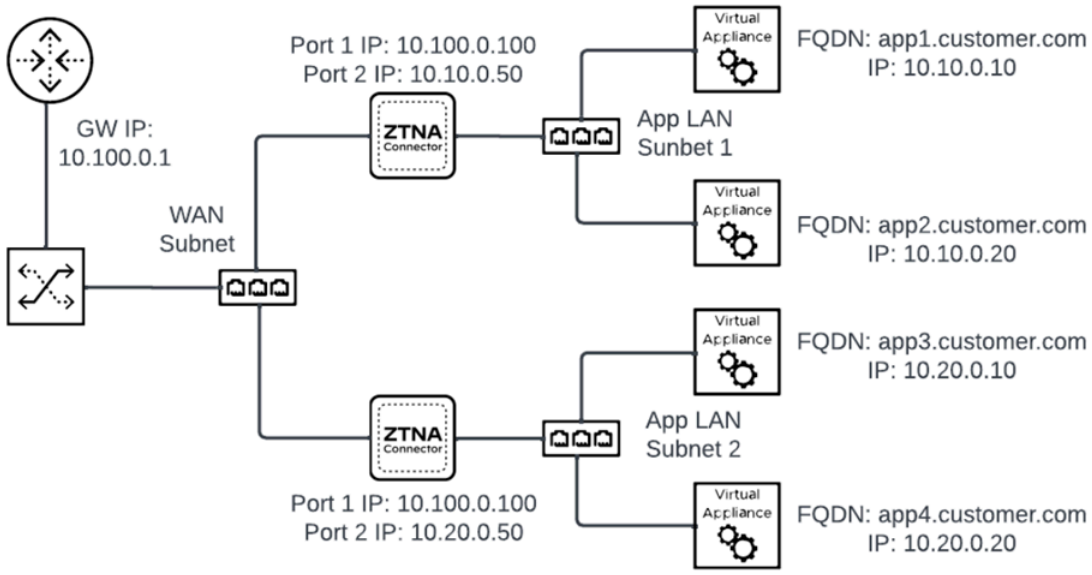
STEP 14 | Prisma SASE ポータルで、**[Workflows (ワークフロー)]** > **[ZTNA Connector (ZTNA コネクタ)]** > **[Connectors (コネクタ)]**に移動し、使用するコネクタを見つけて、 トンネルが稼働していることを確かめます。



Prisma Access ZTNAコネクタがサポートするKVMデプロイメント

2アームデプロイメントを使用してKernel-based Virtual Machine (カーネルベース仮想マシン - KVM)をデプロイします。次の図は、NATゲートウェイを備えた2アームモードでKVMを使用したZTNAコネクタ ネットワークデプロイメントの例を示しています。

©2025 Palo Alto Networks, Inc.



KVMを使用したZTNAコネクタのオンボード

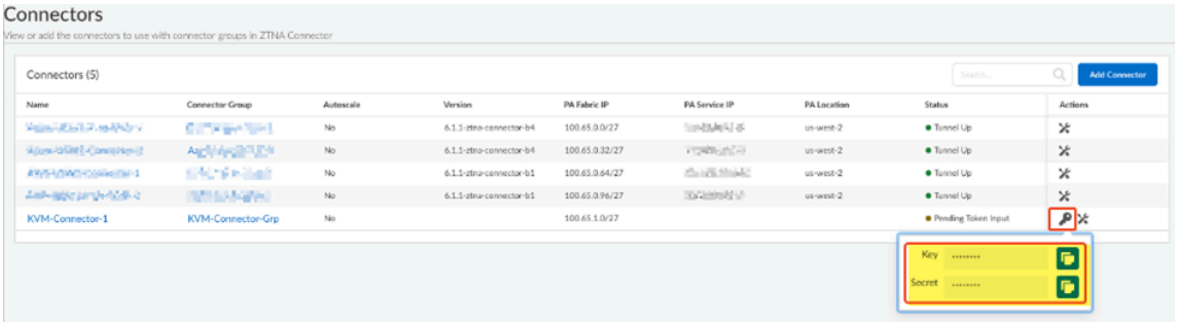
カーネルベースの仮想マシン(KVM)を使用してZTNAコネクタをオンボードするには、次の手順を実行します。

始める前に、次の前提条件を満たしていることを確認してください。

- **Updates (更新) > Software Updates (ソフトウェア更新) > Prisma Access ZTNA Connector for KVM**の下にあるCustomer Support Portal (CSP: カスタマー サポート ポータル)からZTNAコネクタHyper-Vイメージをダウンロードします。
- ZTNA Connectorの最小ホスティング環境を満たすKVMホストがあることを確認してください。

STEP 1 | KVM host用のコネクタ グループとコネクタを作成します 。

STEP 2 | [ワークフロー] > [**ZTNA** コネクタ] > [コネクタ]を選択し、KVM host用に作成したコネクタを見つけて、[ステータス]領域でトークンをコピー し 、 キー と シークレットの値をコピーします。



STEP 3 | CSPからダウンロードした**qcow**イメージをKVM hostにアップロードします。

©2025 Palo Alto Networks, Inc.

STEP 4 | まだ行っていない場合は、KVMホスト上で仮想ブリッジ インターフェイスを構築して関連付け、次のコマンドを入力してホストを準備します。

- `brctl addbr virbr0`
- `brctl addbr virbr0`
- `brctl addbr virbr1`
- `brctl addif virbr1 ens192`

STEP 5 | KVMホストにVMをデプロイするには、コマンドを実行します。 `virt-install` コマンドを次のオプションを設定して設定します。

- `-name` は、仮想マシンの名前です。
- `-vcpu` は**4**です。
- `-memory` は**16384** (16ギガバイト)です。
- `-disk`は、KVMホスト上の**qcow**イメージの場所と名前です。
- `-network`は、このVMに接続する仮想インターフェイスを参照します (ZTNAコネクタのインターフェイスをデプロイする必要があります)。

次に、KVM ホストのデプロイに使用するサンプル コマンドを示します。ここで、 `<kvm-file-name>` は、CSPからダウンロードしたqcowファイルの名前です。

```
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 | 次のコマンドを入力して、VMコンソールに接続します。

```
virsh console ztna-conn-1
```

対話式CLIインストール・プログラムが開始されます。

STEP 7 | IONモデル、キー、シークレットを設定します。

1. 表示される選択肢から **1(ion 200v**のION モデル) を選択します。

```
root@ubuntu-kvm-vm:/home/ubuntu-kvm/Desktop# virsh console
 ztna-conn-1 Connected to domain ztna-conn-1 Escape character
 is ^] イオンモードの選択:1) ion 200v 2) ion 3102v 3) ion 3104v
 4) ion 3108v 5) ion 7108v 6) ion 7116v 7) ion 7132v 8) ion
 9100v 番号または数量を選択してください:1CPU:合格（必要数4）メモリ：
合格（必要8.0G）ディスク：検証できませんでした (40.0G が必要) ネット
ワーク:合格 (必要 1) 変更する項目を選択するか、構成を送信します:1) モ
デル: ion 200v 2) ION キー:3) シークレットキー4) コントローラ1:コ
ントローラー - DHCP 5) ポート 1:無効/未使用 6) ポート2:無効/未使用
 7) ポート3:無効/未使用 8) ポート4:無効/未使用 9) ポート5:無効/未使用
 10) ポート6:無効/未使用 11) ポート7:無効/未使用 12) ポート8:無効/未使
用 13) ポート9:無効/未使用 14) 送信して再起動
```


©2025 Palo Alto Networks, Inc.

2. オプション**2**を選択し、ZTNAコネクタUI から保存したキーを入力して、コネクタからキーを入力します。

```
番号または数量を選択してください:2ION キー[なし]を入力: xxxxxxxxxx-
yyyyyyyy-zzz-1234-1234-abcdefghijkl 変更する項目を選択するか、設定
を送信します:1) モデル: ion 200v 2) IONキー: xxxxxxxxx-yyyyyyyy-
zzz-1234-1234-abcdefghijkl 3) シークレットキー:4) コントローラ1:コ
ントローラー - DHCP 5) ポート 1:無効/未使用 6) ポート2:無効/未使用
 7) ポート3:無効/未使用 8) ポート4:無効/未使用 9) ポート5:無効/未使用
 10) ポート6:無効/未使用 11) ポート7:無効/未使用 12) ポート8:無効/未使
用 13) ポート9:無効/未使用 14) 送信して再起動
```

3. オプション **3** を選択し、ZTNAコネクタUIから保存したシークレットを入力して、ZTNAコネクタ シークレットを入力します。

```
番号または数量を選択してください:3IONシークレット[なし]を入力:
 abcde12345 変更する項目を選択するか、設定を送信します:1) モデル: ion
 200v 2) IONキー: xxxxxxxxx-yyyyyyyy-zzz-1234-1234-abcdefghijkl
 3) シークレットキー: abcde12345 4) コントローラー1:コントローラー -
 DHCP 5) ポート 1:無効/未使用 6) ポート2:無効/未使用 7) ポート3:無
効/未使用 8) ポート4:無効/未使用 9) ポート5:無効/未使用 10) ポート6:無
効/未使用 11) ポート7:無効/未使用 12) ポート8:無効/未使用 13) ポー
ト9:無効/未使用 14) 送信して再起動
```

STEP 8 | WANポート オプションを構成します。

1. オプション **5**（ポート1）を選択します。

```
番号または数量を選択してください:5 ポート1:1) ロール:無効にする 2) ポート
変更をキャンセルする 3) 適用して戻る
```

2. オプション **1**(パブリック/WAN) を選択します。

```
番号または数量を選択してください:1 ポートのロールを選択:1) インターネット
接続ポート (PublicWAN) 2) プライベート WAN ポート (PrivateWAN) 3) バ
イパス ポート ペア 1 (WAN ポート) 4) バイパス ポート ペア 1 (LAN ポー
ト) 5) バイパス ポート ペア 2 (WAN ポート) 6) バイパス ポート ペア 2
 (LAN ポート) 7) バイパス ポート ペア 3 (WAN ポート) 8) バイパス ポー
ト ペア 3 (LAN ポート) 9) バイパス ポート ペア 4 (WAN ポート) 10) バ
イパス ポート ペア 4 (LAN ポート) 11) 無効/未使用
```

3. (任意) スタティックIPアドレスを設定する必要がある場合は、オプション **2** を選択し、IPアドレス、ゲートウェイ、およびDNSサーバー パラメータを設定します。それ以外の場合は、オプション **1** を選択します。

```
番号または数量を選択してください:1 ポート1:1) ロール:PublicWAN 2) 設定
方法:DHCP 3) ポート変更をキャンセル 4) 適用して戻る
```

 ©2025 Palo Alto Networks, Inc.

4. メイン メニューに戻るにはオプション**4**を 選択します。

```
番号または数量を選択してください:4 変更する項目を選択するか、設定を送
信します。1) モデル: ion 200v 2) IONキー: xxxxxxxxx-yyyyyyyy-
zzz-1234-1234-abcdefghijkl 3) シークレットキー: abcde12345 4) コ
ントローラー1:コントローラー - DHCP 5) ポート 1:パブリックWAN - DHCP
 6) ポート2:無効/未使用 7) ポート3:無効/未使用 8) ポート4:無効/未使用
 9) ポート5:無効/未使用 10) ポート6:無効/未使用 11) ポート7:無効/未
使用 12) ポート8:無効/未使用 13) ポート9:無効/未使用 14) 送信して再
起動 変更する項目を選択するか、設定を送信します。1) モデル: ion 200v
 2) IONキー: xxxxxxxxx-yyyyyyyy-zzz-1234-1234-abcdefghijkl
 3) シークレットキー: abcde12345 4) コントローラー1:コントローラー
 - DHCP 5) ポート 1:パブリックWAN - DHCP 6) ポート2:無効/未使用
 7) ポート3:無効/未使用 8) ポート4:無効/未使用 9) ポート5:無効/未使用
 10) ポート6:無効/未使用 11) ポート7:無効/未使用 12) ポート8:無効/未使
用 13) ポート9:無効/未使用 14) 送信して再起動
```

STEP 9 | LAN ポート オプションを構成します。

1. オプション **6**（ポート2）を選択します。

```
番号または数量を選択してください:6 ポート2:1) ロール:無効にする 2) ポート
変更をキャンセルする 3) 適用して戻る
```

2. オプション**2**（PrivateWAN）を選択します。

```
番号または数量を選択してください:2 ポートのロールを選択:1) インターネット
接続ポート (PublicWAN) 2) プライベート WAN ポート (PrivateWAN) 3) バ
イパス ポート ペア 1 (WAN ポート) 4) バイパス ポート ペア 1 (LAN ポー
ト) 5) バイパス ポート ペア 2 (WAN ポート) 6) バイパス ポート ペア 2
 (LAN ポート) 7) バイパス ポート ペア 3 (WAN ポート) 8) バイパス ポー
ト ペア 3 (LAN ポート) 9) バイパス ポート ペア 4 (WAN ポート) 10) バ
イパス ポート ペア 4 (LAN ポート) 11) 無効/未使用
```

3. (任意) スタティックIPアドレスを設定する必要がある場合は、オプション **2** を選択し、IPアドレス、ゲートウェイ、およびDNSサーバー パラメータを設定します。それ以外の場合は、オプション **1** を選択します。

```
番号または数量を選択してください:2 ポート2:1) ロール:PrivateWAN 2) 設定
方法:DHCP 3) ポート変更をキャンセル 4) 適用して戻る
```

4. メイン メニューに戻るにはオプション**4**を 選択します。

```
番号または数量を選択してください:4 変更する項目を選択するか、設定を送
信します。1) モデル: ion 200v 2) IONキー: xxxxxxxxx-yyyyyyyy-
zzz-1234-1234-abcdefghijkl 3) シークレットキー: abcde12345 4) コ
ントローラー1:コントローラー - DHCP 5) ポート 1:パブリックWAN - DHCP
 6) ポート2:プライベートWAN - DHCP 7) ポート3:無効/未使用 8) ポー
ト4:無効/未使用 9) ポート5:無効/未使用 10) ポート6:無効/未使用 11) ポー
```

 ©2025 Palo Alto Networks, Inc.

```
ト7:無効/未使用 12) ポート8:無効/未使用 13) ポート9:無効/未使用 14) 送信して再起動
```

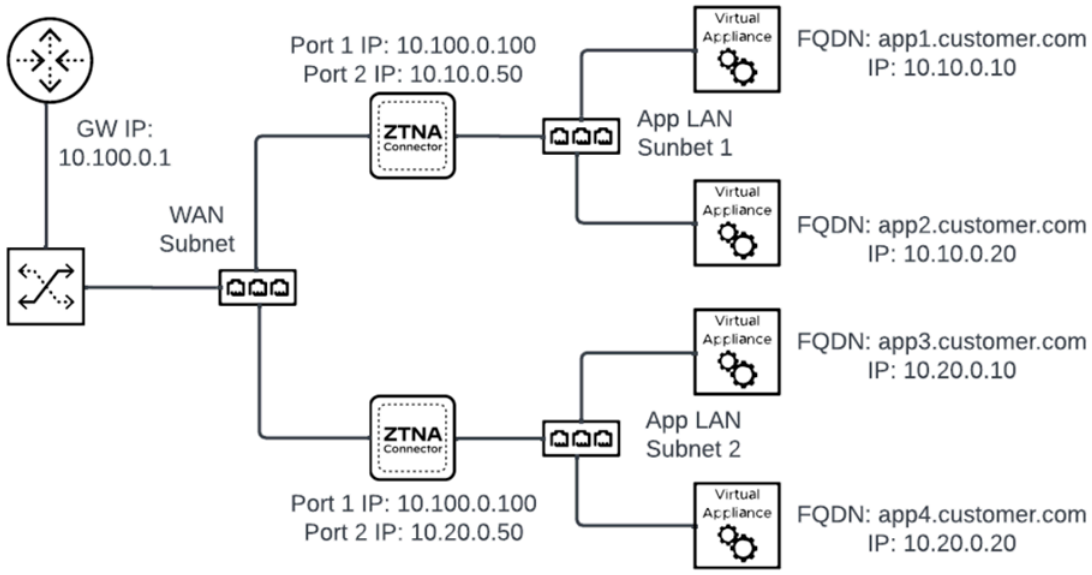
STEP 10 | コネクタを保存して再起動します。

```
番号または数量を選択してください:14 警告!この構成が送信されると、すべてのハードウェアが署名され、ログに記録され、Prisma SDWAN クラウド コントローラーの ION キー/シークレット キーに永続的に関連付けられます。つまり、この「SUBMIT (送信)」機能の後は、ハードウェア（ディスク、ネットワーク カード）を追加/削除することはできません。この「SUBMIT (送信)」以降にハードウェアの変更が必要な場合は、新しいIONキーとシークレット キーを使用してIONを再デプロイする必要があります。ハードウェアを追加または削除する必要がある場合は、以下の「N」と回答し、IONをシャットダウンして、今すぐ変更を行ってください。これらの変更を今すぐ送信しますか?[N]: y 構成を構築しています... [VFF:CFG] ZeroTouch Config を開始しています - 構成ファイル パーサー [VFF:CFG] Config/INI ファイルとしてロード/解析しようとしています。 [VFF:CFG] 構成スタイル ファイルが正常にロードされました。 [VFF:CFG] コントローラ1が CONTROLLER/DHCP に正常に設定されました。 [VFF:CFG] ポート1が PUBLICWAN/DHCP に正常に設定されました。 [VFF:CFG] ポート2が PRIVATEWAN/DHCP に正常に設定されました。 [VFF:CFG] 警告:ポート 3 には構成セクションがありませんでした。デフォルトでは無効になっています。[VFF:CFG] 警告:ポート 4 には構成セクションがありませんでした。デフォルトでは無効になっています。[VFF:CFG] 警告:ポート 5 には config セクションがありませんでした。デフォルトでは無効になっています。[VFF:CFG] 警告:ポート 6 には構成セクションがありませんでした。デフォルトでは無効になっています。[VFF:CFG] 警告:ポート 7 には構成セクションがありませんでした。デフォルトでは無効になっています。[VFF:CFG] 警告:ポート 8 には構成セクションがありませんでした。デフォルトでは無効になっています。[VFF:CFG] 警告:ポート 9 には構成セクションがありませんでした。デフォルトで無効になっています。[VFF:CFG] Config/INI ファイル パーサーが成功しました。[VFF:KVM] メニュー構成が終了し、通常の起動を続行します...再起動理由: 製造
```

Prisma AccessZTNAコネクタがサポートするHyper-Vのデプロイメント

2アームデプロイメントを使用してMicrosoft Hyper-Vハイパーバイザーをデプロイします。次の図は、NATゲートウェイを備えた2アームモードでHyper-Vを使用したZTNAコネクタ ネットワークデプロイメントの例を示しています。

©2025 Palo Alto Networks, Inc.



Hyper-Vを使用してZTNAコネクタをオンボードする

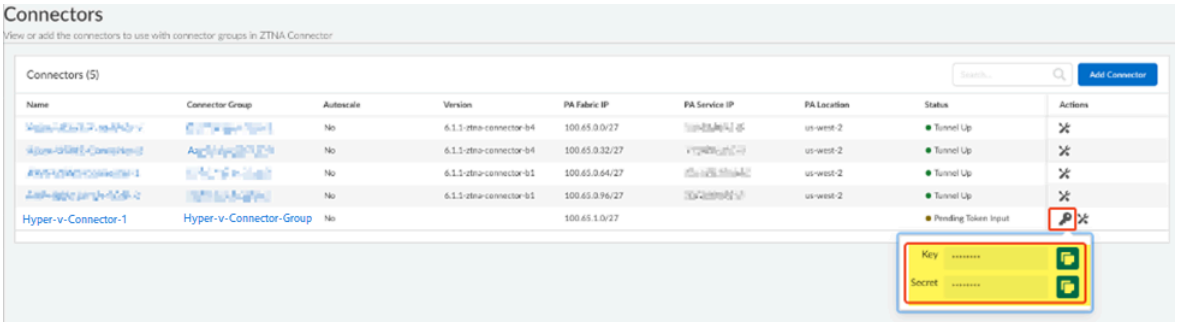
Microsoft Hyper-V 仮想マシン(VM)を使用してZTNAコネクタをオンボードするには、次の手順を実行します。

始める前に、次の前提条件を満たしていることを確認してください。

- カスタマーサポートポータル（CSP） の [アップデート] > [ソフトウェアアップデート] > **Prisma Access ZTNA Connector for Hyper-V (Hyper-V用のZTNAコネクタ)**からZTNAコネクタHyper-Vイメージをダウンロードします。
- ZTNA コネクタの最小 ホスティング環境を 満たすHyper-V VMがあることを確認します。

STEP 1 | Hyper-V VM 用のコネクタ グループとコネクタを作成します 。

STEP 2 | [ワークフロー] > **[ZTNA** コネクタ] > [コネクタ]を選択し、Hyper-V VM用に作成したコネクタを見つけて、[ステータス]領域でトークンをコピー し 、 キー と シークレットの値をコピーします。



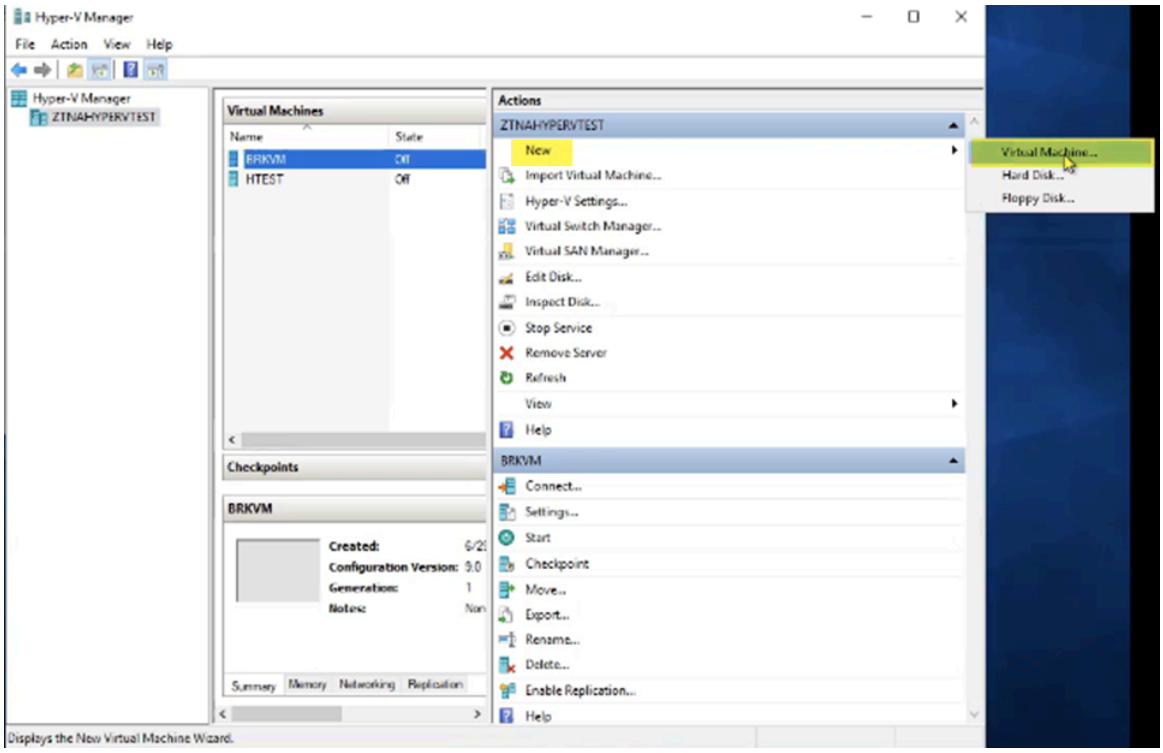
STEP 3 | CSPからダウンロードした**vhd**イメージをHyper-V VMにアップロードします。
選択した場所がHyper-V VMからアクセスできることを確認してください。

各Hyper-V VMには1つの (vhd) ファイルが必要です。

©2025 Palo Alto Networks, Inc.

STEP 4 | Hyper-V マネージャーに移動し、[アクション] > [新規] > [仮想マシン]を選択して新しい仮想マシンを作成します。

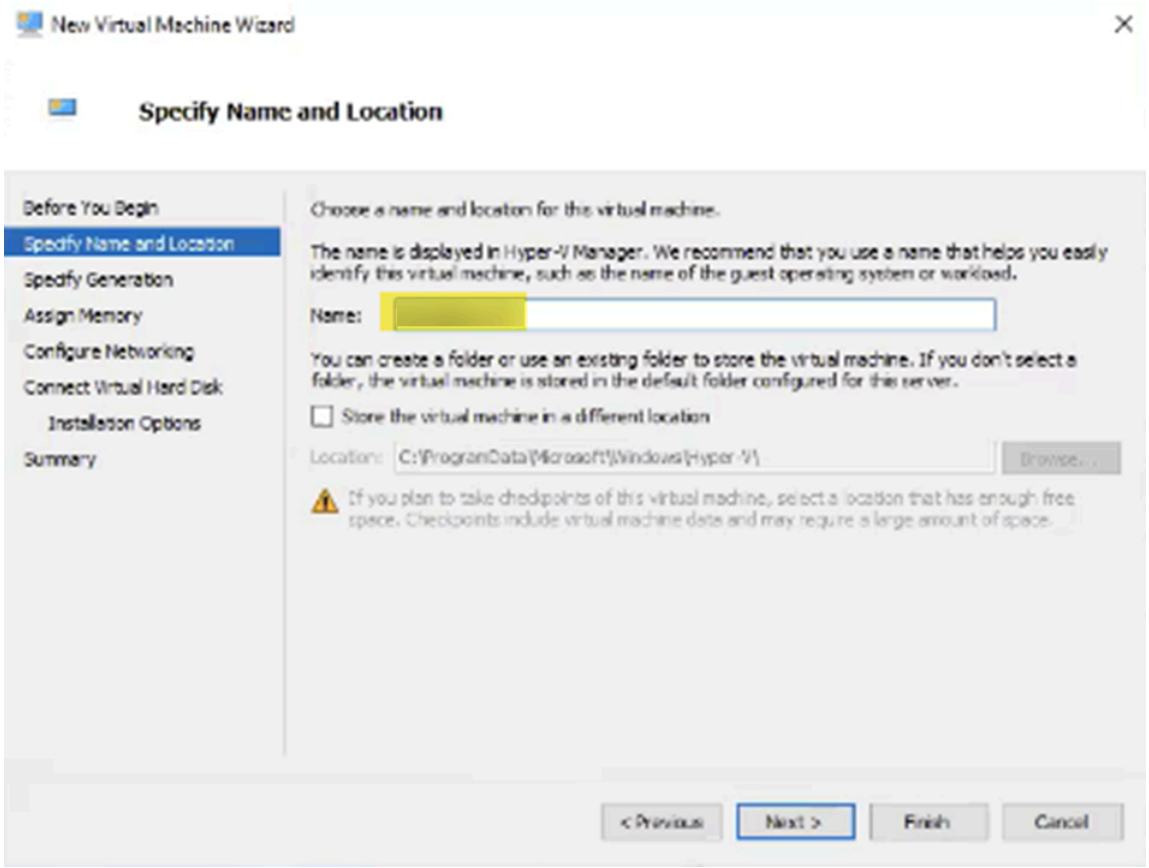
このワークフローは、MicrosoftサーバーにHyper-V VMをデプロイするために実行する手順を示しています。Hyper-V UIは環境によって異なる場合があります。



STEP 5 | 次の 画面に進み、VMの一意の名前を入力して、 次の ページに進みます。

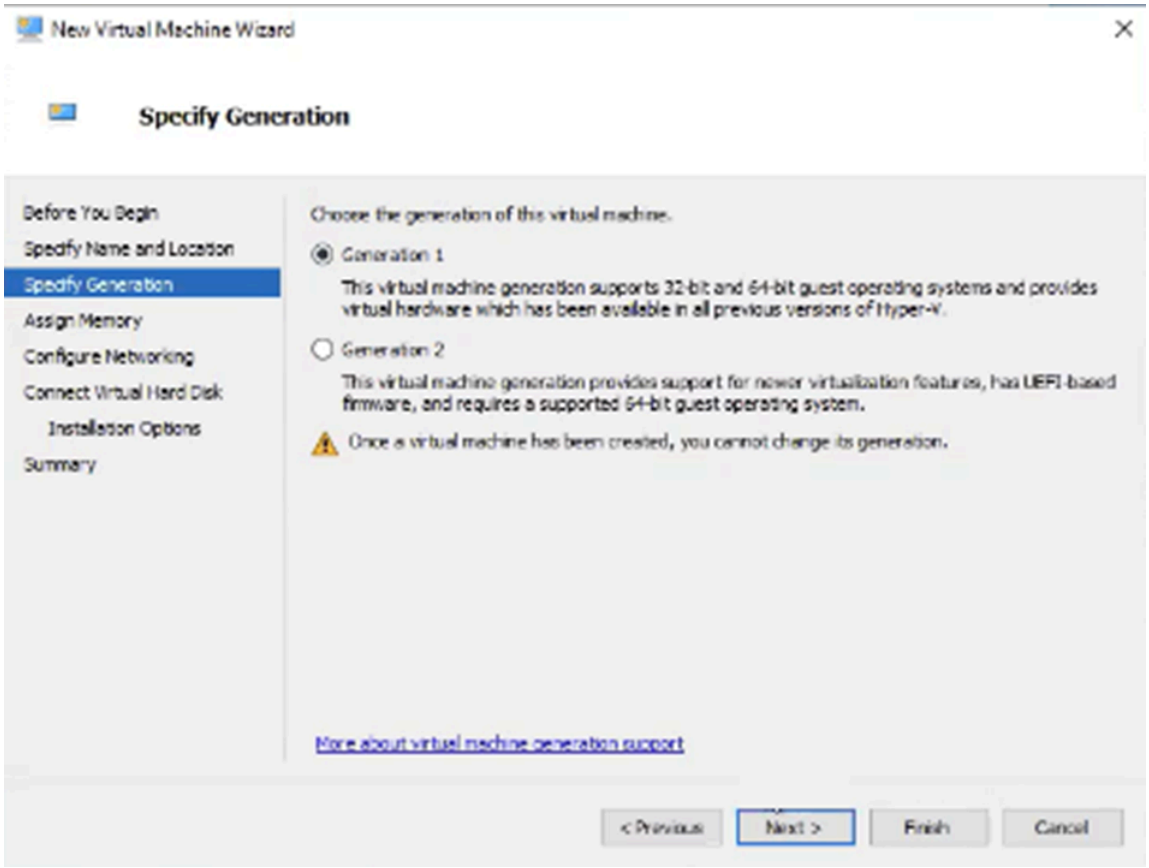
©2025 Palo Alto Networks, Inc.

STEP 6 | (任意) VMの場所を変更するには、[仮想マシンを別の場所に保存する]を選択し、場所を選択します。



©2025 Palo Alto Networks, Inc.

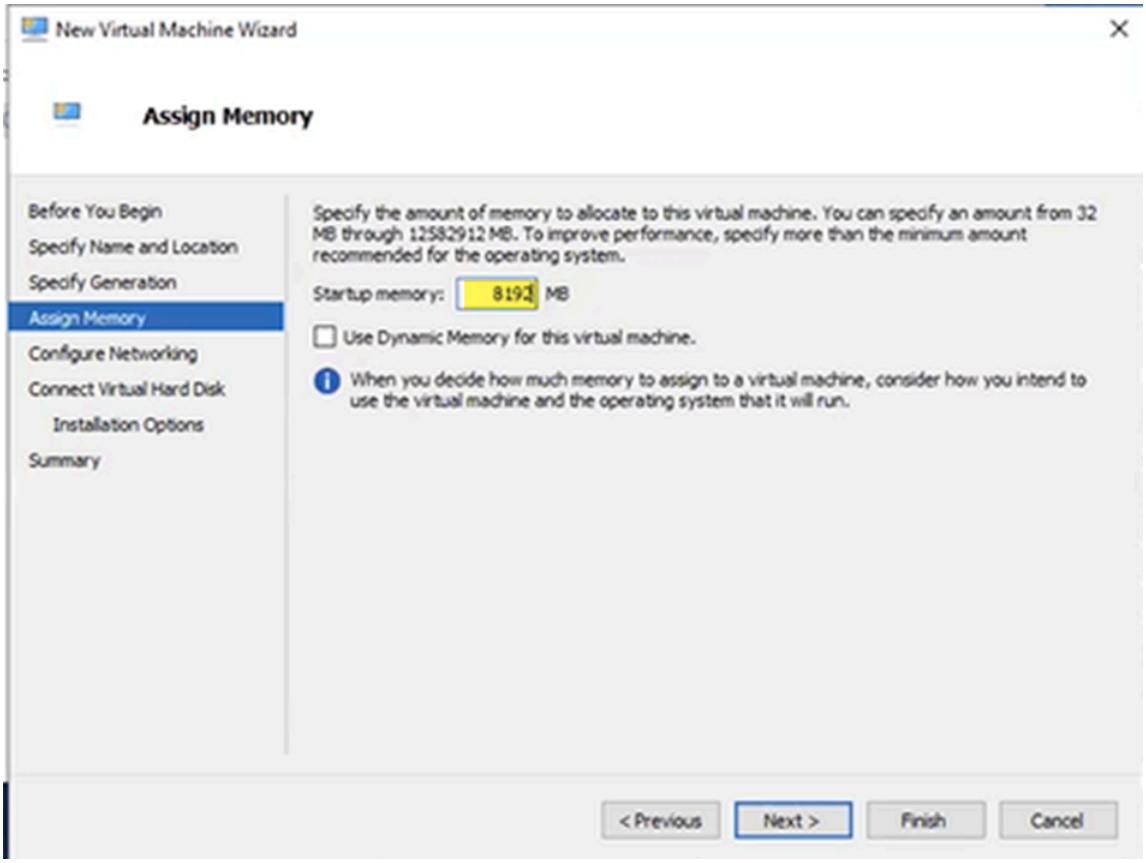
STEP 7 | VM 世代として第**1**世代 を選択し、[次へ] ページに進みます。
これは、ZTNAコネクタvhdファイルがサポートする世代です。



 ©2025 Palo Alto Networks, Inc.

STEP 8 | VMにメモリを割り当てます。

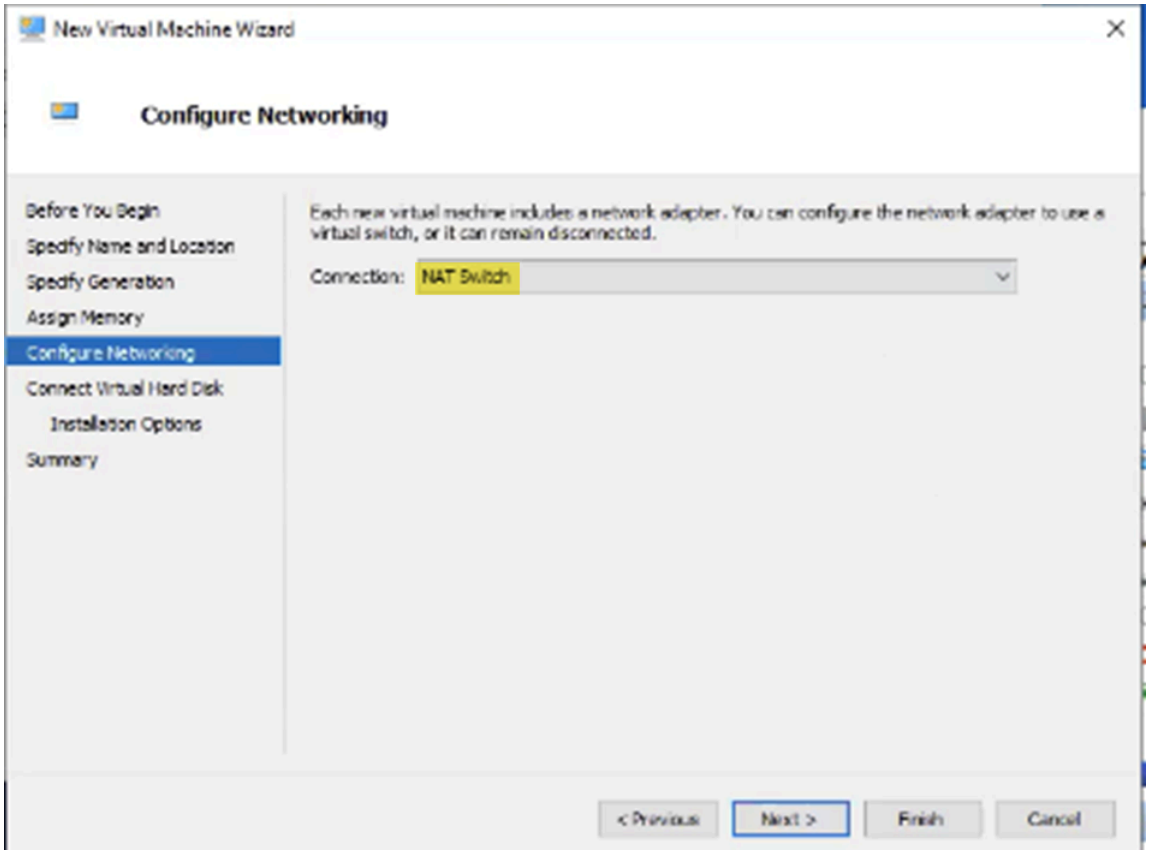
Hyper-V VM の 最小要件 を満たす **8192**MB (8 GB) の最小メモリを割り当てて、 次の ページに進みます。



©2025 Palo Alto Networks, Inc.

STEP 9 | VM のネットワークを構成してから、 次の ページに進みます。

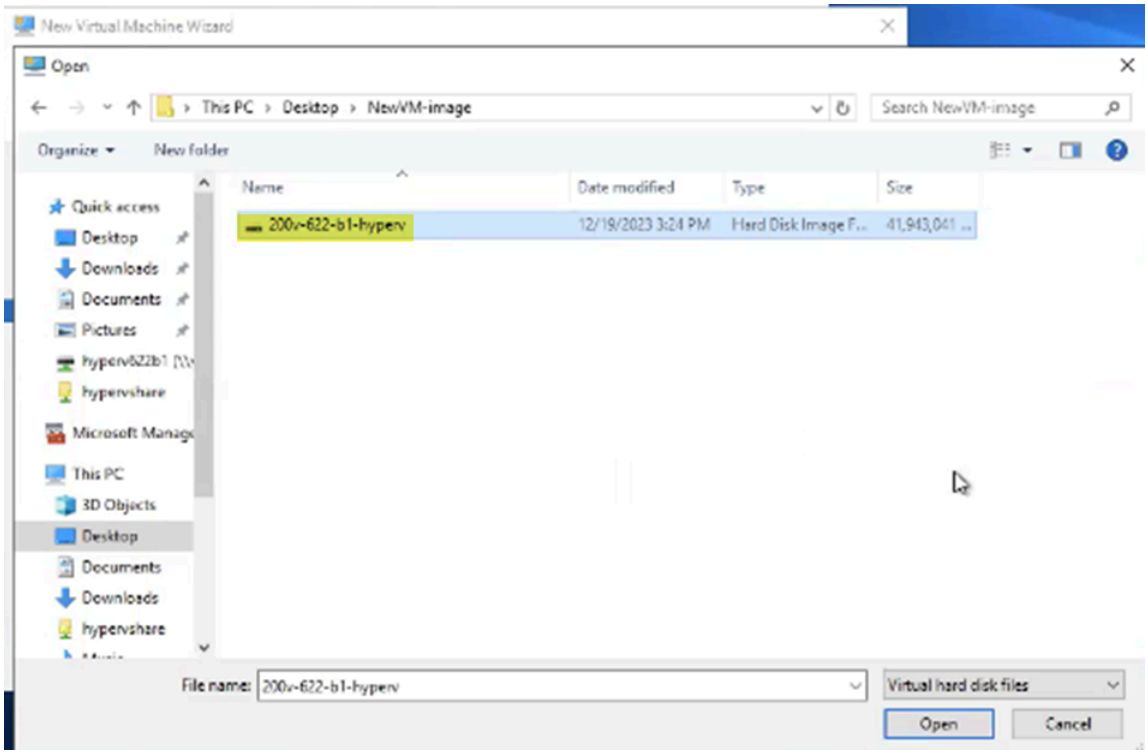
使用するネットワークは構成によって異なります。この例では、ネットワークに **NAT**スイッチ を使用します。



©2025 Palo Alto Networks, Inc.

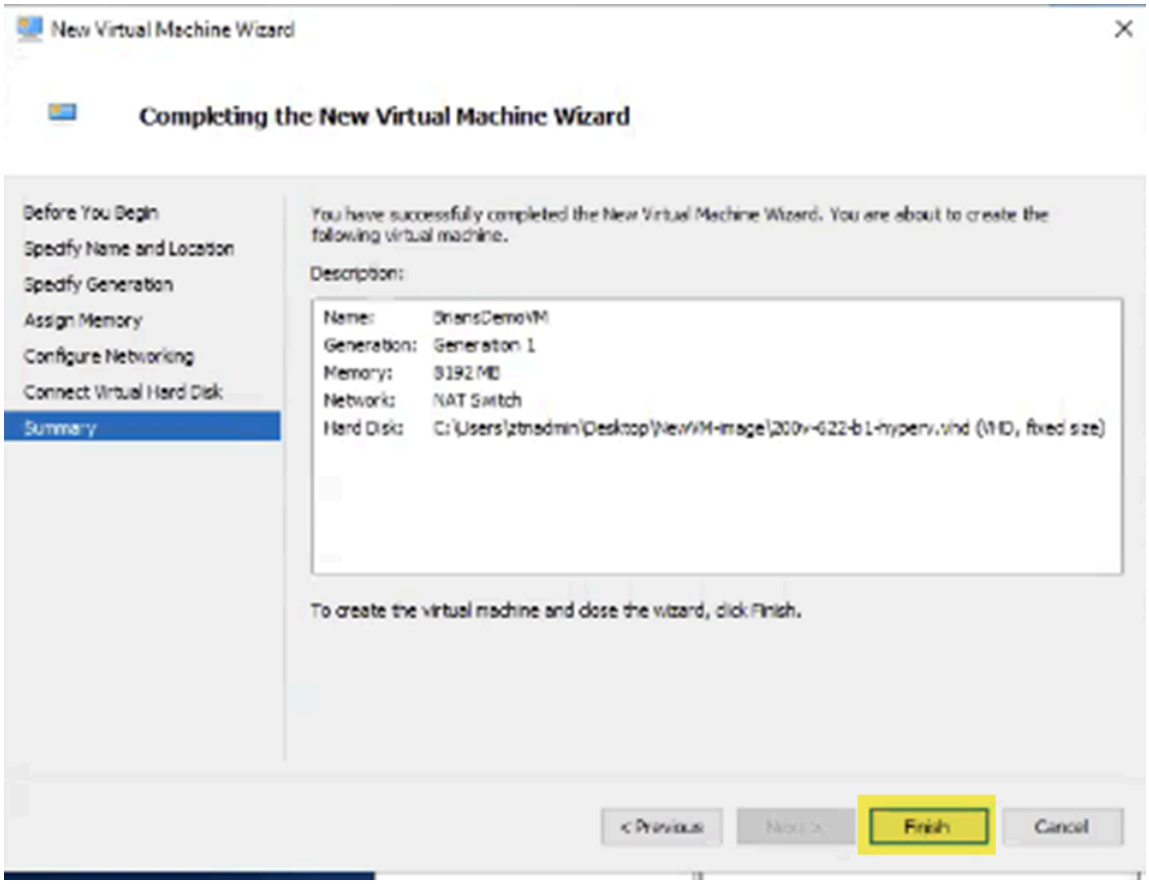
STEP 10 | 仮想ハードディスクを接続します。

1. [既存の仮想ハードディスクを使用する]を選択し、ダウンロードしたvhdファイルを参照します 。
2. ダウンロードした vhd ファイルを選択して 開き 、 次の ページに進みます。



©2025 Palo Alto Networks, Inc.

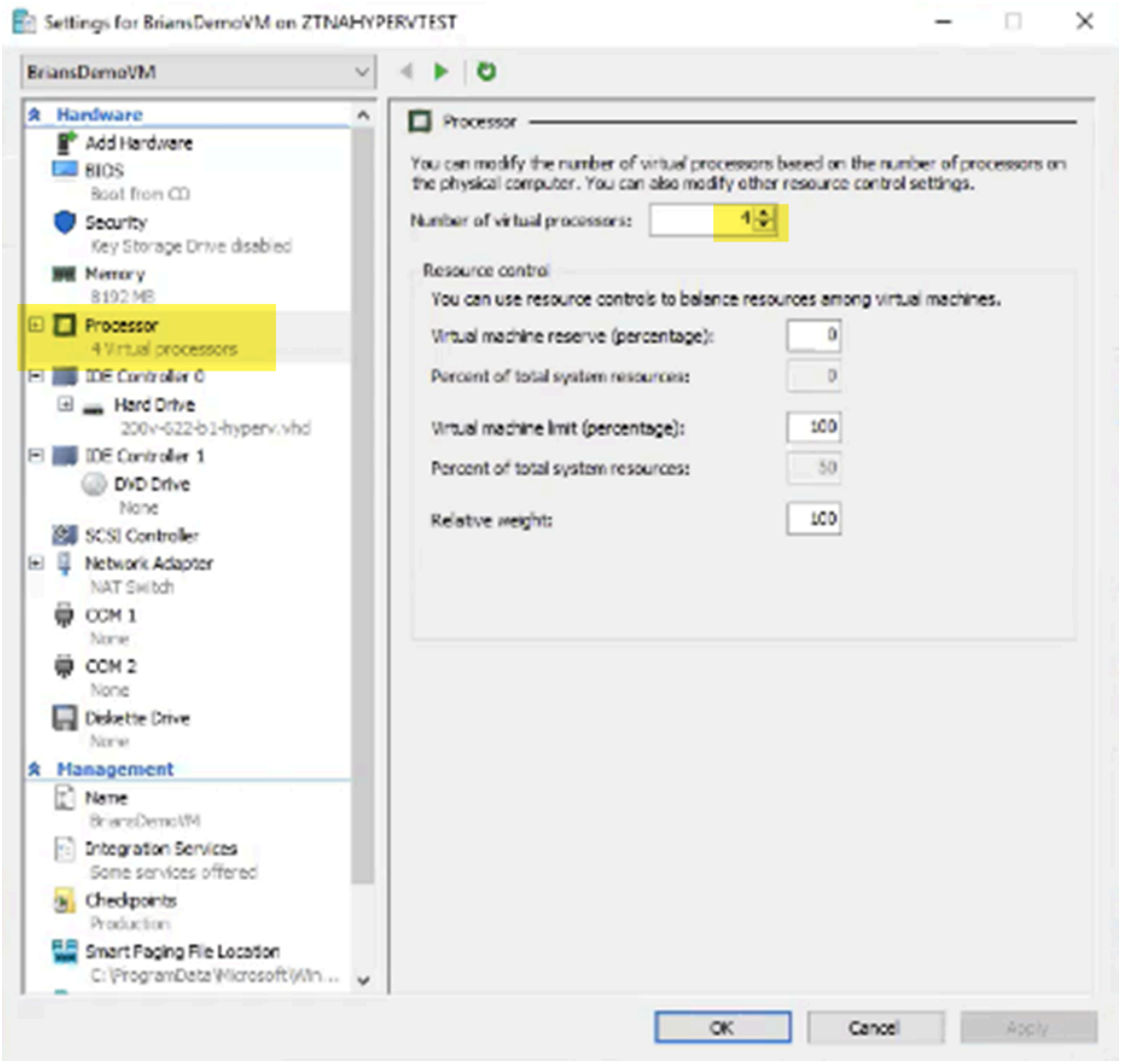
STEP 11 | 新しい VM ウィザードを終了します 。



Hyper-VがVMを作成します。

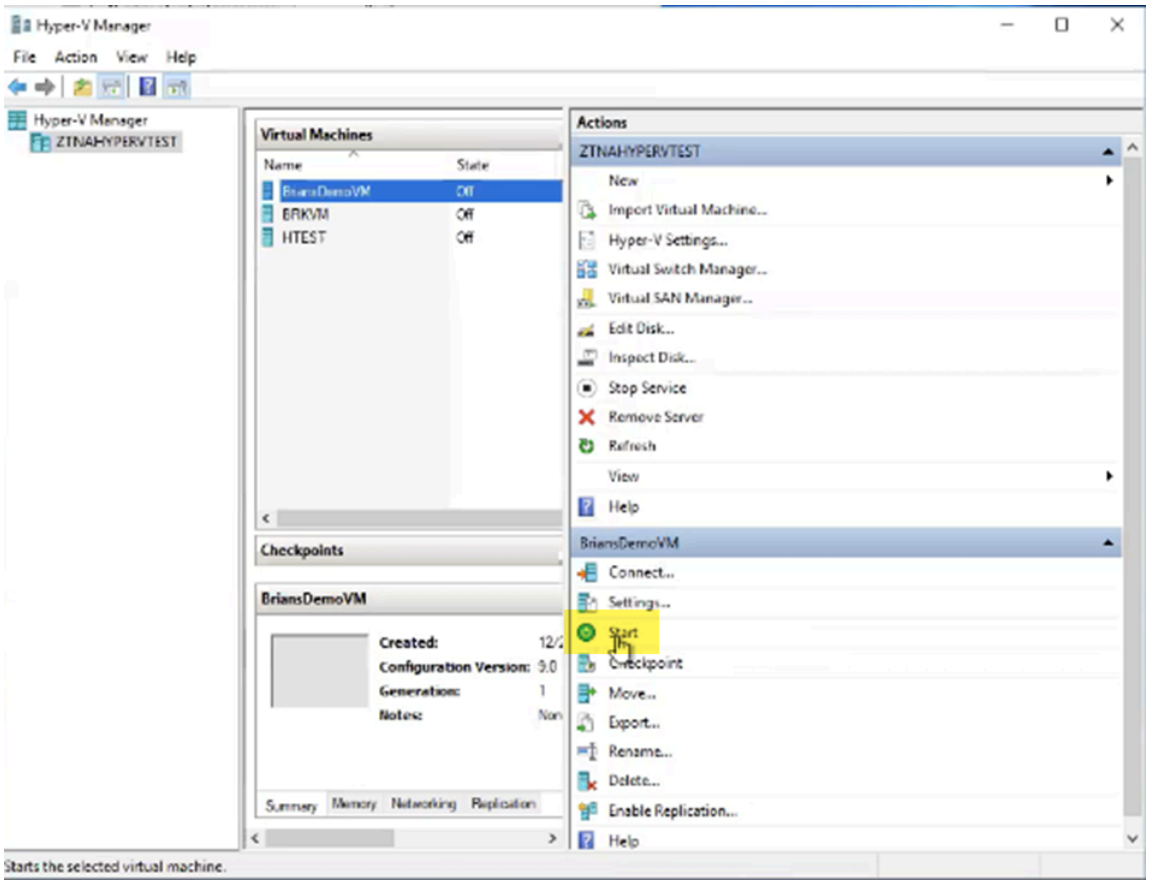
©2025 Palo Alto Networks, Inc.

STEP 12 | **[プロセッサ]** 領域に移動して少なくとも**4**つの仮想プロセッサを選択し、VMに少なくとも4つのプロセッサがあることを確認します。

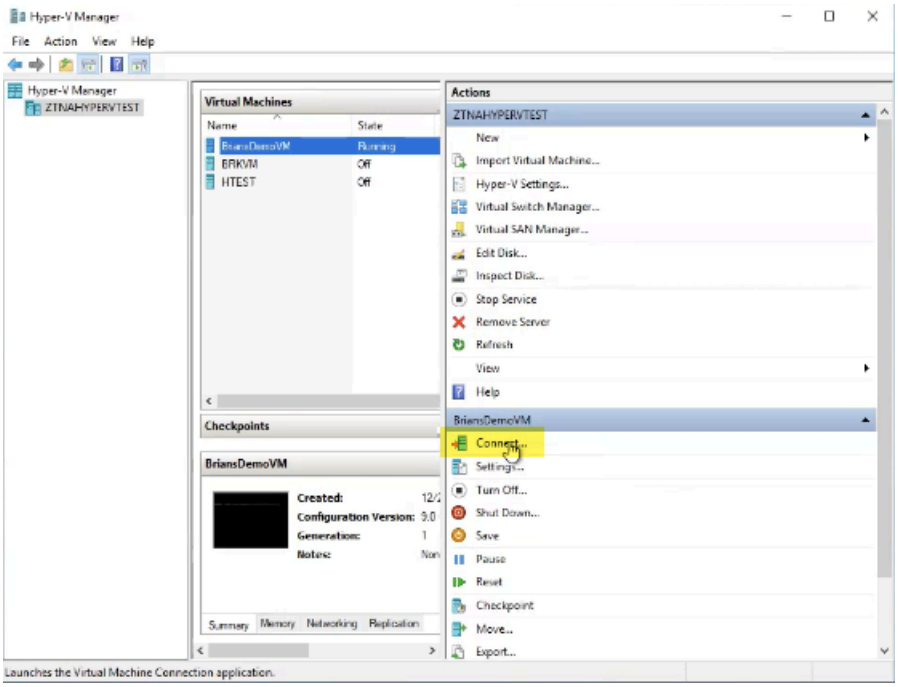


 ©2025 Palo Alto Networks, Inc.

STEP 13 | VMを起動します 。



STEP 14 | シリアルコンソールに接続します 。



 ©2025 Palo Alto Networks, Inc.

STEP 15 | 対話型CLIインストール プログラムが初期化されるのを待ってから、IONモデル、キー、およびシークレットを構成します。

1. 表示される選択肢から **1(ion 200v**のION モデル) を選択します。

```
IONモデルを選択してください:1) ion 200v 2) ion 3102v 3) ion 3104v
 4) ion 3108v 5) ion 7108v 6) ion 7116v 7) ion 7132v 8) ion
 9100v 番号または数量を選択してください:1CPU:合格（必要数4）メモリ：合
格（必要8.0G）ディスク：検証できませんでした (40.0G が必要) ネットワー
ク:合格 (必要 1) 変更する項目を選択するか、構成を送信します:1) モデル:
 ion 200v 2) ION キー:シークレットキー4) コントローラ1:コントローラー
 - DHCP 5) ポート 1:無効/未使用 6) ポート2:無効/未使用 7) ポート3:無
効/未使用 8) ポート4:無効/未使用 9) ポート5:無効/未使用 10) ポート6:無
効/未使用 11) ポート7:無効/未使用 12) ポート8:無効/未使用 13) ポー
ト9:無効/未使用 14) 送信して再起動
```

2. オプション**2**を選択し、ZTNAコネクタUI から保存したキーを入力して、コネクタからキーを入力します。

```
番号または数量を選択してください:2ION キー[なし]を入力: xxxxxxxxxx-
yyyyyyyy-zzz-1234-1234-abcdefghijkl 変更する項目を選択するか、設定
を送信します:1) モデル: ion 200v 2) IONキー: xxxxxxxxx-yyyyyyyy-
zzz-1234-1234-abcdefghijkl 3) シークレットキー:4) コントローラ1:コ
ントローラー - DHCP 5) ポート 1:無効/未使用 6) ポート2:無効/未使用
 7) ポート3:無効/未使用 8) ポート4:無効/未使用 9) ポート5:無効/未使用
 10) ポート6:無効/未使用 11) ポート7:無効/未使用 12) ポート8:無効/未使
用 13) ポート9:無効/未使用 14) 送信して再起動
```

3. オプション **3** を選択し、ZTNAコネクタUIから保存したシークレットを入力して、ZTNAコネクタ シークレットを入力します。

```
番号または数量を選択してください:3IONシークレット[なし]を入力:
 abcde12345 変更する項目を選択するか、設定を送信します:1) モデル: ion
 200v 2) IONキー: xxxxxxxxx-yyyyyyyy-zzz-1234-1234-abcdefghijkl
 3) シークレットキー: abcde12345 4) コントローラー1:コントローラー -
 DHCP 5) ポート 1:無効/未使用 6) ポート2:無効/未使用 7) ポート3:無
効/未使用 8) ポート4:無効/未使用 9) ポート5:無効/未使用 10) ポート6:無
効/未使用 11) ポート7:無効/未使用 12) ポート8:無効/未使用 13) ポー
ト9:無効/未使用 14) 送信して再起動
```

STEP 16 | WANポート オプションを構成します。

1. オプション **5**（ポート1）を選択します。

```
番号または数量を選択してください:5 ポート1:1) ロール:無効にする 2) ポート
変更をキャンセルする 3) 適用して戻る
```

2. オプション **1**(パブリック/WAN) を選択します。

```
番号または数量を選択してください:1 ポートのロールを選択:1) インターネット
接続ポート (PublicWAN) 2) プライベート WAN ポート (PrivateWAN) 3) バ
イパス ポート ペア 1 (WAN ポート) 4) バイパス ポート ペア 1 (LAN ポー
```


©2025 Palo Alto Networks, Inc.

```
ト) 5) バイパス ポート ペア 2 (WAN ポート) 6) バイパス ポート ペア 2
 (LAN ポート) 7) バイパス ポート ペア 3 (WAN ポート) 8) バイパス ポー
ト ペア 3 (LAN ポート) 9) バイパス ポート ペア 4 (WAN ポート) 10) バ
イパス ポート ペア 4 (LAN ポート) 11) 無効/未使用
```

3. (任意) スタティックIPアドレスを設定する必要がある場合は、オプション **2** を選択し、IPアドレス、ゲートウェイ、およびDNSサーバー パラメータを設定します。それ以外の場合は、オプション **1** を選択します。

```
番号または数量を選択してください:1 ポート1:1) ロール:PublicWAN 2) 設定
方法:DHCP 3) ポート変更をキャンセル 4) 適用して戻る
```

4. メイン メニューに戻るにはオプション**4**を 選択します。

```
番号または数量を選択してください:4 変更する項目を選択するか、設定を送
信します。1) モデル: ion 200v 2) IONキー: xxxxxxxxx-yyyyyyyy-
zzz-1234-1234-abcdefghijkl 3) シークレットキー: abcde12345 4) コ
ントローラー1:コントローラー - DHCP 5) ポート 1:パブリックWAN - DHCP
 6) ポート2:無効/未使用 7) ポート3:無効/未使用 8) ポート4:無効/未使用
 9) ポート5:無効/未使用 10) ポート6:無効/未使用 11) ポート7:無効/未
使用 12) ポート8:無効/未使用 13) ポート9:無効/未使用 14) 送信して再
起動 変更する項目を選択するか、設定を送信します。1) モデル: ion 200v
 2) IONキー: xxxxxxxxx-yyyyyyyy-zzz-1234-1234-abcdefghijkl
 3) シークレットキー: abcde12345 4) コントローラー1:コントローラー
 - DHCP 5) ポート 1:パブリックWAN - DHCP 6) ポート2:無効/未使用
 7) ポート3:無効/未使用 8) ポート4:無効/未使用 9) ポート5:無効/未使用
 10) ポート6:無効/未使用 11) ポート7:無効/未使用 12) ポート8:無効/未使
用 13) ポート9:無効/未使用 14) 送信して再起動
```

STEP 17 | LAN ポート オプションを構成します。

1. オプション **6**（ポート2）を選択します。

```
番号または数量を選択してください:6 ポート2:1) ロール:無効にする 2) ポート
変更をキャンセルする 3) 適用して戻る
```

2. オプション**2**（PrivateWAN）を選択します。

```
番号または数量を選択してください:2 ポートのロールを選択:1) インターネット
接続ポート (PublicWAN) 2) プライベート WAN ポート (PrivateWAN) 3) バ
イパス ポート ペア 1 (WAN ポート) 4) バイパス ポート ペア 1 (LAN ポー
ト) 5) バイパス ポート ペア 2 (WAN ポート) 6) バイパス ポート ペア 2
 (LAN ポート) 7) バイパス ポート ペア 3 (WAN ポート) 8) バイパス ポー
ト ペア 3 (LAN ポート) 9) バイパス ポート ペア 4 (WAN ポート) 10) バ
イパス ポート ペア 4 (LAN ポート) 11) 無効/未使用
```


©2025 Palo Alto Networks, Inc.

3. (任意) スタティックIPアドレスを設定する必要がある場合は、オプション **2** を選択し、IPアドレス、ゲートウェイ、およびDNSサーバー パラメータを設定します。それ以外の場合は、オプション **1** を選択します。

```
番号または数量を選択してください:2 ポート2:1) ロール:PrivateWAN 2) 設定方法:DHCP 3) ポート変更をキャンセル 4) 適用して戻る
```

4. メイン メニューに戻るにはオプション**4**を 選択します。

```
番号または数量を選択してください:4 変更する項目を選択するか、設定を送信します。1) モデル: ion 200v 2) IONキー: xxxxxxxxx-yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) シークレットキー: abcde12345 4) コントローラー1:コントローラー - DHCP 5) ポート 1:パブリックWAN - DHCP 6) ポート2:プライベートWAN - DHCP 7) ポート3:無効/未使用 8) ポート4:無効/未使用 9) ポート5:無効/未使用 10) ポート6:無効/未使用 11) ポート7:無効/未使用 12) ポート8:無効/未使用 13) ポート9:無効/未使用 14) 送信して再起動
```

STEP 18 | コネクタを保存して再起動します。

```
番号または数量を選択してください:14 警告!この構成が送信されると、すべてのハードウェアが署名され、ログに記録され、Prisma SDWAN クラウド コントローラーの ION キー/シークレット キーに永続的に関連付けられます。つまり、この「SUBMIT (送信)」機能の後は、ハードウェア（ディスク、ネットワーク カード）を追加/削除することはできません。この「SUBMIT (送信)」以降にハードウェアの変更が必要な場合は、新しいIONキーとシークレット キーを使用してIONを再デプロイする必要があります。ハードウェアを追加または削除する必要がある場合は、以下の「N」と回答し、IONをシャットダウンして、今すぐ変更を行ってください。これらの変更を今すぐ送信しますか?[N]: y 構成を構築しています... [VFF:CFG] ZeroTouch Config を開始しています - 構成ファイル パーサー [VFF:CFG] Config/INI ファイルとしてロード/解析しようとしています。 [VFF:CFG] 構成スタイル ファイルが正常にロードされました。 [VFF:CFG] コントローラ1が CONTROLLER/DHCP に正常に設定されました。 [VFF:CFG] ポート1が PUBLICWAN/DHCP に正常に設定されました。 [VFF:CFG] ポート2が PRIVATEWAN/DHCP に正常に設定されました。 [VFF:CFG] 警告:ポート 3 には構成セクションがありませんでした。デフォルトでは無効になっています。[VFF:CFG] 警告:ポート 4 には構成セクションがありませんでした。デフォルトでは無効になっています。[VFF:CFG] 警告:ポート 5 には構成セクションがありませんでした。デフォルトでは無効になっています。[VFF:CFG] 警告:ポート 6 には構成セクションがありませんでした。デフォルトでは無効になっています。[VFF:CFG] 警告:ポート 7 には構成セクションがありませんでした。デフォルトでは無効になっています。[VFF:CFG] 警告:ポート 8 には構成セクションがありませんでした。デフォルトでは無効になっています。[VFF:CFG] 警告:ポート 9 には構成セクションがありませんでした。デフォルトで無効になっています。[VFF:CFG] Config/INI ファイル パーサーが成功しました。[VFF:KVM] メニュー構成が終了し、通常の起動を続行します...再起動理由: 製造
```

 ©2025 Palo Alto Networks, Inc.

ZTNAコネクタを監視する

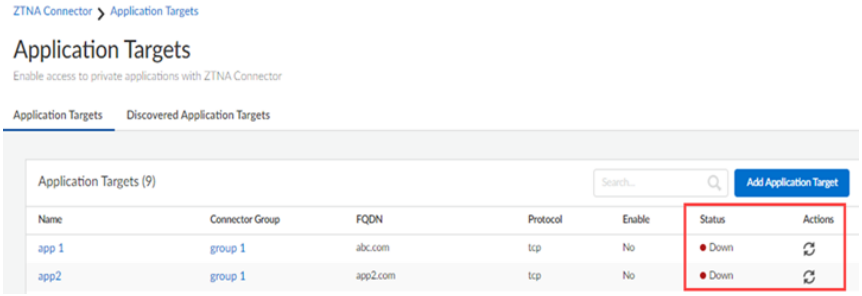
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ ZTNA コネクタ アドオン ライセンス アドオン ライセンスを含む Essential ライセンスには、8つのZTNAコネクタ、100個のFQDN、および4つのIPサブネット機能が含まれます。 アドオン ライセンスを含む Advanced ライセンスには、40個の ZTNA コネクタ、300個のFQDN、および 1024 個のIPサブネット機能が含まれます。 アドオン ライセンスを含むプレミアム ライセンスには、200個のZTNAコネクタ、4000個のFQDN、および1024個のIPサブネット機能が含まれます。 ❑ ZTNAコネクタアドオンライセンスを購入しない場合は、 Prisma Accessライセンスには、4 つのコネクタ、40 個の FQDN、および 4 つの IP サブネットが含まれます。この機能は、ご使用の環境で ZTNA コネクタを試す目的で提供されています。

すべてのZTNAコネクタ コンポーネントは、発生した問題のトラブルシューティングに役立つ明確なステータス情報、ログ、診断ツールを提供します。ZTNAコネクタのデプロイメントを監視するには、次のツールを使用します。

©2025 Palo Alto Networks, Inc.

Prisma SASE プラットフォーム内からアプリケーションとコネクタのステータスを表示します。

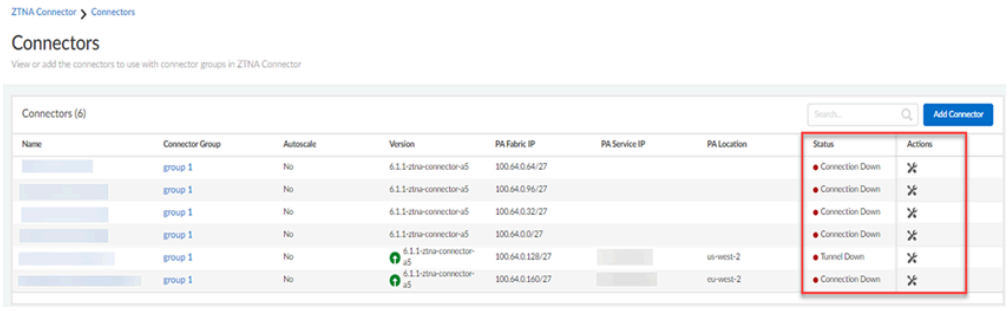
- **[Workflows (ワークフロー)] > [ZTNA Connector (ZTNA コネクタ)] > [Application Targets (アプリケーション ターゲット)]** を選択し、すべてのアプリケーション ターゲットの ステータス が **Up (稼働中)**であることを確認します。



ステータスが **[Down (ダウン)]**と表示されている場合、コネクタはアプリケーションに到達できません。アプリケーションの問題を修正したら、**[Action (アクション)]**列のステータスの更新ボタンをクリックし、 ステータスが**[Up (稼働中)]** に変わることを確認します (ステータスは1分ごとに自動的に更新されます)。

アプリケーションがZTNAコネクタから到達可能である (最後に成功したDNS解決結果を使用) が、ZTNAコネクタからのアプリケーションFQDN のDNS 解決が失敗した場合も、ステータスはUpになります。

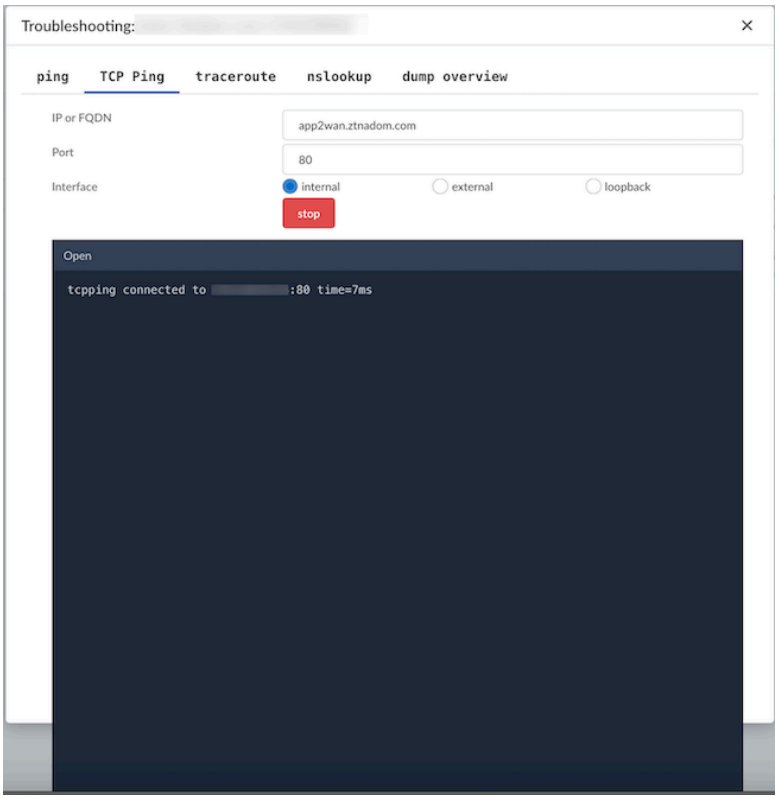
- **Workflows (ワークフロー) > ZTNA Connector (ZTNA コネクタ) > Connectors (コネクタ)** を選択し、すべてのコネクタの ステータス が**Up** であることを確認します。



ステータスに**Tunnel Down (トンネルダウン)**と表示されている場合、コネクタVMとPrisma Accessがダウンしています。ステータスに**[Connection Down (接続ダウン)]** と表示されている場合、コネクタ VM がダウンしていることを示します。診断アイコン をクリックして、コネクタへのリモートシェル接続を起動し、問題

 ©2025 Palo Alto Networks, Inc.

のトラブルシューティングを行います。接続の問題を診断するために、**ping**、**TCP Ping**、**traceroute**、**nslookup**、または **dump summary** を実行できます。



©2025 Palo Alto Networks, Inc.

ZTNAコネクタのログの表示

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ ZTNA コネクタ アドオン ライセンス アドオン ライセンスを含む Essential ライセンスには、8つのZTNAコネクタ、100個のFQDN、および4つのIPサブネット機能が含まれます。 アドオン ライセンスを含む Advanced ライセンスには、40個の ZTNA コネクタ、300個のFQDN、および 1024 個のIPサブネット機能が含まれます。 アドオン ライセンスを含むプレミアム ライセンスには、200個のZTNAコネクタ、4000個のFQDN、および1024個のIPサブネット機能が含まれます。 ❑ ZTNAコネクタアドオンライセンスを購入しない場合は、 Prisma Accessライセンスには、4 つのコネクタ、40 個の FQDN、および 4 つの IP サブネットが含まれます。この機能は、ご使用の環境で ZTNA コネクタを試す目的で提供されています。

すべてのZTNAコネクタ トラフィックはStrata Logging Serviceに記録されます。Prisma Accessログをを保存するには、Strata Logging Serviceに適切な量のログストレージを見積もり、購入する必要があります。ZTNA Connectorログを保存するために、Strata Logging Service容量ストレージの合計の割合を10%増やすことをお勧めします。

必要なログタイプをStrata Logging Serviceに転送するログ転送プロファイルが設定されていることを確認してください。 ログ・ストレージのクォータが90%に達すると、Strata Logging Serviceがさらにストレージを購入するよう電子メール通知を送信します。追加のストレージを購入しない場合、古いログはパージされます。

Prisma Accessに使用している管理インターフェイス（Panorama またはクラウド管理）に関係なく、Prisma Access (Managed by Strata Cloud Manager) の**[Incidents & Alerts (**インシデントとアラート**)]** > **[Log Viewer (**ログビューア**)]**でログを表示できます。

ZTNA Connector は、次のネットワークログを提供します。

©2025 Palo Alto Networks, Inc.

- 監査ログ - Prisma SASE Platformを通じて利用でき、ZTNA Connectorでの管理者の設定変更の記録を提供します。これらのログは、コンプライアンスとトラブルシューティングの目的で使用できます。

  監査ログは、時間範囲、サイト、デバイス、およびタイプでフィルタリングできます。監査ログには、次の詳細が表示されます。

  - 特定のユーザーが特定の IP アドレスからエンタープライズ ポータルに試行したログインの数。
  - アプリケーションまたはアプリケーション コネクタがオンボードされているか、削除されているか。
  - コネクタのアップグレードがスケジュールされている場合。
  - すべてのシステム変更と試行されたアクセスの表示。

  ZTNA Connector 監査ログは、 Prisma Access Webインターフェイスでは利用できません。監査ログを表示するには、 サポートケース パロアルトネットワークスのテクニカルサポートにご相談ください。
- トラフィックログは、各セッションの開始と終了のエントリを表示します。各エントリには、日時、送信元ゾーン、宛先ゾーン、アドレスおよびポート、アプリケーション名、フローに適用されるセキュリティ ルール名、ルール アクション（allow、deny、または drop）、入力/出力インターフェイス、バイト数、およびセッション終了理由などが記載されます。
  - Type[タイプ] 列は、そのエントリがセッションの開始または終了のどちらのエントリなのかを示します。
  - Action[アクション]列はファイアウォールが、そのセッションを許可、拒否またはドロップしたことを示します。
  - 「ドロップ」は、トラフィックをブロックしたセキュリティ ルールが適用されていずれかのアプリケーションが指定されたことを示し、「拒否」はルールが適用されてある特定のアプリケーションが識別されたことを示します。
  - アプリケーションが識別される前にトラフィックが廃棄された場合 (あるルールにより特定のサービスのトラフィックがすべて廃棄された場合など)、そのアプリケーション列 は「該当なし」と表示します。
  - ZTNA コネクタの App-ID は、カスタム App-ID です。
  - トラフィックがモバイルユーザーゲートウェイにヒットした場合、 宛先アドレス 列には、RFC 6598 IP アドレスが表示されます。
- 設定ログ - ZTNA コネクタ設定の変更に関するエントリを表示します。各エントリには、日付と時刻、管理者のユーザー名、管理者が変更を行った IP アドレス、クライアントのタイプ、実行されたコマンドのタイプ、コマンドのステータス (成功または失敗)、設定パス、および変更前と変更後の値が含まれます。
- Strata Cloud Manager
- Panorama

 ©2025 Palo Alto Networks, Inc.

ZTNAコネクタのログの表示 (Panorama)

Prisma Access (Managed by Panorama) Access で ZTNA コネクタのログを表示するには、以下のワークフローを使用します。

STEP 1 | Prisma Accessにログインします。

STEP 2 | **[Monitor (監視)]** > **[Logs (ログ)]**を選択します。

STEP 3 | リストからログタイプを選択します。監査、 トラフィック、および 設定 ログ。

STEP 4 | 列ヘッダーの右側にある矢印をクリックし、 **Columns**[Columns]を選択します。

STEP 5 | リストから表示する列を選択します。ログは自動的に更新されて選択に一致するようになります。

STEP 6 | 特定のログ エントリの スパイグラス アイコンをクリックします。**Detailed Log View** [詳細ログ ビュー]はセッションの送信元と送信先ならびにログエントリに関連するセッションリストの詳細情報を持っています。

ZTNAコネクタのログの表示 (Strata Cloud Manager)

Cloud Managed Prisma AccessでZTNA Connectorのログを表示するには、次のワークフローを使用します。

STEP 1 | Prisma Access (Managed by Strata Cloud Manager)にログインします。

STEP 2 | **[Incidents & Alerts (インシデントとアラート)]** > **[Log Viewer (ログ ビューアー)]**を選択します。

STEP 3 | 表示するログのタイプを選択します。監査、ファイアウォール/トラフィックおよび、設定ログ。

STEP 4 | ログを表示する時間範囲を選択します。

STEP 5 | 次のクエリ文字列を指定して、ZTNA コネクタログのリストを絞り込みます。**Subtype = 'netflow' AND Device Name = 'PA_CONN'** .

ログには、次の詳細が含まれます。

- タイムスタンプ
- コネクタ名
- クライアントの元の送信元IPアドレス
- クライアントの元の送信元ポート
- コネクタの変換されたIPアドレス
- コネクタの変換されたポート
- 変換された宛先IPアドレス
- 変換された宛先ポート

©2025 Palo Alto Networks, Inc.

送信元NATを使用した ZTNA コネクタ接続のユーザー ID マッピングを保持する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 5.1.1

Prisma Access の ZTNA コネクタを使用して、プライベート アプリケーションを保護できます。ユーザー ID に基づいてアプリケーションへのアクセスを制限するには、プライベート アプリケーションが配置されているデータ センターまたは本社に次世代ファイアウォール (NGFW) を導入し、ユーザー ID マッピングに基づいて NGFW でポリシー ルールを設定します。

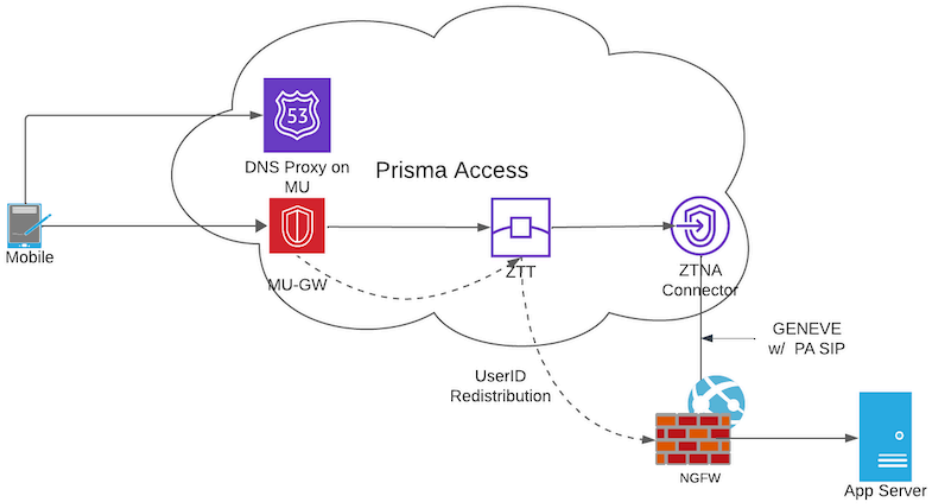
デプロイメントで、プライベート アプリケーションが配置されているデータ センターまたは本社の場所で次世代ファイアウォール (NGFW) を使用し、ZTNA コネクタが送信元NAT を実行する場合、NGFW はユーザー ID マッピングを取得できません。ZTNA コネクタ上の送信元NAT により、マッピングに不可欠なクライアント IP アドレスを NGFW が取得できなくなります。NGFW がこのクライアント IP アドレスを取得できない場合、ユーザー ID マッピングに基づいて作成したゾーンベースのセキュリティ ポリシー ルールを適用できません。

ZTNA コネクタには、NGFW で保護されたデータセンター内でユーザー ID を有効にするために次の役割があります。

1. NGFW がユーザー ID 再配信エージェントに接続できるように、NGFW から地域の ZTNA コネクタ トンネル ターミネータ (ZTT) への安全な接続を提供します。
2. FQDN アプリケーションの場合、ヘルス プローブが tcpping に設定され、アプリケーションはデータ センター アプリケーションをプローブして、アプリケーションが稼働していて、この個々のコネクタから到達可能かどうかを判断します。
3. オプションとして元の送信元 IP アドレスを含む Geneve パケット内に、ユーザーからアプリへの NAT 後のデータセンター空間 IP パケットをカプセル化します。

次の図は、NGFW に送信元 IP アドレスとユーザー ID のマッピングを提供し、元の Prisma Access 送信元IPアドレス オプションを含む Generic Network Virtualization Encapsulation (Geneve) でカプセル化されたデータ パケットを NGFW に配信するネットワーク要素を示しています。これらの要素により、NGFW はユーザー ID に基づいてセキュリティ ポリシー ルールを効果的に適用できるようになります。

©2025 Palo Alto Networks, Inc.



制限事項:

- ZTNA コネクタによるユーザー ID サポートは、次のバージョン以降でのみ利用可能です:
  - Prisma Access データプレーン:10.2.4 バージョン以降
  - Saas_エージェント:5.1.0 バージョン以降
  - NGFW バージョン:11.2.0 バージョン以降
  - コネクタバージョン:6.2.4-ztna-connector-b3 バージョン以降
- ICMP プローブは、ユーザー ID ベースのコネクタ グループに接続されている FQDN ターゲットではサポートされません。
- UID エージェントの NGFW サービス ルート構成では、静的 IP アドレスを持つインターフェースのみがサポートされます。NGFW インターフェースが動的モード (DHCP による IP アドレスの割り当て) に設定されている場合、NGFW から ZTT へのユーザー ID チャネルは ZTNA コネクタ ユーザー ID のサポートを確立できません。この問題を解決するには、静的 IP アドレスを使用して NGFW 上の UID エージェントに使用するインターフェースを設定する必要があります。
- ping や traceroute などの診断ツールは、ユーザー ID ベースのコネクタではサポートされていません。

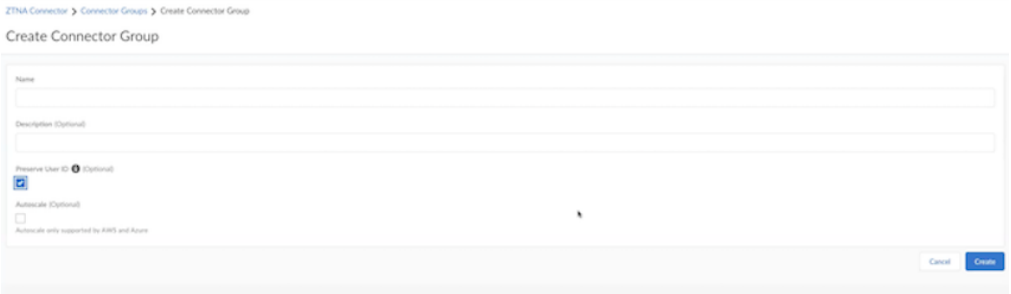
この手順では、次のネットワーク構成が確立されていることを前提としています。

- プライベート アプリが配置されている本社またはデータ センターに NGFW を導入しました。
- NGFW で作成したゾーン (アントラスト ゾーンとトラスト ゾーン) に基づいて、NGFW にセキュリティ ポリシー ルールを適用しました。これらのセキュリティ ポリシー ルールには、ユーザー ID の適用が含まれます。

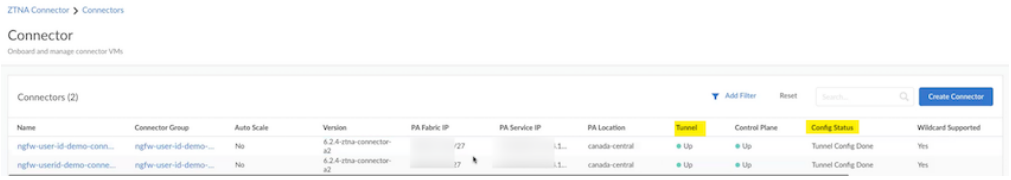
ネットワークがユーザー ID マッピングを本社またはデータ センターに配信していることを確認するには、以下の手順を実行します。これにより、NGFW は GlobalProtect から学習したユーザー ID マッピングに基づいてセキュリティ ポリシー ルールを適用できるようになります。

©2025 Palo Alto Networks, Inc.

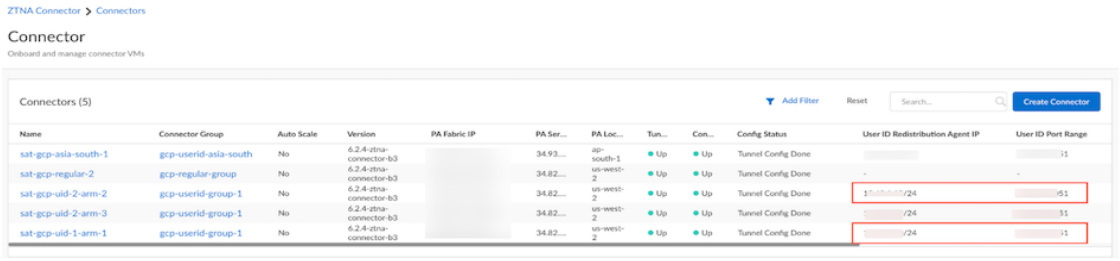
STEP 1 | コネクタ グループを作成し、 ユーザー **ID** の保持を有効にして、 コネクタを追加します。



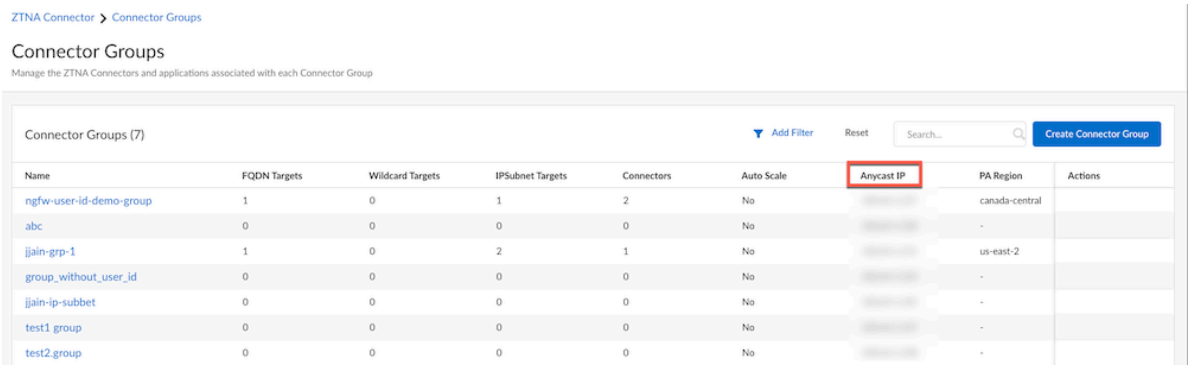
STEP 2 | データ センターにコネクタをデプロイしてオンボードし 、 トンネルが稼働して機能している かどうかを確認します。



STEP 3 | コネクタ に移動し、コネクタの ユーザー **ID** 再配信エージェント **IP** と ユーザー **ID** ポート範囲をメモします。NGFW でユーザー ID 再配信エージェントを構成するには、これらの IP アドレスとポート範囲が必要です。



また、 コネクタ グループ に移動して、**Anycast IP**をメモします。この IP アドレスは、この送信元 IP アドレスからの TCP アプリケーション プローブを許可するように NGFW セキュリティ ポリシー ルールを構成するために必要です。



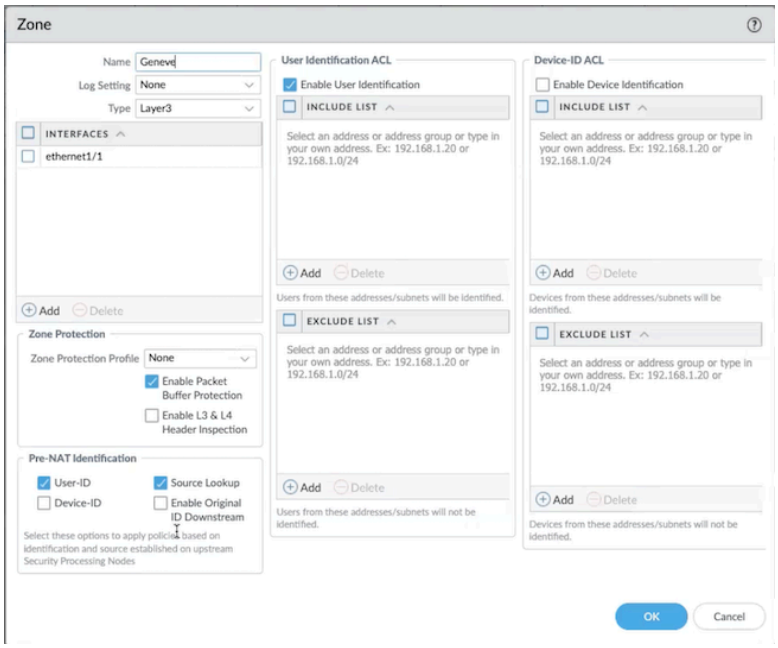
 ©2025 Palo Alto Networks, Inc.

STEP 4 | NGFW で Pre-NAT 識別パラメータを入力します。

1. NGFW UI にログインし、[ネットワーク > ゾーン] に移動して 2 つのゾーン (ZTNA コネクタを接続するインターフェースのゾーンとアプリケーション サーバーを接続するインターフェースのゾーン) を追加する か、既存のゾーンを選択します。

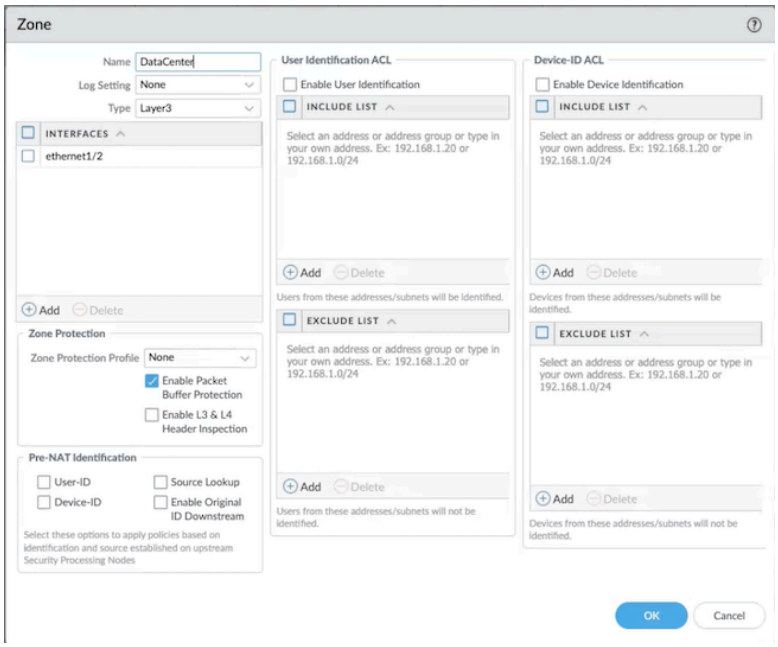
   1. ZTNA コネクタに接続するインターフェースを持つゾーンに対して、次の **NAT**事前識別 パラメータを選択します。

      - **User-ID**- IP アドレスが NAT される前に使用されたモバイル ユーザーの User-ID マッピングを保持します。セキュリティ ポリシー ルールで User-ID を使用している場合は、これを有効にします。
      - ソース検索-GlobalProtectから受信した元の送信元IPアドレスを照合できます。



   2. アプリケーション サーバー ゾーンに接続するインターフェースの場合、**NAT**事前識別 パラメータを選択する必要はありません。

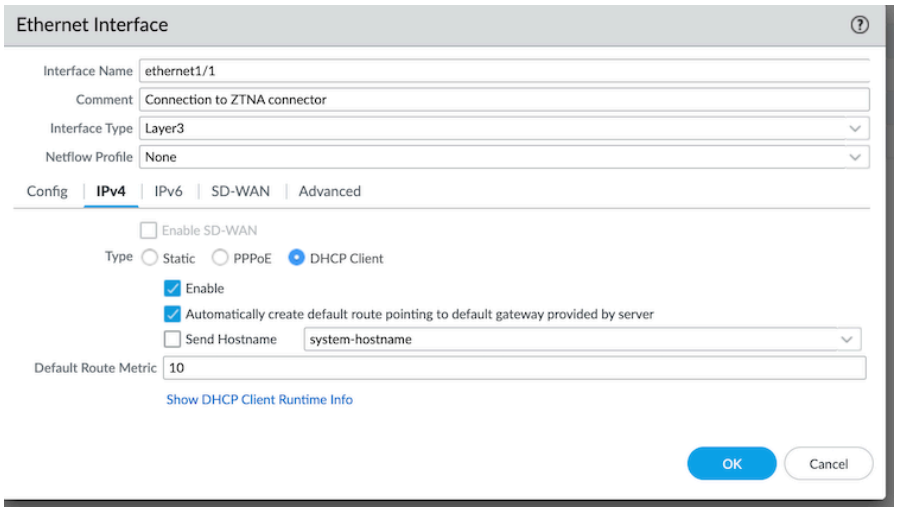
©2025 Palo Alto Networks, Inc.



3. **OK** をクリックし、変更を **Commit (**コミット**)** します。

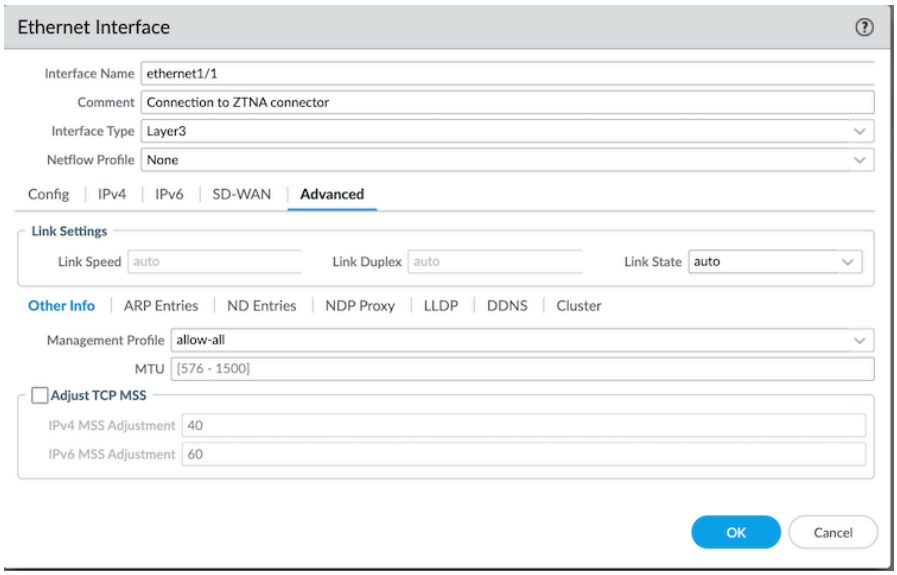
2. インターフェースに IP アドレスを追加します。

   1. **[**ネットワーク**] > [**インターフェース**] > [**イーサネット**]**に移動します。
   2. ZTNA コネクタとアプリケーション サーバーに接続するインターフェースを選択し、構成します。インターフェース名と インターフェース タイプをレイヤー **3**に追加します。



   3. アプリケーション サーバーに接続されているイーサネット インターフェースの場合は、**[**サーバーが提供するデフォルト ゲートウェイを指すデフォルト ルートを自動的に作成する**]** チェック ボックスをオフにします。

 ©2025 Palo Alto Networks, Inc.



3. 「インターフェース」 に移動し、インターフェースに静的 IP アドレスを追加します。ZTNA コネクタ ゾーン (Geneve) に ZTNA コネクタ接続インターフェースを追加し、アプリケーション サーバー ゾーン (データ センター) にアプリケーション サーバー接続インターフェースを追加します。

STEP 5 | NGFWとのコマンドライン インターフェース(CLI)セッションを作成し、設定モードで次のコマンドを入力します。

```
set deviceconfig setting preserve-prenat-feature yes
```

将来この機能を無効にする必要がある場合は、`set deviceconfig setting preserve-prenat-feature no` と入力します。

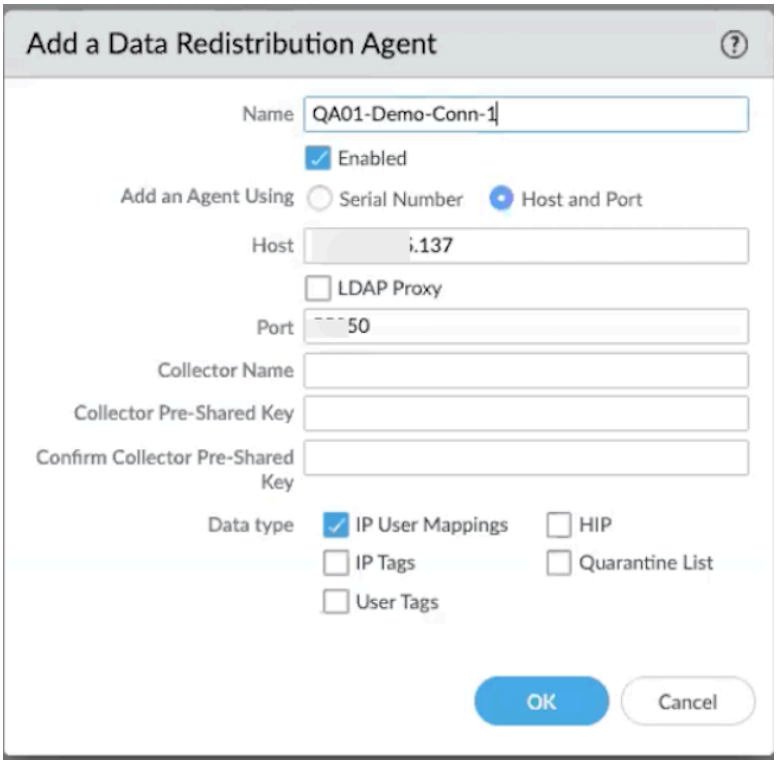
©2025 Palo Alto Networks, Inc.

STEP 6 | ユーザー *ID* の再配信を設定する場合は、手順 *3*「ユーザー ***ID*** ポート範囲」で指定した範囲内の各ポートに再配信エージェント エントリを追加する必要があります。たとえば、範囲が *55050* ～ *55055* の場合、デプロイした *ZTNA* コネクタ リージョンの数に合わせて *6* つのエントリを構成する必要があります。

範囲内の各ポートについて、手順 *3* の *[*ユーザー ***ID*** 再配信エージェント ***IP]*** から *[*ホスト*]* フィールドに *1* つの *IP* アドレスを選択します。*ZTNA* コネクタ レベルで冗長性が必要な場合は、 ユーザー ***ID*** 再配信エージェント ***IP*** から *2* つのアドレスを選択し、両方の *IP* アドレスに完全なポート範囲を適用できます。あるいは、 ユーザー ***ID*** 再配信エージェント ***IP*** 内のすべての *IP* アドレス上のすべてのポートを構成することもできます。

ユーザー **ID** 再配信エージェント **IP**内の 1 つ以上のアドレスを使用して、 ユーザー **ID** ポート範囲の 範囲内の各ポートに再配信エージェントを追加します。

1. NGFW UI で、[デバイス] に移動し、[データ再配信]を選択します。
2. [追加] をクリックし、 名前 を追加して、[有効] チェックボックスをオンにします。
3. ホストとポートを選択し、手順 3 の ユーザー **ID** 再配信エージェント **IP** をホストに追加し、手順 3 でコピーした ユーザー **ID** ポート範囲 を追加します。
4. **[IP** ユーザー マッピング] チェック ボックスをオンにして、**[OK]**をクリックします。

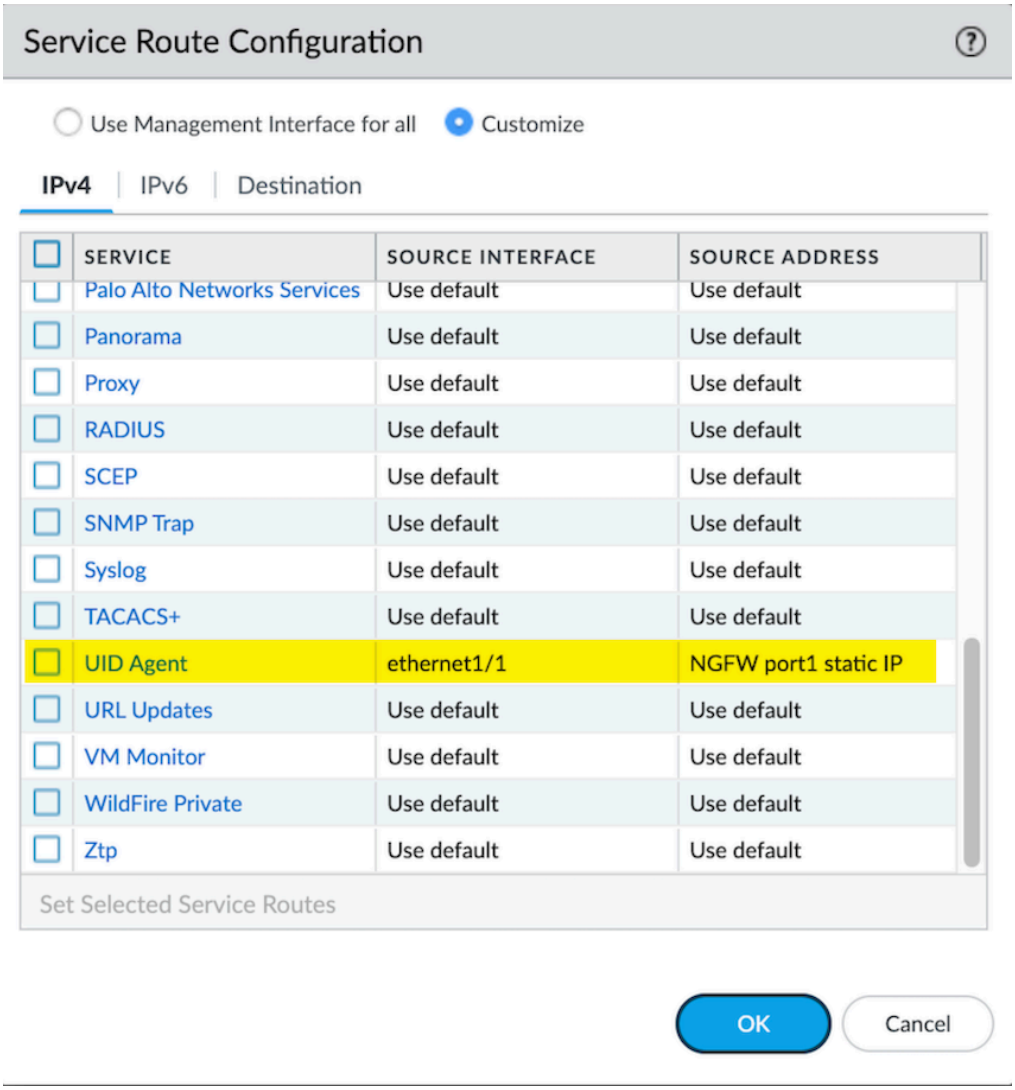


5. **Commit** [コミット]をクリックして設定を保存します。

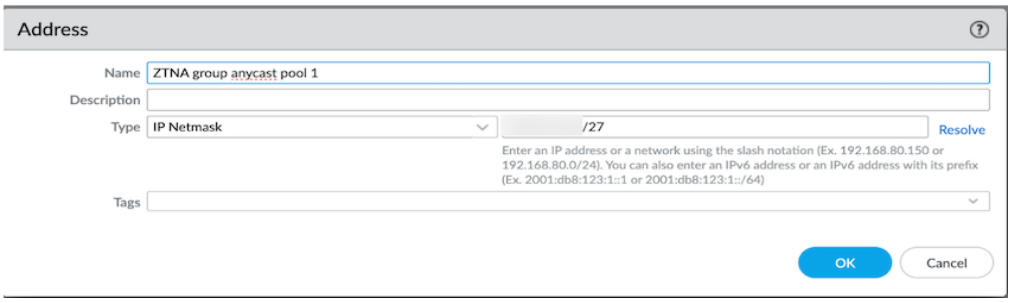
©2025 Palo Alto Networks, Inc.

STEP 7 | NGFW UI で、[デバイス > セットアップ] > [サービス] > [サービス ルート構成] > **[UID** エージェントの > カスタマイズ]に移動します。

1. **IPv4**の下で、 ソース インターフェース として イーサネット**1/1**(ZTNA コネクタに面したインターフェース) を選択し、 ソース アドレスを追加します。



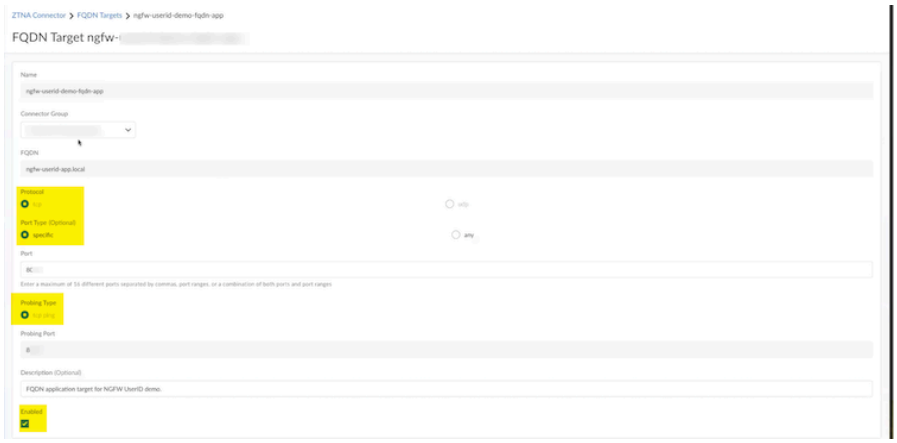
STEP 8 | 送信元 IP アドレスを持つ TCP パケットを許可するセキュリティ ポリシー ルールを追加します。手順 3 でコピーした Anycast IP アドレスである送信元 IP アドレスを追加し、**[OK]**をクリックします。



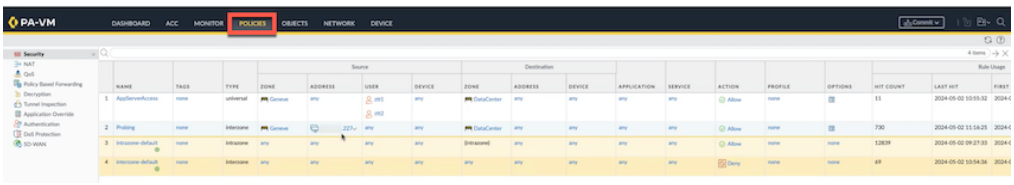
 ©2025 Palo Alto Networks, Inc.

STEP 9 | (任意) TCP プロービングを有効にします。

1. FQDN ターゲットを作成するには:
   1. **[ワークフロー] > [アプリケーション ターゲット] > [FQDN ターゲット]** に移動し、**[FQDN ターゲットの作成]**をクリックします。
   2. 名前 を追加し、 コネクタ グループを選択します。
   3. **tcp**、**specific**、**tcp ping**、および **Enabled** を有効にします。ポート を追加し、「作成」をクリックします。



STEP 10 | NGFW UI で、「ポリシー」 に移動し、ユーザー ID ベースのポリシーを定義します。



 ©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

動的権限アクセス設定を構成する

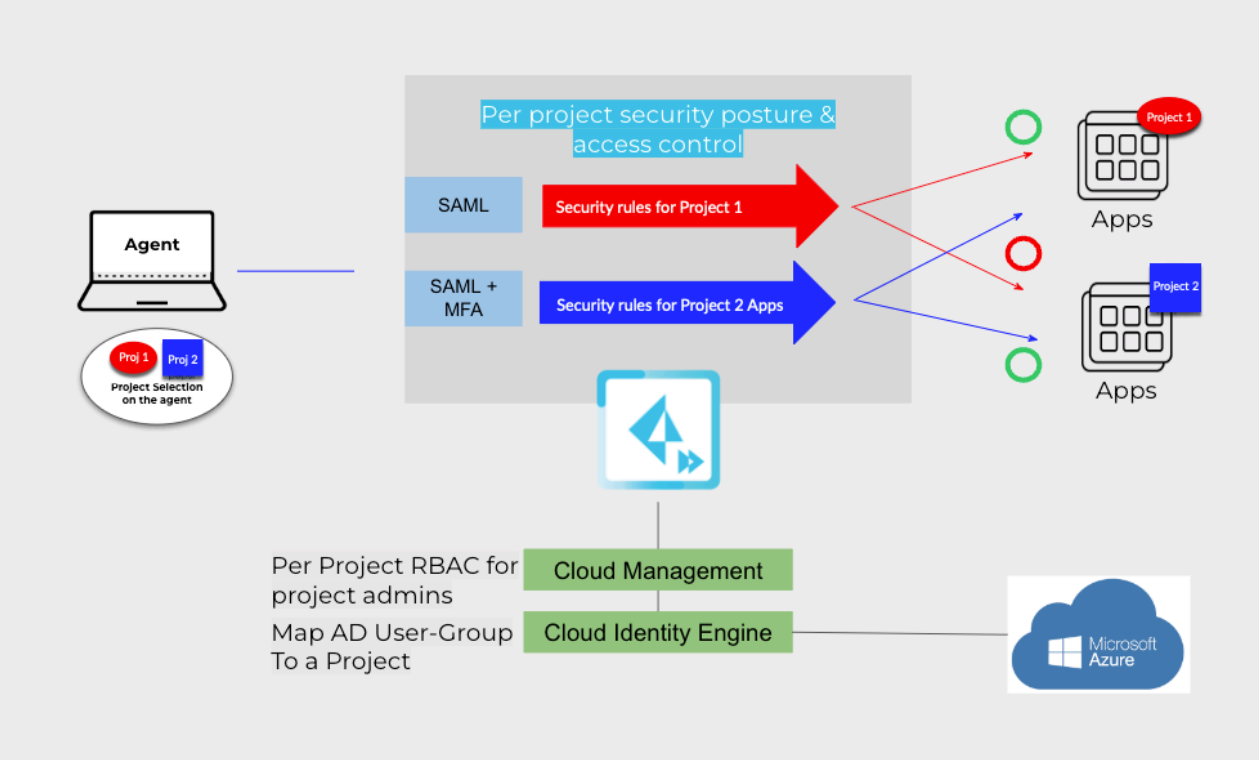
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Accessのライセンス ❑ Prisma Access 5.1 ❑ ロール:スーパーユーザー

顧客プロジェクトにアクセスできるユーザーを制御する必要がある IT エンタープライズおよび IT 対応サービス (ITES) 企業の場合、 動的権限アクセスは 、ユーザーが割り当てられたプロジェクトにのみアクセスできるように、シームレスで安全な区分化された方法を提供します。これらの企業では通常、従業員に複数の顧客プロジェクトを割り当て、これらのプロジェクトへのサイロ化されたアクセスを提供することで、承認されたユーザーが一度にアクセスできる顧客プロジェクトは1つだけになるようにしています。

動的特権アクセスとは何ですか?

動的な特権アクセスは、ユーザーがPrisma Access Agentで選択したワークフローやプロジェクトに基づいて、ユーザーにダイナミックな特権を提供するPrisma Accessの機能です。プロジェクトに割り当てられたユーザー グループとIPプールの組み合わせに基づいて、ユーザーに動的な権限を与えることができます。このユニークな組み合わせがプロジェクトを定義します。動的権限アクセスを使用すると、ネットワーク内のリソースを分離して、割り当てられているプロジェクトに応じてユーザーのみがアクセスできるようにすることができます。

Prisma Accessでは、プロジェクト管理者がプロジェクト定義の作成と管理を行えるように、プロジェクト管理者と呼ばれる新しい定義済みロールが利用できる。プロジェクト管理者は、Prisma Accessロケーション グループを選択してプロジェクトをマッピングし、プロジェクトとロケーション グループに基づいて、DHCPを使用してIPアドレスの割り当てを作成することができます。プロジェクト管理者は、Strata Cloud Managerで割り当てられているプロジェクトのみを管理できます。



エンドユーザーが、管理対象デバイスでダイナミック特権アクセスが有効になっているPrisma Access Agentにログインすると、以下のワークフローが実行されます。

1. エンド ユーザーは、割り当てられているプロジェクト (たとえば、プロジェクト 1) を選択します。
2. ユーザー IDはCloud Identity Engineで認証され、ユーザーのユーザー グループがプロジェクトにマッピングされます。
3. 認証が成功し、ユーザー グループがプロジェクト管理者によって設定されたプロジェクト基準と一致すると、ユーザーはプロジェクト1のプロジェクト固有の設定と、プロジェクトごとにセキュリティ体制とアクセス制御を提供するセキュリティ ルールを通じて、ネットワーク

©2025 Palo Alto Networks, Inc.

内のリソースにアクセスできるようになります。 セキュリティ インフラストラクチャは、セキュリティ ルールを適用して、ユーザー アクセスをそのプロジェクトに属するリソースとアプリケーションのみに制限します。他のプロジェクトのリソースやアプリケーションへのアクセスは許可されていません。

4. ユーザーが別のプロジェクト (たとえば、プロジェクト2) に切り替えると、以前のプロジェクト (プロジェクト1) からサインアウトされます。その後、プロジェクト固有の設定とプロジェクトのセキュリティ ルールに基づいて、2番目のプロジェクトのリソースにアクセスできるようになります。

Strata Cloud Managerを使用してユーザーのプロジェクト活動を監視し、ネットワーク内のサービ ス消費とセキュリティ状況を表示することで、Prisma Access Agentデプロイメント状況を可視化できます。

©2025 Palo Alto Networks, Inc.

AAからBBまでのダイナミック特権アクセスを有効にする

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ モバイルユーザーサブスクリプション付きPrisma Accessライセンス ❑ アクティベーション リンク ❑ Strata Logging Service ❑ Cloud Identity Engine ❑ Prisma Access Agent ❑ ロール：カスタマー サポート ポータルにアクセスできるマルチテナント スーパーユーザーまたはスーパーユーザー

ダイナミック特権アクセスを使用すると、IT管理者はエンド ユーザーを複数の顧客プロジェクトにマッピングできます。承認されたユーザーは、一度に1つの顧客プロジェクトにのみアクセスできます。

ダイナミック特権アクセスは、新しいPrisma Access テナントのアクティベーション時のオプション機能です。この機能を有効にしてテナントをアクティブ化すると、DPA はテナントの有効期間中設定され、無効にすることはできません。

DPAを有効にするオプションは、新しいPrisma Accessテナントの最初のアクティベーション時に1回だけ利用できます。テナントがアクティブ化されると、アドオンや更新を含む以降のすべてのアクティブ化に対してオプションは非表示になります。既存のテナントにはご利用いただけません。

STEP 1 | お使いのテナントでこの機能を有効にするには、Palo Alto Networksのアカウント担当者にお問い合わせください。

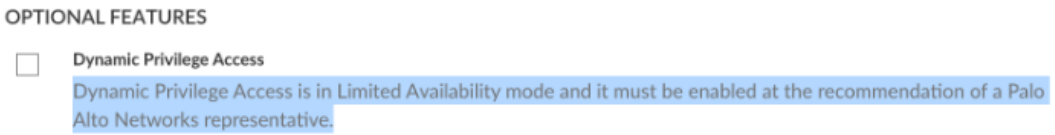
STEP 2 | Prisma Access (Managed by Strata Cloud Manager)のライセンスをアクティベートします。

STEP 3 | ライセンスを割り当て、 サービス接続を計画し、それに応じて ロケーションを追加します。

STEP 4 | 利用可能なアドオンを有効にします。

©2025 Palo Alto Networks, Inc.

STEP 5 | 動的権限アクセスのチェックボックスをオンにします。



STEP 6 | 利用規約に同意します。

STEP 7 | 今すぐアクティベートします。有効化する製品とアドオン（例：Prisma AccessまたはStrata Logging Service）がプロビジョニングされました。サブスクリプションがアクティブ化されると、進行状況が表示されます。プロセスが完了すると、テナントのステータスが Upと表示されます。これで、購入した製品のインスタンスがプロビジョニングされたテナントが作成されました。テナントには、このプロセスを開始したときに使用したアカウントである1人のユーザーがいます。

STEP 8 | 残りの製品セットアップを完了するには、 購入した製品にアクセスし 、インストール後の必要な構成を実行する必要があります。製品の詳細については、以下を参照してください。

- オープンAPI
- Strata Logging Serviceスタート ガイド
- Prisma Access (Managed by Strata Cloud Manager)管理者ガイド
- Cloud Identity Engine スタートガイド

STEP 9 | ユーザー アクセスを追加し 、 ロールを割り当てます。

プロジェクトに基づいて、 プロジェクト管理者 としてユーザーにアクセス権を付与します。

 ©2025 Palo Alto Networks, Inc.

動的権限アクセスのためにCloud Identity Engineでユーザー グループ マッピングを承認する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Accessライセンス ❑ 最低限必要なPrisma Accessバージョン:5.1 ❑ ロール:スーパーユーザー

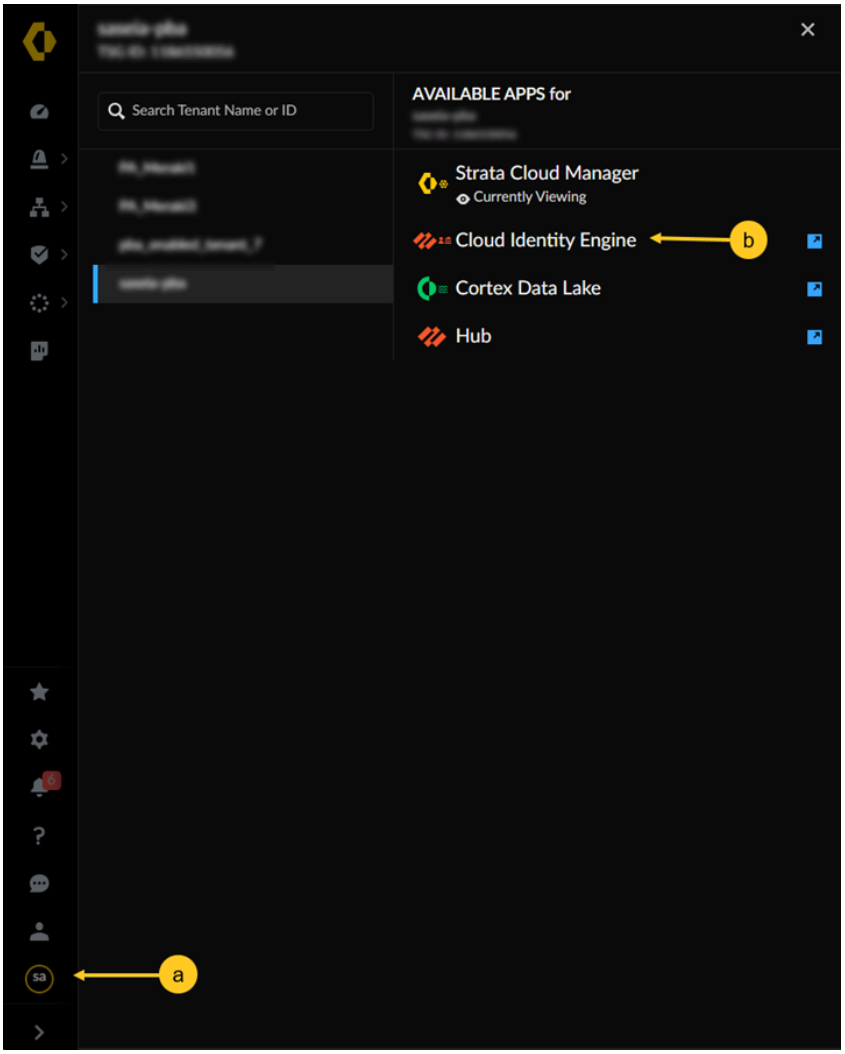
始める前に、次の前提条件を満たしていることを確認してください。

- Dynamic Privilege Access functionalityを有効にするには、Palo Alto Networksのアカウント担当者にお問い合わせください
- Cloud Identity Engine をアクティブ化し 、最初のテナントを作成します。
- Cloud Identity Engineをセットアップする。

このワークフローでは、AzureをIdPとして使用します。OktaをIdPとして使用することもできます。

©2025 Palo Alto Networks, Inc.

STEP 1 | Strata Cloud Managerから、テナントに関連付けられているCloud Identity Engineアプリを開きます。

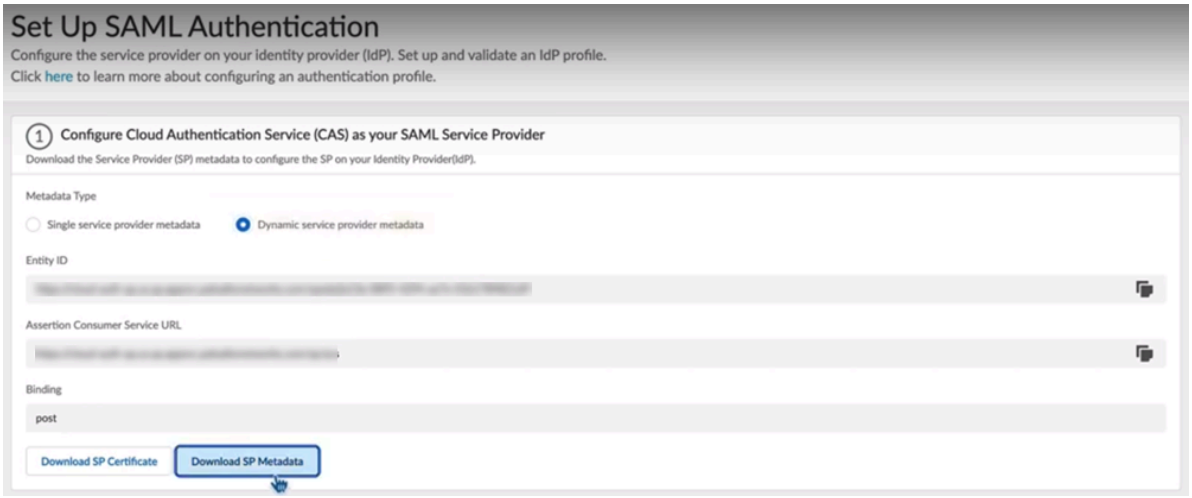


STEP 2 | モバイル ユーザーのIdPとして Azureディレクトリ またはOktaディレクトリを追加します。

©2025 Palo Alto Networks, Inc.

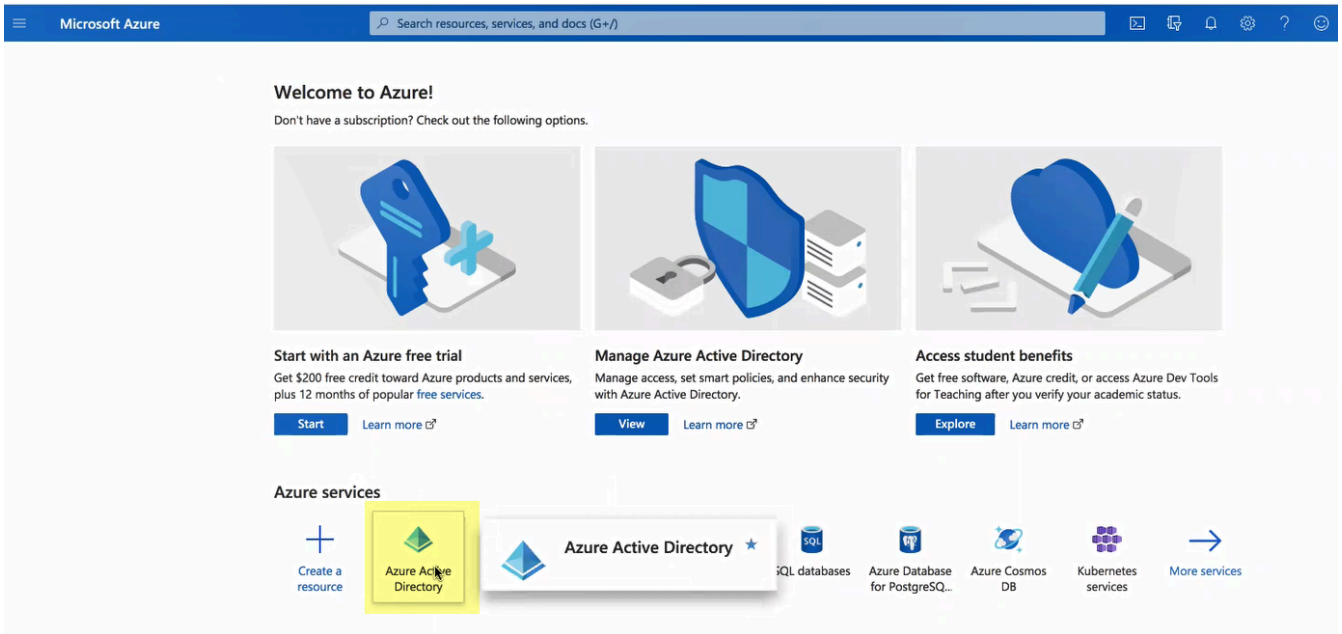
STEP 3 | Cloud Identity EngineアプリでSPメタデータをダウンロードします。

1. [認証] > [認証タイプ] > [新しい認証タイプの追加]に移動します。
2. SAML 2.0 認証タイプを設定します 。
   動的サービス プロバイダー メタデータを選択します。
3. **SP** メタデータをダウンロードします。



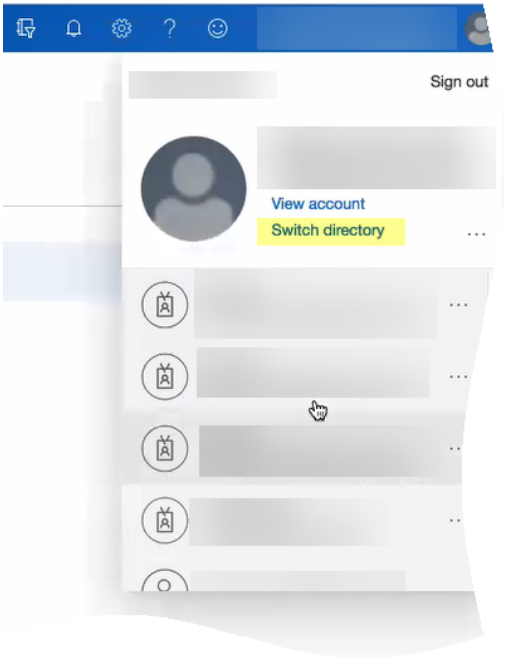
4. Azureポータルで、Azure Active Directory (アクティブディレクトリ - AD)を選択します。

   Azureポータルで必要な手順をすべて完了していることを確認してください。

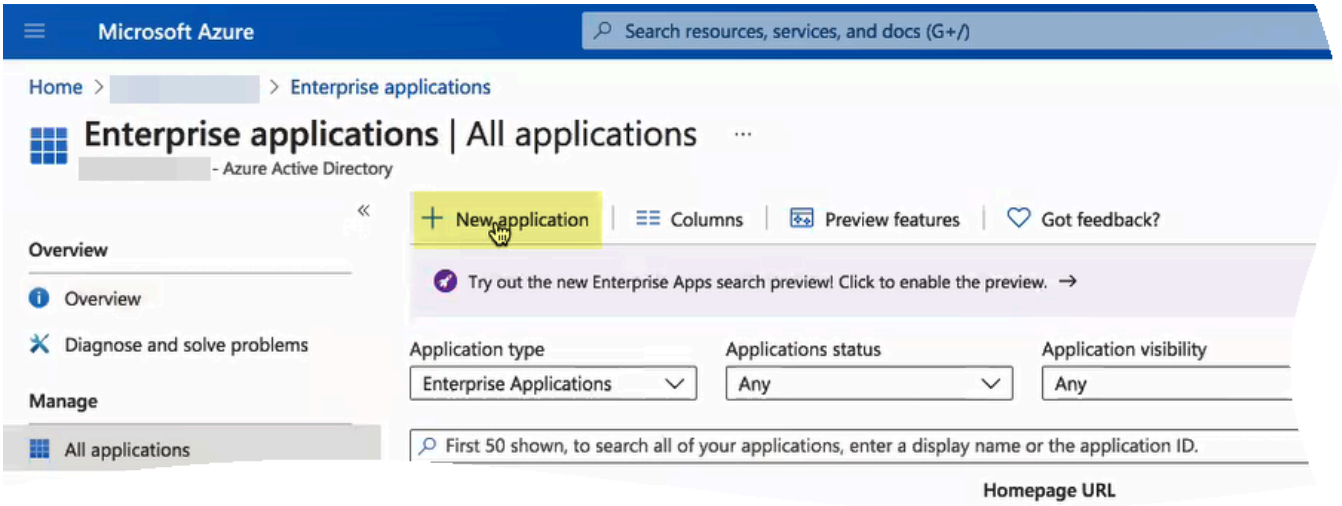


   複数のディレクトリがある場合は、ディレクトリを切り替えて、Cloud Identity Engineで使用するディレクトリを選択します。

 ©2025 Palo Alto Networks, Inc.



5. **Enterprise Applications**（エンタープライズアプリケーション）を選択して、**+New Application**（+新しいアプリケーション）をクリックします。



6. **`Palo Alto Networks Cloud Identity Engine - Cloud Authentication Service`**を検索し、Azure Active Directory (AD) シングル サインオン統合を作成します 。

   アプリケーションの作成中に必要に応じてアプリ名をカスタマイズします。

7. アプリケーションが読み込まれたら、[ユーザーとグループ]を選択し、[ユーザー/グループの追加]を選択して 、このアプリケーションに 割り当てます 。

   認証 Cloud Identity EngineのAzure IdPを使用するユーザーとグループを選択します。

 ©2025 Palo Alto Networks, Inc.

構成が完了したらテストできるように、使用しているアカウントを必ず割り当ててください。テストを正常に完了するには、アカウントを追加した後にページを更新する必要がある場合があります。

8. シングル サインオンをセットアップし 、**SAML**を選択します。
9. 手順3.cで Cloud Identity Engineアプリからダウンロードしたメタデータ ファイルを参照して[追加]をクリックし、メタデータ ファイルをアップロードします。
10. メタデータのアップロード後、次の形式を使用してサインオン**URL**としてリージョン エンドポイントを入力します: https://<RegionUrl>.paloaltonetworks.com/sp/acs（ここで<RegionUrl>はリージョンのエンドポイントです)。

    または、返信URLをサインオンURLにコピーします。
11. **Save**（保存）を選択して、設定内容を保存します。

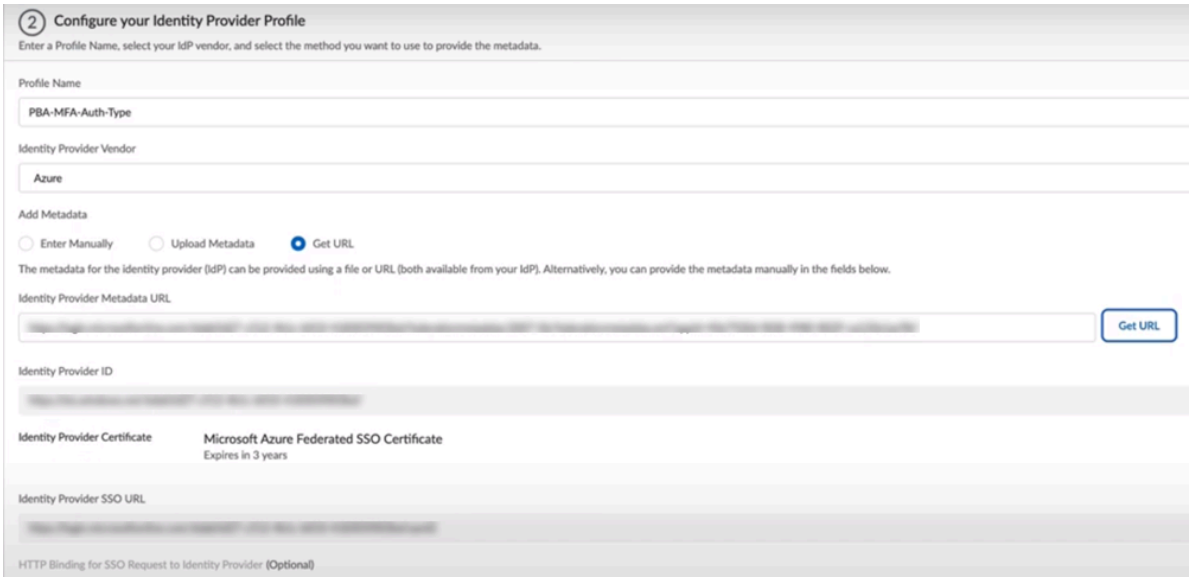
STEP 4 | 条件付きアクセス ポリシーを構成して、選択したユーザー グループでMFAを有効にします。

1. アプリケーションの[概要] > [条件付きアクセス] > [ポリシーの作成]に移動します。
2. 新しいポリシーを追加します。
3. ポリシー名を入力します。
4. [ユーザー]セクションで、[ユーザーとグループの選択]を含め、それに応じてプロジェクト グループを選択します。
5. ターゲット リソースを確認します。
6. ポリシーをトリガーする条件を選択します。
7. アクセス制御で多要素認証を要求するを使用してアクセスを許可します 。
8. セレクターを [オン]に切り替えてポリシーを有効にし、条件付きアクセスを作成します。

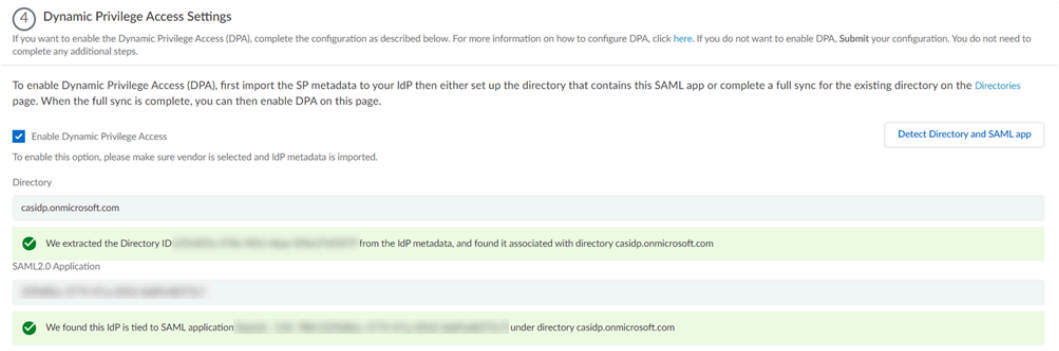
 ©2025 Palo Alto Networks, Inc.

STEP 5 | 認証タイプとしてIdPベンダーを追加します。

1. シングル サインオン > **SAML**証明書 を選択し、アプリ フェデレーション メタデータ **URL**をコピーします。
2. Cloud Identity Engine アプリで、[認証] [> 認証タイプ] > [新しい認証タイプの追加]を選択します。
3. SAML 2.0 認証タイプを設定します 。
4. **[ID** プロバイダー プロファイルの構成]で、 プロファイル名を入力します。
5. **IDP** ベンダーとして **Azure** を選択します。
6. **[URL**を取得]を選択し、ステップ5.aのURLを貼り付けます。次にメタデータを取得するための**URL** を取得します 。



7. アイデンティティプロバイダーで多要素認証を有効にします。
8. プロファイル構成を確認するには、 **SAML** セットアップをテストします 。
9. Prisma Accessが認証に使用するSAML属性を選択します。
10. 動的特権アクセスを有効にします。
    手順2で追加したディレクトリとSAMLアプリを必ず同期してください。



11. IdPプロファイルを送信します 。

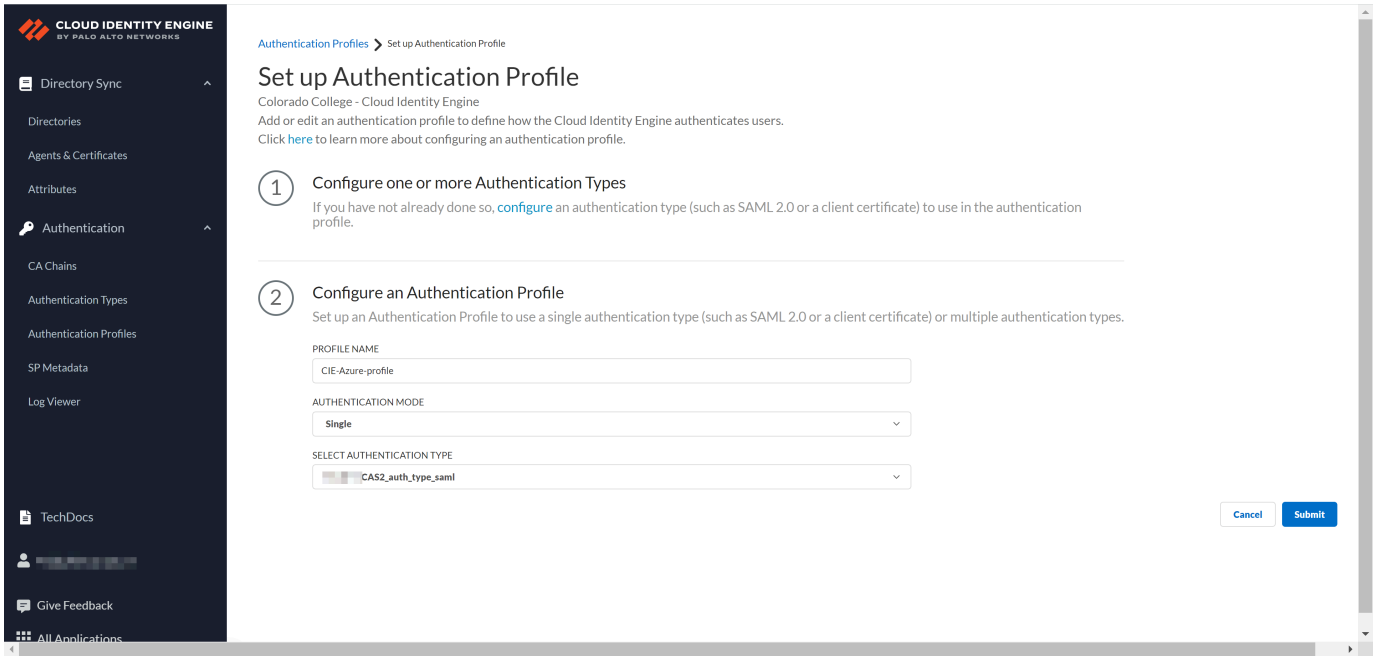
 ©2025 Palo Alto Networks, Inc.

STEP 6 | 3から5までの手順を繰り返して、MFAを必要としないユーザー グループのSAMLアプリを設定します。

> *MFA*を必要としないユーザー グループの手順5.gでは、*MFA* を有効にしないでください。

STEP 7 | MFAユーザー グループと非MFAユーザー グループの認証プロファイルを追加します。

1. [認証] > [認証プロファイル] > [認証プロファイルの追加]を選択します。
2. プロファイル名を入力します。
3. 認証方式を選択します。
4. MFAを必要とするユーザー グループに基づいて、手順またはから認証タイプを選択し、送信します。

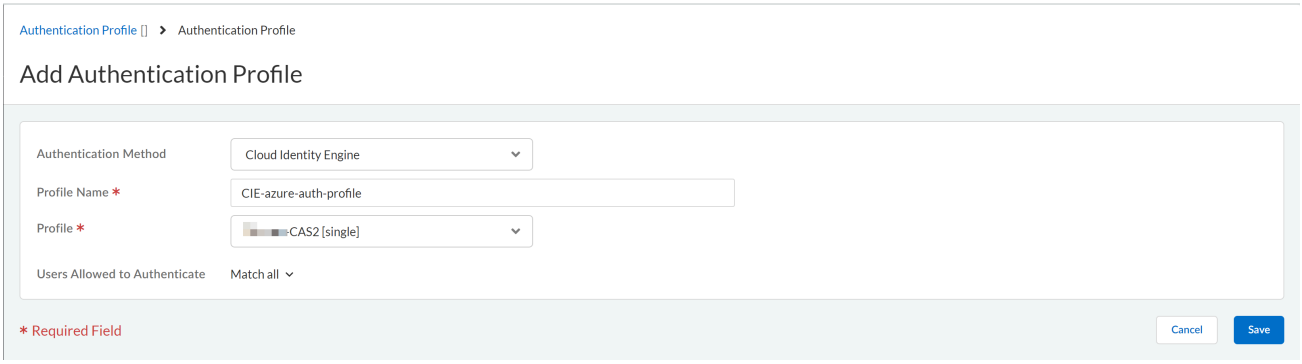


 ©2025 Palo Alto Networks, Inc.

STEP 8 | Cloud Identity EngineからPrisma Accessに認証プロファイルを追加します。

1. Strata Cloud Manager で、[管理] > [設定] > **[NGFWとPrisma Access]** > **[ID**サービス] > [認証] > [認証プロファイル]を選択します。

   構成スコープを**Access Agent**モバイル ユーザー コンテナーに設定してください。
2. プロファイルを追加します。
3. 認証方法として**Cloud Identity Engine** を選択します。
4. **Profile Name (**プロファイル名)を入力します。
5. 手順 7からCloud Identity Engineアプリに追加したプロファイルを選択します。
6. 変更を保存します。



STEP 9 | モバイル ユーザーに認証を添付します。

1. Strata Cloud ManagerからPrisma Accessを起動します。
2. **[Manage (**管理)] > **[Configuration (**設定)] > **[NGFWとPrisma Access]**を選択します。
3. 作成したプロジェクト スニペットにスコープを設定し、[セキュリティサービス] > [セキュリティ ポリシー]に移動します。
4. 特定のプロジェクトDHCP範囲とそのプロジェクトベースのユーザー グループからのトラフィックのみを許可するポリシーを作成します。

©2025 Palo Alto Networks, Inc.

Access Agentを有効にします。

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ MacOS 12以降のデスクトップデバイスまたはWindows 10バージョン2024以降またはWindows 11デスクトップデバイス ❑ モバイルユーザーサブスクリプション付きのPrisma Accessライセンス ❑ ロール:スーパーユーザー

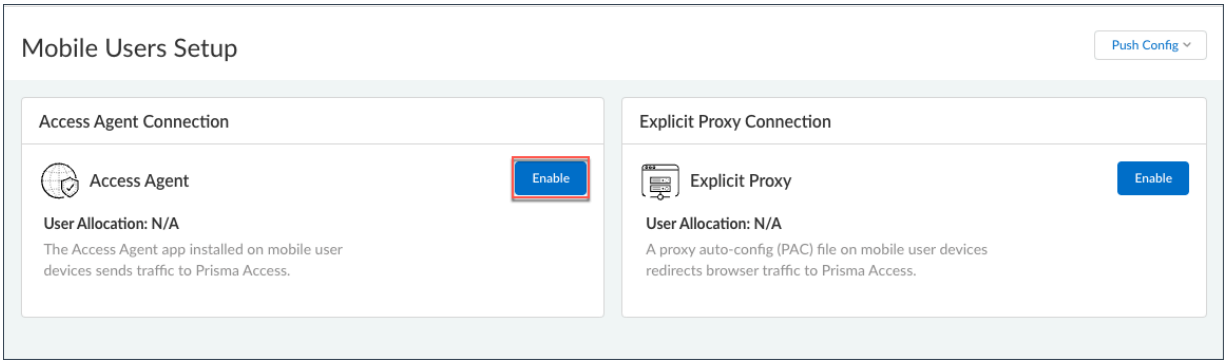
ユーザをオンボード接続する前に、Strata Cloud Managerを使用してモバイル ユーザー接続タイプとして**Access Agent**を有効にする必要があります。接続タイプを有効にした後、モバイルユーザー デバイスにインストールされたPrisma Access AgentsはPrisma Accessにトラフィックを送信できるようになります。

Prisma Access Agentを有効にし始める前に、動的権限アクセスのためにCloud Identity Engineでユーザー グループ マッピングを承認するを確認してください。

STEP 1 | [ワークフロー] > [**Prisma Access** セットアップ] > [モバイルユーザ] を選択します。

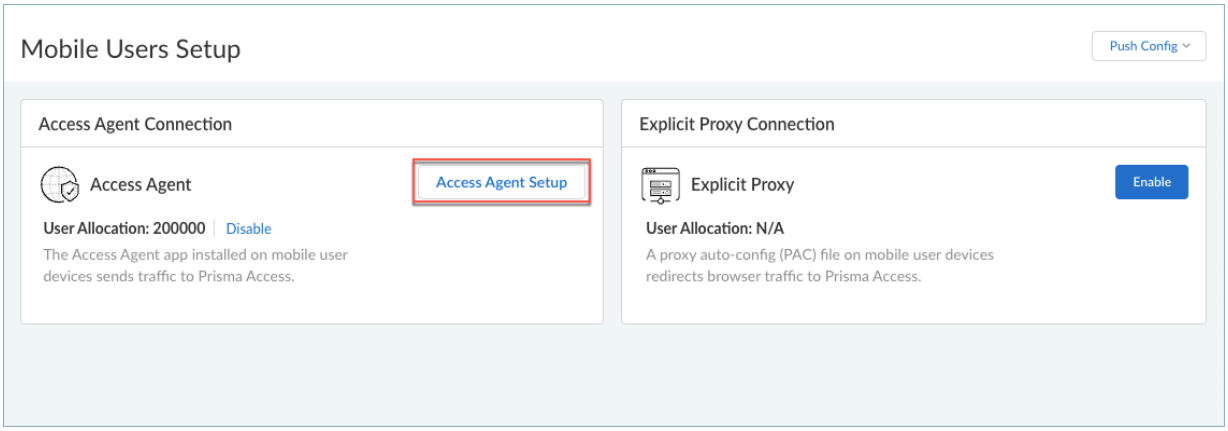
STEP 2 | Access Agentを有効にします。

明示的プロキシは*Prisma Access*エージェントではサポートされていません。

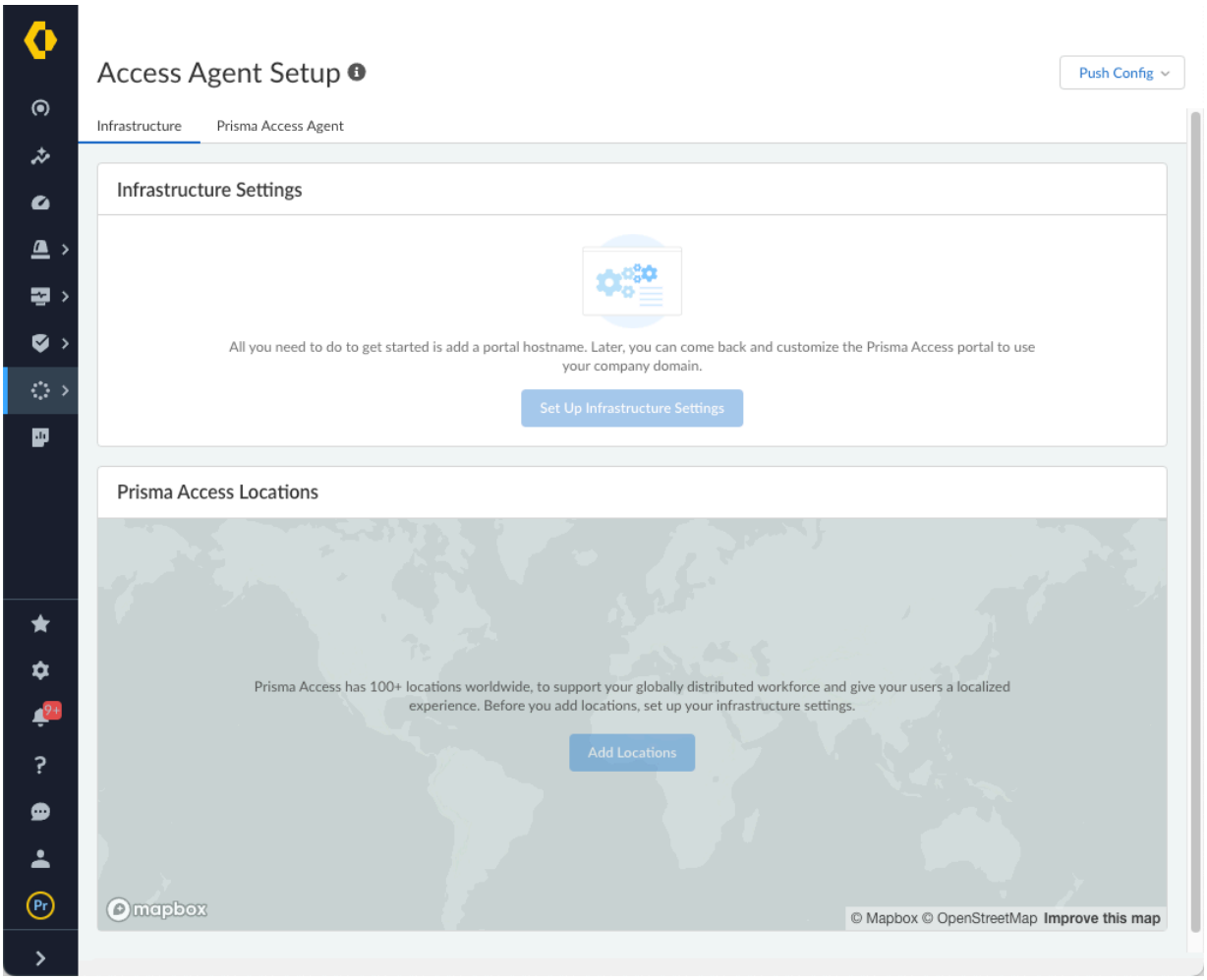


 ©2025 Palo Alto Networks, Inc.

STEP 3 | **[Access Agentセットアップ]**をクリックして、モバイルユーザーのオンボーディングを開始します。



Access Agentのセットアップページが表示されます。



 ©2025 Palo Alto Networks, Inc.

動的権限アクセスのためのエージェント インフラストラクチャの設定

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ モバイルユーザーサブスクリプション付きのPrisma Accessライセンス ❑ MacOS 12以降のデスクトップデバイスまたはWindows 10バージョン2024以降またはWindows 11デスクトップデバイス ❑ ロール:スーパーユーザー

Prisma Accessがモバイル ユーザー環境をプロビジョニングできるように、Prisma Access Agentのインフラ設定を構成します。次に、Prisma Access Agentユーザーが接続するPrisma Accessロケーションを選択します。

また、データセンターまたは本社のプライベート アプリにアクセスするためのサービス接続を作成した場合は、オプションで Dynamic Privilege Access の SC-NAT サポートを有効にしたり、Dynamic Privilege Access のルート集約を有効にして ネットワークに送信されるルートの数を減らしたりすることもできます。

インフラストラクチャ設定を構成する

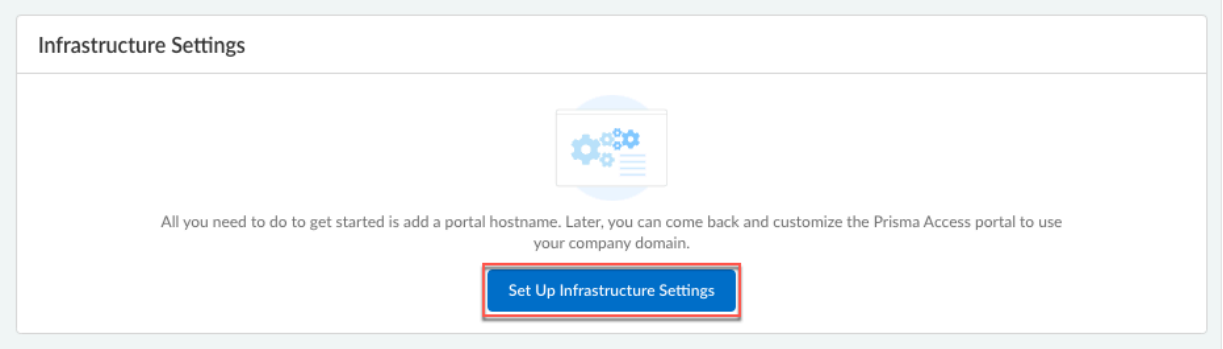
ユーザがインターネット アクセスのみPrisma Accessを利用できるように、Prisma Accessはデフォルトの IPアドレス プールとクラウド・デフォルトのDNSサーバを提供します。ただし、モバイルユーザーが本社、データセンター、またはPrisma Accessにオンボードしたリモートネットワークサイトにある社内リソースにアクセスできるようにしたい場合は、クライアント IP アドレス プールを割り当てる必要があります。 Prisma AccessはIP アドレス プールを使用して、モバイル ユーザーに IP アドレスを割り当て、Prisma Access サービス インフラストラクチャをセットアップします。

インフラストラクチャ設定を構成する前に、少なくとも *1* つのプロジェクトを構成していることを確認してください。そうしないと、インフラストラクチャ設定をコミットしてプッシュしようとすると、コミットが失敗します。詳細については、「プロジェクトを作成する」を参照してください。

STEP 1 | Strata Cloud Managerで、**[ワークフロー] > [Prisma Access セットアップ] > [Access Agent] > [インフラストラクチャ]**を選択します。

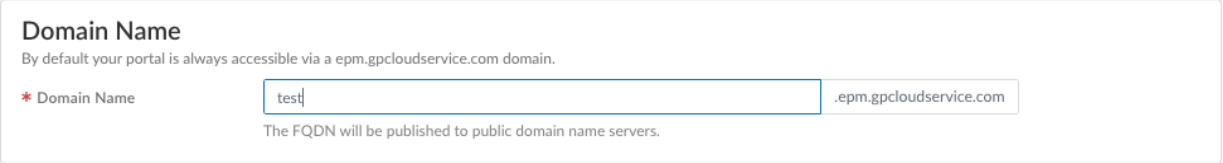
©2025 Palo Alto Networks, Inc.

STEP 2 | インフラストラクチャを初めて設定する場合は、[インフラストラクチャ設定のセットアップ]をクリックします。それ以外の場合は、 インフラストラクチャ設定を編集します。



STEP 3 | Prisma Accessエージェントが接続するサービスの ドメイン名 にホスト名を追加します。

デフォルトでは、ユーザーはホスト名と**.epm.gpcloudservice.com** ドメインに基づくFQDNを使用してサービスにアクセスできます。

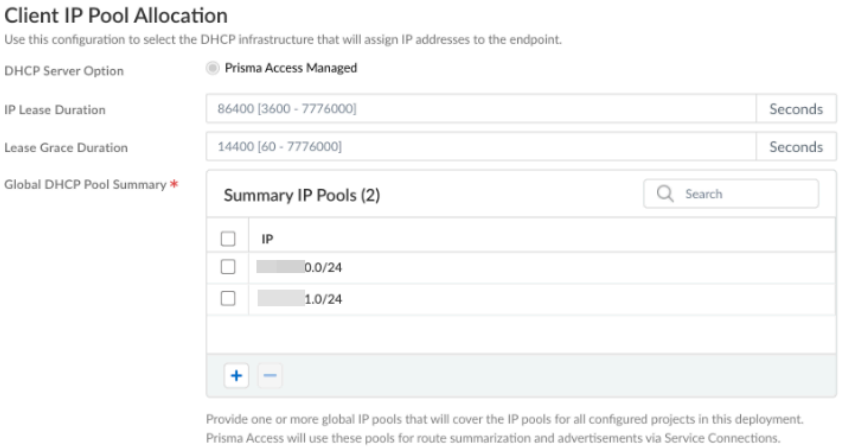


STEP 4 | クライアント**IP**プール割り当てでは、 Prisma Accessは動的権限アクセスのためにエンドポイントへの IP アドレスの割り当てを管理する DHCP サーバーを提供します。

Prisma Accessからのプロジェクト名とロケーショングループ ID は、DHCP 要求の一部です。特定のプロジェクトに接続する各Prisma Access Agentには、そのプロジェクトの IP サブネットから IP アドレスが割り当てられます。ユーザーが別のプロジェクトに変更すると、プ

©2025 Palo Alto Networks, Inc.

ロジェクトの IP サブネットとは異なる IP アドレスが Prisma Access Agentに割り当てられます。



次のオプションを設定できます。

- **IP**リース期間- DHCPサーバーがPrisma Access AgentにIPアドレスをクライアントに割り当てる時間（秒単位）を指定します。デフォルトの IP アドレスのリース期間は 86,400 秒です。
- リース猶予期間- リースの有効期限が切れた後、Prisma Access Agentがその IP アドレスリースを使用し続けられる 時間を指定する。デフォルトのリース猶予期間は 14,400 秒です。
- グローバル **DHCP** プール サマリー-SC-NAT を有効にする IP プールを選択するか、 ルート集約用のグローバル サマリー IP プールを設定および選択します。

STEP 5 | インフラストラクチャ設定を保存します 。

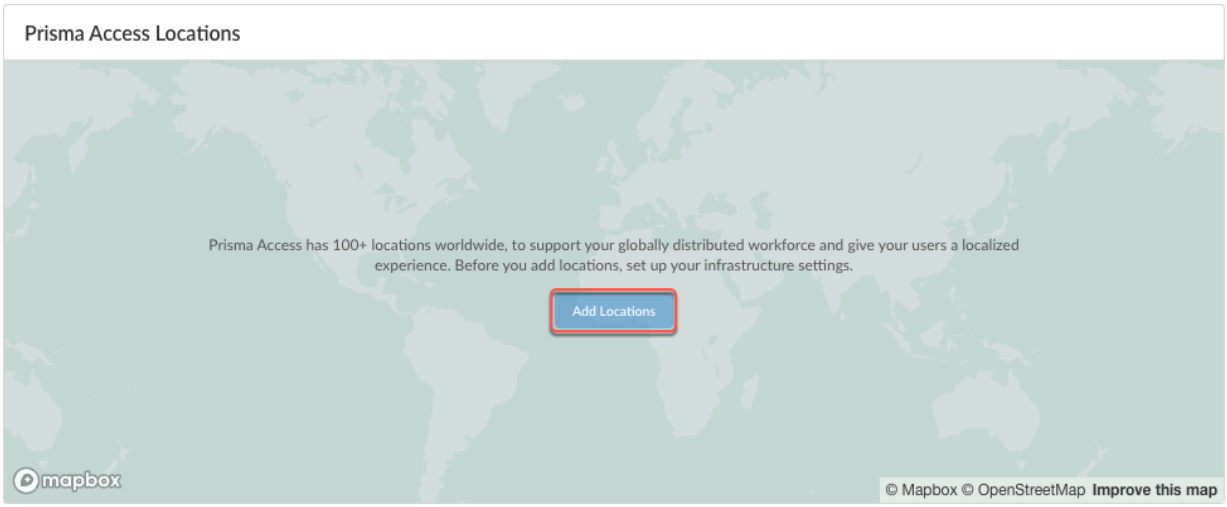
Prisma Accessロケーションの選択

Prisma Access Agentユーザーをサポートする Prisma Accessロケーションを追加します。場所グループは、動的権限アクセスに使用されます。

STEP 1 | Strata Cloud Managerで、[ワークフロー] > **[Prisma Access** セットアップ] > **[Access Agent]** > [インフラストラクチャ]を選択します。

©2025 Palo Alto Networks, Inc.

STEP 2 | インフラストラクチャを初めて設定する場合は、 場所を追加します。それ以外の場合は、**Prisma Access**ロケーションを編集します。



STEP 3 | モバイル ユーザーが接続するPrisma Accessの場所を選択します。

ライセンス契約に応じて、ローカルまたは世界全域の場所を選択できます。マップには、Prisma Access for Usersをデプロイできるリージョンが表示されます。さらにPrisma Accessは、各地域内に複数の場所を提供し、ユーザーがユーザーのロケールに合わせたユーザー エクスペリエンスを提供する場所に接続できるようにします。最高のパフォーマンスをお求めの場合は、[すべて選択] を選択してください。または、選択した各地域内でユーザーがアクセスする必要がある特定の場所を選択します。デプロイを1つのリージョンに制限することで、デプロイメントされたリージョンをよりきめ細かく制御し、ポリシーや業界の規制で必要なリージョンを除外できます。

*Prisma Access*エージェントの場合、*Prisma Access*を次の*Strata Logging Service*リージョンにデプロイできます。

- アメリカ
- ドイツ
- インド

より多くの地域が利用可能になると、このリストは更新されます。

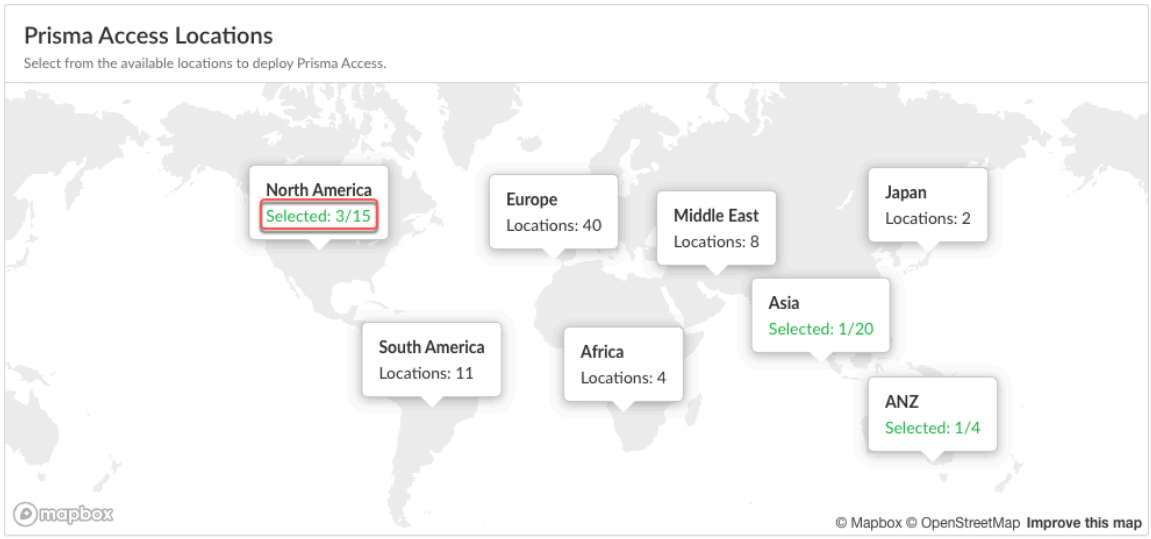
場所の数を制限する場合、最適なユーザー エクスペリエンスを実現するために、ユーザーに最も近い場所、またはユーザーと同じ国にある場所を選択してください。モバイル ユーザー

©2025 Palo Alto Networks, Inc.

が居住する国で場所が利用できない場合は、最高のパフォーマンスを得るために、ユーザーに最も近い場所を選択してください。

このセクションの画像は説明のみを目的として提供されています。

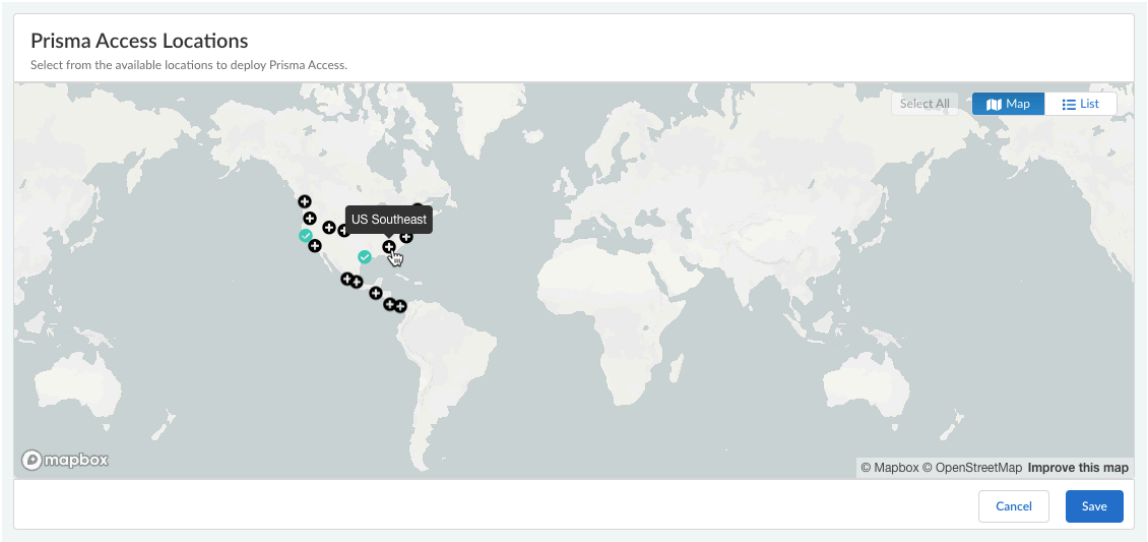
1. 地図上で利用可能な地域を選択します。



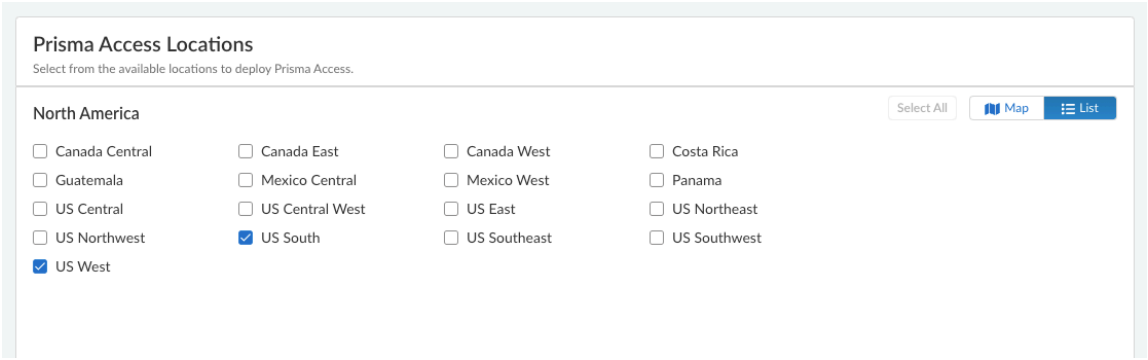
©2025 Palo Alto Networks, Inc.

2. 追加したい場所のプラス記号 + をクリックします。

   マップビューとリストビューを切り替えることができます。すべての場所を選択することもできます。



   リスト ビューでは、Prisma Access をデプロイできる場所のリストから選択できます。地域内のすべてのサイトを選択できます。



3. Prisma Accessの場所設定を保存します 。

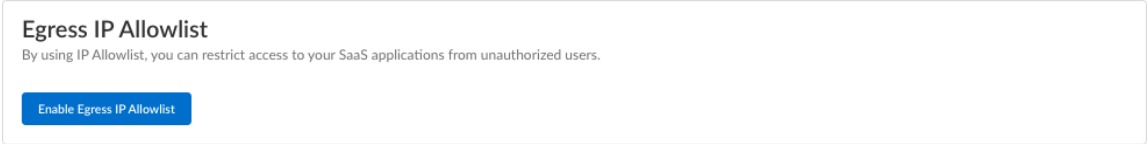
STEP 4 | (任意) 権限のないユーザーによるSaaSアプリケーションへのアクセスを制限します。

既存のモバイルユーザーのデプロイメントおよび新しいユーザーのオンボーディング中に、出口IP許可リストを有効にできます。既存のPrisma Accessデプロイメントに対して出口IP許可リストを有効にすると、Prisma Accessは、すでに場所に割り当てられているすべての出口IPアドレスを出口IP許可リストに移行します。新しいPrisma Accessデプロイメントの場合、Prisma Access Agentモバイル ユーザーをオンボードするときに、出口IP許可リストを有効にします。場所を追加したり、自動スケーリング イベントが発生するたびに、Prisma Accessが割り当てる新しい出口IPアドレスを取得し、SaaSアプリケーションの許可リストに

©2025 Palo Alto Networks, Inc.

追加する必要があります。その後、構成をPrisma Accessデプロイメントにプッシュして、場所に割り当てられた出口IP許可リストを確認できます。

1. 出口IP許可リストを有効にすると、 オンボードされたPrisma Accessの場所のIPアドレスが表示されます。



2. 割り当てられたアドレスをコピーして、SaaSアプリケーションの許可リストに追加します。
3. 移行して、Prisma Accessでオンボードされた場所に割り当てられたIPアドレスを確認します。
4. 新しくオンボードされた場所または自動スケーリング イベント中にIPアドレスを取得します。
    1. ロケーション名を選択して、その場所に割り当てられた新しい出口IPアドレスを見つけます。
    2. Prisma Accessで確認する前に、これらのIPアドレスをSaaSアプリケーションの許可リストに追加します。
    3. 割り当てられた出口IPアドレスを保存します。

動的な権限アクセスのSC-NATサポートを有効にする

DPAを使用しており、データセンターまたは本社のプライベート アプリケーションにアクセスするためのサービス接続を作成している場合は、動的な特権アクセス（DPA）のSC-NATサポートを使用してください。インフラ サブネットのIPアドレスが重複すると、DPA環境内の複数のプロジェクトでIPアドレスが枯渇する可能性があります。この問題を解決するために、Prisma Accessは次のようなIPアドレス用の送信元NAT (SNAT) を実装できます。

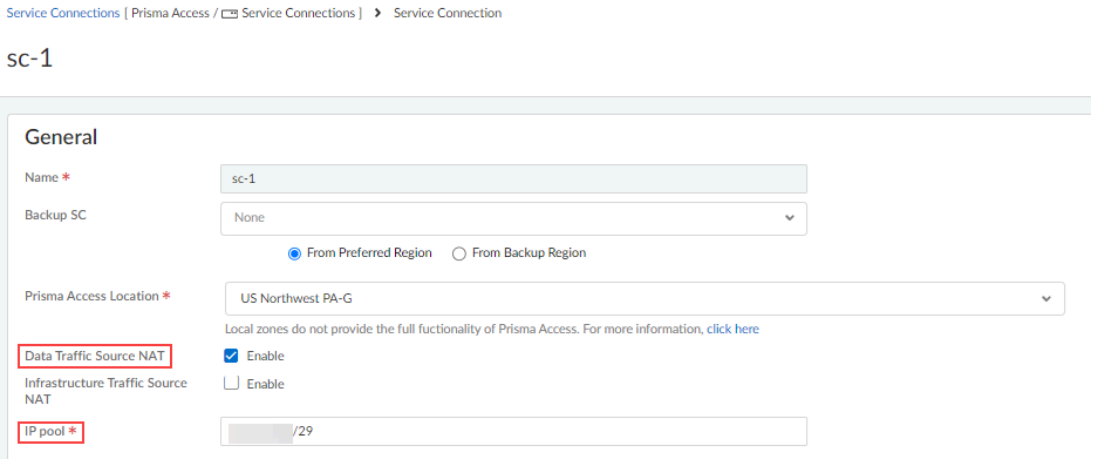
- サービス接続を使用してプライベート アプリにアクセスするモバイル ユーザーの単一IPアドレスをPrisma Accessにマップさせます
- 簡単にルーティングできるSNATを提供
- IPプールの重複を排除
- Prisma Accessとデータセンターまたは本社の間のIPプールのIPv4枯渇を解消します

DPA のお客様は、サービス接続を使用してクライアントの場所を Prisma Access にオンボードできます。ただし、複数のプロジェクトが複数のデータセンター上に大規模な IP プールを持つ場合があり、プライベート IP プールが枯渇する可能性があります。この問題を解決するために、Prisma Access の動的権限アクセスでは、定義されたプールを使用した SC-NAT のサポートが提供されます。顧客は、IP プールを分割するために、インフラストラクチャ サブネットの代わりに SC-NAT を使用するオプションがあります。サービス接続企業アクセス ノード (SC-CAN) に対して SC-NAT を有効にすると、そのサービス接続に対して SC-NAT が常にサポートされます。

DPA を有効にすると、プロジェクトごとに SC-NAT をオン (SC-NAT を使用する場合) またはオフ (インフラストラクチャ サブネットを使用する場合) にすることができます。

 ©2025 Palo Alto Networks, Inc.

1. Strata Cloud Manager で、[ワークフロー] > **[Prisma Access** セットアップ] > [サービス接続]を選択します。
2. サービス接続 テーブルからサービス接続を選択します。
3. データ トラフィック ソース **NAT**のチェック ボックスをクリックします。
4. **[データ トラフィック ソース NAT]** チェック ボックスをクリックすると、必須の **[IP** プール] フィールドが表示されます。SC-NAT を有効にするサブネットを入力します。
5. 変更を保存します。



動的権限アクセスのルート集約を有効にする

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.2 イノベーション ❑ 最小Prisma Accessデータプレーン バージョン:11.2.3 ❑ モバイルユーザーサブスクリプション付きPrisma Accessライセンス ❑ ロール:スーパーユーザー

数百のルートしか収容できないシンプルなクラウド ルーターなど、容量が限られたオンプレミス ハードウェアを持つ企業の場合、Prisma Access は、オンプレミス ネットワークへのルートをアドバタイズするときにモバイル ユーザー (MU) ルートを要約できます。ルート集約により、データセンターのルート容量内にとどまることで、これらのデバイスの要件が最小限に抑えられます。

ルート集約を有効にするには、複数のプロジェクトで使用できる大規模な IP プールのリストであるグローバル サマリー プールを構成できます。ユーザーが Prisma Access エージェントを使用してプロジェクトに接続し、エージェントにグローバル サマリー プールの範囲内の IP アドレスが割り当てられている場合、Prisma Access サービス接続は、より小さい集約ルートではなく、グローバル サマリー プールをアドバタイズします。

プロジェクトのルート集約を説明するために、次のシナリオを検討してください。

©2025 Palo Alto Networks, Inc.

- 10.10.0.0/16 のグローバル サマリー プールを設定し、サービス接続 **SC-A**でルート集約オプションを有効にします。
- **User-A** は 、IP プロジェクト プール 10.10.10.0/24 が割り当てられている **Project-A**に接続します。接続すると、Prisma Access Agent は 10.10.10.10/32 IP アドレスを取得します。
- **User-B** は 、IP プロジェクト プール 10.10.11.0/24 が割り当てられている **Project-B**に接続します。接続すると、Prisma Access Agent は 10.10.11.10/32 IP アドレスを取得します。
- この場合、サービス接続は、eBGP を介してオンプレミス ネットワークへの /24 集約ルートではなく、1 つのサブネット (10.10.0.0/16 のグローバル サマリー プール) のみをアドバタイズします。

- *Prisma Access* は、プロジェクトの一部ではない *IP* プールを要約しません。
- プロジェクト内のプロジェクト *IP* プールは重複する可能性があり、グローバル サマリー *IP* プールも重複する可能性があります。
- グローバル サマリー プールは、複数のプロジェクトに関連付けられたプロジェクト *IP* プールを含む大規模な *IP* プールである必要があります。

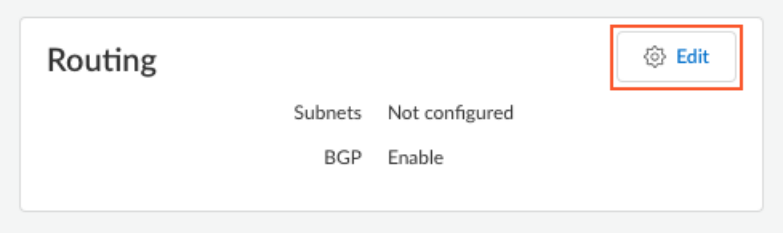
Strata Cloud Manager でプロジェクトのルート集約を有効にするには:

STEP 1 | プロジェクト設定で、プロジェクトの IP プールを構成するには以下より行います。**[Manage (管理)] > [NGFW とPrisma Access] > [<Snippet>] > [オブジェクト] > [Dynamic Privilege Access (動的な特権アクセス)] > [プロジェクト]**。

STEP 2 | **[ワークフロー] > [Prisma Access セットアップ] > [Access Agent] > [インフラストラクチャ設定]**でグローバル サマリー IP プールを構成します 。

STEP 3 | サービス接続でルート集約を有効にします。

1. **[ワークフロー] > [Prisma Access セットアップ] > [サービス接続]**に移動します。
2. サービス接続 テーブルからサービス接続を選択します。
3. ルーティング設定を編集します 。



4. アドバタイズする前にモバイル ユーザー ルートを要約するを選択します。



 ©2025 Palo Alto Networks, Inc.

STEP 4 | ルーティング設定を保存します 。

STEP 5 | サービス接続設定を保存します 。

STEP 6 | Prisma Access へのすべての管理者のプッシュ構成を実行します 。

©2025 Palo Alto Networks, Inc.

スニペットを作成する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ モバイルユーザーサブスクリプション付きのPrisma Accessライセンス ❑ ロール:スーパーユーザー

デプロイメントに素早くプッシュできるように、Prisma Access Agentsの設定をグループ化するスニペットを作成できる。スニペットを使用すると、一連のプロジェクトベースのデプロイメントの共通の基本設定を標準化できます。これにより、既知の良好な設定で新しいデバイスをすばやくオンボーディングでき、新しいデバイスのオンボーディングに必要な時間を短縮できます。

スニペットを作成したら、スニペットをスコープに関連付け、ユーザーをスコープに割り当て、そのユーザーにプロジェクト管理者ロールを付与します。その後、ユーザーはプロジェクト管理者としてログインし、スニペットを使用してPrisma Access Agentのプロジェクト設定を管理することができます。プロジェクト管理者は、自分が割り当てられているスニペットのPrisma Access Agent設定のみを変更できます。

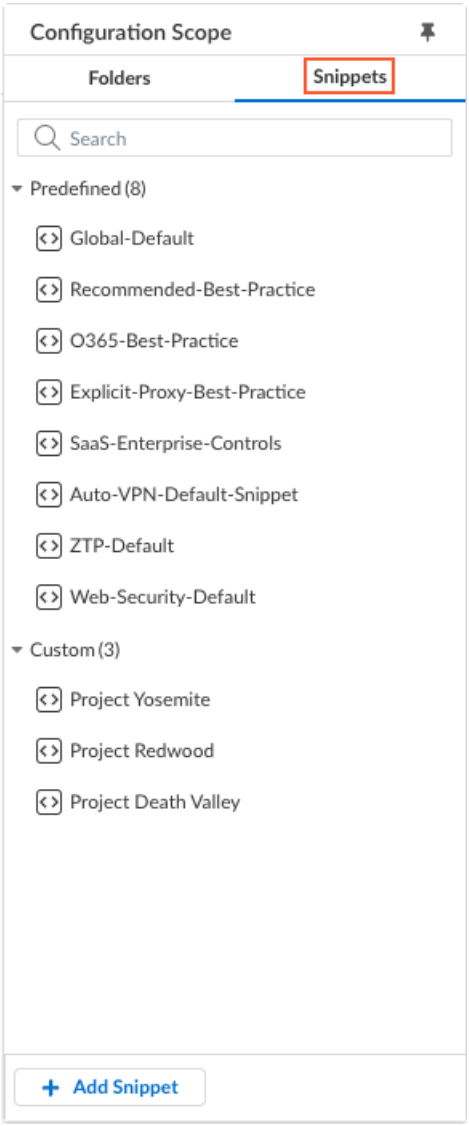
スニペットを作成するには、次の手順を実行します。

STEP 1 | スーパーユーザーとしてStrata Cloud Managerにログインします。

STEP 2 | **[Manage (管理)]** > **[Configuration (設定)]** > **[NGFWとPrisma Access)]**を選択します。

©2025 Palo Alto Networks, Inc.

STEP 3 | [概要]を選択し、[構成範囲]を展開してスニペットを表示します。



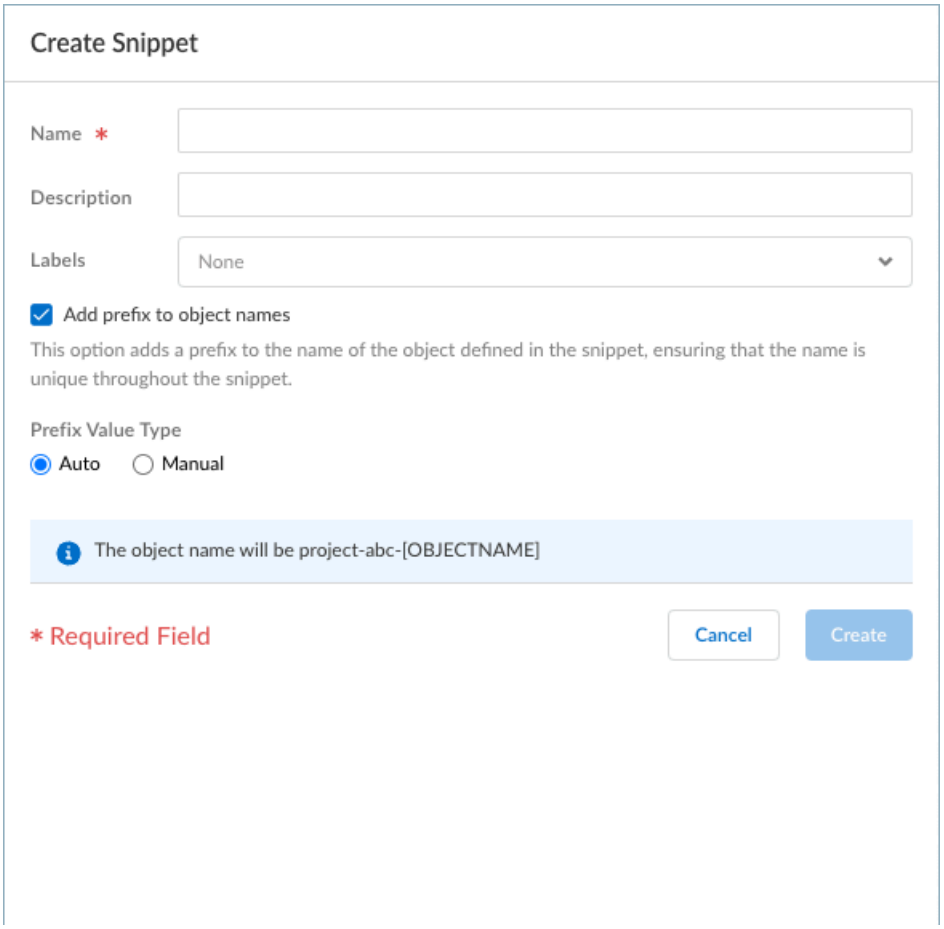
©2025 Palo Alto Networks, Inc.

STEP 4 | スニペットを追加し、次の詳細を入力します。

1. スニペットの名前を入力します。
2. （任意）スニペットの**Description**（説明）を入力します。
3. （任意）必要に応じて、1つ以上の**Labels (**ラベル**)**を割り当てます。

   既存のラベルを選択するか、作成したいラベルを入力して新しいラベルを作成できます。
4. オブジェクト名がスニペット全体で一意になるように、オブジェクト名にプレフィックスを追加します。 **[Add prefix to object name (**接頭辞をオブジェクト名に追加**)]** はデフォルトで有効になっています。

   ランダムなプレフィックスを自動生成するか、[手動]を選択して独自のプレフィックス値を追加するかを選択します。プレフィックス値は英数字で、最大6文字です。



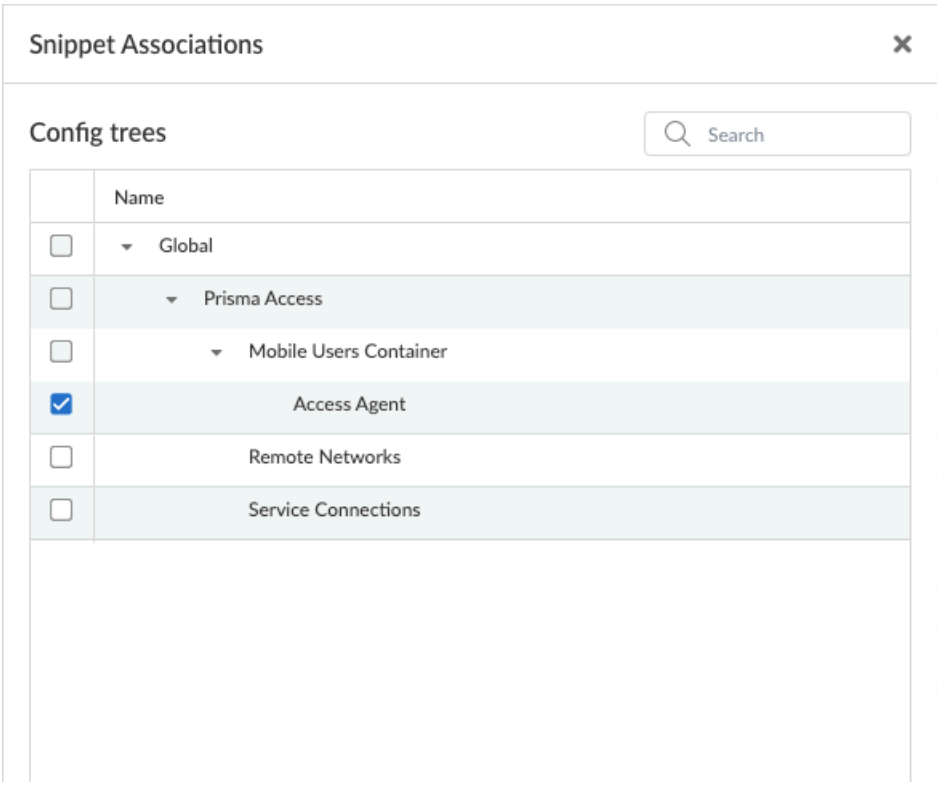
   プレフィックスは **xxxxxx**-という形式になります。オブジェクトを追加すると、Strata Cloud Managerはオブジェクト名にプレフィックスを事前に入力します。
5. スニペットを作成します。

   スニペットを作成すると、そのスニペットの設定スコープに入ります。スニペットスコープ内で作成したすべての設定は、スニペットに対してのみ適用されます。

©2025 Palo Alto Networks, Inc.

STEP 5 | スニペットを **Access Agent** フォルダーに関連付けます。

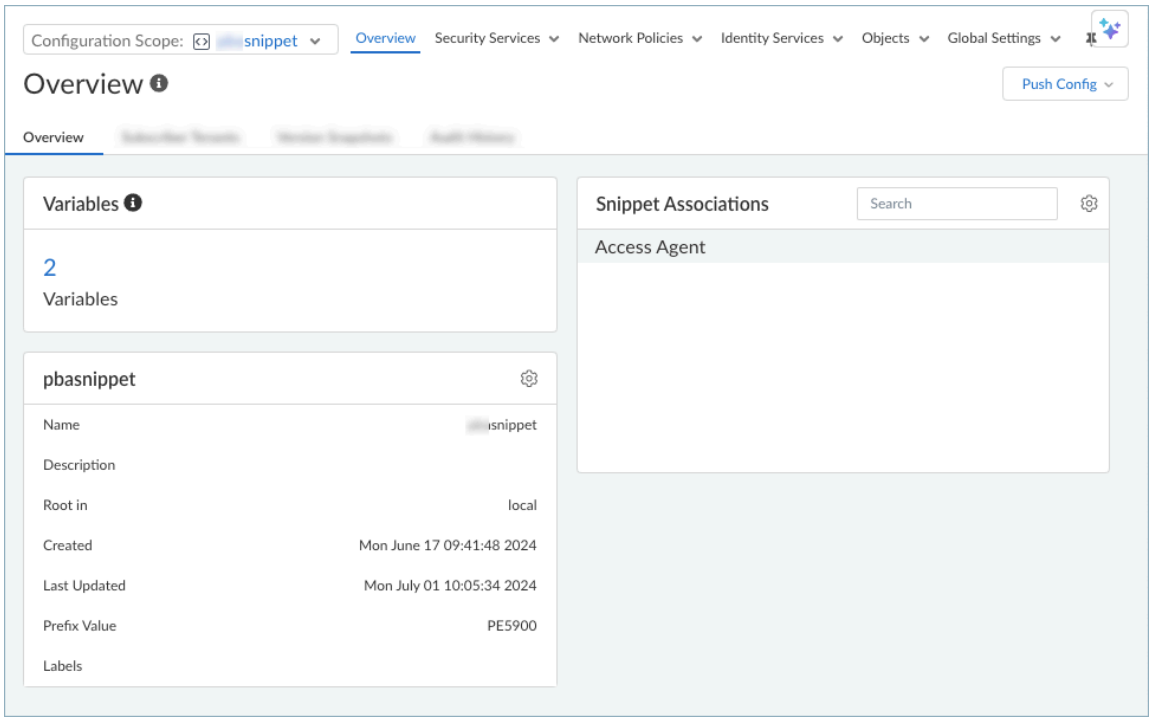
1. スニペットの「概要」ページで、**[Snippet Associations (スニペットの関連付け)]**設定を選択します。
2. 設定ツリーから**[Access Agent (アクセスエージェント)]**選択します。



3. **[X]** をクリックして [Snippet Associations (スニペットの関連付け)] ウィンドウを閉じます。

   Access Agentが[Snippet Associations (スニペットの関連付け)]のリストに表示されます。

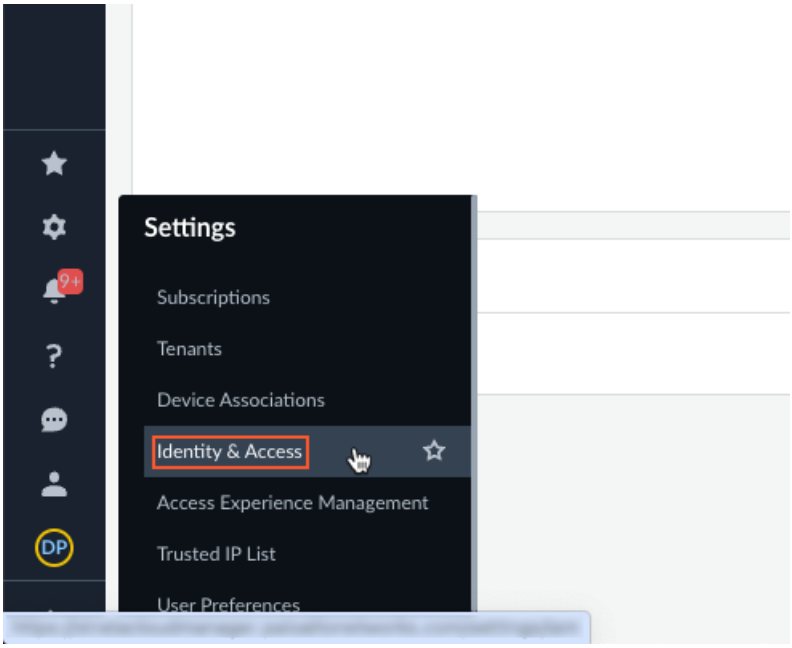
©2025 Palo Alto Networks, Inc.



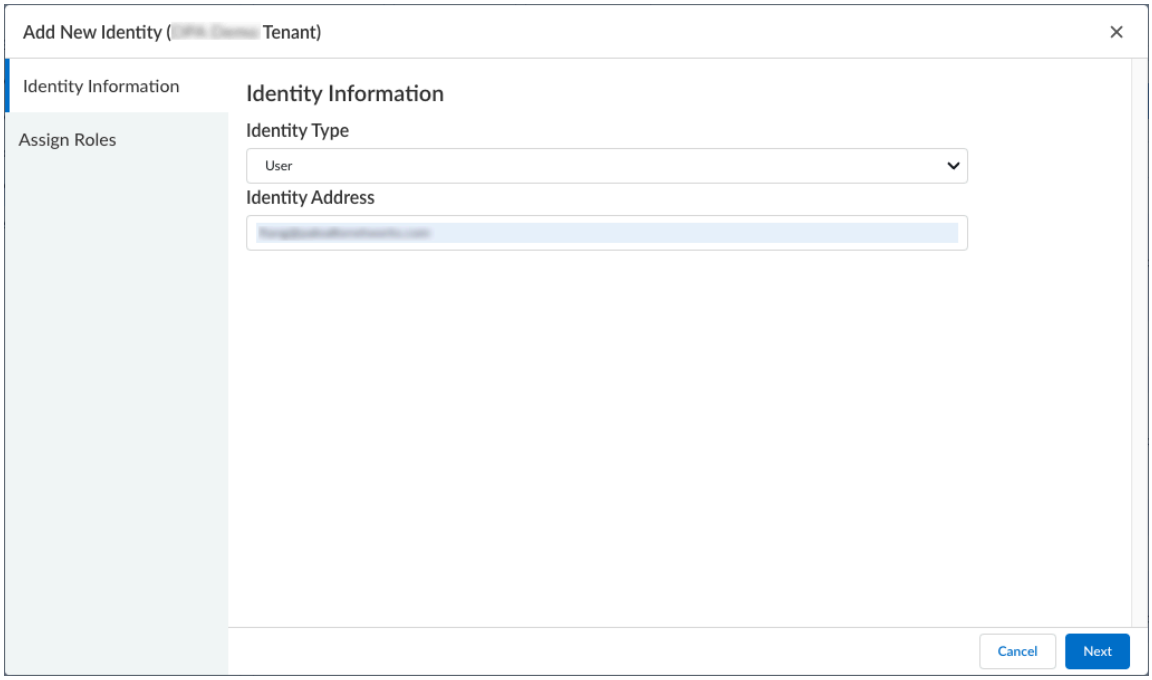
©2025 Palo Alto Networks, Inc.

STEP 6 | まだ行っていない場合は、プロジェクトを管理するユーザーのIDを作成し、そのユーザーにプロジェクト管理者プッシュロールを割り当てます。

1. Strata クラウドマネージャーから、[設定] > [ID とアクセス] を選択します。

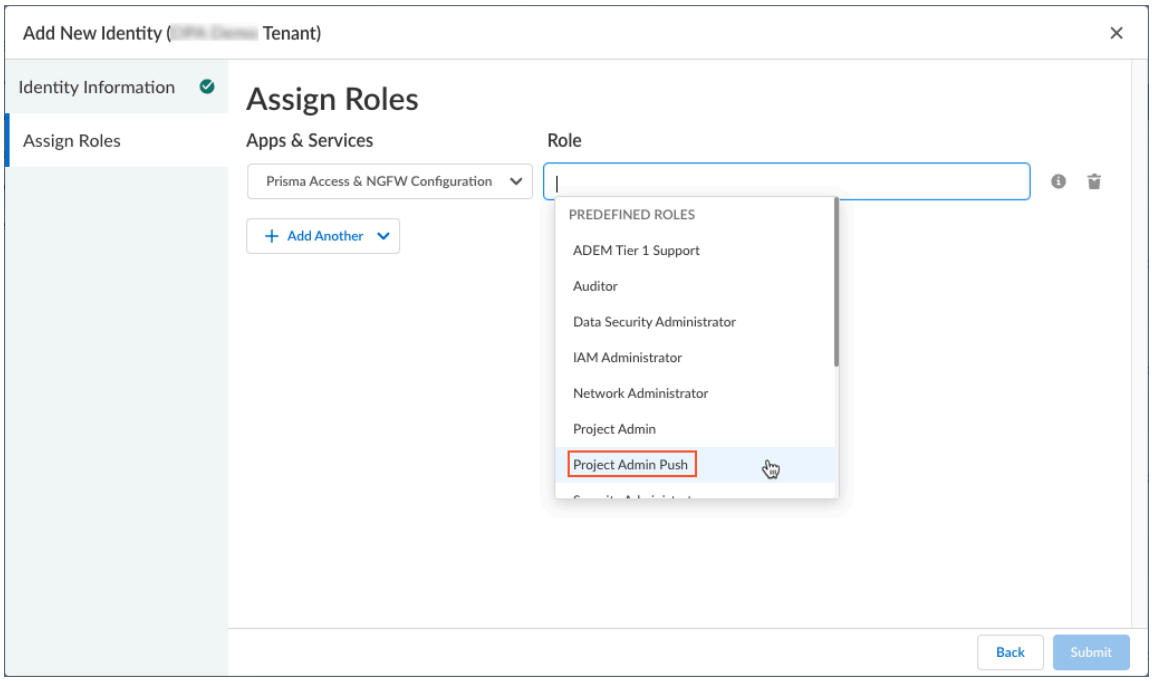


2. [ID を追加]を選択します。
3. プロジェクト管理者になるユーザーの **ID** アドレスを入力し、[次へ] をクリックします。



4. **[Add Access (アクセスを追加)] > [Prisma Access & NGFW設定]を選択し、Project Admin Push (プロジェクト管理者プッシュ)** ロールをユーザーに選択します。

©2025 Palo Alto Networks, Inc.



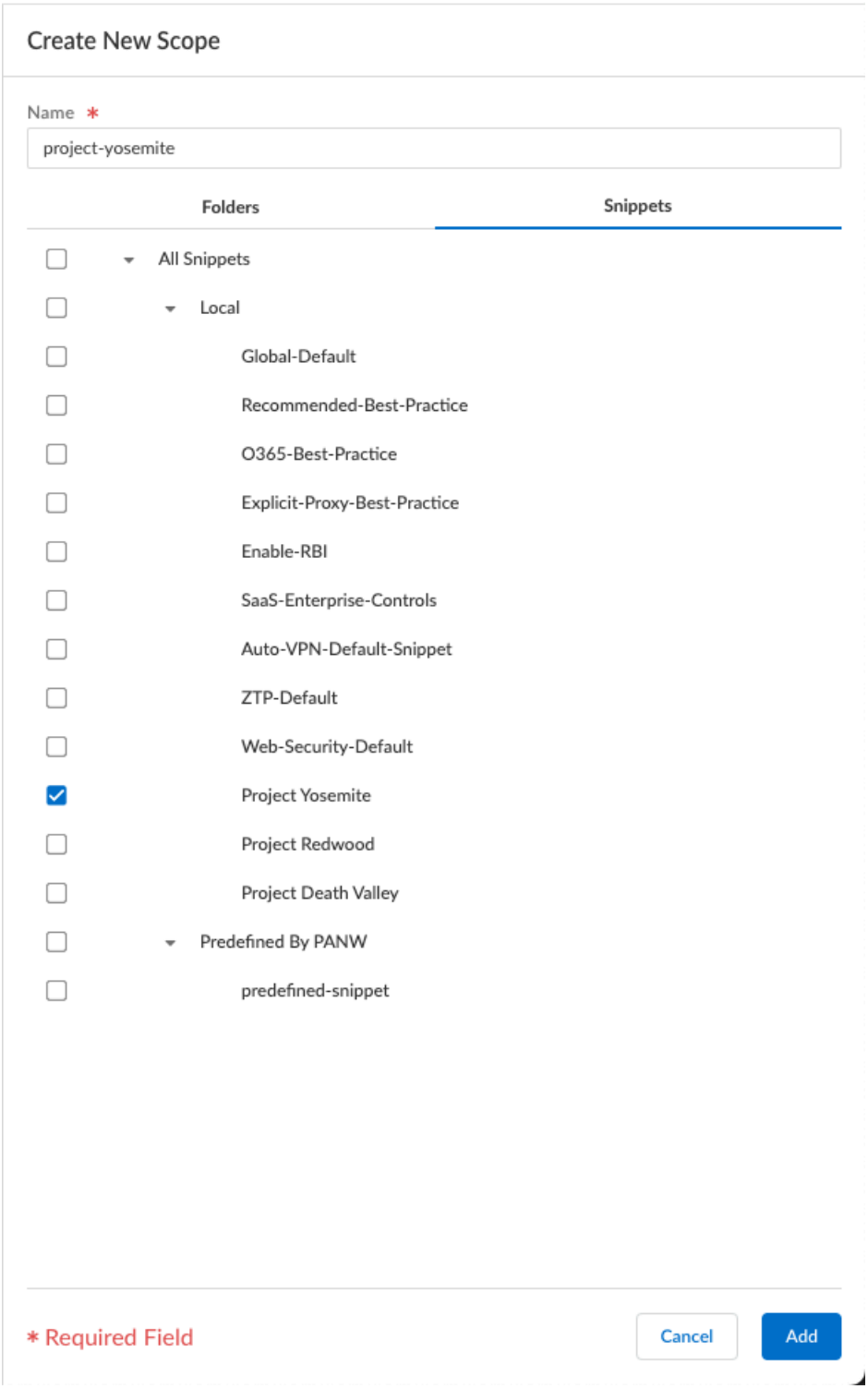
5. **Submit**（送信）をクリックします。

©2025 Palo Alto Networks, Inc.

STEP 7 | スニペットの管理スコープを作成し、ユーザーをそのスコープに割り当てます。

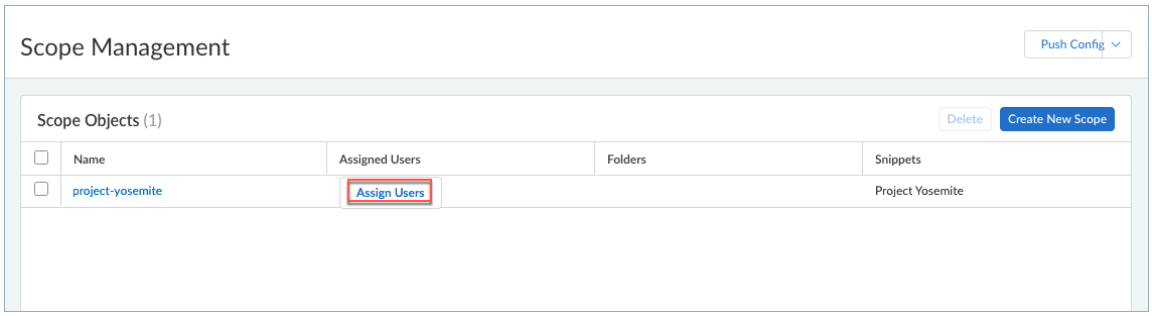
1. **[Manage (管理)]** > **[Access Control (アクセス制御)]** > **[Scope Management (スコープ管理)]**を選択します。
2. 新しいスコープを作成します。
3. スコープの名前を入力し、スニペットを表示します。
4. スニペットをスコープに関連付けます。作成したスニペットを選択し、追加します。

©2025 Palo Alto Networks, Inc.

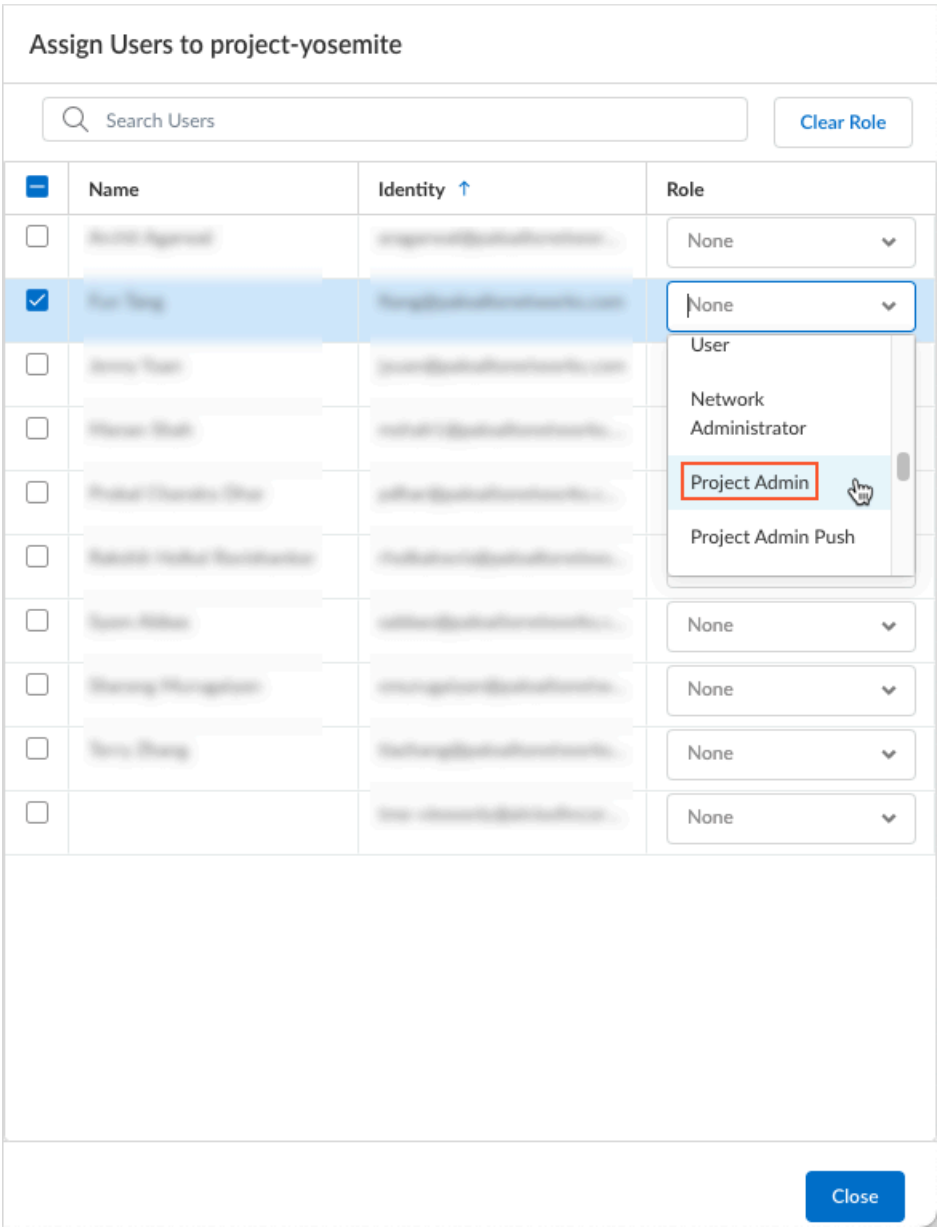


5. スコープオブジェクトで、スニペット用に作成したスコープにユーザーを割り当てます。

 ©2025 Palo Alto Networks, Inc.



6. ユーザーをスコープに割り当てるには、リストからユーザーを選択し、そのユーザーにプロジェクト管理者のロールを付与します。



7. **Close** the window.
8. 設定をプッシュします。

©2025 Palo Alto Networks, Inc.

1. **[Manage (管理)]** > **[Operations (オペレーション)]** > **[Push Config (設定をプッシュ)]**を選択します。
2. **[All Admins (すべての管理者)]** [admin scope (管理者範囲)] を選択し、 **[Push Config (設定をプッシュ)]** > **[Push (プッシュ)]**を選択します。

プッシュ設定操作が完了すると、スニペットが作成され、ロールがスニペットに関連付けられます。

割り当てられたユーザ（プロジェクト管理者）は、Strata Cloud Managerにログインし、作成したスニペットを使用してプロジェクト固有のPrisma Access Agent設定を行うことができます。ユーザーは、割り当てられていない他のスコープを表示することはできますが、設定の変更などの操作はできません。

©2025 Palo Alto Networks, Inc.

プロジェクト固有のPrisma Access Agent設定を設定する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ モバイルユーザーサブスクリプション付きのPrisma Accessライセンス ❑ MacOS 12以降のデスクトップデバイスまたはWindows 10バージョン2024以降またはWindows 11デスクトップデバイス ❑ ロール:プロジェクト管理者

スーパーユーザ管理者がインフラをセットアップし、スニペットを作成し、スニペットを自分に割り当てた後、プロジェクト管理者としてログインすることで、Prisma Access Agentを使用してプロジェクトにログインする際にエンドポイントに割り当てられるプライベートIP、スプリット トンネル、DNS情報など、プロジェクト固有のPrisma Access Agents設定を設定することができます。

1つまたは複数のPrisma Access Agentsに対してプロジェクト固有の設定を作成することも、デフォルトのエージェ ント設定を使用することもできます。管理するプロジェクトごとに異なるエージェントを使用することも、複数のプロジェクトでエージェントを共有することもできます。

動的権限アクセスエージェントのエージェントトラフィックを管理するための転送プロファイルを設定する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ モバイルユーザーサブスクリプション付きのPrisma Accessライセンス ❑ MacOS 12以降のデスクトップデバイスまたはWindows 10バージョン2024以降またはWindows 11デスクトップデバイス ❑ ロール:プロジェクト管理者

転送プロファイルは、 スプリット トンネル設定のセットアップやトンネル接続外のトラフィックの管理など、トラフィック転送ルールとトラフィック適用を構成および管理するための単一の画面を提供します。転送プロファイルは、他のモバイル アクセス エージェントで発生するトラフィック ポリシーの断片的な構成を改善し、構成できるルールとエントリの数の制限を大

 ©2025 Palo Alto Networks, Inc.

幅に拡張します。関連する構成を簡素化し、明確さを向上させることで、エンドポイント トラフィックをどのようにルーティングおよび適用するかに集中できます。

転送プロファイルは、複数の論理的かつ順序付けられたセクションを含むプロファイル タイプです。これらのセクションでは、エージェントが接続をどのように制御するかを決定する前に、接続が通過するさまざまなフェーズについて説明します。この組織構造により、各セクションの順序付けられたエントリを表示することで、トラフィックが特定の方法でルーティングされる理由を理解するのに役立ちます。各セクション内で、エントリを追加、編集、削除、または並べ替えることができます。

転送プロファイルを設定したら、エージェント設定ページでユーザーまたはユーザー グループに割り当てることができます。

トラフィック転送ルールは、転送プロファイルの上から下に適用されます。したがって、最も具体的なルールを最初に設定し、最も具体的でないルールを最後に設定するなど、転送プロファイルをトップダウン方式で設定します。

転送ルール

転送プロファイルは、送信元アプリケーションまたは宛先ドメインと宛先IPアドレスのトラフィックがトンネルを通過するかトンネル外を通過するか、DNSトラフィックを分割するかどうか、および有効なトラフィック適用を指定する一連のトラフィック転送ルールで構成されます。ルールに一致するトラフィックは、トラフィック転送仕様に従ってPrisma Accessに転送されます。転送ルールの仕様は、次のセクションに分かれています。

- ソースアプリケーション – ルールが適用されるプライベートアプリまたはSaaSアプリを指定します。エンドポイントからのトラフィックがソース アプリと一致する場合、トラフィックは転送ルールに従ってルーティングされます。
- 宛先- ルールが適用されるドメインとIPアドレスを指定します。トラフィックが宛先(FQDNまたはIPアドレスとして指定) と一致すると、トラフィックは転送ルールに従ってルーティングされます。

トラフィックの適用

各転送プロファイルには、次のことを可能にするトラフィック強制設定も含まれています。

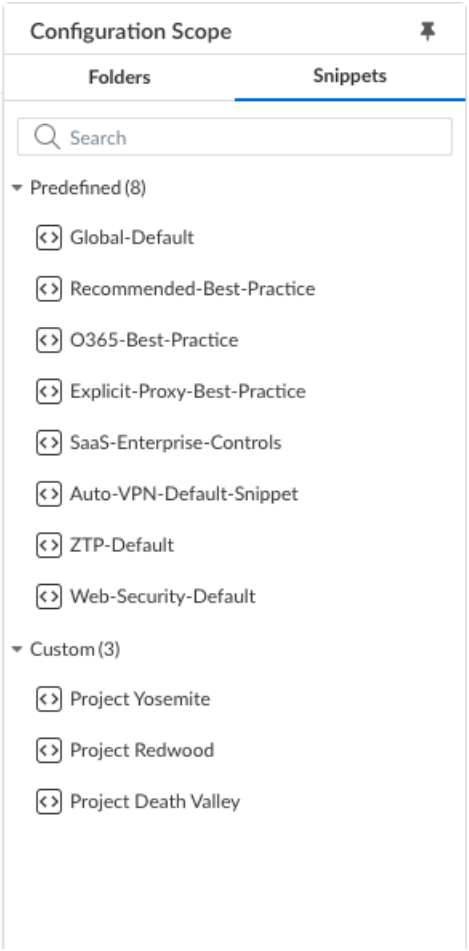
- 転送ルールに一致しないすべてのアウトバウンド トラフィックをブロックします
- エージェントがトンネルに接続されている場合 は、送信 LAN アクセスをブロックします
- エージェントがトンネルに接続されている場合は、受信アクセスをブロックします

転送プロファイルを構成するには、次の手順を実行します。

STEP 1 | プロジェクト管理者としてStrata Cloud Managerにログインします。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | **[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access] > [Overview (概要)]**を選択し、設定スコープを展開して**[Snippets (スニペット)]**を表示します。

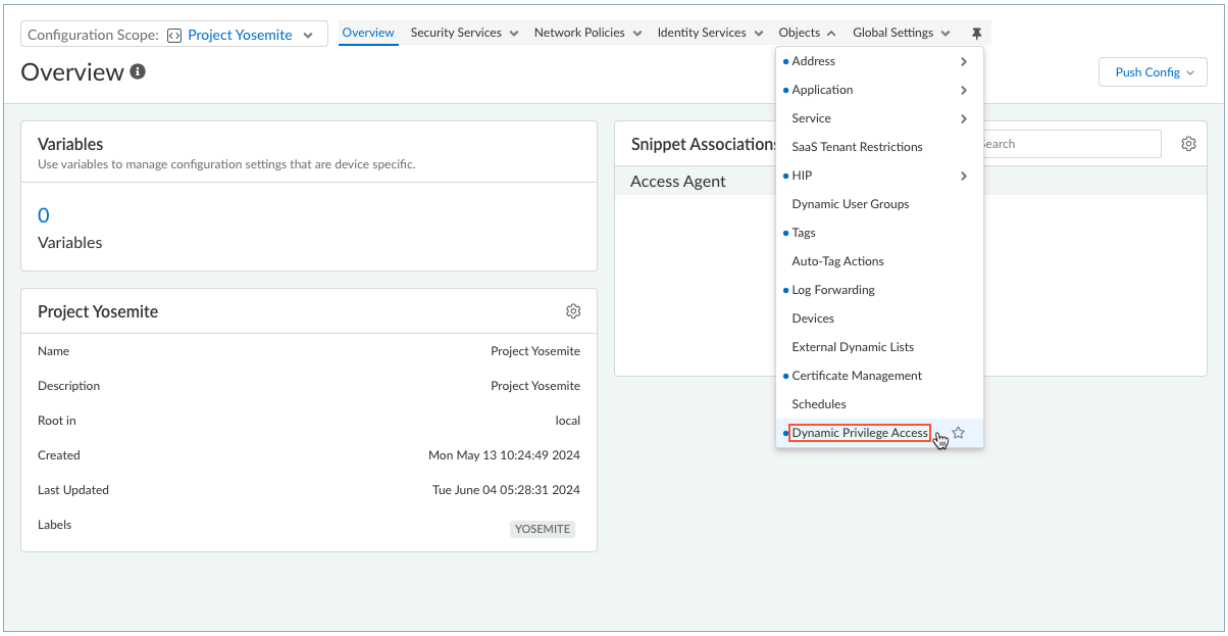


STEP 3 | スーパーユーザー管理者から割り当てられたスニペットを選択します。

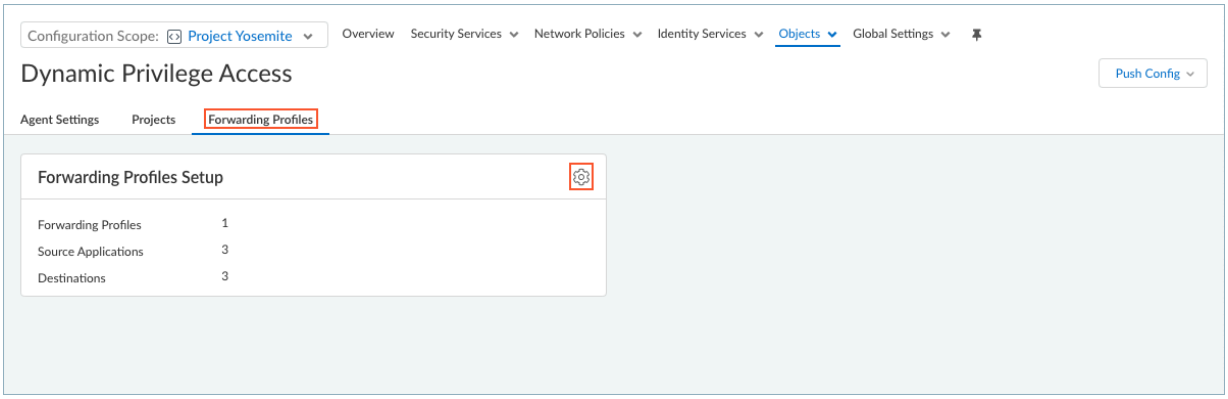
自分に割り当てられていないスニペットを表示することもできますが、設定の変更など、スニペットを操作することはできません。

 ©2025 Palo Alto Networks, Inc.

STEP 4 | [オブジェクト] > [動的権限アクセス] を選択して、動的権限アクセス設定を開きます。



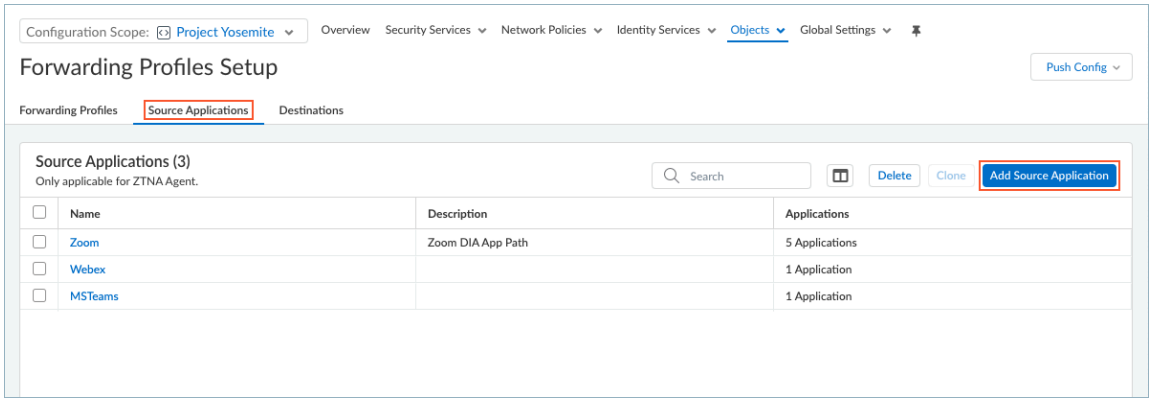
STEP 5 | 転送プロファイル を選択し、 転送プロファイルの設定を編集します。



 ©2025 Palo Alto Networks, Inc.

STEP 6 | SaaSまたはパブリック クラウド アプリケーション名に基づいて分割トンネルを作成する場合は、ソース アプリケーションを設定します。

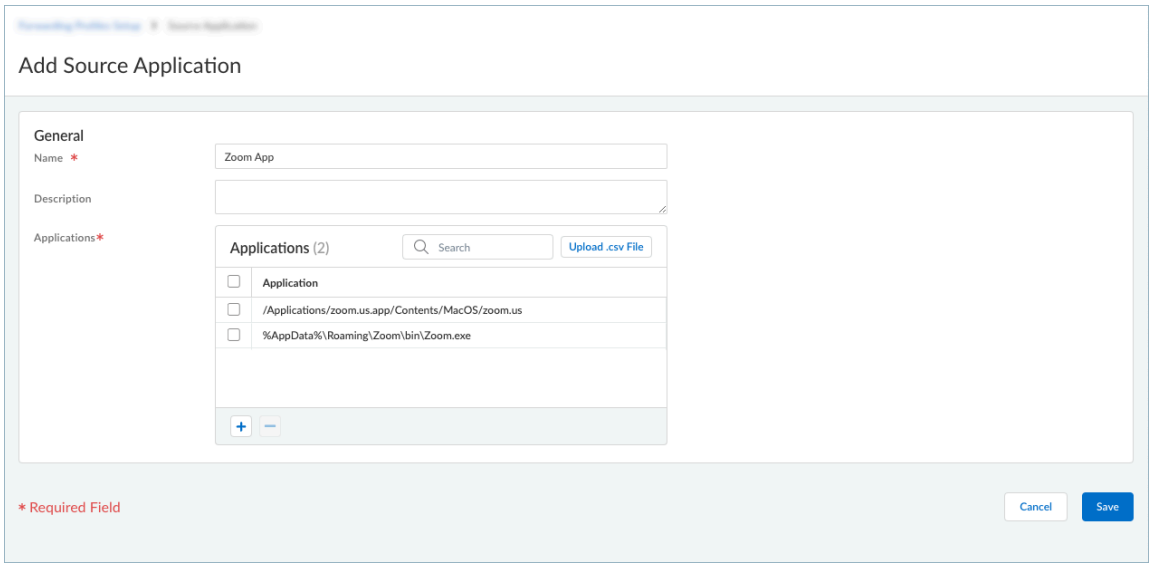
1. 転送プロファイルの設定ページで、ソースアプリケーションを選択し、 > ソースアプリケーションの追加を選択します。



2. 追加するアプリケーションに意味のある名前を入力します。
3. アプリケーション テーブルで+をクリックし、アプリケーションの完全なパスを入力します。1つ以上のアプリケーションを追加して、トンネル内のアプリケーション トラフィックを除外するか含めるかを管理できます。

   アプリケーション トラフィックを除外することを選択した場合 (転送ルールで直接接続を選択)、これらのアプリケーションからのトラフィックは、トンネル (仮想アダプタ) ではなく、エンドポイント上の物理アダプタを介して送信されます。

   アプリケーション トラフィックを含めることを選択した場合 (転送ルールでトンネル接続を選択)、除外トラフィック基準を満たしている場合でも、これらのアプリケーションからのトラフィックはPrisma Accessにルーティングされます。



   たとえば、Zoomアプリケーションからのトラフィックを管理するには、次の完全なパスを追加します。

   - Windowsエンドポイント: **%AppData%\Roaming\Zoom\bin\Zoom.exe**

 ©2025 Palo Alto Networks, Inc.

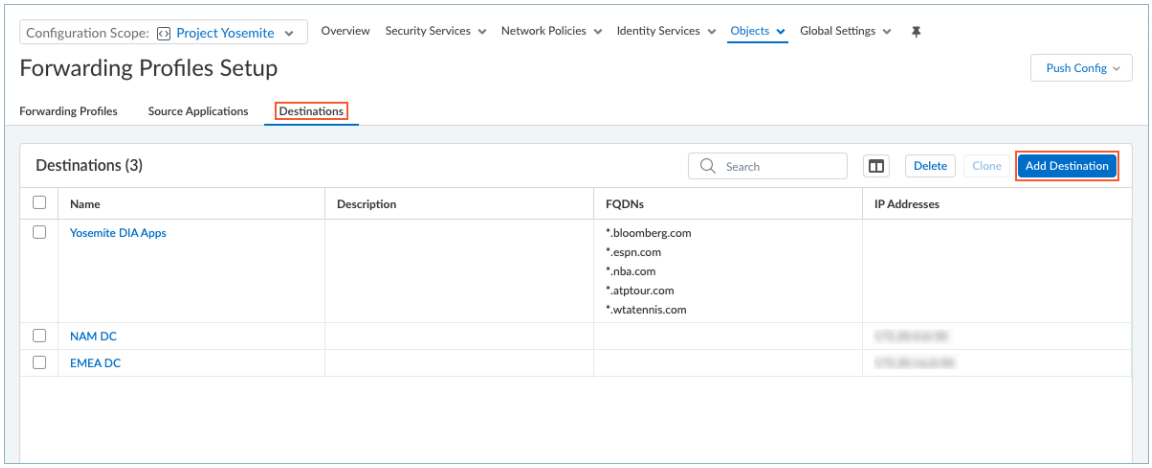
- MacOSエンドポイント: **/Applications/zoom.us.app/Contents/MacOS/zoom.us**

アプリケーションのリストがカンマ区切り値形式 (.csv) のテキスト ファイルにある場合は、**.csv**ファイルをアップロードできます。

4. ソースアプリケーションを保存します 。
5. ソース アプリケーションをさらに追加するには、これらの手順を繰り返します。

STEP 7 | 宛先ドメインまたはアクセス ルートに基づいて分割トンネルを作成する場合は、宛先を設定します。

1. 転送プロファイルの設定ページで、 宛先 > 宛先の追加を選択します。



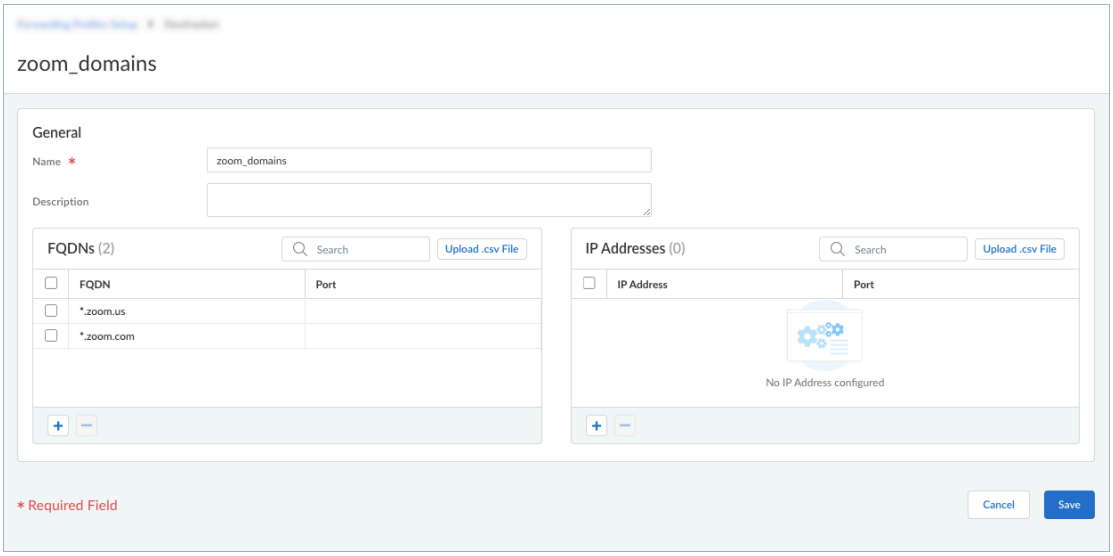
2. 追加する宛先に意味のある名前を入力します。
3. ドメイン名、アクセス ルート、またはその両方を指定して宛先を追加します。
   - 宛先ドメインを追加するには、**FQDN**テーブルで**+**をクリックし、宛先ドメインのFQDNを入力します。オプションでポートを追加できます。ポートを指定しない

©2025 Palo Alto Networks, Inc.

場合は、指定されたドメインのすべてのポートが転送ルールの対象となります。トラフィック管理用に1つ以上のドメインを追加できます。

ドメイン名に基づいてトラフィックを除外することを選択した場合 (転送ルールで直接接続を選択)、ドメインからのトラフィックは、トンネル (仮想アダプタ) ではなく、エンドポイントの物理アダプタを介して送信されます。

ドメイン名に基づいてトラフィックを含めることを選択した場合 (転送ルールでトンネル接続を選択)、ドメインからのトラフィックは、除外トラフィック基準を満たしていてもPrisma Accessにルーティングされます。



- アクセス ルートを追加するには、**IP** アドレステーブルで**+**をクリックし、宛先サブネットを入力します。トラフィック管理のために1つ以上のアクセス ルートを追加できます。

  IP アドレスにワイルドカード文字を含めないでください。転送プロファイルでは、*IP*アドレスのワイルドカードはサポートされていません。

  ルートまたはアプリケーションを含めたり除外したりしない場合は、すべてのリクエストがトンネルを介してルーティングされます (分割トンネルなし)。また、ユーザーがPrisma Accessに接続するたびに、すべてのトラフィックが検査され、ポリシーが適用されます。

  アクセス ルートを除外するようにスプリット トンネル トラフィックを定義すると (転送ルールで直接接続を選択)、これらのルートは仮想アダプタ (トンネル) 経由でトンネル経由で送信されるのではなく、エンドポイントの物理アダプタ経由で送信されます。アクセス ルートによってスプリット トンネル トラフィックを除外することで、遅延の影響を受けやすいトラフィックや高帯域幅のトラフィックをトンネルの外部に送信し、その他のすべてのトラフィックをトンネル経由でルーティングして、Prisma Accessゲートウェイによる検査とポリシーの適用を行うことができます。

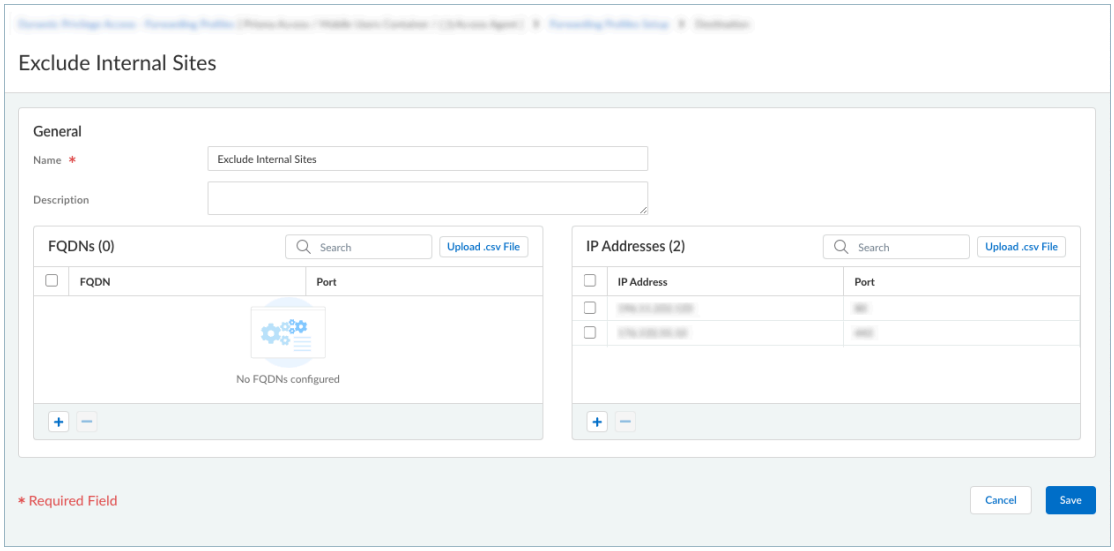
  アクセス ルートを含めるようにスプリット トンネル トラフィックを定義すると (転送ルールで トンネル 接続を選択)、Prisma Accessゲートウェイはこれらのルートを

©2025 Palo Alto Networks, Inc.

リモート ユーザーのエンドポイントにプッシュし、これらのエンドポイントがトンネル経由で送信できるトラフィックを指定します。

含まれるルートよりも具体的な除外ルートを指定します。そうしないと、意図したよりも多くのトラフィックが除外される可能性があります。

IPアドレスのリストが.csv形式のテキスト ファイルにある場合は、**.csv**ファイルをアップロードできます。

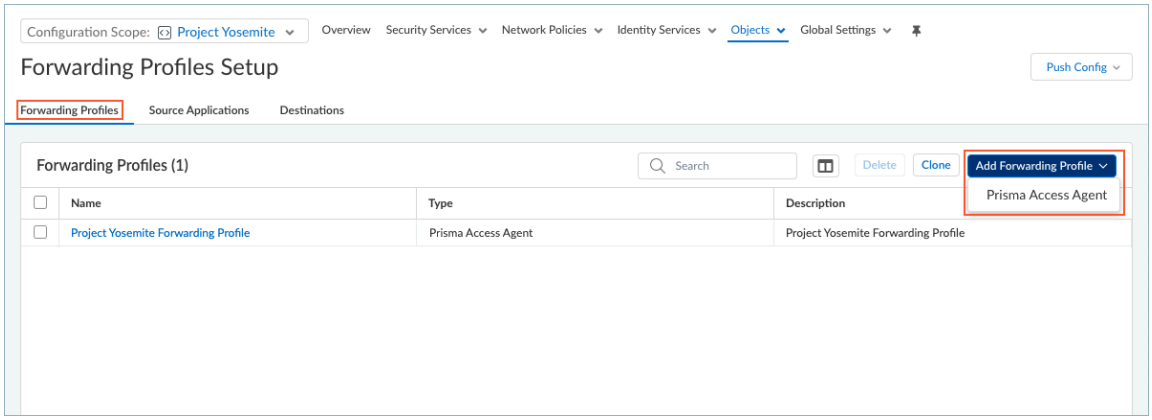


4. 目的地を保存します 。
5. 目的地をさらに追加するには、これらの手順を繰り返します。

©2025 Palo Alto Networks, Inc.

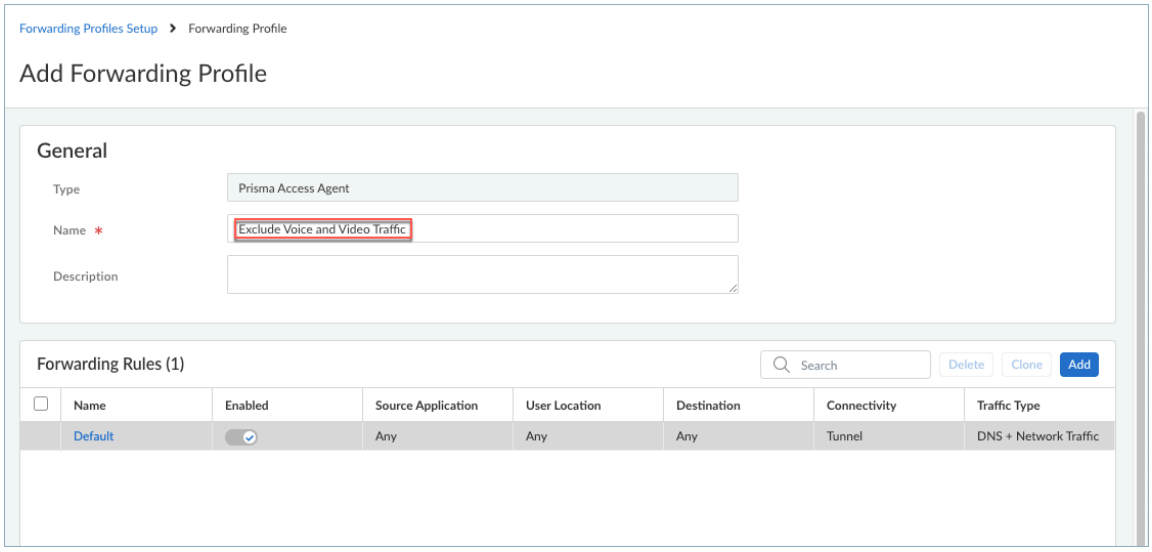
STEP 8 | 設定した送信元アプリケーションまたは宛先に基づいてトラフィックを許可または除外する転送プロファイルを作成します。

1. 転送プロファイルを追加するには、[転送 プロファイル] > [転送プロファイルの追加] > **Prisma Access Agent**を選択します。



転送プロファイルを編集するには、「転送プロファイル」テーブルでプロファイルの名前を選択します。

2. 転送プロファイルに意味のある 名前 を入力します。
3. 転送ルールを追加します 。

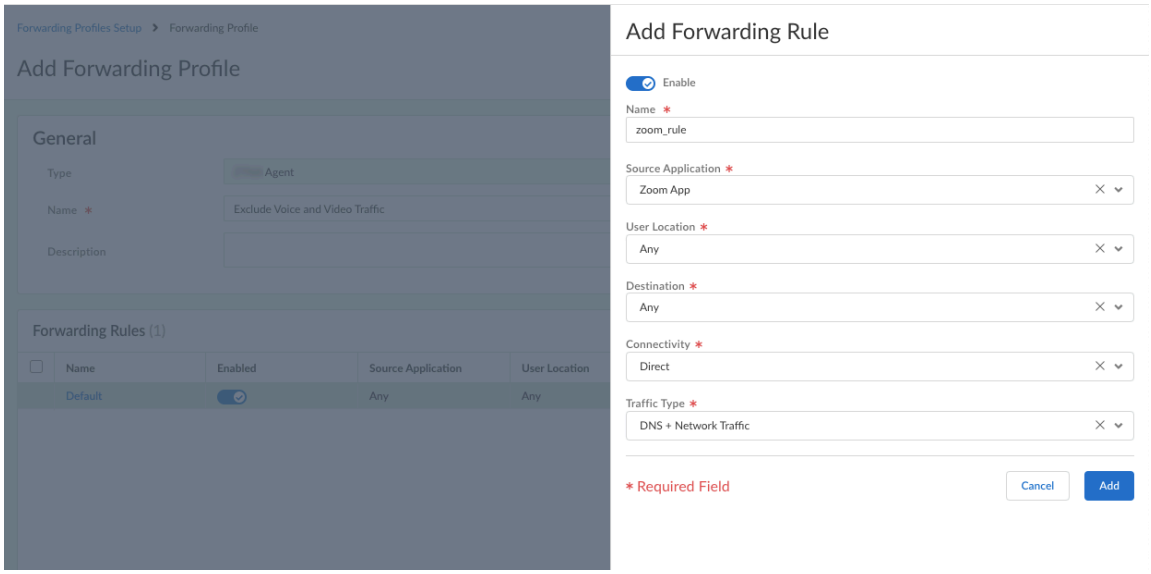


転送ルール テーブルには、転送プロファイルを構成するルールが表示されます。すべての転送プロファイルには、すべてのDNSおよびネットワーク トラフィックをトンネル経由で送信する デフォルトの転送ルールが含まれています。追加した新しいルール

 ©2025 Palo Alto Networks, Inc.

は、デフォルトのルールの上に配置されます。デフォルトの転送ルールを削除または移動することはできませんが、 接続 設定を変更することはできます。

4. 転送ルールの仕様を入力します。



1. ルールを **Enable** (有効) にします。
2. ルールの **Name** [名前] を入力します。
3. 以前に定義したソース アプリケーションを選択します。[任意]を選択した場合、転送ルールはすべてのソース アプリケーションからのトラフィックに適用されます。

   ルールは、指定されたソース アプリケーションによって接続が行われた場合にのみ一致します。
4. ユーザーロケーションを選択します。ユーザーの場所を設定していない場合、またはルールが任意のユーザーの場所に一致することを許可する場合は、[任意]を選択します。(動的権限アクセスが有効なエージェントには適用されません。)

   ルールは、エンドポイントが指定したユーザーの場所に接続されている場合にのみ一致します。
5. 以前に定義した宛先を選択します。[任意]を選択した場合、転送ルールは任意の宛先ドメインまたはIPアドレスからのトラフィックに適用されます。

   ルールは、接続先が指定された宛先ドメインまたはIPアドレスと一致する場合にのみ一致します。
6. 接続性を選択します:
   - 直接- トラフィックをトンネルの外部に送信します。選択されたアプリケーションまたは宛先のすべてのトラフィックは、検査なしでエンドポイントの物理アダプタに直接送信されます。
   - トンネル- トラフィックをトンネル経由で送信します。選択されたアプリケーションまたは宛先に送信されるすべてのトラフィックは、検査とポリシーの適用のためにトンネルを介してPrisma Accessに送信されます。
7. トラフィック タイプを選択:

 ©2025 Palo Alto Networks, Inc.

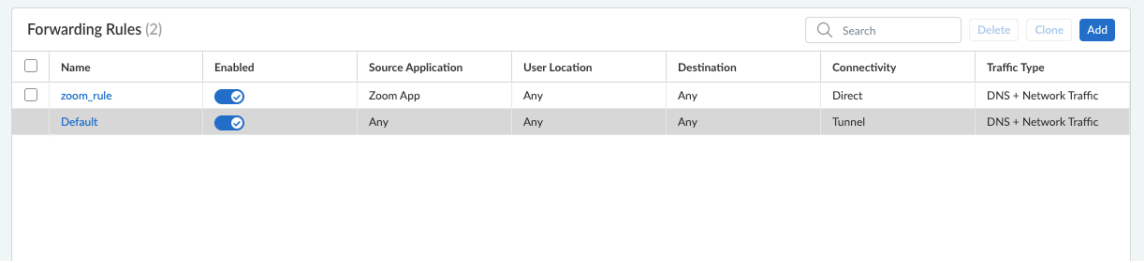
スプリットDNSを使用して、ユーザーがネットワーク トラフィックに加えて、アプリケーションやリソースに対するDNSクエリをトンネル経由で送信するか、トンネルの外部に送信できるようにするかどうかを指定します。

- **DNS+**ネットワーク トラフィック- 含めるか除外するか指定した宛先ドメインに基づく分割トンネルが、そのドメインのDNSトラフィックと関連するネットワーク アプリケーション トラフィックに適用されるようにします。
- ネットワーク トラフィック- DNSトラフィックには適用されず、ネットワーク アプリケーション トラフィックにのみ適用されるルールを含めるか除外します。すべてのDNSトラフィックは、含めるか除外するかを指定した宛先ドメインに基づいて、分割トンネルに関係なくトンネルを通過します。

*Windows*エージェントの場合、***DNS+***ネットワーク トラフィック 分割トンネル オプションは、アプリケーション ベースの分割トンネル ルールではサポートされません。アプリケーション名に基づいてトンネルからのトラフィックを含めるか除外するようにスプリット トンネリングを設定し、***[DNS+**ネットワーク トラフィック**]***を選択した場合、除外されたアプリと含められたアプリの*DNS*クエリ パケットはスプリット トンネル ルールに従いません。

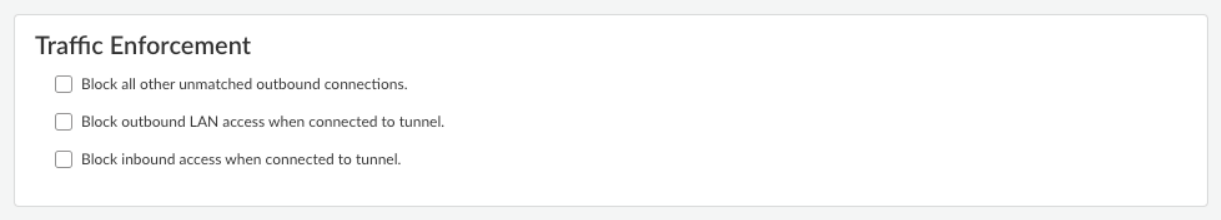
5. 転送ルールを追加します 。

   ルールが転送ルール テーブルに追加されます。転送プロファイルに複数のルールを追加できます。



 ©2025 Palo Alto Networks, Inc.

STEP 9 | トラフィック強制オプションを構成して、トラフィックを強制する方法を決定します。



これらのオプションは動的権限アクセスには推奨されないため、必ず すべての オプションの選択を解除して ください。

- その他の一致しないアウトバウンド接続をすべてブロックする- 有効にすると、どの転送ルールにも一致しないすべての接続がブロックされます。トラフィックはトンネル経由で送信されません。
- トンネルに接続しているときにアウトバウンド**LAN**アクセスをブロックする- 有効にすると、エージェントがトンネルに接続されているときにローカル ネットワークへの直接アクセスがブロックされます。

  ローカルネットワークへのアクセスをブロックすると、すべてのトラフィックがローカル アダプタに送信されないようになります。また、プリンタなどのローカルサブネット上のリソースにもアクセスできなくなります。アクセス ルート、宛先ドメイン、およびアプリケーションに基づく分割トンネル トラフィックは、引き続き期待どおりに機能します。

  このオプションを無効にすると、エンド ユーザーはPrisma Access Agentを使用してPrisma Accessに最初に接続しなくても、ローカル リソースにアクセスできるようになります。
- トンネルに接続したときにインバウンドアクセスをブロックする- 有効にすると、トンネルからのすべてのインバウンド接続がブロックされます。

STEP 10 | 転送プロファイルを保存します 。

STEP 11 | **[Push Config (設定のプッシュ)]** > を選択して設定を > プッシュします。このアクションにより、転送プロファイルがエージェント設定ページで選択できるようになります。

動的特権アクセスエージェントの転送プロファイル構成の確認とトラブルシューティング

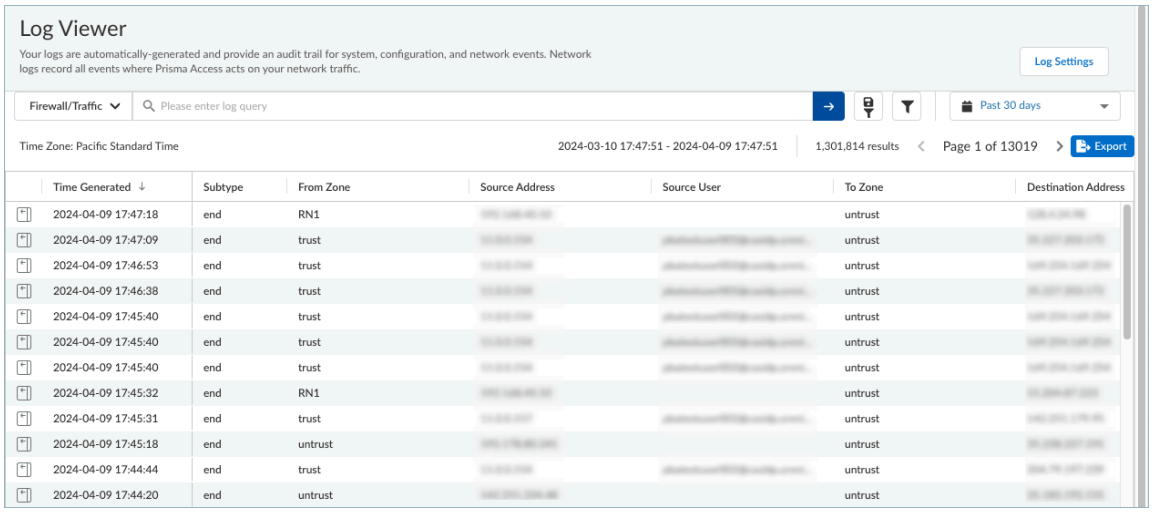
どこで使用できますか?	何が必要ですか?
• Prisma Access（Strata Cloud Managerによる管理）	❑ Prisma Access 5.1 優先またはイノベーション ❑ モバイルユーザーサブスクリプション付きのPrisma Accessライセンス ❑ MacOS 12以降のデスクトップデバイスまたはWindows 10バージョン2024以降またはWindows 11デスクトップデバイス ❑ ロール:スーパーユーザー

©2025 Palo Alto Networks, Inc.

転送プロファイルを設定した後、トラフィック ログ ファイルを表示して、トラフィックが意図したとおりに送信されているかどうかを確認できます。トラフィック ログは、Strata Cloud Managerログ ビューアで表示するか、エンドポイントでPrisma Accessコマンドライン ツール (PACli) を使用して表示できます。

Strata Cloud Managerログビューアからトラフィックログファイルを表示するには:

1. **[Incidents & Alerts (インシデントとアラート)]** > **[Log Viewer (ログ ビューアー)]**を選択します。
2. 詳細については、ファイアウォール/トラフィックログを参照してください。



 ©2025 Palo Alto Networks, Inc.

エンドポイントのトラフィック ログ ファイルを表示するには:

1. **Prisma Access Agent** > 管理でリモートシェル を起動するか、エンドユーザーのデバイスでWindowsコマンドプロンプトまたはMacOSターミナルウィンドウを開きます。
2. 転送プロファイルに転送ルールを表示するには、次のコマンドを発行します。
   - Windows の場合:

     ```
     "C:\Program Files\Palo Alto Networks\Prisma Access Agent
     \pacli" traffic show
     ```

   - MacOSの場合:

     ```
     /Applications/Prisma\ Access\ Agent.app/Contents/Helpers/
     pacli traffic show
     ```

   *PACli*ツール (*pacli*) の環境変数を設定している場合は、「***pacli traffic show***」と入力するだけです。



サンプルPACliコマンドライン出力には、転送ルールの優先順位を含む、転送プロファイルで有効な転送ルールを含むテーブルが表示されます。転送プロファイルのトラ

 ©2025 Palo Alto Networks, Inc.

フィック適用の選択肢も表示されます。この表は、転送プロファイルで設定した転送ルールに対応しています。

3. 転送ルールの詳細を表示するには、次のコマンドを発行します。

```
PACLIトラフィックは<number>を示します
```

ここで、**<number>**は優先順位欄の番号です。例:

```
[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. スプリットトンネルの問題をトラブルシューティングするには、トンネルの内部または外部にあるエージェントトラフィックを調べる必要がある場合があります。これを行うには、Prisma Access Agent接続ログを表示します。次のコマンドを発行します。

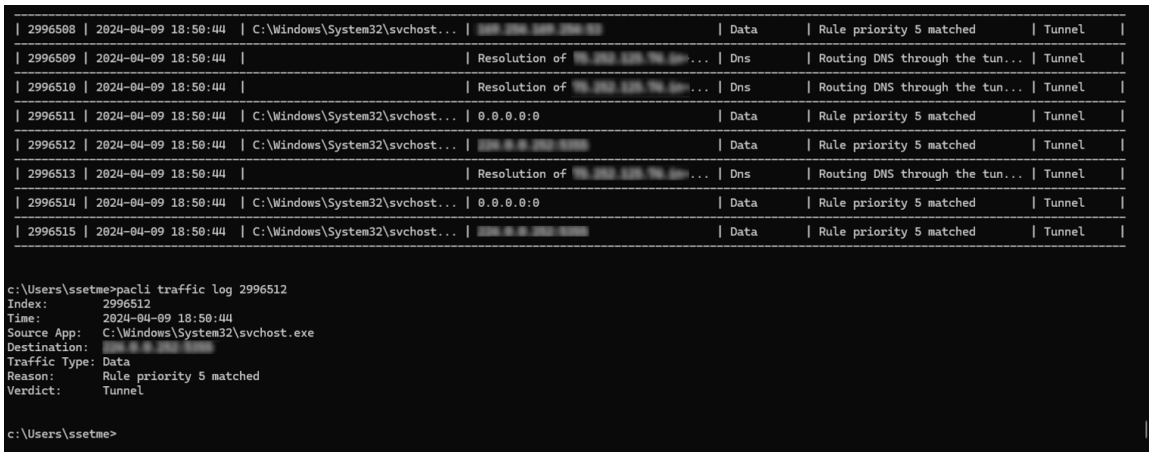
```
pacli traffic log
```

```
[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    |
```

個々のログエントリを表示するには、次のコマンドを発行します:

```
pacli traffic log<index>
```

ここで、**<index>**はエントリーのインデックス番号に対応しています。例：



また、次のコマンドを発行して、接続ログをファイルにエクスポートしてさらに分析することもできます:

```
pacli traffic log export <filename>
```

動的特権アクセスのためのPrisma Access Agentアプリケーション設定

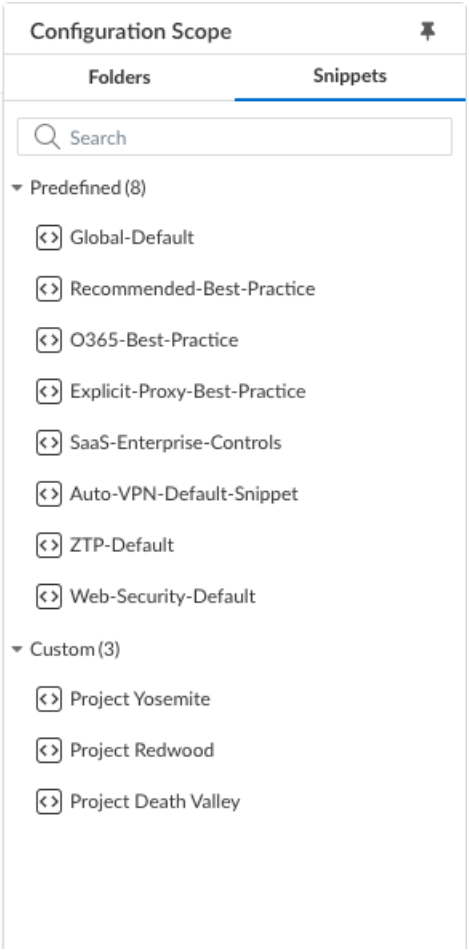
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ モバイルユーザーサブスクリプション付きのPrisma Accessライセンス ❑ MacOS 12以降のデスクトップデバイスまたはWindows 10バージョン2024以降またはWindows 11デスクトップデバイス ❑ ロール:プロジェクト管理者

Strata Cloud Managerには、すべてのプロジェクトのすべてのユーザーグループに適用されるデフォルトのPrisma Access Agentアプリ構成が用意されています。プロジェクト内のエンド ユーザーがPrisma Access Agentとどのようにやり取りするかをカスタマイズするために、アプリ構成を追加することができます。

STEP 1 | プロジェクト管理者としてStrata Cloud Managerにログインします。

©2025 Palo Alto Networks, Inc.

STEP 2 | **[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access] > [Overview (概要)]**を選択し、設定スコープを展開して**[Snippets (スニペット)]**を表示します。

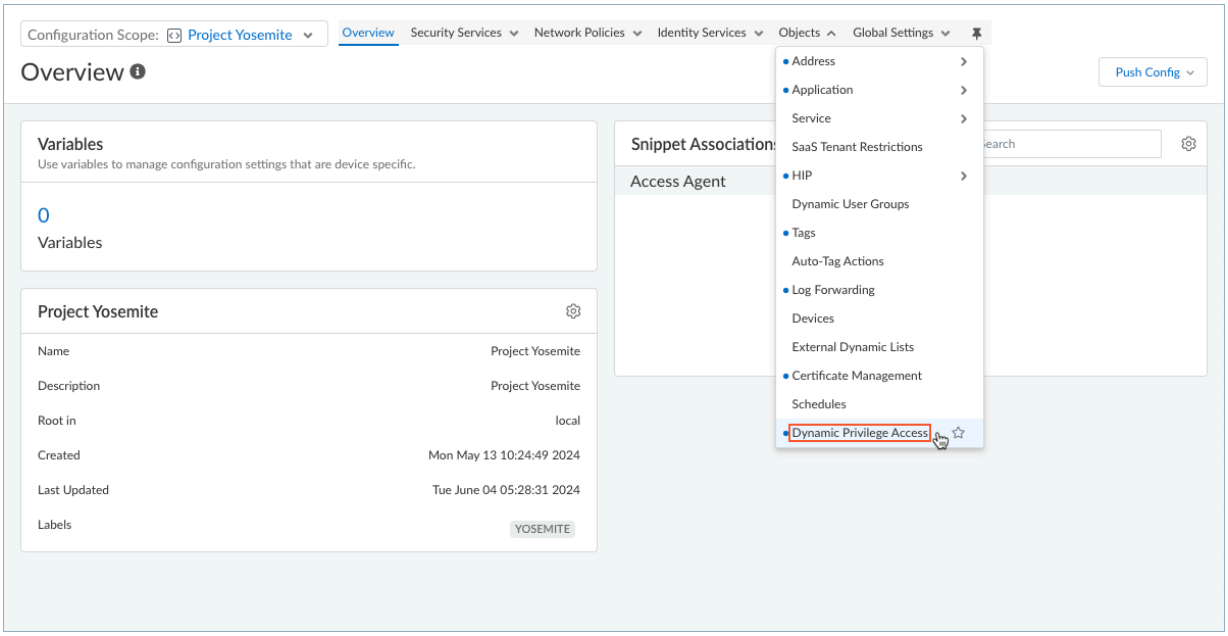


STEP 3 | スーパーユーザー管理者から割り当てられたスニペットを選択します。

自分に割り当てられていないスニペットを表示することもできますが、設定の変更など、スニペットを操作することはできません。

©2025 Palo Alto Networks, Inc.

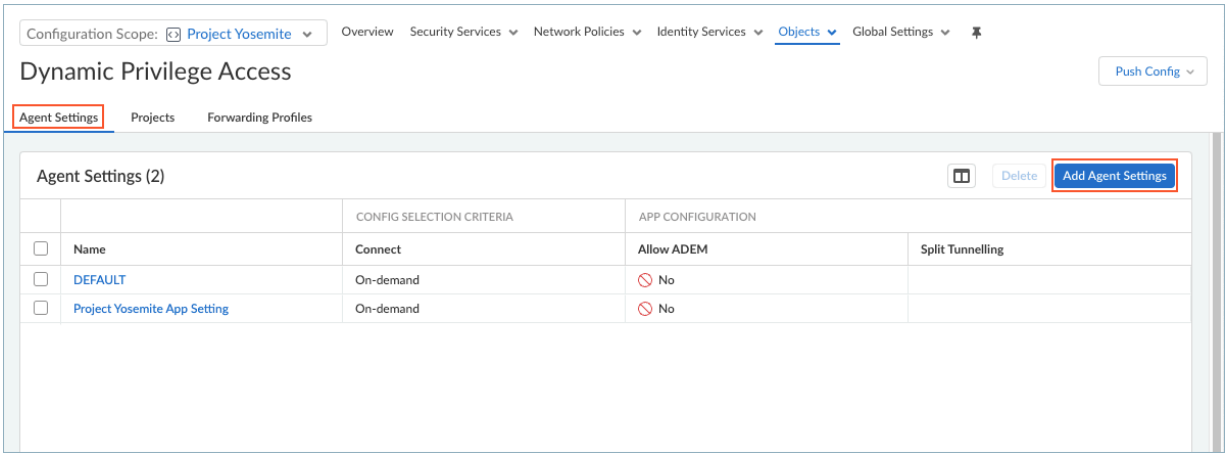
STEP 4 | [オブジェクト] > [動的権限アクセス] を選択して、動的権限アクセス設定を開きます。



STEP 5 | エージェント設定タブを選択します。

STEP 6 | Strata Cloud Managerはデフォルトのエージェント設定を提供します。デフォルト設定を使用したくない場合。[エージェント設定を追加]を選択します。

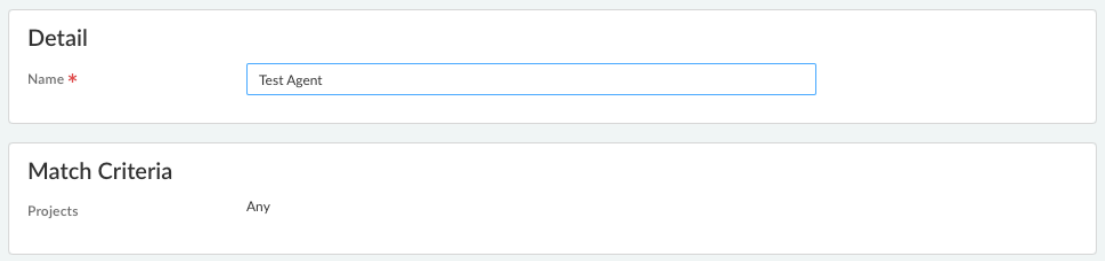
エージェントの設定を編集するには、テーブルからエージェント名を選択します。



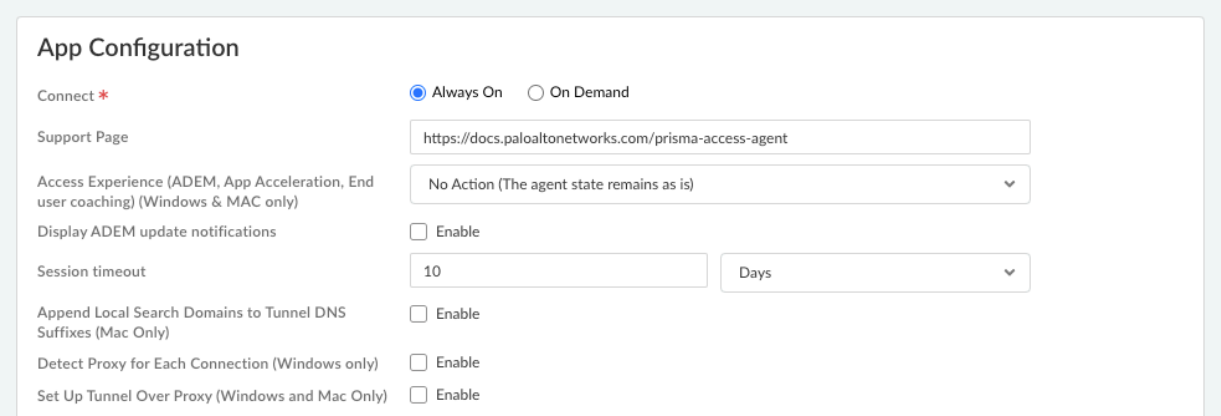
©2025 Palo Alto Networks, Inc.

STEP 7 | アプリの設定ルールを作成します。構成ルールは、1つ以上のプロジェクトを、それらのプロジェクトに固有の特定の設定に関連付けます。

1. ルールの **Name** [名前] を入力します。
2. プロジェクトを追加して 一致基準 を指定します。プロジェクトの条件に一致するユーザとグループは、Prisma Access Agentを使ってプロジェクトにログインすると、アプリの設定を受け取ります。
   - すべてのユーザーに設定を配布するには、プロジェクトを**Any (任意)**に設定します。
   - 特定のプロジェクトにログインするユーザーに構成を展開するには、[プロジェクト]を[プロジェクトの追加]に設定し、プロジェクトのリストから選択します。



STEP 8 | Prisma Access Agentのアプリ設定を構成します。



- 接続—Prisma Access AgentがPrisma Accessに接続する方法を指定します。この設定は必須です。
  - ユーザーがエンドポイントにログオンするたびに、Prisma Access Agentへの接続を自動的に確立するには、[常にオン]を選択します。
  - ユーザーが **Prisma Access Agent** の [接続 (ロックアイコン)] をクリックしたときにのみ **Prisma Access** に接続するには、[ユーザーが接続 (オンデマンド)] をクリックしたときのみ **Prisma Access** に接続します。
- サポート ページ- Prisma Access Agent でユーザーがサポート リソースをクリックしたときにアクセスできる Web サイトを入力します。

  Prisma Access Agentのドキュメント用のウェブサイトがデフォルトのサポートページです。
- **Access**エクスペリエンス（**ADEM**、アプリアクセラレーション、エンドユーザーコーチング）（**Windows**および**MAC**のみ）—Prisma Access Agentアプリのインストール中に自律

©2025 Palo Alto Networks, Inc.

型DEM（ADEM）エンドポイントエージェントをインストールするかどうかを指定し、エンドユーザーがアプリからユーザーエクスペリエンステストを有効または無効にできるようにします。

- インストール
- アクションなし(エージェント状態はそのまま)
- アンインストール

クラウド管理Prisma Accessで ADEM の概要について詳しくは、「自律型 DEM を使用して開始する」を参照してください。

- **ADEM**の更新通知を表示する–エンドポイントでアップデートが利用可能になったときにADEMからの通知を表示するには、この設定を有効にします。
- セッションタイムアウト - Prisma Access Agent ユーザーセッションは、ユーザーが Prisma Access ゲートウェイ (ロケーション) に接続し、正常に認証されると作成されます。セッションは、定義されたスプリットトンネルルールに基づいてトンネルするトラフィックを決定する特定のゲートウェイに割り当てられます。Prisma Access データプレーンの最小バージョンは 11.2 でなければなりません。

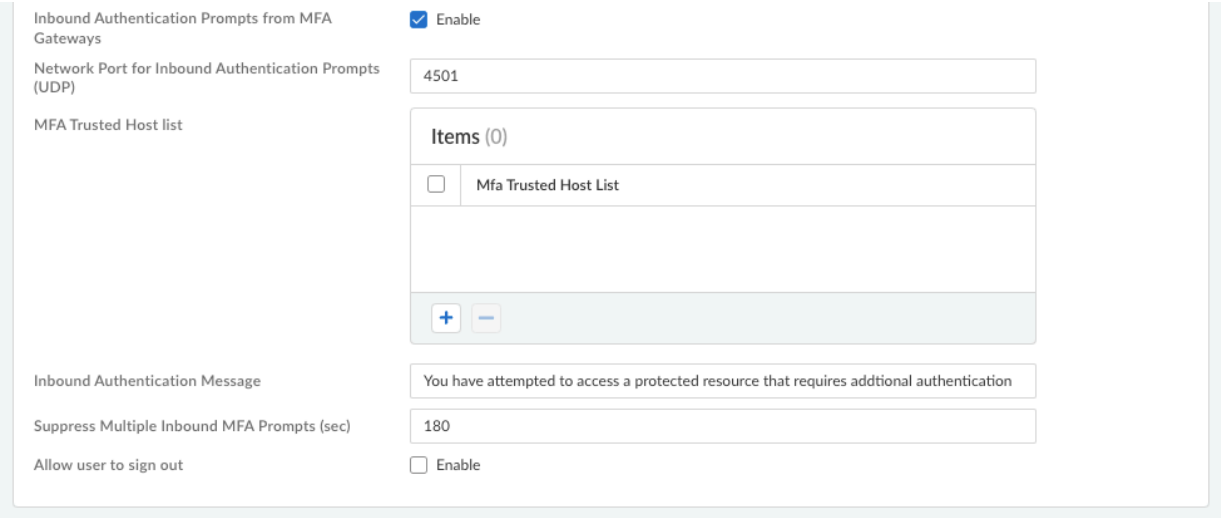
  セッションが非活動のためにタイムアウトするまでに経過する必要がある時間を指定してください。この設定は必須です。

  *Prisma Access*で*Nebula (10.2)*データプレーンを使用している場合、セッションタイムアウト値は設定できず、デフォルトでは7日です。
- トンネル**DNS**サフィックスにローカル検索ドメインを追加する（**Mac**のみ）–この設定を有効にすると、MacOSエンドポイントのローカルDNS検索ドメインにトンネルDNS検索ドメインが追加されます。エンドポイントのローカルDNS検索ドメインにトンネル検索ドメインを追加することで、ユーザーは頻繁に訪れるローカルおよびリモートの企業ウェブサイトやサーバーに完全なアドレスを入力することなく迅速にアクセスできるようになります。
- 各接続のプロキシを検出する（**Windows**のみ）–この設定を有効にすると、すべての接続でプロキシを自動的に検出します。この設定を無効にすると、ゲートウェイ接続のプロキシを自動的に検出し、そのプロキシをPrisma Accessへの後続の接続に使用します。
- プロキシ経由でトンネルを設定する（**Windows**および**Mac**のみ）–この設定を有効にして、Prisma Access Agentのプロキシ使用に基づいてネットワークトラフィックの動作を構成します。プロキシを使用するようにPrisma Accessエージェントに要求するには、[有効]を選択します。この設定を無効にすると、Prisma Access Agentにプロキシをバイパスさせることが要求されます。Prisma Access Agent プロキシの使用に応じて、エンドポイントのOS、トンネル タイプ、ネットワーク トラフィックの挙動が異なります。

  このオプションを無効にすると、Prisma Access Agentはプロキシをバイパスします。すべてのHTTPまたはHTTPSトラフィックは、プロキシまたはPACファイルのルールに一致する場合、目的の宛先に到達する前にPrisma Access Agentトンネルを通過する必要があります。プロキシをバイパスすることで、ユーザーがトンネルを通らずに検査とポリシーの強

 ©2025 Palo Alto Networks, Inc.

制を行うことなく、ウェブリソースにアクセスするための個人用プロキシを設定するのを防ぐことができます。



- 最適化された**MTU**—最大伝送単位（MTU）は、伝送中にパケットで送信できる最大のパケットサイズです。このオプションを有効にすると、パケット送信に使用する最適なMTUを自動的に決定します。

  Prisma Access Agentの接続は、標準の1500バイトよりもMTU値が低い複数のISPやネットワークホップを通過できます。静的エージェントMTU値がISPが提供しているものよりも低い場合、過剰なフラグメンテーションと追加のオーバーヘッドが発生し、スループットが低下します。ISPネットワークパスでのパケットのドロップは、再送信を引き起こし、最適でないパフォーマンスに寄与します。

  最適化された**MTU**を有効にすることで、最適なMTU値の手動での決定と設定の煩わしさを回避でき、ユーザーが生産性に影響を与えるパフォーマンスの低下を経験するのを防ぐことができます。

  最適化された**MTU**はデフォルトで有効になっています。それを無効にすると、MTUを手動で設定できます。構成可能な**MTU**（バイト）の範囲は256～1420バイトです。デフォルトは 1,400 バイトです。
- **MFA**ゲートウェイからのインバウンド認証プロンプト—多要素認証（MFA）をサポートするには、Prisma Access Agentエンドポイントがゲートウェイから受信するUDPプロンプトを受信し、確認する必要があります。この設定を有効にすると、Prisma Access AgentエンドポイントがUDPプロンプトを受信して応答できるようになります。この設定はデフォルトで有効になっています。この設定を無効にして、ゲートウェイからのUDPプロンプトをブロックします。
- インバウンド認証プロンプト用のネットワークポート **(UDP)** — Prisma Access AgentエンドポイントがMFAゲートウェイからのインバウンド認証プロンプトを受信するために使用するポート番号を指定します。デフォルト ポートは 4501 です。ポートを変更するには、1 ～ 65535 の数値を指定します。
- **MFA**信頼ホストリスト—Prisma Accessエージェントエンドポイントが多要素認証のために信頼できるファイアウォールまたは認証ゲートウェイのホストを追加します。GlobalProtectエンドポイントが指定されたネットワーク ポートで UDP メッセー

 ©2025 Palo Alto Networks, Inc.

ジを受信した場合、UDPプロンプトが信頼されたゲートウェイから来ているときにのみ、GlobalProtectは認証メッセージを表示します。

- インバウンド認証メッセージ–追加認証が必要なリソースにユーザーがアクセスしようとしたときに表示する通知メッセージをカスタマイズします。

  ユーザーが追加認証が必要なリソースにアクセスしようとすると、Prisma Access Agentはインバウンド認証プロンプトを含むUDPパケットを受信し、このメッセージを表示します。UDPパケットには、多要素認証の設定時に指定した認証ポータルページのURLも含まれています。Prisma Access Agentは自動的にURLをメッセージに付加します。

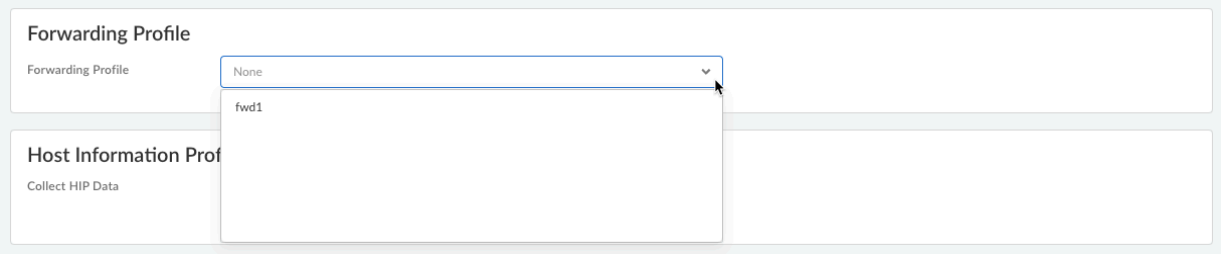
  以下に例を示します。

  > 追加の認証が必要となる、保護されたリソースにアクセスしようとしています。続行しますか?

  メッセージは255文字以下にしてください。

- 複数のインバウンドMFAプロンプトを抑制する（秒）–Prisma Accessエージェントが複数のインバウンドUDPプロンプトを抑制できるまでの待機秒数を指定します。デフォルト値は180秒です。
- ユーザーがサインアウトできるようにする–この設定を有効にすると、ユーザーがPrisma Accessエージェントからサインアウトできるようになります。この設定はデフォルトで無効になっています。

STEP 9 | エージェントとPrisma Access間のトラフィックの流れを管理するために、以前に設定した転送プロファイルを選択します。



STEP 10 | DNS設定の構成 動的権限アクセスの場合。

STEP 11 | ホスト情報プロファイルの設定

STEP 12 | Prisma Access Agentの設定を完了したら、[保存]をクリックします。

動的特権アクセスのためのDNS設定

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	☐ Prisma Access 5.1 Innovation ☐ モバイルユーザーサブスクリプション付きのPrisma Accessライセンス

©2025 Palo Alto Networks, Inc.

どこで使用できますか?	何が必要ですか?
	❑ MacOS 12以降のデスクトップデバイスまたはWindows 10バージョン2024以降またはWindows 11デスクトップデバイス ❑ ロール:プロジェクト管理者

Prisma Accessが内部ドメインを解決できるように、DNSサーバーを構成することができる。

STEP 1 | Strata Cloud Managerから、**[Manage (管理)]** > **[Configuration (設定)]** > **[NGFWとPrisma Access]** > **[Overview (概要)]** を選択し、設定スコープを展開して**[Snippets (スニペット)]**を表示します。

STEP 2 | スーパーユーザー管理者から割り当てられたスニペットを選択します。

STEP 3 | **[オブジェクト]** > **[動的権限アクセス]** を選択して、動的権限アクセス設定を開きます。

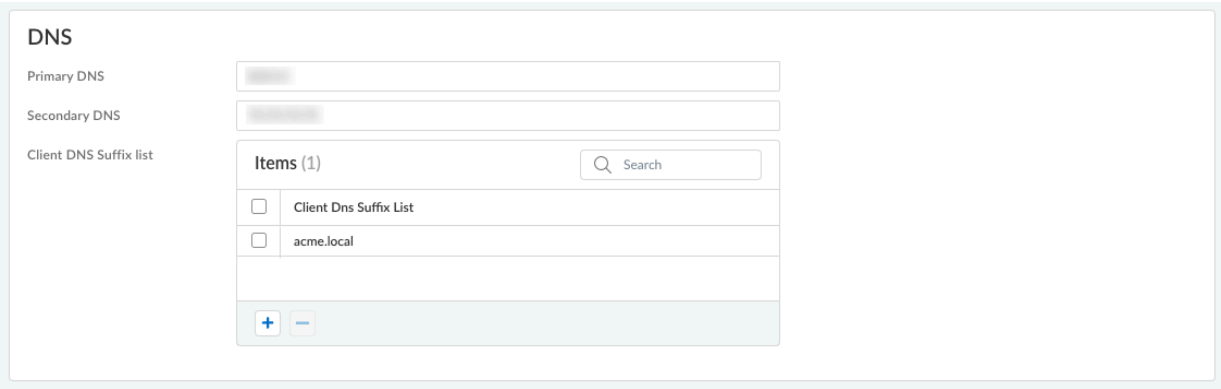
STEP 4 | エージェント設定タブを選択します。

STEP 5 | エージェント設定を追加する か、エージェント設定テーブルから既存の設定を選択します。

STEP 6 | Prisma Accessが内部ドメイン名を解決するために使用するプライマリ**DNS** サーバとセカンダリ**DNS** サーバを入力する。

STEP 7 | クライアント**DNS**サフィックスリストを追加して、**`acme.local`**などのように、解決できない非修飾ホスト名が入力されたときに、クライアントがローカルで使用するサフィックスを指定することができます。

ドメイン サフィックスの前にワイルドカード (*) 文字を入力しないでください (例: acme.com)。複数のサフィックスを追加できます。



 ©2025 Palo Alto Networks, Inc.

動的権限アクセスのためのHIPデータ収集設定を構成する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ MacOS 12以降のデスクトップデバイスまたはWindows 10バージョン2024以降またはWindows 11デスクトップデバイス ❑ モバイルユーザーサブスクリプション付きのPrisma Accessライセンス ❑ ロール:プロジェクト管理者

Prisma Access Agentは、実行中のホストに関する情報を収集し、接続が成功するとこのホスト情報をPrisma Accessの場所 (ゲートウェイ) に送信します。ゲートウェイは、Prisma Access Agentによって送信されたこの生のホスト情報を、定義したホスト情報プロファイル (HIP) オブジェクトおよびHIPプロファイルと照合します。一致していると認められた場合、HIP マッチ ログにエントリが生成されます。さらに、ポリシー ルールでHIPプロファイルの一致が認められると、対応するセキュリティ ポリシーが適用されます。

「グローバル エージェント設定の編集」ページの 「**HIP**通知」 タブでは、HIP通知の作成、HIPオブジェクトの作成と管理、すべてのエンドポイントのPrisma Accessエージェントに適用されるHIPプロファイルの作成と管理を行うことができます。

ここでは、Prisma Access Agentが収集または除外するカスタムHIPデータを定義できます。このオプションを有効にすると、Prisma Access AgentはMacOSまたはWindowsオペレーティング システムを実行しているデバイスからデータを収集します。

たとえば、カスタム チェックを使用すると、エンドポイントに特定のアプリケーションがインストールされているかどうか、または実行されているかどうかを確認できます。カスタム チェックで収集するように定義したデータは、Prisma Access Agentが収集し、Prisma Access Agentが接続したときにPrisma Accessに送信する生のホスト情報データに含まれます。

STEP 1 | Strata Cloud Managerから、**[Manage (管理)]** > **[Configuration (設定)]** > **[NGFWとPrisma Access]** > **[Overview (概要)]** を選択し、設定スコープを展開して**[Snippets (スニペット)]**を表示します。

STEP 2 | スーパーユーザー管理者から割り当てられたスニペットを選択します。

STEP 3 | [オブジェクト] > [動的権限アクセス] を選択して、動的権限アクセス設定を開きます。

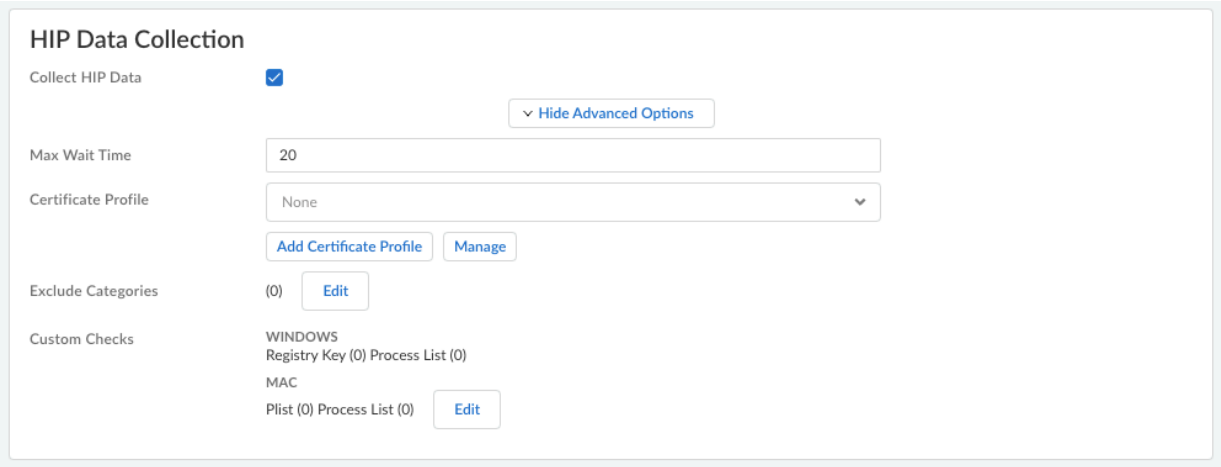
STEP 4 | エージェント設定タブを選択します。

STEP 5 | エージェント設定を追加する か、エージェント設定テーブルから既存の構成を選択します。

STEP 6 | ホスト情報プロファイル (HIP) セクションで、**HIP**データの収集 を選択して、プロジェクトを使用してログインしたエンドポイントでのHIPデータ収集を有効にします。

©2025 Palo Alto Networks, Inc.

STEP 7 | **Show Advanced Options**（詳細オプションの表示）を選択します。



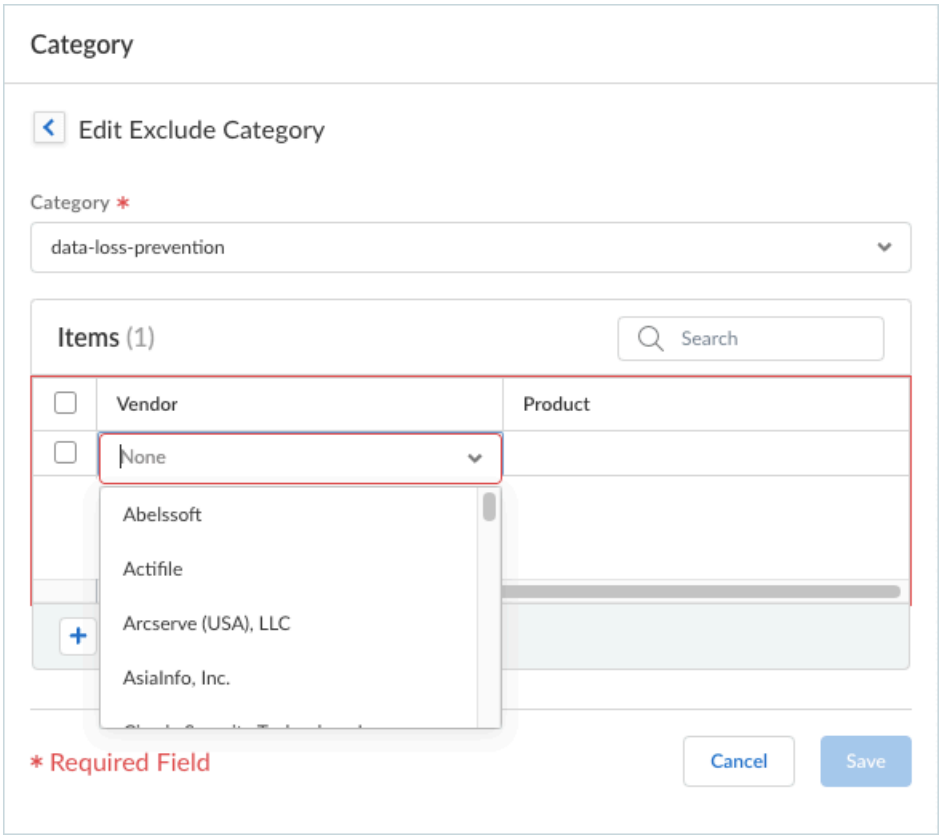
STEP 8 | 利用可能なデータを送信する前にPrisma Access AgentがHIPデータを検索する最大待機時間(秒単位) を指定します。範囲は10 ～ 60秒で、デフォルトは20秒です。

STEP 9 | 除外カテゴリを編集して、 特定のカテゴリ、またはカテゴリ内のベンダー、アプリケーション、バージョンをHIPデータ収集から除外します。

HIP収集から除外する**[Category (カテゴリ)]**（データ損失防止など）を選択します。カテゴリの選択後、特定の**Vendor (ベンダー)** を**Add**（追加）したのちに、そのベンダーの特定の製

©2025 Palo Alto Networks, Inc.

品を**Add**（追加）することで、必要に応じて除外内容を詳細に設定することが可能です。除外リストに複数のベンダーおよび製品を追加できます。各ダイアログで設定を保存します 。



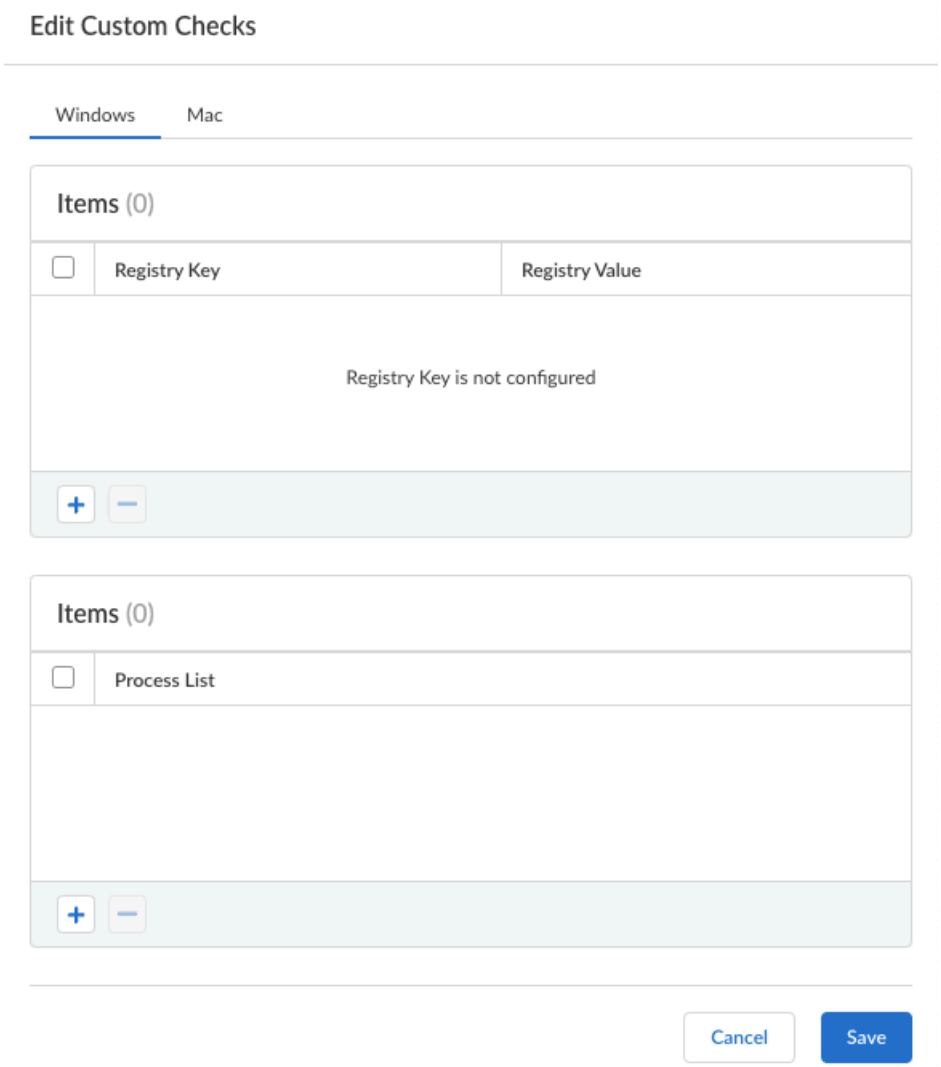
ベンダー全体を除外したくない場合は、ベンダーからの特定のパッチを除外できます。ベンダーを追加した後、次の形式を使用して、パッチ名または番号、およびオプションでHIPレポートからパッチ更新を除外する日付を指定できます。

```
除外: [kb-article-id1:MM/DD/YYYY]、[kb-article-id2:MM/DD/YYYY]
```

ここで、**<kb-article-id>**は属性の名前または番号（例：**<kb-article-id>2267602</kb-article-id>**）、**MM/DD/YYYY**はHIPレポートからパッチを除外する日付を指定します。日付を設定しない場合、パッチは無期限にHIPレポートから除外されます。日付を設定することを選択した場合、パッチは指定された日付まで除外されます。

©2025 Palo Alto Networks, Inc.

STEP 10 | Custom Checks（カスタム チェック）を編集し、この設定を実行しているホストから収集するカスタム データを定義し、カテゴリおよびベンダーを追加します。



たとえば、HIPオブジェクト作成対象のVendor [ベンダー] リストやProduct [製品] リストに含まれていない必須アプリケーションがある場合、カスタムチェックを作成して、アプリケーションがインストールされているか（対応するWindowsレジストリキーまたはMac plistキーががあるか）、あるいは実行中か（対応する実行中プロセスがあるかどうか）を判定できます。

- **Windows**– 特定のレジストリキーまたはレジストリ値のチェックを追加 します。データ収集を特定の Registry Value（レジストリ値）に制限するには、特定のレジストリ値を **Add**（追加）して定義します。
- **Mac**– 特定の **Plist** キーまたは キー値のチェックを追加します 。特定のキー値に対するデータ収集を制限するには、Key（キー）値を**Add**（追加）します。OKをクリックして設定を保存します。
- **Process List**（プロセス リスト） – エンドポイントで実行中かどうかをチェックする対象のプロセスを **Add**（追加）します。たとえば、ソフトウェア アプリケーションが実行して

©2025 Palo Alto Networks, Inc.

いるかどうかを判別するには、実行可能ファイルの名前をプロセス リストに追加します。プロセスは**Windows** タブおよび**Mac**タブのいずれにも追加できます。

完了したら、カスタム チェック設定を保存します 。

STEP 11 | プロジェクト固有のPrisma Access Agent設定の構成が完了したら、構成を保存します。

 ©2025 Palo Alto Networks, Inc.

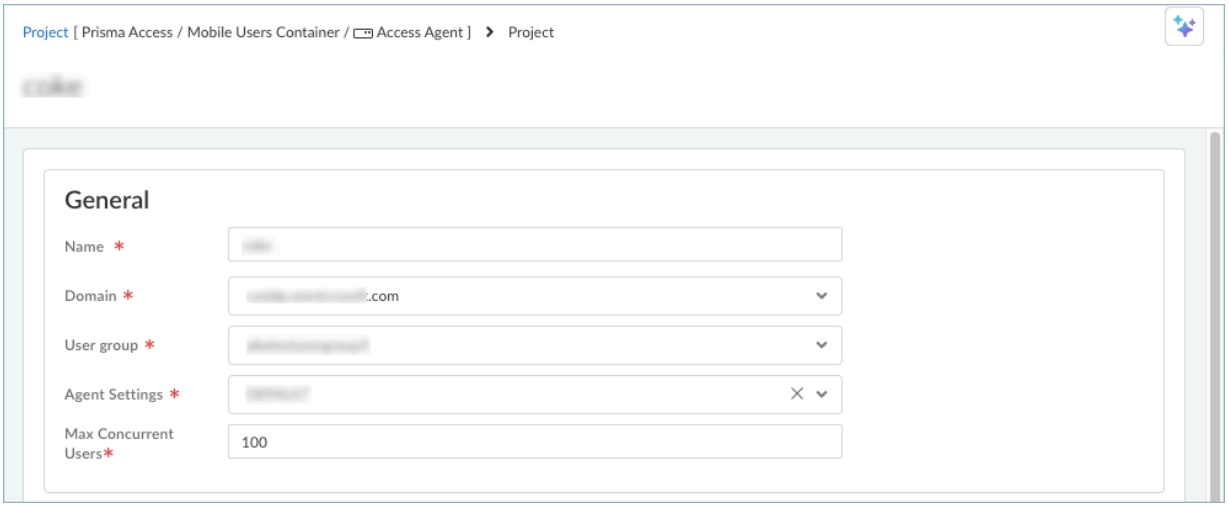
プロジェクトを作成する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Accessライセンス ❑ 最低限必要なPrisma Accessバージョン:5.1 ❑ ロール:スーパーユーザー

Prisma Access Agentを使ってユーザーにアクセスさせたいプロジェクトを追加します。プロジェクト管理者だけがプロジェクト定義を作成および管理できます。

STEP 1 | **[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access]**を選択します。

STEP 2 | 作成したプロジェクト スニペットにスコープを設定し、**[オブジェクト] > [動的権限アクセス] > [プロジェクト] > [プロジェクトの追加]**に移動します。

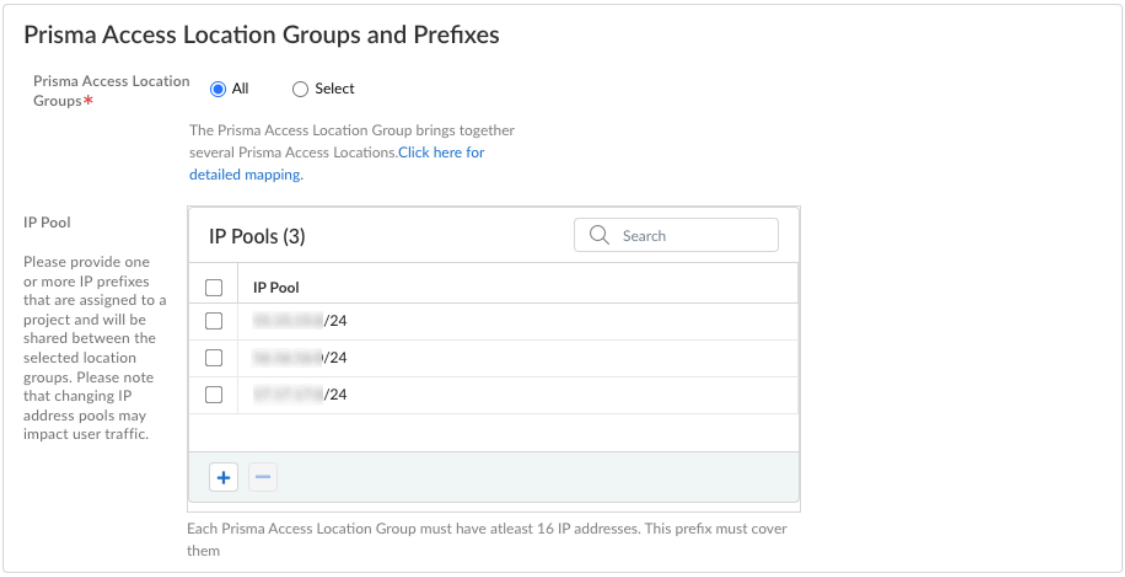


1. プロジェクト名を入力します。
2. Cloud Identity Engineに追加したドメイン と、ディレクトリにマップされたユーザー グループを選択します。
3. 以前に追加したエージェント設定 と、プロジェクトの最大同時ユーザー数を選択します。
4. **Prisma Access**ロケーショングループを選択します。場所グループのリストは、GlobalProtectゲートウェイを追加する場所に基づいて入力されます。

   作成するプロジェクトは、IPプールとロケーション グループに関連付けられます。ユーザーは、Prisma Access Agentを使用して接続するプロジェクトとPrisma Accessのコンピューティング ロケーションに基づいてIPアドレスを取得します。プロジェクトは、プロジェクトに関連付けられているロケーション グループ内のロケーションにのみ接続できます。Prisma Access ロケーション グループとPrisma Accessコン

©2025 Palo Alto Networks, Inc.

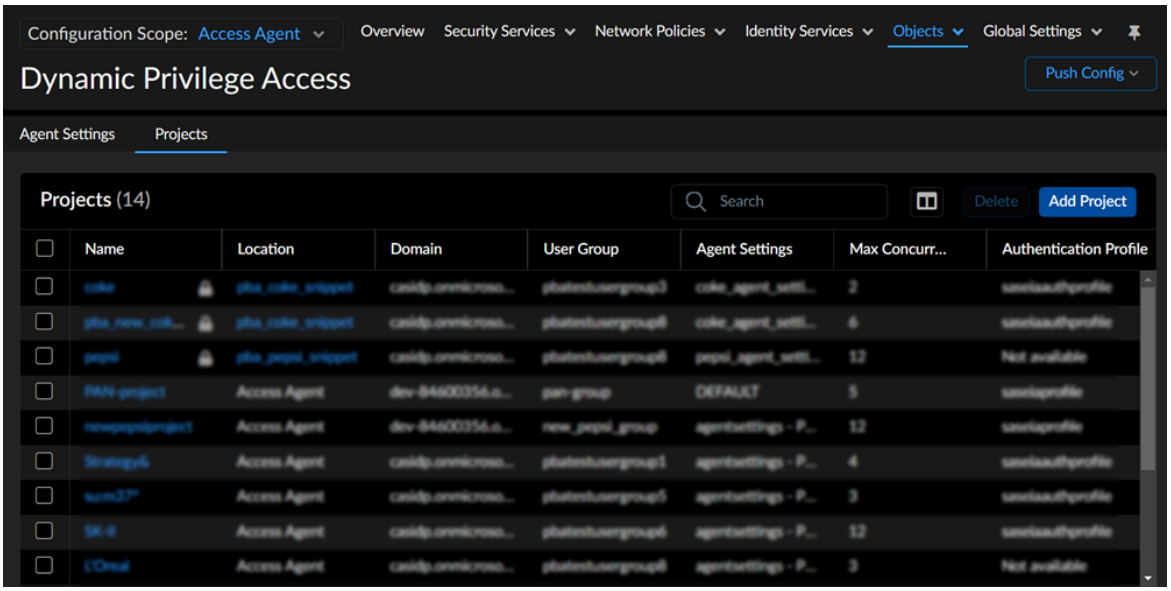
ピューティング ロケーション間のマッピングを表示するには[詳細なマッピングについてはここをクリック] を選択します。



5. プロジェクトの**IP**プールを追加または選択します。IPプレフィックスはプロジェクトに割り当てられ、選択したPrisma Accessロケーション グループ間で共有されます。

   これらのプロジェクトIPプールを要約すると、ネットワークに送信されるルートの数を減らすことができます。

6. プロジェクト設定を保存します 。



 ©2025 Palo Alto Networks, Inc.

- 構成スコープでプロジェクト スニペットを選択すると、その特定のプロジェクトに関連する設定と詳細のみにアクセスできます。
- プロジェクト管理者またはプロジェクト プッシュ管理者として*Strata Cloud Manager*にログインすると、アクセスできるプロジェクトの詳細のみを表示できます。別のプロジェクト スニペットの構成スコープを選択した場合、別のプロジェクトの設定と詳細にアクセスすることはできません。
- プロジェクトを切り替えるには、異なるプロジェクトの資格情報を使用して、別のプロジェクト管理者またはプロジェクト プッシュ管理者として*Strata Cloud Manager*に再度ログインする必要があります。

STEP 3 | 変更を **Push**（プッシュ）します。

Prisma Accessでプロジェクトを作成した後、ユーザーがPrisma Access Agentを使ってそのプロジェクトに認証できるようになるまで、最大15分かかることがあります。

©2025 Palo Alto Networks, Inc.

動的権限アクセスのためのトラフィックステアリング

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Accessライセンス ❑ 最低限必要なPrisma Accessバージョン:5.1 ❑ ロール:プロジェクト管理者

トラフィック ステアリングを使用して、プロジェクトのトラフィックをサービス接続とプロジェクト固有のルートに転送します。

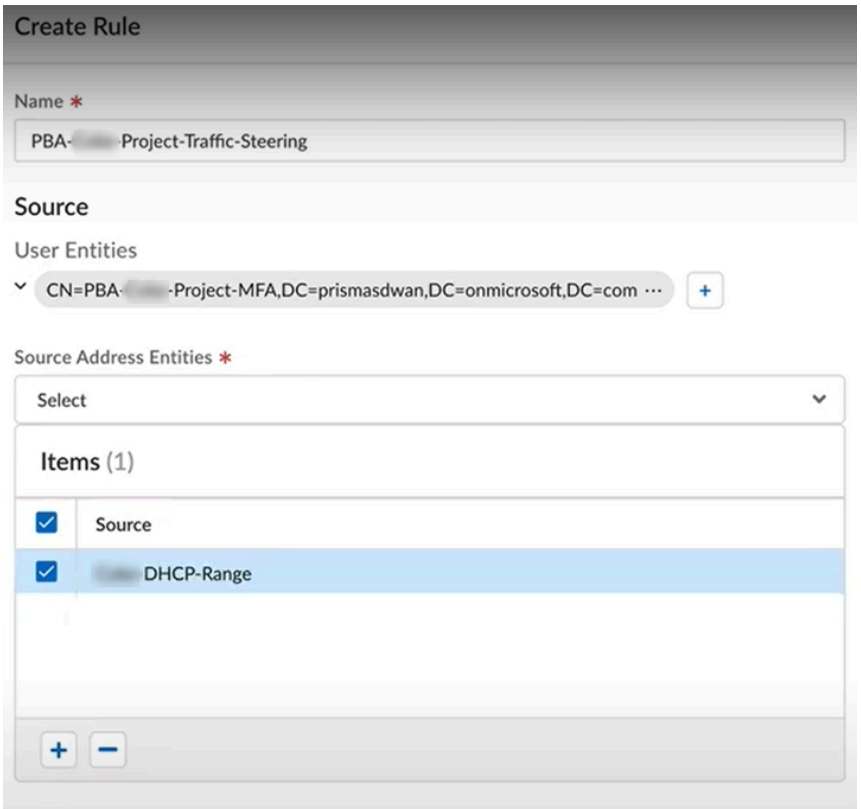
STEP 1 | **[Workflows (ワークフロー)] > [Prisma Accessセットアップ] > [Service Connections (サービス接続)]**を選択します。

STEP 2 | サービス接続を追加します。

STEP 3 | トラフィックをルーティングするには、 詳細設定 を編集します。

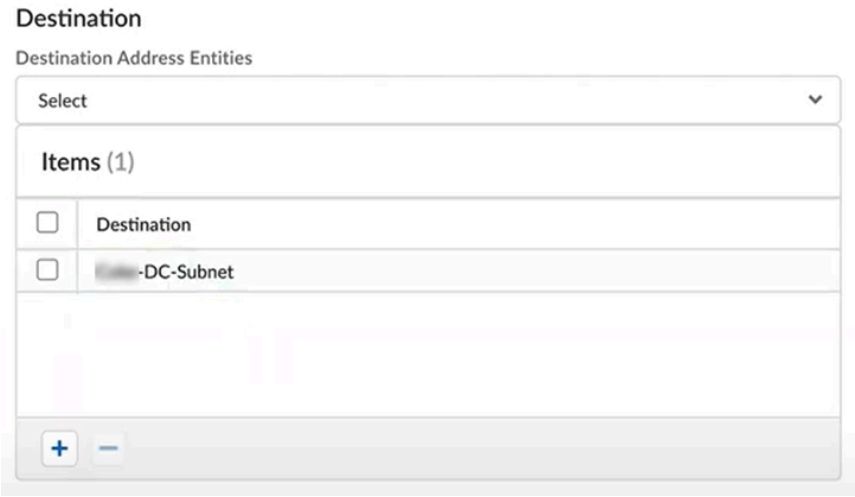
STEP 4 | プロジェクトの トラフィック ステアリング の下にルールを追加します 。

STEP 5 | 送信元 をユーザーと一致させ、プロジェクトのDHCP範囲を 送信元アドレス エンティティとして追加します。

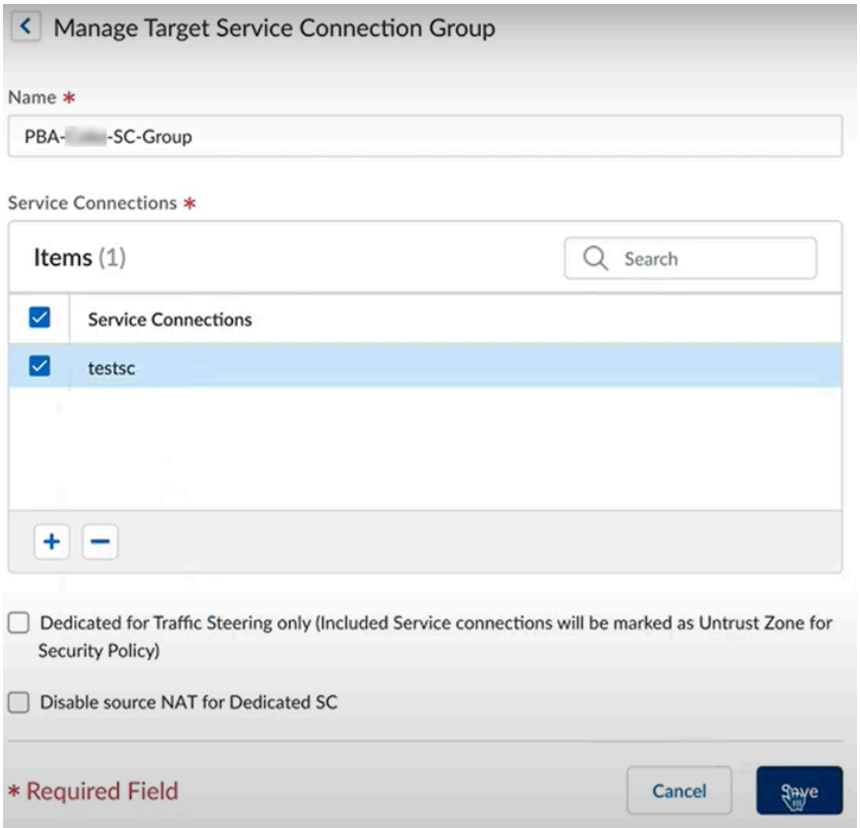


 ©2025 Palo Alto Networks, Inc.

STEP 6 | 宛先アドレスのエンティティにマッチさせます。



STEP 7 | サービスとアクションを選択します。



STEP 8 | 変更をコミットしてプッシュします。

©2025 Palo Alto Networks, Inc.

動的な特権アクセスのためのPrisma Access Agentのセットアップ

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ モバイルユーザーサブスクリプション付きのPrisma Accessライセンス ❑ MacOS 12以降のデスクトップデバイスまたはWindows 10バージョン2024以降またはWindows 11デスクトップデバイス ❑ ロール:スーパーユーザー

エンド ユーザーは、ユーザが割り当てられている顧客プロジェクトに基づいて、 Prisma Access Agentを使用して組織のネットワークにアクセスします。

プロジェクト固有のエージェント設定を設定し、プロジェクトを作成したら、段階的ロールアウトやグローバル・エージェント設定など、他のPrisma Access Agent 設定を構成することができます。

以下のPrisma Access Agent設定を行うことができます：

- Prisma Access Agentの段階的なロールアウトを構成する
- Prisma Access エージェントの一般的なグローバル設定を構成する
- Prisma Access AgentのHIP通知を設定する

Prisma Access Agentの段階的なロールアウトを設定する

どこで使用できますか?	何が必要ですか?
• Prisma Access（Strata Cloud Managerによる管理）	❑ Prisma Access 5.1 優先またはイノベーション ❑ モバイルユーザーサブスクリプション付きのPrisma Accessライセンス ❑ MacOS 12以降のデスクトップデバイスまたはWindows 10バージョン2024以降またはWindows 11デスクトップデバイス ❑ ロール:スーパーユーザー

Prisma Access Agentのアップグレード ロールアウト機能により、管理者は特定の順序でデバイス グループをアップグレードできるようになります。アップグレードのロールアウトによ

 ©2025 Palo Alto Networks, Inc.

り、Prisma Access AgentsをアップグレードするためにJamf ProやMicrosoft Intuneなどのモバイル デバイス管理 (MDM) ソフトウェアに依存する必要がなくなります。

ステージアップグレードのロールアウトは、エンドユーザーのデバイスに*Prisma Access Agent*を最初にデプロイメントしたまたはインストールの後にのみ行うことができます。

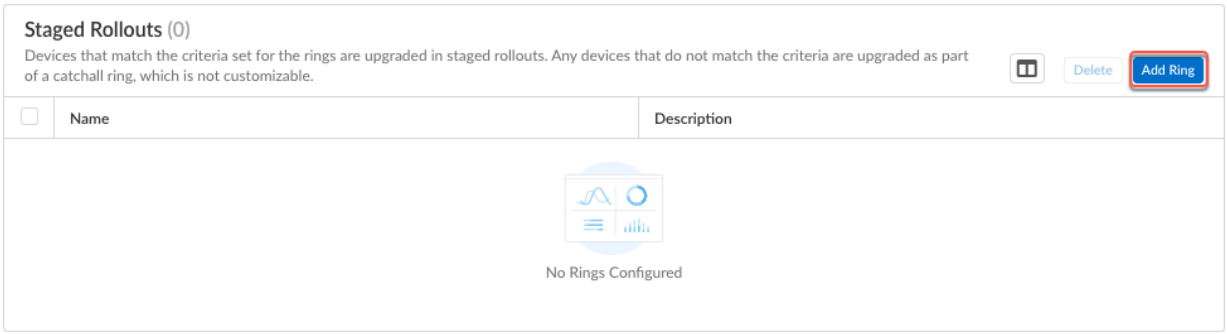
Prisma Access Agentのアップグレードのロールアウトを段階的に行うには、ユーザー、グループ、オペレーティング システムに基づく一致条件を使用してアップグレード リングを構成できます。基準に一致するデバイスは、アップグレード リング (リング 0 ～ リング 4、デフォルト リング) の順序でアップグレードされます。

Prisma Access AgentのAccess Agentセットアップ ページを使用してモバイル ユーザーをオンボードするときに、オプションでアップグレード リングを定義できます。エージェントの初期構成時にアップグレード リングを定義しないことを選択した場合、すべてのデバイスはデフォルトのリングに配置されます。後でPrisma Accessエージェントのセットアップ ページに戻り、アップグレード リングを定義して、構成をPrisma Accessにプッシュできます。これらの変更は、次の段階的なロールアウト中、または段階的なロールアウトを停止して開始した後に有効になります。

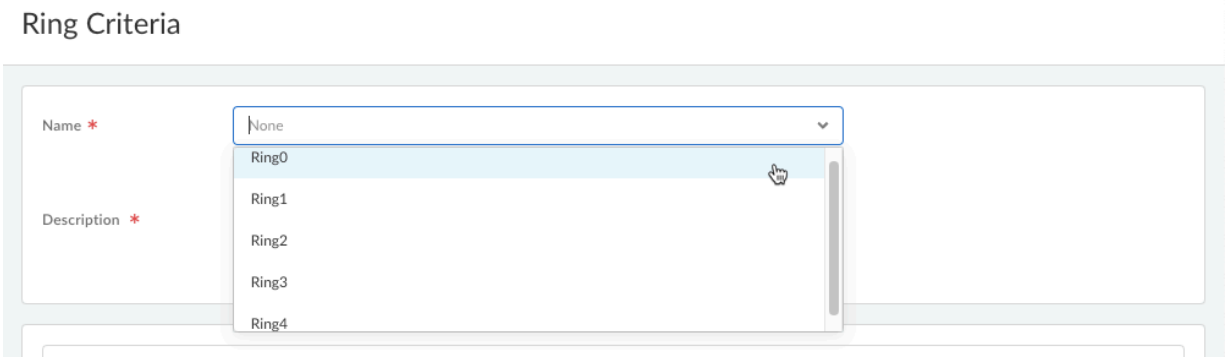
アップグレード リングを構成するには:

STEP 1 | Strata Cloud Managerで、[ワークフロー] > **[Prisma Access** セットアップ] > **[Access Agent]** > **[Prisma Access Agent]**を選択します。

STEP 2 | [段階的なロールアウト] セクションで、[リングを追加]をクリックします。



STEP 3 | リングの事前定義済みの名前 を選択します。**Ring0** から**Ring4**まで選択できます。最初に追加するリングは **Ring0**です。



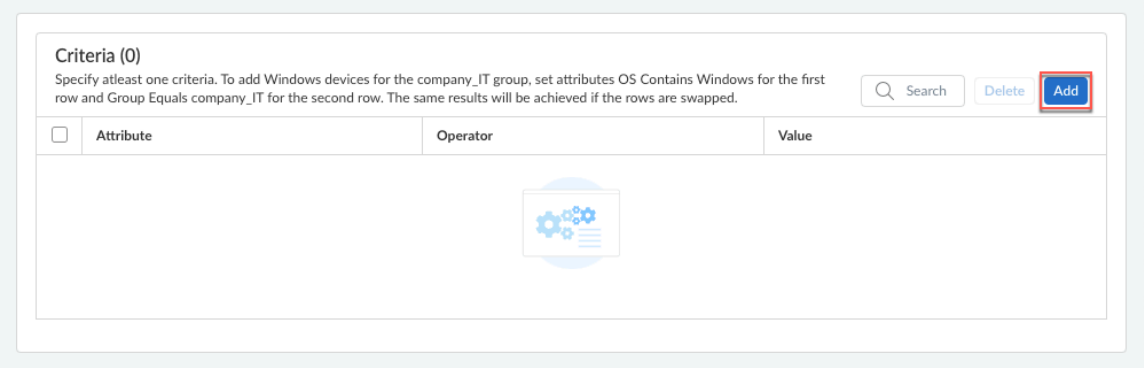
 ©2025 Palo Alto Networks, Inc.

STEP 4 | リングのわかりやすい 説明 を入力します。

©2025 Palo Alto Networks, Inc.

STEP 5 | ユーザー、 グループ、または デバイスの **OS** 属性に基づいて、リングの基準を指定します。

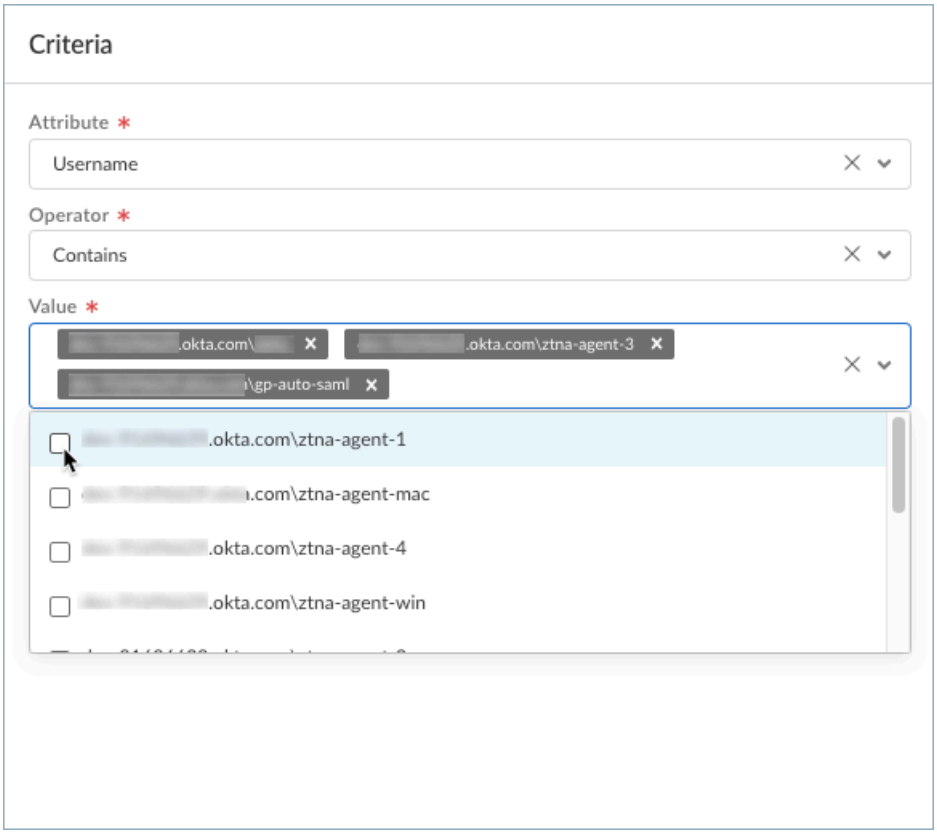
1. 条件を追加します 。



2. 各基準について、 属性、 演算子、 値を選択し、**[追加]**をクリックします。条件ごとに選択できる属性と演算子は1つだけです。値は、属性と演算子に選択した内容によって異なります。

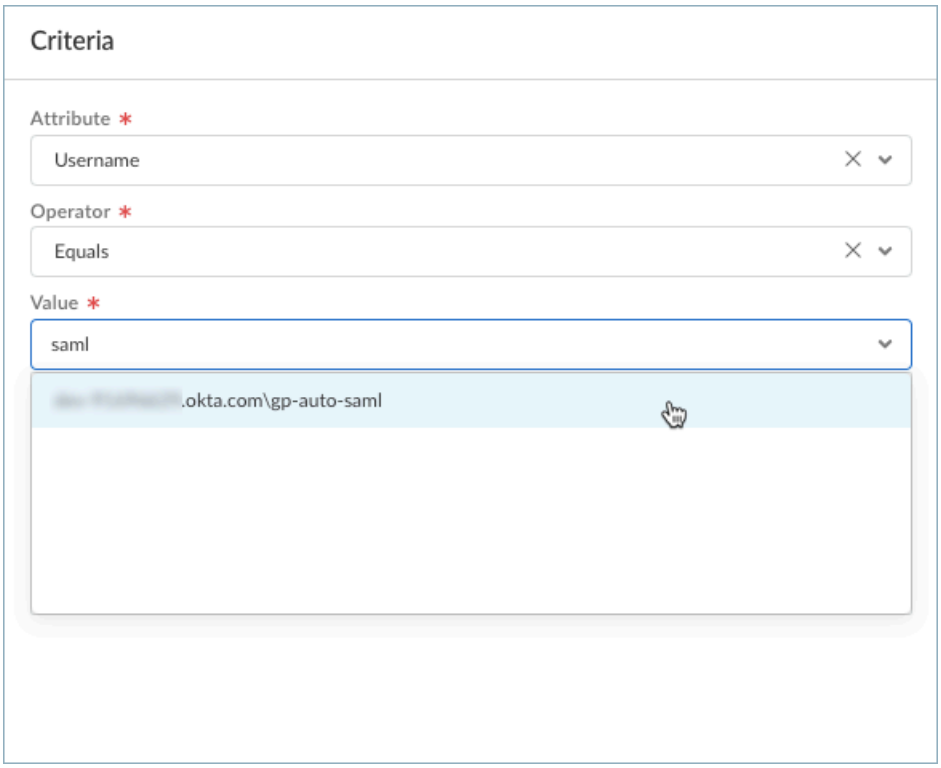
   - ユーザー名 属性の場合:

     - **[Operator (演算子)] > [Contains (含む)]**を選択した場合は、「値」 リストからユーザー名を選択または検索します。検索を開始するには、ユーザー名を入力します。リストから1つ以上のユーザー名を選択できます。



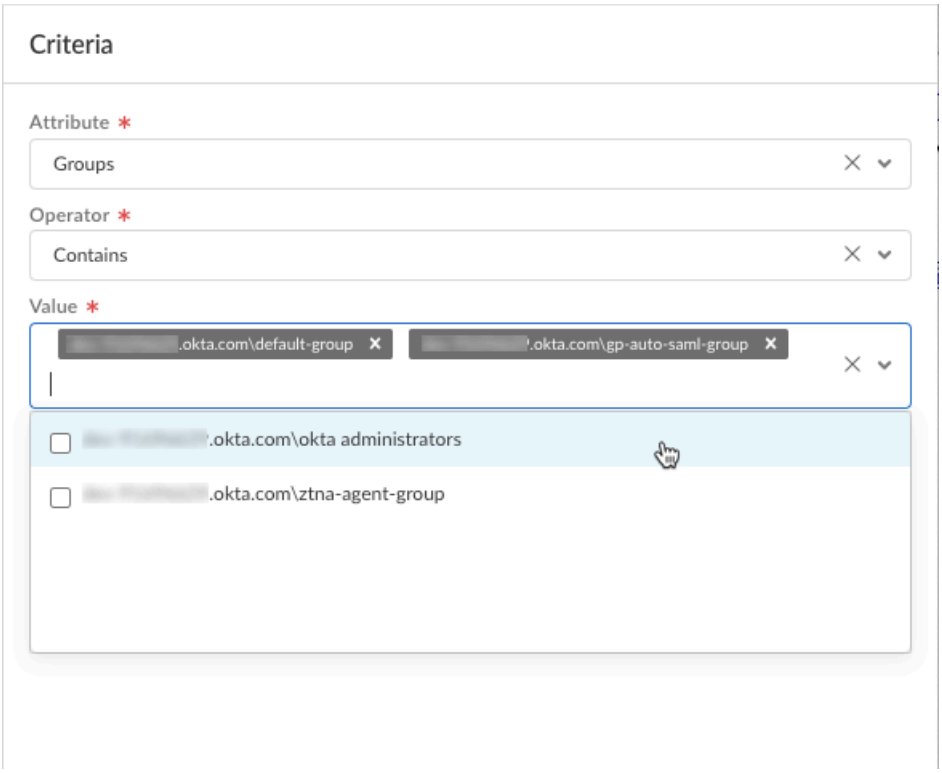
 ©2025 Palo Alto Networks, Inc.

- **[Operator (演算子)] > [Equals (等しい)]**を選択した場合は、「値」 リストからユーザー名を選択または検索します。検索を開始するには、ユーザー名を入力します。リストからユーザー名を1つ選択できます。

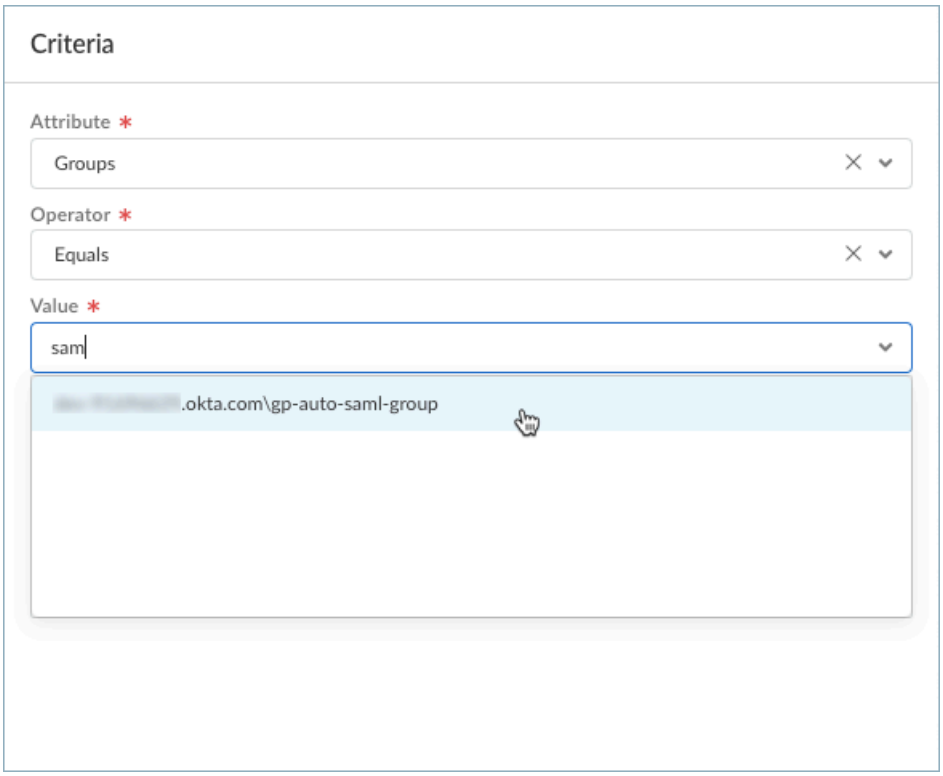


- グループ 属性の場合:
  - **[Operator (演算子)] > [Contains (含む)]**を選択した場合は、「値」 リストからグループを選択または検索します。検索を開始するには、グループ名を入力します。リストから1つ以上のグループを選択できます。

©2025 Palo Alto Networks, Inc.



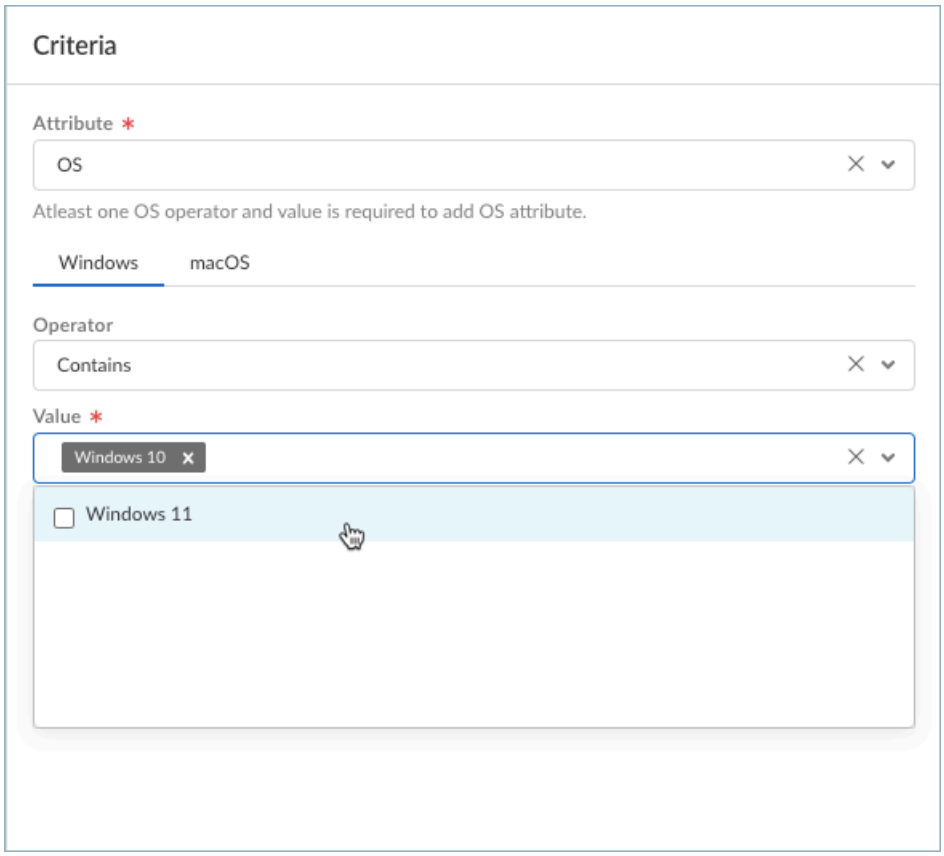
- **[Operator (**演算子**)]** > **[Equals (**等しい**)]**を選択した場合は、「値」 リストからグループを選択または検索します。検索を開始するには、グループ名を入力します。リストから1つのグループを選択できます。



- **OS** 属性では、OSタイプ **(Windows** または**MacOS)** を選択します。次に：

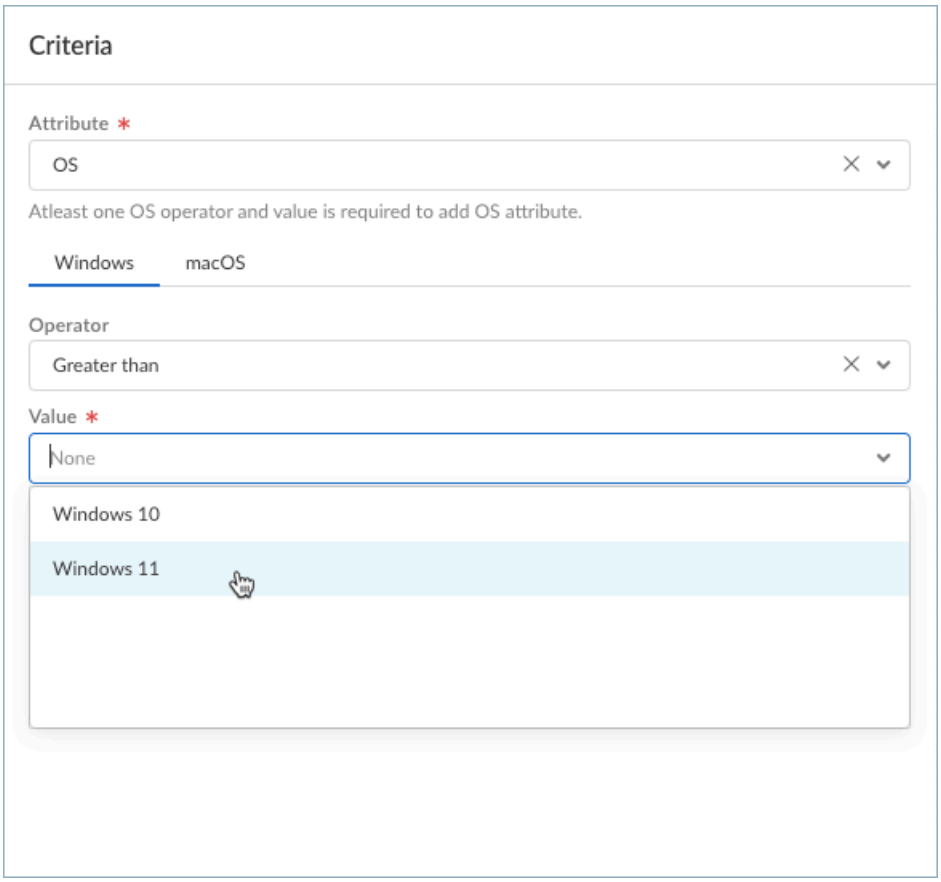
 ©2025 Palo Alto Networks, Inc.

- **[Operator (演算子)] > [Contains (含む)]**を選択した場合は、 値 リストから1つ以上のOSバージョンを検索または選択します。検索を開始するには、OSとバージョンを入力します。リストから1つ以上のOSバージョンを選択できます。



- [より大きい] または [より小さい] 演算子を選択した場合は、「値」 リストからOSバージョンを検索または選択します。検索を開始するには、OSとバージョンを入力します。リストから OS バージョンを1つ選択できます。

©2025 Palo Alto Networks, Inc.



3. 必要に応じて、さらに条件を追加します 。リングごとに最大3つの条件を指定できます。

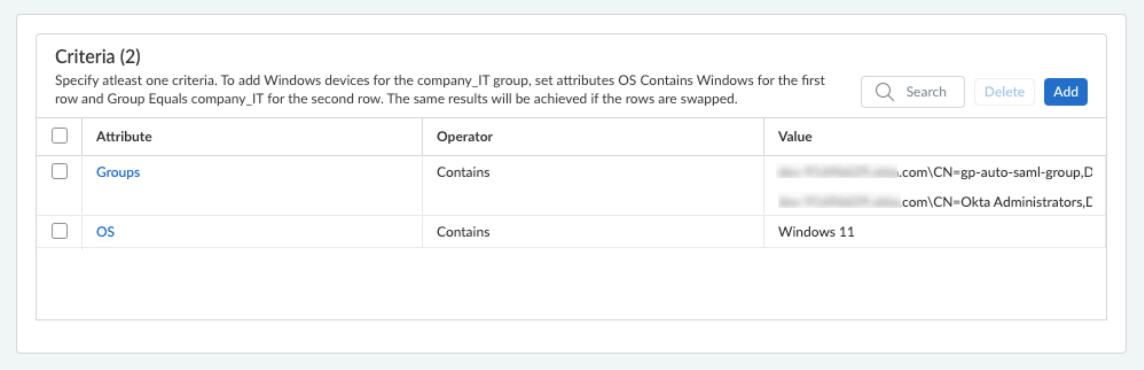
   属性はリングごとに1回だけ使用できます。属性を使用して条件を追加すると、その属性は属性ドロップダウンに表示されなくなります。

   条件を追加すると、その条件が「リング条件」ページの 「条件」 テーブルに表示されます。Prisma Accessが基準を評価する際、同じセルにリストされている値は論理OR演

©2025 Palo Alto Networks, Inc.

算子を使用して評価され、行間の属性と値は論理AND演算子を使用して評価されます。

たとえば、次の画像の条件は、**gp-auto-saml-group**または**Okta Administrators**グループに属し、Windows 11オペレーティング システムを実行しているデバイスと一致します。



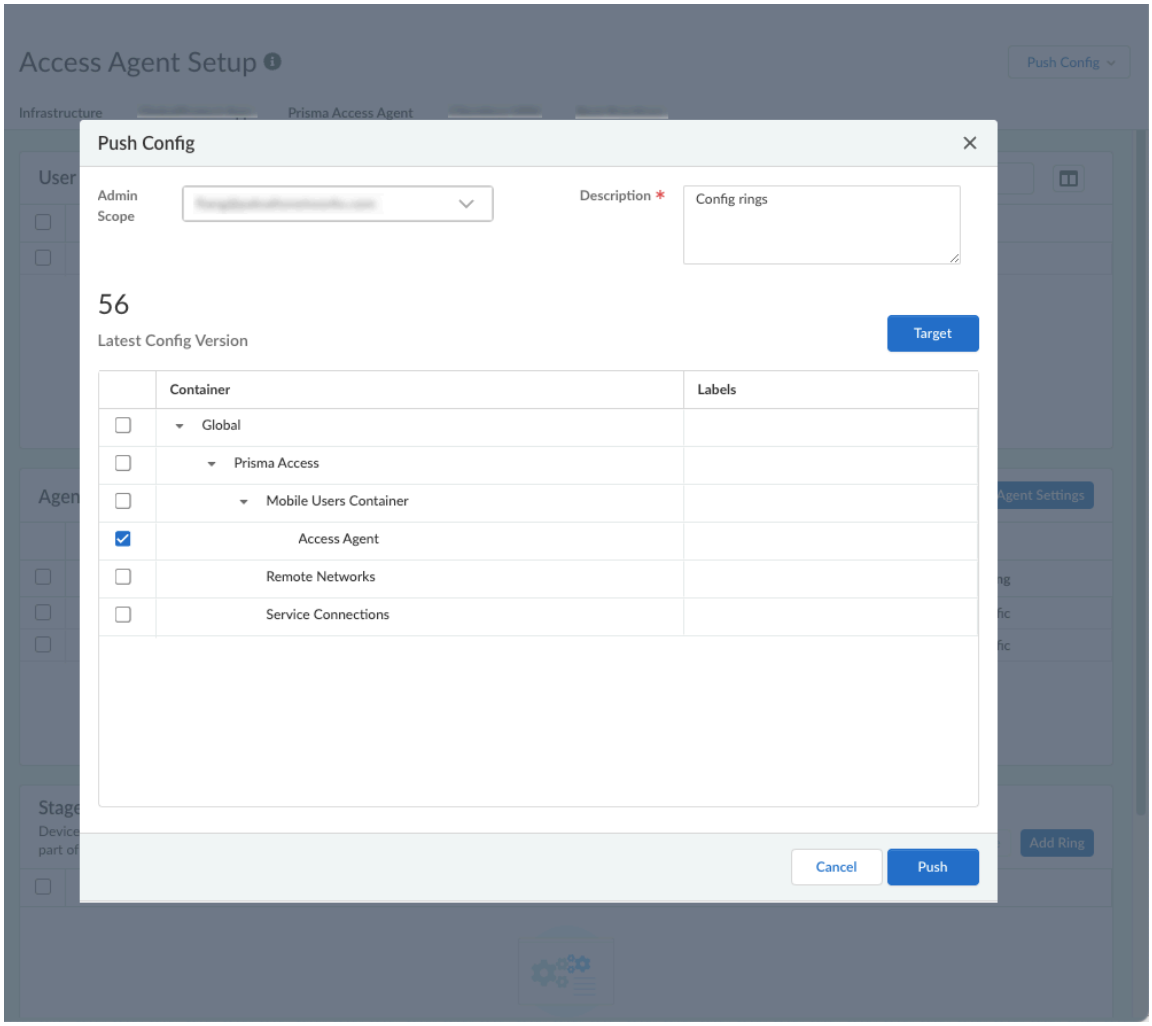
4. リング基準を保存します 。

STEP 6 | さらにリングを作成するには、手順 2 ～ 5 を繰り返します。合計5つのリング (リング 0 からリング 4) を作成できます。

©2025 Palo Alto Networks, Inc.

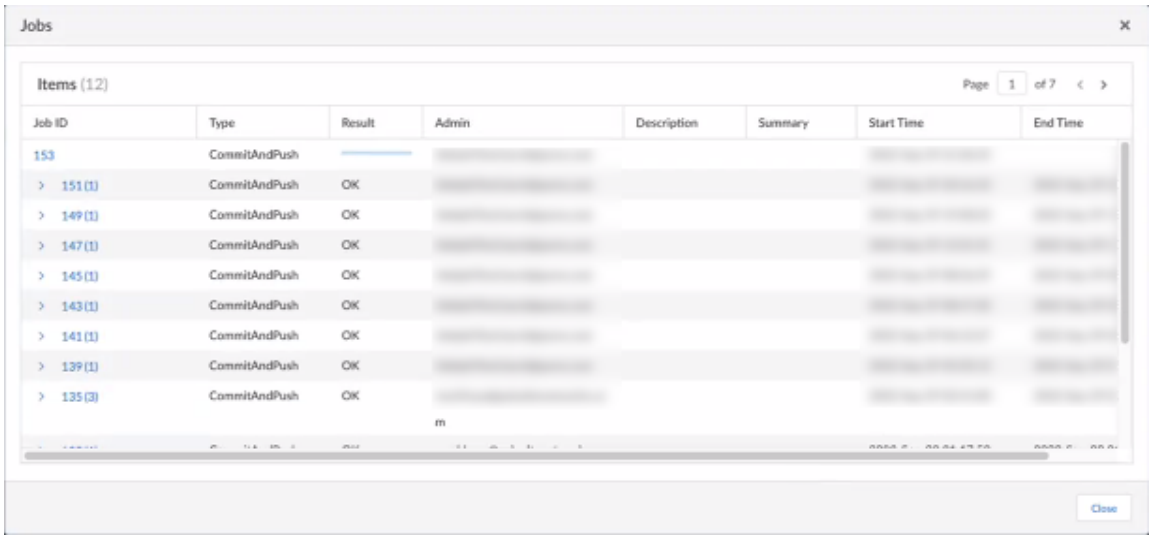
STEP 7 | Prisma Accessに設定をプッシュします。

1. **[Push Config (設定のプッシュ)]** > **[Push (プッシュ)]**を選択します。
2. ジョブの説明を入力します。
3. **[Global (グローバル)]** > **[Prisma Access]** > **[Mobile Users (モバイルユーザー)]** > **[Access Agent]** コンテナを選択し、**[Push (プッシュ)]**をクリックします。



4. ジョブが完了するまで待ってから、「ジョブ」ダイアログを閉じます 。

©2025 Palo Alto Networks, Inc.



STEP 8 | Strata Cloud Managerの**[Prisma Access Agent]** > [管理]で段階的なロールアウトを監視できます 。

Prisma Access Agents向けの一般的なグローバル設定を構成する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	☐ Prisma Access 5.1 Innovation ☐ モバイルユーザーサブスクリプション付きのPrisma Accessライセンス ☐ MacOS 12以降のデスクトップデバイスまたはWindows 10バージョン2024以降またはWindows 11デスクトップデバイス ☐ ロール:スーパーユーザー

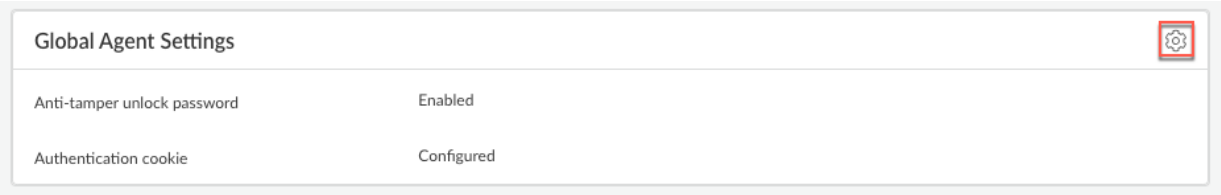
すべてのエンドポイントにわたってPrisma Accessエージェントに適用されるグローバル エージェント設定をカスタマイズできます。

一般的なグローバル エージェント設定には、エンド ユーザーのデバイスからPrisma Access Agentをアンインストールするなど、ユーザーがPrisma Access Agentを改ざんするのを防ぐ改ざん防止機能の設定が含まれます。さらに、認証オーバーライド設定、非アクティブ タイムアウト設定を構成したり、隔離されたデバイスのログインをブロックしたりすることもできます。

STEP 1 | Strata Cloud Manager から、**[ワークフロー]** > **[Prisma Access セットアップ]** > **[Access Agent]** > **[Prisma Access Agent]**を選択します。

©2025 Palo Alto Networks, Inc.

STEP 2 | グローバル エージェント設定を編集します。



STEP 3 | **General** (全般) を選択します。

STEP 4 | 改ざん防止ロック解除パスワードを設定します。

改ざん防止機能を有効にすることで、権限のないユーザーによるPrisma Access Agentの改ざんを防ぐことができ、Prisma Access Agentを保護できます。改ざん防止機能により、エンドポイント上の次のPrisma Access Agentリソースを保護できます。Prisma Access Agentのフォルダーとファイル - 権限のないユーザーは、Prisma Access Agent関連のファイルやフォルダーを削除したり、名前を変更したりすることはできません。Prisma Access Agentサービスおよびホスト情報プロファイル (HIP) プロセス - 権限のないユーザーは、Prisma Access Agent関連のサービスおよびHIPプロセスを停止できません。HIPプロセスは、Prisma Access Agentが実行されているホストに関する情報を収集し、検査のためにホスト情報をPrisma Accessに送信します。ユーザーがプロセスを停止しようとする場合、改ざん防止ロック解除パスワードを入力する必要があります。Prisma Access Agentレジストリ キー (Windows の場合) または .plist ファイル (macOS の場合) - 権限のないユーザーは、Prisma Access AgentのWindowsレジストリ キーまたは.plistファイルを削除または更新できません。PACliコマンドライン インターフェイス - 権限のないユーザーは、PACliコマンドライン インターフェイスを使用してPrisma Access Agentまたは改ざん防止機能を無効にすることはできません。コマンドラインでトラブルシューティングのために特定のアクションを実行する必要がある管理者および承認済みユーザーは、プロンプトが表示されたときに、改ざん防止ロック解除 (スーパーバイザー) パスワードを入力する必要があります。

Prisma Access Agentのトラブルシューティングを行うために改ざん防止機能のロックを解除するには、改ざん防止ロック解除パスワード (スーパーバイザー パスワードとも呼ばれます) を設定する必要があります。

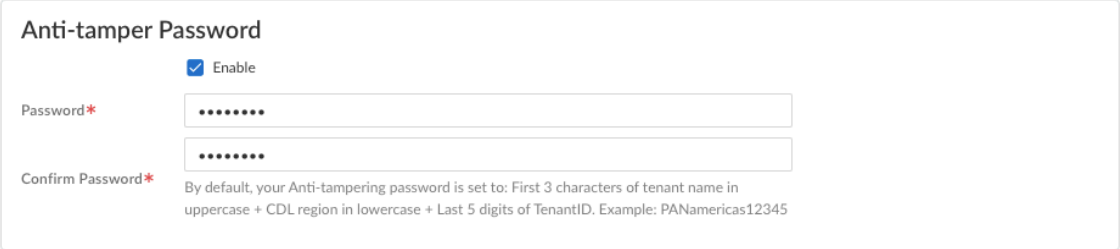
1. 改ざん防止ロック解除パスワード

   改ざん防止パスワードを有効にしない場合は、パスワードは割り当てられず、Prisma Access Agentのコマンド ラインでプロンプトが表示されたときに、ユーザーは任意のパスワード (空のパスワードを含む) を入力できます。

   改ざん防止パスワードを有効にした後で無効にすると、ユーザーはスーパーバイザ パスワードを入力せずに、エージェント上で **`pacli enable`**、**`pacli hip status`**、**`pacli protect enable`**、**`pacli switchto GlobalProtect`** コマンドなどの特定のPACliコマンドを実行できるようになります。パスワードの入力を求められた場合は**Enter**キーを押すだけです。

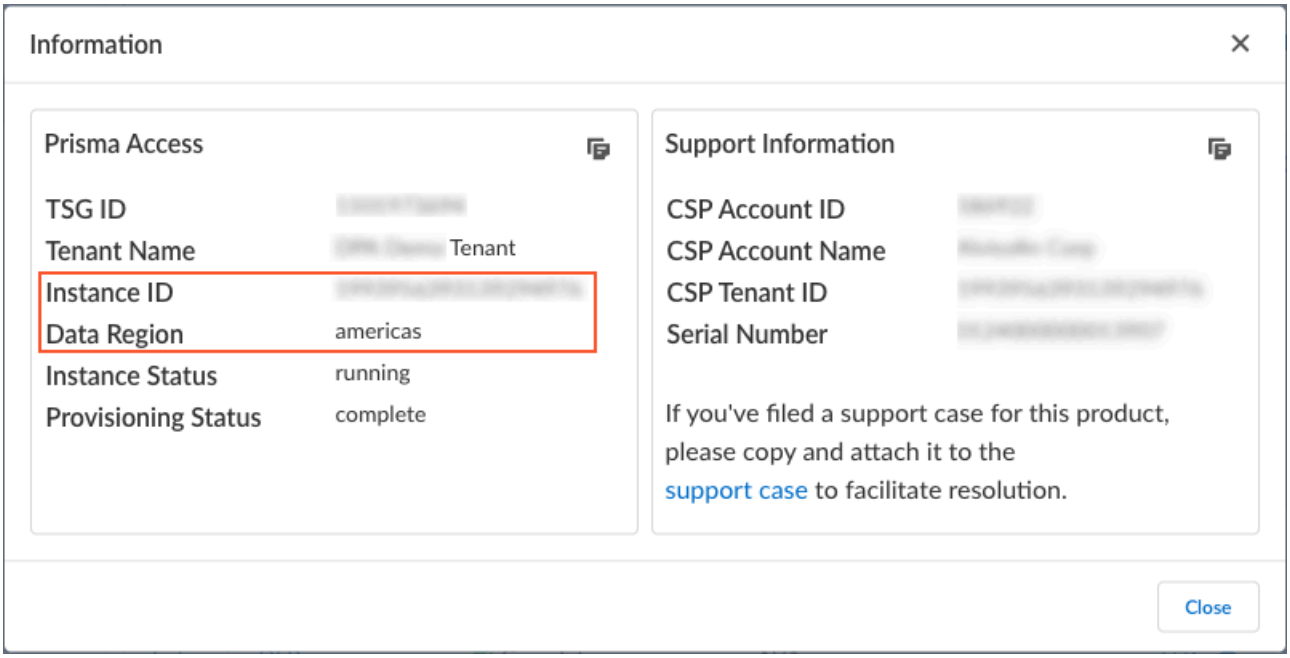
©2025 Palo Alto Networks, Inc.

2. パスワードを入力し、パスワードを再入力してパスワードの確認を行います 。パスワードには最低8文字の英数字が必要です。



パスワードを指定しない場合は、デフォルトのパスワードが使用されます。デフォルトでは、改ざん防止パスワードは、Prisma Accessテナント名の最初の3文字 (大文字)、Prisma Accessデータ リージョン (小文字)、およびPrisma AccessインスタンスIDの最後の5桁に設定されます。次に例を示します。**PANamericas56789**。

Prisma AccessインスタンスID とデータリージョンは設定 > テナント > を選択することで取得できます。 **<your_tenant>** Prisma Accessのシリアル番号の横にある [サポート情報の表示] ツールヒントを選択します。

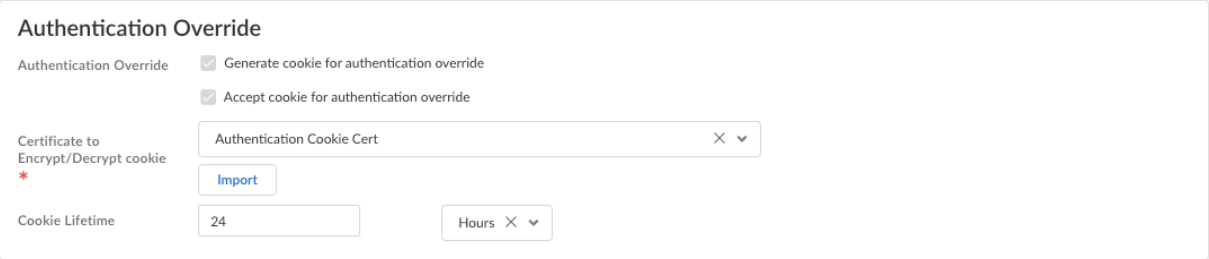


エージェントにさらに高いレベルのセキュリティを提供するには、デフォルトのパスワードが最も安全ではない可能性があるため、新しい改ざん防止ロック解除パスワードを設定してデフォルトのパスワードをオーバーライドします。

STEP 5 | 認証オーバーライド 設定を構成して、Prisma Accessがユーザー認証用に安全で暗号化されたCookieを生成して受け入れることを許可します。認証オーバーライドにより、ユー

©2025 Palo Alto Networks, Inc.

ザーは指定された **Cookie**有効期間中に1回だけログイン資格情報を提供できるようになります。



- **Generate cookie for authentication override**（認証オーバーライド用**Cookie**を生成）— Prisma Accessが暗号化されたエンドポイント固有のCookieを生成し、その認証用Cookieをエンドポイントに発行できるようにします。
- **Accept cookie for authentication override**（**Cookie**による認証オーバーライドを許可）— Prisma Accessが暗号化された有効なCookieを使用してユーザーを認証できるようにします。有効なCookieをアプリが提示した場合、Prisma AccessはポータルまたはPrisma Accessが暗号化したCookieであることを確認し、復号化を行ってユーザーを認証します。
- **Certificate to Encrypt/Decrypt Cookie**（**Cookie**暗号化/復号化時の証明書） — Cookieを暗号化および復号化するために使用するRSA証明書を選択します。
- **Cookie Lifetime**（**Cookie** の有効期間） — Cookie が有効な時間数、日数、または週数を指定します（デフォルトは 24 時間）。時間の範囲は1 ～ 72、週の範囲は1 ～ 52、日の範囲は1 ～ 365です。クッキーの有効期限が切れると、ユーザーはログイン資格情報を再入力する必要があります。次に、Prisma Accessは新しいCookieを暗号化してエージェントに送信します。この値は、設定したCookieの有効期間と同じでも異なっていてもかまいません。

STEP 6 | 非アクティブ ログアウトの分数を入力して、アイドル状態のユーザーがPrisma Access Agentからログアウトされるまでの時間を指定します。

非アクティブ ログアウト期間を使用すると、セキュリティ ポリシーを適用して、Prisma Accessに接続している間にエンドポイントからのトラフィックを監視し、非アクティブなPrisma Access Agentセッションをすばやくログアウトすることができます。非アクティブなログアウト期間を短く設定できます。Prisma Access Agentがトンネル経由でトラフィックをルーティングしなかった場合、またはゲートウェイが設定された時間内にエンドポイントからHIPチェックを受信しなかった場合、ユーザーはログアウトされます。

STEP 7 | 隔離されたデバイスからのPrisma Access Agentユーザーのログインを防止するには、隔離されたデバイスのログインをブロックします 。

この設定が有効になっているときにユーザーが隔離されたデバイスからログインしようとすると、Prisma Access Agentはデバイスが隔離されており、ユーザーはそのデバイスからログインできないことをユーザーに通知します。この設定が有効でない場合、ユーザは通知を受け取りますが、そのデバイスからのログインは可能です。

STEP 8 | 設定を**[Save (**保存**)]**します。

©2025 Palo Alto Networks, Inc.

動的権限アクセスのHIP通知を構成する Prisma Access Agent

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ モバイルユーザーサブスクリプション付きのPrisma Accessライセンス ❑ MacOS 12以降のデスクトップデバイスまたはWindows 10バージョン2024以降またはWindows 11デスクトップデバイス ❑ ロール:スーパーユーザー

「グローバル エージェント設定の編集」ページの 「**HIP**通知」 タブでは、ホスト情報プロファイル通知の作成、HIPオブジェクトの作成と管理、すべてのエンドポイントのPrisma Accessエージェントに適用される HIPプロファイルの作成と管理を行うことができます。

Prisma Access Agentは、実行中のホストに関する情報を収集し、接続が成功するとこのホスト情報をPrisma Accessの場所 (ゲートウェイ) に送信します。ゲートウェイは、Prisma Access Agentによって送信されたこの生のホスト情報を、定義したHIPオブジェクトおよびHIPプロファイルと照合します。一致していると認められた場合、HIP マッチ ログにエントリが生成されます。さらに、ポリシー ルールでHIPプロファイルの一致が認められると、対応するセキュリティ ポリシーが適用されます。

HIPチェックはアプリケーションがゲートウェイに接続したときに実行され、その後のチェックはPrisma Accessエージェントが接続されている間、1時間ごとに実行されます。Prisma Accessエージェントは、以前のHIPチェックが変更された場合、更新されたHIPレポートを要求することができます。エンドポイントごとのゲートウェイには、最新のHIPレポートのみが保持されます。

ポリシーの適用にホスト情報を使用することで、重要なリソースにアクセスするリモート ホストが適切に整備された、セキュリティ標準に準拠した粒度の細かいセキュリティを実現でき、その後に、ネットワーク リソースへのアクセスを許可できます。たとえば、機密データ システムへのアクセスを許可する前に、データにアクセスするホストのハード ドライブの暗号化を確実に有効にすることが必要になる場合があります。エンドポイント システムで暗号化が有効になっている場合のみアプリケーションへのアクセスを許可するセキュリティ ルールを作成して、このポリシーを適用できます。

さらに、このルールに準拠していないエンドポイントについては、アクセスが拒否された理由をユーザーに警告する通知メッセージを作成できます。不足している暗号化ソフトウェアのインストール プログラムにアクセスできる場所へのリンクを提供することもできます。ユーザーがそのファイル共有にアクセスできるようにするには、特定のHIPプロファイルが一致するホストに対して特定の共有へのアクセスを許可する、対応するセキュリティ ルールを作成する必要があります。

次のタスクを完了できます。

- 動的権限アクセス用のHIP通知を作成する Prisma Access Agent
- 動的権限アクセスのためのHIPオブジェクトの作成と管理 Prisma Access Agent

©2025 Palo Alto Networks, Inc.

- 動的権限アクセスのためのHIPプロファイルの作成と管理 Prisma Access Agent

動的権限アクセス用のHIP通知を作成する Prisma Access Agent

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ モバイルユーザーサブスクリプション付きのPrisma Accessライセンス ❑ MacOS 12以降のデスクトップデバイスまたはWindows 10バージョン2024以降またはWindows 11デスクトップデバイス ❑ ロール:スーパーユーザー

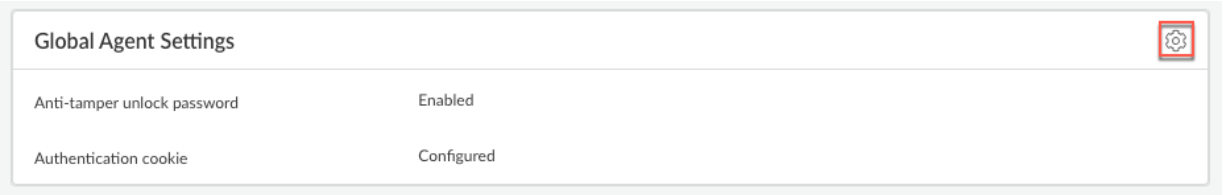
HIPプロファイルのセキュリティ ルールが適用されたときにエンド ユーザーに表示される通知メッセージを定義できます。

ユーザーの設定がポリシー内のHIPプロファイルと一致するか一致しない場合に通知メッセージを表示するかどうかは、ポリシーと、HIPの一致 (または不一致) がユーザーにとって何を意味するかによって大きく異なります。つまり、一致とは、ネットワーク リソースへのフル アクセスが許可されていることを意味するのでしょうか、それともコンプライアンス違反の問題によりアクセスが制限されているということですか?

たとえば、会社の必須のアンチウイルスおよびアンチスパイウェア ソフトウェア パッケージがインストールされていない場合に一致するHIPプロファイルを作成するとします。HIPプロファイルに一致するユーザーに対してHIP通知メッセージを作成し、ソフトウェアをインストールする必要があることを通知できます。または、これらと同じアプリケーションがインストールされている場合にHIPプロファイルが一致するなら、プロファイルに一致しないユーザーに対してメッセージを作成することが必要になる場合があります。

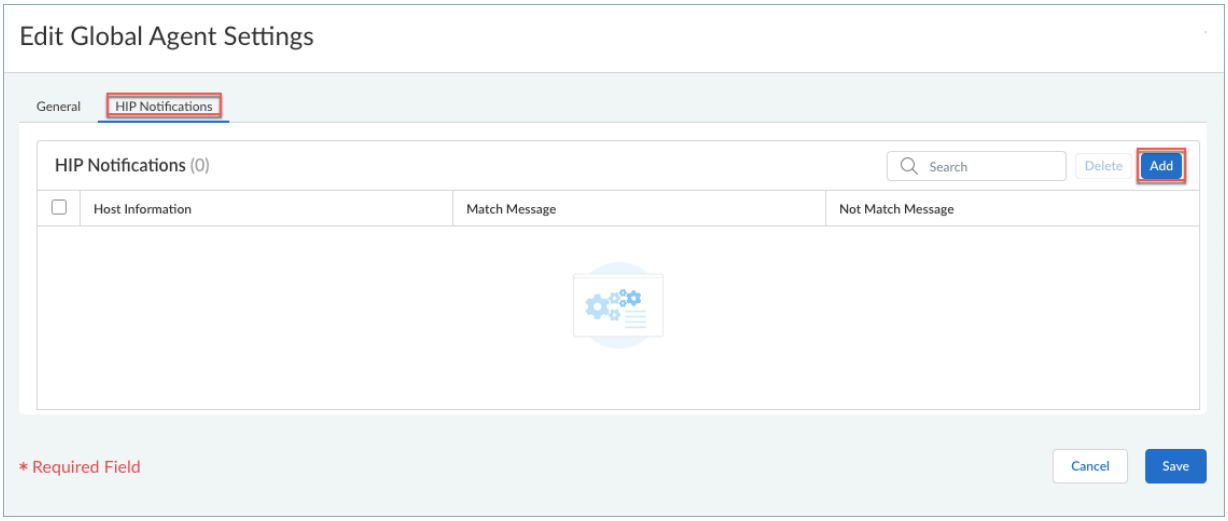
STEP 1 | Strata Cloud Manager から、[ワークフロー] > **[Prisma Access** セットアップ] > **[Access Agent]** > **[Prisma Access Agent]**を選択します。

STEP 2 | **Global Agent**設定を編集します。

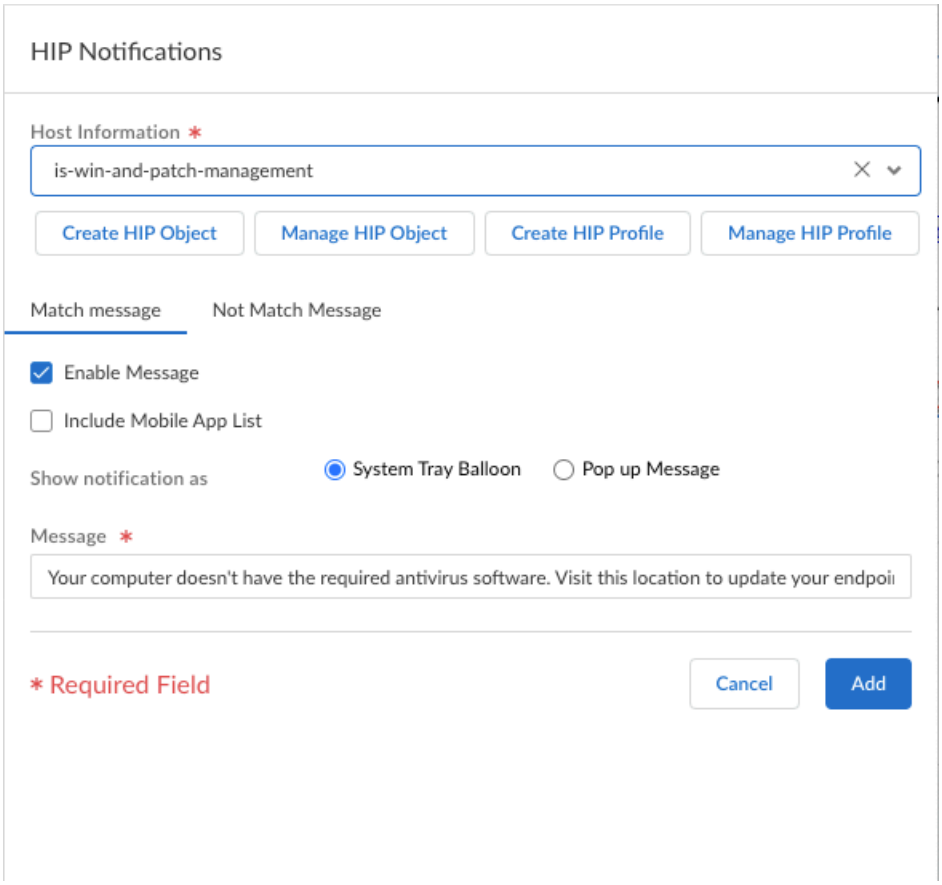


 ©2025 Palo Alto Networks, Inc.

STEP 3 | **[HIP通知]を選び[追加]をクリックします。**



STEP 4 | **Host Information**（ホスト情報）ドロップダウンから、このメッセージが適用されるHIPプロファイルを選択します。



HIPプロファイルがない場合は、HIPプロファイルを作成する必要があります。

STEP 5 | 対応するHIPプロファイルが一致または不一致のときにメッセージを表示するかどうかによって、**Match Message**（メッセージの一致）または**Not Match Message**（一致しないメッセージ）を選択します。場合によっては、照合するオブジェクトおよびポリシーの対

©2025 Palo Alto Networks, Inc.

象に応じて、一致する場合と一致しない場合の両方でメッセージの作成が必要になることがあります。

STEP 6 | **Enable Message**（メッセージを有効にする）を選択し、メッセージをシステムトレイのバルーンとして表示するか、ポップアップメッセージとして表示するかを選択します。

STEP 7 | メッセージ テキストを入力し、[追加]をクリックします。

STEP 8 | 定義するメッセージごとにこの手順を繰り返します。

動的権限アクセスのためのHIPオブジェクトの作成と管理 Prisma Access Agent

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ モバイルユーザーサブスクリプション付きのPrisma Accessライセンス ❑ MacOS 12以降のデスクトップデバイスまたはWindows 10バージョン2024以降またはWindows 11デスクトップデバイス ❑ ロール:スーパーユーザー

Prisma AccessゲートウェイでHIPオブジェクトとHIPプロファイルを作成することにより、監視またはポリシー適用に使用するホスト属性を定義できます。

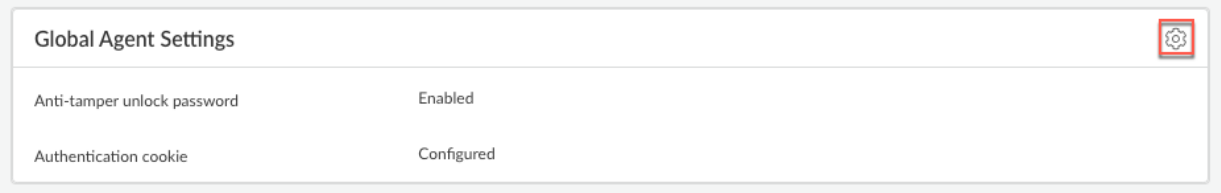
HIPオブジェクトは、Prisma Access Agentによって報告された生データからポリシーを適用するために使用するホスト情報をフィルター処理するために使用される一致条件で構成されます。たとえば、生のホスト データにはエンドポイントにインストールされている複数のウイルス対策パッケージに関する情報が含まれている可能性がありますが、関心があるのは特定の1つのアプリケーションだけである可能性があります。この場合は、適用において関心のある特定のアプリケーションに一致するHIPオブジェクトを作成します。

必要なHIPオブジェクトを判別する最良の方法は、収集したホスト情報をどのように使用してポリシーを適用するかを判別することです。HIPオブジェクト自体は、セキュリティ ポリシーで使用されるHIPプロファイルを作成できるようにする構成要素にすぎません。したがって、特定の種類の必須ソフトウェアの存在、特定のドメインのメンバーシップ、特定のOSなど、1つの項目に一致させることで、オブジェクトをシンプルに保つようにしてください。これを行うことで、きめ細かいHIP拡張ポリシーを柔軟に作成できるようになります。

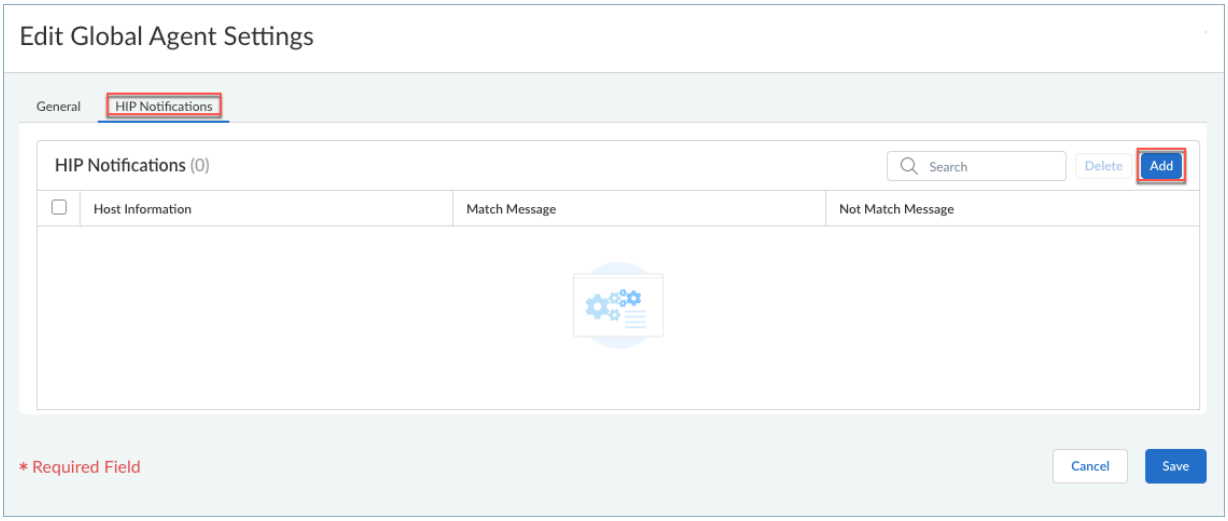
STEP 1 | Strata Cloud Manager から、**[ワークフロー] > [Prisma Access セットアップ] > [Access Agent] > [Prisma Access Agent]**を選択します。

©2025 Palo Alto Networks, Inc.

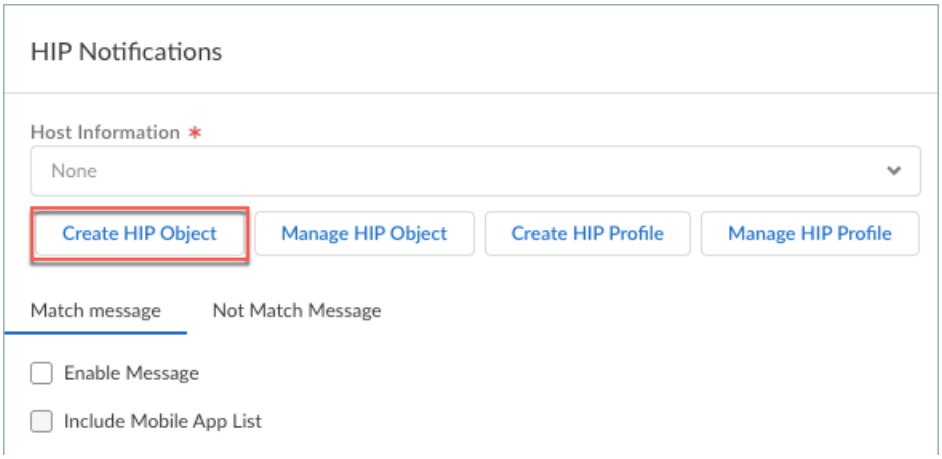
STEP 2 | **Global Agent**設定を編集します。



STEP 3 | **[HIP**通知**]**を選び**[**追加**]**をクリックします。



STEP 4 | **HIP**オブジェクトの作成をクリックします。



STEP 5 | オブジェクトの名前と説明を入力します。

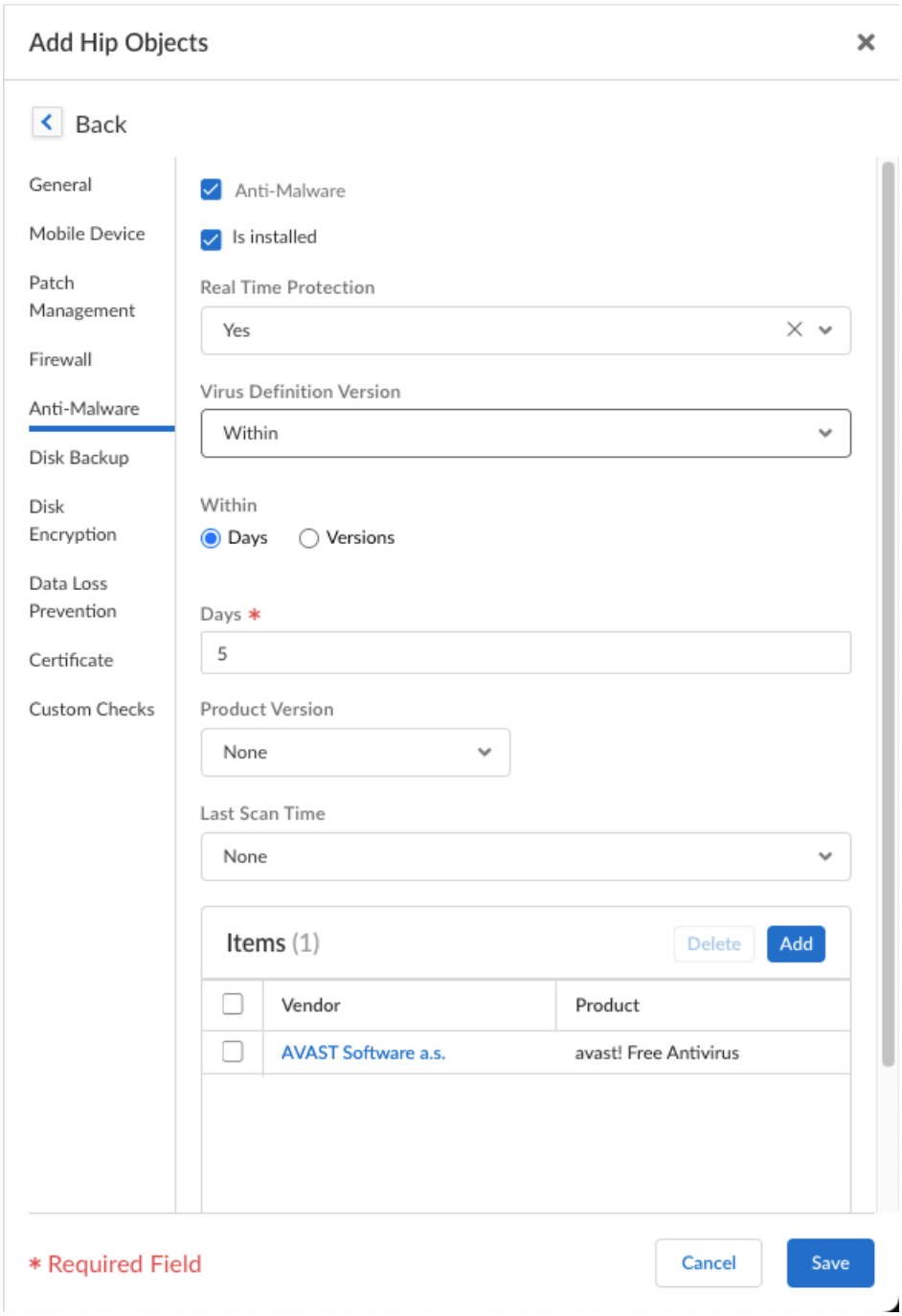
STEP 6 | 照合するホスト情報のカテゴリに対応するタブを選択し、チェック ボックスをオンにして、このカテゴリに対して照合するオブジェクトを有効にします。

たとえば、アンチウイルスまたはアンチスパイウェア ソフトウェアに関する情報を検索するオブジェクトを作成するには、**Anti-Malware**（アンチマルウェア） タブを選択し、次

©2025 Palo Alto Networks, Inc.

に**Anti-Malware**（アンチマルウェア） チェック ボックスをオンにして、対応するフィールドを利用できるようにします。フィールドに入力して、目的の一致条件を定義します。

たとえば、次の図は、エンドポイントにAVAST Free Antivirusソフトウェア アプリケーションがインストールされていて、**Real Time Protection**（リアルタイム保護）が有効であり、過去5日間に更新されたマルウェア定義がある場合に一致するHIPオブジェクトを作成する方法を示しています。



HIP オブジェクト内で、照合するカテゴリごとにこの手順を繰り返します。詳細は、表:データ収集カテゴリを参照してください。

©2025 Palo Alto Networks, Inc.

STEP 7 | HIPオブジェクトを保存して追加します 。

STEP 8 | HIPオブジェクトを管理するには、HIP通知テーブルから既存のオブジェクトを選択するか、「グローバル エージェント設定の編集」ページで 「追加」 をクリックしてHIP通知ウィンドウを開きます。

そこから、「**HIP**オブジェクトの管理」 をクリックして、構成したHIPオブジェクトのリストを表示します。HIPオブジェクトを選択して、 削除、複製、または移動することができます。

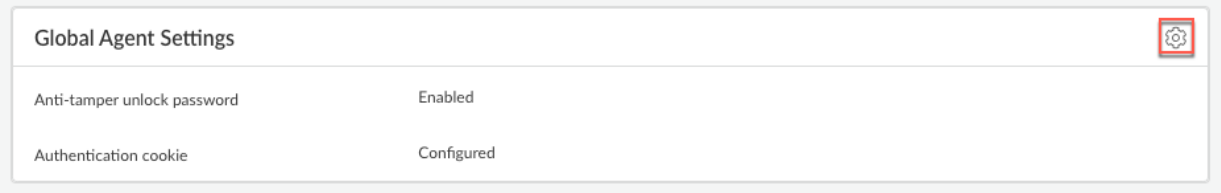
動的権限アクセスのための**HIP**プロファイルの作成と管理 **Prisma Access Agent**

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ モバイルユーザーサブスクリプション付きのPrisma Accessライセンス ❑ MacOS 12以降のデスクトップデバイスまたはWindows 10バージョン2024以降またはWindows 11デスクトップデバイス ❑ ロール:スーパーユーザー

HIPプロファイルは、ホスト情報プロファイルオブジェクトのコレクションです。モニタリングまたはセキュリティ ポリシー適用のために、まとめて評価されます。HIPプロファイルを作成すると、Booleanロジックを使用して、以前に作成したHIPオブジェクトとHIPプロファイルを組み合わせることができます。たとえば、作成したHIPプロファイルに対してトラフィック フローを評価し、一致か不一致かを判定することができます。一致がある場合、対応するポリシー ルールが適用されます。一致がなければ、他のポリシー一致条件と同様に、フローは次のルールと照合して評価されます。

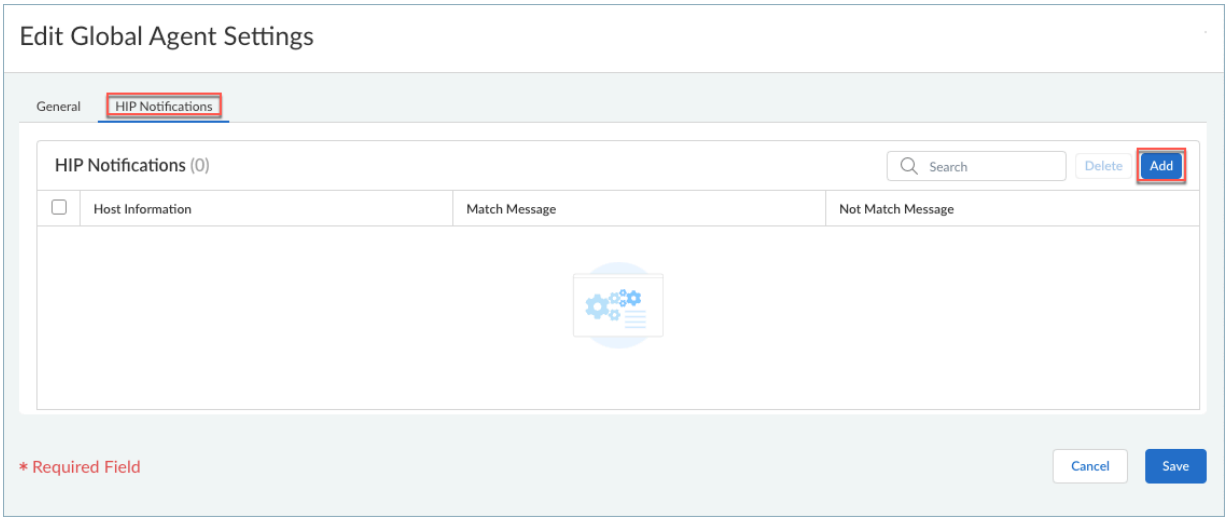
STEP 1 | Strata Cloud Manager から、**[**ワークフロー**] > [Prisma Access** セットアップ**] > [Access Agent] > [Prisma Access Agent]**を選択します。

STEP 2 | **Global Agent**設定を編集します。

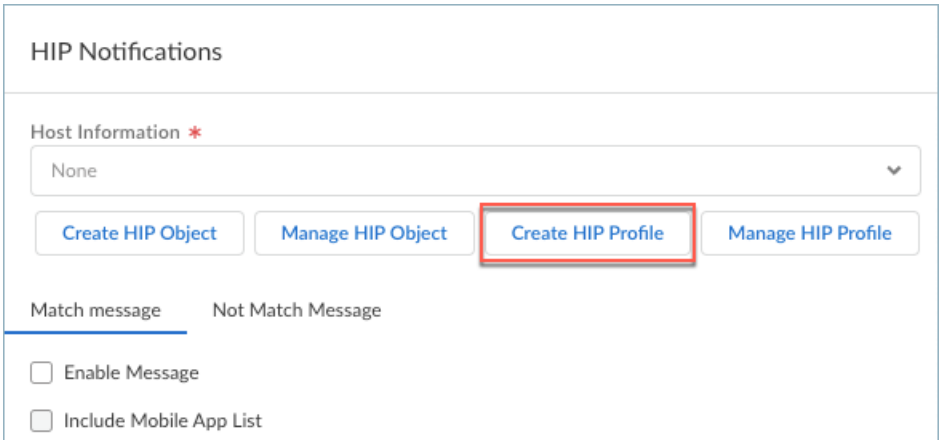


 ©2025 Palo Alto Networks, Inc.

STEP 3 | **[HIP通知]を選び[追加]をクリックします。**



STEP 4 | **[HIPプロファイルの作成]をクリックします。**



STEP 5 | **Name**（名前）および**Description**（説明）を入力してプロファイルを識別します。

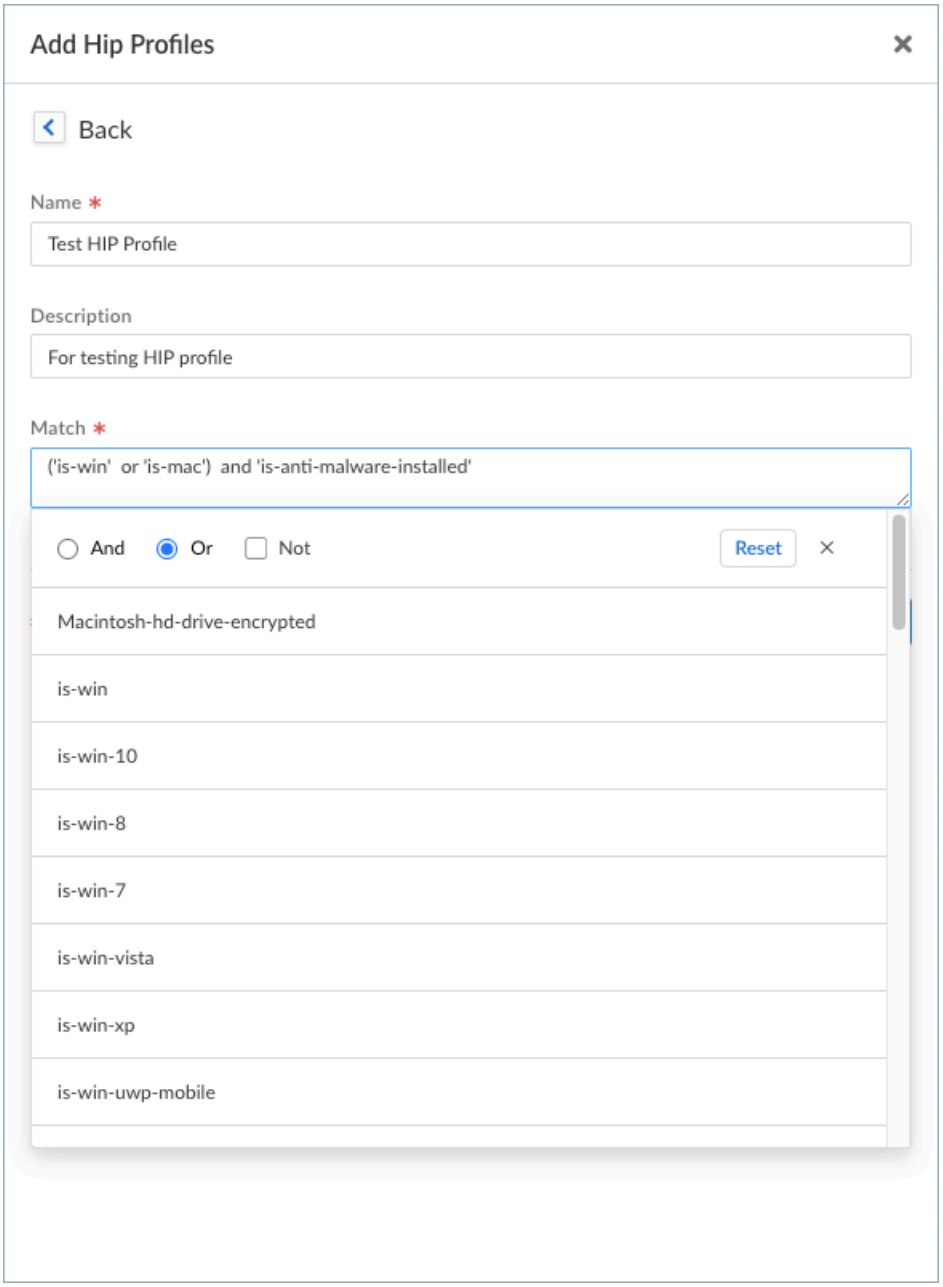
STEP 6 | [一致]フィールド内をクリックしてHIPプロファイルビルダーを開きます。

1. 一致条件として使用するHIPオブジェクトまたはプロファイルをリストから選択します。
2. ブール演算子（**And**、**And**）を選択します。オブジェクトの条件がフローに当てはまらない場合にのみ HIP プロファイルでオブジェクトを一致として評価する場合、オブジェクトを追加する前に、**Not** チェック ボックスをオンにします。
3. 最初のHIPオブジェクトに対して評価する別のHIPオブジェクトまたはプロファイルを選択します。

STEP 7 | 続けて、作成するプロファイルに必要なだけ一致条件を追加して、追加した条件の間に Boolean 演算子ラジオ ボタン（**And** または **And**）を選択します）ここでも必要に応じて **Not** チェック ボックスを使用します）。HIPプロファイルには、最大2,048文字まで入力できます。

©2025 Palo Alto Networks, Inc.

STEP 8 | 複雑なBoolean式を作成する場合は、**Match**（一致）テキスト ボックス内の適切な位置に手動で小括弧を追加して、HIPプロファイルが意図したロジックを使用して評価されるようにします。



STEP 9 | HIPプロファイルを保存して追加します 。

STEP 10 | HIPプロファイルを管理するには、HIP通知テーブルから既存のプロファイルを選択するか、「グローバル エージェント設定の編集」ページで **[追加]** をクリックしてHIP通知ウィンドウを開きます。

そこから**[HIP**プロファイルを管理]をクリックして、設定したHIPプロファイルのリストを表示します。HIPプロファイルを選択して、削除、複製、または移動することができます。ここからHIPプロファイルを追加することもできます。

©2025 Palo Alto Networks, Inc.

Prisma Access Agent設定をプッシュします。

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ モバイルユーザーサブスクリプション付きのPrisma Accessライセンス ❑ MacOS 12以降のデスクトップデバイスまたはWindows 10バージョン2024以降またはWindows 11デスクトップデバイス ❑ ロール:スーパーユーザー

Prisma Access Agent構成を完了した後、または構成を更新した後、構成をPrisma Accessにプッシュする必要があります。

コミットをプッシュする前に少なくとも*1*つのプロジェクトを作成してください。そうしないと、コミットは失敗します。

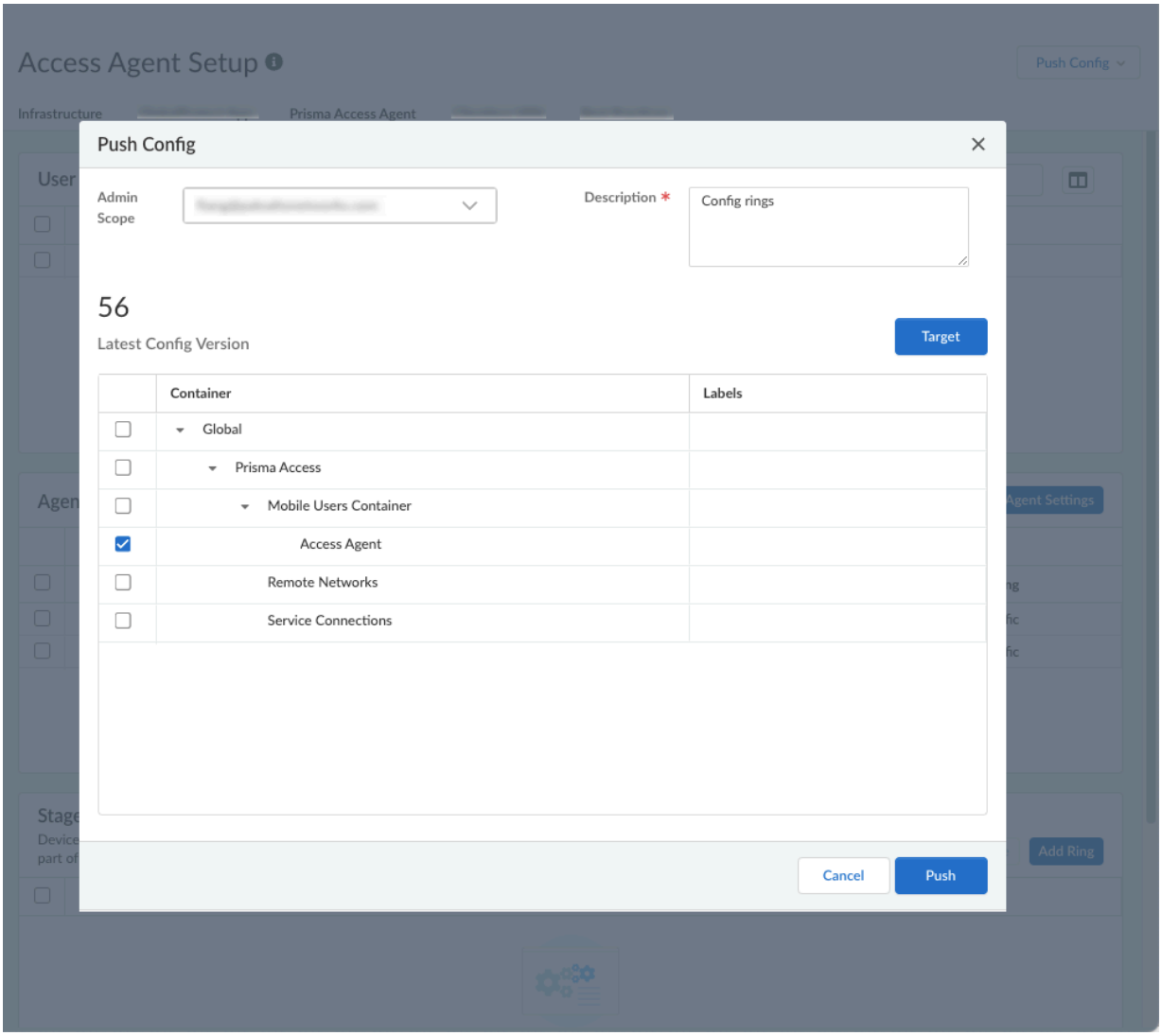
STEP 1 | [ワークフロー] > **Prisma Access**[セットアップ] > **[Access Agent]**を選択します。

STEP 2 | **[Push Config (**設定のプッシュ**)]** > **[Push (**プッシュ**)]**を選択します。

STEP 3 | ジョブの説明を入力します。

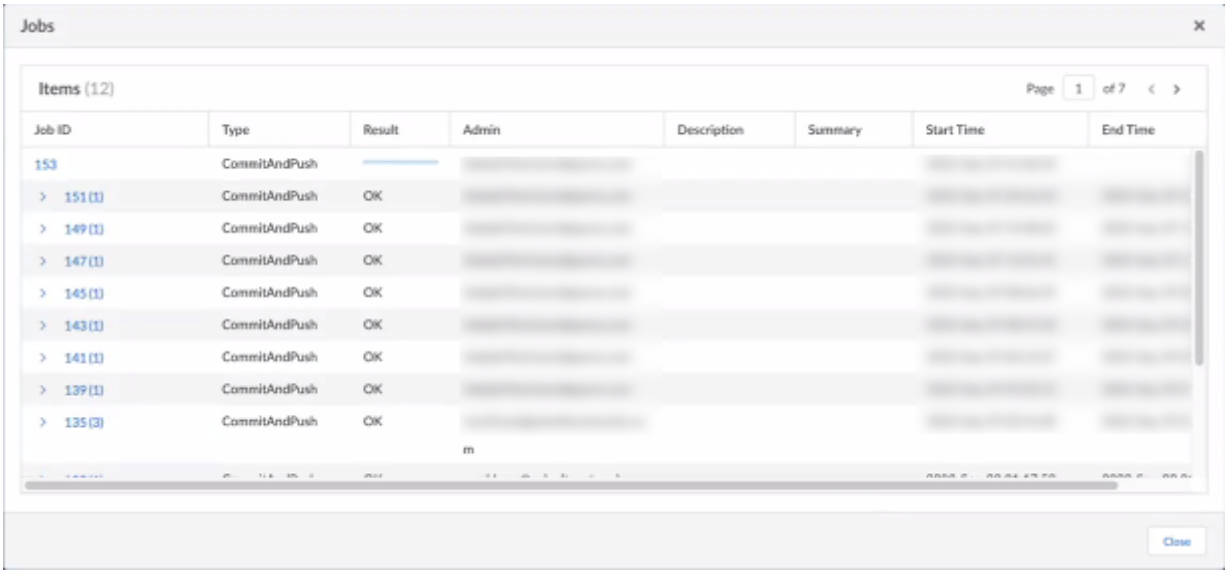
©2025 Palo Alto Networks, Inc.

STEP 4 | **[Global (グローバル)] > Prisma Access > [Mobile Users (モバイルユーザー)] > [Access Agent]** コンテナを選択し、**[Push (プッシュ)]**をクリックします。



 ©2025 Palo Alto Networks, Inc.

STEP 5 | ジョブが完了するまで待ってから、「ジョブ」ダイアログを閉じます 。



 ©2025 Palo Alto Networks, Inc.

動的特権アクセス有効化Prisma Access Agentパッケージをダウンロードする

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 Innovation ❑ モバイルユーザーサブスクリプション付きのPrisma Accessライセンス ❑ ロール:スーパーユーザー

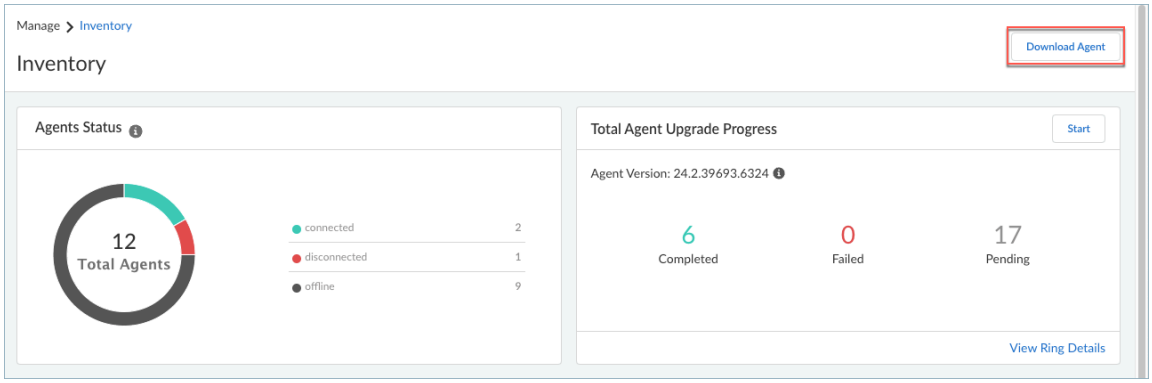
Prisma Access Agentとプロジェクト固有のPrisma Access Agent設定を行った後、Prisma Access Agentパッケージをダウンロードして、エンドユーザーがダウンロードしてインストールできるようにすることができます。

さらに、設定ファイルをダウンロードしたことを確認してください。エージェントとプロジェクト固有のエージェント設定は、Prisma AccessのテナントIDとサーバードメインとともにPrisma Access Agent設定ファイルに保存されます。この設定ファイルは、Prisma Access Agentのインストールと登録の際に使用されます。

©2025 Palo Alto Networks, Inc.

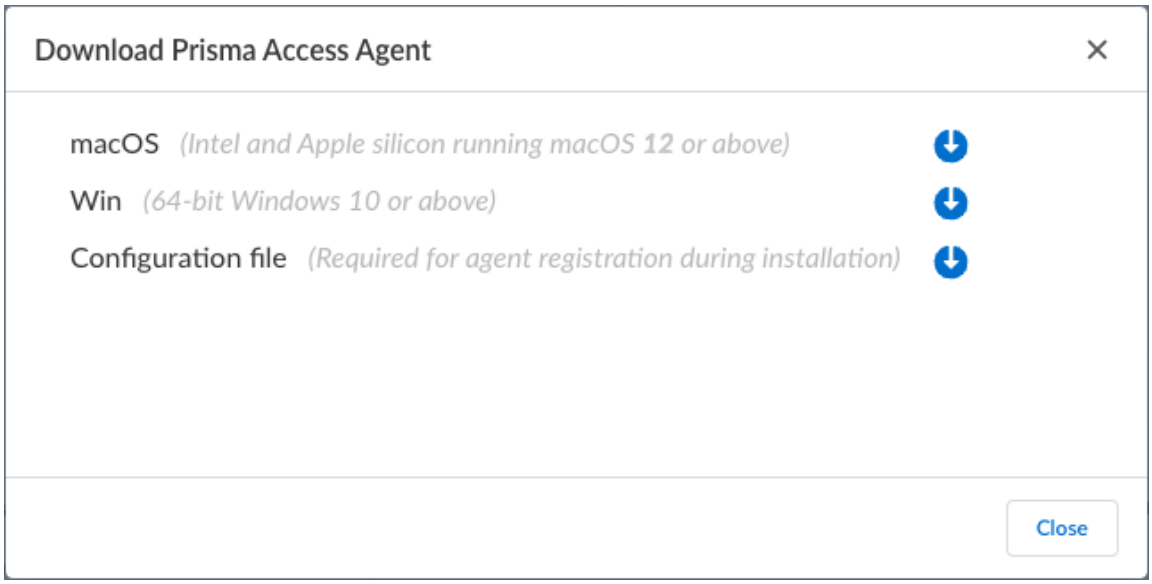
STEP 1 | Prisma Access Agentパッケージと設定ファイルをダウンロードします。

1. **[Manage (管理)]** > **Prisma Access Agent** > **[Inventory (インベントリ)]**を選択します。
2. エージェントをダウンロードをクリックします。



3. ダウンロードしたい項目に対応する下矢印をクリックします。

   設定ファイルは、Prisma Access Agentのインストールと登録の際に使用されるため、必ずダウンロードしてください。



4. パッケージをシステム上の場所に保存し、[エージェントのダウンロード] ダイアログを閉じます 。

STEP 2 | 組織のネットワーク内の中央の場所にパッケージをアップロードするか、エンドユーザーがPrisma Access Agentをダウンロードしてインストールできるように、パッケージを配信します。

©2025 Palo Alto Networks, Inc.

Prisma Access Agentを使用してプロジェクトにアクセスする

どこで使用できますか?	何が必要ですか?
• Prisma Access Agent	❑ MacOS 12以降のデスクトップデバイスまたはWindows 10バージョン2024以降またはWindows 11デスクトップデバイス ❑ インターネット アクセス

顧客プロジェクトにアクセスできるユーザーを制御する必要がある IT または IT 対応サービス (ITES) 企業の場合、動的権限アクセスは、ユーザーが割り当てられたプロジェクトにのみアクセスできるように、シームレスで安全な区分化された方法を提供します。

管理者がPrisma AccessとPrisma Access Agentに動的な特権アクセスを設定した場合、Prisma Access Agentを使って自分がアサインされたプロジェクトにアクセスし、作業することができます。

プロジェクトにログインすると、組織のネットワーク、ネットワーク内のリソース、またはプロジェクトに固有のサービスとしてのソフトウェアアプリケーションにアクセスできます。次の方法をご覧ください。

- 動的特権アクセスに対応したPrisma Access Agentにログインします。
- 接続状況の確認
- ダイナミックプリビレッジアクセスを有効にしたPrisma Access Agentの環境設定を変更します。
- 別のPrisma Accessロケーションに接続する
- アプリの通知を見る

また、別のプロジェクトにアサインされた場合は、別のプロジェクトに切り替えたり、Prisma Access Agentを別のサーバーに接続したりすることができます。

Prisma Access Agentをインストールします

どこで使用できますか?	何が必要ですか?
• Prisma Access Agent	❑ 管理者権限が付与されている、MacOS 12以降のデスクトップデバイスまたはWindows 10バージョン2024以降またはWindows 11デスクトップデバイス ❑ インターネット アクセス

©2025 Palo Alto Networks, Inc.

管理者があなたのデバイスにPrisma Access Agentをプッシュしなかった場合は、手動でMacOSまたはWindowsデバイスにPrisma Access Agentをインストールすることができます。

*Prisma Access Agent*と*GlobalProtect*アプリケーションは同じデバイス上に共存できるが、*Prisma Access*に接続できるのはどちらか一方のみです。お使いのデバイスに*GlobalProtect*アプリケーションもインストールされ、有効になっている場合、*Prisma Access Agent*のインストールは自動的に*GlobalProtect*アプリケーションを無効にします。*Prisma Access Agent*をインストールした後、*GlobalProtect*アプリケーションを使用するには、GlobalProtectアプリケーションに切り替える必要があります。

- macOS
- Windows

Prisma Access Agent(MacOS) をインストールします。

MacOSデバイスにPrisma Access Agentを手動でインストールするには:

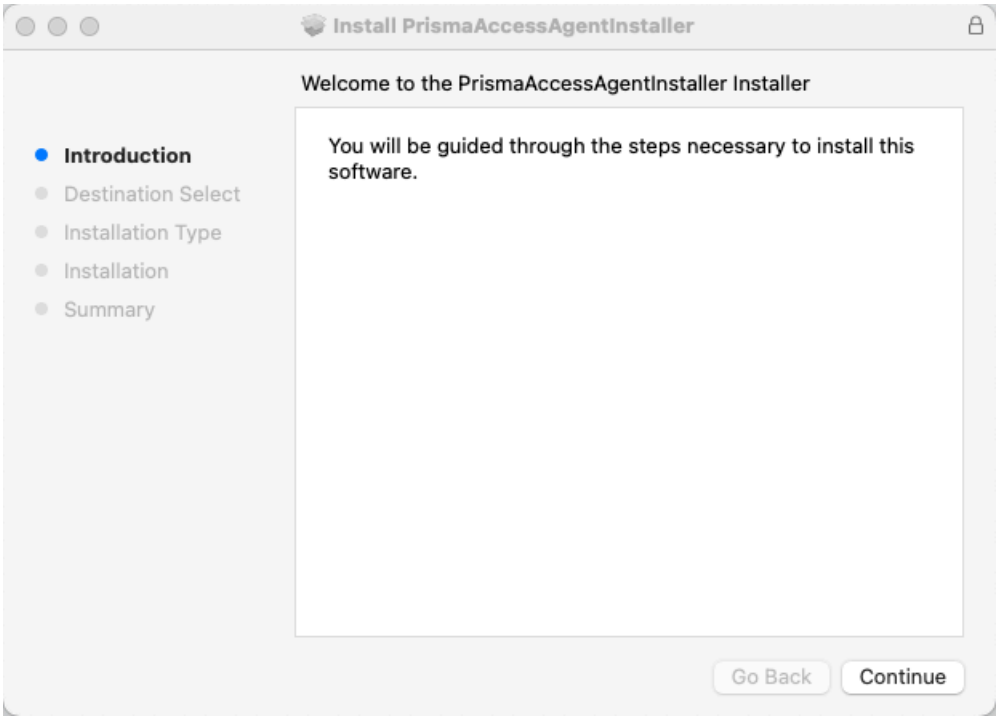
STEP 1 | 管理者から提供されたPrisma Access Agentパッケージを入手します。パッケージ名の形式は次のとおりです。

```
PrismaAccessAgentInstaller_<version>.pkg
```

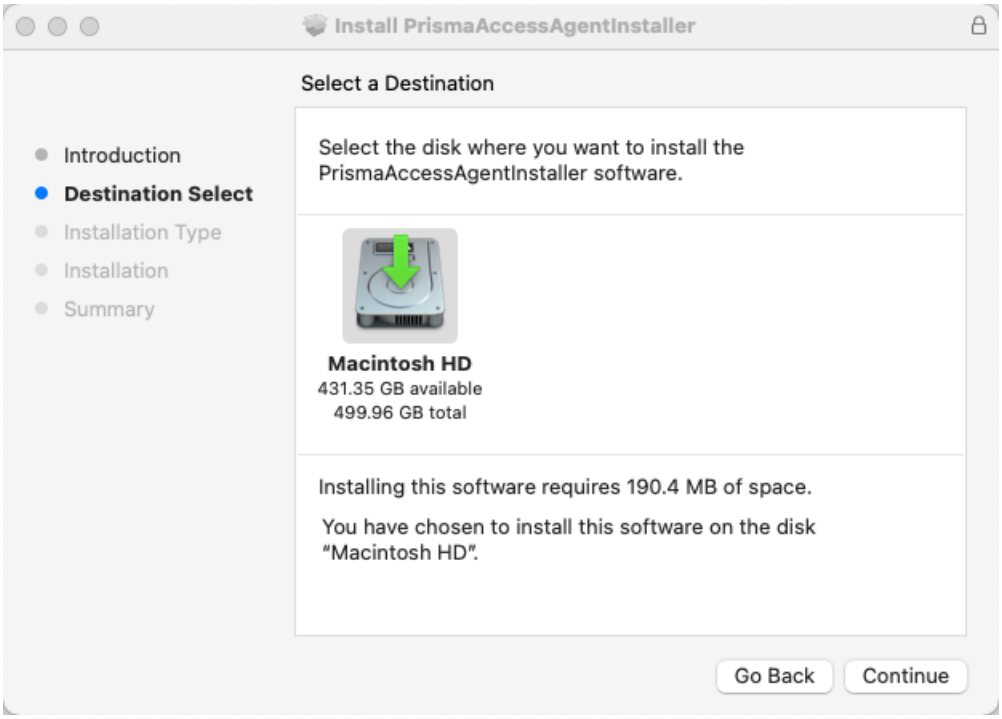

©2025 Palo Alto Networks, Inc.

STEP 2 | ダウンロード フォルダー (またはインストール パッケージを配置した場所) でインストール パッケージを開き、プロンプトに従ってPrisma Access Agentをインストールします。

1. インストーラーから、[続行]をクリックします。

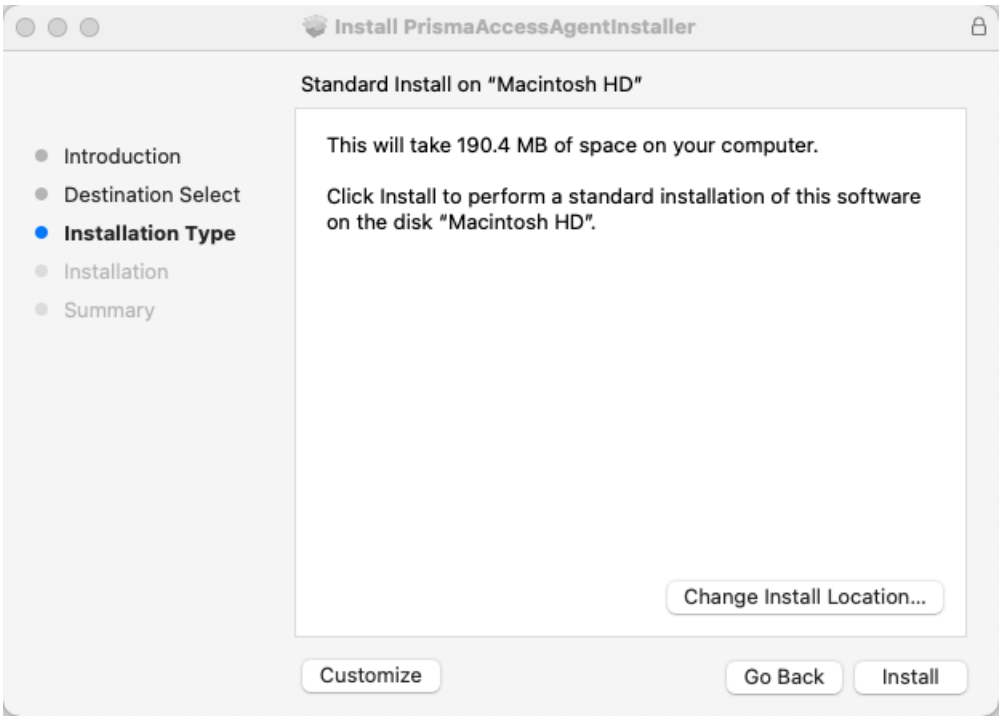


2. Prisma Access Agentをインストールするフォルダーを選択し、[続行]をクリックします。



3. 「インストール タイプ」ページの情報を確認し、[インストール]をクリックします。

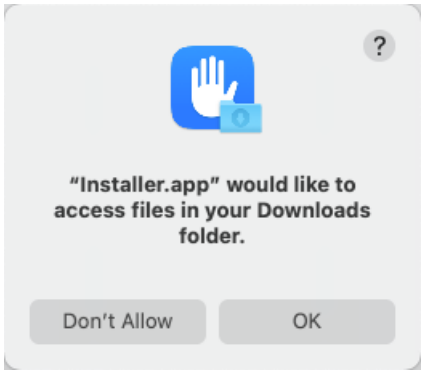
 ©2025 Palo Alto Networks, Inc.



4. プロンプトが表示されたら、 ユーザー名とパスワードを入力し、[ソフトウェアのインストール]をクリックしてインストールを開始します。

   または、Touch ID (有効になっている場合) を使用してこの手順を完了することもできます。

5. インストール パッケージをダウンロードしたフォルダー内のファイルにインストーラーがアクセスできるようにするかどうかを確認するメッセージが表示されたら、**[OK]**をクリックします。



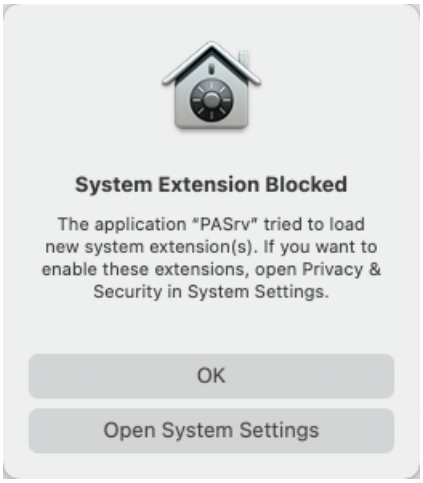
6. デフォルトでは、MacOSはPrisma Access Agentシステム拡張機能をブロックします。管理者がPrisma Access Agentに次のトラフィック転送ルールを設定した場合、システム拡張機能またはネットワーク拡張機能が表示されます。

   - スプリット トンネリング - ネットワーク トラフィックをPrisma Access接続経由または接続外に送信します。
   - スプリットDNS - ネットワーク トラフィックに加えて、Prisma Access経由またはPrisma Access外部でアプリケーションとリソースのDNSクエリを送信します。

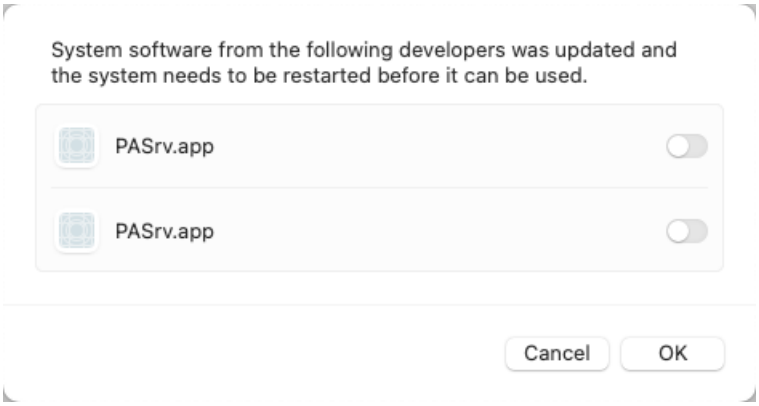
©2025 Palo Alto Networks, Inc.

Prisma Access Agentを動作させるには、システム拡張機能を有効にする必要があります。

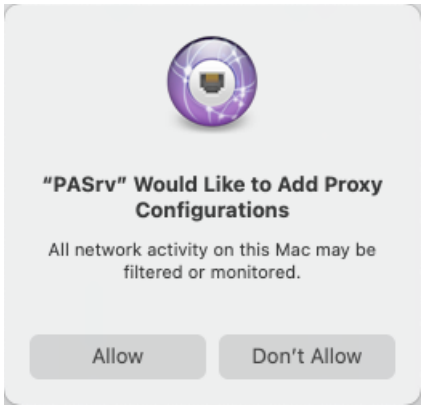
1. [システム設定を開く]をクリックします。



2. [プライバシーとセキュリティ] ウィンドウで、[一部のシステム ソフトウェアは使用前に注意が必要です]の [詳細] をクリックします。
3. 両方の**PASrv.app** アプリを有効にして、**[OK]**をクリックします。



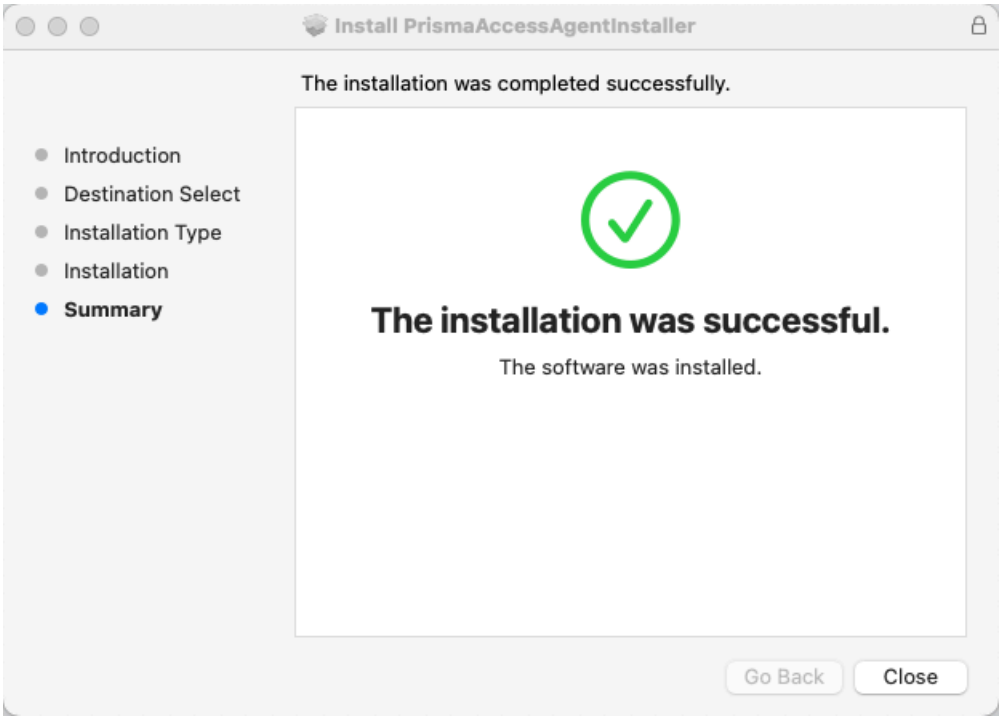
7. 管理者がネットワーク アクセスにPrisma Access接続を強制する機能を有効にしている場合は、ネットワーク コンテンツをフィルターするための構成を追加するように求められます。続行するには、[許可]をクリックします。



©2025 Palo Alto Networks, Inc.

これを許可すると、Prisma Access Agent はセキュリティ上の目的でネットワーク接続をフィルタリングおよび監視します。

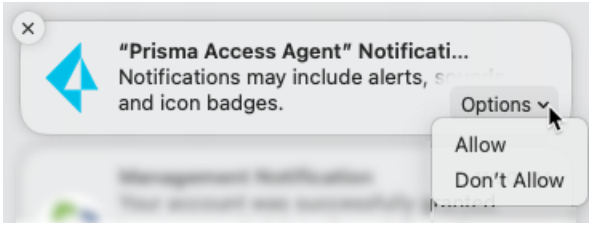
8. インストール完了後、ウィザードを閉じます。



9. 管理者が、Prisma Accessエージェントとともに Autonomous DEMエージェントをインストールするようにエージェントを構成した場合は、**[OK]** をクリックして再度プロンプトが表示されないようにします。
10. Prisma Access Agent通知ポップアップをクリックして、通知設定ウィンドウを開きます。

STEP 3 | プロンプトが表示されたら、Prisma Access Agent通知を有効にします。

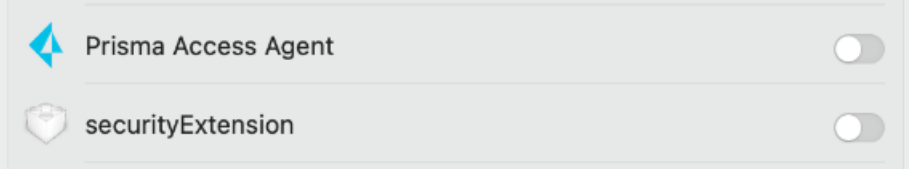
Prisma Access Agent通知ポップアップがデスクトップに表示されたら、ポップアップの上にカーソルを移動し、[オプション] > [許可]を選択します。



©2025 Palo Alto Networks, Inc.

STEP 4 | Prisma Access AgentがSafariブラウザのデータにアクセスするには、セキュリティ拡張機能とPrisma Access Agentにフルディスク アクセスを許可する必要があります。

1. MacOSから、[システム設定] > [プライバシーとセキュリティ] > [フルディスク アクセス]を選択します。アプリのリストから**Prisma Access Agent**と**securityExtension**を有効にします。



2. プロンプトが表示されたら、変更を有効にするためにPrisma Access Agentを終了して再度開きます 。

Prisma Access Agentをインストールする **(MacOS)**

Prisma Access Agent を使用する必要がなくなった場合は、手動でアンインストールできます。エージェントをアンインストールすると、企業ネットワークにアクセスできなくなり、エンドポイントが組織のセキュリティ ポリシーによって保護されなくなることに注意してください。

開始する前に、管理者が Prisma Access Agent の改ざん防止機能を有効にしている場合は、管理者から改ざん防止ロック解除パスワードを取得する必要があります。エージェントをアンインストールするには、管理者権限が必要です。

コマンドライン インターフェイスから Prisma Access Agent をアンインストールするには、次の手順を実行します。

STEP 1 | MacOSデバイスでは、ターミナル ウィンドウを開き、次のコマンドを実行します。

```
sudo /Applications/Prisma\ Access\ Agent.app/Contents/Helpers/
uninstaller
```

STEP 2 | プロンプトが表示されたら管理者パスワードを入力します。

STEP 3 | スーパーバイザーパスワードの入力を求められた場合は、改ざん防止ロック解除パスワードを入力します。それ以外の場合は、**Enter** キー を押してアンインストールを開始します。

Prisma Access Agent とその拡張機能は削除されます。

Prisma Access Agent (Windows) をインストールします

WindowsデバイスにPrisma Access Agentを手動でインストールします。

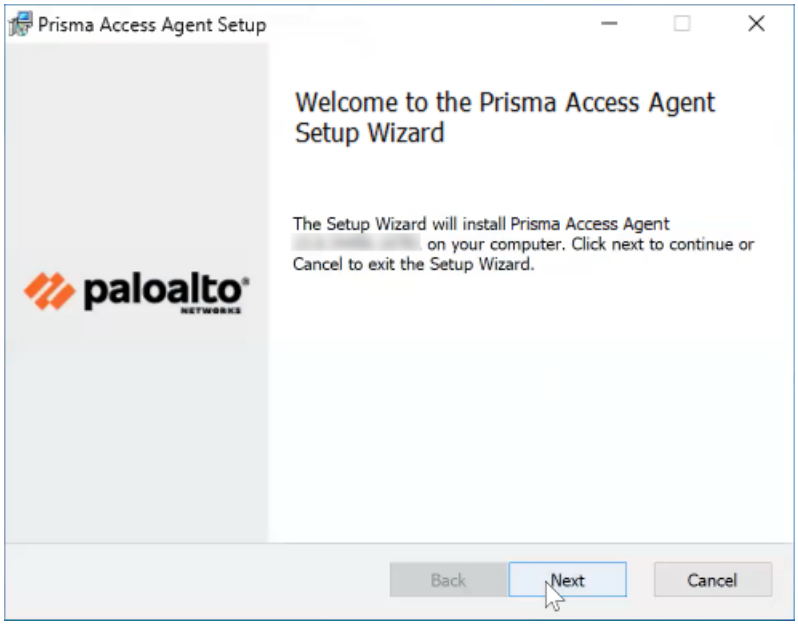
STEP 1 | 管理者から提供されたPrisma Access Agentパッケージを入手します。パッケージ名の形式は次のとおりです。

`PrismaAccessAgent_x64_<version>.msi`

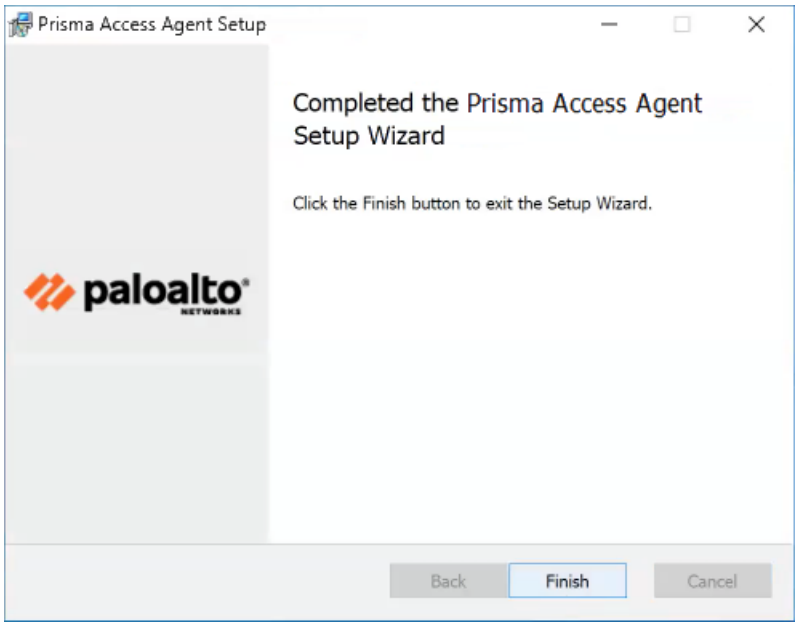
©2025 Palo Alto Networks, Inc.

STEP 2 | ダウンロード フォルダー (またはインストール パッケージを配置した場所) で、インストール パッケージ アイコンをダブルクリックし、プロンプトに従ってPrisma Access Agentをインストールします。

1. セットアップウィザードが表示されたら、[次へ] をクリックして続行します。



2. エンドユーザー使用許諾契約書を確認し、[使用許諾契約書の条項に同意します]を選択して、[次へ]をクリックします。
3. **Install**（インストール）をクリックし、インストールを開始します。
4. このアプリがデバイスに変更を加えることを許可するかどうかを確認するメッセージが表示されたら、[はい]をクリックします。
5. インストールが完了したら、[完了]をクリックします。



©2025 Palo Alto Networks, Inc.

6. 管理者が、Prisma AccessエージェントとともにAutonomous DEMエージェントをインストールするようにエージェントを構成した場合は、**[OK]** をクリックして再度プロンプトが表示されないようにします。

Prisma Access Agentをインストールする (Windows)

Prisma Access Agentは、不要になった場合は手動でアンインストールできます。エージェントをアンインストールすると、企業ネットワークにアクセスできなくなり、組織のセキュリティポリシーによってエンドポイントが保護されないことに注意してください。

始める前に、プリズマアクセスエージェントで改ざん防止機能が有効になっている場合は、管理者から改ざん防止ロック解除パスワードを入手する必要があります。エージェントをアンインストールするには、管理者権限が必要です。

Prisma Access Agentをアンインストールするには、次の手順を実行します。

STEP 1 | Prisma Access Agentを有効にする

1. コマンドプロンプトウィンドウで次のコマンドを実行します。

```
"C:\Program Files\Palo Alto Networks\Prisma Access Agent
\pacli" traffic show
```

2. スーパーバイザのパスワードの入力を求められたら、改ざん防止ロック解除パスワードを入力します。

STEP 2 | 設定からプリズマアクセスエージェントをアンインストールします。

- Windows の場合:
  1. ［スタート］メニューを開きます。
  2. [設定] > アプリ] > インストール済みアプリを選択します。
  3. [**Prisma Access Agent**]までスクロールします。
  4. [その他のオプション > のアンインストール]を選択します。
  5. アンインストールを続行するかどうかの確認メッセージが表示されたら、「はい」をクリックします。
- Windows の場合:
  1. ［スタート］メニューを開きます。
  2. [設定] > アプリ] > アプリと機能を選択します。
  3. [**Prisma Access Agent**]までスクロールします。
  4. [その他 > アンインストール]を選択します。
  5. アンインストールを続行するかどうかの確認メッセージが表示されたら、「はい」をクリックします。

©2025 Palo Alto Networks, Inc.

ダイナミック特権アクセス有効化Prisma Access Agentにログインする。

どこで使用できますか?	何が必要ですか?
• Prisma Access Agent	☐ MacOS 12以降のデスクトップデバイスまたはWindows 10バージョン2024以降またはWindows 11デスクトップデバイス ☐ インターネット アクセス

組織のネットワーク、リソース、SaaSアプリケーション、またはインターネットにアクセスするには、ログイン資格情報を使用してPrisma Access Agentにログインします。

Prisma Access Agentにログインすると、最適なPrisma Accessの場所 (ゲートウェイと呼ばれることもあります) を使用してネットワークに自動的に接続されます。通常、ベストロケーションは、最高のパフォーマンスの提供が可能なように自動で選択され、使用者の母語でのＷｅｂサイトの閲覧などのユーザーエクスペリエンスの向上に貢献します。デバイスが組織のネットワーク外にある場合、エージェントはネットワークへの接続時に最高のパフォーマンスが得られる最適な場所を見つけます。

開始する前に、Prisma Access Agentをデバイスにインストールする必要があります。通常、管理者は、組織のネットワーク、リソース、アプリケーションにアクセスするために使用するデバイスにPrisma Access Agentをデプロイします。エージェントは、管理者が定義したポリシー ルールに従って構成され、デバイスにデプロイされます。ただし、管理者がPrisma Access Agentをデバイスにデプロイしていない場合は、Prisma Access Agentを手動でインストールする必要があります。

Prisma Accessが組織でどのようにセットアップされているかに応じて、管理者は以下のログイン情報を提 供する必要があります：

- Prisma Access Agentを管理するサービスをホストするPrisma Accessサーバーの名前。Prisma Accessの設定によっては、複数のサーバーが存在することもある。
- 組織で*Dynamic Privilege Access* (ダイナミック特権アクセス)を使用している場合、あなたが担当するプロジェクト名。Dynamic Privilege Access (ダイナミック特権アクセス)を使用すると、割り当てられたプロジェクトに基づいて組織のネットワークとリソースにアクセスできるため、誤って別のプロジェクトのリソースにアクセスすることはありません。複数のプロジェクトを担当することになった場合でも、簡単にプロジェクトを切り替えることができます。

オペレーティングシステムの設定に応じて、アプリアイコンとアプリのインターフェースがダークモードとライトモードで表示されます。

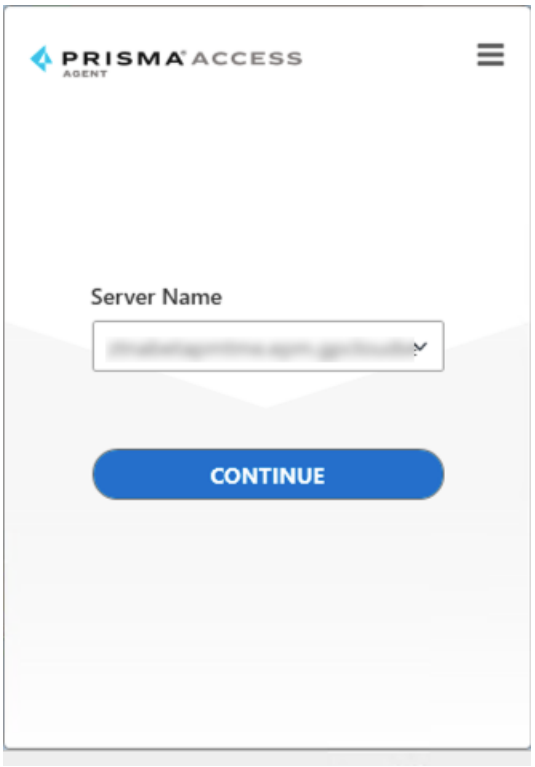
次の手順を実行して、Prisma Access Agentにログインします。

STEP 1 | MacOSメニューバーまたはWindowsタスクバーから Prisma Access Agentアイコンをクリックしてプリズマ Access Agentを起動します。

©2025 Palo Alto Networks, Inc.

STEP 2 | プロンプトが表示されたら、管理者が指定したPrisma Accessサーバーのサーバー名を入力または選択し、[続行]をクリックします。

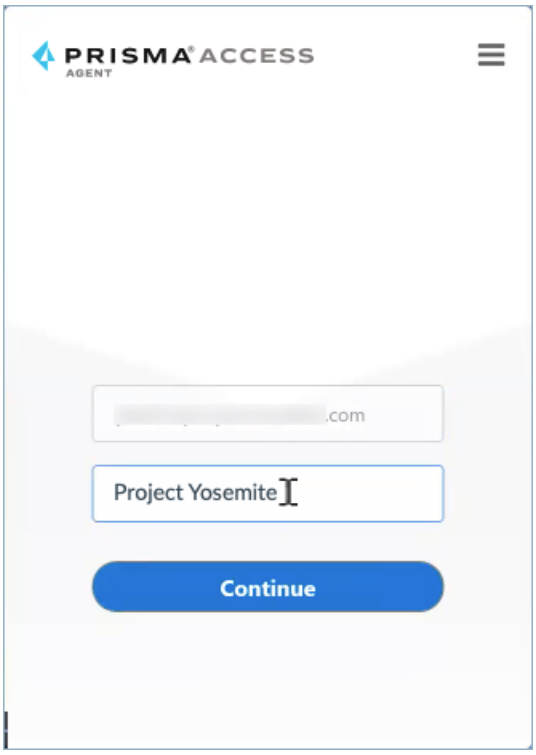
サーバー名の形式は**<example.domain.com>**で、**https://**プロトコルはありません。サーバー名の最大長は256文字です。



©2025 Palo Alto Networks, Inc.

STEP 3 | 管理者から送信されたプロジェクト名を入力し、続行します。

プロジェクト名の最大長は32文字です。



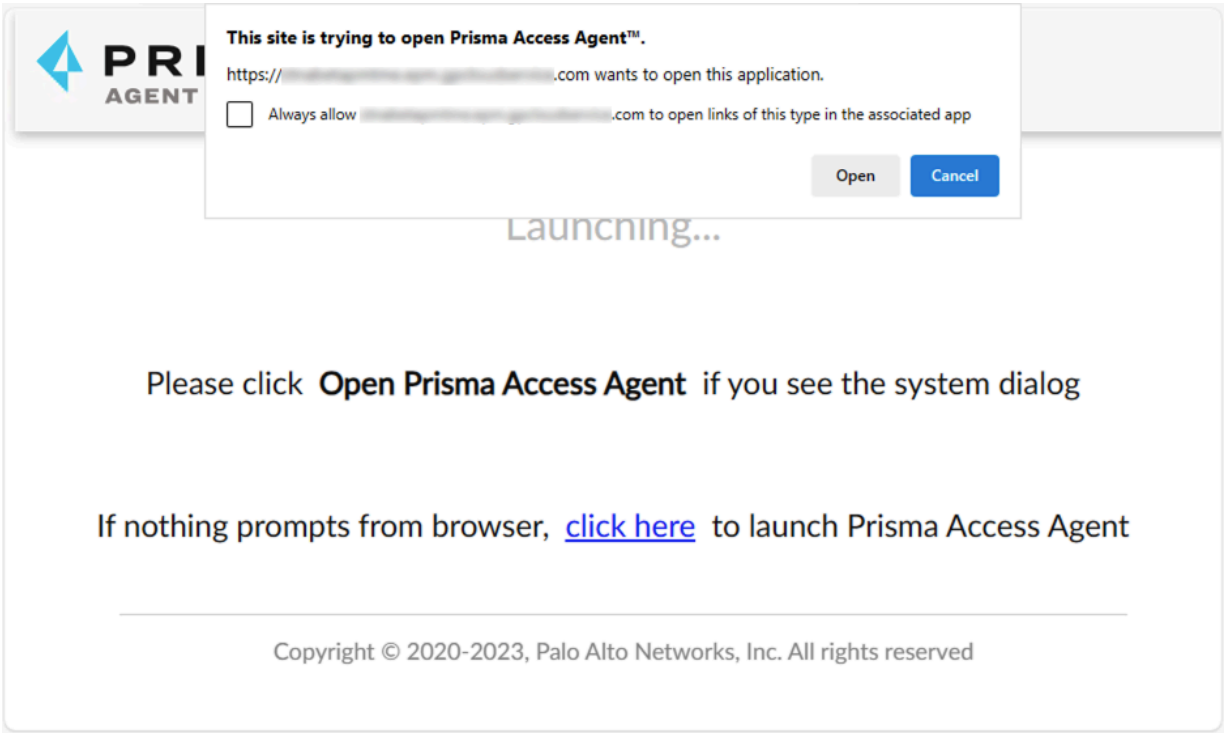
STEP 4 | デフォルトのWebブラウザーに表示されるログイン ページで、組織のログイン資格情報を入力して、OktaやAzure Active Directory (AD) などの組織のシングル サインオン (SSO) アプリにサインインします。

管理者が多要素認証 (MFA) を有効にしている場合は、ログイン時にブラウザで追加の検証を完了する必要があります。

©2025 Palo Alto Networks, Inc.

STEP 5 | Web ブラウザにプロンプトが表示されたら、[開く]をクリックします。

次回ログイン時にブラウザにプロンプトを表示したくない場合は、「常に許可」**<site>**を選択します。これらの種類のリンクを関連付けられたアプリで開くには、[開く] をクリックします (デフォルトのWebブラウザーでサポートされている場合)。

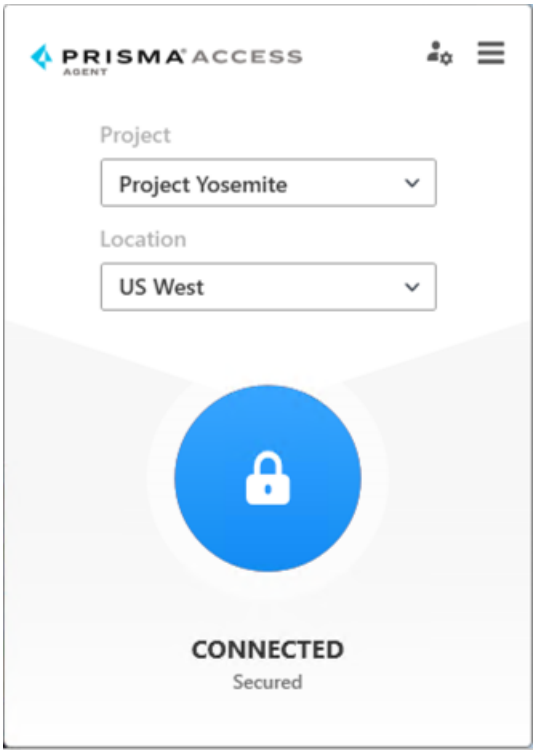


STEP 6 | Prisma Access AgentがPrisma Accessに接続するまで待ちます。



 ©2025 Palo Alto Networks, Inc.

STEP 7 | ログインに成功すると、利用可能な最適なPrisma Accessの場所に自動的に接続されます。プロジェクトを使用してサイン インした場合は、プロジェクトに最適な場所に接続されます。



インターネットへの安全なアクセスに加えて、組織のリソースやSaaSアプリにアクセスできるようになりました。

管理者が*Prisma Access Agent*の常時オ ンモードを有効にしている場合、組織のポリシーにより、*Prisma Access*から切断することはできません。ただし、*Prisma Access*の場所を変更することは可能です。

管理者が*Prisma Access Agent*のオンデマンド モードを有効にしている場合、*Prisma Access*に接続するにはロック・アイコンをクリックする必要があります。

動的権限アクセスの設定を変更して有効にする Prisma Access Agent

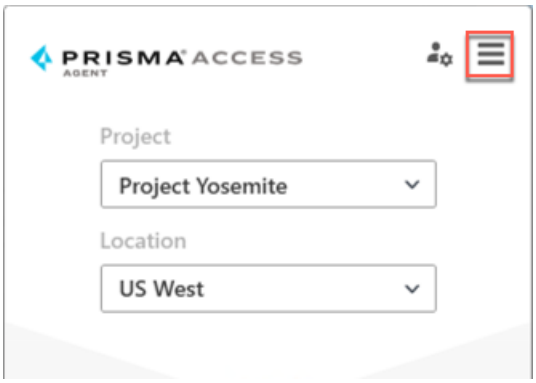
どこで使用できますか?	何が必要ですか?
• Prisma Access Agent	☐ MacOS 12以降のデスクトップデバイスまたはWindows 10バージョン2024以降またはWindows 11デスクトップデバイス ☐ インターネット アクセス

©2025 Palo Alto Networks, Inc.

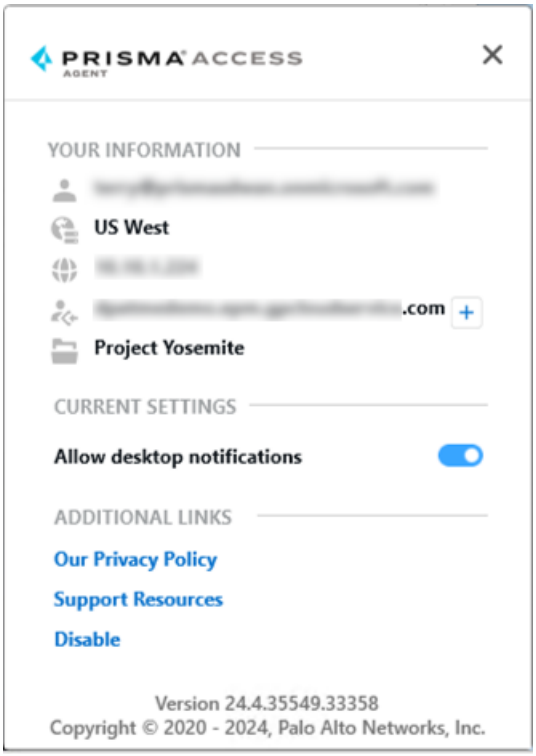
Prisma Access Agent設定ウィンドウを使用して、デバイスに関する情報の表示や、デスクトップ通知の有効化などのエージェントのオプションを変更できます。

STEP 1 | MacOSメニューバーまたはWindowsタスクバーから Prisma Access Agentアイコンをクリックして Prisma Access Agentを起動します。

STEP 2 | ハンバーガー メニューをクリックして設定ウィンドウを開きます。



STEP 3 | 設定ウィンドウでは、次の情報を表示できます。



Icon（アイコン）	詳説
	あなたのユーザーID。
	お使いのデバイスが接続されているPrisma Accessロケーション。

©2025 Palo Alto Networks, Inc.

Icon（アイコン）	詳説
	Prisma AccessロケーションのIPアドレス。
	接続している管理インターフェイス (サーバー) のホスト名または IP アドレス。プラス (+) アイコンをクリックすると、別のサーバーに接続できます。
	にサインインしているプロジェクト。

STEP 4 | メニューバー（MacOSの場合）またはタスクバー（Windowsの場合）でPrisma Access Agent通知を受け取るには、デスクトップ通知を許可します。この設定はデフォルトで有効になっています。

デスクトップ通知は、インストール時に設定した「応答不可」設定に従います。インストール時に、オペレーティング システムによってPrisma Access Agentからの通知を許可するように求められます。

STEP 5 | Prisma Access Agent が収集するデータとその情報の使用方法について詳しくは、当社のプライバシー ポリシーをご覧ください。

STEP 6 | Prisma Access Agentで発生する可能性のある問題についてのサポートを受けるには、[サポート リソース]をクリックします。

STEP 7 | 管理者が許可している場合は、Prisma Access Agentを サインアウトする ことができます。

STEP 8 | 管理者がこの機能を有効にしている場合は、Prisma Access Agentを無効にして、GlobalProtectアプリケーション に切り替えることができます (デバイスにインストールされている場合)。

STEP 9 | お使いのPrisma Access Agentのバージョンを表示します。

STEP 10 | ウィンドウを閉じるには、**X**をクリックします。

ダイナミック特権アクセス有効Prisma Access Agentを別の場所に接続する

どこで使用できますか?	何が必要ですか?
• Prisma Access Agent	❑ MacOS 12以降のデスクトップデバイスまたはWindows 10バージョン2024以降またはWindows 11デスクトップデバイス ❑ インターネット アクセス

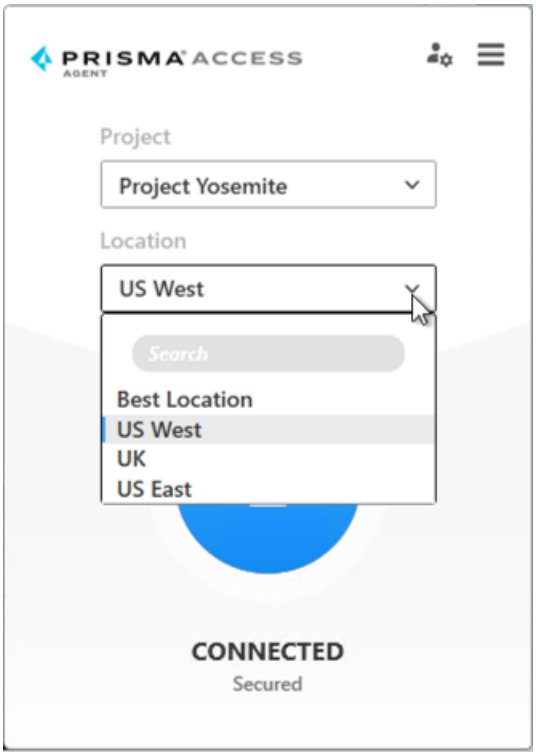
©2025 Palo Alto Networks, Inc.

Prisma Access Agentにログインすると、利用可能な最高のPrisma Accessロケーションに自動的に接続されます。ロケーションの変更は、ゲートウェイのドロップダウンで実行できます。

STEP 1 | MacOSメニューバーまたはWindowsタスクバーから Prisma Access Agentアイコンをクリックしてを起動します。

STEP 2 | 別のロケーションを選択します。場所を検索するか、リストから場所を選択することができます。

利用可能なロケーションのリストは、応答時間、可用性、その他の要素に基づいて、最適なエクスペリエンスに従って並べ替えられます。最高のエクスペリエンスを提供するロケーションが **Best Location (**ベストロケーション**)**として表示されます。



STEP 3 | 管理者がPrisma Access Agentのオンデマンドモードを有効にしている場合は、ロック アイコンをクリックして、新しく選択した場所に接続します。そうでなければ、Prisma Access Agentはロケーションを変更します。

別のプロジェクトへの切り替える

どこで使用できますか?	何が必要ですか?
• Prisma Access Agent	❑ MacOS 12以降のデスクトップデバイスまたはWindows 10バージョン2024以降またはWindows 11デスクトップデバイス ❑ インターネット アクセス

©2025 Palo Alto Networks, Inc.

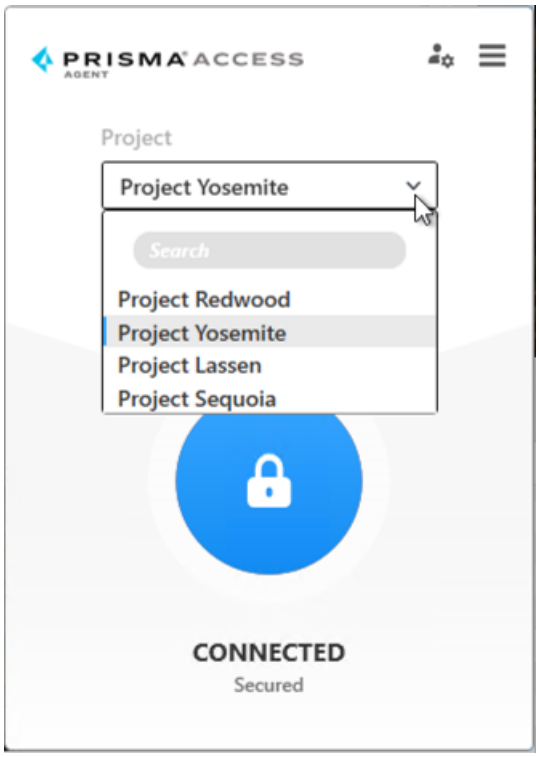
組織内の複数のプロジェクトに割り当てられている場合は、別のプロジェクトに切り替えて、そのプロジェクトに関連付けられたネットワークとリソースにアクセスできます。

切り替えようとしているプロジェクトが別のサーバーからアクセスできる場合は、まずそのサーバーに切り替える必要があります。

STEP 1 | MacOSメニューバーまたはWindowsタスクバーから Prisma Access Agentアイコンをクリックして Prisma Access Agentを起動します。

STEP 2 | 別のプロジェクトを選択します。場所を検索するか、リストから場所を選択することができます。

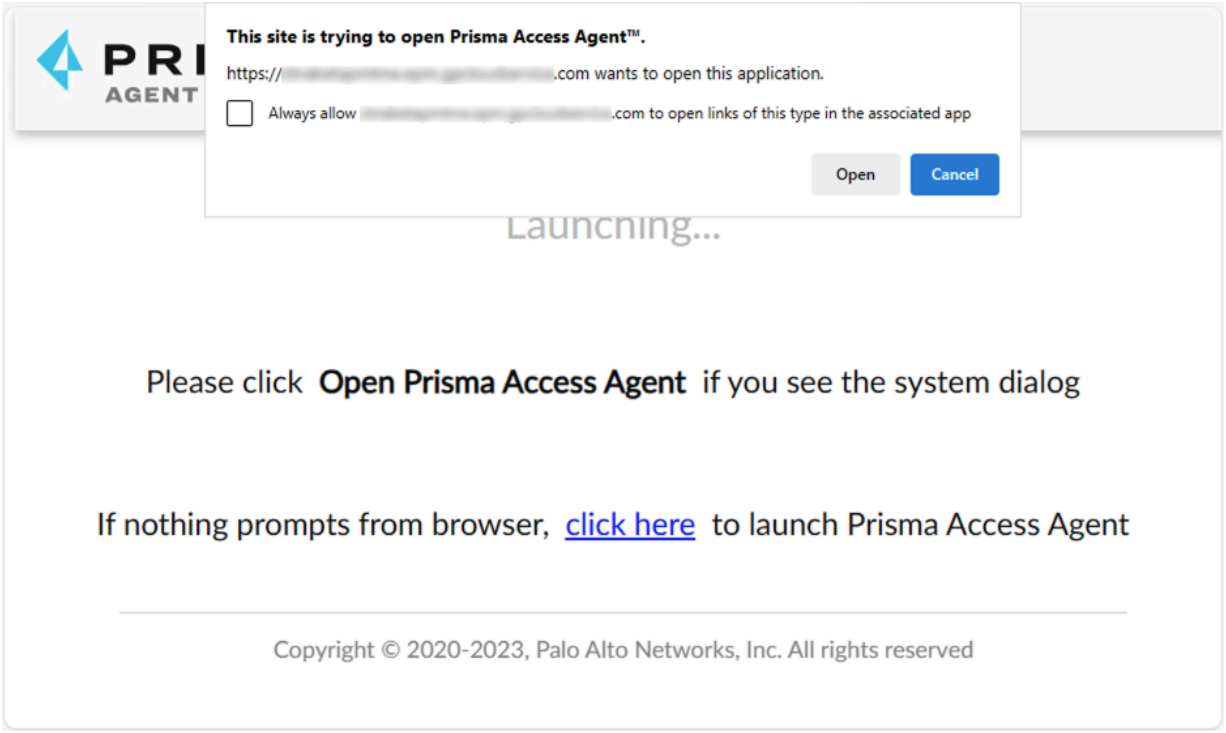
切り替え先のプロジェクトに割り当てられている必要があります。



STEP 3 | 管理者がPrisma Access Agentのオンデマンドモードを有効にしている場合、プロジェクトを切り替えるにはロックアイコンをクリックします。それ以外の場合、Prisma Access Agentはプロジェクトの切り替えに進みます。

©2025 Palo Alto Networks, Inc.

STEP 4 | プロジェクトを切り替えるたびに、Prisma Access Agentは現在のプロジェクトから切断され、新しく選択したプロジェクトに接続します。再度をPrisma Access Agentを開くように指示される場合もあります。



ダイナミック特権アクセス有効Prisma Access Agentを別のサーバーに接続する

どこで使用できますか?	何が必要ですか?
• Prisma Access Agent	❑ MacOS 12以降のデスクトップデバイスまたはWindows 10バージョン2024以降またはWindows 11デスクトップデバイス ❑ インターネット アクセス

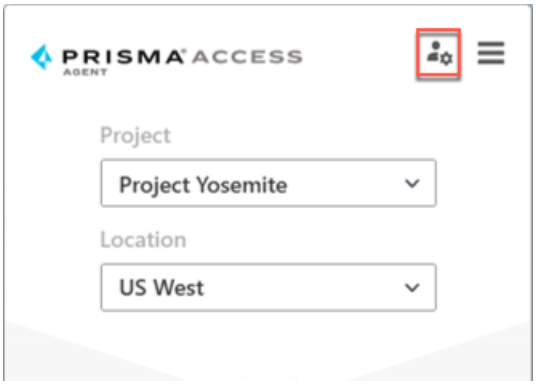
Prisma Accessサーバーのインスタンスは、テナントとも呼ばれます。管理者が複数のPrisma Accessサーバーを設定している場合は、別のサーバーに接続して、そのサーバー経由でネットワークまたはリソースにアクセスできます。

たとえば、別のプロジェクトで作業する必要があるが、そのプロジェクトには別のサーバーからしかアクセスできない、などです。そのプロジェクトに変更する前に、そのサーバに接続する必要があります。

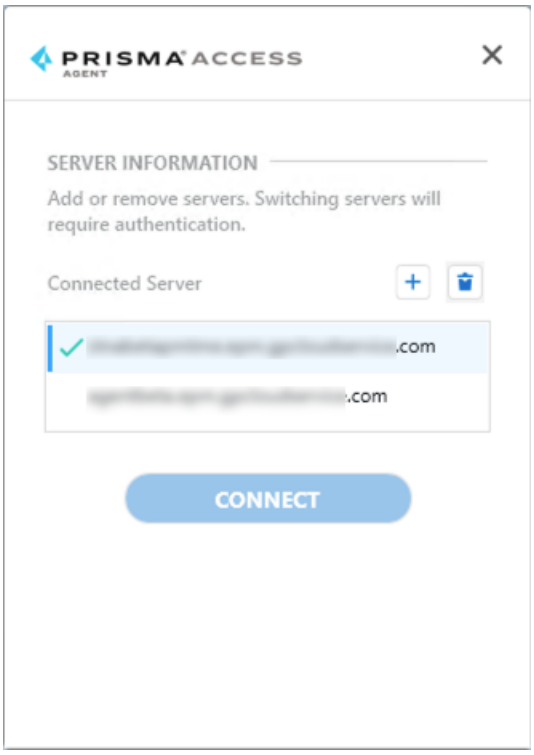
STEP 1 | MacOSメニューバーまたはWindowsタスクバーから Prisma Access Agentアイコンをクリックしてを起動します。

©2025 Palo Alto Networks, Inc.

STEP 2 | サーバー管理アイコンを選択してサーバー設定を編集します。



STEP 3 | サーバー情報ウィンドウには、接続しているサーバーが表示されます。他のサーバーがリストされている場合は、そのうちの1つを選択して接続できます。

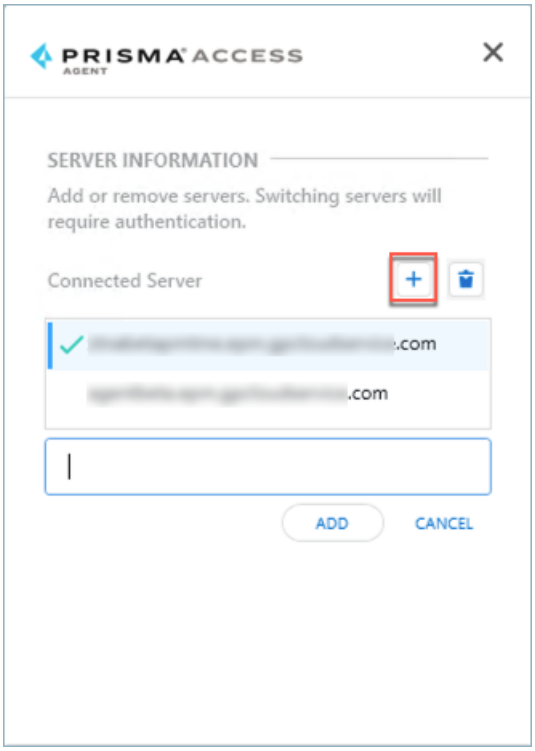


©2025 Palo Alto Networks, Inc.

STEP 4 | サーバーを追加する必要がある場合は、次の手順を実行します。

1. **+** 記号をクリックします。
2. 新しいサーバー名（管理者から提供されたもの）を入力して 追加します 。

   サーバー名の形式は **<example.domain.com>**で、**https://**はありません。サーバー名の最大長は256文字です。このページで許可されるサーバーの最大数は20です。



3. サーバーを追加したら、それを選択して [接続]をクリックします。

STEP 5 | 確認ウィンドウが表示されたら、[はい] をクリックして現在のサーバーから切断し、他のサーバーに接続します。シングル サインオンの資格情報を再度入力する必要があります。

STEP 6 | プロンプトが表示されたら、プロジェクト名を指定して新しいサーバにログインします（該当する場合）。

Prisma Access AgentとGlobalProtectアプリケーションの切り替え

どこで使用できますか?	何が必要ですか?
• Prisma Access Agent	❑ MacOS 12以降のデスクトップデバイスまたはWindows 10バージョン2024以降またはWindows 11デスクトップデバイス ❑ インターネット アクセス

一部の組織では、Prisma Access Agentは、GlobalProtectアプリケーションがすでにインストールされているユーザー デバイスにインストールされます。Prisma Access Agentをインストール

©2025 Palo Alto Networks, Inc.

した後、必要に応じてPrisma Access AgentとGlobalProtectアプリケーションを切り替えることができます。

GlobalProtectアプリケーションに切り替えると、Prisma Access Agentは無効状態になります。無効状態の場合:

- Prisma Accessロケーションへのすべてのトラフィックが無効になり、多要素認証（MFA）が無効になります。

  Prisma Access Agent と GlobalProtect はどちらも同じ GlobalProtect ポートを使用して MFA リクエストを受信しますが (特定のアプリケーションの追加認証用)、このポートを一度に使用できるのは 1 つのエージェントだけです。Prisma Access Agentを無効にすると、ポートは解放され、GlobalProtect が使用できるようになります。
- サーバーとの通信は継続されるため、エージェントは引き続き段階的なロールアウトアップグレード、ADEM 通知、管理者からのリモートシェルリクエストを受信し、HIP チェックを実行できます。
- 管理者が設定した場合、アンチタンパー機能は引き続き機能し、エージェントを不正な改ざんから保護します。
- MacOSデバイスでは、Prisma Access Agentのシステム拡張とネットワーク拡張は引き続きアクティブになり、コンテンツフィルターも引き続きアクティブになります。
- 別のサーバーに切り替えると、Prisma Access Agent は自動的に再び有効になります。エージェントが無効になっているときに Prisma Access ロケーションに接続しようとすると、エージェントは最適なロケーションに接続します。

Prisma Access Agent アプリまたは Prisma Access コマンドラインツール (PacLI) のいずれかを使用して、2 つのアプリを切り替えることができます。

- Prisma Access Agentアプリケーション
- Prisma Accessコマンドライン (PACli)

Prisma Access AgentとGlobalProtectアプリケーションの切り替え（Prisma Access Agentアプリ使用）

GlobalProtect™アプリに切り替える前に、Prisma Accessエージェントを無効にする必要があります。管理者がユーザーがPrisma Accessエージェントを無効にできるように機能を設定した場合、アプリを使用してPrisma Accessエージェントを無効にできます。Prisma Accessエージェントを無効にした後、GlobalProtectアプリを起動できます。

管理者はこのテナントレベルの機能を有効にするために*Palo Alto Networks*チームに連絡する必要があります。それはのエージェント設定としては利用できません。

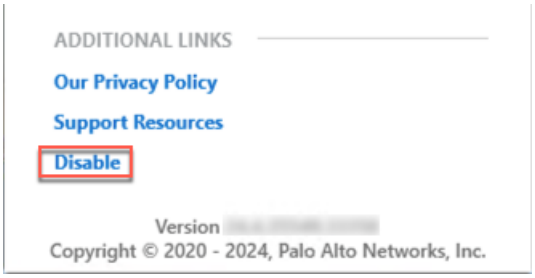
©2025 Palo Alto Networks, Inc.

Prisma Access AgentからGlobalProtectアプリケーションに切り替えるには:

1. Prisma Access Agentを有効にする

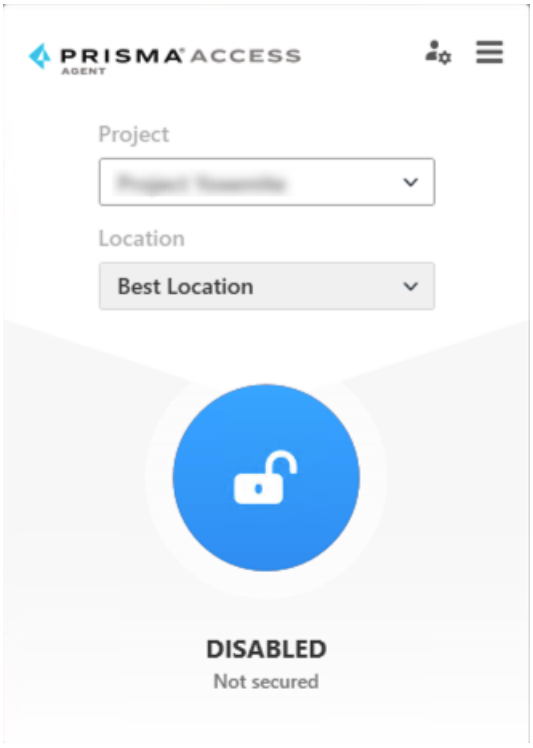
   エージェントを初めて無効にする場合は、Prisma Accessエージェントアプリを開き、Prisma Accessエージェントからサインアウトします。

   1. ハンバーガーメニューを選択し、サインアウトを選択します。
   2. 再度Prisma Accessエージェントアプリにログインして、設定ウィンドウに無効にするリンクを表示させます。
2. ハンバーガー メニューをクリックして設定ウィンドウを開きます。
3. Prisma Access Agentを有効にする



4. **X**をクリックして設定ウィンドウを閉じます。

   Prisma Accessエージェントは無効になっています。



5. GlobalProtectアプリを起動し、接続してGlobalProtectに接続します。

©2025 Palo Alto Networks, Inc.

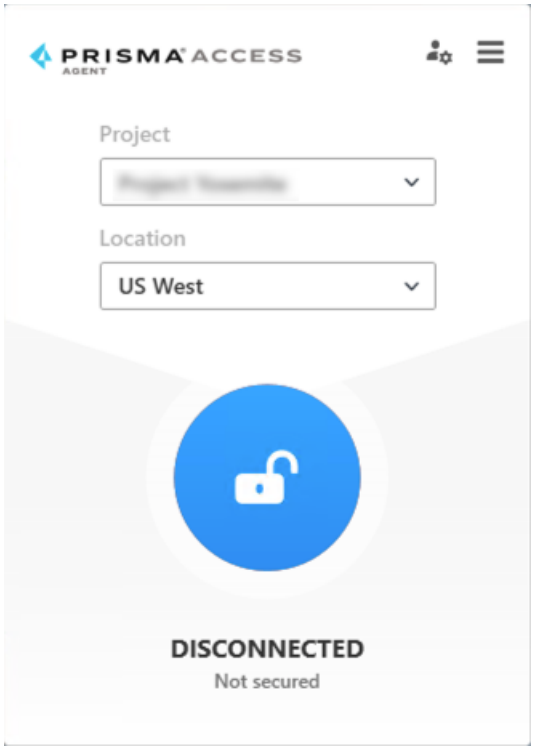
Prisma Access AgentからGlobalProtectアプリケーションに切り替えるには:

1. GlobalProtectアプリケーションを開きます。
2. オプションメニューをクリックし、切断を選択します。
3. Prisma Access Agentにログインする
4. ハンバーガー メニューをクリックして設定ウィンドウを開きます。
5. Prisma Access Agentを有効にする



6. **X**をクリックして設定ウィンドウを閉じます。
7. エージェントが常時接続モードの場合、エージェントは有効で、最適な場所に接続します。

   エージェントがオンデマンドモードの場合、Prisma Accessエージェントは有効ですが、接続されていません。ロックアイコンをクリックしてPrisma Accessの場所に接続します。



©2025 Palo Alto Networks, Inc.

Prisma Access AgentとGlobalProtectアプリケーションの切り替え（PACliツールの使用）

Prisma Access AgentとGlobalProtectアプリケーションを切り替えるには、Prisma Accessコマンドライン ツール (PACli) を実行します。GlobalProtectアプリに切り替える際、管理者がPrisma Access Agentのオンボーディング時にアンチタンパーロック解除パスワードを設定すると、PACliツールからパスワードの入力が求められます。目的のアプリに切り替えると、現在使用していたアプリが無効になります。

STEP 1 | Prisma Access AgentからGlobalProtectアプリケーションに切り替えるには:

1. エージェントを切り替えるには、**switchto**コマンドを実行します。
   - MacOSデバイスでは、ターミナル ウィンドウを開き、次のコマンドを実行します。

     ```
     sudo /Applications/Prisma\ Access\ Agent.app/Contents/
     Helpers/pacli switchto GlobalProtect
     ```

   - Windowsデバイスでは、コマンド プロンプト ウィンドウを開き、次のコマンドを実行します。

     ```
     "C:\Program Files\Palo Alto Networks\Prisma Access Agent
     \pacli" switchto GlobalProtect
     ```

2. （macOS）プロンプトが表示されたら、管理者パスワードを入力します。
3. プロンプトが表示されたら、**Y**と入力してGlobalProtectアプリケーションに切り替えます。
4. スーパーバイザのパスワードの入力を求められた場合は、改ざん防止ロック解除パスワードを入力します。

   以下のテキストは、macOSデバイスでPrisma Access AgentからGlobalProtectに切り替える例を示しています。

   ```
   <username@hostname> ~ % cd /Applications/Prisma\ Access\
    Agent.app/Contents/Helpers <username@hostname> Helpers
    % sudo ./pacli switchto GlobalProtect スーパーバイザ
   のパスワードを入力します。Prisma Access Agentを無効にしまし
   た。GlobalProtectサービスを開始しています。これには最大15分かかる
   場合があります。SuccessfulyはGlobalProtectを起動した。切り替え完
   了<username@hostname>ヘルパー%
   ```

   このアクションにより、GlobalProtectサービスが停止し、改ざん防止機能とともにPrisma Access Agentサービスが開始されます。Prisma Access Agentが無効になったことを示すエントリがPrisma Access Agentのログに書き込まれます。たとえば、

   ```
   <username@hostname>~% cd /Applications/Prisma\ Access\
    Agent.app/Contents/Helpers <username@hostname> Helpers % . /
   pacli event .740 2024-12-11 23:20:57 改ざん検知エージェントが無効
   ```


©2025 Palo Alto Networks, Inc.

```
に 741 2024-12-11 23:20:57 エージェントトンネルトンネルが切断されました。
```

5. （任意） **pacli switchto status** コマンドを実行して、 **switchto** コマンドのステータスを表示します。
   以下のテキストは、macOSで**switchto**コマンドのステータスを確認する例です。

```
<username@hostname> ~ % cd /Applications/Prisma\
 Access\ Agent.app/Contents/Helpers <username@hostname>
 Helpers % sudo ./pacli switchto status Prisma Access
 Agent:GlobalProtectの無効化：有効な<username@hostname>ヘルパー%
```

STEP 2 | Prisma Access Agentに戻すには:

1. エージェントを切り替えるには、**switchto**コマンドを実行します。
   - MacOSデバイスでは、ターミナル ウィンドウを開き、次のコマンドを実行します。

```
sudo /Applications/Prisma\ Access\ Agent.app/Contents/
Helpers/pacli switchto PrismaAccessAgent
```

   - Windowsデバイスでは、コマンド プロンプト ウィンドウを開き、次のコマンドを実行します。

```
"C:\Program Files\Palo Alto Networks\Prisma Access Agent
\pacli" switchto PrismaAccessAgent
```

2. （macOS）プロンプトが表示されたら、管理者パスワードを入力します。
3. プロンプトが表示されたら、**Y** と入力してPrisma Access Agentに切り替えます。
4. スーパーバイザのパスワードの入力を求められた場合は、改ざん防止ロック解除パスワードを入力します。

   以下のテキストは、macOSデバイスでGlobalProtectアプリからPrisma Access Agentに切り替える例です。

```
<username@hostname> ~ % cd /Applications/Prisma\ Access\
 Agent.app/Contents/Helpers <username@hostname> Helpers %
 sudo ./ pacli switchto PrismaAccessAgent Password:スーパーバイザのパスワードを入力:GlobalProtectサービスを停止しています。これには最大15分かかる場合があります。GlobalProtect を無効にします。Prisma Access Agentの起動に成功しました。切り替え完了<username@hostname>ヘルパー%
```

   このアクションにより、GlobalProtectサービスが停止し、改ざん防止機能とともにPrisma Access Agentサービスが開始されます。Prisma Access Agentが有効になったことを示すエントリがPrisma Access Agentのログに書き込まれます。たとえば、

```
<username@hostname>~% cd /Applications/Prisma\ Access\
 Agent.app/Contents/Helpers <username@hostname> Helpers % . /
```

 ©2025 Palo Alto Networks, Inc.

```
pacli event .742 2024-12-11 23:21:05 改ざん検知エージェントが有効
 743 2024-12-11 23:21:21 エージェントトンネルトンネルが接続されまし
た。
```

プリズマアクセスエージェントに切り替えた後、エージェントが常時接続モードの場合、エージェントは有効になり、最適な場所に接続します。エージェントがオンデマンドモードの場合、エージェントは有効になりますが、切断されます。

5. （任意） **pacli switchto status** コマンドを実行して、 **switchto** コマンドのステータスを表示します。

   以下のテキストは、macOSで**switchto**コマンドのステータスを確認する例です。

```
<username@hostname> ~ % cd /Applications/Prisma\
 Access\ Agent.app/Contents/Helpers <username@hostname>
 Helpers % sudo ./pacli switchto status Prisma Access
 Agent:GlobalProtectを有効にする：無効<username@hostname>ヘルパー%
```


©2025 Palo Alto Networks, Inc.

動的特権アクセス ユーザーの表示と監視

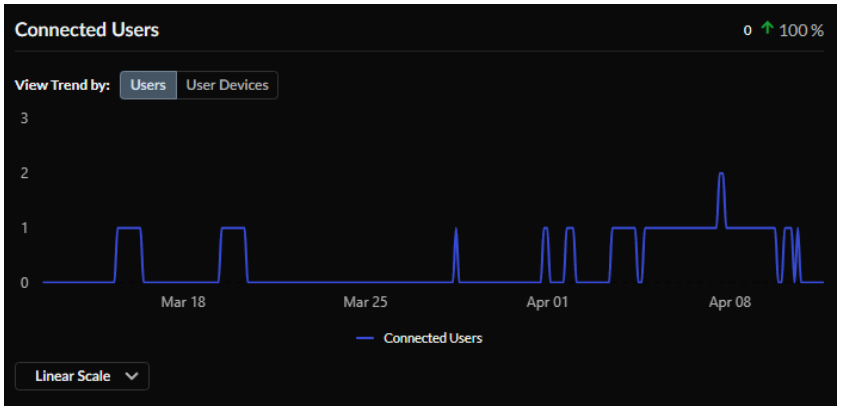
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	☐ Prisma Accessライセンス

動的特権アクセスにより、Prisma Accessは、ユーザーが取り組んでいるプロジェクトに基づいて、モバイルユーザーフローに異なるネットワークおよびセキュリティポリシールールを適用できます。環境内のユーザーベースのアクセス情報を表示するには、Strata Cloud Manager コマンド センターの**[Insights (知見)]** > **[Users (ユーザー)]** に移動します。

接続ユーザー

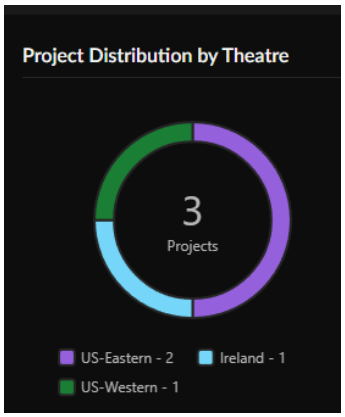
接続されているユーザーを表示して、現在接続されているユーザーまたは接続されているユーザーのデバイスを表示します。上矢印または下矢印は、この時間範囲と以前の時間範囲を比較して、接続されているユーザーやデバイス数の差をパーセントで判断します。

Prisma Access Agentに現在接続しているユーザーの数を表示するには、「ユーザー別のトレンドを表示」を選択し、「ユーザー端末別のトレンドを表示」をクリックして、現在Prisma Access Agentに接続しているユーザー端末の数を確認してください。

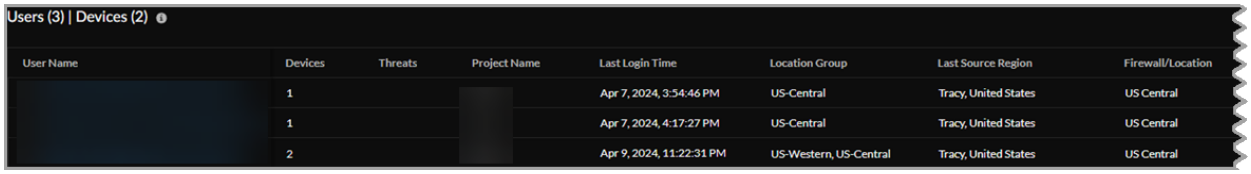


シアター別のプロジェクト配信を表示して、場所または劇場ごとのプロジェクト数を確認してください。

©2025 Palo Alto Networks, Inc.



ユーザー | デバイス テーブルは、各ユーザーおよびデバイスに関連付けられたプロジェクト名を示しています。ユーザーごとに接続されているデバイスの数、最終ログイン時間、最終ソース位置、最後に接続されたPrisma Accessの位置、ソースインターネットプロトコル、OSファミリーとバージョンを確認することもできます。

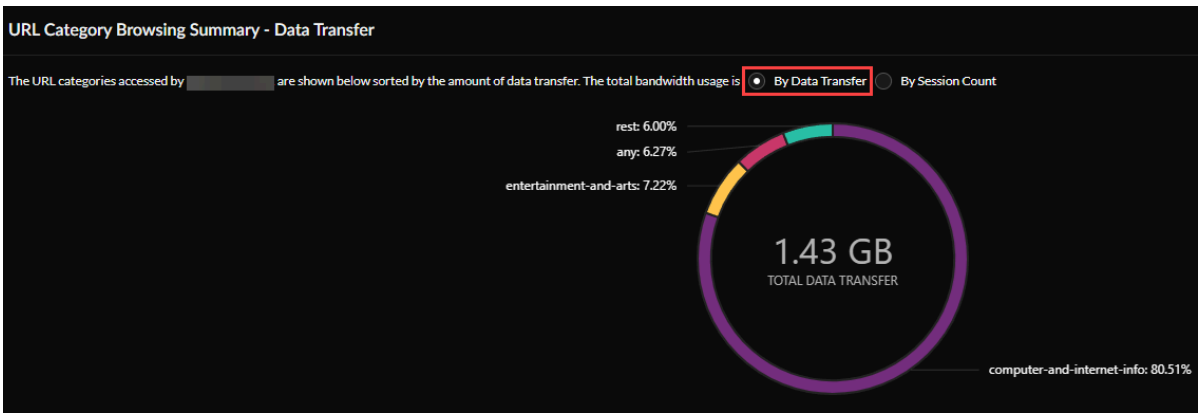


プロジェクト名を選択して、プロジェクトページに移動します。

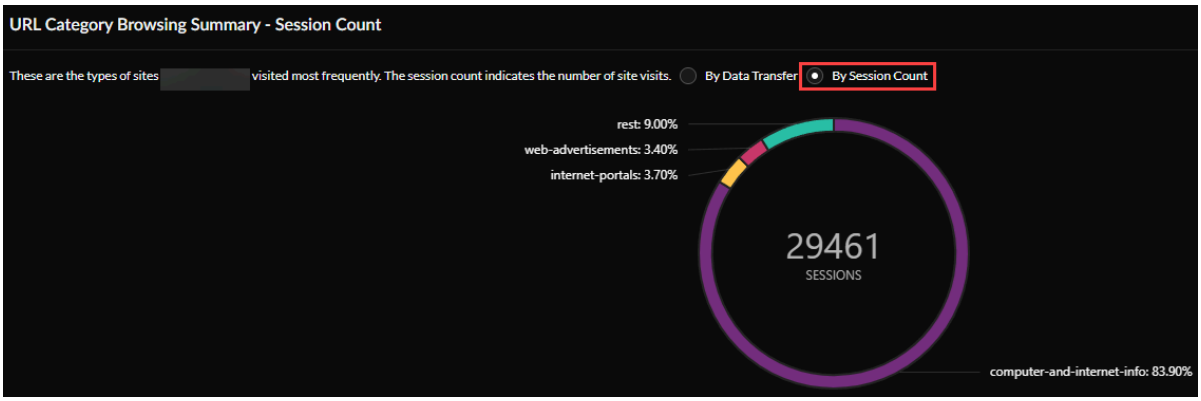
ユーザー名を選択して、アクティビティや接続性などのユーザー詳細を表示します。

アクティビティ

URL閲覧カテゴリの概要 - データ転送 - データ転送またはセッション数による閲覧カテゴリのデータ転送概要を表示します。データ転送量でソートされたトップ**10**の**URL**カテゴリのリストも表示できます。



 ©2025 Palo Alto Networks, Inc.



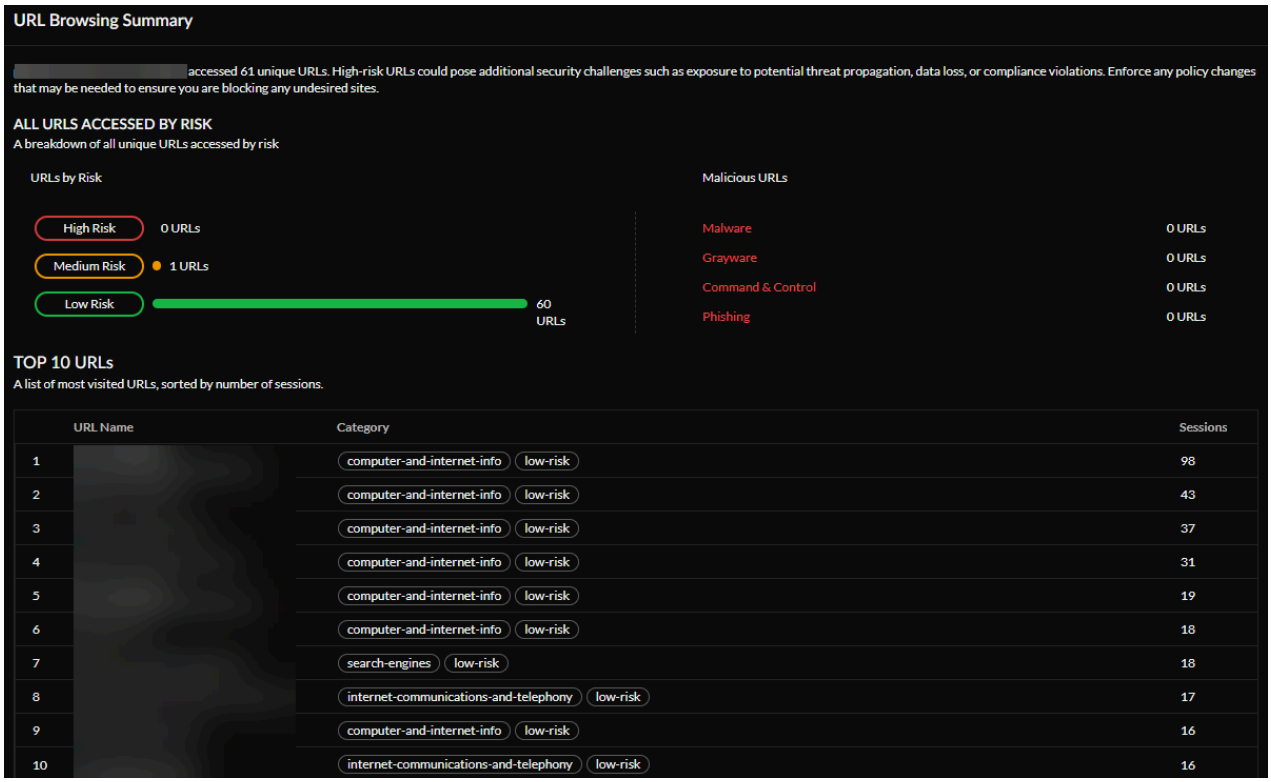
TOP 10 URL CATEGORIES

A list of top URL categories, sorted by data transferred.

	Category	Unique URLs	Data Transfer
1	computer-and-internet-info	42	7.21 MB
2	internet-communications-and-telephony	6	703 KB
3	search-engines	4	616 KB
4	shopping	1	141 KB
5	internet-portals	3	130 KB
6	web-based-email	1	121 KB
7	streaming-media	1	49.5 KB
8	any		43.6 KB
9	online-storage-and-backup	1	11.9 KB
10	unknown	1	5.22 KB

URLブラウジングの概要 - リスクによってアクセスしたすべてのURLを含むURLブラウジングの概要を確認してください。リスク（高、中、低）別にURLの内訳を表示し、アクセスした悪意のあるURLの数を確認できます。訪問したトップ**10**の**URL**のリストと、それぞれのURLを訪問した回数も表示できます。

©2025 Palo Alto Networks, Inc.

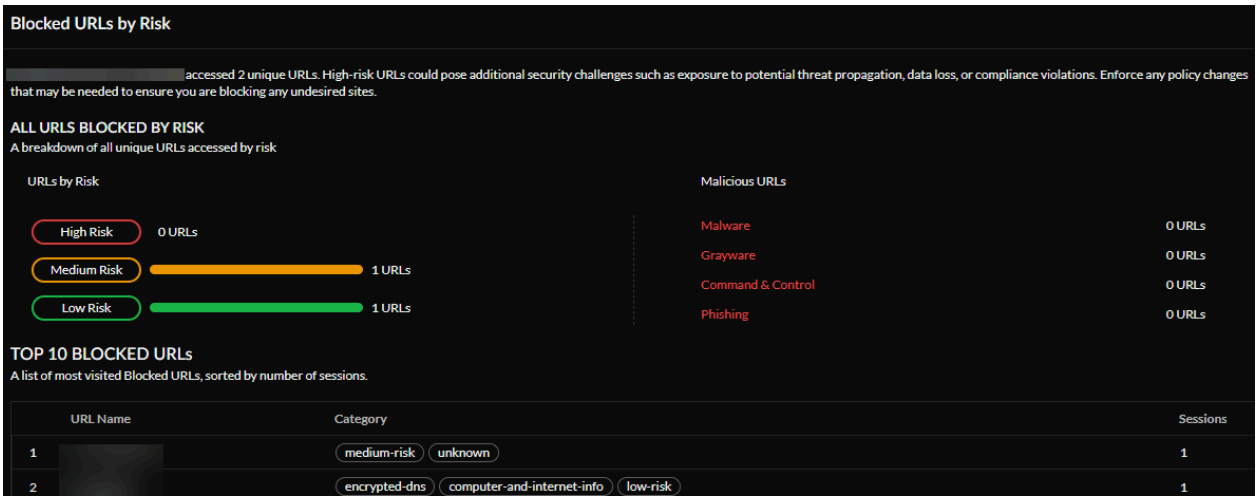


URLフィルタリングログを表示—転送された総データに関する詳細を表示するには、**[URL**フィルタリングログを表示]を選択します。ログは、システム、設定、およびネットワークイベントの監査証跡を提供します。ネットワークログは、Prisma Accessがネットワークで動作するすべてのイベントを記録します。

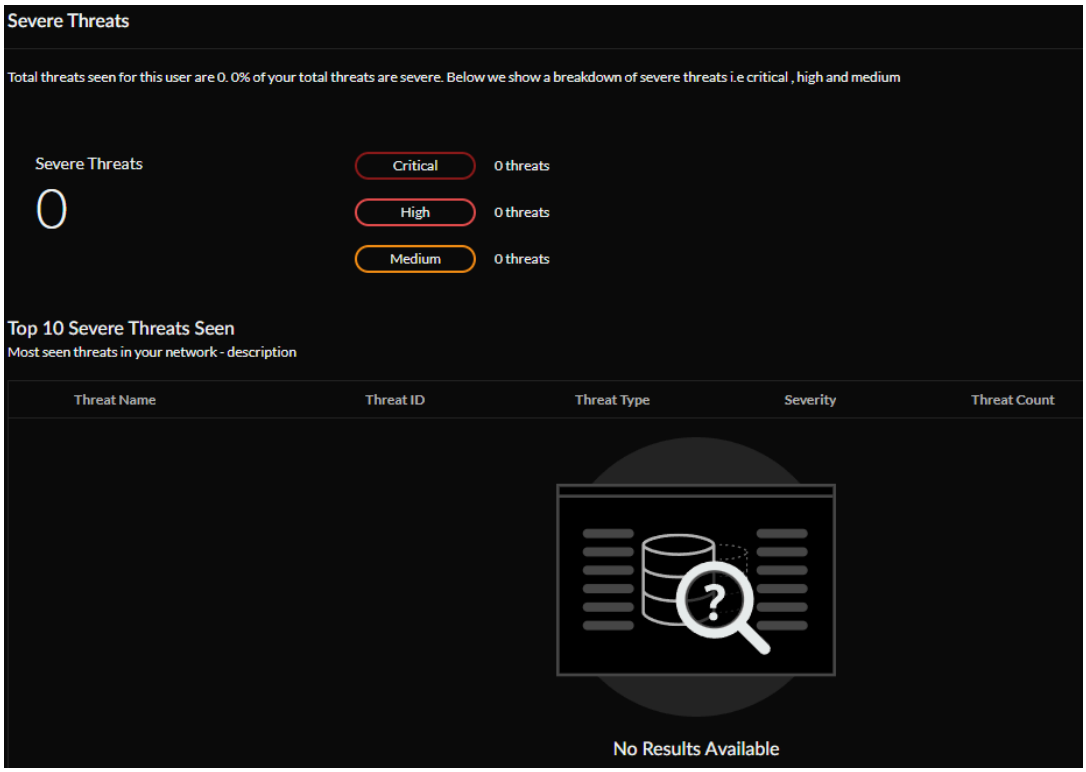
- すべてのログデータを表示するか、ドロップダウンを使用してファイアウォール**/URL**、一般、またはエンドポイントでフィルタリングします。これらのフィルターには、選択できるいくつかのサブフィルターもあります。
- ログクエリを入力してください。このフィールドをクリックして、最初に使用するクエリの選択を表示し、クエリを構築します。
- 時間範囲を選択します。デフォルトは60分を過ぎています。
- ログ設定を選択して、 Strata Logging Serviceダッシュボードを表示します。Strata Logging Serviceは、ログの配信メカニズムを管理します。

リスクによってブロックされた**URL** - リスクによってブロックされたURLにアクセスしたか、アクセスしようとしたかを確認してください。リスクの高い URL は、潜在的な脅威の伝播、データ損失、またはコンプライアンス違反など、追加のセキュリティ上の課題を引き起こす可能性があります。望ましくないサイトをブロックするために必要なポリシー変更を強制する。あなたが最も訪れた上位**10**のブロックされた**URL**のリストも、セッション数でソートされて表示されます。

©2025 Palo Alto Networks, Inc.



深刻な脅威–あなたの脅威のうち、どれが深刻かを確認してください。深刻な脅威は、クリティカル、高、中の脅威にさらに分類されます。お使いの環境で見られるトップ**10**の深刻な脅威のリストも表示できます。



接続

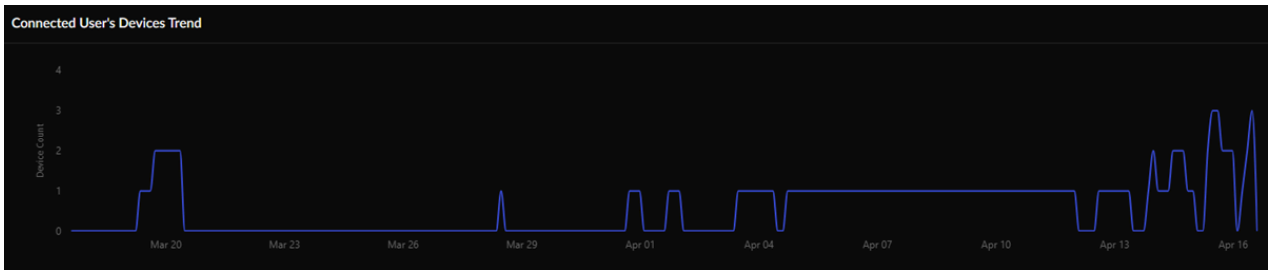
選択した時間範囲でユーザーの接続情報を表示するには、任意のユーザー名を選択してください。

アクティブプロジェクト–選択した期間中にアクティブだったプロジェクトと、それぞれのプロジェクトがアクティブになった日付を確認できます。

接続されたユーザーのデバイストレンドと接続されたユーザーのデバイス - メインユーザーページでは、すべての接続されたユーザーとそのプロジェクトを見ることができます。接続性ページ

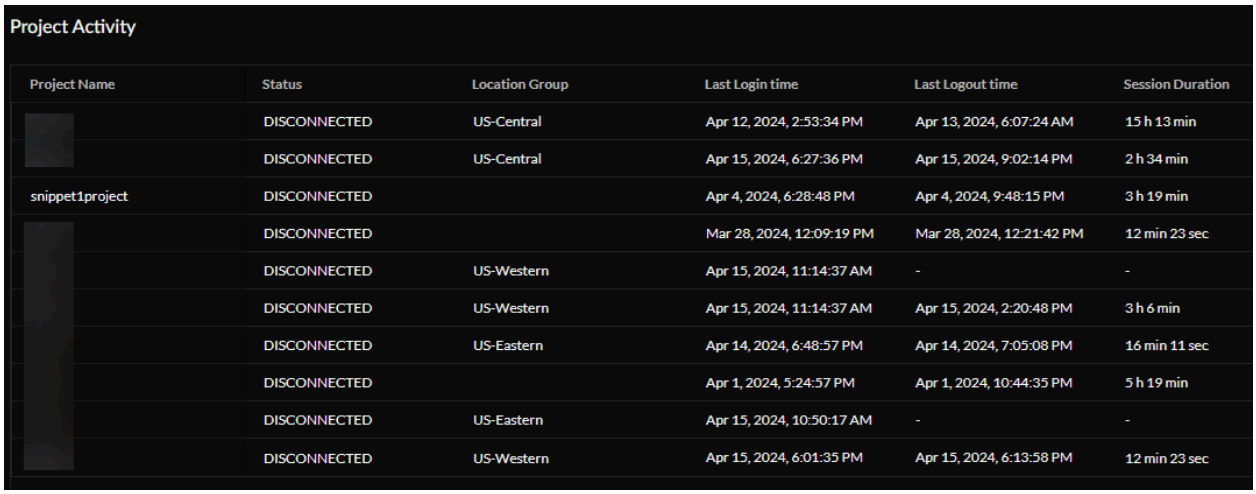
 ©2025 Palo Alto Networks, Inc.

では、選択した時間範囲内での個々の**Connected User's Devices (**接続しているユーザーのデバイス**)**トレンドと、デバイス名、最後のユーザーソースIPアドレス、最後のプライベートIPアドレス、最後のユーザーの位置、最後のログイン時間、最後のログアウト時間、最後のセッションの持続時間など、接続しているユーザーのデバイスに関する詳細を表示します。





プロジェクト活動–セッションごとのユーザーのプロジェクト活動を表示します。セッションの現在の状態、ユーザーが各プロジェクトにログインした時刻、ログアウトした時刻、各セッションの持続時間を確認できます。



プロジェクト別の総ユーザーアクティビティ - 選択した期間中にユーザーが各プロジェクトに費やした時間を表示します。

©2025 Palo Alto Networks, Inc.

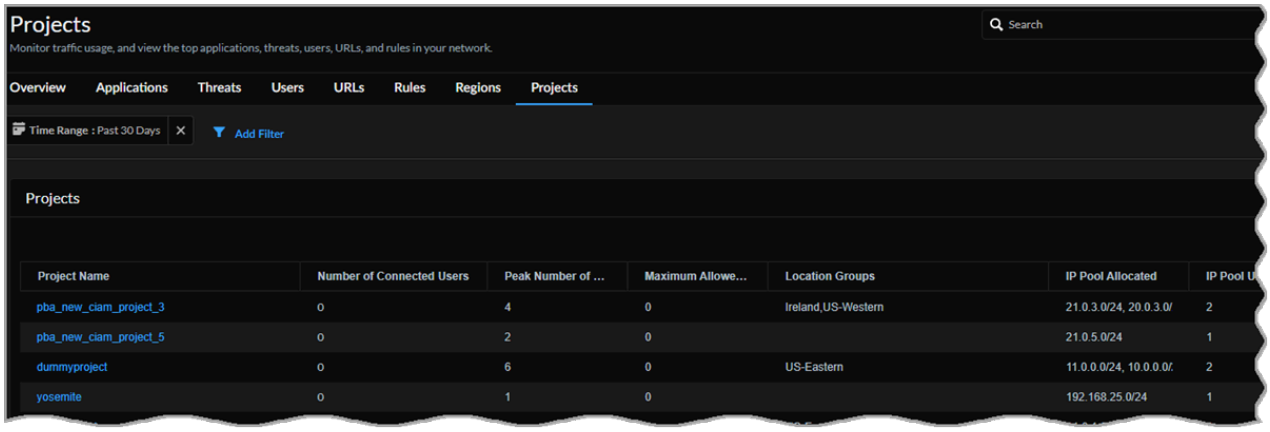
動的権限アクセス プロジェクトの表示と監視

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

Strata Cloud Manager を使用してユーザーのプロジェクトのアクティビティを監視することで、Prisma Access Agentのデプロイメントを可視化できます。環境内のプロジェクトベースのアクセス情報を表示するには、Strata Cloud Manager コマンド センターの **[Activity Insights (アクティビティの知見)] > [プロジェクト]** に移動します。

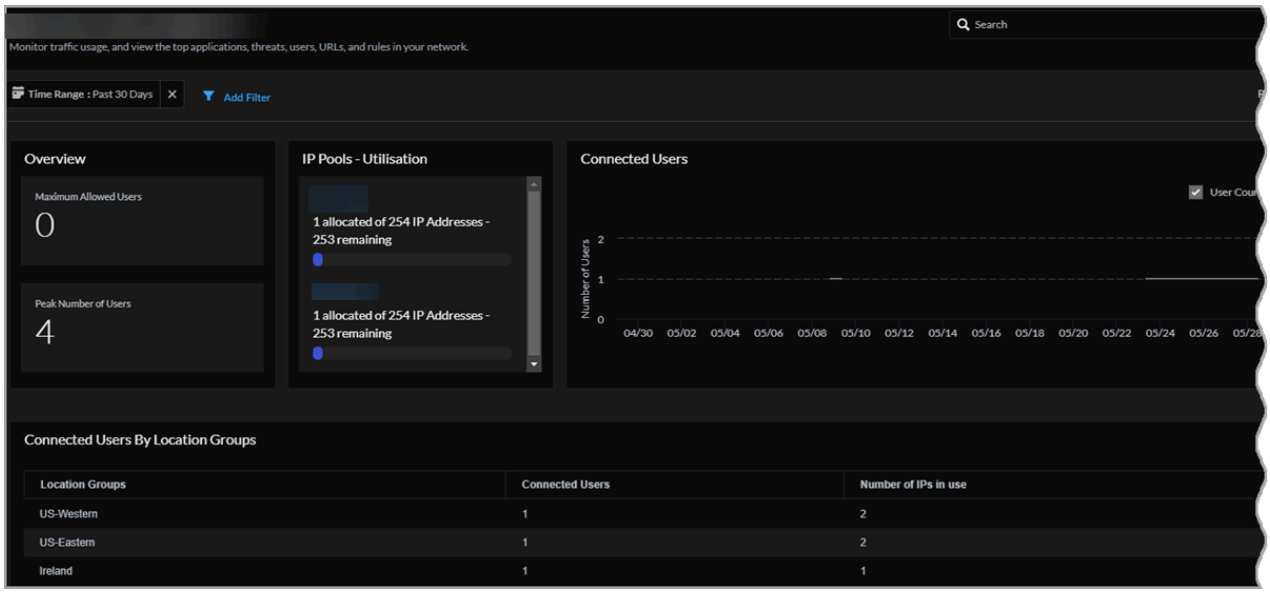
プロジェクト

プロジェクト テーブルには、選択した期間中にユーザーが Prisma Access を使用してアクセスしたプロジェクトの全体像が表示されます。各プロジェクトの接続ユーザー数、ピークユーザー数、最大許可ユーザー数、Prisma Access ロケーション グループ、割り当てられた IP アドレス プール、使用されている IP プール、使用可能な IP アドレスの数、および最後に接続された Prisma Access ロケーションを確認できます。



プロジェクト名 を選択すると、そのプロジェクトの詳細ページに移動します。プロジェクト名 (次の画像ではぼかして表示) がページの左上隅に表示されます。

©2025 Palo Alto Networks, Inc.

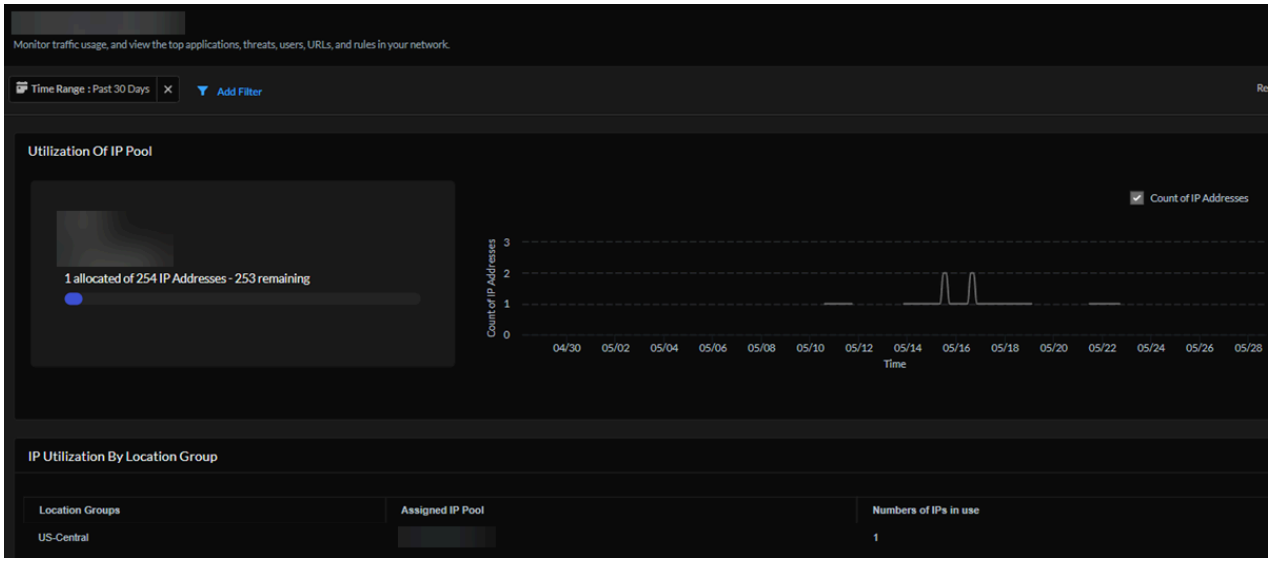


概要

プロジェクトの詳細ページの 概要 には、このプロジェクトに許可されている最大ユーザー数と、選択した期間のピーク時のユーザー数が表示されます。

IPプール - 使用率

このプロジェクト内のプールで使用中の IP の数とまだ使用可能な IP の数を表示します。特定の IP プールを選択して詳細ページに移動します (次の画像を参照)。ここで、この IP プールの使用率、使用されている IP アドレスの数、および Prisma Access ロケーション グループ別の IP アドレスの使用率を確認できます。



接続ユーザー

選択した期間に接続したユーザーのグラフを表示します。グラフ内の任意のポイントにマウスを合わせると、そのポイントのユーザー数が表示されます。

©2025 Palo Alto Networks, Inc.

ロケーショングループ別の接続ユーザー

所属する Prisma Access ロケーション グループ 別にユーザー数を表示します。各 ロケーション グループで使用されている IP アドレスの数も確認できます。

©2025 Palo Alto Networks, Inc.

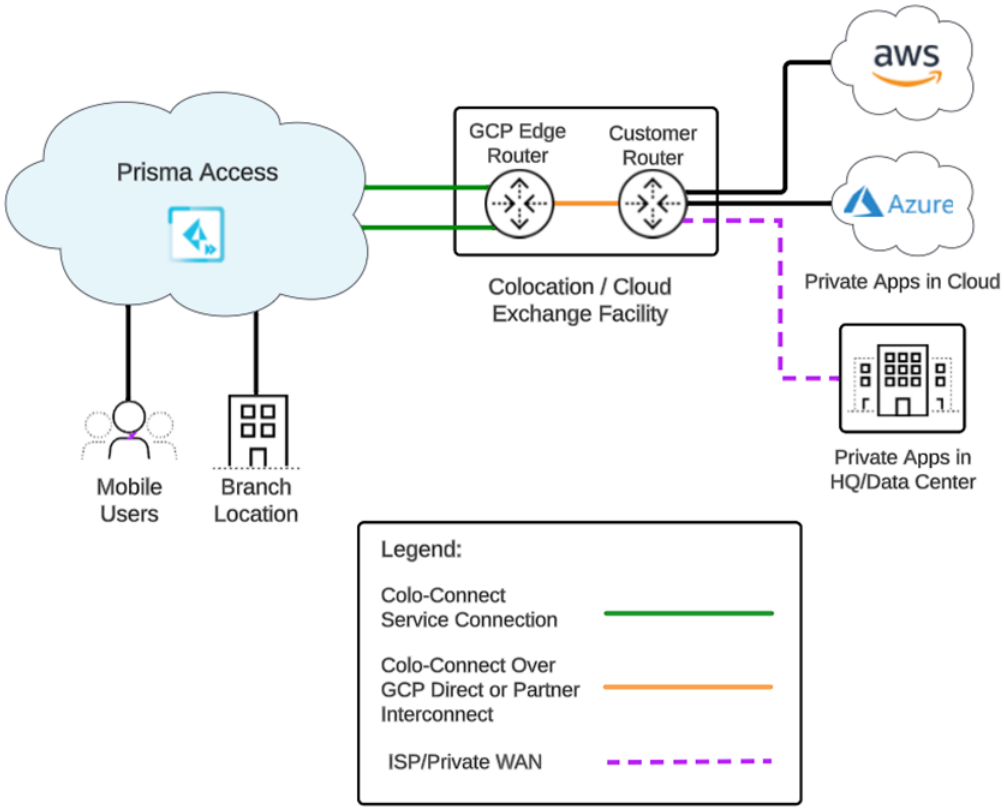
©2025 Palo Alto Networks, Inc.

Prisma Access Colo-Connect

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access (Managed by Panorama)デプロイメントで、最小クラウドサービス プラグイン・バージョン 4.1 と最小データプレーン バージョン10.2.4を実行します。 ❑ Colo-Connectアドオンライセンス

今日、大企業は、高帯域幅と低遅延の要件により、ハイブリッドなマルチクラウドアーキテクチャのプライベートアプリケーションに到達するために、Coloベースのパフォーマンスハブを構築しています。通常、これらのハブには、1つ以上のクラウド プロバイダーへの相互接続と、プライベートWANまたはリースWANを介したオンプレミス データセンターへの接続が含まれます。パフォーマンス ハブは、パブリック クラウドとオンプレミス インフラストラクチャ間のトラフィックを高速でルーティングでき、基盤となる相互接続インフラストラクチャにより回復性があります。

Colo-Connectは、Coloベースのパフォーマンスハブのコンセプトに基づいて構築されており、高帯域幅(最大20 Gbps)のプライベート接続に加えて、既存のパフォーマンスハブからPrisma Accessへのシームレスなレイヤー2/3接続を提供します。次の図は、サービス接続とダイレクトまたはパートナー相互接続を使用して、GCPインスタンスにPrisma Accessがオンボードされている様子を示したものです。この設定により、インターネットへの露出が制限され、プライベートなアプリケーション接続にプライベート接続を使用できるようになります。



Prisma Access Colo-Connectは、クラウドネイティブのGCPインターコネクト技術を活用して、プライベートアプリケーションへの高帯域幅サービス接続を提供します。

- プライベートアプリケーションアクセスのためのリージョンあたりの高帯域幅(最大20 Gbps)スループット
- Google Cloud Platform (GCP)を使用した専用およびパートナー相互接続の両方をサポート
- インターコネクト リンクごとに複数のVLANアタッチメントをサポートします。
- 地域の冗長性

©2025 Palo Alto Networks, Inc.

Colo-Connectの使用例

Prisma AccessColo-Connectは、次のユースケースに示すように、プライベートアプリをセキュリティで保護するための高帯域幅の双方向接続を提供します。

プライベートアプリへの高帯域幅アクセス

組織がColoにネットワーク拠点を持ち、Coloの機能を活用して、オンプレミス、パブリック クラウド、またはその両方でホストされているアプリへのプライベート接続を構築している場合、 Prisma AccessはColo-Connectを介してそのColoインフラストラクチャの一部になることができます。GCPが提供する専用インターコネクトまたはパートナーインターコネクトのいずれかを使用してColo-Connectを構成し、プライベートアプリアクセス用にリージョンあたり最大20Gbpsのスループットを得ることができます。

例えば、コロケーションに直接接続できるデータセンターや本社が1つ以上あり、高帯域幅でセキュアなプライベート アプリ アクセスのためにPrisma Accessに接続したいとします。この場合、パートナーインターコネクトをPrisma AccessColo-Connectは、ユーザーにアプリへの安全なアクセスを提供します。Coloの機器は、データセンターだけでなくパブリック クラウドにもピアリングされているため、パブリック クラウドでホストされている任意のプライベート アプリへのアクセスを提供することもできます。

Colo-Connectは既存のIPSecトンネルベースのサービス接続と共存するため、高帯域幅のマルチギガビットスループットを必要としない小規模なデータセンターへのプライベートアプリケーションアクセスを提供する必要がある場合は、それらのデータセンターへのサービス接続も使用できます。BGPルーティングを使用してサービス接続を構成し、ネットワークをサービス接続およびColo-Connect接続と互換性を持たせることができます。

プライベートアプリケーション向けのプライベート接続

Colo-Connectは、ユーザーがインターネット経由でプライベートアプリにアクセスする代わりにプライベートアプリにアクセスするためのプライベートネットワークを活用できるため、プライベートアプリの制御とセキュリティのレベルがさらに向上します。

サードパーティのNaaSプロバイダーの使用

このユースケースでは、MegaportやPacketFabricなどのサードパーティのNetwork as a Service (NaaS) プロバイダーを活用して、Coloとパブリック クラウドで実行されているアプリケーション、またはsalesforce.comや BoxなどのSaaSプロバイダーと接続します。サードパーティのネットワークとPrisma Accessの間にネットワーク接続を確立し、接続されたサービス、クラウド、アプリケーションへの広帯域アクセスを提供したいとします。次の作業を行えます。

- NaaSプロバイダーのネットワーク機器をハブとして使用して、特定のリージョンのパブリック クラウドVPCまたはパブリック SaaS プロバイダーで実行されているユーザーとアプリケーション間の接続を提供します。
- NaaSプロバイダのネットワーク機器とPrisma Accessの間でBGPセッションを確立します。

©2025 Palo Alto Networks, Inc.

サードパーティの*NaaS*ソリューションを*Prisma Access*で*Colo-Connect*使用することは、*Palo Alto Networks*によって検証されていません。*GCP*への相互接続の設定や、*Colo-Connect*サービス接続用の*Prisma Access*への*GRE*トンネルの作成など、サードパーティプロバイダーでサポートされる機能を評価することをお勧めします。

©2025 Palo Alto Networks, Inc.

Colo-ConnectはService ConnectionsやZTNA Connectorと何が違いますか?

Palo Alto Networksでは、プライベートアプリケーションへのアクセスを保護するために、サービス接続、ZTNAコネクタ、およびColo-Connectの3つの方法を提供しています。サービス接続とZTNA Connectorはどちらもインターネット経由のプライベートアプリケーションへのアクセスを保護し、Colo-Connectはデータセンターへのプライベート接続を確立します。帯域幅と差別化要因の比較については、次の表を参照してください。

デプロイメント タイプ			
機能	Colo-Connect	ZTNA コネクタ	サービスコネクション
コンピューティング リージョンあたりの最大帯域幅	20 Gbps	10 Gbps	5 Gbps
スループット	データセンターへの20 Gbps双方向プライベート接続	データセンターあたり最大10 Gbps	接続あたり1 Gbps
Equinix Cross-ConnectやMegaportなどのSDN/NaaSプロバイダーとの互換性	あり	なし	いいえ
データセンター間のオーバーラップネットワーク	いいえ	あり	いいえ
その他の利点	Coloによるハイブリッドおよびマルチクラウドの既存のデプロイメントへの簡単なオンボーディング	ハイブリッドおよびマルチクラウド展開でのプライベートアプリケーションのオンボーディングの簡素化	オンプレミスのアクティブ ディレクトリのサポート
オンプレミス デプロイメントが必要ですか?	いいえ	あり	いいえ

©2025 Palo Alto Networks, Inc.

Colo-Connectのサポートされていない機能

次の機能は、Colo-Connectではサポートされていません。

- Traffic Steering (トラフィックステアリング)の使用時に、Colo-Connectサービス接続をターゲットサービス接続として設定します。
- プライベート アプリ アクセスのIPv6サポート
- IPv6でのeBGPピアリング

©2025 Palo Alto Networks, Inc.

Prisma Access Colo-Connectの要件と前提条件

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access (Managed by Panorama)デプロイメントが稼働するクラウドサービスプラグインバージョンの最小バージョンは4.1データプレーンバージョンは10.2.4以上です ❑ Colo-Connectアドオンライセンス

Colo-Connectのオンボーディングと構成を開始する前に、このチェックリストに従って必要な情報と前提条件を確認してください。

- ❑ Colo 施設プロバイダーにアクセスできることを確認します (たとえば、Equinixカスタマーポータルにアクセスできる)。
- ❑ CPE が GRE と BGP をサポートできることを確認してください。

  Colo-Connect サービス接続では GRE トンネルが使用されます。
- ❑ Colo-Connect に使用する相互接続タイプ (パートナー相互 接続または 専用相互接続) を決定します。
  - パートナーインターコネクト- パートナーとの相互接続にはPrisma Accessからのペアリングキーが必要です。このキーはPrisma Accessオンボーディングの際に受け取ります。

    パートナー相互接続を作成する場合は、サービス プロバイダ (SP) がGCPで承認されたSPであり、SPとGCP間の接続がすでに確立されていることを確認してください。
  - 専用相互接続–
    - オンボーディングを開始する前に、Prisma Accessでクロスコネクトケーブルを接続するColoのロケーションを決定します。 。Palo Alto Networksが専用リンクを注文するには、コロケーションが必要です。
    - 回路を構成できるように、基本的なネットワーク相互接続を理解しておいてください。
    - 専用相互接続をプロビジョニングした後、 それをテストする必要があります。
- ❑ サブネット要件- リージョンごとに各 Colo-Connect 接続に使用する RFC-1918 IPv4 サブネットを決定します。 Prisma Accessは、これらのサブネットを内部通信とネットワークに使用します。

  特定のテナント内のすべてのColo-Connectリージョン間でサブネットを一意にします。Colo-Connectサブネットは、Prisma Accessインフラサブネットおよびモバイル ユーザー プールと重複することはできません。最小サブネット サイズとして/28を使用します。

©2025 Palo Alto Networks, Inc.

- リンク (相互接続) の要件- リンクを構成するときは、次のガイドラインに従ってください。
  - 各Colo-Connectアドオン ライセンスには、10 Gbps容量のリンクが1つ含まれています。少なくとも2つのリンクが必要なため、Colo-Connectデプロイメントでは少なくとも2つのライセンスを購入する必要があります。
  - 各リージョンに2つのリンクをオンボードします。

    これらのリンクは両方とも、異なる可用性ゾーン (エッジ ドメイン) に存在する必要があります。
  - (専用相互接続のデプロイメントのみ) テナントに6つ以上のリンクをオンボードする場合は、Palo Alto Networksのアカウント担当者またはパートナーに連絡してください。担当者またはパートナーは、サイト信頼性エンジニアリング (SRE) チームに連絡して、特定のテナントの割り当てを増やすリクエストを送信します。

- 接続要件–
  - 各リージョンに2つの接続をオンボードします。

    両方の接続は異なるエッジ ドメインにある必要があります。
  - アクティブ/バックアップ モードまたはアクティブ/アクティブ モードでの接続は、同じ帯域幅である必要があります。
  - 接続をアクティブ/アクティブ構成で設定するか、アクティブ/バックアップ構成で設定するかを決定します。
- **Colo-Connect**サービス接続要件–
  - 各サービス接続には2つの接続が必要です。
  - 特定のサービス接続の各接続は、異なるリンクと異なるエッジ ドメイン上にある必要があります。
  - colo-routerでBGP IPアドレスとして使用するアドレスとGREトンネルのローカルIPアドレスをメモします。これらのアドレスは、サービス接続の作成時に使用します。
  - サービス接続は同じリンク タイプ (パートナー相互接続リンクまたは専用相互接続リンクのいずれか) 上にある必要があります。
- 既存の**IPSec**ベースのサービス接続との相互運用性- Palo Alto Networksでは、Colo-ConnectとIPSecトンネルベースのサービス接続を異なるリージョンにデプロイすることを強くお勧めします。さらに、IPSecトンネルベースのサービス接続からColo-Connectサービス接続に移行する場合は、メンテナンス ウィンドウをスケジュールする必要があります。IPSecトンネルベースのサービス接続からColo-Connectサービス接続に移行した後、Colo-Connectサービス接続が稼働し始めてからメンテナンス期間が終了する前に、IPSecベースのサービス接続を削除します。

©2025 Palo Alto Networks, Inc.

Prisma Access Colo-Connect を設定する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access (Managed by Panorama)デプロイメントで、最小クラウドサービス プラグイン・バージョン 4.1 と最小データ プレーン バージョン10.2.4を実行します。 ❑ Colo-Connectアドオンライセンス

Prisma Access Colo-Connectは次のコンポーネントで構成されています。

- **Colo**— Equinix などのホスト ネットワーク、プライベート クラウド インフラストラクチャ、パブリック クラウド インフラストラクチャにラック スペース、電源、接続を提供するコロケーション施設。
- 専用相互接続- 特定のGCPコンピューティング リージョン内のルーターとGCPエッジ ルーター間の専用のレイヤー2 またはレイヤー3物理接続。専用の相互接続により、オンプレミス ネットワークとGoogleネットワーク間の直接的な物理接続が実現します。

  インターコネクトはPrisma AccessUIでは*Link* (リンク)と呼ばれています。
- **GCP VLAN**アタッチメント- 同じリンクを共有する他の論理接続からトラフィックを分離する、リンク上の論理レイヤー2接続。

  VLANアタッチメントは、Prisma AccessUIでは*Connections* (接続)と呼ばれています。
- パートナー相互接続- 特定のGCPコンピューティング リージョン内のサービス プロバイダー所有のルーターとGCPエッジ ルーター間のレイヤー3物理接続。パートナー相互接続は、サポートされているサービス プロバイダーを通じてオンプレミス ネットワークとVPCネットワーク間の接続を提供します。

  Colo-Connect は、専用相互接続とパートナー相互接続の両方をサポートします。
- **Colo (顧客)** ルーター- Colo施設内の相互接続を介してGCPクラウド ルーターとのeBGPを確立し、GREトンネルを介してColo-Connectサービス接続とのeBGPを確立するColo施設内のルーティング デバイス。これは、専用相互接続用の顧客ルーター、またはサービス プロバイダがパートナー相互接続を介してGCPとレイヤー2接続している場合に使用されます。サービス プロバイダーは、GCPクラウド ルーターとのレイヤー3接続がある場合、Coloルーターを所有します。
- **GCP** エッジ ルーター- コロケーション経由でGCPと顧客/パートナー ネットワーク間の物理的な接続を提供するGCPのネットワーク エッジ 機器。
- クラウドルーター- クラウド上のGCPソフトウェアが、コロケーション内のネットワーク機器（ルーターやレイヤー3ファイアウォールなど）とBGPセッションを確立し、Prisma Accessとお客様のネットワーク間のトラフィックをルーティングします。このコンポーネントを設定する必要はありません。Prisma Accessによって自動的に設定されます。

Colo-Connect を設定するには、まず既存のネットワーク環境に関する情報を収集し、必要なネットワーク コンポーネントがすべて揃っていることを確認する必要があります。すべての前

 ©2025 Palo Alto Networks, Inc.

提条件が満たされていることを確認し、パートナーまたは専用の相互接続を使用して組織のネットワークにColo-Connectをデプロイします。

- Strata Cloud Manager
- Panorama

Prisma Access Colo-Connect を設定する（Strata Cloud Manager）

Colo-Connect を設定するには、まず既存のネットワーク環境に関する情報を収集し、必要なネットワーク コンポーネントがすべて揃っていることを確認する必要があります。すべての前提条件が満たされていることを確認し、パートナーまたは専用の相互接続を使用して組織のネットワークにColo-Connectをデプロイします。

パートナー相互接続を使用したPrisma AccessColo-Connect-デプロイメントの設定

パートナー相互接続を使用してPrisma Access Colo-Connect を設定するには、以下の手順を実行します。

STEP 1 | Colo-Connect 接続用のサブネットを作成します。

ここで作成したサブネットは、後の手順で作成する接続とサービス接続で使用します。

1. Strata Cloud Manager から、**[Workflows (ワークフロー)]** > **[Prisma Access**セットアップ**]** > **[Colo-Connect]**に移動します。
2. プレフィックスを追加し、Colo-ConnectサブネットのPrisma Accessロケーションを追加します。

   サポートされているcolo-connectロケーションのリストについては 、こちらをご覧ください。最小サブネット /28 を入力します。
3. (任意) 複数の場所にColo-Connectインスタンスを作成する予定の場合は、場所ごとにサブネットを追加します。

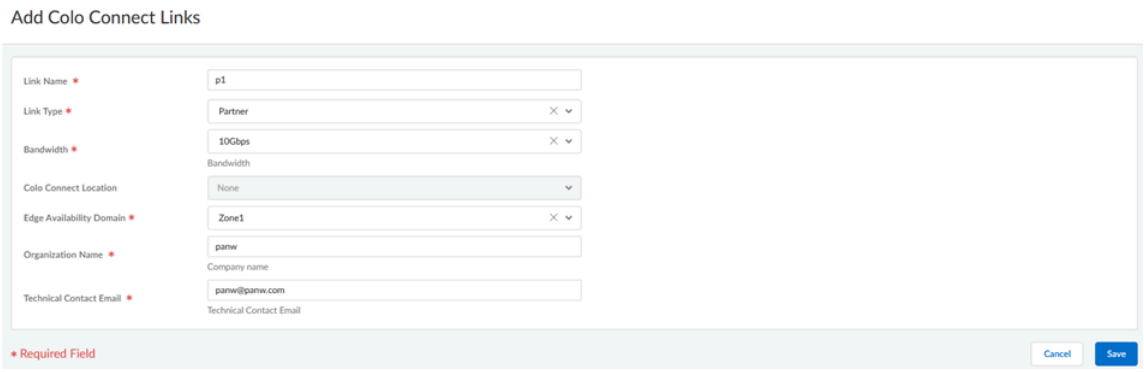
   ロケーションごとに1つのサブネットを構成できます。



 ©2025 Palo Alto Networks, Inc.

STEP 2 | 新しいColo-Connectリンク (相互接続とも呼ばれます) を追加します。

1. **[Workflows (ワークフロー)] > [Prisma Accessセットアップ] > [Colo-Connect] [Add Link** リンクを追加]に移動します。
2. リンクに一意の リンク名を付けます。
3. リンク タイプとして パートナー 相互接続を選択します。
4. 残りのColo-Connectリンク パラメータを指定します。
   - 帯域幅として **10Gbps** または **20Gbps** を選択します。
   - エッジ可用性ドメインとしてゾーン**1**またはゾーン**2** を選択します。この値は、エッジ可用性ドメインに使用される GCP ゾーン から取得します。
   - このリンクに使用する 組織名 を入力します。
   - このリンクに使用する メールアドレス を入力してください。どのメールアドレスでも構いません。



5. 手順2.a ～ 2.dを繰り返し、別のエッジ可用性ドメインで別のリンクを作成します。

STEP 3 | Colo-Connectの接続 (*VLAN* アタッチメントとも呼ばれます) を作成します。

1. **[Workflows (ワークフロー)] > [Prisma Accessセットアップ] > [Colo-Connect][Add Connection (接続を追加)]**に移動します。
2. 接続設定を構成します。
   - 一意の 接続名を入力します。
   - 前の手順で設定したリンクから リンク名 を選択します。

     VLAN IDを入力する必要はありません。パートナー相互接続で作成された VLAN では設定できません。
   - 接続の 帯域幅 を選択します。

     1 Gbps、**2 Gbps**、**5 Gbps**、**10 Gbps**、**20 Gbps**から選択できます。

     相互接続に複数の接続を構成する場合は、接続の合計帯域幅が相互接続の帯域幅を超えないようにしてください。たとえば、パートナー相互接続が10 Gbps の場合、

©2025 Palo Alto Networks, Inc.

それぞれ1 Gbpsの接続を10個構成できますが、すべての接続の合計が10 Gbpsを超えることはできません。

デプロイメントに*16*を超える接続が必要な場合は、*Palo Alto Networks*アカウント チームに連絡してください。アカウント チームは、リクエストに対応するために*SRE*ケースを開きます。

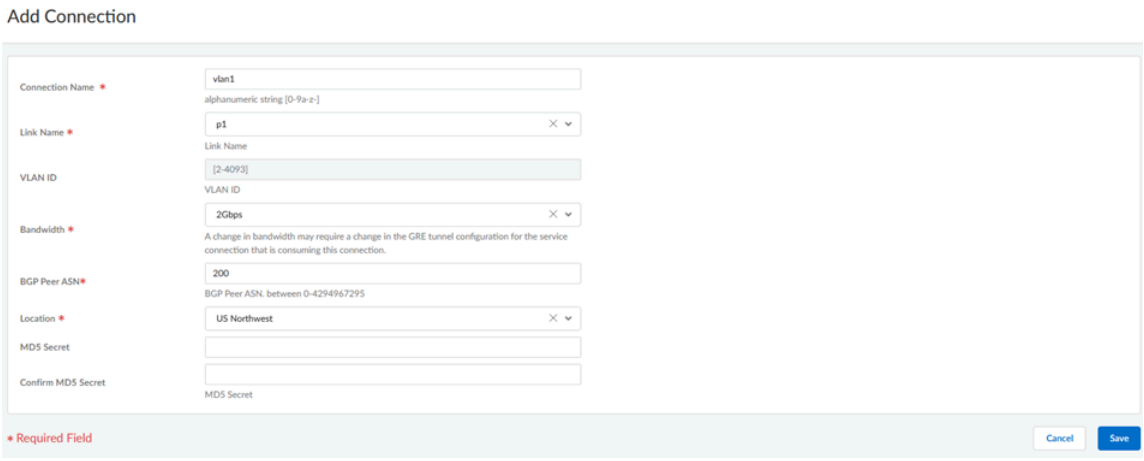
- **BGP**ピア**ASN** を入力します。

  Colo内の顧客のオンプレミス ルーターの自律システム (AS) 番号を入力します。範囲は1 ～ 4294967295です。

- 前の手順で作成した接続名からロケーションを選択します。

  指定する場所には、すでにサブネットを追加しておく必要があります。

- (任意) BGP**MD5**シークレットを入力します。



3. 完了するまで接続を作成し続けます。

   2つの接続を作成します。両方の接続は同じリージョン内にある必要があり、各接続は別々のゾーン内にある必要があります。これらの接続は、後の手順で作成するサービス接続で使用します。

STEP 4 | 構成をプッシュします。

コミット ジョブが完了したら、ブラウザーを更新して、[接続]の下のペアリング キーを表示します。

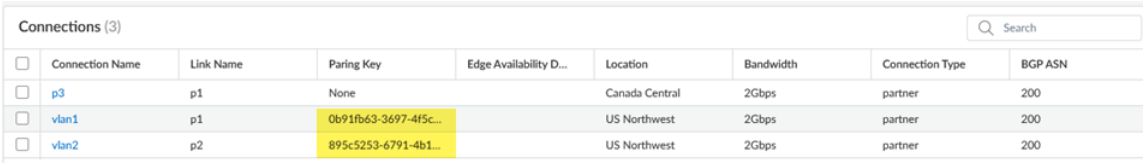
©2025 Palo Alto Networks, Inc.

STEP 5 | ペアリング キー を取得し、GCP でパートナー相互接続の構成を完了します。

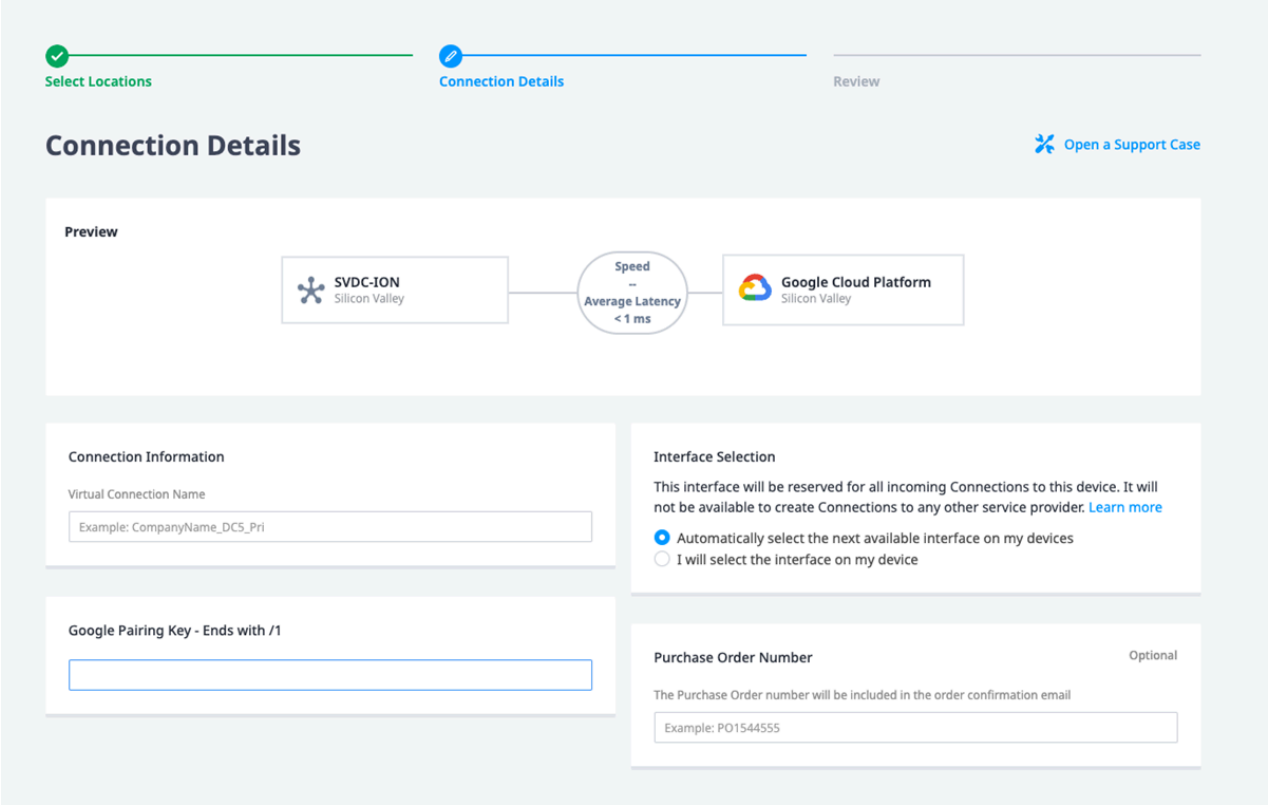
このペアリング キーは、Coloで パートナー相互接続 を設定するときに使用します。

新しい接続を初めてオンボードすると、[接続] 領域の [ステータス]に [ステータス]が**[PENDING_PARTNER]**に、**[BGP** ステータス]が**[DOWN]**に表示されます。接続ステータスを **ACTIVE**にするには、ペアリング キーを取得して、Coloで接続を入力します。

1. [ワークフロー] > **[Prisma Access**セットアップ] > **[Colo-Connect]** > [接続] に移動して、ペアリング キーをコピーします。



2. Coloに新しいVLAN接続を作成します。



3. ペアリング キーをColo VLANに貼り付けます。

   GCPはペアリング キーが消費されたことを検出し、VLANステータスを **ACTIVE**にし、Colo内のオンプレミス ルーターで構成するためのBGP IPアドレスを生成します。Prisma AccessはこれらのIPを使用して、ColoルーターとGCPクラウド ルーター間の各関連VLAN上で eBGP隣接関係を開始します。

STEP 6 | Colo-Connect 接続用に、顧客 (Colo) ルーターにeBGP ルーティングを作成します 。

顧客ルータとクラウド ルータ間の接続を確保するには、BGPピアリングを設定する必要があります。

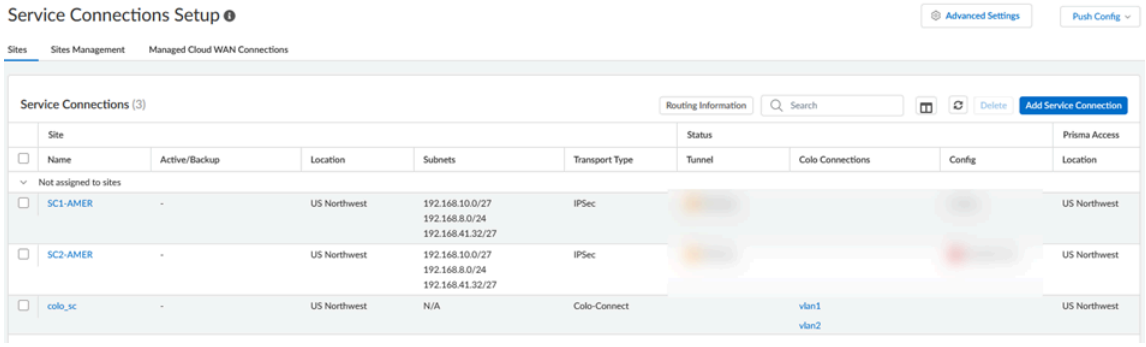
©2025 Palo Alto Networks, Inc.

STEP 7 | Colo-Connectで使用するサービス接続を設定します 。

STEP 8 | 構成をプッシュします。

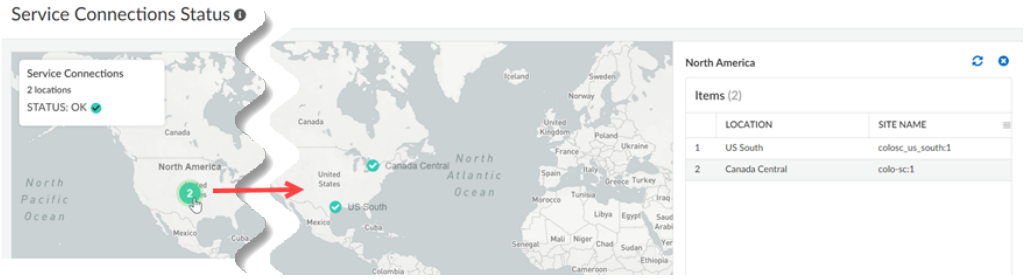
STEP 9 | Colo-Connect接続のステータスを確認します。

1. Colo-Connect 接続で使用されるサービス接続のステータスを確認するには、「ワークフロー] > **[Prisma Access** セットアップ] > [サービス接続]に移動します。



2. **[Manage (**管理**)]** > **[Configuration (**設定**)]** > **[NGFW**と**Prisma Access]**を選択します。構成スコープを**Prisma Access**に設定します。Prisma Accessの同期ステータスの下にあるサービス接続の同期ステータスを選択します。Colo-Connect接続がデプロイされているリージョンを選択します。

   - Colo-Connect接続とBGPルーティングの両方が稼働している場合、ステータスには **OK** と表示されます。
   - Colo-Connect接続は稼働しているが、BGPルーティングが稼働していない場合、ステータスには 警告が表示されます。
   - Colo-Connect接続とBGPルーティングがダウンしている場合、ステータスには **Down**と表示されます。
   - Colo-Connect接続は稼働していないが、BGPルーティングが稼働している場合、ステータスには エラーが表示されます。



3. 詳細については、リージョンボックスをクリックして、**[**ステータス**]** タブで情報を確認してください。

STEP 10 | [ワークフロー] > **[Prisma Access**セットアップ] > **[Colo Connect]**に移動して、Colo-Connect接続のペアリング キーを含む接続詳細を確認します。

 ©2025 Palo Alto Networks, Inc.

専用相互接続を使用したColo-Connect-デプロイメントの設定

専用相互接続を使用してPrisma Access Colo-Connect を設定するには、以下の手順を実行します。

STEP 1 | Colo-Connect 接続用のサブネットを作成します。

ここで作成したサブネットは、後の手順で作成する接続とサービス接続で使用します。

1. Strata Cloud Manager から、**[Workflows (ワークフロー)]** > **[Prisma Access**セットアップ**]** > **[Colo-Connect]**に移動します。次に 歯車のアイコンをクリックして設定を編集します。
2. **Colo-Connect**サブネットのプレフィックスを追加し、Prisma Accessロケーション (**PA** ロケーション) を指定します。

   最小サブネット /28 を入力します。
3. (任意) 複数の場所にColo-Connectインスタンスを作成する予定の場合は、場所ごとにサブネットを追加します。

   ロケーションごとに1つだけサブネットを構成できます。

©2025 Palo Alto Networks, Inc.

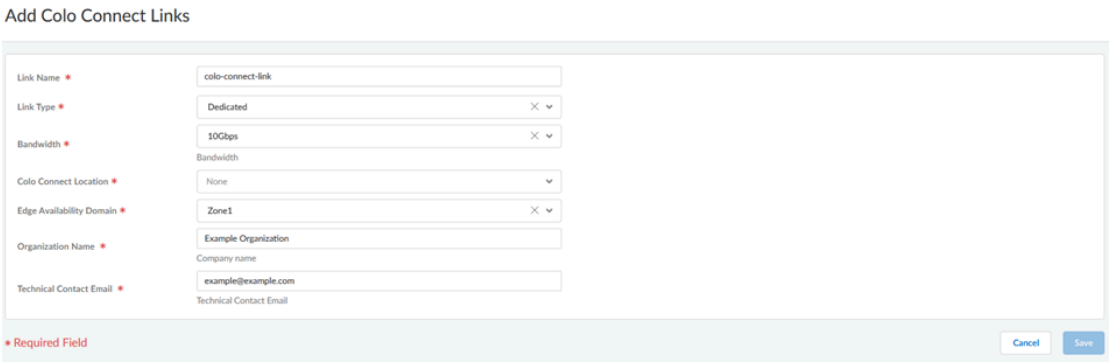
STEP 2 | 新しいColo-Connectリンク (相互接続とも呼ばれます) を追加します。

1. **[Workflows (ワークフロー)] > [Prisma Accessセットアップ] > [Colo-Connect] [Add Link** リンクを追加]に移動します。
2. リンクに一意の リンク名を付けます。
3. リンク タイプとして 専用 相互接続を選択します。
4. 残りのColo-Connectリンク パラメータを指定します。
   - 帯域幅として **10Gbps** または **20Gbps** を選択します。

     *20 Gbps*を選択した場合は、LACPを使用して専用相互接続リンクを*2*つの*10 Gbps*リンクに集約する必要があります。

     専用相互接続リンクの帯域幅を指定してコミットし、変更をプッシュした後は、その帯域幅を変更することはできません。
   - ドロップダウン リストから **Colo-Connect**ロケーションを選択します。

     専用相互接続に使用したのと同じ場所を選択してください。
   - エッジ可用性ドメインとしてゾーン**1**またはゾーン**2** を選択します。この値は、エッジ可用性ドメインに使用される GCP ゾーン から取得します。
   - このリンクに使用する 組織名 を入力します。
   - クラウド プロバイダーから LOA-CFA の詳細を受信する 電子メール を入力します。
     - GCP はこのメールを使用して、 認可書および接続施設割り当て書 (LOA-CFA)を送信します。LOA-CFA が Colo プロバイダーに送信され、接続のインストールを開始できることを確認してください。



STEP 3 | 専用接続が作成されると、Colo 施設は 接続をテストし 、テストが完了して使用できる状態になったことを通知します。

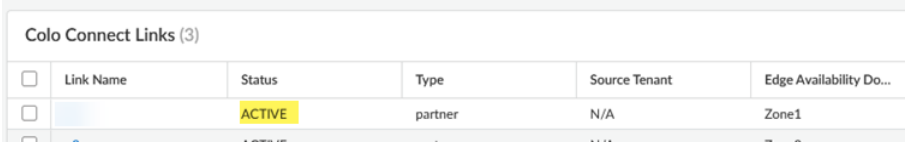
いいえ Prisma Access この手順では設定が必要です。Colo施設がテスト済みであることを知らせるまで、Prisma AccessでColo-Connect接続を作成しないでください。

©2025 Palo Alto Networks, Inc.

STEP 4 | Colo-Connectの接続 (*VLAN* アタッチメントとも呼ばれます) を作成します。

1. [ワークフロー] > **[Prisma Access** セットアップ**]** > **[Colo-Connect]** > **[Colo Connect** リンク**]**に移動して、専用リンクのステータスがアクティブであることを確認します。

   専用リンクのステータスがアクティブになるまで、Colo-Connectリンクを作成することはできません。



2. **[Workflows (**ワークフロー**)]** > **[Prisma Access**セットアップ**]** > **[Colo-Connect][Add Connection (**接続を追加**)]**に移動します。
3. 接続設定を構成します。
   - 接続の一意の 名前 を入力します。
   - 前の手順で構成したリンクからリンク名を選択します。
   - (任意) 接続の**VLAN ID**を入力します。

     手動で値を入力しない場合は、相互接続ベンダー (GCP) によって VLAN ID が生成されます。
   - 接続の 帯域幅 を選択します。

     1 Gbps、**2 Gbps**、**5 Gbps**、**10 Gbps**、**20 Gbps**から選択できます。

     相互接続に複数の接続を構成する場合は、接続の合計帯域幅が相互接続の帯域幅を超えないようにしてください。たとえば、20 Gbpsの専用相互接続の場合、それぞ

©2025 Palo Alto Networks, Inc.

れ2 Gbpsの接続を10個構成できますが、すべての接続の合計が20 Gbpsを超えることはできません。

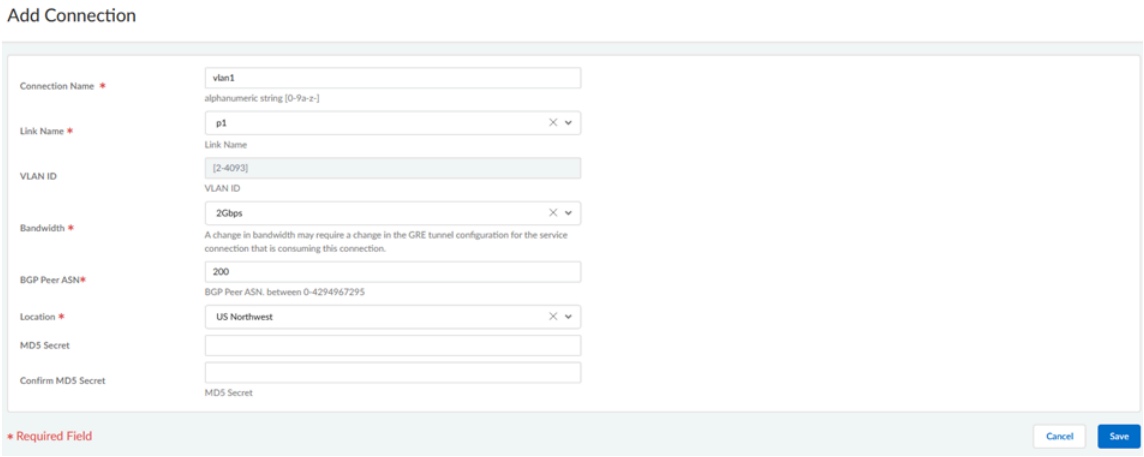
- **BGP**ピア**ASN** を入力します。

  Colo内の顧客のオンプレミス ルーターの自律システム (AS) 番号を入力します。範囲は1 ～ 4294967295です。

- 前の手順で作成した接続名からロケーションを選択します。

  指定する場所には、すでにサブネットを追加しておく必要があります。

- (任意) BGP**MD5**シークレットを入力します。



4. 完了するまで接続を作成し続けます。

   2つの接続を作成します。両方の接続は同じリージョン内にある必要があり、各接続は別々のゾーン内にある必要があります。これらの接続は、後の手順で作成するサービス接続で使用します。

STEP 5 | 構成をプッシュします。

STEP 6 | 顧客ルータでeBGP ルーティングを設定します 。

顧客ルータ間の接続を確保するには、BGPピアリングを設定する必要があります。

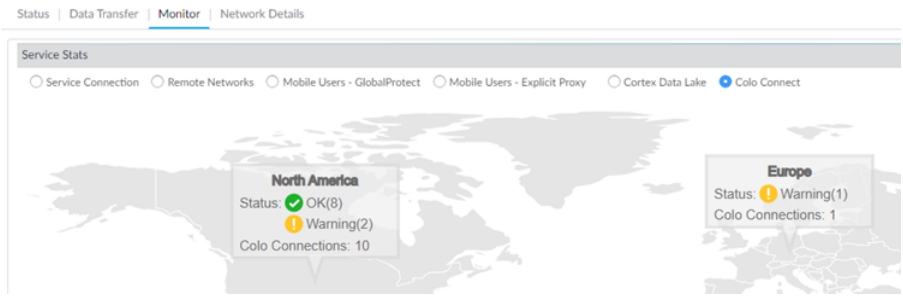
STEP 7 | Colo-Connectで使用するサービス接続を設定します 。

STEP 8 | 構成の変更をコミットしてプッシュし 、プッシュ スコープで**Colo-Connect**が選択されていることを確認します。

©2025 Palo Alto Networks, Inc.

STEP 9 | Colo-Connect接続のステータスを確認します。

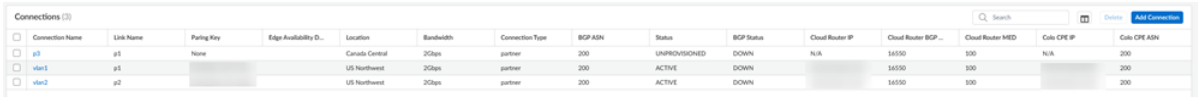
1. Colo-Connect 接続で使用されるサービス接続のステータスを確認するには、**[Manage (管理)]** > **[Configuration (設定)]** > **[NGFWとPrisma Access]**に移動します。構成スコープを**Prisma Access**に設定します。
2. Colo-Connect 接続が展開されているリージョンにマウスを移動します。
   - Colo-Connect接続とBGPルーティングの両方が稼働している場合、ステータスには **OK** と表示されます。
   - Colo-Connect接続は稼働しているが、BGPルーティングが稼働していない場合、ステータスには 警告が表示されます。
   - Colo-Connect接続とBGPルーティングがダウンしている場合、ステータスには **Down**と表示されます。
   - Colo-Connect接続は稼働していないが、BGPルーティングが稼働している場合、ステータスには エラーが表示されます。



3. 詳細については、リージョンボックスをクリックして、[ステータス] タブで情報を確認してください。

STEP 10 | **[ワークフロー]** > **[Prisma Accessセットアップ]** > **[Colo-Connect]** > **[Connections (接続)]**に進んで、Colo-Connect接続のネットワーク詳細を確認し、詳細を表示します。

専用リンクの場合、 ペアリング キーは**N/A**と表示されます。



顧客ルータで**VLAN eBGP**ルーティングを構成する

GCPは、デプロイメントの次の段階で顧客 (Colo) ルーターとクラウド ルーターのIPアドレスを作成します。

- パートナー相互接続の場合、ペアリング キーがColo (Equinixなど) によって使用された後に、GCPはIPアドレスを作成します。
- 専用相互接続の場合、Colo-Connect接続 (VLAN アタッチメント) をオンボードし、変更をコミットしてプッシュすると、GCPによってIPアドレスが作成されます。

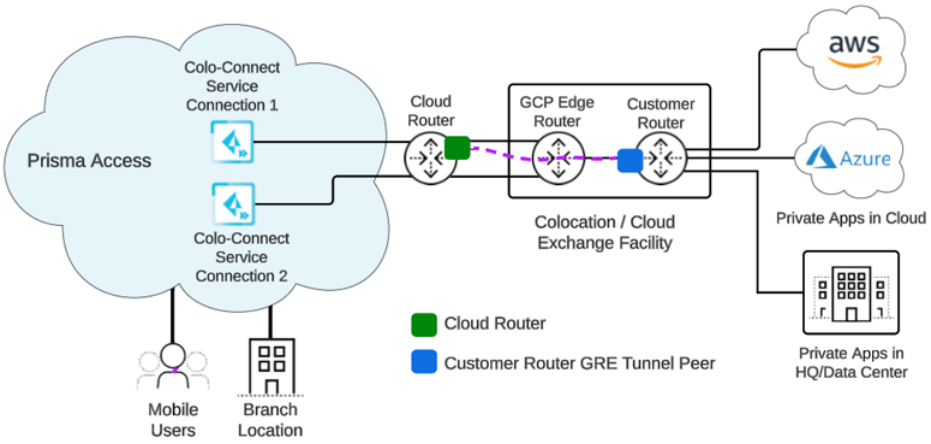
正しいルーティングを確実に行うには、次の操作を行う必要があります。

- ColoルーターのIPアドレス（Prisma Accessの**Colo CPE IP**）をローカルeBGP IPアドレスとして設定します。

©2025 Palo Alto Networks, Inc.

- クラウド ルーターのIPアドレス (**Cloud Router IP**) を ColoルーターのeBGPピア アドレスとして設定します。

完了すると、Coloルータとクラウド ルータ間の接続 (VLANアタッチメント) にeBGPが設定されます。



このルーティングを作成することは、GREトンネル ルーティングを設定するための最初のステップです。サービス接続の構成中にGREトンネルを設定すると、GREトンネル ルーティングが完了します。

Coloとクラウド ルーター間のルーティングを構成するには、次の手順に従います。

STEP 1 | Strata Cloud Managerから、サブネット、リンク、接続を作成し、**Push Config**を実行します。

相互接続タイプ (パートナーまたは専用)に固有のワークフローを使用します。パートナー相互接続の場合は、ペアリング キーをColo VLANに貼り付けたことを確認してください。

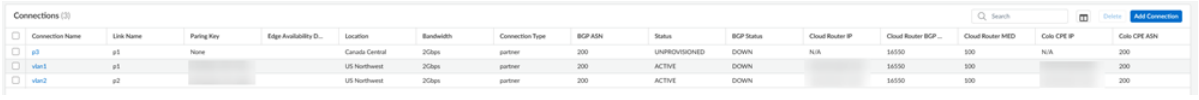
STEP 2 | [ワークフロー] > **[Prisma Access** セットアップ] > **[Colo-Connect]** > [接続]に移動します。

STEP 3 | 次の接続要素をメモします。

- **Colo CPE IP**
- クラウドルーター **IP**
- クラウドルーター **BGP ASN**

次の例では:

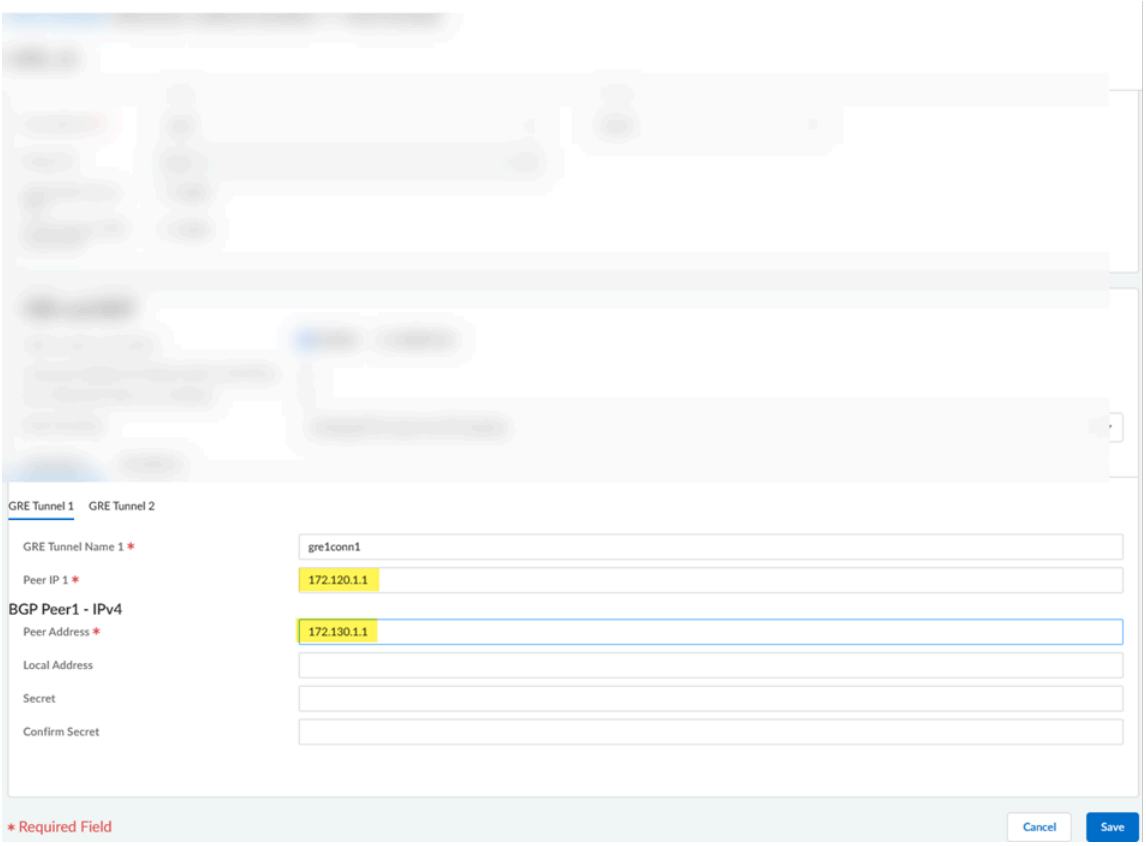
- vlan-central-1接続の場合、**Colo CPE IP**は 169.254.24.170/29、Cloud**Router IP**は169.254.24.169/29、Cloud**Router BGP ASN**は16550 です。vlan-central-2 接続の場合、Colo CPE IPは169.254.120.74/29、Cloud Router IPは169.254.120.73/29、Cloud Router BGP
- **ASN**は**16550** です
- 。



 ©2025 Palo Alto Networks, Inc.

STEP 4 | Colo-Connectサービス接続を設定するときに、ローカルGRE IPアドレスに使用するIPアドレスを決定します。

これらは、Colo-Connect サービス接続 ([ワークフロー] > **[Prisma Access**セットアップ] > [サービス接続]) を設定するときに構成します。ピア**IP 1** 領域および必要に応じて ピア**IP 2** 領域。



最大10Gbpsのスループットをサポートするようにサービス接続を構成する場合は、 接続**1**と接続**2**にそれぞれ1つのトンネルを配置し、各サービス接続に合計2つのトンネルを配置します。

10 Gbpsを超えるスループット (最大20 Gbps) をサポートするようにサービス接続を構成する場合は、 接続と接続**2**にそれぞれ2つのトンネルを配置し、各サービス接続に合計4つのトンネルを配置します。

次の例では、10 Gbpsを超えるスループット用にトンネルが設定されており、接続ごとに2つのトンネルが使用され、次のピアIPアドレスが使用されています。

- 接続 1 の場合は 172.120.1.1
- 接続 1 の場合は 172.130.1.1
- 接続 2 の場合は 172.121.1.1
- 接続 2 の場合は 172.131.1.1

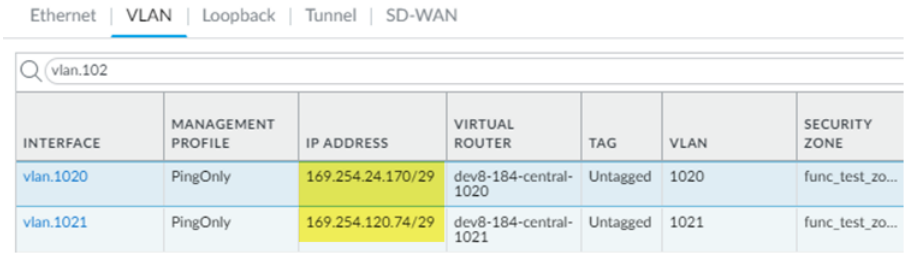
©2025 Palo Alto Networks, Inc.

STEP 5 | Colo ルーターにログインします。

次の構成スクリーンショットでは、ColoルーターとしてPalo Alto Networks次世代ファイアウォールを使用しています。

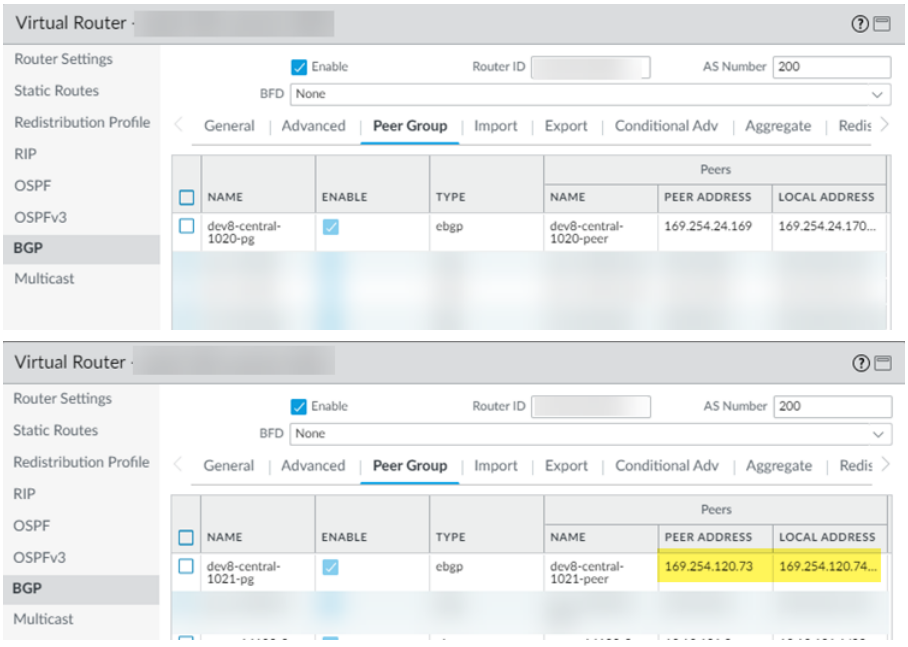
STEP 6 | **Colo CPE IP** アドレスをIPアドレスとして指定して、VLANインターフェイスを追加します。

次世代ファイアウォールをColoルーターとして使用している場合は、 ネットワーク > インターフェイス > **VLAN** に移動し、VLANインターフェイス を追加して 、 仮想ルーターの名前を指定します。



STEP 7 | ColoルーターのIPアドレス (**Colo CPE IP**) をローカルeBGP IPアドレスとして設定し、クラウド ルーターのIPアドレス (**Cloud Router IP**) を Colo ルーターのeBGPピア アドレスとして設定します。

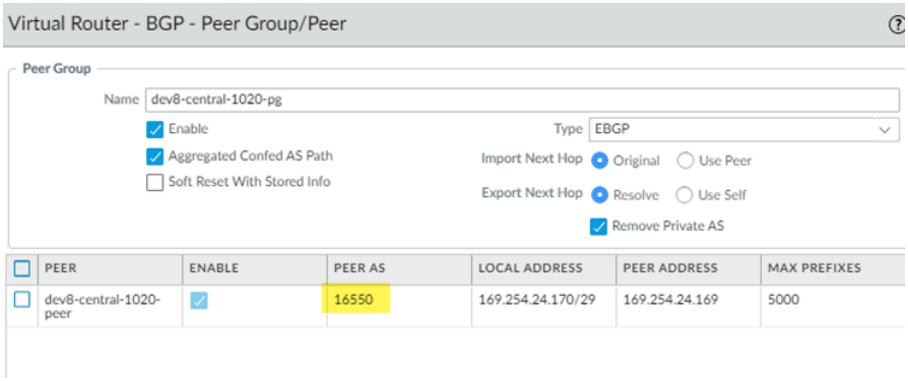
次世代ファイアウォールを Colo ルーターとして使用している場合は、[ネットワーク > 仮想ルーター]に移動して仮想ルーターを 追加し 、**[BGP]** > [ピア グループ]に移動して、 ピア アドレス として **Colo CPE IP** を 入力し、 ローカル アドレスとして クラウド ルーター**IP**を入力します。



 ©2025 Palo Alto Networks, Inc.

STEP 8 | **Cloud Router BGP ASN**をeBGP ピアの自律システム番号 (ASN) として設定します。

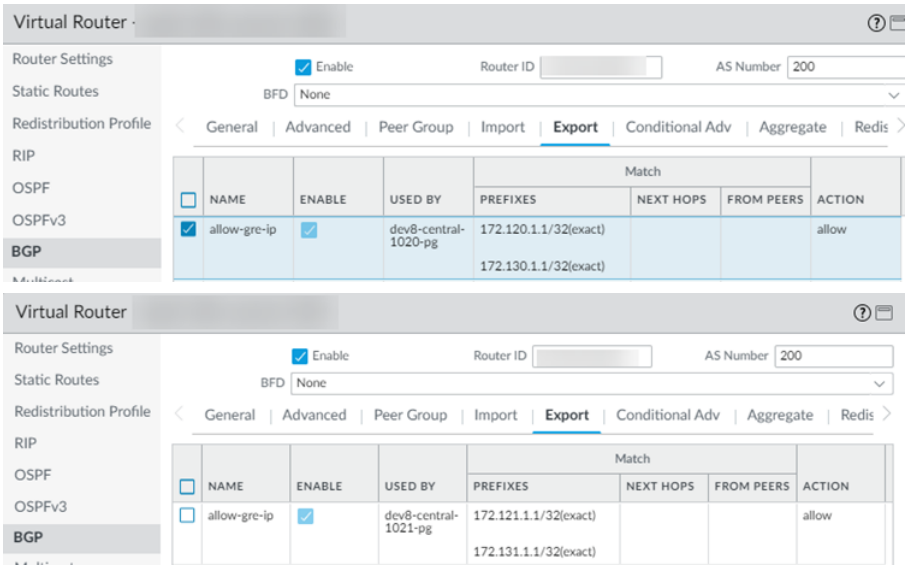
次世代ファイアウォールを Colo ルーターとして使用している場合は、[ネットワーク] > [仮想ルーター]に移動して仮想ルーターを追加し 、**[BGP]** > [ピア グループ]に移動してピア グループを追加し 、 ピア**AS** として **16500**を選択します。



STEP 9 | ローカルGRE IPアドレスのみをクラウド ルーターのピアIPアドレスにアドバタイズできるようにするBGPエクスポート ポリシーを作成します。

クラウド ルーターは限られた数のルートしか受信できないため、サービス接続GREトンネルのIPアドレス間のルーティングのみがクラウド ルーターに送信されるようにポリシーを作成する必要があります。

Colo ルーターとして次世代ファイアウォールを使用している場合は、[ネットワーク] > [仮想ルーター]に移動して仮想ルーター を追加し 、**[BGP]** > [エクスポート]に移動してエクスポート ルール を追加し 、ピアIPアドレスとして使用される IP アドレス を一致させて 、[許可]の[アクション] を作成します。



STEP 10 | Colo-Connectサービス接続を作成します。

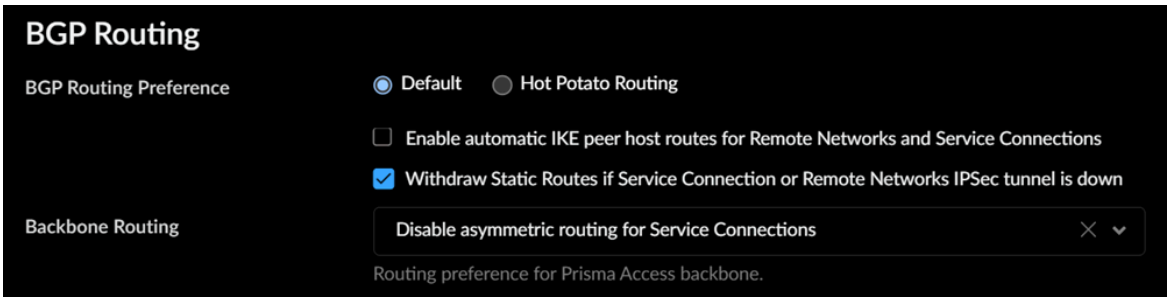
©2025 Palo Alto Networks, Inc.

Colo-Connectサービス接続を作成する

Colo-Connectはサービス接続を使用しますが、Prisma Accessサービス接続では、IPSecトンネルの代わりにGREトンネルを使用し、ルーティングには常にBGPを使用します。Colo-Connectサービス接続を構成するには、次の手順を実行します。

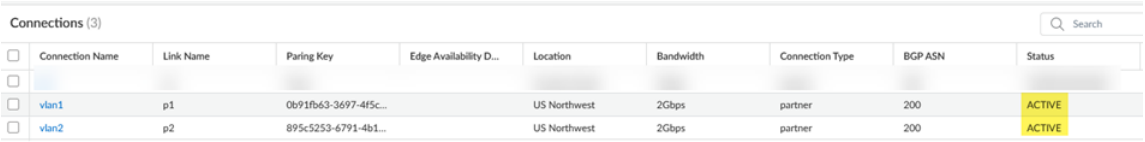
STEP 1 | [ワークフロー] > **[Prisma Access**セットアップ**]** > [サービス接続] > [詳細設定]に移動し、[サービス接続またはリモート ネットワーク **IPSec** トンネルがダウンしている場合は静的ルートを取り消す]を選択して、Prisma Accessが静的ルートを取り消すことを確認します。

この選択肢を選択すると、GRE トンネルがダウンした場合に、GRE トンネルによって使用される静的ルートが取り消されるようになります。



STEP 2 | ワークフロー > **Prisma Access** セットアップ > **Colo-Connect** > 接続 タブに移動し、 ステータスを確認して接続がアクティブ 状態であることを確認します。

接続のステータス がアクティブになるまで、サービス接続を構成することはできません。

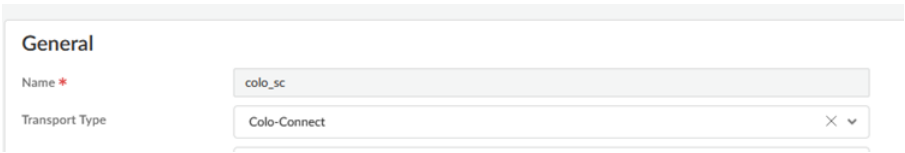


STEP 3 | **[Manage (管理)]** > **[Configuration (設定)]** > **[NGFW**と**Prisma Access]** に移動し、構成範囲を **Prisma Access**に設定します。

STEP 4 | Colo-Connect構成がサービス接続領域にプロビジョニングされるように、**Prisma Access** 同期ステータスを更新します。

STEP 5 | [ワークフロー] > **[Prisma Access]** > [サービス接続] [サービス接続の追加]に移動し、一意の[名前]を付けて、[トランスポート タイプ] で **[Colo-Connect]**を選択します。

入力する名前の長さが*31*文字以下であることを確認してください。 *32*文字以上の名前を入力すると、*Prisma Access*インフラストラクチャでトンネルが誤ってマッピングされます。



 ©2025 Palo Alto Networks, Inc.

STEP 6 | サービス接続で使用する2つの接続 (接続**1** と 接続 **2**) を選択します。

これらの接続は2つの異なるゾーンに存在する必要があります。



STEP 7 | 接続**1**と接続**2**のアクティブまたはバックアップを選択します

サービス接続を設定するときは、次のガイドラインに従ってください。

- 次のモードで接続を構成できます。
  - アクティブ/アクティブ
  - アクティブ/バックアップ
  - バックアップ/アクティブ

  両方の接続を バックアップ/バックアップ モードで構成することは無効であり、サポートされていません。
- 接続の帯域幅はすべてのモードで同じである必要があります。
- 接続は異なるゾーンに存在する必要があります。
- サービス接続に指定できる最大帯域幅は20 Gbps です。接続に **20 Gbps** の 帯域幅 を指定した場合、その接続を アクティブ/アクティブ 構成で使用することはできません (アクティブ/バックアップとして設定する必要があります)。
- 同じサービス接続で専用相互接続とパートナー相互接続を混在させないでください。また、サービス接続が異なるゾーンを使用するようにしてください。この表は、ゾーン、場所、帯域幅、およびロールがサービス接続のガイドラインと要件に従っていることを前提として、サービス接続で許可される構成と許可されない構成を示しています。

接続**1**は、	接続 **2**は、	有効な**Colo-Connect**サービス接続構成に属していますか**?**
パートナー接続 1	パートナー接続 2	はい
専用接続 1	専用接続 2	はい
パートナー接続 1	パートナー接続 1	いいえ
専用接続 1	専用接続 1	いいえ
パートナー接続	専用接続	いいえ

©2025 Palo Alto Networks, Inc.

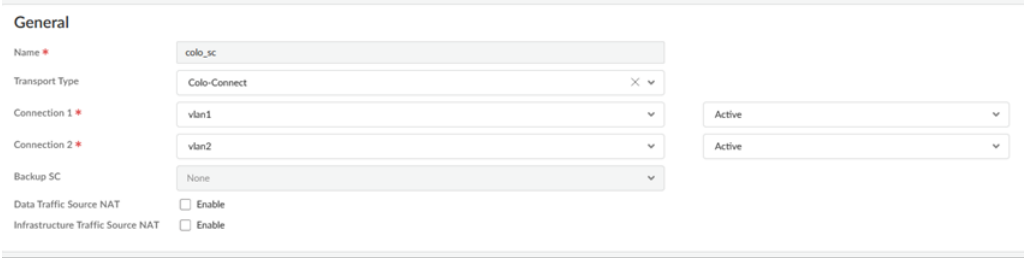
STEP 8 | (オプション、ホット ポテト ルーティング デプロイメントの場合のみ) ホット ポテト ルーティング構成で、優先バックアップ(バックアップ **SC**)として使用するサービス接続を選択します。

Colo-Connect サービス接続として構成されているサービス接続のみを選択できます。 接続障害が発生した場合、Prisma Accessは優先サービス接続として選択したバックアップSCを使用します。2つ以上のサービス接続を作成した場合、バックアップ サービス接続を選択すると、非対称ルーティングの問題を防ぐことができます。

STEP 9 | (任意) モバイル ユーザーのソースNATを有効にします (GlobalProtect IPプール アドレス、インフラストラクチャ サブネット内のIPアドレス、またはその両方)。

Prisma AccessGlobalProtectモバイルユーザーとデータセンターのプライベートアプリケーションおよびリソース間のNATトラフィックに使用される1つまたは複数のサービス接続でサブネットを指定することができます。

- データ トラフィック ソース**NAT**を有効にする- モバイル ユーザIPアドレス プール アドレスに対してNATを実行し、それらのアドレスがデータ センターにアドバタイズされないようにし、サービス接続で指定したサブネットのみがデータ センターでアドバタイズされ、ルーティングされるようにします。
- インフラストラクチャ トラフィック ソース**NAT**を有効にする- インフラストラクチャ サブネットのアドレスに対して NAT を実行し、それらのアドレスがデータ センターにアドバタイズされないようにし、サービス接続で指定したサブネットのみがデータ センターでアドバタイズされ、ルーティングされるようにします。
- **IP**プール- モバイル ユーザーのIPアドレス プール、インフラストラクチャ サブネット、またはその両方でNATを実行するために使用されるIPアドレス プールを指定します。プライベートIP (RFC 1918) サブネットまたはルーティング ドメイン内でルーティング可能で、モバイル ユーザー - GlobalProtect IPアドレス プールまたはインフラストラクチャ サブネットと重複しない適切なサブネットを使用します。/25から/32までのサブネットを入力します。



STEP 10 | **GRE** および**BGP**領域で、サービス接続のGREトンネルとBGP設定を構成します。

BGPは常に有効に設定されます。

1. （任意）以下の選択肢から選択します：
   - 顧客宅内機器 (CPE) の eBGP ピアからの送信プレフィックスに企業アクセス ノード (サービス接続) の**no-export**コミュニティを追加するには、**[Add no-export**

 ©2025 Palo Alto Networks, Inc.

community (エクスポート禁止コミュニティの追加)] を **[Enabled Out (有効アウト)]**に設定します。この機能はデフォルトでは 無効になっています。

ホットポテト ルーティング モードではこの機能を使用しないでください。

- BGP 経由で顧客構内設備 (CPE) に送信されるモバイル ユーザー IP サブネット アドバタイズメントの数を減らすには、**[Summarize Mobile User Routes before advertising (アドバタイズする前にモバイル ユーザー ルートを集約する)]**を選択します。

  デフォルトでは、Prisma Accessは、モバイルユーザーのIPアドレスプールを、/24サブネットのブロックでアドバタイズします。それを要約すると、指定したサブネットに基づいてプールがアドバタイズされます。たとえば、Prisma Accessは、パブリックユーザーのモバイルIPプールを、アドバタイズ前に10.8.1.0/24、10.8.2.0/24、10.8.3.0/24などのサブネットに分割するのではなく、/20のサブネットを使用して10.8.0.0/20のプールをアドバタイズします。これらのアドバタイズを要約することで、CPEルーティングテーブルに保存されるルート数を削減できる可能性があります。たとえば、限定された数のルートを受け付けるクラウドVPNゲートウェイ（仮想プライベートゲートウェイ（VGW）またはトランジットゲートウェイ（TGW））で、IPプールの要約を使用することができます。

  > ホットポテトルーティングを有効にしてルート集約を有効にすると、*Prisma Access*は非対称ルーティングを引き起こす可能性のある *AS-PATH* を先頭に追加しなくなりました。ホットポテトルーティングでルート要約を有効にする前に、データセンターまたは本社からのリターントラフィックの、対称的なリターンが保証されていることを確認してください。

- Prisma AccessBGPピアが、組織のネットワークにルートを転送することを防止します。**Don't Advertise Prisma Access Routes**（**Prisma Access**ルートをアドバタイズしない）.

  デフォルトで、Prisma Accessは、ローカルルート、および他のサービス接続、リモートネットワーク、およびモバイルユーザーサブネットから受信するすべてのプレフィックスを含め、すべてのBGPルーティング情報をアドバタイズします。Prisma AccessによるBGPアドバタイズメントの送信を防止しながら、受信したBGP情報を使って、他のBGPネイバーからルートを学習するには、このチェックボックスを選択します。

  > このオプションを選択した場合、*Prisma Access*は*BGP*アドバタイズメントを送信しないため、オンプレミスの機器で静的ルートを設定して、*Prisma Access*に戻るルートを確立する必要があります。

- 「ルート交換」設定とは何ですか？

2. GREトンネルを使用してサービス接続のルーティングを設定します。
3. Strata Cloud Manager から、 [ワークフロー] > **[Prisma Access** セットアップ] > [サービス接続] に戻り 、接続 **1** の **GRE** トンネル名 **1** と ピア **IP 1** を入力して 接続 **1** の GRE トンネルを作成します。10 Gbps を超える帯域幅が必要な場合は、接続 1 の 2 番目のト

©2025 Palo Alto Networks, Inc.

ンネルの **GRE** トンネル名 **2** と ピア **IP 2** を 入力します。次に、同じ手順を繰り返して接続 **2** の GRE トンネルを作成します。

接続内のGREトンネルの各ペアは、最大10 Gbpsの帯域幅をサポートします。10 Gbpsを超える帯域幅が必要な場合は、接続ごとに2つのトンネルを構成します。以下に例を示します。

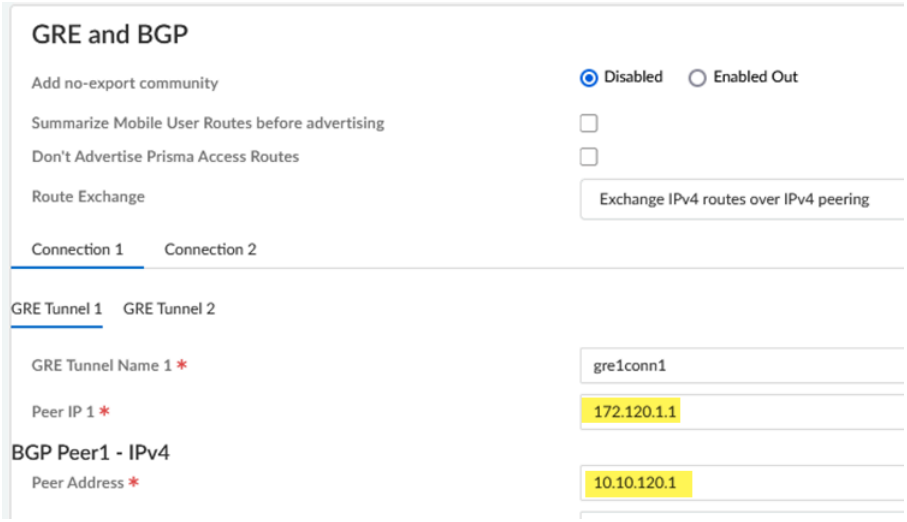
ピア IPには、コロケーション内のオンプレミス ルーターのGRE IPアドレスを入力します。

BGP値にはIPv4アドレスを使用します。IPv6はサポートされていません。

4. BGP ピア1の ピア アドレス と ローカル アドレス を入力し、接続1に2 番目が必要な場合は BGP ピア2のアドレスとローカル アドレスを入力します。

   ピア アドレスには、ColoルーターのBGP ピアIPアドレスを入力します。 ローカル アドレスには、GREトンネル経由のBGPネットワーク確立に使用されるアドレスを入力します。

5. (任意) BGPシークレットを設定するには、 シークレットとシークレットの確認の値を入力します。

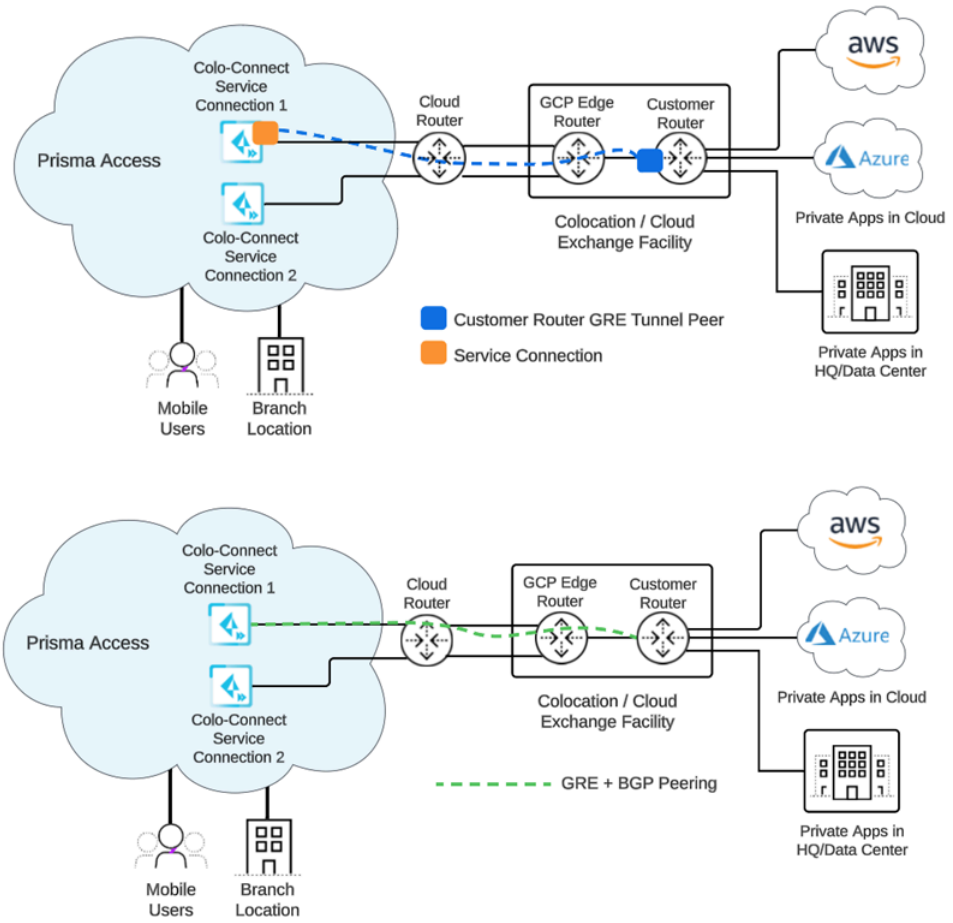


STEP 11 | 構成の変更をコミットしてプッシュし 、プッシュ スコープで**Colo-Connect**が選択されていることを確認します。

GREトンネルを使用してサービス接続のルーティングを設定します。

Coloルータは、GRE トンネル ピアIPアドレスをクラウド ルータにアドバタイズし、クラウド ルータからGREトンネルのサブネットを学習します。顧客ルータの VLAN 経由で eBGP ルーティングを最初に設定したときに、GRE トンネルのローカル到達可能性をアドバタイズしました。クラウド ルータとColoルータがColoサブネットとローカルGRE IPアドレスのルートを相互にアドバタイズして学習すると、サービス接続で使用される GRE トンネルがアクティブ (アップ) になります。

©2025 Palo Alto Networks, Inc.



ルーティングを設定し、サービス接続にGREトンネルを追加するには、次の手順を実行します。

STEP 1 | BGP ピア1のピア アドレスとローカル アドレスに使用するIPアドレスをメモします。また、接続1に2つ目のIPアドレスが必要な場合は、BGP ピア2 のIPアドレスもメモします。

次の例では、次のピア アドレスとローカル アドレスを使用します。

- ピア アドレス- 接続 1の場合は10.10.120.0 および10.10.130.1、接続2の場合は10.10.120.2および 10.10.130.2
- ローカル アドレス- 接続1の場合は 10.10.120.2 と 10.10.130.2、接続2の場合は 10.10.121.2と 10.10.131.2

STEP 2 | サービス接続でピア**IP1** に使用する IP アドレスと、必要に応じてピア**IP2**アドレスをメモします。

これらのIPアドレスを使用して、ローカルGRE IPアドレスがColo-Connectサービス接続にアドバタイズされるのを防ぐ拒否ポリシーを作成します。

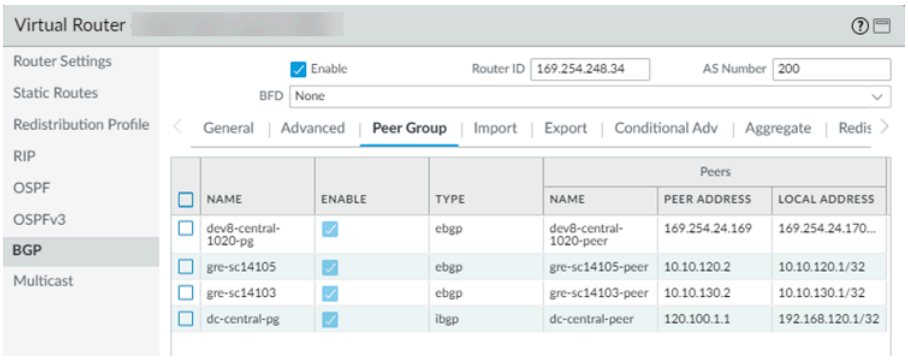
このドキュメントのすべての例では、次のIPアドレスを使用します。

- 接続 1 の場合は 172.120.1.1
- 接続 2 の場合は 172.121.1.1

©2025 Palo Alto Networks, Inc.

STEP 3 | ピアおよびローカルIPアドレスのピア グループを構成します。

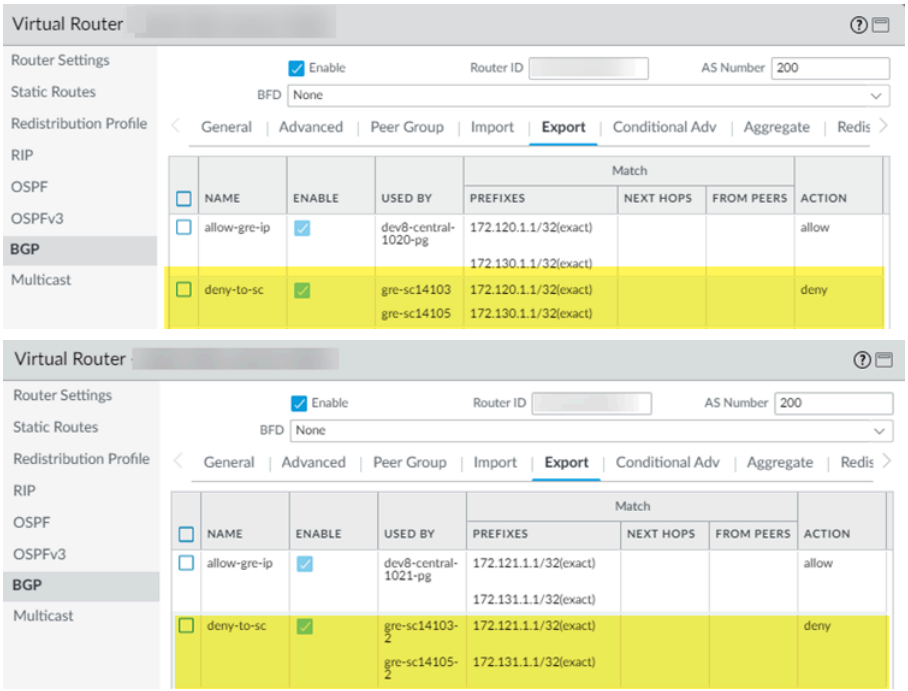
次世代ファイアウォールを Colo ルーターとして使用している場合は、[ネットワーク] > [仮想ルーター]に移動し、[仮想ルーター][追加] に移動して、**[BGP]** > [ピア グループ]に移動し、[ピア アドレス] として[ピア アドレス] を入力し、[ローカルアドレス]として [ローカルアドレス] を入力します。



STEP 4 | 設定したピアIPアドレス (172.120.1.1、172.130.1.1、172.121.1.1、および 172.131.1.1) を拒否するBGPエクスポート ポリシーを作成し、作成したピア グループに適用します。

このエクスポート ポリシーは、ローカル GREトンネル ピアIPアドレスにDENYルールを適用し、他のすべてのルートをサービス接続にアドバタイズできるようにします。

Colo ルーターとして次世代ファイアウォールを使用している場合は、[ネットワーク] > [仮想ルーター]に移動して仮想ルーター を追加し 、**[BGP]** > [エクスポート]に移動してエクスポート ルール を追加し 、ピアIPアドレスとして使用される IP アドレス を一致させて 、[拒否]の[アクション] を作成します。



 ©2025 Palo Alto Networks, Inc.

Colo-Connectサービス接続の帯域幅を増減する

サービス接続を構成するときは、それに関連付ける接続 (VLAN アタッチメント) に基づいて帯域幅を構成します。サービス接続ごとに2つの接続を割り当て、接続ごとに1つまたは2つのGREトンネルを割り当てます。

各Colo-Connectサービス接続は最大 20 Gbps をサポートしますが、サービス接続内の各GREトンネルは10 Gbpsをサポートします。このため、Colo-Connectサービス接続でGREトンネルを追加または削除してリンクの合計帯域幅を変更する必要があり、その結果、サービス接続帯域幅が10 Gbpsを超えたり下回ったりすることがあります。

Colo-Connectサービス接続の帯域幅を増やす

既存のサービス接続の帯域幅を10 Gbps以上に増やすには、次の手順を実行します。

STEP 1 | [ワークフロー] > **[Prisma Access** セットアップ] > **[Colo-Connect]**に移動します。

STEP 2 | サービス接続に関連付けられている リンク名 を選択します。

STEP 3 | リンク（相互接続）の 帯域幅 を増やします。

STEP 4 | 構成をプッシュします。

STEP 5 | [ワークフロー] > **[Prisma Access** セットアップ] > [サービス接続]に移動します。

STEP 6 | Colo-Connect サービス接続に追加の GRE トンネルを追加します。

STEP 7 | 構成をプッシュします。

STEP 8 | GREトンネルのVLAN eBGPルーティングおよび サービス接続ルーティング のエクスポート ポリシーにGREローカル (ピア) IPアドレスを追加します。

Colo-Connectサービス接続の帯域幅を減らす

既存のサービス接続の帯域幅を10 Gbps以上に減らすには、次の手順を実行します。

STEP 1 | [ワークフロー] > **[Prisma Access** セットアップ] > **[Colo-Connect]**に移動します。

STEP 2 | サービス接続に関連付けられている リンク名 を選択します。

STEP 3 | リンク（相互接続）の 帯域幅 を減らします。

STEP 4 | 構成をプッシュします。

余分なGREトンネルを削除するためにサービス接続を再構成する必要はありません。 Prisma Accessは、サービス接続プッシュ スコープで変更をコミットしてプッシュすると、リンクの帯域幅を検出して下げ、余分なトンネルを削除します。

Colo-Connect接続を削除する

Colo-Connect接続を削除するには、設定の逆の順序で、次の手順を実行します。

STEP 1 | ワークフロー] > **[Prisma Access** セットアップ] > サービス接続]に移動し、サービス接続を選択して[削除] することで、接続に関連付けられているサービス接続を削除します。

©2025 Palo Alto Networks, Inc.

STEP 2 | 構成をプッシュします。

STEP 3 | 「ワークフロー」 > **[Prisma Access**セットアップ**]** > **[Colo-Connect]**の順に進み、[オンボーディング] セクションで [接続名] を選択して 削除することで、接続に関連付けられている Colo-Connect 接続を削除します 。

STEP 4 | リンク名 を選択して 削除し、Colo-Connect リンクを削除します 。

STEP 5 | GREトンネルのVLAN eBGPルーティングおよびサービス接続ルーティングのエクスポートポリシーからGREローカル (ピア) IPアドレスを削除します。

Prisma Access Colo-Connect を設定する（Panorama）

パートナー相互接続を使用した**Prisma AccessColo-Connect-**デプロイメントの設定

パートナー相互接続を使用してPrisma Access Colo-Connect を設定するには、以下の手順を実行します。

STEP 1 | Colo-Connect 接続用のサブネットを作成します。

ここで作成したサブネットは、後の手順で作成する接続とサービス接続で使用します。

1. **[Panorama]** > **[**クラウドサービス**]** > **[**構成**]** > **[Colo-Connect]** へと移動し、歯車のアイコンをクリックして設定を編集します。
2. **Colo-Connect**サブネットを追加し、Prisma Accessロケーション (**PA**ロケーション) を指定します。

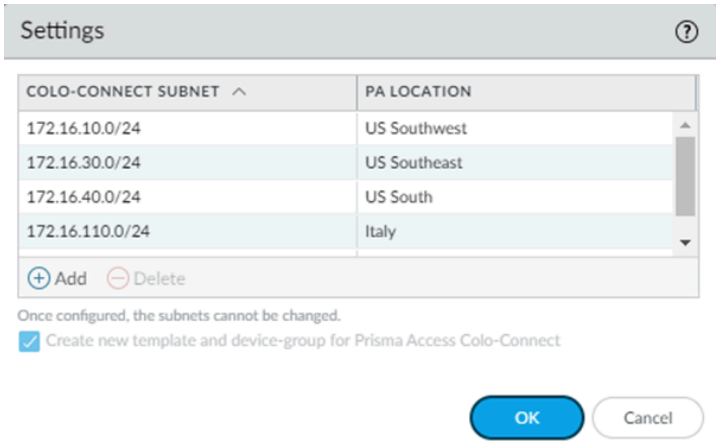
   最小サブネット /28 を入力します。
3. (任意) 複数の場所にColo-Connectインスタンスを作成する予定の場合は、場所ごとにサブネットを追加します。

   ロケーションごとに1つのサブネットを構成できます。
4. **Prisma Access Colo-Connect** の新しいテンプレートとデバイス グループの作成を選択します。

   Colo-Connect デプロイメントを初めて構成する場合は、このチェック ボックスをオンにして、テンプレートとデバイス グループ (それぞれ Colo_Connect_Template と Colo_Connect_Device_Group) が Colo-Connect 用に作成されるようにします。これら

©2025 Palo Alto Networks, Inc.

のテンプレートとデバイス グループを作成すると、このチェックボックスはグレー表示されます。

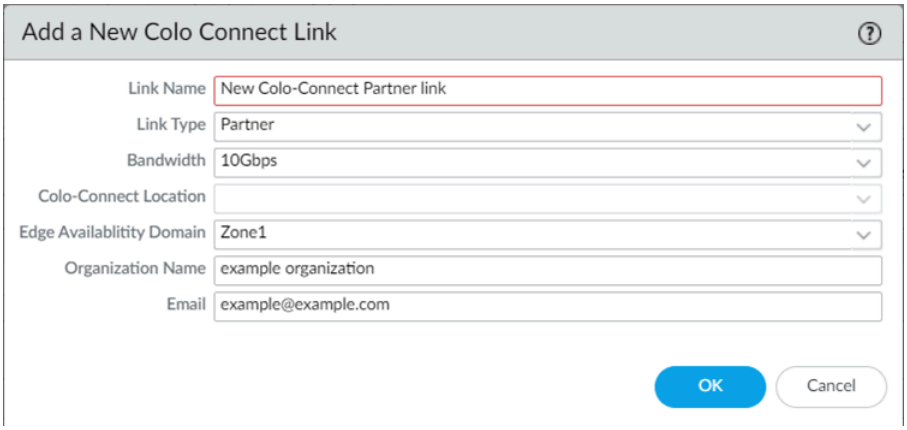


STEP 2 | 新しいColo-Connectリンク (相互接続とも呼ばれます) を追加します。

1. **Panorama** > クラウドサービス > **Configuration** (設定) > **Colo-Connect** > **Colo Connect**リンク へと移動し、 Colo-Connectリンクを追加します。.
2. リンクに一意の リンク名を付けます。
3. パートナーのインターコネクトを選択します。

   VLAN IDを入力する必要はありません。VLANアタッチメントの設定を完了するためにペアリングキーを使用する際に、ColoがVLAN IDを提供します。
4. 残りのColo-Connectリンク パラメータを指定します。
   - 帯域幅として **10Gbps** または **20Gbps** を選択します。

     専用相互接続リンクの帯域幅を指定し、変更をコミットしてプッシュした後に変更することはできません。
   - エッジ可用性ドメインとしてゾーン**1**またはゾーン**2** を選択します。この値は、エッジ可用性ドメインに使用される GCP ゾーン から取得します。
   - このリンクに使用する 組織名 を入力します。
   - このリンクに使用する メールアドレス を入力してください。どのメールアドレスでも構いません。



©2025 Palo Alto Networks, Inc.

STEP 3 | Colo-Connectの接続 (*VLAN* アタッチメントとも呼ばれます) を作成します。

1. **Panorama** > クラウドサービス > **Configuration** (設定) > **Colo-Connect** > オンボーディング へと移動し、新規接続を追加します。.
2. 接続設定を構成します。
   - 接続の一意の 名前 を入力します。
   - 前の手順で構成したリンクからリンク名を選択します。
   - 接続の 帯域幅 を選択します。

     1 Gbps、**2 Gbps**、**5 Gbps**、**10 Gbps**、**20 Gbps**から選択できます。

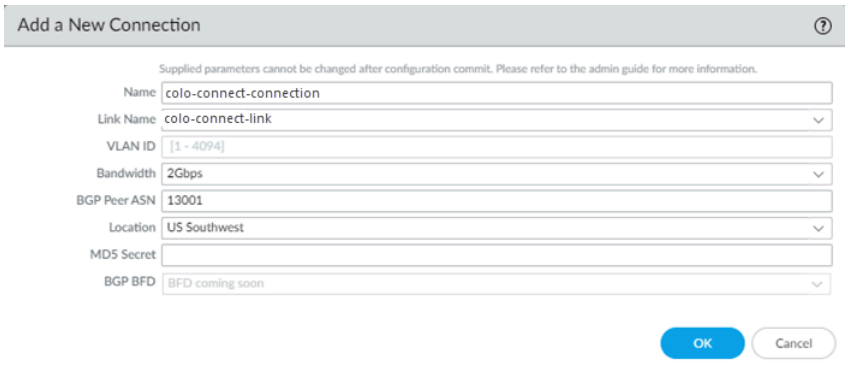
     相互接続に複数の接続を構成する場合は、接続の合計帯域幅が相互接続の帯域幅を超えないようにしてください。たとえば、パートナー相互接続が10 Gbps の場合、それぞれ1 Gbpsの接続を10個構成できますが、すべての接続の合計が10 Gbpsを超えることはできません。

     デプロイメントに*16*を超える接続が必要な場合は、*Palo Alto Networks*アカウント チームに連絡してください。アカウント チームは、リクエストに対応するために*SRE*ケースを開きます。
   - **BGP**ピア**ASN** を入力します。

     Colo内の顧客のオンプレミス ルーターの自律システム (AS) 番号を入力します。範囲は1 ～ 4294967295です。
   - 前の手順で作成した接続名からロケーションを選択します。

     指定する場所には、すでにサブネットを追加しておく必要があります。
   - (任意) BGP**MD5**シークレットを入力します。

     BGP BFDフィールドは将来の*Colo-Connect*リリースのために予約されています。



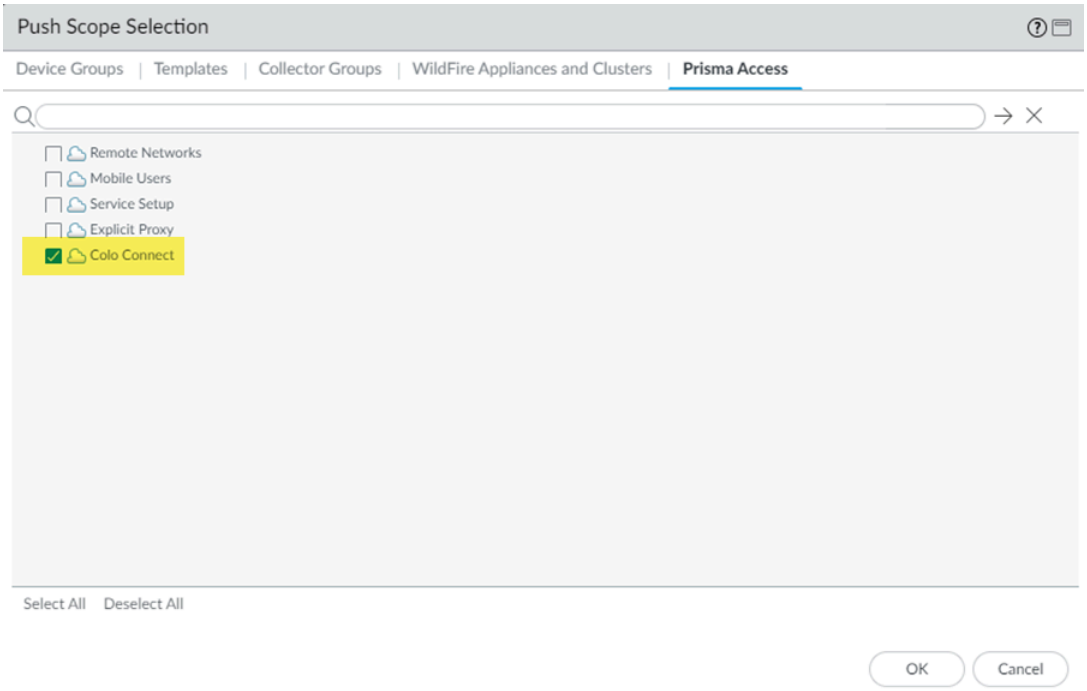
3. 完了するまで接続を作成し続けます。

   2 つの接続を作成する必要があります。両方の接続は同じリージョン内にある必要があり、各接続は別々のゾーン内にある必要があります。これらの接続は、後の手順で作成するサービス接続で使用します。

 ©2025 Palo Alto Networks, Inc.

STEP 4 | 変更をコミット、プッシュ配信します。

1. **[Commit（コミット）] > [Commit and Push（コミットしてプッシュ）]**に移動します。
2. 選択内容の編集をクリックし、プッシュスコープでColo-Connectが選択されていることを確認します。



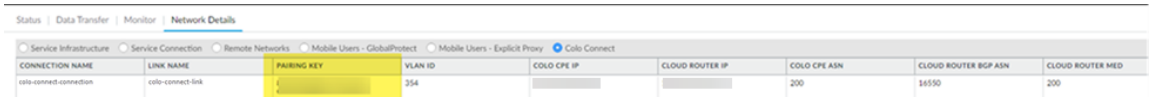
3. **OK** をクリックして、プッシュ スコープに対する変更を保存します。
4. 変更を **Commit and Push**（コミットしてプッシュ）します。

STEP 5 | ペアリング キー を取得し、GCP でパートナー相互接続の構成を完了します。

このペアリング キーは、Coloで パートナー相互接続 を設定するときに使用します。

新しい接続を最初にオンボーディングする際、Colo-Connect オンボーディングエリアのステータスは **PENDING_PARTNER**で、**BGP** ステータスは**DOWN**と表示されます。接続ステータスを **ACTIVE**にするには、ペアリング キーを取得して、Coloで接続を入力します。

1. **[Panorama] > [クラウドサービス] > [ステータス] > [ネットワークの詳細] > [Colo Connect]**へ移動し、 **[Pairing Key (ペアリングキー)]**をコピーします。



2. Coloで新しいVLAN接続を作成します (例: Equinix)。
3. ペアリング キーをColo VLANに貼り付けます。

   GCPはペアリング キーが消費されたことを検出し、VLANステータスを **ACTIVE**にし、Colo内のオンプレミス ルーターで構成するためのBGP IPアドレスを生成します。これらのアクションにより、ColoルータとGCPクラウド ルータ間のVLAN経由のeBCGルーティングが開始されます。

©2025 Palo Alto Networks, Inc.

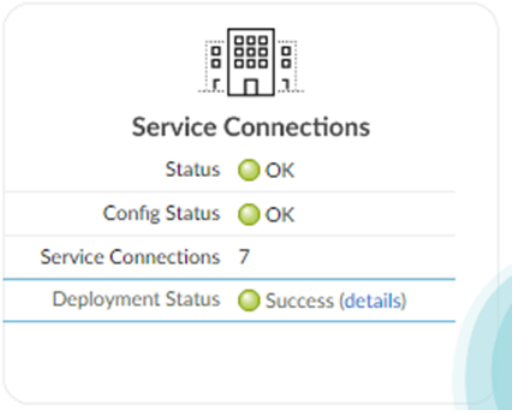
STEP 6 | Colo-Connect 接続用に、顧客 (Colo) ルーターにeBGP ルーティングを作成します 。
顧客ルータとクラウド ルータ間の接続を確保するには、BGPピアリングを設定する必要があります。

STEP 7 | Colo-Connectで使用するサービス接続を設定します 。

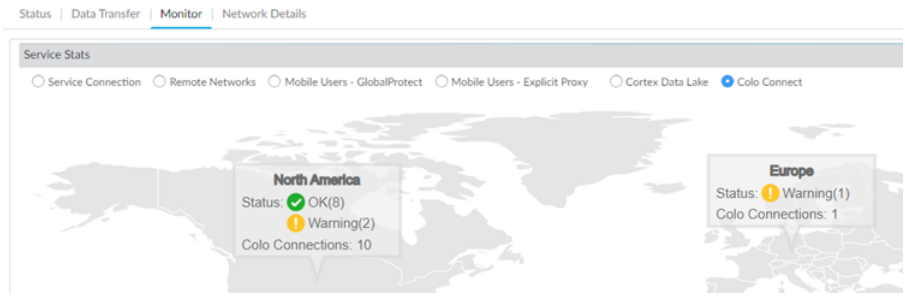
STEP 8 | 構成の変更をコミットしてプッシュし 、プッシュ スコープで**Colo-Connect**が選択されていることを確認します。

STEP 9 | Colo-Connect接続のステータスを確認します。

1. Colo-Connect 接続で使用されるサービス接続のステータスを確認するには、**[Panorama]** > **[クラウドサービス]** > **[ステータス]** > > **[Colo Connect]** > **[Monitor (モニター)]**へと順に移動します。



2. Colo-Connect 接続が展開されているリージョンにマウスを移動します。
   - Colo-Connect接続とBGPルーティングの両方が稼働している場合、ステータスには **OK** と表示されます。
   - Colo-Connect接続は稼働しているが、BGPルーティングが稼働していない場合、ステータスには 警告が表示されます。
   - Colo-Connect接続とBGPルーティングがダウンしている場合、ステータスには **Down**と表示されます。
   - Colo-Connect接続は稼働していないが、BGPルーティングが稼働している場合、ステータスには エラーが表示されます。



3. 詳細については、リージョンボックスをクリックして、**[ステータス]** タブで情報を確認してください。

©2025 Palo Alto Networks, Inc.

STEP 10 | **[Panorama]** > [クラウドサービス] > [ステータス] > [ネットワークの詳細] > **[Colo Connect]**を開き、以下のフィールドの情報を表示して、Colo-Connect 接続のペアリングキーを含むネットワークの詳細を確認します。

Prisma Access Colo-Connectの設定—専用インターコネクトを使用したデプロイメント

専用相互接続を使用してPrisma Access Colo-Connect を設定するには、以下の手順を実行します。

STEP 1 | Colo-Connect 接続用のサブネットを作成します。

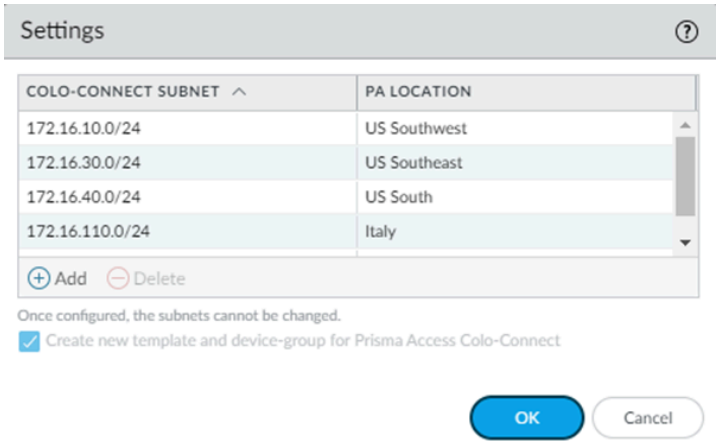
ここで作成したサブネットは、後の手順で作成する接続とサービス接続で使用します。

1. Prisma Accessを管理するPanoramaから、**[Panorama]** > [クラウドサービス] > [構成] > **[Colo-Connect]**へと移動し、歯車のアイコンをクリックして設定を編集します。
2. **Colo-Connect**サブネットを追加し、Prisma Accessロケーション (**PA**ロケーション) を指定します。

   最小サブネット /28 を入力します。
3. (任意) 複数の場所にColo-Connectインスタンスを作成する予定の場合は、場所ごとにサブネットを追加します。

   ロケーションごとに1つだけサブネットを構成できます。
4. **Prisma Access Colo-Connect** の新しいテンプレートとデバイス グループの作成を選択します。

   Colo-Connect デプロイメントを初めて構成する場合は、このチェック ボックスをオンにして、テンプレートとデバイス グループ (それぞれ Colo_Connect_Template と Colo_Connect_Device_Group) が Colo-Connect 用に作成されるようにします。これらのテンプレートとデバイス グループを作成すると、このチェックボックスはグレー表示されます。



 ©2025 Palo Alto Networks, Inc.

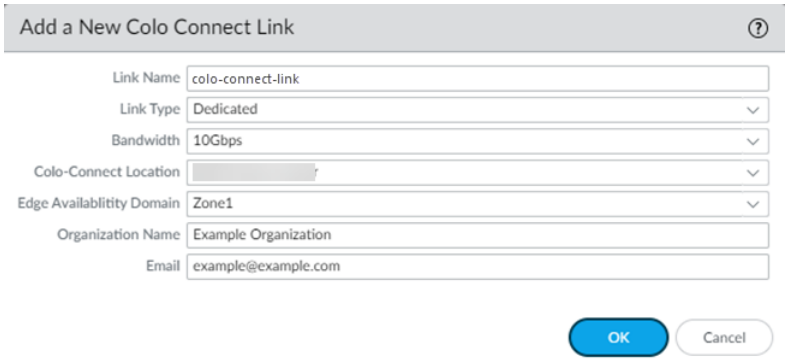
STEP 2 | 新しいColo-Connectリンク (相互接続とも呼ばれます) を追加します。

1. **Panorama** > クラウドサービス > **Configuration** (設定) > **Colo-Connect** > **Colo Connect**リンク へと移動し、 Colo-Connectリンクを追加します。.
2. リンクに一意の リンク名を付けます。
3. 専用 相互接続を選択します。
4. 残りのColo-Connectリンク パラメータを指定します。
   - 帯域幅として **10Gbps** または **20Gbps** を選択します。

     *20 Gbps*を選択した場合は、LACPを使用して専用相互接続リンクを*2*つの*10 Gbps*リンクに集約する必要があります。

     専用相互接続リンクの帯域幅を指定し、変更をコミットしてプッシュした後に変更することはできません。
   - ドロップダウン リストから **Colo-Connect**ロケーションを選択します。

     専用相互接続に使用したのと同じ場所を選択してください。
   - エッジ可用性ドメインとしてゾーン**1**またはゾーン**2** を選択します。この値は、エッジ可用性ドメインに使用される GCP ゾーン から取得します。
   - このリンクに使用する 組織名 を入力します。
   - クラウド プロバイダーから LOA-CFA の詳細を受信する 電子メール を入力します。
     - GCP はこのメールを使用して、 認可書および接続施設割り当て書 (LOA-CFA)を送信します。LOA-CFA が Colo プロバイダーに送信され、接続のインストールを開始できることを確認してください。



STEP 3 | 専用接続が作成されると、Colo 施設は 接続をテストし 、テストが完了して使用できる状態になったことを通知します。

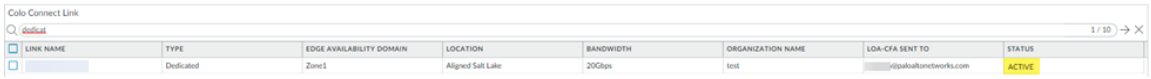
いいえ Prisma Access この手順では設定が必要です。Colo施設がテスト済みであることを知らせるまで、Prisma AccessでColo-Connect接続を作成しないでください。

©2025 Palo Alto Networks, Inc.

STEP 4 | Colo-Connectの接続 (*VLAN* アタッチメントとも呼ばれます) を作成します。

1. 専用リンクのステータスがアクティブになっていることを確認するには、 **Panorama** > クラウドサービス > 構成 > **Colo-Connect** > **Colo Connect**リンクへと移動します。

   専用リンクのステータスがアクティブになるまで、Colo-Connectリンクを作成することはできません。



2. **Panorama** > クラウドサービス > **Configuration** (設定) > **Colo-Connect** > オンボーディング へと移動し、新規接続を追加します。.
3. 接続設定を構成します。
   - 接続の一意の 名前 を入力します。
   - 前の手順で構成したリンクからリンク名を選択します。
   - (任意) 接続の**VLAN ID**を入力します。

     手動で値を入力しない場合は、相互接続ベンダー (GCP) によって VLAN ID が生成されます。
   - 接続の 帯域幅 を選択します。

     1 Gbps、**2 Gbps**、**5 Gbps**、**10 Gbps**、**20 Gbps**から選択できます。

     相互接続に複数の接続を構成する場合は、接続の合計帯域幅が相互接続の帯域幅を超えないようにしてください。たとえば、20 Gbpsの専用相互接続の場合、それぞ

©2025 Palo Alto Networks, Inc.

れ2 Gbpsの接続を10個構成できますが、すべての接続の合計が20 Gbpsを超えることはできません。

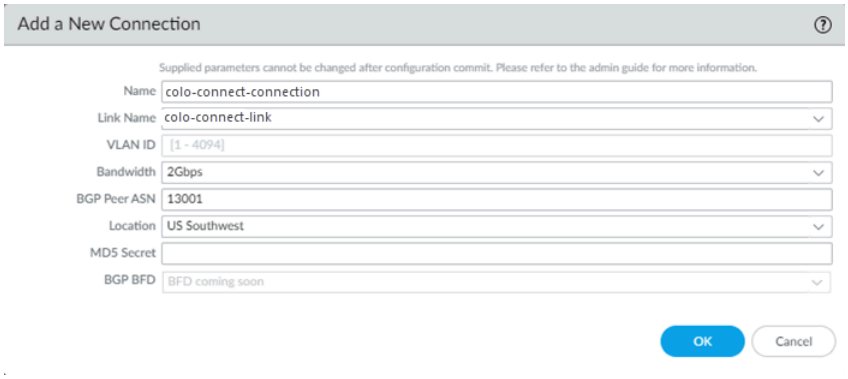
- **BGP**ピア**ASN** を入力します。

  Colo内の顧客のオンプレミス ルーターの自律システム (AS) 番号を入力します。範囲は1 ～ 4294967295です。

- 前の手順で作成した接続名からロケーションを選択します。

  指定する場所には、すでにサブネットを追加しておく必要があります。

- (任意) BGP**MD5**シークレットを入力します。



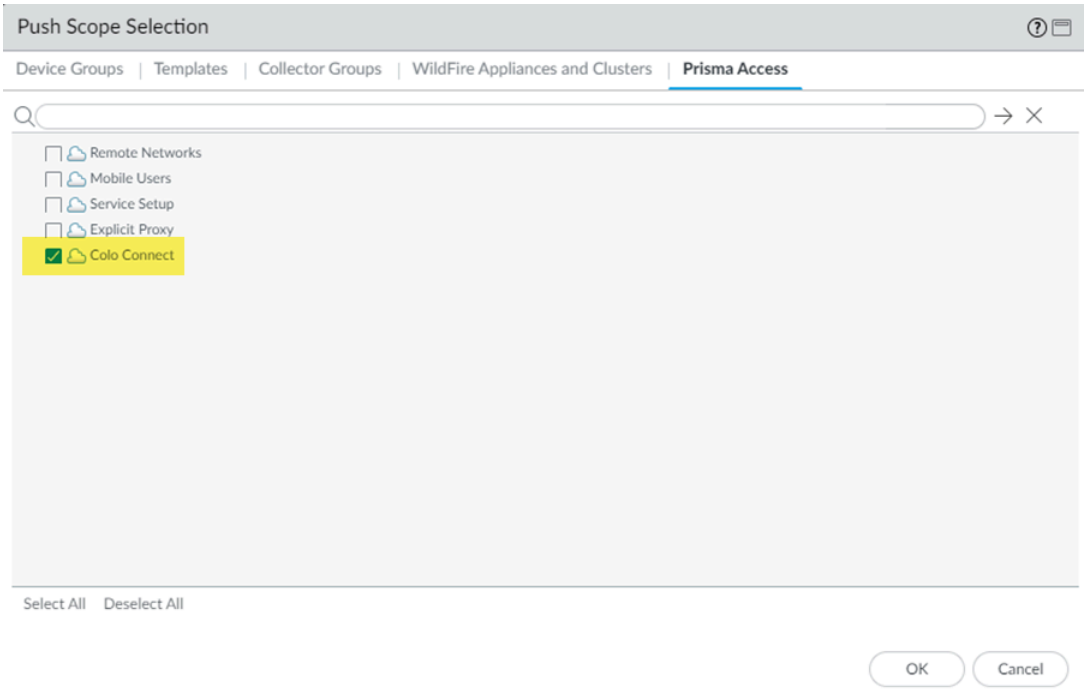
4. 完了するまで接続を作成し続けます。

   2 つの接続を作成する必要があります。両方の接続は同じリージョン内にある必要があり、各接続は別々のゾーン内にある必要があります。これらの接続は、後の手順で作成するサービス接続で使用します。

©2025 Palo Alto Networks, Inc.

STEP 5 | 変更をコミット、プッシュ配信します。

1. **[Commit**（コミット）**] > [Commit and Push**（コミットしてプッシュ）**]**に移動します。
2. 選択内容の編集をクリックし、プッシュスコープでColo-Connectが選択されていることを確認します。



3. **OK** をクリックして、プッシュ スコープに対する変更を保存します。
4. 変更を **Commit and Push**（コミットしてプッシュ）します。

STEP 6 | 顧客ルータでeBGP ルーティングを設定します 。

顧客ルータ間の接続を確保するには、BGPピアリングを設定する必要があります。

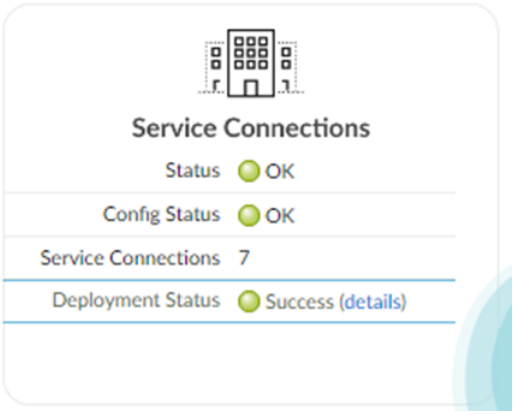
STEP 7 | Colo-Connectで使用するサービス接続を設定します 。

STEP 8 | 構成の変更をコミットしてプッシュし 、プッシュ スコープで**Colo-Connect**が選択されていることを確認します。

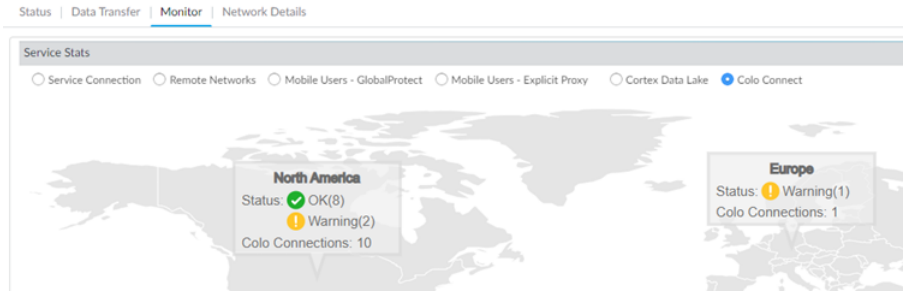
©2025 Palo Alto Networks, Inc.

STEP 9 | Colo-Connect接続のステータスを確認します。

1. Colo-Connect 接続で使用されるサービス接続のステータスを確認するには、**[Panorama]** > **[クラウドサービス]** > **[ステータス]** > > **[Colo Connect]** > **[Monitor (モニター)]**へと順に移動します。



2. Colo-Connect 接続が展開されているリージョンにマウスを移動します。
   - Colo-Connect接続とBGPルーティングの両方が稼働している場合、ステータスには **OK** と表示されます。
   - Colo-Connect接続は稼働しているが、BGPルーティングが稼働していない場合、ステータスには 警告が表示されます。
   - Colo-Connect接続とBGPルーティングがダウンしている場合、ステータスには **Down**と表示されます。
   - Colo-Connect接続は稼働していないが、BGPルーティングが稼働している場合、ステータスには エラーが表示されます。

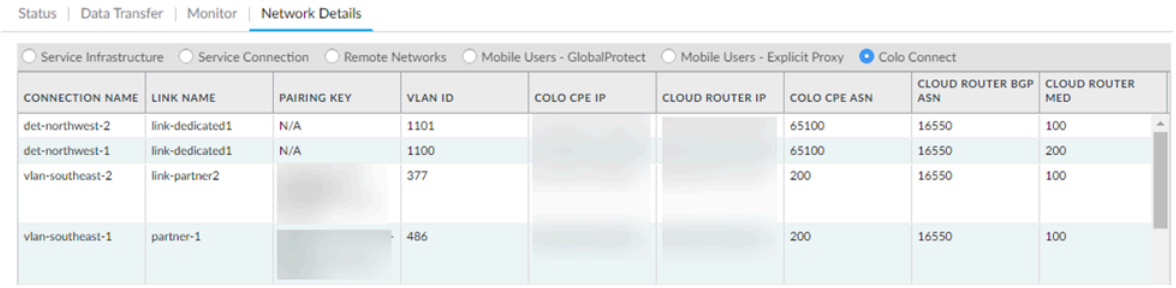


3. 詳細については、リージョンボックスをクリックして、**[ステータス]** タブで情報を確認してください。

©2025 Palo Alto Networks, Inc.

STEP 10 | Colo-Connect接続のネットワークの詳細を確認するには、 **[Panorama]** > **[クラウドサービス]** > **[ステータス]** > **[ネットワークの詳細]** > **[Colo Connect]**へと移動し、 詳細を表示します。

専用リンクの場合、 ペアリング キーは**N/A**と表示されます。



顧客ルータでVLAN eBGPルーティングを構成する

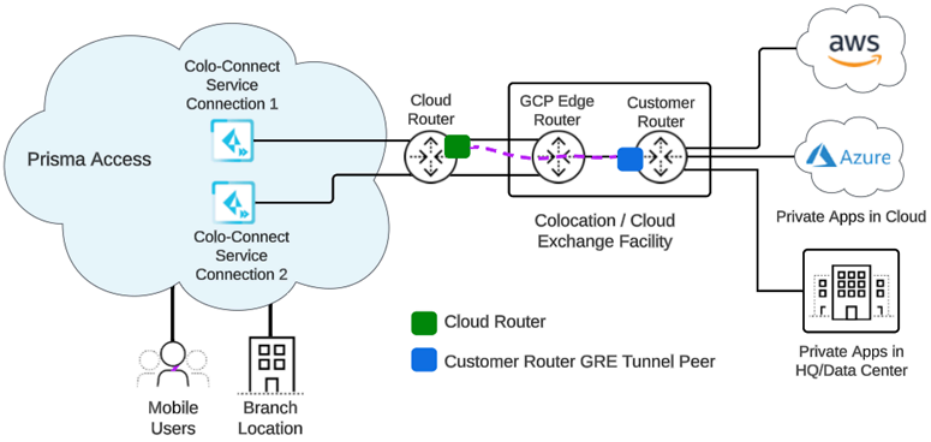
GCPは、デプロイメントの次の段階で顧客 (Colo) ルーターとクラウド ルーターのIPアドレスを作成します。

- パートナー相互接続の場合、ペアリング キーがColo (Equinixなど) によって使用された後に、GCPはIPアドレスを作成します。
- 専用相互接続の場合、Colo-Connect接続 (VLAN アタッチメント) をオンボードし、変更をコミットしてプッシュすると、GCPによってIPアドレスが作成されます。

正しいルーティングを確実に行うには、次の操作を行う必要があります。

- ColoルーターのIPアドレス（Prisma AccessUIの**Colo CPE IP**）をローカルVLAN IPアドレスとローカルeBGP IPアドレスとして設定します。
- クラウド ルーターのIPアドレス (**Cloud Router IP**) を ColoルーターのeBGPピア アドレスとして設定します。

完了すると、Coloルータとクラウド ルータ間の接続 (VLANアタッチメント) にeBGPが設定されます。



 ©2025 Palo Alto Networks, Inc.

このルーティングを作成することは、GREトンネル ルーティングを設定するための最初のステップです。サービス接続の構成中にGREトンネルを設定すると、GREトンネル ルーティングが完了します。

Coloとクラウド ルーター間のルーティングを構成するには、次の手順に従います。

STEP 1 | Prisma Accessを管理するPanoramaから、サブネット、リンク、接続を作成し、変更をコミットしてプッシュします。

相互接続タイプ (パートナーまたは専用)に固有のワークフローを使用します。パートナー相互接続の場合は、ペアリング キーをColo VLANに貼り付けたことを確認してください。

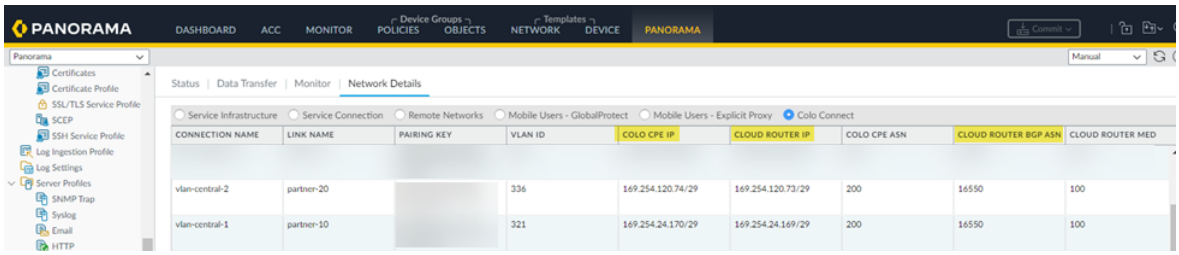
STEP 2 | **[Panorama]** > [クラウドサービス] > [ステータス] > [ネットワークの詳細] > **[Colo Connect]**へ移動します。

STEP 3 | 次の接続要素をメモします。

- **Colo CPE IP**
- クラウドルーター **IP**
- クラウドルーター **BGP ASN**

次の例では:

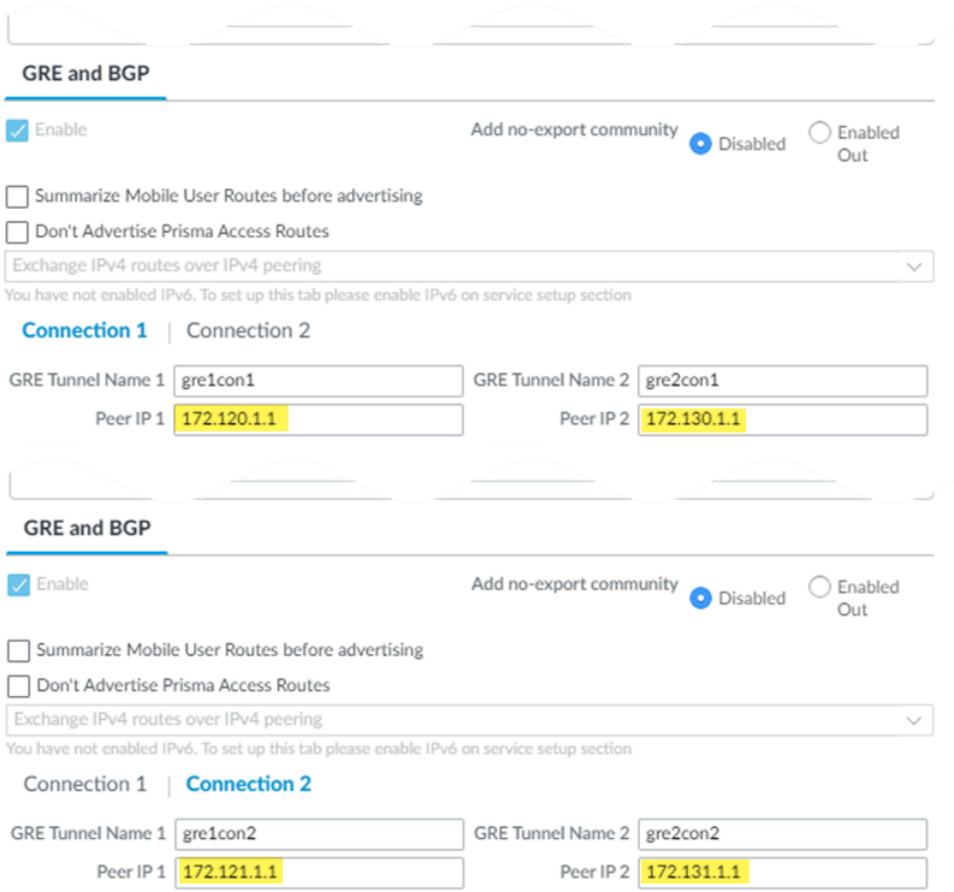
- vlan-central-1接続の場合、**Colo CPE IP**は 169.254.24.170/29、Cloud**Router IP**は 169.254.24.169/29、Cloud**Router BGP ASN**は16550 です。vlan-central-2 接続の場合、Colo CPE IPは169.254.120.74/29、Cloud Router IPは169.254.120.73/29、Cloud Router BGP
- **ASN**は**16550** です
- 。



 ©2025 Palo Alto Networks, Inc.

STEP 4 | Colo-Connectサービス接続を設定するときに、ローカルGRE IPアドレスに使用するIPアドレスを決定します。

これらは、ピア IP 1 およびピア IP 2 領域で Colo-Connect サービス接続(**Panorama** > クラウドサービス > 設定 > サービス接続)を設定するときに構成します。



最大10Gbpsのスループットをサポートするようにサービス接続を構成する場合は、 接続**1**と接続**2**にそれぞれ1つのトンネルを配置し、各サービス接続に合計2つのトンネルを配置します。

10 Gbpsを超えるスループット (最大20 Gbps) をサポートするようにサービス接続を構成する場合は、 接続**1**と接続**2**にそれぞれ2つのトンネルを配置し、各サービス接続に合計4つのトンネルを配置します。

次の例では、10 Gbpsを超えるスループット用にトンネルが設定されており、接続ごとに2つのトンネルが使用され、次のピアIPアドレスが使用されています。

- 接続 1 の場合は 172.120.1.1
- 接続 1 の場合は 172.130.1.1
- 接続 2 の場合は 172.121.1.1
- 接続 2 の場合は 172.131.1.1

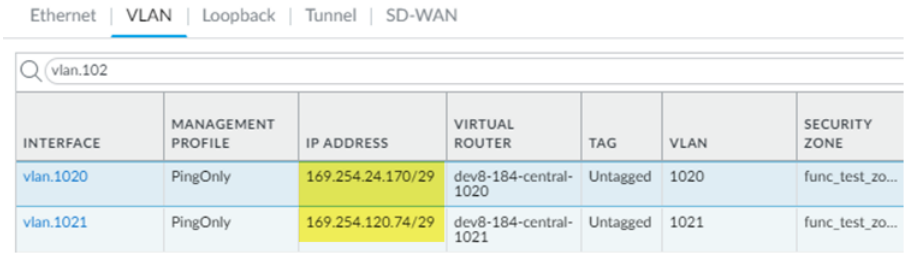
©2025 Palo Alto Networks, Inc.

STEP 5 | Colo ルーターにログインします。

次の構成スクリーンショットでは、ColoルーターとしてPalo Alto Networks次世代ファイアウォールを使用しています。

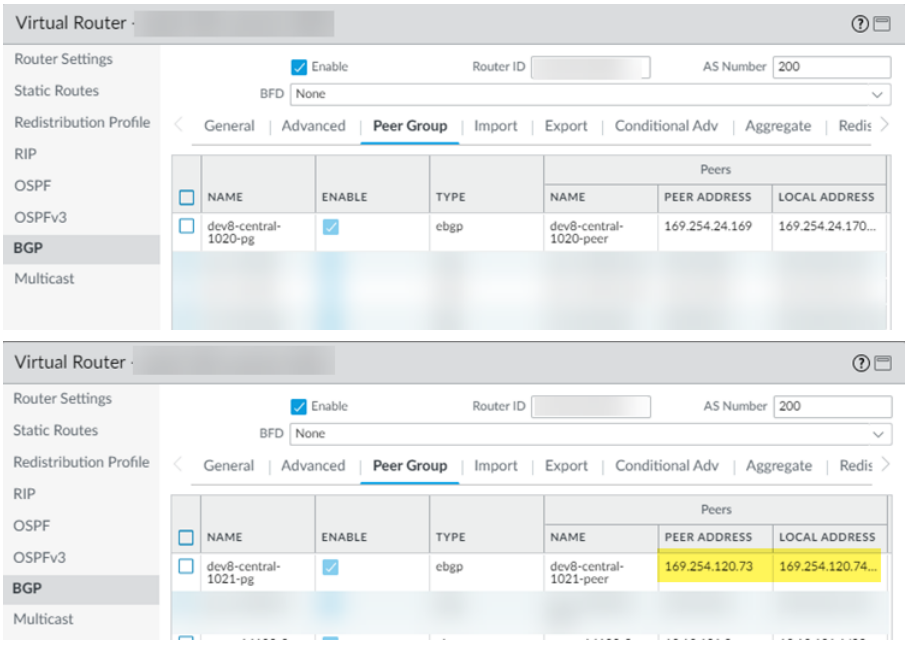
STEP 6 | **Colo CPE IP** アドレスをIPアドレスとして指定して、VLANインターフェイスを追加します。

次世代ファイアウォールをColoルーターとして使用している場合は、 ネットワーク > インターフェース > **VLAN** に移動し、VLANインターフェイス を追加して 、 仮想ルーターの名前を指定します。



STEP 7 | ColoルーターのIPアドレス (**Colo CPE IP**) をローカルeBGP IPアドレスとして設定し、クラウド ルーターのIPアドレス (**Cloud Router IP**) を Colo ルーターのeBGPピア アドレスとして設定します。

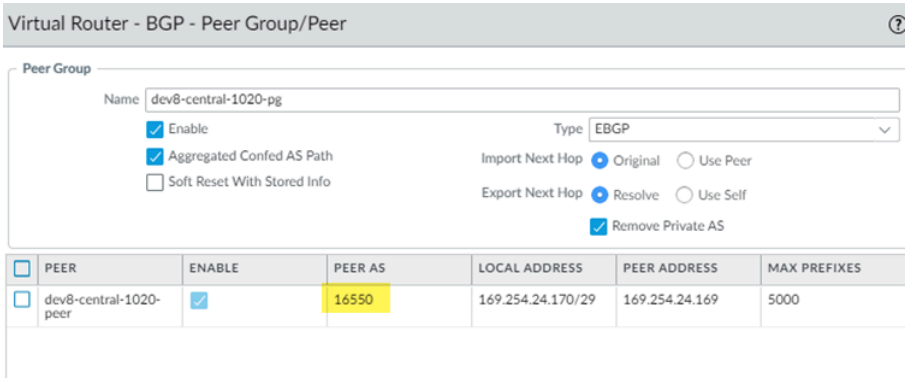
次世代ファイアウォールを Colo ルーターとして使用している場合は、[ネットワーク > 仮想ルーター]に移動して仮想ルーターを 追加し 、**[BGP]** > [ピア グループ]に移動して、 ピア アドレス として **Colo CPE IP** を 入力し、 ローカル アドレスとして クラウド ルーター**IP**を入力します。



 ©2025 Palo Alto Networks, Inc.

STEP 8 | **Cloud Router BGP ASN**をeBGP ピアの自律システム番号 (ASN) として設定します。

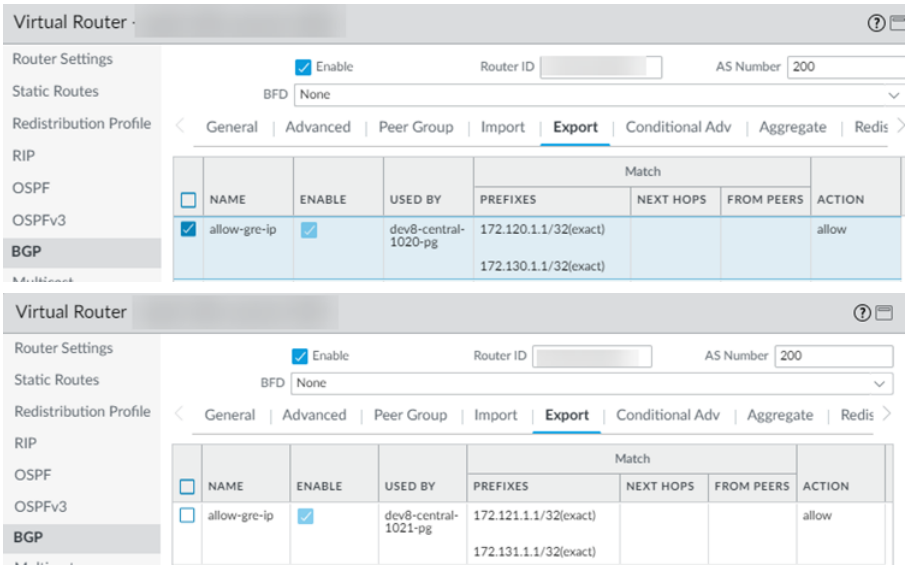
次世代ファイアウォールを Colo ルーターとして使用している場合は、[ネットワーク] > [仮想ルーター]に移動して仮想ルーターを追加し 、**[BGP]** > [ピア グループ]に移動してピア グループを追加し 、 ピア**AS** として **16500**を選択します。



STEP 9 | ローカルGRE IPアドレスのみをクラウド ルーターのピアIPアドレスにアドバタイズできるようにするBGPエクスポート ポリシーを作成します。

クラウド ルーターは限られた数のルートしか受信できないため、サービス接続GREトンネルのIPアドレス間のルーティングのみがクラウド ルーターに送信されるようにポリシーを作成する必要があります。

Colo ルーターとして次世代ファイアウォールを使用している場合は、[ネットワーク] > [仮想ルーター]に移動して仮想ルーター を追加し 、**[BGP]** > [エクスポート]に移動してエクスポート ルール を追加し 、ピアIPアドレスとして使用される IP アドレス を一致させて 、[許可]の[アクション] を作成します。



STEP 10 | Colo-Connectサービス接続を作成します。

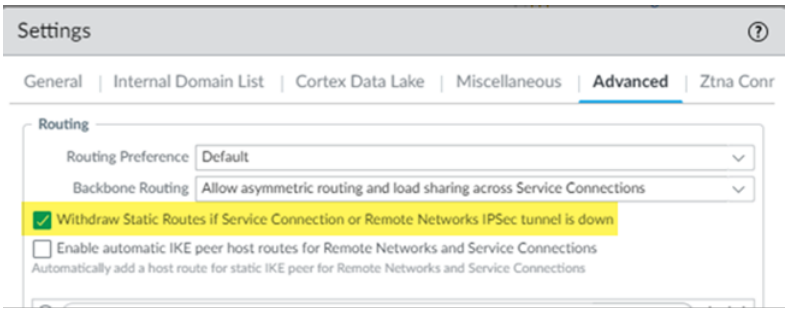
 ©2025 Palo Alto Networks, Inc.

Colo-Connectサービス接続を作成する

Colo-Connectはサービス接続を使用しますが、Prisma Accessサービス接続では、IPSecトンネルの代わりにGREトンネルを使用し、ルーティングには常にBGPを使用します。Colo-Connectサービス接続を構成するには、次の手順を実行します。

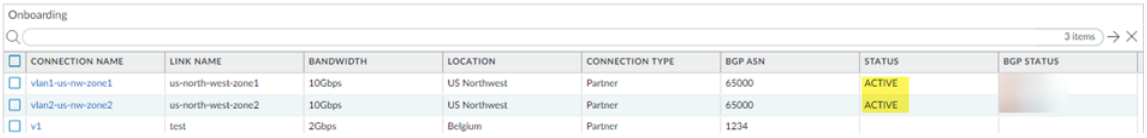
STEP 1 | Prisma Accessを管理する Panoramaから、Panorama Cloud Services構成のサービス セットアップに移動し、歯車アイコンをクリックして設定を編集し、サービス接続またはリモート ネットワーク IPSec トンネルがダウンしている場合はスタティック ルートを取り消すを選択して、Prisma Accessがスタティック ルートを取り消すことを確認します。

この選択肢を選択すると、GREトンネルがダウンした場合に、GREトンネルによって使用されるスタティック ルートが取り消されるようになります。



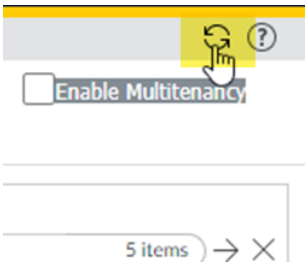
STEP 2 | **Colo-Connect**タブに移動し、Onboarding エリアのステータスフィールドをチェックして、接続が **Active (**アクティブ**)**状態であることを確認します。

接続のステータス がアクティブになるまで、サービス接続を構成することはできません。



STEP 3 | **Panorama** > **Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Service Connection**（サービス接続）へと移動します。

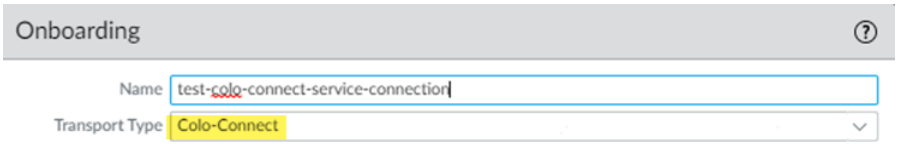
STEP 4 | Panorama UI の右上にある更新をクリックし、サービス接続エリアに Colo-Connect 設定がプロビジョニングされるようにします。



©2025 Palo Alto Networks, Inc.

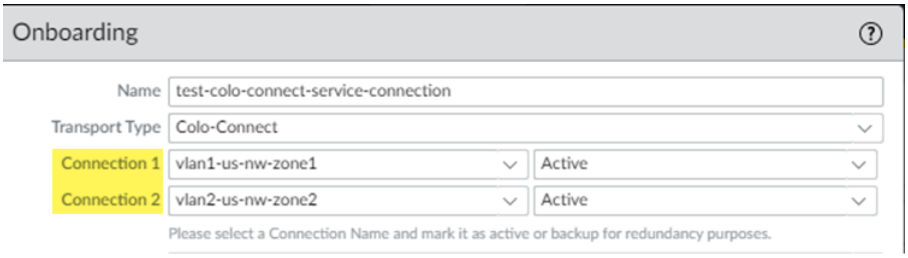
STEP 5 | サービス接続を追加し、一意の名前を付け、トランスポートタイプとして**Colo-Connect**を選択します。

入力する名前の長さが*31*文字以下であることを確認してください。 *32*文字以上の名前を入力すると、*Prisma Access*インフラストラクチャでトンネルが誤ってマッピングされます。



STEP 6 | サービス接続で使用する2つの接続 (接続**1** と 接続 **2**) を選択します。

これらの接続は2つの異なるゾーンに存在する必要があります。



STEP 7 | 接続**1**と接続**2**のアクティブまたはバックアップを選択します

サービス接続を設定するときは、次のガイドラインに従ってください。

- 次のモードで接続を構成できます。
  - アクティブ/アクティブ
  - アクティブ/バックアップ
  - バックアップ/アクティブ

  両方の接続を バックアップ/バックアップ モードで構成することは無効であり、サポートされていません。
- 接続の帯域幅は、すべてのモードで同じである必要があります。
- 接続は異なるゾーンに存在する必要があります。
- サービス接続に指定できる最大帯域幅は20 Gbps です。接続に **20 Gbps** の 帯域幅 を指定した場合、その接続を アクティブ/アクティブ 構成で使用することはできません (アクティブ/バックアップとして設定する必要があります)。
- 同じサービス接続で専用相互接続とパートナー相互接続を混在させないでください。また、サービス接続が異なるゾーンを使用するようにしてください。この表は、ゾーン、場

©2025 Palo Alto Networks, Inc.

所、帯域幅、およびロールがサービス接続のガイドラインと要件に従っていることを前提として、サービス接続で許可される構成と許可されない構成を示しています。

接続1は、	接続 2は、	有効なColo-Connectサービス接続構成に属していますか?
パートナー接続 1	パートナー接続 2	はい
専用接続 1	専用接続 2	はい
パートナー接続 1	パートナー接続 1	いいえ
専用接続 1	専用接続 1	いいえ
パートナー接続	専用接続	いいえ

STEP 8 | (任意、ホットポテトルーティングデプロイ環境のみ) 優先するバックアップ（Backup SC）として使用するサービス接続を選択します。

Colo-Connect サービス接続として構成されているサービス接続のみを選択できます。 接続障害が発生した場合、Prisma Accessは優先サービス接続として選択したバックアップSCを使用します。2つ以上のサービス接続を作成した場合、バックアップ サービス接続を選択すると、非対称ルーティングの問題を防ぐことができます。

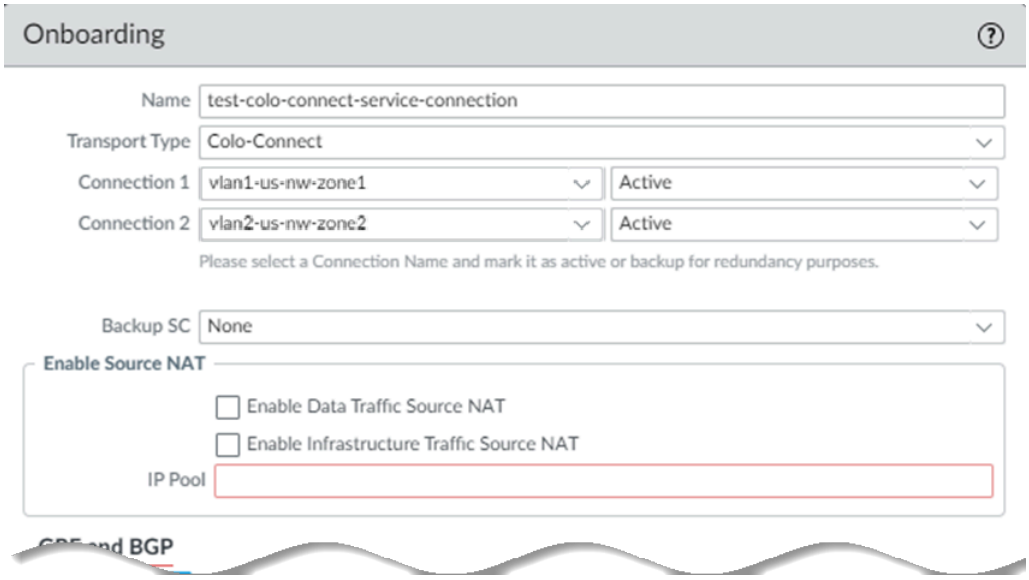
STEP 9 | (任意) モバイル ユーザーのソースNATを有効にします (GlobalProtect IPプール アドレス、インフラストラクチャ サブネット内のIPアドレス、またはその両方)。

Prisma AccessGlobalProtectモバイルユーザーとデータセンターのプライベートアプリケーションおよびリソース間のNATトラフィックに使用される1つまたは複数のサービス接続でサブネットを指定することができます。

- データ トラフィック ソース**NAT**を有効にする- モバイル ユーザIPアドレス プール アドレスに対してNATを実行し、それらのアドレスがデータ センターにアドバタイズされないようにし、サービス接続で指定したサブネットのみがデータ センターでアドバタイズされ、ルーティングされるようにします。
- インフラストラクチャ トラフィック ソース**NAT**を有効にする- インフラストラクチャ サブネットのアドレスに対して NAT を実行し、それらのアドレスがデータ センターにアドバタイズされないようにし、サービス接続で指定したサブネットのみがデータ センターでアドバタイズされ、ルーティングされるようにします。
- **IP**プール- モバイル ユーザーのIPアドレス プール、インフラストラクチャ サブネット、またはその両方でNATを実行するために使用されるIPアドレス プールを指定します。プライベート IP (RFC 1918) サブネットまたはルーティング ドメイン内でルーティング可能で、モバイル ユーザー - GlobalProtect IPアドレス プールまたはインフラストラクチャ サ

©2025 Palo Alto Networks, Inc.

ブネットと重複しない適切なサブネットを使用します。/25から/32までのサブネットを入力します。



STEP 10 | **GRE** および**BGP**領域で、サービス接続のGREトンネルとBGP設定を構成します。

BGPは常に有効に設定されます。

1. （任意）以下の選択肢から選択します：

   - 顧客宅内機器 (CPE) の eBGP ピアからのアウトバウンド プレフィックスに企業アクセス ノード (サービス接続) の**no-export**コミュニティを追加するには、**[Add no-export community (エクスポート禁止コミュニティの追加)]** を **[Enabled Out (有効アウト)]**に設定します。この機能はデフォルトでは 無効になっています。

     ホットポテト ルーティング モードではこの機能を使用しないでください。

   - Prisma AccessBGPピアが、組織のネットワークにルートを転送することを防止します。**Don't Advertise Prisma Access Routes**（**Prisma Access**ルートをアドバタイズしない）.

     デフォルトで、Prisma Accessは、ローカルルート、および他のサービス接続、リモートネットワーク、およびモバイルユーザーサブネットから受信するすべてのプレフィックスを含め、すべてのBGPルーティング情報をアドバタイズします。Prisma AccessによるBGPアドバタイズメントの送信を防止しながら、受信したBGP情報を使って、他のBGPネイバーからルートを学習するには、このチェックボックスを選択します。

     このオプションを選択した場合、*Prisma Access*は*BGP*アドバタイズメントを送信しないため、オンプレミスの機器でスタティック ルートを設定して、*Prisma Access*に戻るルートを確立する必要があります。

   - BGP 経由で顧客構内設備 (CPE) に送信されるモバイル ユーザー IP サブネット アドバタイズメントの数を減らすには、**[Summarize Mobile User Routes before**

©2025 Palo Alto Networks, Inc.

advertising (アドバタイズする前にモバイル ユーザー ルートを集約する**)]**を選択します。

デフォルトでは、Prisma Accessは、モバイルユーザーのIPアドレスプールを、/24サブネットのブロックでアドバタイズします。それを要約すると、Prisma Accessは指定したサブネットに基づいてプールがアドバタイズされます。たとえば、Prisma Accessは、パブリックユーザーのモバイルIPプールを、アドバタイズ前に10.8.1.0/24、10.8.2.0/24、10.8.3.0/24などのサブネットに分割するのではなく、/20のサブネットを使用して10.8.0.0/20のプールをアドバタイズします。これらのアドバタイズを要約することで、CPEルーティングテーブルに保存されるルート数を削減できる可能性があります。たとえば、限定された数のルートを受け付けるクラウドVPNゲートウェイ（仮想プライベートゲートウェイ（VGW）またはトランジットゲートウェイ（TGW））で、IPプールの要約を使用することができます。

ホットポテトルーティングを有効にしてルート集約を有効にすると、*Prisma Access*は非対称ルーティングを引き起こす可能性のある *AS-PATH* を先頭に追加しなくなりました。ホットポテトルーティングでルート要約を有効にする前に、データセンターまたは本社からのリターントラフィックの、対称的なリターンが保証されていることを確認してください。

2. GREトンネルを使用してサービス接続のルーティングを設定します。
3. Prisma Accessを管理するPanoramaから 前のページに戻る **Panorama** > クラウドサービス > 構成 > サービス接続 GRE トンネル 接続 **1** を入力して **GRE** トンネル名 **1**とピア**IP 1** 対して 接続 **1** また、10 Gbps を超える帯域幅が必要な場合は、 **GRE** トンネル名**2** そして ピア**IP 2** を入力します。接続 1 の 2 番目のトンネル用の場合、次に、同じ手順を繰り返して、接続**2**用のGREトンネルを作成します。

   接続内のGREトンネルの各ペアは、最大10 Gbpsの帯域幅をサポートします。10 Gbpsを超える帯域幅が必要な場合は、接続ごとに2つのトンネルを構成します。以下に例を示します。

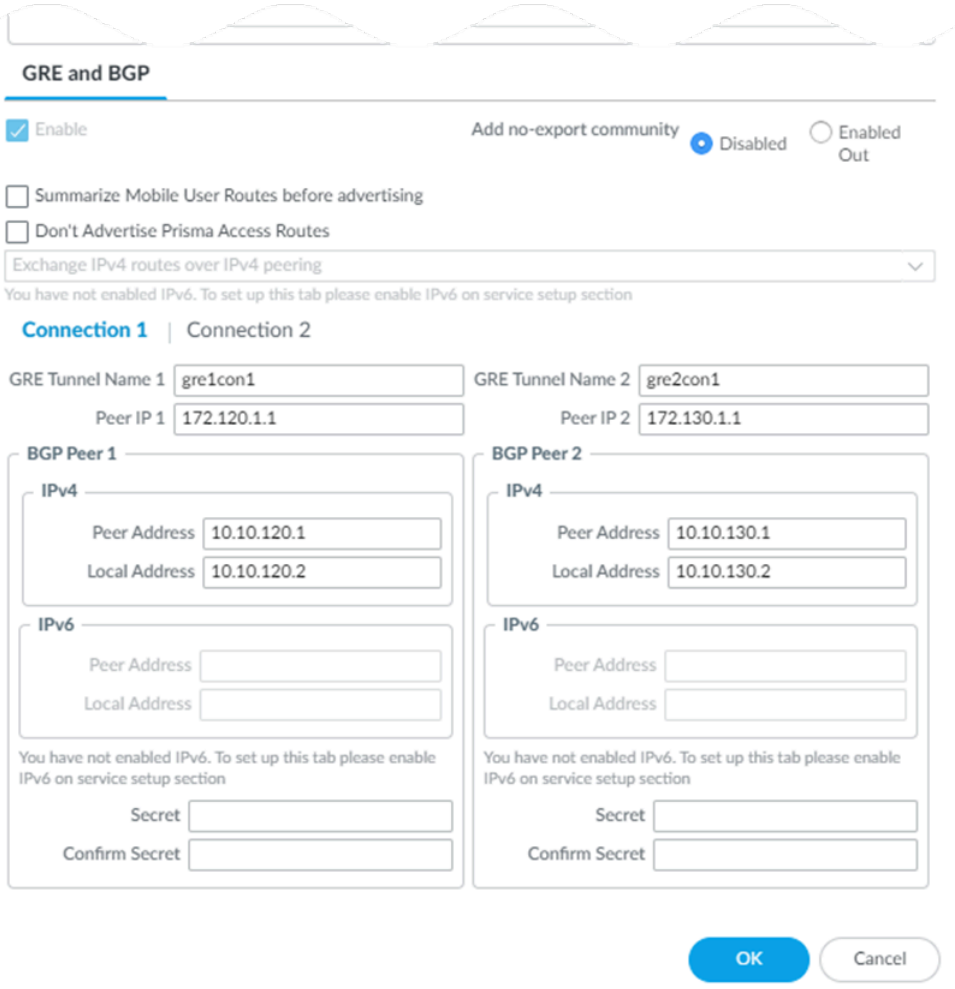
   ピア IPには、コロケーション内のオンプレミス ルーターのGRE IPアドレスを入力します。

   BGP値にはIPv4アドレスを使用します。IPv6はサポートされていません。
4. BGP ピア1の ピア アドレス と ローカル アドレス を入力し、接続1に2 番目のトンネルが必要な場合は BGP ピア2のアドレスとローカル アドレスを入力します。

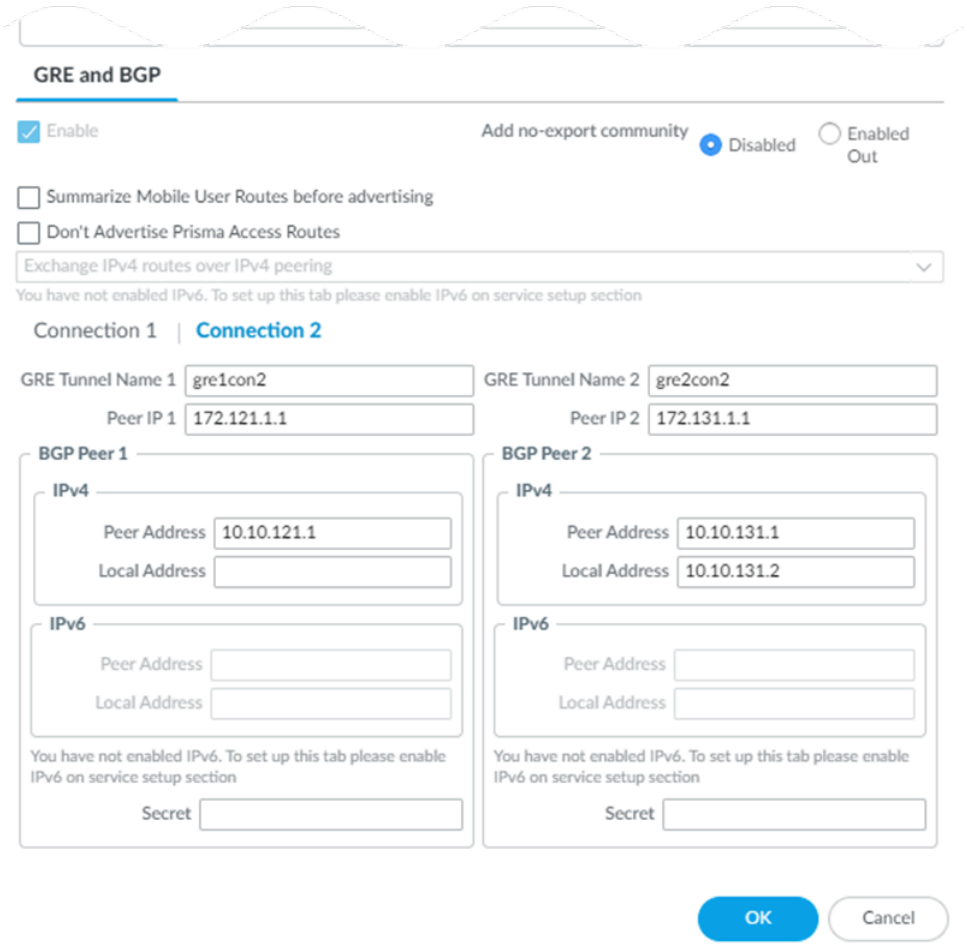
   ピア アドレスには、ColoルーターのBGP ピアIPアドレスを入力します。 ローカル アドレスには、GREトンネル経由のBGPネットワーク確立に使用されるアドレスを入力します。

©2025 Palo Alto Networks, Inc.

5. (任意) BGPシークレットを設定するには、 シークレットとシークレットの確認の値を入力します。



©2025 Palo Alto Networks, Inc.

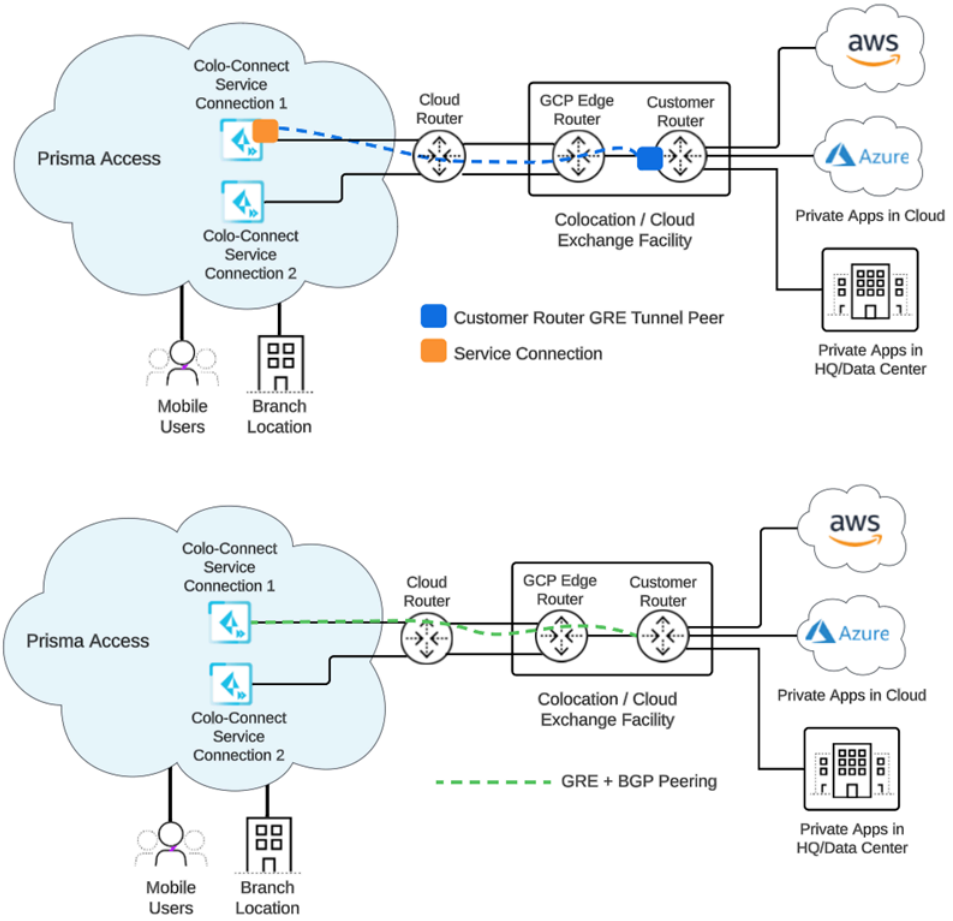


STEP 11 | 構成の変更をコミットしてプッシュし、プッシュ スコープで**Colo-Connect**が選択されていることを確認します。

GREトンネルを使用してサービス接続のルーティングを設定します。

Coloルータは、GRE トンネル ピアIPアドレスをクラウド ルータにアドバタイズし、クラウド ルータからGREトンネルのサブネットを学習します。顧客ルータの VLAN 経由で eBGP ルーティングを最初に設定したときに、GRE トンネルのローカル到達可能性をアドバタイズしました。クラウド ルータとColoルータがColoサブネットとローカルGRE IPアドレスのルートを相互にアドバタイズして学習すると、サービス接続で使用される GRE トンネルがアクティブ (アップ) になります。

©2025 Palo Alto Networks, Inc.



ルーティングを設定し、サービス接続にGREトンネルを追加するには、次の手順を実行します。

STEP 1 | BGPピア1と、接続1に2つ目のトンネルが必要な場合は、BGPピア2のピアアドレスとローカルアドレスに使用するIPアドレスをメモしておきます。

次の例では、次のピア アドレスとローカル アドレスを使用します。

- ピア アドレス- 接続 1の場合は10.10.120.0 および10.10.130.1、接続2の場合は10.10.120.2および 10.10.130.2
- ローカル アドレス- 接続1の場合は 10.10.120.2 と 10.10.130.2、接続2の場合は10.10.121.2と 10.10.131.2

©2025 Palo Alto Networks, Inc.

STEP 2 | サービス接続でピア**IP1** に使用する IP アドレスと、必要に応じてピア**IP2**アドレスをメモします。

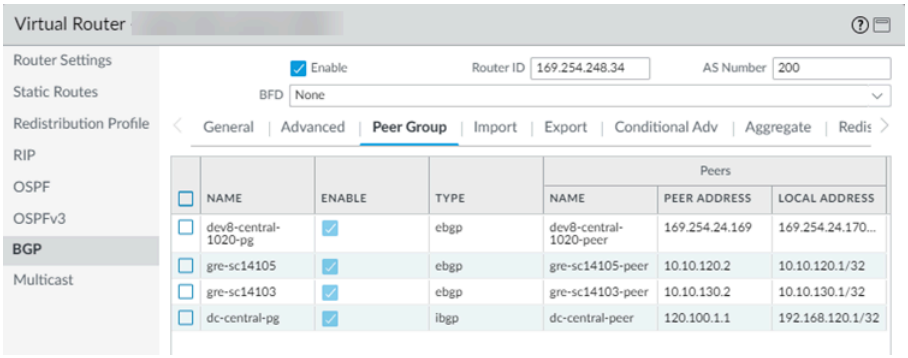
これらのIPアドレスを使用して、ローカルGRE IPアドレスがColo-Connectサービス接続にアドバタイズされるのを防ぐ拒否ポリシーを作成します。

このドキュメントのすべての例では、次のIPアドレスを使用します。

- 接続 1 の場合は 172.120.1.1
- 接続 1 の場合は 172.130.1.1
- 接続 2 の場合は 172.121.1.1
- 接続 2 の場合は 172.131.1.1

STEP 3 | ピアおよびローカルIPアドレスのピア グループを構成します。

次世代ファイアウォールを Colo ルーターとして使用している場合は、[ネットワーク] > [仮想ルーター]に移動し、[仮想ルーター][追加] に移動して、**[BGP]** > [ピア グループ]に移動し、[ピア アドレス] として[ピア アドレス] を入力し、[ローカルアドレス]として [ローカルアドレス] を入力します。



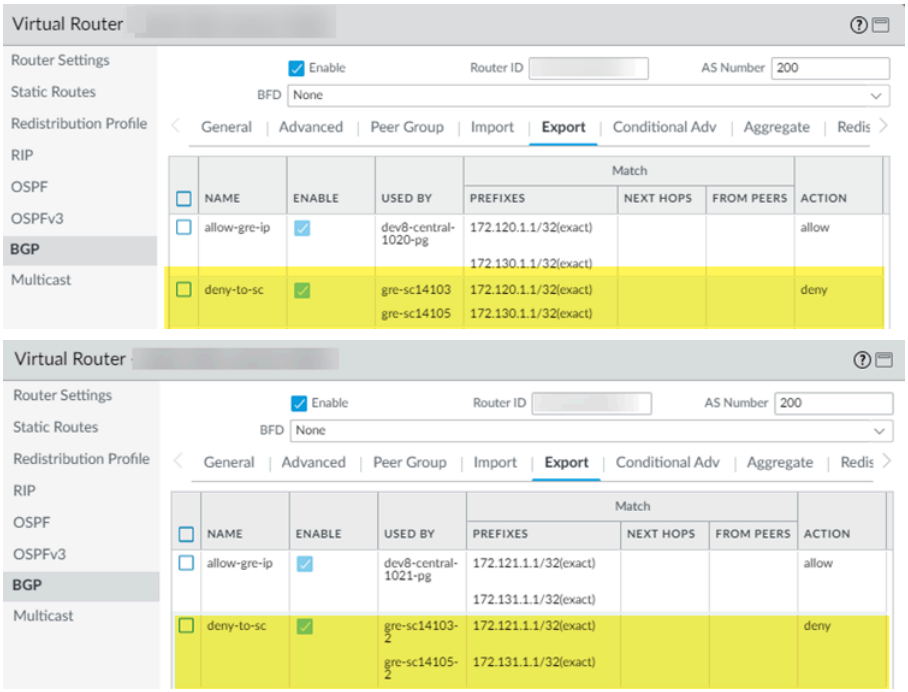
STEP 4 | 設定したピアIPアドレス (172.120.1.1、172.130.1.1、172.121.1.1、および 172.131.1.1) を拒否するBGPエクスポート ポリシーを作成し、作成したピア グループに適用します。

このエクスポート ポリシーは、ローカル GREトンネル ピアIPアドレスにDENYルールを適用し、他のすべてのルートをサービス接続にアドバタイズできるようにします。

Colo ルーターとして次世代ファイアウォールを使用している場合は、[ネットワーク] > [仮想ルーター]に移動して仮想ルーター を追加し 、**[BGP]** > [エクスポート]に移動してエクスポー

©2025 Palo Alto Networks, Inc.

トルールを追加し、ピアIPアドレスとして使用されるIPアドレスを一致させて、[拒否]の[アクション]を作成します。



Colo-Connectサービス接続の帯域幅を増減する

サービス接続を構成するときは、それに関連付ける接続 (VLAN アタッチメント) に基づいて帯域幅を構成します。サービス接続ごとに2つの接続を割り当て、接続ごとに1つまたは2つのGREトンネルを割り当てます。

各Colo-Connectサービス接続は最大 20 Gbps をサポートしますが、サービス接続内の各GREトンネルは10 Gbpsをサポートします。このため、Colo-Connectサービス接続でGREトンネルを追加または削除してリンクの合計帯域幅を変更する必要があり、その結果、サービス接続帯域幅が10 Gbpsを超えたり下回ったりすることがあります。

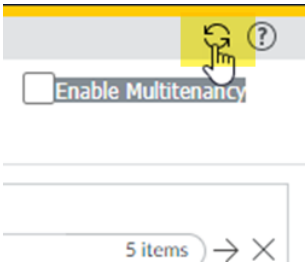
Colo-Connectサービス接続の帯域幅を増やす

既存のサービス接続の帯域幅を10 Gbps以上に増やすには、次の手順を実行します。

STEP 1 | **[Panorama] > [Cloud Services（クラウドサービス）] > [Configuration（設定）] > [Colo-Connect]**へと移動します。

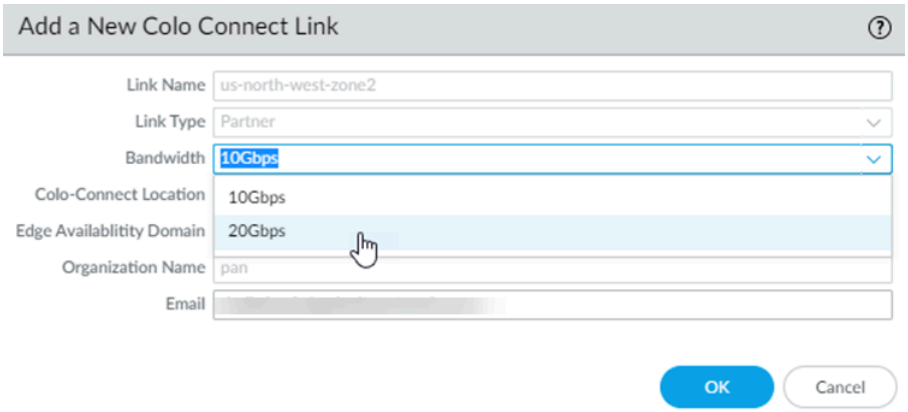
©2025 Palo Alto Networks, Inc.

STEP 2 | Panorama UI の右上にある **[Panorama]** > **[クラウドサービス]** > **[Configuration (設定)]** > **[Service Connection (サービス接続)]**へと移動し、 更新 をクリックして、サービス接続エリアに Colo-Connect 設定がプロビジョニングされるようにします。



STEP 3 | サービス接続に関連付けられている リンク名 を選択します。

STEP 4 | リンク（相互接続）の 帯域幅 を増やします。

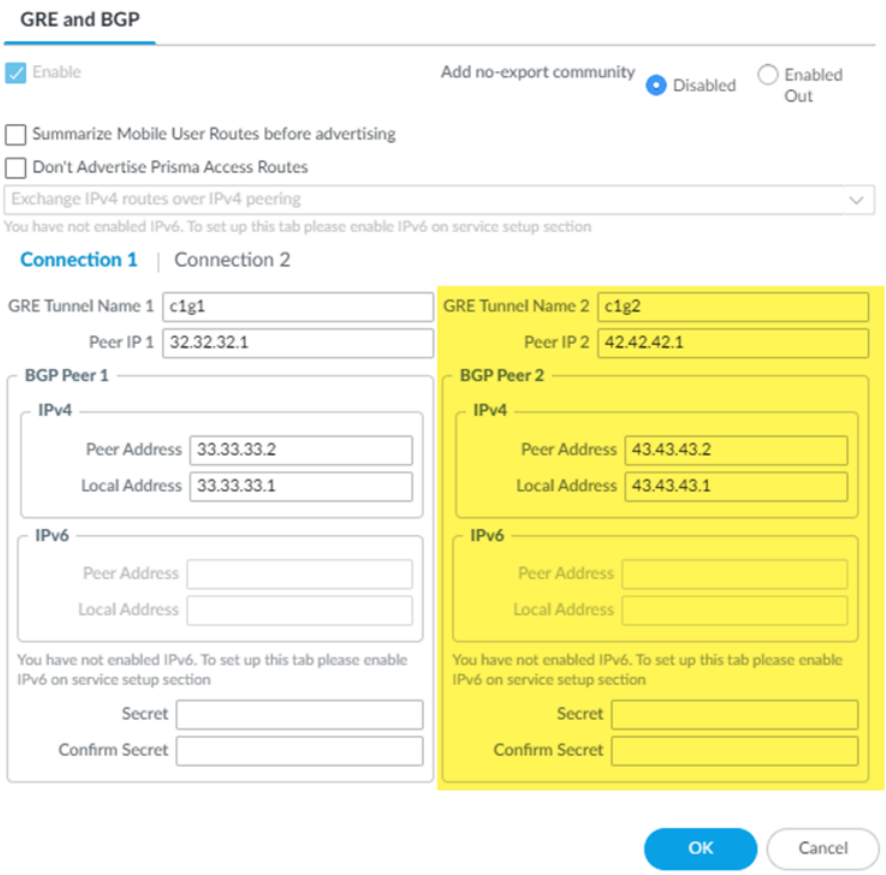


STEP 5 | **[Push Scope (プッシュスコープ)]**で**Colo-Connect**のみを選択し、変更を**Commit and Push (コミットしてプッシュ)**します。

STEP 6 | **[Panorama]** > **[Cloud Services（クラウドサービス）]** > **[Configuration（設定）]** > **[Service Connection（サービス接続）]** > ***<service-connection-name>*** > **[Onboarding (オンボーディング)]**へと移動します。

©2025 Palo Alto Networks, Inc.

STEP 7 | Colo-Connect サービス接続に追加の GRE トンネルを追加します。



STEP 8 | **[Push Scope (プッシュスコープ)]**で**[Service Connections (サービス接続)]**を選択し、変更を**[Commit and Push (コミットしてプッシュ)]**します。

STEP 9 | GREトンネルのVLAN eBGPルーティングおよびサービス接続ルーティングのエクスポートポリシーにGREローカル (ピア) IPアドレスを追加します。

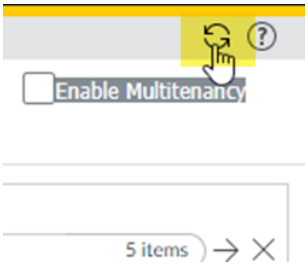
Colo-Connectサービス接続の帯域幅を減らす

既存のサービス接続の帯域幅を10 Gbps以上に減らすには、次の手順を実行します。

STEP 1 | **[Panorama] > [Cloud Services**（クラウドサービス）**] > [Configuration**（設定）**] > [Colo-Connect]**へと移動します。

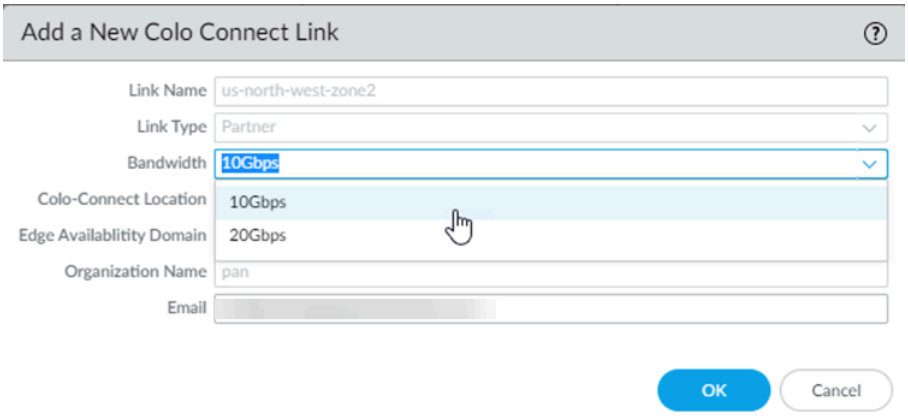
©2025 Palo Alto Networks, Inc.

STEP 2 | Panorama UI の右上にある **[Panorama]** > **[クラウドサービス]** > **[Configuration (設定)]** > **[Service Connection (サービス接続)]**へと移動し、 更新 をクリックして、サービス接続エリアに Colo-Connect 設定がプロビジョニングされるようにします。



STEP 3 | サービス接続に関連付けられている リンク名 を選択します。

STEP 4 | リンク（相互接続）の 帯域幅 を減らします。



STEP 5 | **[Push Scope (プッシュスコープ)]**で**Colo-Connect**のみを選択し、変更を**Commit and Push (コミットしてプッシュ)**します。

STEP 6 | **[Push Scope (プッシュスコープ)]**で**[Service Connections (サービス接続)]**を選択し、変更を**[Commit and Push (コミットしてプッシュ)]**します。

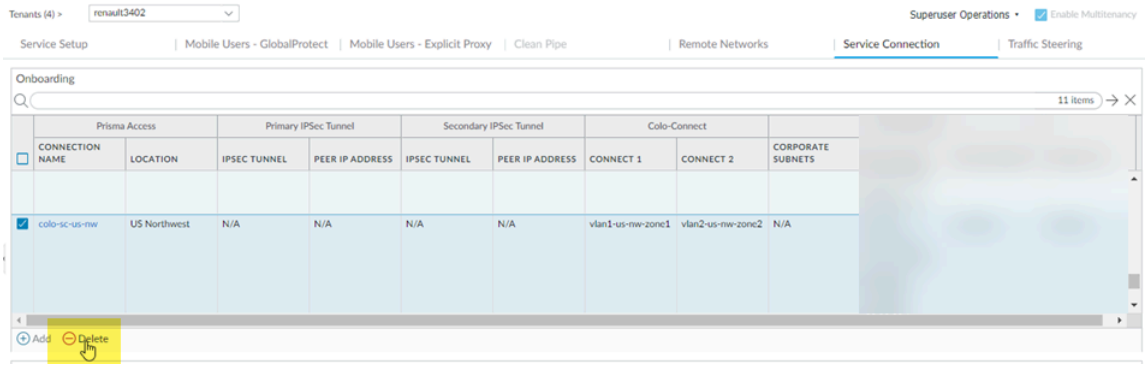
余分なGREトンネルを削除するためにサービス接続を再構成する必要はありません。 Prisma Accessは、サービス接続プッシュ スコープで変更をコミットしてプッシュすると、リンクの帯域幅を検出して下げ、余分なトンネルを削除します。

Colo-Connect接続を削除する

Colo-Connect接続を削除するには、設定の逆の順序で、次の手順を実行します。

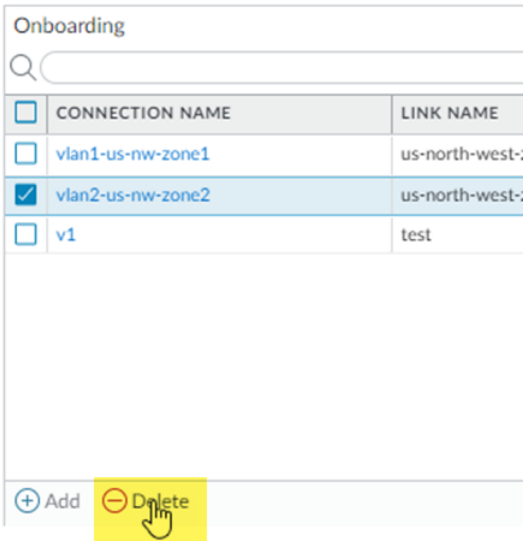
©2025 Palo Alto Networks, Inc.

STEP 1 | 接続に関連付けられているサービス接続を削除するには、 **[Panorama] > [Cloud Services (クラウドサービス)] > [Configuration (設定)] > [Service Connection (サービス接続)]**へと移動し、サービス接続を選択し、それを[消去]します。



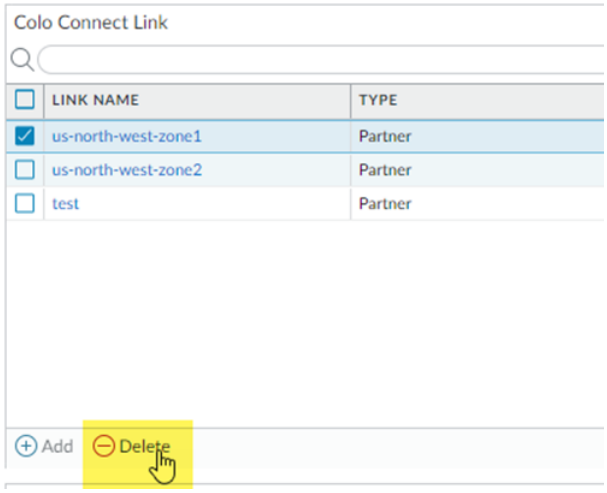
STEP 2 | **[Push Scope (プッシュスコープ)]**で**[Service Connections (サービス接続)]**を選択し、変更を**[Commit and Push (コミットしてプッシュ)]**します。

STEP 3 | 接続に関連付けられているColo-Connect接続を削除するには、**[Panorama] > [クラウドサービス] > [Configuration (設定)] > [Colo-Connect]**へと移動し、 **[オンボーディング]**セクションで接続名を選択し、削除します。



 ©2025 Palo Alto Networks, Inc.

STEP 4 | リンク名 を選択して 削除し、Colo-Connect リンクを削除します 。



STEP 5 | GREトンネルのVLAN eBGPルーティングおよびサービス接続ルーティングのエクスポートポリシーからGREローカル (ピア) IPアドレスを削除します。

©2025 Palo Alto Networks, Inc.

Prisma Accessでのアプリの高速化

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ 最低 Prisma Accessバージョン5.0イノベーション ❑ Prisma Accessのライセンス ❑ アプリの高速化には Prisma Access データプレーンバージョン 10.2.10が必要です。 ❑ App Acceleration アドオン ライセンス App Accelerationライセンスには、自律型DEM (ADEM) の30日間評価ライセンスが含まれており、ADEMからApp Accelerationパフォーマンス メトリックを取得できます。

App Accelerationは、アプリのパフォーマンス低下の原因に直接対処し、リアルタイムでその影響を軽減することで、Prisma AccessGlobalProtect およびリモート ネットワーク ユーザーのユーザー エクスペリエンスを大幅に向上させます。

アプリにアクセスする際のユーザー エクスペリエンスが低下する主な原因は、動的コンテンツ (ユーザーごとに個別にオンデマンドで処理する必要があるコンテンツ) とネットワーク接続の問題です。

App Accelerationでは、次の機能が提供されます。

トップ **SaaS** アプリの高速化- Prisma SASE のアプリ高速化は、動的コンテンツを高速化し、トップ SaaS アプリの応答時間を改善します。ユーザーがリクエストする前に、各ユーザーが必要とする動的コンテンツを安全かつインテリジェントに準備します。

その結果、App Accelerationはアプリケーションとそれを実行するAPIの応答時間を大幅に短縮し、ユーザー エクスペリエンスを向上させて生産性を高めます。

高速化されたアプリケーションは、「サポートされているアプリ」セクションにリストされます。

ネットワーク アクセラレーション- ユーザーがアプリにアクセスすると、パケット損失、ワイヤレス接続の低下、ネットワークの輻輳などの要因によってスループットが低下し、アプリのパフォーマンスが低下することがあります。これらのネットワークの問題は、従業員のエクスペリエンスに悪影響を及ぼし、生産性を低下させる可能性があります。

インターネットが考案された当時、ネットワークは均質化されており、ワイヤレス接続はまだ初期段階でした。TCPのような基本的なプロトコルは、もともとこれらのネットワーク用に作成されました。今日、ネットワークはもはや均一ではなく、ワイヤレス接続によってユーザー エクスペリエンスは大きく変化します。ユーザーがネットワーク状態の低下を経験すると、TCPは問

題がデバイスの制限、ネットワークの制限、または物理的な制約のいずれによって発生したかを区別できません。

App Accelerationは、クライアント構成やアプリケーションを変更することなく、次の点を安全に理解します。

- デバイス機能- クライアントエンドポイントの種類
- ネットワーク機能- ネットワークの種類
- アプリのコンテキスト- 使用されているアプリの種類

App Accelerationは、デバイス、ネットワーク、アプリケーションのコンテキストを理解してスループットを最大化し、変化するネットワーク状況に合わせてリアルタイムで調整します。

直接インターネット アクセスと比較すると、App Accelerationでは、Prisma Access経由で接続する場合、TCPトラフィックのスループットが大幅に向上します。

Prisma SASEインシデントおよびアラートで、App Accelerationによるスループットの向上を確認できます。AI搭載の 自律型DEM (ADEM) は App Accelerationと統合され、高速化されたアプリケーションの数や全体的なパフォーマンスの向上などの指標を提供します。

©2025 Palo Alto Networks, Inc.

アプリの高速化の要件とガイドライン

App Accelerationを構成するときは、次のガイドラインと要件に注意してください。

- サポートされているアプリ- App Accelerationは次のアプリをサポートしています。
  - Amazon S3
  - Azure ストレージ
  - ボックス
  - Google ドライブ
  - マイクロソフト365:
    - My Content
  - Microsoft OneDrive
  - Salesforce
  - SAP Ariba
  - ServiceNow
  - Slack (ファイルのダウンロード)
  - Zoom：
    - チャットからのファイルのダウンロード
    - クラウド録画のダウンロード
    - Zoom チームチャット
- サポートされているロケーション- App AccelerationはすべてのPrisma Access地域で利用可能です 。しかし以下のロケーションを除きます:
  - すべての ローカルゾーン
  - バーレーン
  - 中国
  - アイルランド
  - 南アフリカ 西
  - スウェーデン アラブ
  - 首長国連邦
- 信頼されたルート**CA**のアップロード- 次の手順に示すように、信頼されたルートCAを設定し、コミットおよびプッシュ操作を実行してから、App Accelerationのセットアップ中にそれを選択する必要があります。Strata Cloud Managerを使用してApp Accelerationを構成する場合は、Prisma Accessスコープでルート CAを設定します。使用する証明書を変更する場合は、選択する前に変更した証明書をコミットしてプッシュする必要もあります。
- 転送信頼証明書および信頼されたルート**CA** -次の手順に従って、アップロードしたCA/証明書を 転送信頼証明書および信頼されたルートCAとして有効にします。SSL復号化が高速化されたアプリに適用される場合、証明書を前方信頼証明書および信頼されたルートCAとして

©2025 Palo Alto Networks, Inc.

マークする必要があります。そうしないと、ユーザーがそれらのアプリにアクセスしようとしたときに SSL エラーが発生します。

- 未サポート**Prisma Access** 機能- 以下の機能はApp Accelerationをサポートしていません。これらの機能が有効になっているPrisma Accessデプロイメントは高速化されません。
  - IPv6

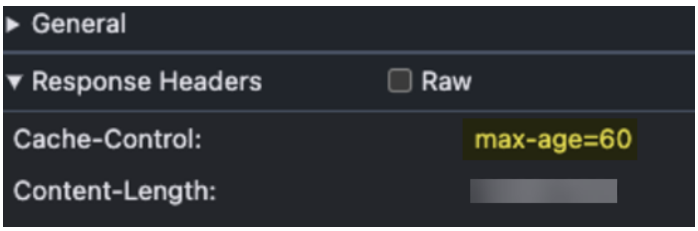
    IPv6が構成されている場合、App AccelerationはIPv6ネットワークと共存しますが、IPv4 TCPトラフィックのみが高速化されます。IPv6トラフィックは高速化されませんが、正常に機能します。
  - 重複サブネットを使用するリモートネットワーク （ Prisma Access (Managed by Strata Cloud Manager)デプロイメントではデフォルトでサポートされ、Prisma Access (Managed by Panorama)デプロイメントで構成可能です。
- **App Acceleration**ガイドライン:
  - **QUIC**プロトコルのサポート- 一部のブラウザ (Google Chrome など) では、デフォルトでQuick UDP Internet Connections (QUIC) プロトコルが使用される場合があります。レイヤー7 App Accelerationは、QUICを使用するトラフィックでは使用できません。回避策として、App Accelerationを構成するときにQUICプロトコルを無効にします。
  - **SaaS**アプリと**Zy-*** 応答ヘッダー- 上位のSaaSアプリに対してApp Accelerationが有効になっているPrisma Accessデプロイメントに接続するユーザーには、Zy-ServerやZy-Acceleratedなど、Zy-*という名前の応答ヘッダーとzy_sidセッション クッキーが表示されます。

    応答ヘッダーが Zy-Accelerated の場合、値**1**は応答が高速化されたことを示し、値**0**は応答が高速化されなかったことを示します。
  - コンテンツのローカリゼーション- 高速化されたSaaSアプリがユーザーのIPアドレスまたはユーザーIDのみに基づいてコンテンツをローカライズする場合、そのアプリで高速化が有効になっていても、そのコンテンツはローカライズされません。
  - アクションが拒否に設定されているセキュリティポリシールールのデフォルト動作の変更- 送信元または宛先アドレス、アプリケーション、またはサービスに基づくルールを使用して、App Accelerationを通過するトラフィックに適用されるアクションが 拒否 に設定されているセキュリティポリシールールがある場合、トラフィックは3ウェイハンドシェイクを完了しますが、 Prisma Accessはブロックし、拒否 ポリシーは設定どおりに機能します。
  - **Amazon S3**および**Azure Blob Storage**の キャッシュ制御- Amazon S3およびAzure Blob Storageのバケットとファイルには、一連のHTTP応答ヘッダーが関連付けられています。これらの値の1つは`cache-control`です。キャッシュ制御値が次の場合、ファイルは高速化されません：
    - アンセット
    - 次の値に設定：`max-age=0`

 ©2025 Palo Alto Networks, Inc.

- の値に設定：`max-age=no-cache`

Amazon S3およびAzure Blob StorageのApp Accelerationのメリットを得るには、`cache-control` `max-age` を0より大きい値に設定します。



- アクティビティ インサイトの共有ドメインを持つアプリ- App Accelerationを使用する場合、レイヤー7 アクセラレーションはドメインに基づいて行われます。特定の条件下では、2つのアプリが同じドメインを共有している場合、アクティビティ インサイトのアプリ レポートで、1つのアプリのレイヤー7 トラフィックが別のアプリに起因すると判断されることがあります。たとえば、MS TeamsとOneDriveアプリからのトラフィックが同じドメインを共有している場合、MS TeamsアプリのレポートはOneDriveの下に表示されます。
- 長時間接続とシステム ログ- App Accelerationは、個々のTCP接続が終了するとレイヤー4ログを書き込みます。短命の接続はアプリケーションによって頻繁に作成されるため、短命の接続の場合、この動作は透過的です。

  App Accelerationは、接続がアクティブな期間全体のメトリックを収集します。マウントされたSMBネットワーク ドライブで使用されるような長時間の接続の場合、この動作により、接続の終了時にのみメトリックが収集されるように見えることがあります。

©2025 Palo Alto Networks, Inc.

App Accelerationを設定する

Prisma AccessでApp Accelerationを設定するには、デプロイメントに応じて次のいずれかのタブを選択します（Prisma Access (Managed by Strata Cloud Manager) または Prisma Access (Managed by Panorama)）。

- Strata Cloud Manager
- Panorama

©2025 Palo Alto Networks, Inc.

Prisma Accessでアプリケーション アクセラレーションを設定する （Strata Cloud Manager）

Prisma Access (Managed by Strata Cloud Manager)デプロイメントでアプリケーション アクセラレーションを設定するには、このタスクを完了してください。

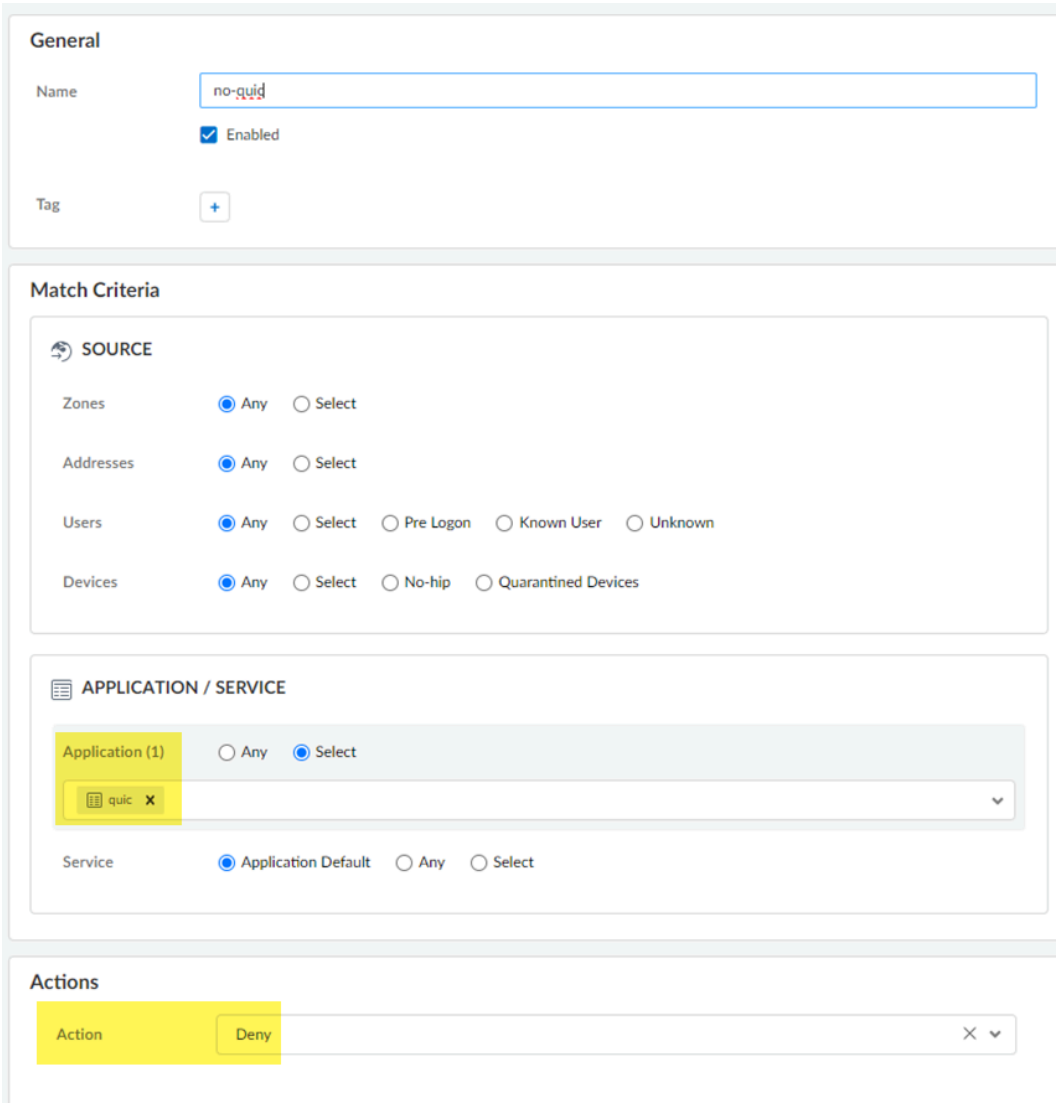
©2025 Palo Alto Networks, Inc.

STEP 1 | (任意) Quick UDP Internet Connections (QUIC) プロトコルを無効にします。

App Accelerationは、QUICを無効にせずにレイヤー7でアプリを高速化することはできません。

1. **[Manage (管理)]** > **[Configuration (設定)]** > **[NGFWとPrisma Access]** > **[Security Services (セキュリティ サービス)]** > **[Security Policy (セキュリティ ポリシー)]**そして**[Add Rule (ルールの追加)]** > **[Pre Rules (事前ルール)]**.に移動します。

   このセキュリティ ポリシー ルールをグローバル構成スコープに作成します。
2. アプリケーション/サービス として**quic**を選択し、アクションとして拒否を選択します。

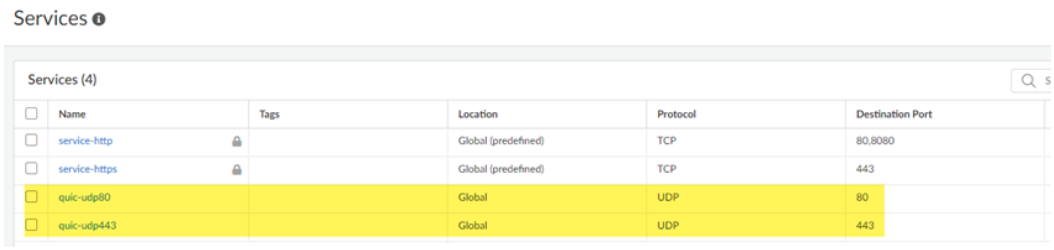


3. 変更を保存します。
4. [管理] > [構成] > **[NGFWとPrisma Access]** > [オブジェクト] > [サービス] > [サービス] [追加] に移動し、UDPポート80およびUDPポート443のサービスを追加します 。

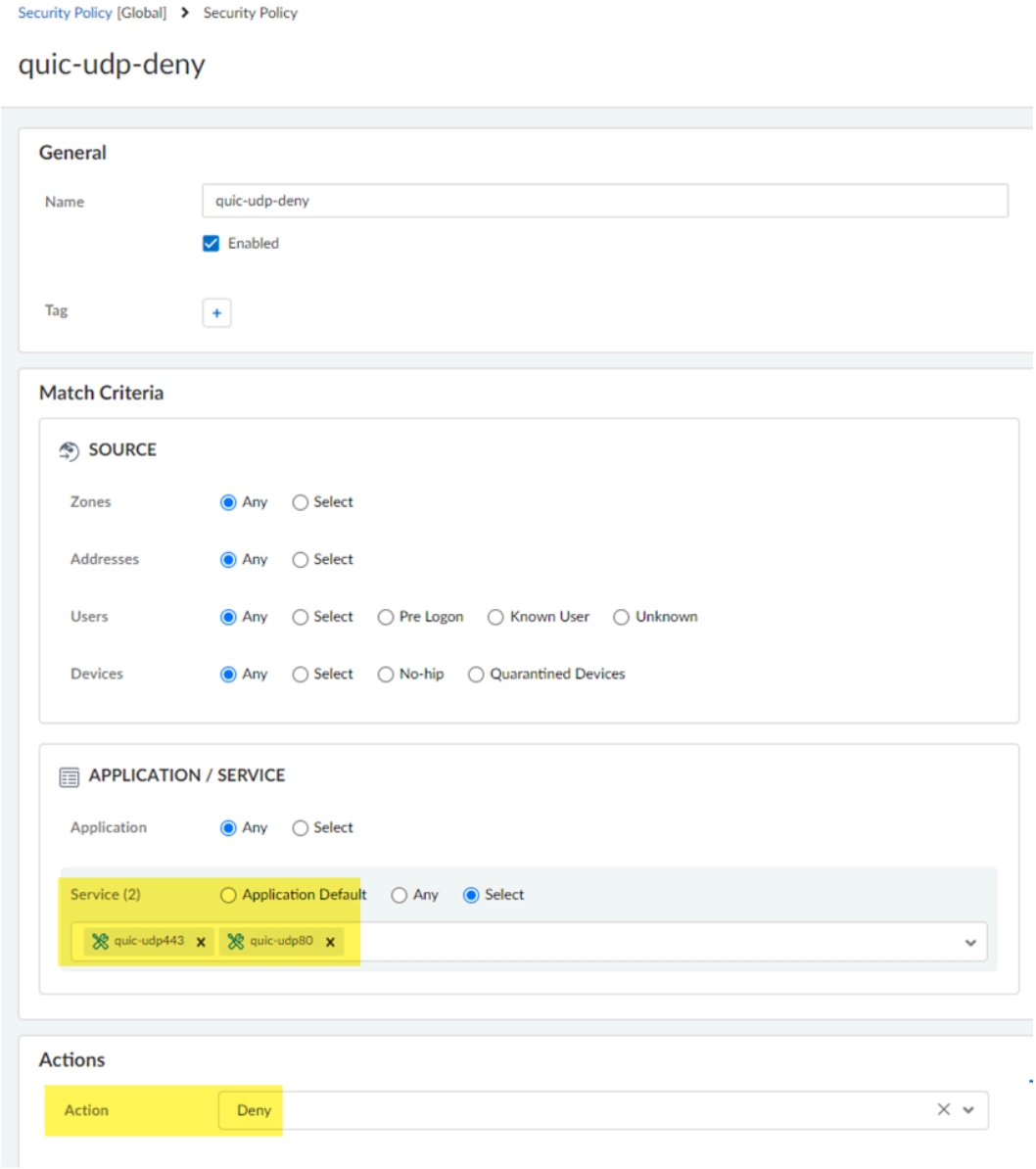
   Palo Alto Networksでは、新しいバージョンのQUICが **unknown-udp**と誤って識別される可能性があるため、UDP ポート80およびUDP ポート443のサービスを追加し、それ

 ©2025 Palo Alto Networks, Inc.

らのポート上のUDPトラフィックをブロックする追加のセキュリティ ポリシーを作成することを推奨しています。



5. [管理] > [構成] > [NGFWとPrisma Access] > [セキュリティ サービス] > [セキュリティ ポリシー][ルールの追加]に戻り、2 番目のセキュリティ ポリシーのルールを追加し、[アプリケーション/サービス] の下のサービスと 拒否のアクションを指定します。



 ©2025 Palo Alto Networks, Inc.

作業が完了すると、2つのセキュリティポリシーが存在することになります。1つはQUICプロトコルをブロックするポリシーで、もう1つはUDPポート80および443のトラフィックをブロックするポリシーです。



STEP 2 | App Accelerationで使用するために、Prisma AccessスコープのStrata Cloud Managerにルート証明局 (CA) 証明書と秘密キーをインポートし、変更をプッシュします。

自己署名ルートCA/証明書は、証明書チェーンの最上位の証明書です。App Accelerationは、ルートCA/証明書を使用して、アクセラレーションされたアプリの証明書を作成します。App Accelerationがアプリ固有の証明書の作成を開始できるように、Prisma Accessにルート CA/証明書をプッシュします。

ルートCA/証明書には次の特性が必要です:

- CAは信頼できるCAである必要があります。
- (推奨) CA は一意であり、App Accelerationにのみ使用される必要があります。
- CAは期限切れにできません。CAの有効期限をメモし、有効期限が切れる前に証明書を更新してください。App Accelerationで使用されているCA/証明書の有効期限が切れると、ユーザーは高速化されたアプリにアクセスしようとしたときにSSLエラーを受け取ります。組織でApp Accelerationを使用している場合は、CAが有効であることを確認することが重要です。
- キーを含める必要があります。
- パスフレーズを使用する必要があります。
- **Prisma Access**スコープ内にある必要があります。
- (モバイル ユーザー - GlobalProtectデプロイメントのみ) ローカル ルート証明書ストアにインストールする必要があります。

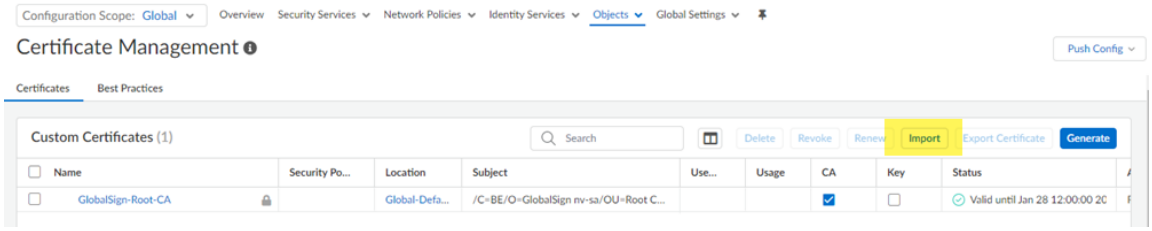
  このインストールは、この手順で説明されているように、信頼できる証明書のリストに追加することで実行できます。または、ActiveDirectoryを使用している場合は、Active

©2025 Palo Alto Networks, Inc.

Directoryグループ ポリシー オブジェクト (GPO) を使用してADからルートCAを配布することもできます。

ルートCA/証明書を変更する必要がある場合は、変更された証明書を使用する前に、証明書をアップロードして変更をコミットする必要があります。

1. **[Manage (管理)]** > **[Configuration (設定)]** > **[NGFWとPrisma Access]** > **[Objects (オブジェクト)]** > **[Certificate Management (証明書管理)]**に移動します。
2. 証明書をインポートします。



3. 次のパラメータを設定します。
   - 証明書の一意の 証明書名（`AppAcceleration_CA`など）を入力します。

     名前は大文字と小文字が区別され、最大31文字まで使用できます。名前には文字、数字、ハイフン、アンダースコアのみを使用してください。
   - **[ファイル]** を選択し 、CAから受信した証明書ファイルを参照して開きます 。
   - フォーマットを選択してください:
     - **Encrypted Private Key and Certificate (PKCS12)[暗号化された秘密鍵と証明書（PKCS12）]** – これは、デフォルトで最も一般的な形式であり、キーおよび証明書が単一のコンテナに（Certificate File [証明書ファイル]）格納されています。
     - **Base64 Encoded Certificate (PEM) [Base64** エンコード済み証明書（**PEM**）**]** – 証明書とは別にキーをインポートする必要があります。この形式を選択した場合は、 キー ファイルを 選択する必要があります。
     - **[Passphrase (パスフレーズ)]**と **[Confirm Passphrase (パスフレーズの確認)]**を入力します。
4. 変更を保存します。

©2025 Palo Alto Networks, Inc.

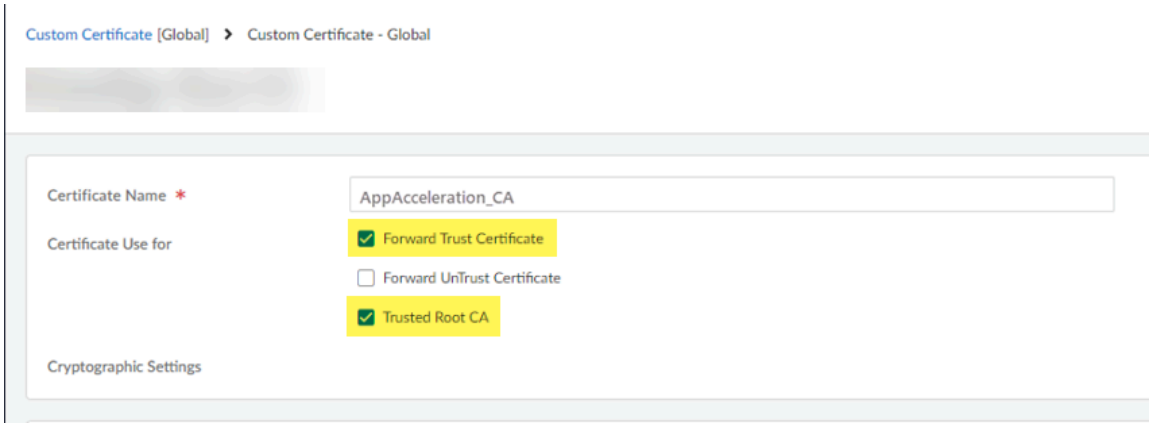


©2025 Palo Alto Networks, Inc.

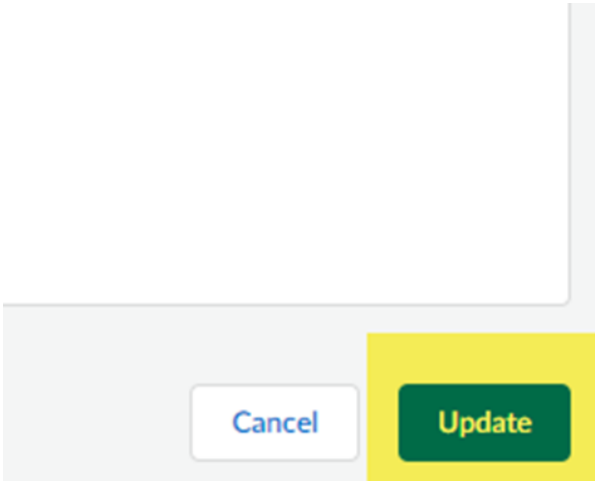
STEP 3 | 追加したルートCA/証明書を、前方信頼証明書および信頼されたルートCAとしてマークします。

証明書を前方信頼証明書および信頼されたルートCAとして指定しないと、SSL復号化を使用しているときにユーザーが高速化されたアプリにアクセスしようとすると、SSLエラーが発生します。

1. 追加したルートCA/証明書を選択します。
2. 証明書を 「転送信頼証明書」 および 「信頼されたルート**CA**」として選択します。

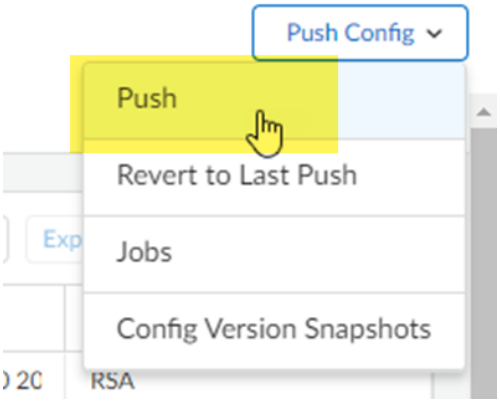


3. 証明書を更新します 。



©2025 Palo Alto Networks, Inc.

STEP 4 | 変更を **Push**（プッシュ）します。

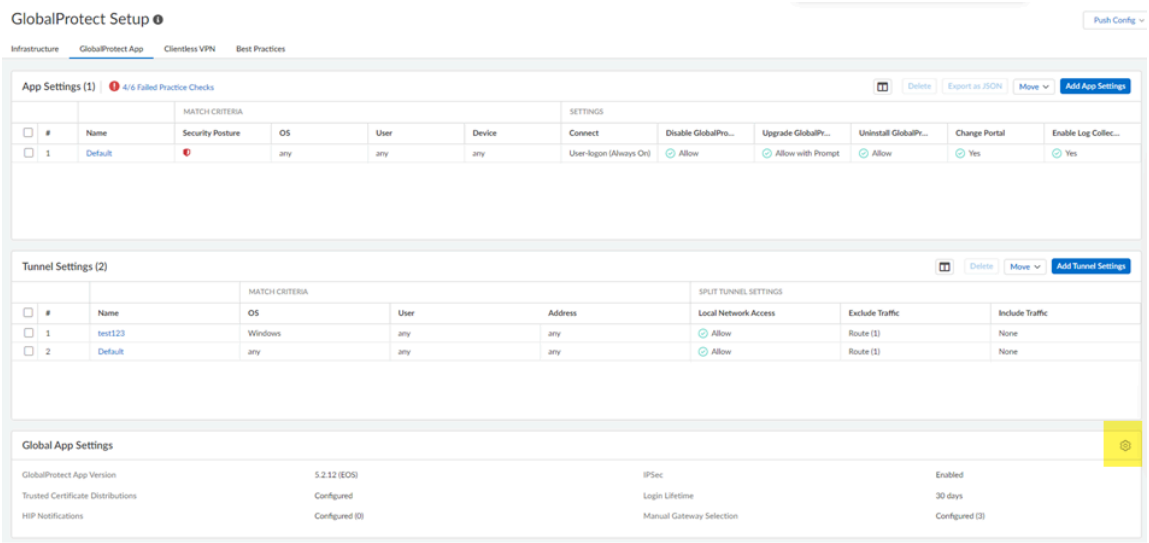


©2025 Palo Alto Networks, Inc.

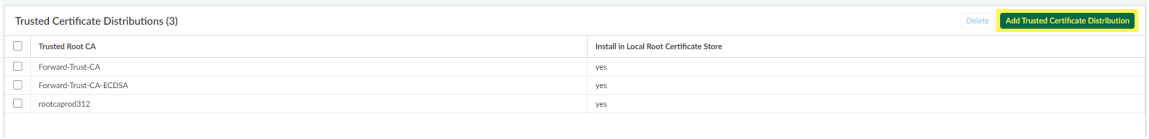
STEP 5 | (モバイル ユーザー - GlobalProtectデプロイメントのみ) 追加したルートCA/証明書をGlobalProtectの信頼できる証明書のリストに追加し、ローカル ルート証明書ストアにインストールします。

あるいは、*ActiveDirectory*を使用している場合は、*Active Directory GPO*を使用して*AD*からルート*CA*を配布できます。

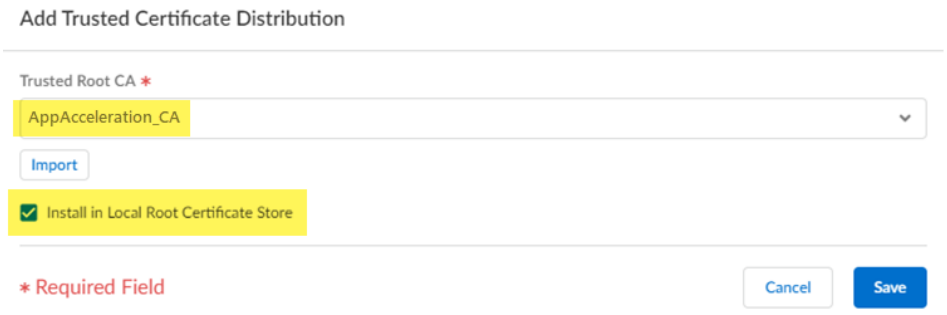
1. [ワークフロー] > **[Prisma Access** セットアップ] > **[GlobalProtect]** > **[GlobalProtect**アプリケーション] > [グローバル アプリ設定]に移動します。
2. 設定を編集するには、歯車をクリックします。



3. 信頼できる証明書配布の追加します。



4. 前の手順で作成した信頼されたルート**CA**を選択し、**[Install in Local Root Certificate Store (**ローカル ルート証明書ストアにインストール**)]**を選択します。

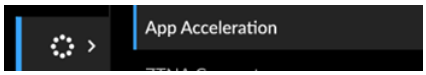


5. 変更を保存します。
6. 変更を **Push**（プッシュ）します。

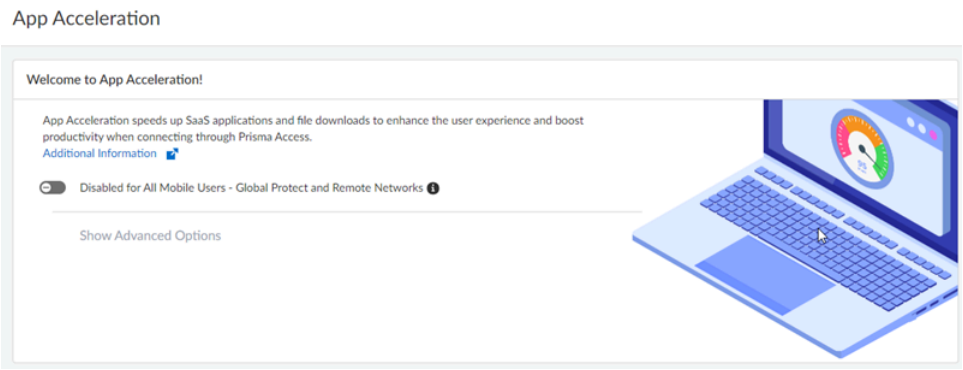
 ©2025 Palo Alto Networks, Inc.

STEP 6 | App Accelerationを有効にし、作成した証明書ファイルを選択します。

1. 左側のナビゲーション バーから **[ワークフロー] > [App Acceleration]** に移動します。

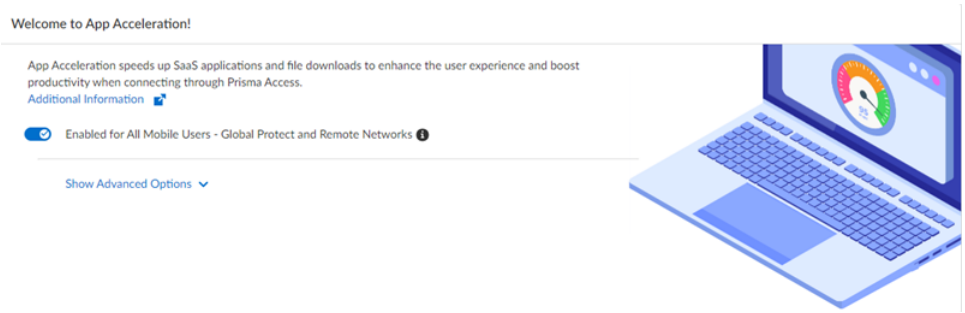


App Accelerationウィンドウが表示されます。



2. スライダーを右に移動すると すべてのモバイル ユーザー **(GlobalProtect** およびリモート ネットワーク**)** に対して**App Acceleration**が有効になります。

コミットが進行中の場合、*App Acceleration*設定はすべてのコミットが完了した後に有効になります。

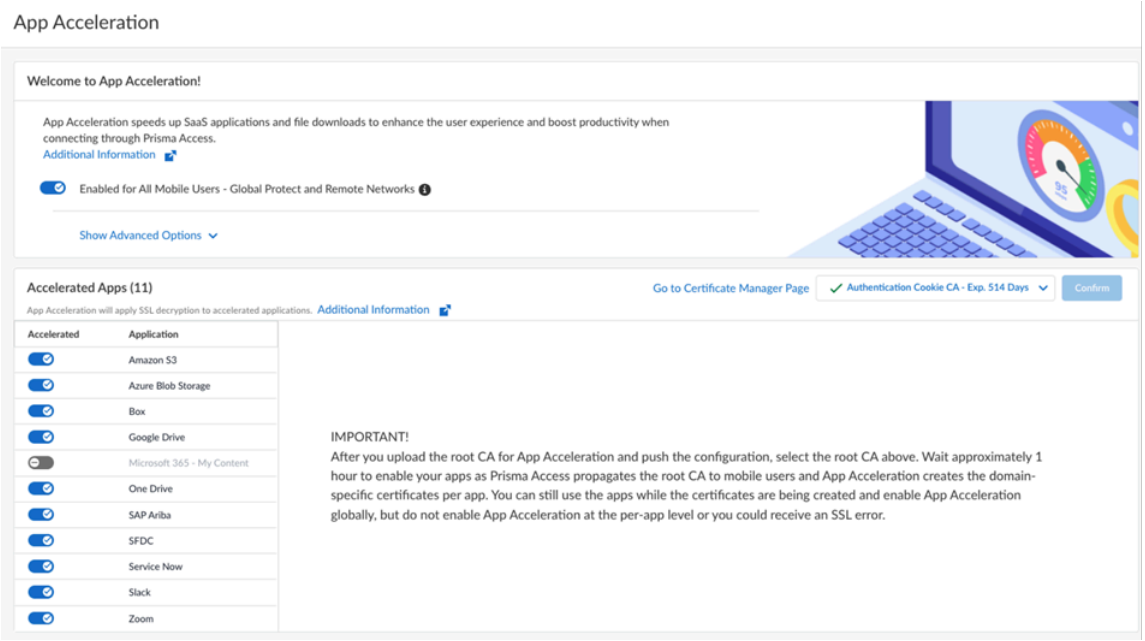


すべてのTCPトラフィックに対してApp Accelerationが有効になります。SaaSアプリを高速化したい場合は、次の手順に示すように、ルートCA/証明書を選択する必要があります。

©2025 Palo Alto Networks, Inc.

STEP 7 | 前の手順で作成した証明書を選択します。

既存の証明書を変更する必要がある場合は、証明書をファイアウォールとユーザーにコミットしてプッシュしたことを確認してから、ここで選択します。新しい証明書を選択する前にコミットする必要があります。



証明書をインポートした後、*App Acceleration*が各アプリに対してドメイン固有の証明書を生成するまで待つ必要があります。このプロセスには最大*1*時間かかる場合があります。その間、 ***[Accelerated Apps (***高速化アプリ***)]*** のスライダーを左に動かしてアプリ高速化を一時的に無効にし、証明書が生成されるまでアプリにアクセスすることができます。そうしないと、証明書が生成されるまで *SSL* エラーが発生する可能性があります。

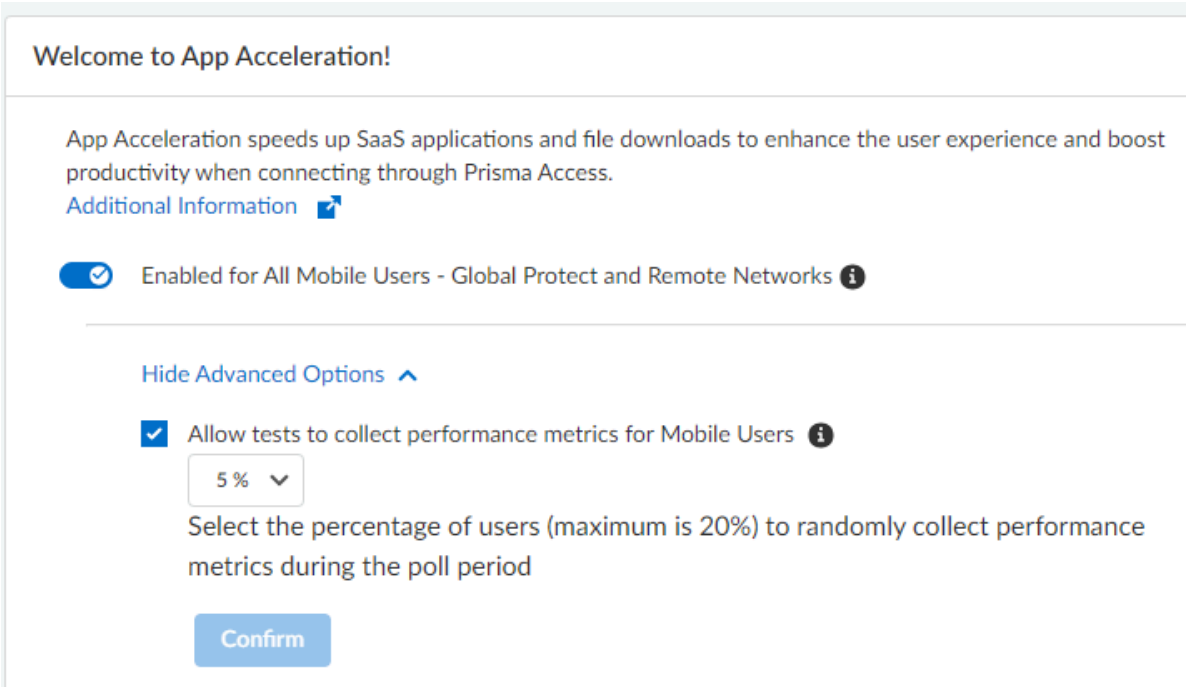
特定のアプリケーションでアクセラレーションをオンにした後、アクセラレーションがアクティブになるまで最大*10*分かかります。

©2025 Palo Alto Networks, Inc.

STEP 8 | (任意) 詳細オプションを表示し 、メトリック テスト パラメータを変更します。

- (任意) パフォーマンス情報を取得するためのメトリックの収集を無効にするには、[テストによるモバイル ユーザーのパフォーマンス メトリックの収集を許可する]の選択を解除します。

  Palo Alto Networksでは、App Accelerationを使用するときにアプリのパフォーマンス向上を確認するためにメトリックの収集を有効にすることをお勧めします。
- (任意) 予測テストが処理されるユーザーの割合をデフォルトの5%から変更するには、ドロップダウンで別の割合を選択し、変更を 確認します 。



 ©2025 Palo Alto Networks, Inc.

Prisma Accessでアプリケーション アクセラレーションを設定する （Panorama）

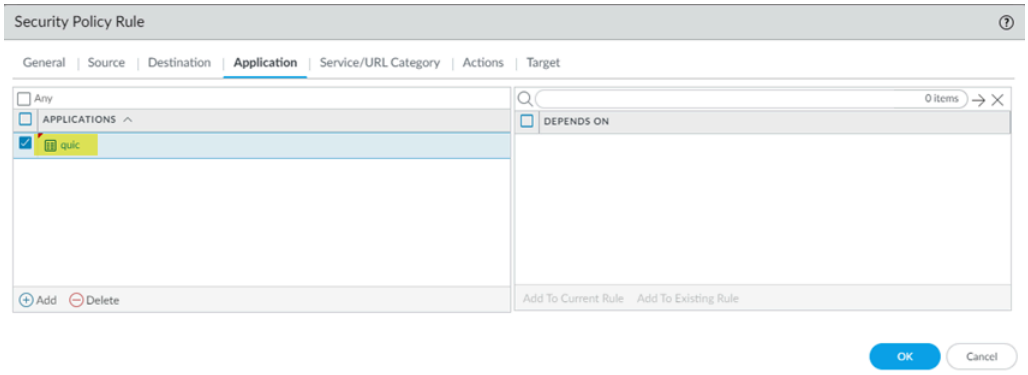
Prisma Access (Managed by Panorama)デプロイメントでアプリケーション アクセラレーションを設定するには、このタスクを完了してください。

STEP 1 | (任意) Quick UDP Internet Connections (QUIC) プロトコルを無効にします。

App Accelerationは、QUICを無効にせずにレイヤー7でアプリを高速化することはできません。

1. [ポリシー] > [セキュリティ] > [事前ルール] に移動して、セキュリティ ポリシーを追加します 。

   共有 デバイス グループにこのセキュリティ ポリシー ルールを作成します。
2. アプリケーションとして**quic**を選択し、 アクション として 拒否を選択します。



3. 2番目のセキュリティ ポリシーを追加します 。

   新しいバージョンのQUICは、**unknown-udp**と誤って識別されることがあります。そのため、UDPポート80およびUDPポート443向けのサービスを追加して、それらのポートへのUDPトラフィックをブロックするセキュリティポリシーを作成することをお勧めします。
4. [サービス/**URL** カテゴリ]で、UDP ポート 80 と UDP ポート 443 の新しいサービスと [アクション] [拒否]を追加します 。

   作業が完了すると、2つのセキュリティポリシーが存在することになります。1つはQUICプロトコルをブロックするポリシーで、もう1つはUDPポート80および443のトラフィックをブロックするポリシーです。

	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 | App Accelerationで使用するためにPanoramaにルート証明局 (CA) 証明書と秘密キーをインポートし、変更をコミットしてプッシュします。

自己署名ルートCA/証明書は、証明書チェーンの最上位の証明書です。App Accelerationは、ルートCA/証明書を使用して、アクセラレーションされたアプリの証明書を作成します。App Accelerationがアプリ固有の証明書の作成を開始できるように、Prisma Accessにルート CA/証明書をプッシュします。

ルートCA/証明書には次の特性が必要です:

- CAは信頼できるCAである必要があります。
- (推奨) CA は一意であり、App Accelerationにのみ使用される必要があります。
- CAは期限切れにできません。CAの有効期限をメモし、有効期限が切れる前に証明書を更新してください。App Accelerationで使用されているCA/証明書の有効期限が切れると、ユーザーは高速化されたアプリにアクセスしようとしたときにSSLエラーを受け取ります。組織でApp Accelerationを使用している場合は、CAが有効であることを確認することが重要です。
- キーを含める必要があります。
- パスフレーズを使用する必要があります。
- (モバイル ユーザー - GlobalProtectデプロイメントのみ) ローカル ルート証明書ストアにインストールする必要があります。

  このインストールは、この手順で説明されているように、信頼できる証明書のリストに追加することで実行できます。または、アクティブディレクトリを使用している場

 ©2025 Palo Alto Networks, Inc.

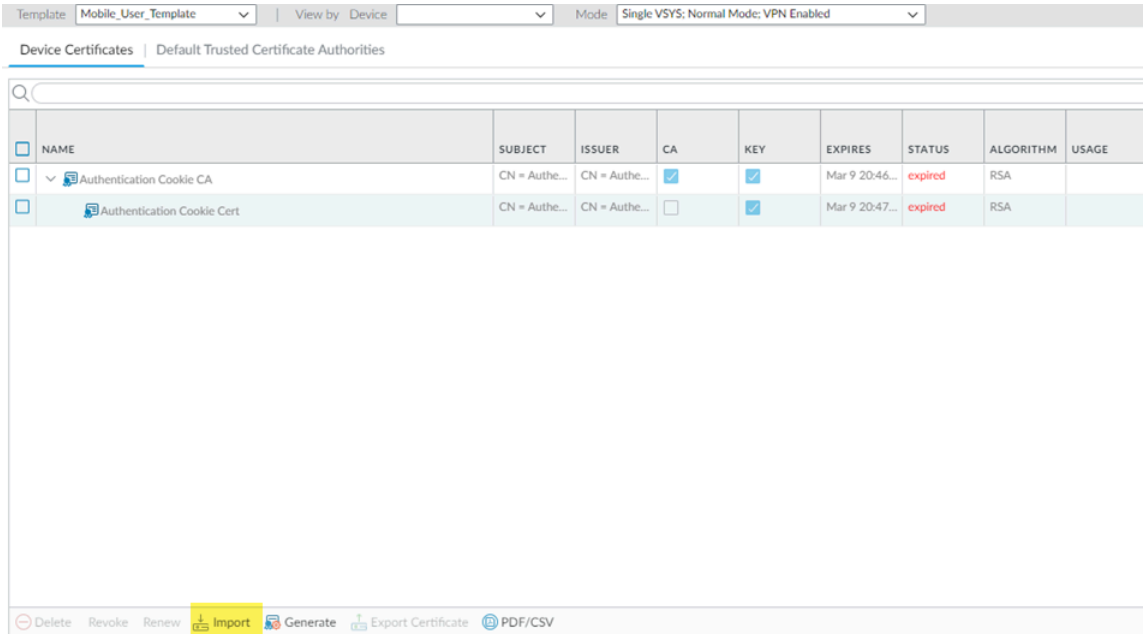
合は、Active Directoryグループ ポリシー オブジェクト (GPO) を使用してADからルートCAを配布することもできます。

ルートCA/証明書を変更する必要がある場合は、変更された証明書を使用する前に、証明書をアップロードして変更をコミットしプッシュする必要があります。

1. [デバイス] > [証明書] > [証明書管理]に移動します。

   Mobile_User_Templateにいることを確認してください。

2. 証明書をインポートします。



3. 次のパラメータを設定します。

   - 証明書の一意の 証明書名（AppAcceleration_CAなど）を入力します。

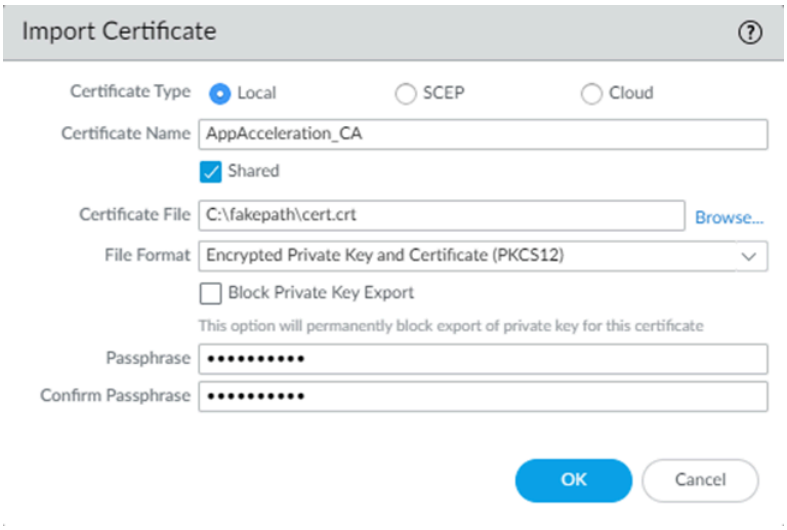
     名前は大文字と小文字が区別され、最大31文字まで使用できます。名前には文字、数字、ハイフン、アンダースコアのみを使用してください。

   - CAから受け取った証明書ファイルを参照して開きます 。
   - フォーマットを選択してください:

     - **Encrypted Private Key and Certificate (PKCS12)**[暗号化された秘密鍵と証明書（**PKCS12**）] – これは、デフォルトで最も一般的な形式であり、キーおよび証明書が単一のコンテナに（Certificate File [証明書ファイル]）格納されています。
     - **Base64 Encoded Certificate (PEM) [Base64** エンコード済み証明書（**PEM**）] – 証明書とは別にキーをインポートする必要があります。この形式を選択した場合は、秘密キーをインポートし、キー ファイルを選択する必要があります。
     - **[Passphrase (**パスフレーズ**)]**と**[Confirm Passphrase (**パスフレーズの確認**)]**を入力します。

4. **OK** をクリックします。

©2025 Palo Alto Networks, Inc.



5. Mobile_User_Template を Remote_Network_Templateに置き換えて、これらの手順を繰り返します。

   モバイル ユーザーとリモート ネットワーク サイトのユーザー向けにアプリを高速化するには、Mobile_User_Template と Remote_Network_Templateの両方にこれらの証明書をインポートする必要があります。

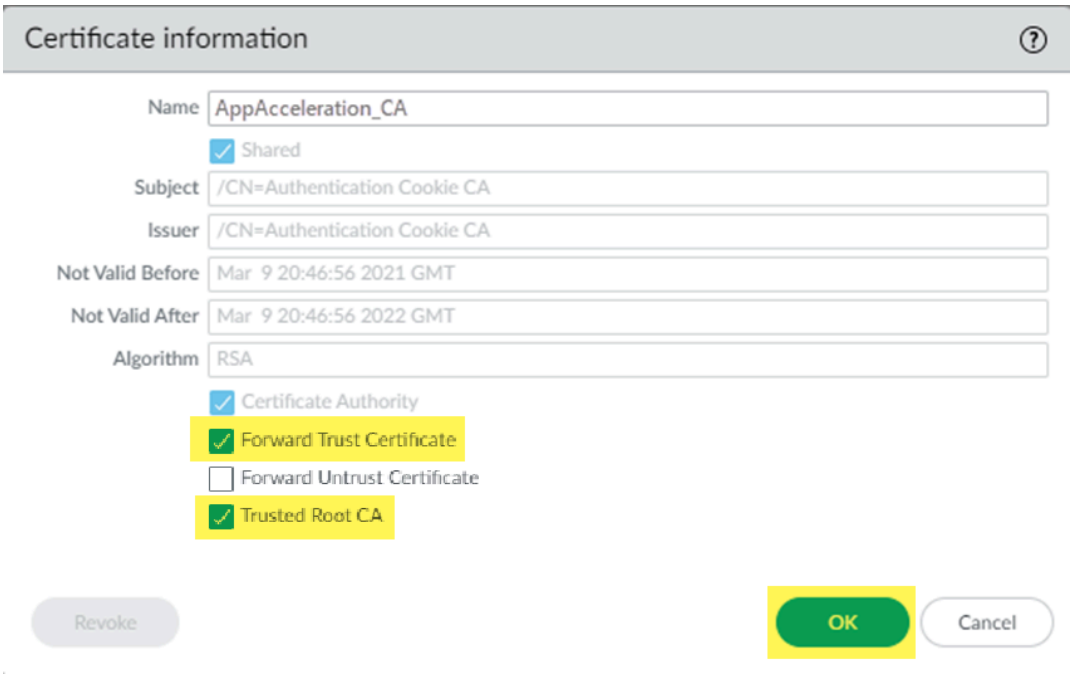
STEP 3 | 追加したルートCA/証明書を、前方信頼証明書および信頼されたルートCAとしてマークします。

証明書を前方信頼証明書および信頼されたルートCAとして指定しないと、SSL復号化を使用しているときにユーザーが高速化されたアプリにアクセスしようとすると、SSLエラーが発生

©2025 Palo Alto Networks, Inc.

します。Mobile_User_Template と Remote_Network_Templateに証明書がある場合は、両方のテンプレートでこの手順を実行します。

1. 追加したルートCA/証明書を選択します。
2. 証明書を「転送信頼証明書」 および「信頼されたルート**CA**」として選択**OK**をクリックします。



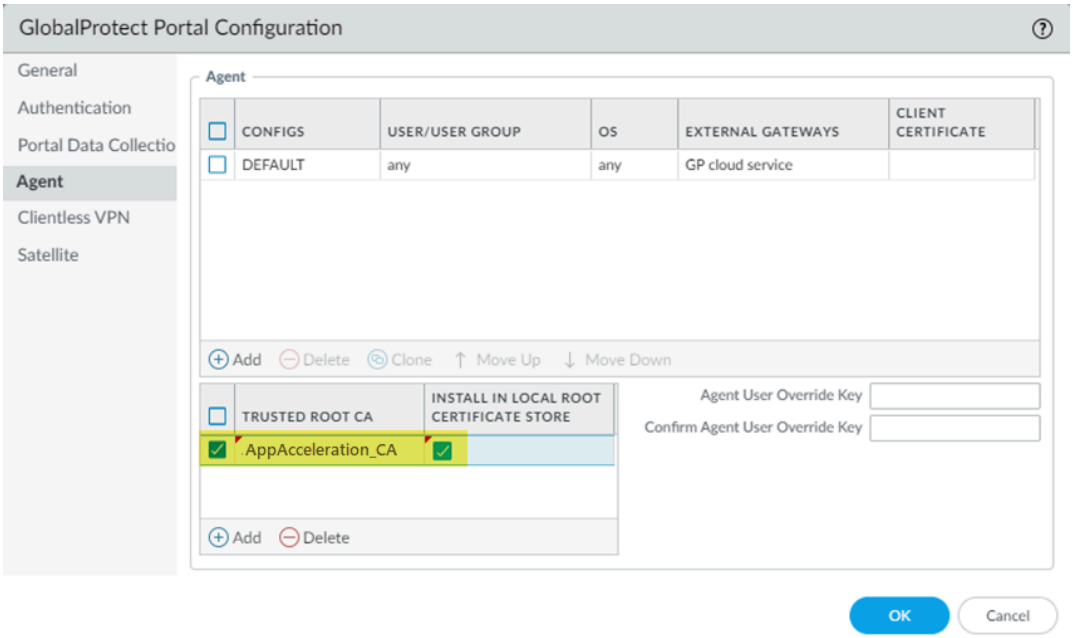
STEP 4 | 変更を **Commit and Push**（コミットしてプッシュ）します。

©2025 Palo Alto Networks, Inc.

STEP 5 | (モバイル ユーザー - GlobalProtectデプロイメントのみ) 追加したルー CA/証明書を、GlobalProtectポータル構成のGlobalProtect信頼済み証明書のリストに追加します。

あるいは、アクティブディレクトリを使用している場合は、*Active Directory GPO*を使用して*AD*からルート*CA*を配布できます。

1. [ネットワーク] > **[GlobalProtect]** > [ポータル] > **[GlobalProtect_Portal]** > [エージェント]に移動します。
   Mobile_User_Templateにいることを確認してください。
2. 前の手順で作成した信頼されたルート CAを追加します 。
3. [ローカル ルート証明書ストアにインストール] を選択します。
4. **OK** をクリックします。

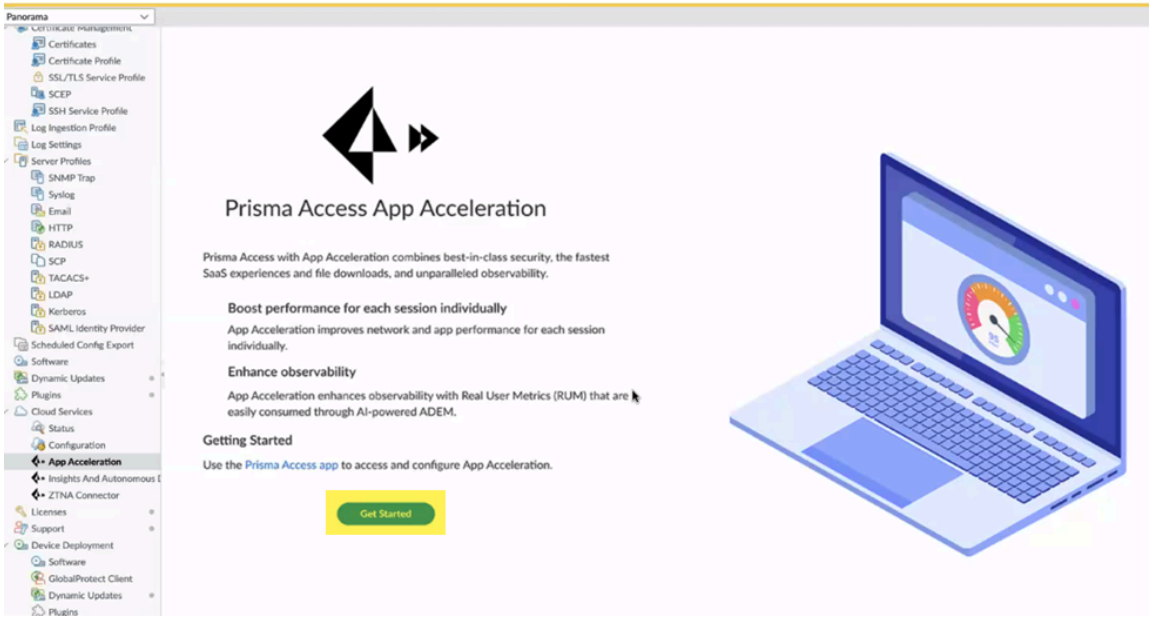


5. 変更を **Commit and Push**（コミットしてプッシュ）します。

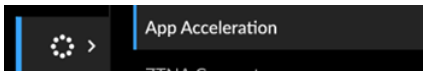
©2025 Palo Alto Networks, Inc.

STEP 6 | App Accelerationを有効にし、作成した証明書ファイルを選択します。

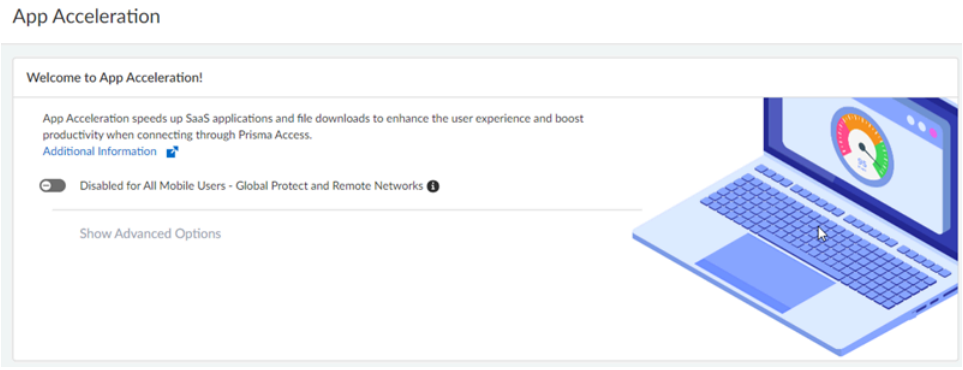
1. **[Panorama]** > **[Cloud Services]** > **[App Acceleration]** にアクセスし、App Accelerationの使用を開始します。



2. 左側のナビゲーション バーから **[ワークフロー]** > **[App Acceleration]** に移動します。



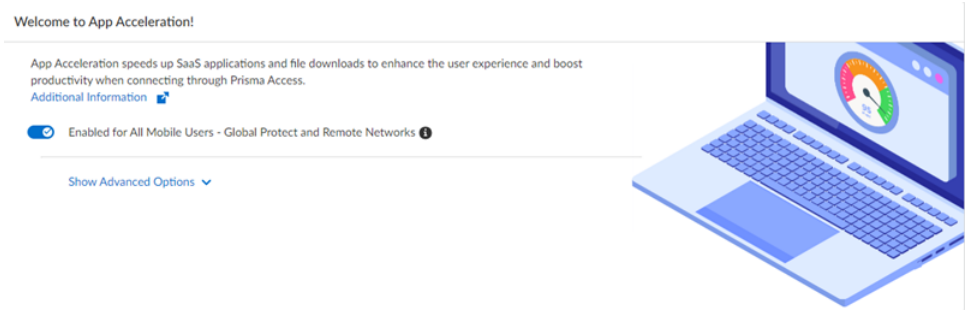
App Accelerationウィンドウが表示されます。



3. スライダーを右に移動すると すべてのモバイル ユーザー **(GlobalProtect** およびリモート ネットワーク**)** に対して**App Acceleration**が有効になります。

コミットが進行中の場合、*App Acceleration*設定はすべてのコミットが完了した後に有効になります。

©2025 Palo Alto Networks, Inc.



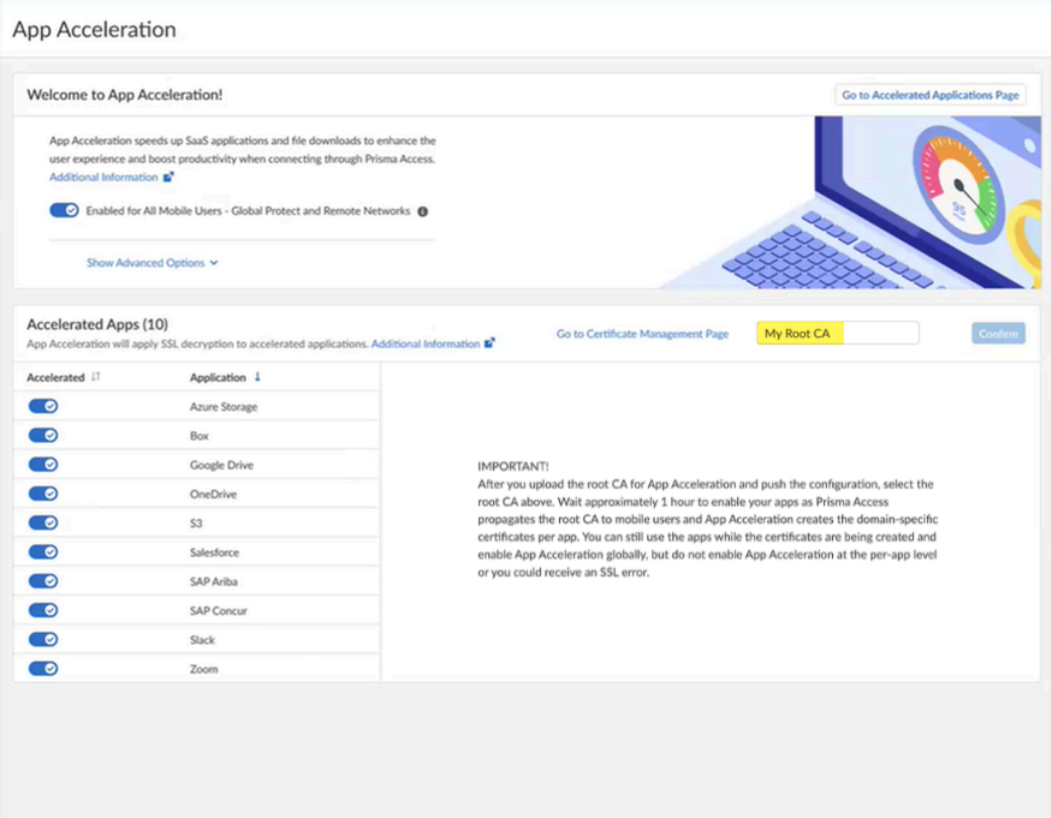
すべてのTCPトラフィックに対してApp Accelerationが有効になります。SaaSアプリを高速化したい場合は、次の手順に示すように、ルートCA/証明書を選択する必要があります。

©2025 Palo Alto Networks, Inc.

STEP 7 | App Acceleration構成で、前の手順で作成した証明書の名前を、Panoramaにリストされているとおりに入力します。

証明書を入力する前に、必ず証明書をコミットしてプッシュしてください。

既存の証明書を変更する必要がある場合は、新しい名前を入力します。名前を入力する必要があります (リストから選択することはできません)。また、名前を入力する前に、新しい証明書をコミットしてプッシュする必要があります。



証明書をインポートした後、*App Acceleration*が各アプリに対してドメイン固有の証明書を生成するまで待つ必要があります。このプロセスには最大*1*時間かかる場合があります。その間、 ***[Accelerated Apps (*高速化アプリ*)]*** のスライダーを左に動かしてアプリ高速化を一時的に無効にし、証明書が生成されるまでアプリにアクセスすることができます。そうしないと、証明書が生成されるまで *SSL* エラーが発生する可能性があります。

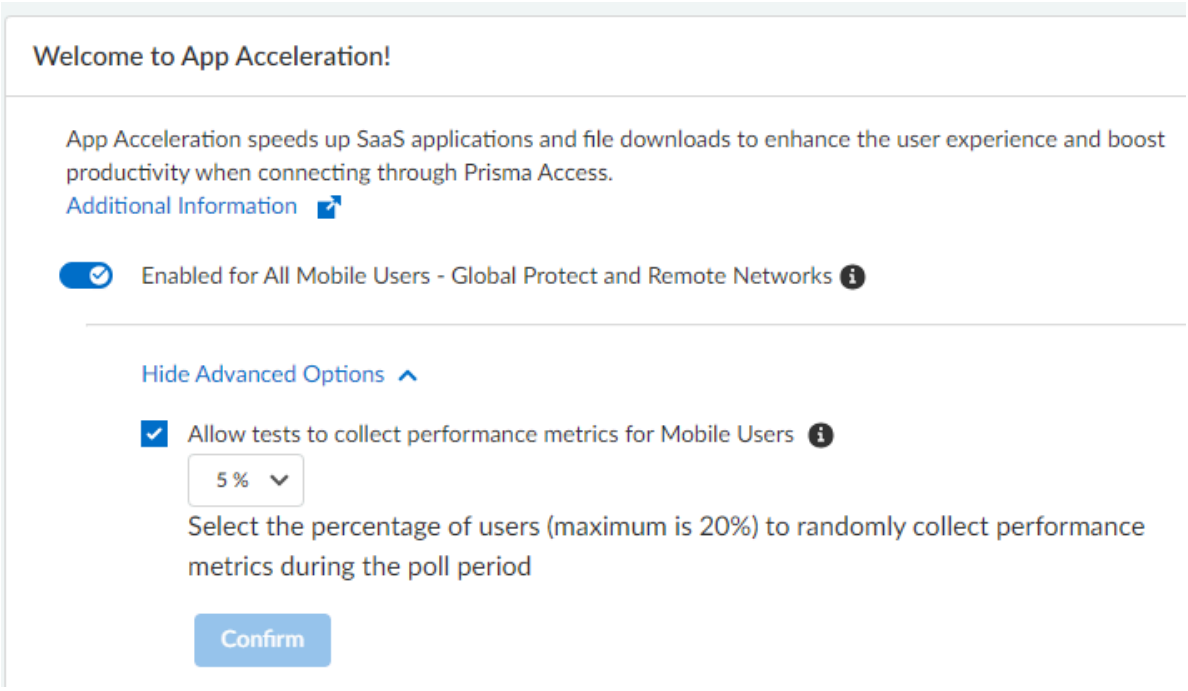
特定のアプリケーションでアクセラレーションをオンにした後、アクセラレーションがアクティブになるまで最大*10*分かかります。

©2025 Palo Alto Networks, Inc.

STEP 8 | (任意) 詳細オプションを表示し 、メトリック テスト パラメータを変更します。

- (任意) パフォーマンス情報を取得するためのメトリックの収集を無効にするには、[テストによるモバイル ユーザーのパフォーマンス メトリックの収集を許可する]の選択を解除します。

  Palo Alto Networksでは、App Accelerationを使用するときにアプリのパフォーマンス向上を確認するためにメトリックの収集を有効にすることをお勧めします。
- (任意) 予測テストが処理されるユーザーの割合をデフォルトの5%から変更するには、ドロップダウンで別の割合を選択し、変更を 確認します 。



 ©2025 Palo Alto Networks, Inc.

Prisma Access モバイルユーザー

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

Prisma Accessではモバイルユーザーを保護するために、2つの接続方法が提されています：ユーザーは、GlobalProtectアプリケーションを使用するか、プロキシ自動構成（PAC）ファイルを使用してPrisma Accessに接続できます。

- **GlobalProtect**アプリケーションでモバイルユーザーを保護する

  以下のモードでGlobalProtectを使用できます:

  - トンネルモード—Prisma AccessのGlobalProtectのデフォルトエージェントモードトンネル（IPSecまたはSSL）をPrisma Accessに確立し、モバイル・ユーザーのすべてのアプリケーション、ポート、プロトコルへのアクセスを保護し、ユーザーがネットワーク内外にいるかにかかわらず、一貫したセキュリティを確保します。

    ユーザーのエンドポイントにインストールされたGlobalProtectアプリケーションは、ユーザーのインターネット、SaaSアプリケーション、および内部および公共のクラウドリソースへのトラフィックを保護します。GlobalProtectアプリをユーザーにデプロイし（Microsoft Windows、Apple macOSおよびiOS、Android、Google Chrome OS、Linuxを実行するスマートフォン、タブレット、またはラップトップで利用可能）、トラフィックをPrisma Accessにトンネリングしてポリシーの実施と脅威防御を行えるようにします。GlobalProtectアプリケーションは、ホスト情報プロファイル（HIP）レポートも提供しており、デバイスの状態に基づいて詳細なルールを作成し、エンドポイントがあなたのセキュリティ基準に準拠していることを確認できます。たとえば、最も最新のパッチ、暗号化、およびウイルス定義が装備されていることを確認し、最も機密性の高いアプリケーションにアクセスできるようにします。また、管理されていないデバイスのユーザーにも安全なアクセスを可能にするには、クライアントレスVPNを有効にします。 Prisma Accessは、ユーザーが現在どこにいるかに基づいて、地域ごとに動的にスケールイン/スケールアウトします。
  - プロキシモード—このモードでは、サードパーティのVPNエージェントを使用しながら、Prisma AccessをセキュアWebゲートウェイとして使用し、一貫性のある優れたSaaSセキュリティを実現することができます。この接続方法は、既存のプライベートアプリVPNをまだ置き換える準備ができていないが、セキュアWebゲートウェイを置き換えたい場合に最適です。例えば、プライベート アクセスのためにサードパーティ製のVPNエージェントを使用しているが、インターネット セキュリティのためにPrisma Accessだけを使用したいとします。この接続方法の利点には次のものが含まれます:
    - プロキシを必要とするコンプライアンスまたはネットワーク要件を満たします
    - PACファイル管理の負担を軽減し、ブラウザを超えたプロキシ対応アプリをサポートします

- オンプレミスのウェブプロキシにバックホールする必要を回避することで、ユーザーエクスペリエンスを向上させます。

- トンネルおよびプロキシモード–このモードでは、プロキシモードを通じてインターネットおよびSaaSアプリケーションへのアクセスを保護し、トンネルモードを通じてプライベートアプリへのアクセスを保護できます。これは、プライベートアプリへの最速で低遅延のアクセスが必要で、お使いのPrisma Accessロケーションが地域内にない場合に特に役立ちます。

  このモードでは、GlobalProtectアプリケーションが最初にあなたが定義したPrisma Access明示型プロキシ転送ルールを評価し、すべてのインターネット向けトラフィックを明示的プロキシに送信します。すべての他のトラフィックについて、アプリは、定義したスプリットトンネルルールに基づいて、どのトラフィックをトンネルを通してGlobalProtectゲートウェイに送信し、どのトラフィックをトンネルから除外するかを決定します。トンネルを使用して、プロキシを認識していないアプリケーションを保護することもできます。

- **PAC**ファイルを使用してモバイルユーザーを保護する

  GlobalProtectを使用してモバイルユーザーを保護することに加えて、Prisma Accessを使用して明示型プロキシを構成できます。明示型プロキシを使用すると、エンドポイントはPACファイルを使用して、Webブラウザやプロキシ対応アプリにトラフィックを宛先サーバーではなくウェブプロキシサーバーに転送するよう指示します。これにより、Webベースのインターネット（HTTPおよびHTTPS）トラフィックが保護されます。

  既存のネットワークですでに明示型プロキシを使用し、クライアント エンドポイントとサーバートにPACファイルをデプロイしている場合、レガシー プロキシ ベースのSWGソリューションからPrisma Accessにスムーズに移行し、モバイル・ユーザーのアウトバウンドインターネット トラフィックを保護することができます。監査やコンプライアンスの目的でプロキシを使用する必要がある場合は、明示型プロキシを使用することもできます。

- **Prisma Access**ブラウザモバイルによるモバイルユーザーの保護

  Prisma Access Browser Mobileは、強力なアクセス制御と明確で直感的なインターフェースを組み合わせることで、モバイルユーザーのセキュリティを簡素化します。ユーザーがVPN、証明書、またはモバイルデバイス管理（MDM）システムに依存することなく、プライベートアプリケーションに安全にアクセスできるようにし、複雑さを軽減し、接続を容易にします。

  BYOD（Bring Your Own Device）環境向けに設計されており、管理されていないデバイス上のプライベートアプリケーションへの安全なアクセスを確保し、組織が重要なリソースを全従業員に拡張できるようにします。タブレットは、Prisma Access Browser Mobileを通じて多目的なデスクトップの代替となり、従来のエンドポイントと同レベルのセキュリティとアクセスを提供します。

  Prisma AccessBrowser Mobileを使用することで、組織はプライベートアプリへのアクセスを効率化し、タブレットベースの生産性を向上させ、さまざまなモバイルプラットフォーム全体で信頼性の高いセキュリティを維持できます。

©2025 Palo Alto Networks, Inc.

モバイルユーザー:グローバルプロテクト

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

GlobalProtectを使用すると、エンドポイントに GlobalProtectアプリケーション をインストールし、GlobalProtect設定をPrisma Accessで構成することでモバイルユーザーを保護できます。GlobalProtectを使用すると、モバイル ユーザーによるすべてのアプリケーション、ポート、プロトコルへのアクセスを保護し、ユーザーがネットワークの内外にいるかどうかに関係なく一貫したセキュリティを実現できます。

GlobalProtectを使用してモバイル ユーザーを保護する場合は、クラウド内の ポータルとゲートウェイ を構成するための設定を定義する必要があります。たとえば、ポータルホスト名の定義、モバイルユーザー向けのIPアドレスプールの設定、内部ドメイン用のDNS設定などの作業を行います。モバイルユーザーの認証に使用する認証プロファイルなど、必要な設定の一部に対しては、既存の設定を利用できる場合もあります。認証プロファイル、証明書、証明書プロファイル、およびサーバープロファイルを持つテンプレートをすでに保有している場合は、セットアップ手続きを簡素化するために、オンボーディング時にそのテンプレートを、事前定義テンプレートスタックに追加できます。

データセンター/本社のロケーションへのアクセスを提供する接続を使用する予定がない場合でも、モバイルユーザーによるリモートネットワークロケーションへの接続を可能にしたい場合、または地理的に異なるエリアに存在するモバイルユーザーが相互のエンドポイントに直接アクセスする必要があるような場合、プレースホルダー値を使って最低1つのサービス接続を設定する必要があります。これが必要な理由は、すべてのリモートネットワークロケーションが完全にメッシュ化されていますが、Prisma Accessインフラ内の内部ネットワークへのアクセスを提供するために、Prisma Accessゲートウェイ（ロケーション）は、ハブアンドスポークアーキテクチャ内のサービス接続に接続するからです。

- Prisma AccessのGlobalProtectの計画チェックリスト
- GlobalProtect モバイルユーザーの設定
- GlobalProtect – トンネル設定のカスタマイズ
- GlobalProtectを無効にするチケットリクエスト(Strata Cloud Manager)
- GlobalProtectモバイルユーザーを監視する
- GlobalProtectモバイル ユーザーデプロイメントのIPアドレス プール
- GlobalProtectアプリケーションがモバイルユーザーのためにPrisma Accessロケーションを選択する方法
- GlobalProtectモバイルユーザーのリスト表示を許可する
- GlobalProtectアプリケーションのアップグレード
- Prisma AccessをオンプレミスのGlobalProtectゲートウェイと統合する

©2025 Palo Alto Networks, Inc.

Prisma AccessのGlobalProtectの計画チェックリスト

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

GlobalProtectを使用してモバイル ユーザーを保護する場合は、次のチェックリストを使用して、サービスを正常に有効にし、モバイル ユーザーに対して一貫したポリシーを適用できることを確認します (エンドポイントにGlobalProtectアプリケーションがインストールされたユーザーを保護し、ユーザーが Clientless VPNを使用してアプリケーションに安全にアクセスできるようにします)。

- インストール前のチェックリスト：
  - **IP**アドレスプール–ユーザー向けのPrisma Accessを設定するには、内部的に使用している他のIPアドレスやインフラサブネットに対して指定したIPアドレスプールとオーバーラップしていないIPアドレスプールを指定する必要があります。

    *RFC 1918*準拠の*IP*アドレスプールを使用することをお勧めします。*RFC 1918*非準拠の（パブリック）*IP*アドレスはサポートされていますが、インターネットのパブリック*IP*アドレス空間と競合する可能性があるため、お勧めできません。

    次の IP アドレスおよびサブネットと重複するサブネットは指定しないでください。Prisma Accessはこれらの IP アドレスおよびサブネットを内部使用のために予約します。

    169.254.0.0/16 および 100.64.0.0/10

    Prisma Accessは、GlobalProtectアプリケーションを使ってPrisma Accessに接続する際に、このIPアドレスプールを使ってエンドポイントの仮想ネットワークアダプタにIPアドレスを割り当てます。Prisma Accessモバイルユーザーゲートウェイに接続する各デバイスには、独自のIPアドレスが必要になります。これらのプールは、モバイル ユーザーのオンボーディング プロセス中に指定します。

    プール内の IP アドレス数は、Palo Alto NetworksではPrisma Accessに接続するモバイルユーザーデバイス数の2倍にすることをお勧めしています。組織がBYODポリシーを採用している場合、または1人のユーザーが複数のユーザーアカウントを保有している場合は、IPプールの割り当て時にそれらの余分なデバイス数も考慮に入れてください。IPアドレスプールの限界に達した場合、その他のモバイルユーザーデバイスは接続できなくなります。

    モバイルユーザーデバイスがゲートウェイに接続する場合、Prisma Accessによって指定したプールからIPアドレスが取得され、/24のブロックでゲートウェイに割り当てられます。より多くのユーザーデバイスがログインして/24ブロックが制限に達すると、Prisma Accessはプールからゲートウェイにさらに /24 ブロックを割り当てます。 Prisma Accessは、ゲートウェイの割り当てに基づいて割り当てられたこれらの /24 サブネットをバックボーンにアドバタイズする。

©2025 Palo Alto Networks, Inc.

- テンプレート– Prisma AccessGlobalProtectのデプロイメントでは、テンプレート スタックと最上位テンプレートが自動的に作成されます。すでにオンプレミスでGlobalProtectを実行しており、既存の設定を活用したい場合は、追加のテンプレートをスタックに追加して、既存のGlobalProtectポータル、GlobalProtectゲートウェイ、User-ID、サーバープロファイル（たとえば、認証サービスへの接続用）、証明書、およびSSL/TLSサービスプロファイル設定をPrisma Access for usersにプッシュすることができます。既存の構成設定のテンプレートがない場合は、Prisma Access (Managed by Panorama)でGlobalProtectをセットアップするときに、必要な構成設定を手動で入力することができます。また、スタックに追加するテンプレートには、モバイルユーザーに対してセキュリティポリシーを適用するために使用するゾーンの、ゾーン設定が含まれていなければなりません。
- 親デバイスグループ–Prisma Access for usersを設定する場合、セキュリティポリシー、セキュリティプロファイル、およびその他のポリシーオブジェクト（アプリケーショングループとオブジェクト、アドレスグループなど）、HIPオブジェクトとプロファイル、およびリモートユーザーに一貫したポリシーを適用するために、サービスが必要とする認証ポリシーをプッシュするために使用する親デバイスグループを指定する必要があります。
- オンボーディングするロケーション–Prisma Accessでは、Prisma Access (Managed by Panorama)でGlobalProtectをセットアップできる世界各地のロケーションを提供しています。ロケーションのオンボーディングを開始する前に、このリストを参照して、モバイルユーザーデプロイ環境のどのロケーションをオンボーディングするのかを判断してください。

  ユーザーにもっとも近いロケーション、またはユーザーと同じ国に存在しているロケーションを選択してください。モバイルユーザーが存在している国ではロケーションを利用できない場合、モバイルユーザーと同じ言語を使用しているロケーションを選択してください。

  ロケーションを地理的地域で分割することもできます。すべてのロケーションを単一の地域にまとめると、その地域に対してIPアドレスプールを指定できます。プールに割り当てるIPアドレス数が限定されている場合などに、この方法が役立ちます。単一の地域IPアドレスプールを利用すると、デプロイした各地域をよりきめ細かく管理でき、ポリシーや業界の規制に応じて、地域を除外することができます。

  Prisma Access for Usersのローカル・ライセンスがあり、GlobalProtectのデプロイメントとExplicit Proxyのデプロイメントがある場合、両方の展開を合わせて最大5つの場所をデプロイできます。両方のデプロイメント間で5つの場所を割り当てる必要があります (たとえば、モバイル ユーザー用に 2 つの場所 (GlobalProtect)、モバイル ユーザー用に3つの場所 (Explicit Proxy))。Worldwide(ワールドワイド)ライセンスをお持ちの場合、場所の最大数に制限はありません。
- ポータルホスト名–ユーザー向けのPrisma Accessでは、デフォルトのドメイン名（`.gpcloudservice.com`）を使って素早く手軽にポータルのホスト名を設定できます。この場合、クラウドサービスがパブリックDNSサーバーにホスト名を自動的に公開し、証明書の生成処理を行います。しかし、ポータルのホスト名に独自の会社ドメインを使用することも可能です。会社のドメイン名を使用する場合は、サービスを設定する前にポータル用に独自の証明書を取得して、証明書を指すようにSSL/TLSサービスプロファイルを設定する必要があります。また、ポータルのホスト名で独自のドメイン名を使用する場合、DNSサーバーがポータルのDNS CNAMEを指すように設定する必要もあります。DNS CNAMEは設定プロセス中に提供されます。

 ©2025 Palo Alto Networks, Inc.

- サービス接続–モバイルユーザーに、認証サーバーなどの内部ネットワーク上のリソース（たとえば、データセンターまたは本社ロケーションの認証サーバー）にアクセスさせる場合、またはモバイルユーザーにリモートネットワークロケーションにアクセスさせる場合、サービス接続を作成、設定する必要があります。

  内部リソースへのアクセスを提供する接続を使用する予定がない場合でも、モバイルユーザーによるリモートネットワークロケーションへの接続を可能にしたい場合、または地理的に異なるエリアに存在するモバイルユーザーが相互のエンドポイントに直接アクセスする必要があるような場合、プレースホルダー値を使って最低1つのサービス接続を設定する必要があります。
- ネットワークでの**IPv6**の使用状況–攻撃面を減らすために、ネットワークのIPv6トラフィックの緩和を行うかどうかを判断します。IPv4トラフィックとIPv6トラフィックの両方を処理できるデュアルスタックエンドポイントでは、デフォルトでモバイルユーザーのIPv6トラフィックはPrisma Accessに送信されるのではなく、エンドポイントのローカルネットワークアダプタに送信されます。そのため、Palo Alto NetworksはIPv6トラフィックのシンクホールを行うように、Prisma Accessを設定することをお勧めしています。
- **GlobalProtect**エンドポイントのログ記録- GlobalProtectアプリケーションを使用するモバイル ユーザーからログを収集するには、次の2つのオプションがあります。
  - **GlobalProtect** エンドポイントからの手動ログ収集- モバイル ユーザーに、Windows、MacOS、Linux デバイス用のGlobalProtectアプリケーションからログを収集してもらいます。このオプションでは追加の構成は必要ありません。
  - トラブルシューティングのための**GlobalProtect**アプリログ収集- GlobalProtectアプリケーションがエンドツーエンドの診断テストを実行し、接続、パフォーマンス、アクセスの問題を解決し、トラブルシューティングと診断ログを生成してStrata Logging Serviceに送信し、さらに分析できるようにします。GlobalProtectアプリケーションがトラブルシューティング・ログを収集するためにStrata Logging Serviceで認証できるように、証明書を生成する必要があります。**Prisma Access (Managed by Strata Cloud Manager)**を使用すると、GlobalProtectアプリケーションを有効にして、トラブルシューティングのためにStrata Logging Serviceからログを収集することができます。**Prisma Access (Managed by Panorama)**の場合、この機能は、**Panorama** > **Cloud Services** > **Configuration** (構成) > サービス セットアップ > **GlobalProtect**アプリケーション ログ収集および**Autonomous DEM**の証明書の生成にあります。構成の詳細については、「トラブルシューティングのためのGlobalProtectアプリケーション ログ収集」を 参照してください。

- インストール後のチェックリスト：
  - パブリック**IP**アドレスをネットワークの許可リストに追加する–ロケーションをオンボーディングしたら、各ロケーションが使用する公開アドレスとIPアドレスを使用して、モバイルユーザーがSaaSやパブリックアプリケーションにアクセスできるように、これらのロケーションのIPアドレスをネットワークの許可リストに追加する必要があります。他のロケーションを追加した場合も、新しく追加したロケーションにPrisma Accessが割り当てる、新しいIPアドレスを取得する必要があります。
  - ゲートウェイ命名の一貫性- 既存のモバイル ユーザー - GlobalProtectデプロイメントがあり、組織で合併と買収 (M&A) 活動を行っている場合は、既存のゲートウェイで以前のブランド名を参照しないようにするか、新しいブランド名を参照するようにする必要がある

 ©2025 Palo Alto Networks, Inc.

可能性があります。この場合、Palo Alto Networksのアカウントチームに連絡し、SREケースをオープンして要求に対応します。Palo Alto Networksでは、この変更をメンテナンスウィンドウまたはオフピーク時間帯にスケジュールすることをお勧めします。Palo Alto Networksは、メンテナンス期間中に名前の変更が必要な、デプロイメント内のすべてのゲートウェイをアップグレードします。

GlobalProtect モバイルユーザーの設定

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

モバイルユーザーを設定する前に、必要なライセンス(Prisma Accessモバイルユーザー向けのStrata Logging Serviceライセンスと適切なファイアウォール ストレージ スペースを備えたライセンス)。モバイルユーザーが他の接続ネットワークに接続する場合は、接続に必要な企業アクセスノード（CAN）を提供するZero Trust Network Access（ZTNA）またはEnterprise Editionのいずれかのライセンスが必要です。

モバイルユーザー用にPrisma Accessを設定するには、以下のものが必要です：

- Prisma Access モバイルユーザー向けライセンス:モバイル ユーザー向けのPrisma Accessライセンスがアクティブ化されていることを確認します。
- モバイルユーザー向け IP アドレスプール:モバイル ユーザーが使用できる重複しないIPアドレス プールが1つ以上あることを確認します。
- ポータルのホスト名:ポータルの完全修飾ドメイン名 (FQDN) を把握していることを確認します。
- GlobalProtect Agent for Mobile Users: モバイルユーザー向けのPrisma Accessには、対応する各エンドポイントにGlobalProtectアプリケーションが必要です。GlobalProtectエージェントをモバイル ユーザー デバイスにインストールするためのデプロイメント戦略が必要になります。
- セキュリティ ポリシー ルール情報:Prisma Access経由のトラフィックを許可または拒否するセキュリティ ポリシールールを導入します。モバイル ユーザー向けにPrisma Accessを構成するときに、どのルールをデプロイするかを知っておく必要があります。
- モバイル ユーザーの地理的位置:モバイル ユーザーをプロビジョニングする場合は、モバイル ユーザーに近い利用可能な地理的な場所を選択する必要があります。

GlobalProtectモバイルユーザーをPrisma Accessにオンボードする方法について説明します。

- Strata Cloud Manager
- Panorama

©2025 Palo Alto Networks, Inc.

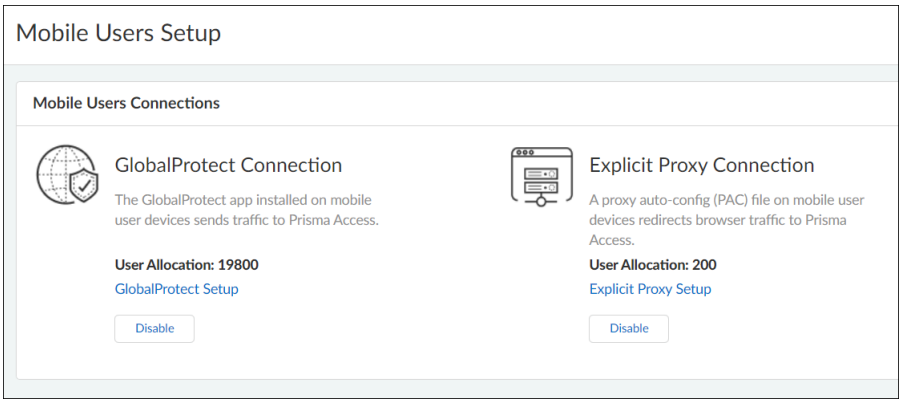
GlobalProtectモバイルユーザーの設定 (Strata Cloud Manager)

数ステップで、GlobalProtectモバイルユーザーをPrisma Accessにオンボーディングする方法は次のとおりです。

1. モバイルユーザー接続タイプとして**GlobalProtect**を有効にします

   [ワークフロー] > [**Prisma Access**セットアップ] > [モバイルユーザー]に移動します。

   モバイル ユーザー ライセンスは、GlobalProtect接続と明示型プロキシ接続の間で分割できます。一部のユーザーはGlobalProtectを介して接続でき、他のユーザーは明示型プロキシを介して接続できます。**GlobalProtect Connection**接続を使用すると、モバイルユーザーデバイスにインストールされたGlobalProtectアプリケーションがトラフィックをPrisma Accessへ送信します。

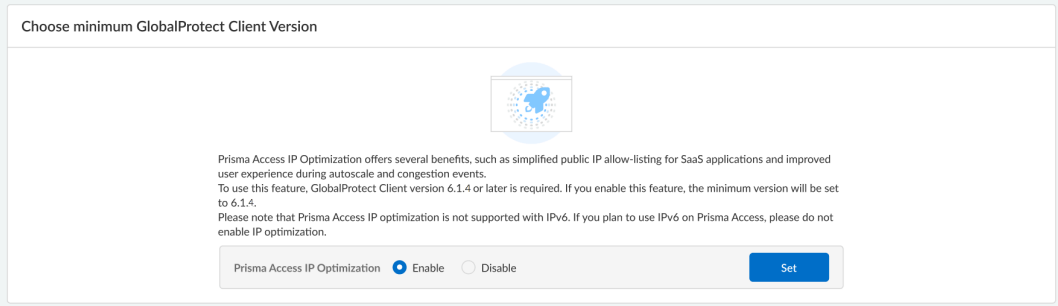


 ©2025 Palo Alto Networks, Inc.

2. インフラストラクチャの基本設定をセットアップする

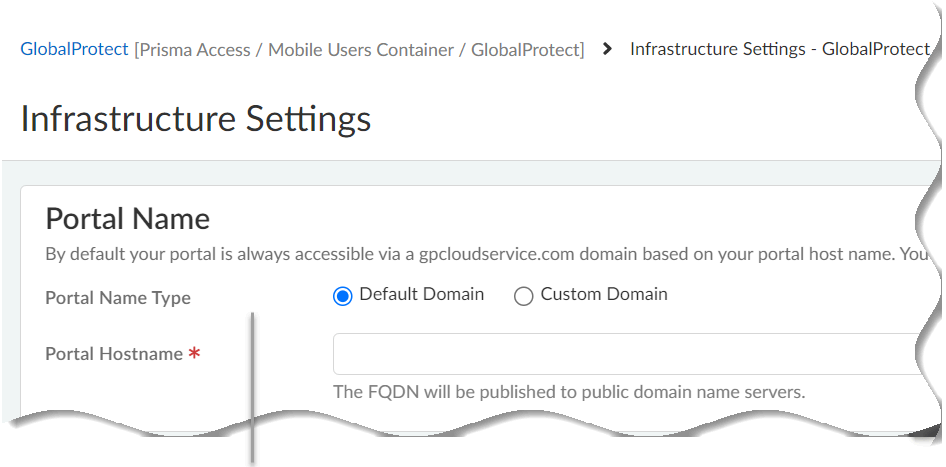
   GlobalProtectに特有のインフラ設定を構成します。最初に入力する必要があるいくつかの必須設定がありますので、Prisma Accessはモバイルユーザー環境をプロビジョニングできます。

   - *GlobalProtect*を初めてセットアップするときに、*Prisma Access*が*IP*最適化を有効にするかどうかを決定します。*IP*最適化を有効にすることを選択するには、GlobalProtectクライアントのバージョン6.1.4以降、*6.2.3*以降、または*6.3.0*以降が必要であり、*IPv6*はサポートされていません。慎重に選んでください。この設定は後で変更できません。
   - *IP*最適化は、機能的に*Prisma AccessGlobalProtect*の新規デプロイメント環境のみを対象としています。既存の*GlobalProtect*デプロイメントは、既存のマルチテナント環境から作成した新しいテナントを含め、対象外です。
   - *GlobalProtect*デプロイメントを*Prisma Access*（オンプレミスのゲートウェイとポータルの使用から）に移行する場合、この機能を有効にする前に、すべてのユーザーが*GlobalProtect*アプリケーションのバージョン*6.1.4*以降、*6.2.3*以降、または*6.3*以降を実行していることを確認してください。

   [Workflows (ワークフロー)] > **[Prisma Accessセットアップ]** > **[GlobalProtect]** > **[Infrastructure (インフラストラクチャ)]** > インフラストラクチャ設定へと移動します。

©2025 Palo Alto Networks, Inc.



GlobalProtect Infrastructure Settings

- ポータル名を指定します。
  - **Use Default Domain**（デフォルトドメインを使用）–このオプションを選択した場合、ポータルホスト名はデフォルトのドメイン名「`.gpcloudservice.com`」を使用します。この場合は、デフォルトのドメイン名に追加するポータル ホスト名を入力するだけです。 ユーザー向けPrisma Accessは必要な証明書を自動的に作成し、ホスト名をパブリックDNSサーバーに公開します。
  - カスタム ドメイン- ポータル ホスト名のドメインを会社のドメイン名 (たとえば、myportal.mydomain.com) と一致させたい場合は、ポータル アドレスをカスタマイズすることもできます。
- GlobalProtectのデプロイメントに対するクライアント**DNS**解決設定を入力します。
  - **DNS**サーバーの地域を選択します（リージョンを追加）。

    Worldwide (全世界地域)またはシアターを選択します。全世界地域とシアターの設定が混在する複数のプロキシ設定を指定した場合、Prisma Accessはロケーション グループ、シアター、全世界地域の順に設定を使用します。Prisma Accessはルールをリストの上から下に評価します。
  - Prisma Accessで 内部ドメインを解決するかどうかを選択します。解決する場合は、**1**つ以上の 内部ドメイン解決ルールを追加します 。
  - ルールの一意の名前を入力します。
  - **Prisma Access**デフォルトを選択して、デフォルトのPrisma AccessDNSサーバーを使用して内部ドメインを解決します。内部DNSサーバーに指定したドメインのみを解決させたい場合は、解決するドメインをドメインリストに入力してください。ドメインの前にアスタリスクを指定してください(例：*.acme.com)最大1,024個のドメインエントリを指定することができます。
  - 内部ドメインにアクセスできる カスタムDNSサーバーがある場合は、 プライマリ**DNS**サーバーとセカンダリ**DNS**サーバーのIPアドレスを指定します。
  - 内部DNSサーバーに、指定したドメインのみを解決させる場合は、**[Domain List**（ドメインリスト）]に解決するドメインを入力します。ドメインの前にアスタリスクを指定

©2025 Palo Alto Networks, Inc.

してください(例：*.acme.com)最大1,024個のドメインエントリを指定することができます。

- 完了したら変更を保存します。

- （任意）クライアントIPプールを指定します。

  デフォルトでは、Prisma Accessより世界中のどこでも使用できる100.127.0.0/16のデフォルトのモバイルユーザーIPアドレスプールが提供されます。各GlobalProtect接続デバイスには、このプールからIPアドレスがPrisma Accessによって割り当てられます。ここで、地域ごとにオプションでIPアドレスプールを追加できます。

  - 場所ごとに、/23 (512 IP アドレス) の最小必須サブネットを入力できます。追加するロケーションには、最低「/23」のサブネットが必要になります。Worldwideサブネットを指定した場合、最低必要なサブネットは「/23」ですが、すべてのユーザーが同時にログインしても対応できるように、ライセンスされているモバイルユーザー数以上のIPアドレスを割り当てられるように、GlobalProtectモバイル ユーザーデプロイメントのIPアドレス プールを用意することをお勧めします。

    社内で使用している他のネットワークや、Prisma Accessサービスインフラの設定(Panorama)の際に割り当てたプールと重複するアドレスを指定しないでください。また、次のIPアドレスとサブネットはPrisma Accessが内部使用のために予約しているため、使用しないでください。

    - 169.254.0.0/16
    - 100.64.0.0/10

    *RFC 1918*準拠の*IP*アドレスプールを使用することをお勧めします。*RFC 1918*非準拠の（パブリック）*IP*アドレスはモバイルユーザー向けにサポートされていますが、インターネットのパブリック*IP*アドレス空間と競合する可能性があるため、これらを使用することはお勧めできません。

- パブリック ドメインのプライマリ**DNS** とパブリック ドメインのセカンダリ**DNS**のDNS設定を指定します。

  - **Prisma Access**デフォルト - デフォルトの Prisma AccessDNS サーバーを使用します。
  - 内部 **DNS**- 内部ドメインの解決に使用するのと同じサーバーを使用します。
  - カスタム- パブリック (外部) ドメインにアクセスできるDNSサーバーがある場合は、そのフィールドにプライマリDNSサーバー アドレスを入力します。
  - クライアント**DNS**サフィックスリストを追加して、解決できない非修飾ホスト名が入力されたときに、クライアントがローカルで使用するサフィックスを指定することができます (例: acme.localなど)。ドメイン サフィックスの前にワイルドカード (*) 文字を入力しないでください (例: acme.com)。複数のサフィックスを追加できます。

3. 詳細設定をセットアップします。

   - (任意) **Static Entries (**スタティックエントリ)を使用して、FQDN を特定のIPアドレスに解決します。

     この機能は、組織内にゲスト インターネット サービスがあり、ゲストが検索エンジンを安全に使用して、会社のポリシーに違反する可能性のある不適切または不快なコンテンツ

 ©2025 Palo Alto Networks, Inc.

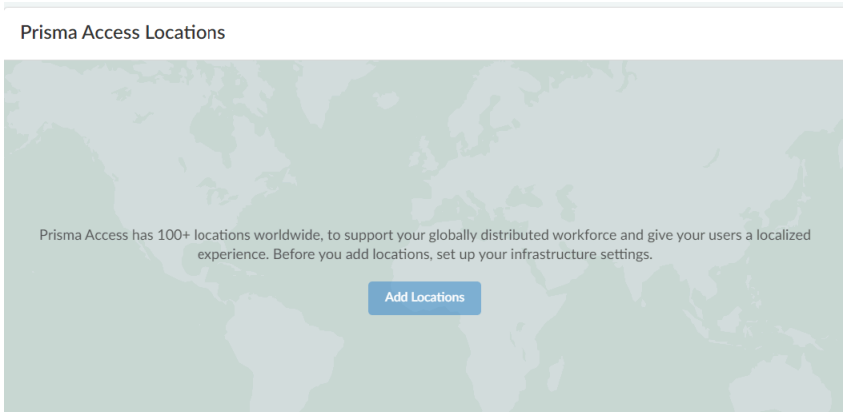
を検索しないようにしたい場合に役立ちます。これを行うには、スタティックエントリルールの一意の 名前 、**FQDN**、およびFQDN 要求を送信するIPアドレスを入力します。



- Prisma AccessにDNSリクエストをプロキシさせたい場合は、**UDP**クエリ再試行（クエリを再試行する間隔（秒）、および再試行の試行回数（秒））の値を設定する。

4. **GlobalProtect**ユーザーが接続する**Prisma Access**場所を選択する

   GlobalProtectユーザーをサポートするPrisma Accessロケーションを追加します。[ワークフロー] > **[Prisma Access**セットアップ] > **[GlobalProtect]** > インフラストラクチャ > **Prisma Access**[ロケーション]へ移動します。



   マップには、次のユーザー向けのPrisma Accessをデプロイできるグローバル地域が表示されます：さらにPrisma Accessは、各地域内に複数の場所を提供し、ユーザーがユーザーのロケールに合わせたユーザー エクスペリエンスを提供する場所に接続できるようにします。最高のパフォーマンスをお求めの場合は、[すべて選択] を選択してください。または、選択した各地域内でユーザーがアクセスする必要がある特定の場所を選択します。デプロイを1つのリージョンに制限することで、デプロイメントされたリージョンをよりきめ細かく制御し、ポリシーや業界の規制で必要なリージョンを除外できます。

   場所の数を制限する場合、最適なユーザー エクスペリエンスを実現するために、ユーザーに最も近い場所、またはユーザーと同じ国にある場所を選択してください。モバイル ユーザーが居住する国で場所が利用できない場合は、最高のパフォーマンスを得るために、ユーザーに最も近い場所を選択してください。

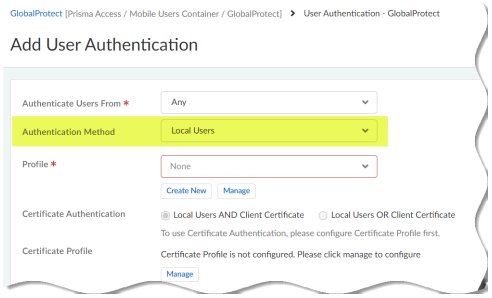
5. **GlobalProtect**ユーザーを認証する

   正当なユーザーのみがサービスやアプリケーションにアクセスできるように、ユーザー認証をセットアップします。[ワークフロー] > **[Prisma Access**セットアップ] > **[GlobalProtect]** > [インフラストラクチャ] > [ユーザー認証]へ移動します。

   セットアップをテストするために、Prisma Accessはローカルで認証するユーザーを追加することもできるし、そのままエンタープライズ レベルの認証をセットアップすることもでき

 ©2025 Palo Alto Networks, Inc.

ます。モバイルユーザーがPrisma Accessに認証できるようにする方法について詳しく学びます。



6. Prisma Accessは、デフォルトでベストプラクティスセキュリティ ポリシー ルールを適用します。これらの規則により、ユーザーは一般のインターネットサイトを安全に閲覧できます。ユーザー：

   - URLに基づいて既知の不正なウェブサイトへのアクセスをブロック
   - 悪意のあることがわかっているファイルのアップロードやダウンロードをブロック
   - 未知の未知の脅威から保護
   - マルウェア、スパイウェア（コマンド/コントロール攻撃）、脆弱性から保護

   初期設定を行った後に、これらのデフォルトルールを確認して更新し、企業のニーズを満たすことができます。

7. モバイルユーザーのロケーションがアクティブであることを確認します。

   初期設定をPrisma Accessにプッシュすると、Prisma AccessはGlobalProtectモバイル ユーザー環境のプロビジョニングを開始します。これには最大15分かかる場合があります。

   *[ワークフロー] > [Prisma Accessセットアップ] > Prisma Access > [インフラストラクチャ設定]*を選択し、インフラストラクチャ設定を編集して、プロビジョニングした各ロケーションにゲートウェイが設定されていることを確認することで、セットアップを検証することもできます。

GlobalProtect — ポータルアドレスをカスタマイズ

Prisma Accessはモバイルユーザーの環境をプロビジョニングするために必要な最小限の設定のみが必要ですので、それをテストできます。ポータルアドレスに会社のドメインを使用したい場合は、初期環境設定後にアドレスを変更できます。

デフォルトでは、Prisma Accessはモバイルユーザーがインターネットおよび本社やデータセンターへの安全なアクセスのために接続する必要があるPrisma Accessポータルアドレスを設定するために、*gpcloudservice.com*ドメインを使用します。環境を最初に設定してテストする際には、このデフォルトドメインを使用する必要があります。初期設定後にドメイン名をカスタマイズして会社のドメインを使用したい場合は、環境設定に戻って編集することができます。これにより、ユーザーが接続するポータルアドレスに自社のドメイン（例：prisma-access.acme.com）が含まれるようになります。

*.gpcloudservice.com ドメインは *Palo Alto Networks* アプリケーションに関連付けられています。

©2025 Palo Alto Networks, Inc.

独自のドメインをPrisma Accessが使用するように設定するには、次のことを行う必要があります:

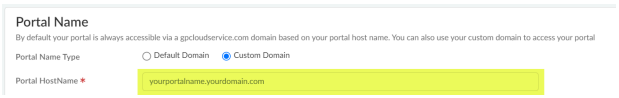
- サービスの証明書を取得します。
- DNSサーバーにCNAMEエントリを作成し、デフォルトのドメインを使用してデフォルトのポータルアドレスをカスタムポータルアドレスにマッピングします。この作業を行う必要があるのは、Prisma Accessが初期プロビジョニング中に設定したポータルアドレスを公開ドメインサーバーに公開するためです。

STEP 1 | **[Workflows (ワークフロー)]** > **[Prisma Accessセットアップ]** > **[GlobalProtect]** > **[Infrastructure (インフラストラクチャ)]**へと移動し、 インフラストラクチャ設定を選択します。

*Strata Cloud Manager*では、ポータルやゲートウェイとサービス接続の間でネットワーク冗長性がデフォルトで有効になっており、モバイルユーザーがアクセス可能なサービスやアプリケーションに対して冗長な接続を確保しています。

STEP 2 | ポータル名タイプをカスタムドメインに設定します。

STEP 3 | 使用したいポータルホスト名を入力してください。



STEP 4 | DNSサーバエントリをマップするポータル**DNS CNAME**を追加します。

STEP 5 | カスタムドメインポータルアドレスにプロビジョニングした証明書をインポートします。

1. インポートする証明書の形式を選択します：
   - **[Encrypted Private Key and Certificate (PKCS12) (暗号化された秘密鍵と証明書（PKCS12）)]** –キーおよび証明書が単一のコンテナ(証明書ファイル)に格納されています。[ファイルの選択]をクリックし、インポートするPKCS12ファイルを参照します。
   - **[Base64 Encoded Certificate (PEM) Base64 (エンコード済み証明書（PEM）)]** – このオプションを選択した場合、証明書とは別にキーファイルをインポートする必要があります。PEM 証明書とキーファイルをインポートするには、［ファイルの選択］をクリックします。
2. 鍵を暗号化するパスフレーズとパスフレーズの確認を入力し、保存をクリックします。

STEP 6 | まだ行っていない場合は、DNSサーバーを設定して、定義したPrisma AccessDNS CNAMEを指すようにしてください。

STEP 7 | 環境設定を保存し、Prisma Accessに設定をプッシュします。

明示型プロキシと**GlobalProtect**の設定スコープの両方を選択してください。

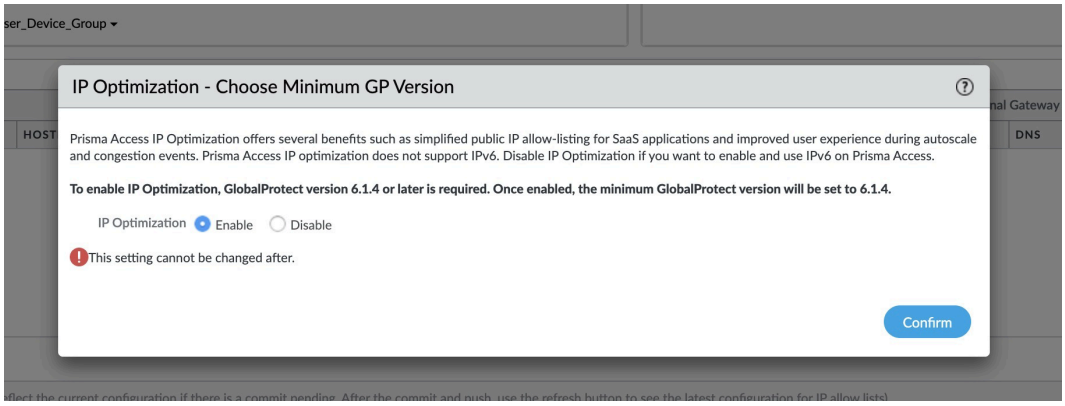
©2025 Palo Alto Networks, Inc.

GlobalProtectモバイルユーザーの設定 (Panorama)

モバイル ユーザー - GlobalProtectデプロイメントを構成するには、次の手順を実行します。開始する前に、Prisma Accessがどのように機能するかを理解し、チェックリストを使用してGlobalProtect のデプロイメントを計画してください。

STEP 1 | **[Panorama]** > [クラウド サービス] > **[Configuration (設定)]** > [モバイル ユーザー - **GlobalProtect]**を選択します。

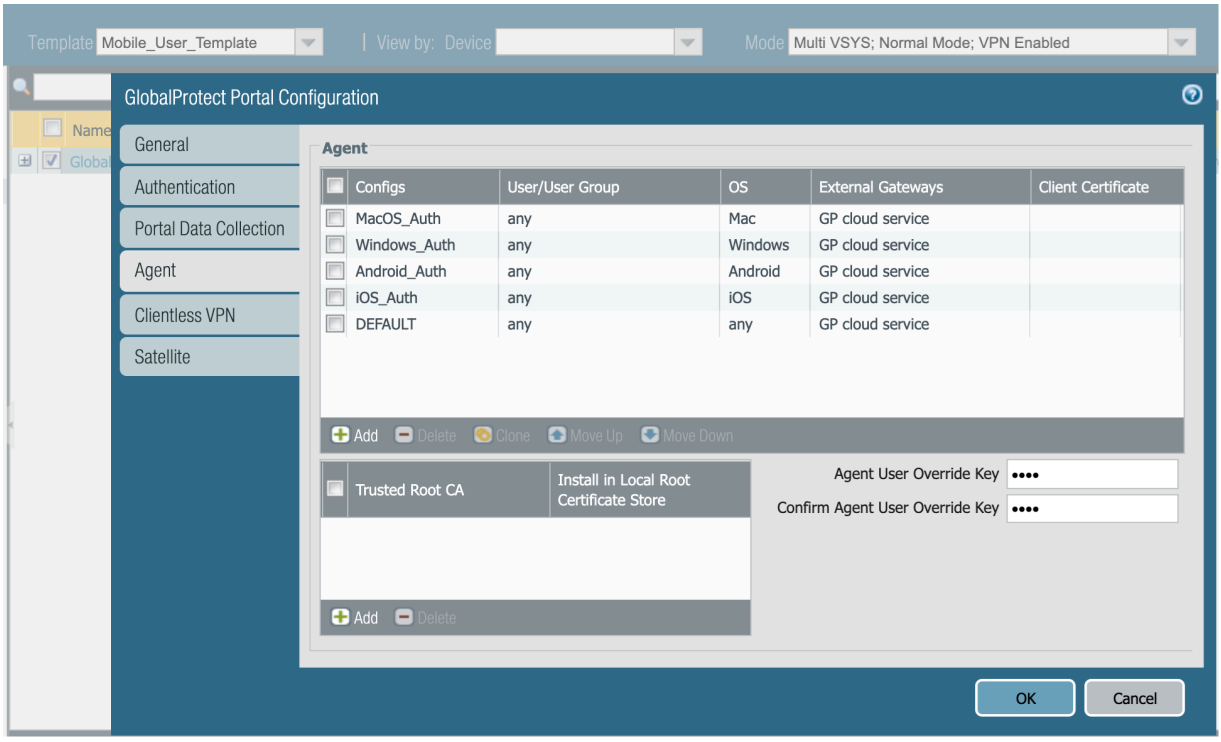
- *GlobalProtect*を初めてセットアップするときに、*Prisma Access*IP最適化を有効にするかどうかを尋ねられます。IP最適化を有効にすることを選択するには、GlobalProtectクライアントのバージョン6.1.4以降、*6.2.3*以降、または*6.3.0*以降が必要であり、*IPv6*はサポートされていません。慎重に選んでください。この設定は後で変更できません。
- IP最適化は、機能的に*Prisma Access*GlobalProtectの新規デプロイメント環境のみを対象としています。既存のGlobalProtectデプロイメントは、既存のマルチテナント環境から作成した新しいテナントを含め、対象外です。
- *GlobalProtect*デプロイメントを*Prisma Access*（オンプレミスのゲートウェイとポータルの使用から）に移行する場合、この機能を有効にする前に、すべてのユーザーが*GlobalProtect*アプリケーションのバージョン*6.1.4*以降、*6.2.3*以降、または*6.3*以降を実行していることを確認してください。



STEP 2 | （任意）Prisma Accessがクライアントにプッシュするエージェント構成をカスタマイズしたい場合は、Mobile_User_Template内のGlobalProtectポータル構成を編集して、新しいエージェント構成を追加します。エージェントを設定した後、その設定がデフォルト

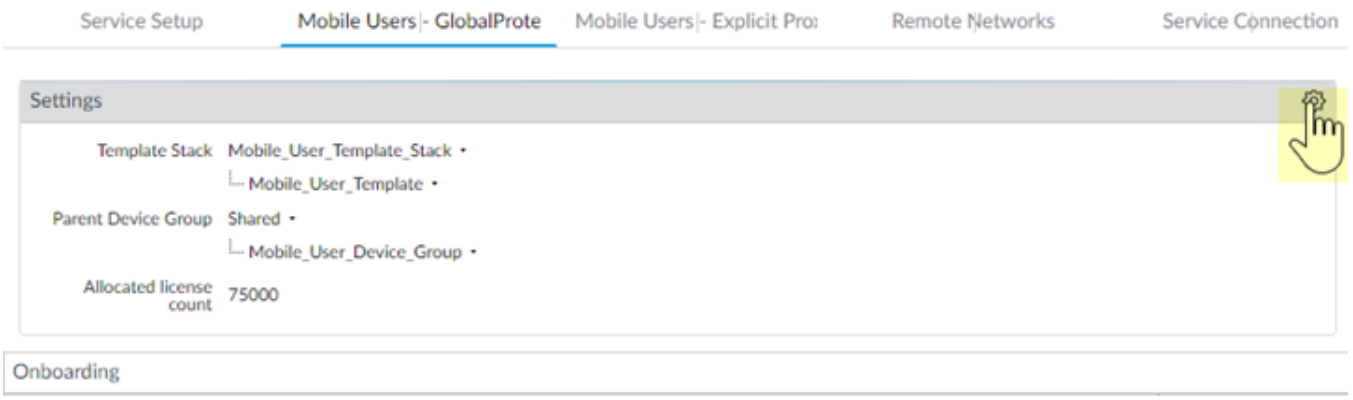
©2025 Palo Alto Networks, Inc.

設定に優先するように、それをテンプレートに事前定義されているDEFAULT（デフォルト）のエージェント設定の上に移動します。このテンプレートを編集する際には、External Gateway（外部ゲートウェイ）エントリを削除または変更しないでください。



STEP 3 | クラウド サービスがポータルとゲートウェイにプッシュするデバイス グループ階層を構成します。

1. **Settings**（設定）を編集します。



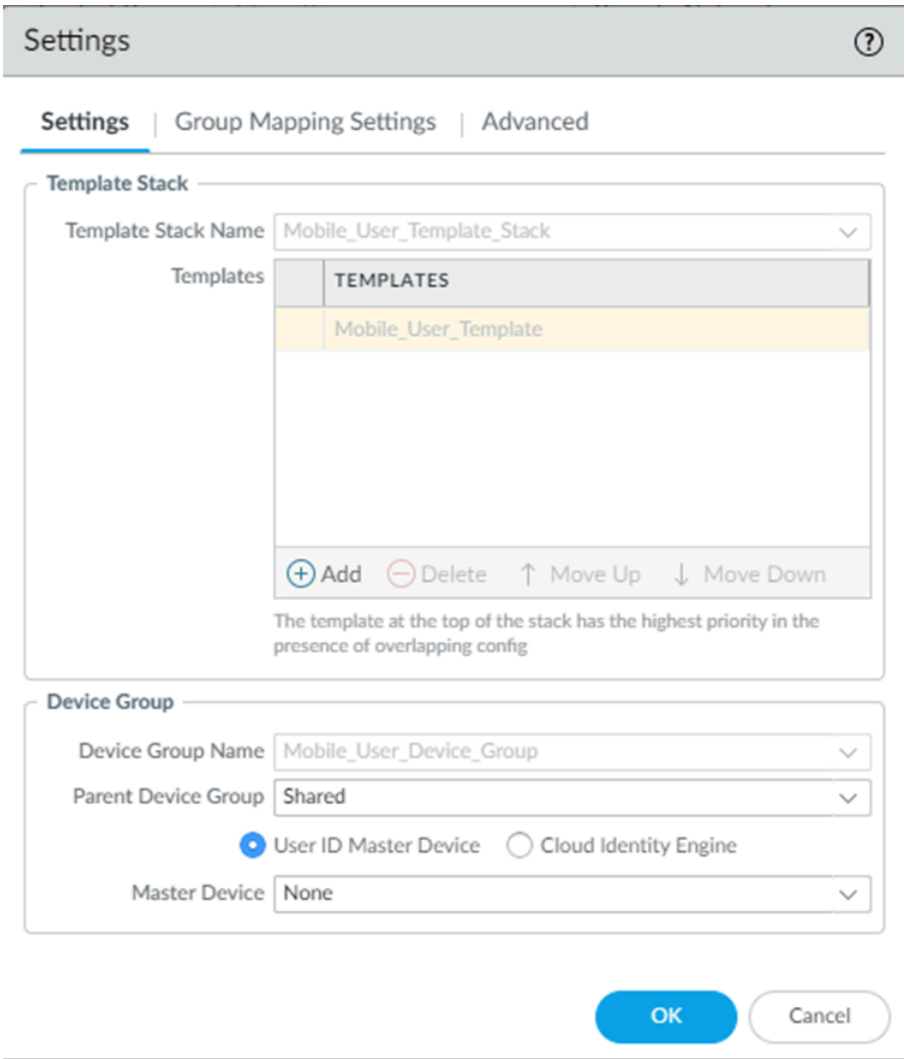
2. デバイスグループセクションで、ユーザー向けPrisma Accessにプッシュするコンフィギュレーション設定を含む親デバイスグループを選択するか、Prisma Accessデバイス

 ©2025 Palo Alto Networks, Inc.

グループの共有階層を使用するために親デバイスグループを**Shared (**共有**)**のままにします。

アドレスグループ、セキュリティポリシー、セキュリティプロファイル、および他のポリシーオブジェクト（アプリケーショングループとオブジェクトなど）、HIPオブジェクトとプロファイル、および認証ポリシーを含め、Prisma Access for usersがここで指定するデバイスグループ階層を使って、モバイルユーザーに一貫したポリシーを適用するために必要な、すべての設定をプッシュします。また、デバイスグループ内の**Panorama/Logging Service**に目的のログタイプを転送する、ログ転送プロファイルを設定していることを確認してください。転送されたログは、Prisma Access for usersにプッシュされます。これは、クラウドサービスがどのログをStrata Logging Serviceに送信するのかを知るための唯一の手段となります。

3. (任意) 次世代ファイアウォールをマスター デバイスとして構成した場合、またはCloud Identity Engineプロファイルを追加して、セキュリティ ポリシーでユーザーとグループの情報を選択できるようにした場合は、**User-ID** マスター デバイスまたは**Cloud Identity Engine**を選択し、作成したマスター デバイスまたはCloud Identity Engineプロファイルのいずれかを選択します。



©2025 Palo Alto Networks, Inc.

STEP 4 | （任意） ユーザーおよびグループ情報を取得するために、Cloud Identity Engine (クラウドIDエンジン)の Directory Sync コンポーネントを使用するようにPrisma Accessを構成します。

Prisma Access **Group Mapping Settings (**グループ マッピング設定**)** でDirectory Sync統合を有効にして構成する前に、Cloud Identity Engine の Directory Sync コンポーネントを構成して、クラウド ディレクトリまたはActive Directory (アクティブディレクトリ - AD)からユーザーおよびグループ情報を取得する必要があります。

STEP 5 | **OK**をクリックして、モバイルユーザー設定を保存します。

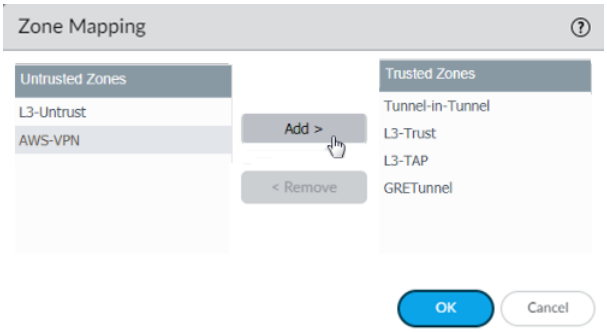
STEP 6 | テンプレートスタック内に設定されているゾーンを、TrustedまたはUntrustedとしてマップします。

Palo Alto Networks次世代ファイアウォール上で、セキュリティポリシーはファイアウォールの物理/仮想インターフェイスにマップされているゾーン間で適用されています。ただし、Prisma Access for usersでは、ネットワーキングインフラが自動的に設定されるため、インターフェイスを設定してそれをゾーンと関連付ける必要はありません。ただし、一貫したセキュリティポリシーを適用するために、組織内で使用するゾーンをTrustまたはUntrustとしてマップして、クラウドサービスからネットワークインフラ内の内部ゾーンにプッシュするポリシールールを、Prisma Access for usersが解釈できるようにする必要があります。

1. ゾーンマッピング設定を編集します。

   デフォルトでは、Mobile_User_Template_Stack内のすべてのゾーンが、Untrusted Zones（信頼しないゾーン）として分類されます。

2. Trustedと指定する各ゾーンを選択して、**Add**（追加）をクリックし、それを**Trusted Zones**（信頼するゾーン）のリストに追加します。



3. **OK** をクリックして変更内容を保存します。

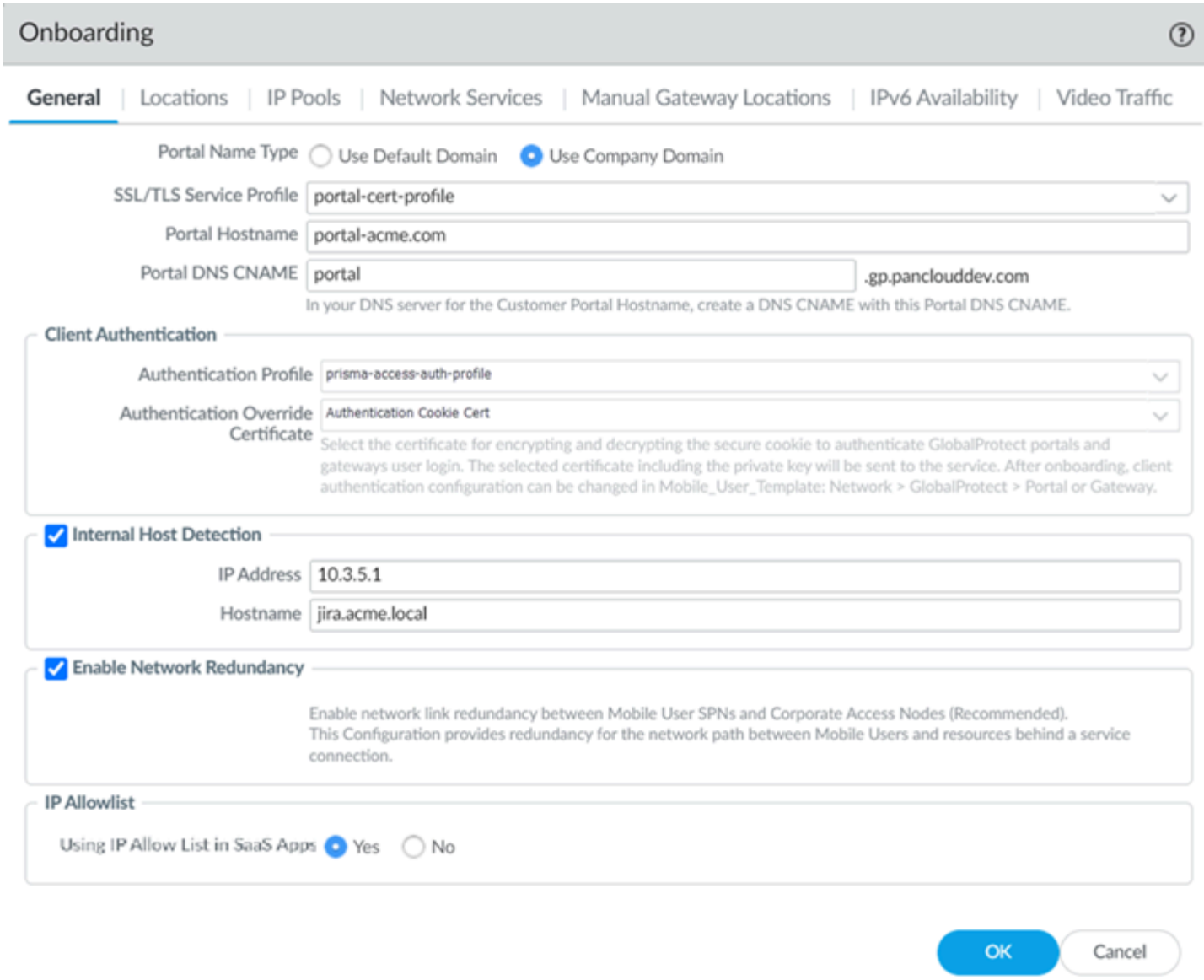
STEP 7 | GlobalProtectポータルと外部ゲートウェイを設定します。

Prisma Accessゲートウェイは、外部ゲートウェイとしてのみ設定できます。内部ゲートウェイとして設定することはできません。

1. Onboarding（オンボーディング）セクションで**Add**（追加）をクリックします。
2. **General**（全般）タブで、**Portal Name Type**（ポータル名タイプ）を指定します。
   - **Use Default Domain**（デフォルトドメインを使用）–このオプションを選択した場合、ポータルホスト名はデフォルトのドメイン名「`.gpcloudservice.com`」を使用します。この場合は、デフォルトのドメイン名に追加するポータル ホスト名を入

 ©2025 Palo Alto Networks, Inc.

力するだけです。 ユーザー向けPrisma Accessは必要な証明書を自動的に作成し、ホスト名をパブリックDNSサーバーに公開します。



すでに既存のポータル名を持つGlobalProtectデプロイメント環境が存在しており、そのポータル名を引き続き使用したい場合は、Prisma Accessポータル名を既存のポータル名にマップするCNAMEを追加します。たとえば、既存のポータル名named portal.acme.comが存在しており、Prisma Accessポータルをこの同じ名前にマップしたい場合は、既存のポータル用にDNSエントリにgpcs2.gpcloudservice.comのCNAMEを追加します。

*.gpcloudservice.com ドメインは *Palo Alto Networks* アプリケーションに関連付けられています。

- **Use Company Domain**（会社のドメインを使用）–ポータルホスト名のドメインを会社のドメイン名（例：myportal.mydomain.com）と一致させる場合に、このオプションを選択します。このオプションを使用する場合、まず独自の証明書

©2025 Palo Alto Networks, Inc.

を入手して、それを指すようにSSL/TLSサービスプロファイルを設定する必要があります。次に、**SSL/TLS Service Profile**（**SSL/TLS**サービスプロファイル）を選択して、**Portal Hostname**（ポータルホスト名）を入力することで、ポータル名を設定することができます。このオプションを使用する場合、内部DNSサーバーが、`.gpcloudservice.com`を持つポータルのホスト名である、**Portal DNS CNAME**（ポータル**DNS CNAME**）を指すようにする必要があります。たとえば、DNSホスト名acme-portal.acme.comを指定した場合、そのホスト名をacme-portal.gpcloudservice.comにマップするDNS CNAMEエントリを、内部DNSサーバー上に作成する必要があります。

新しい証明書をアップロードする必要がある場合は、 証明書と秘密鍵をインポートし、使用されている*SSL/TLS*サービスを表示します。 *Prisma Access [*ネットワーク*] > [GlobalProtect* > ポータル*] > [GlobalProtect_Portal* > 認証*]* の順に選択し、***SSL/TLS*** サービス プロファイル名を確認します。このフィールドは、デフォルトのドメインではなく会社のドメインを使用している場合にのみ表示されます。次に、*[*デバイス > 証明書管理 > ***SSL/TLS*** 証明書プロファイル*]* を選択し、ポータルで使用される *SSL/TLS* プロファイル内の証明書を、インポートした証明書に置き換えることができます。

3. Prisma Accessがモバイルユーザを認証する方法を指定する認証プロファイルを選択するか、新しいプロファイルを作成します。

   認証プロファイル設定を含んでいる親デバイスグループを追加した場合、利用可能なプロファイルのリストにそれが表示されます。デバイスグループにプロファイルをプッシュしなかった場合、ここで認証プロファイルを作成することができます。

   変更をコミットしてプッシュすると、この領域の認証プロファイルと認証オーバーライド証明書に変更を加えることはできなくなり、選択肢は読み取り専用になります。最初のオンボーディング後に変更を加えるには、***Mobile_User_Template***の下にある *1* つ以上の *GlobalProtect* クライアント認証構成を 変更または追加します。

4. モバイルユーザーがポータルとゲートウェイの認証に利用する、保護されたcookieを暗号化する、**Authentication Override Certificate**（認証優先証明書）を選択します。

   認証cookieの暗号化に使用する証明書を含んでいる親デバイスグループを追加した場合、利用可能な証明書のリストにそれが表示されます。デバイスグループに証明書をプッシュしなかった場合、ここでインポートまたは作成することができます。

5. (任意) モバイル ユーザーがサービス接続からアクセス可能なサービスおよびアプリケーションに常にアクセスできるようにするには、ポータルまたはゲートウェイとサービス接続間の ネットワーク冗長性を有効にします 。

   この機能により、モバイル ユーザー データプレーンと異なるコンピューティング場所のサービス接続の間に冗長ネットワーク パスが提供されます。冗長性を有効にすると、ユーザーはデータ センターまたは本社のサービス接続の背後にあるリソースに、より回復力のあるアクセスを提供できます。モバイル ユーザーがリモート ネットワークのリソースにアクセスするにはサービス接続が必要であるため、ユーザーはリモート ネットワークの場所にあるリソースにアクセスする際の回復力も向上します。

 ©2025 Palo Alto Networks, Inc.

6. （任意） 内部ネットワーク上にある時、GlobalProtectエンドポイントにトンネル接続が不要な場合は、**Internal Host Detection**（内部ホスト検出）を有効にします。

   1. [内部ホスト検出] チェック ボックスをオンにします。
   2. **IP Address**（IPアドレス）に、内部ネットワークからのみ到達できるホストのIPアドレスを入力します。
   3. 入力したIPアドレス用のDNS **Hostname**（ホスト名）を入力します。接続を試みるクライアントは、指定されたアドレスでリバースDNSルックアップを試みます。ルックアップが失敗した場合は、クライアントがPrisma Access for usersへのトンネル接続が必要かどうかを判断します。

   *Prisma Access*は、ここで指定した内部ホスト検出設定を 、GlobalProtect ポータル構成 (***[Network (ネットワーク)]*** > ***[GlobalProtect]*** > ***[Portals (ポータル)]*** > ***<portal-config>*** > ***[Agent (エージェント)]*** > ***[DEFAULT (デフォルト)]*** > ***[Internal (インターナル)]***) のデフォルト エージェント設定にコピーします。*GlobalProtect*ポータルでデフォルト エージェントの内部ホスト検出設定を入力した場合、ここでオプションを変更することはできず、ポータルで変更する必要があります。複数のエージェント設定が必要な場合は、*GlobalProtect*ポータルでデフォルトのエージェント設定を入力し、その設定を *Prisma Access*を選択し、 ***[Network (ネットワーク)]*** > ***[GlobalProtect]*** > ***[Portals (ポータル)]*** > ***<portal-config>*** > ***[Agent (エージェント)]*** を選択して、デフォルト以外の構成 を追加し 、デプロイメントの他の部分でその構成を指定します。

7. (任意) 組織が許可リストを使用してパブリック アプリケーションまたは SaaS アプリケーションへのアクセスを制御する場合は、**SaaS** アプリで **IP** 許可リストを使用するかどうかを指定します。

   GlobalProtectのパブリック(出口)IPアドレスを追加するには、以下の手順に従います。–組織内で使用する任意のSaaSアプリケーション許可リストにモバイル ユーザーをデプロイすると、Prisma AccessによってIPアドレスが提供され、環境内で使用する前に許可リストに追加されていることを確認できます。既存のデプロイメントと新しいデプロイメントの両方について、Prisma Access出口IPアドレスのリスティングを許可するように実装できます。

8. (任意)[ネットワーク] > **[GlobalProtect]** > [ポータル] > **[GlobalProtect_Portal** > エージェント]を選択し、カスタマイズする構成を選択するか、[デフォルト]、[アプリ]の順に選択して、GlobalProtect アプリの設定をカスタマイズします (たとえば、GlobalProtect が使用する接続方法を指定します)。

STEP 8 | モバイルユーザーをデプロイする**Locations**（ロケーション）、およびそれらのロケーションに関連する地域を選択します。

Locations（ロケーション）タブにはマップが表示されます。マップを強調表示すると、グローバルな地域（Americas（アメリカ）、Europe（欧州）、およびAsia Pacific（アジア太平洋））および各地域内で利用できるロケーションが表示されます。地域を選択して、次に各地域で展開するロケーションを選択します。単一の地域に展開を限定すると、展開した地域をよりきめ細かく管理でき、ポリシーや業界の規制によって、必要な地域を除外することが

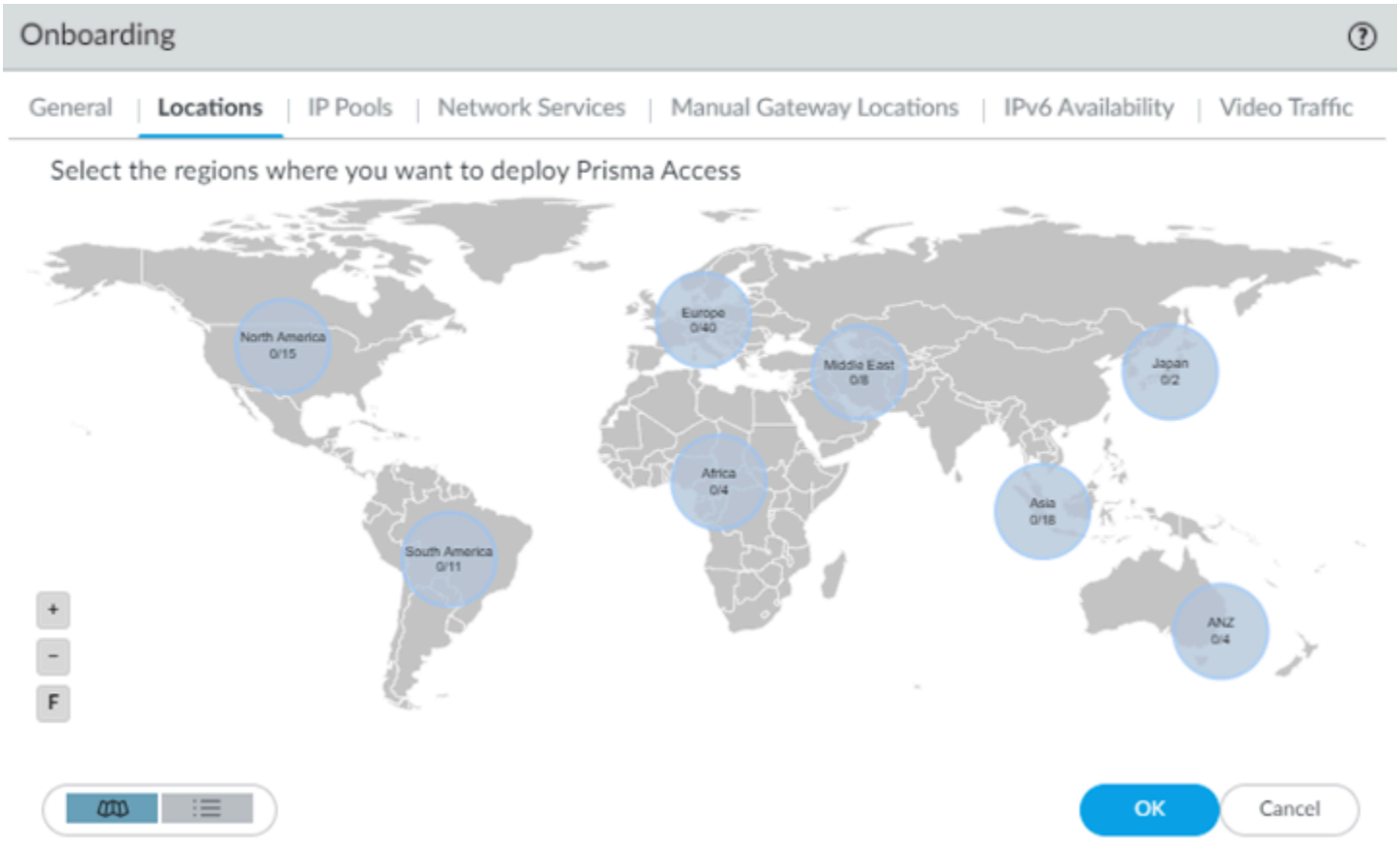
 ©2025 Palo Alto Networks, Inc.

できます。モバイルユーザーにもっとも近い地域内のロケーションを選択するか、または自社のポリシーや業界規制の要件を満たすロケーションを選択することができます。

他のロケーションが利用できない場合は、*Prisma Access*によってモバイルユーザーのフォールバックロケーションとして*Hong Kong*（香港）、*Netherlands Central*（オランダ中央部）、および*US Northwest*（米国北西部）が使用されます。そのため、モバイルユーザーのオンボーディング時には、これらのロケーションの中から最低*1*つは有効にしておくことを強くお勧めします。

2 つのアスタリスクで示される場所は、 ローカル ゾーンです。このような立地は、コンピュート、ストレージ、データベース、インフラストラクチャー サービスを人口や産業の中心地の近くに配置することになりますが、いくつかの制限もあります。ローカル ゾーンを追加するには、Palo Alto Networksの担当者にお問い合わせください。

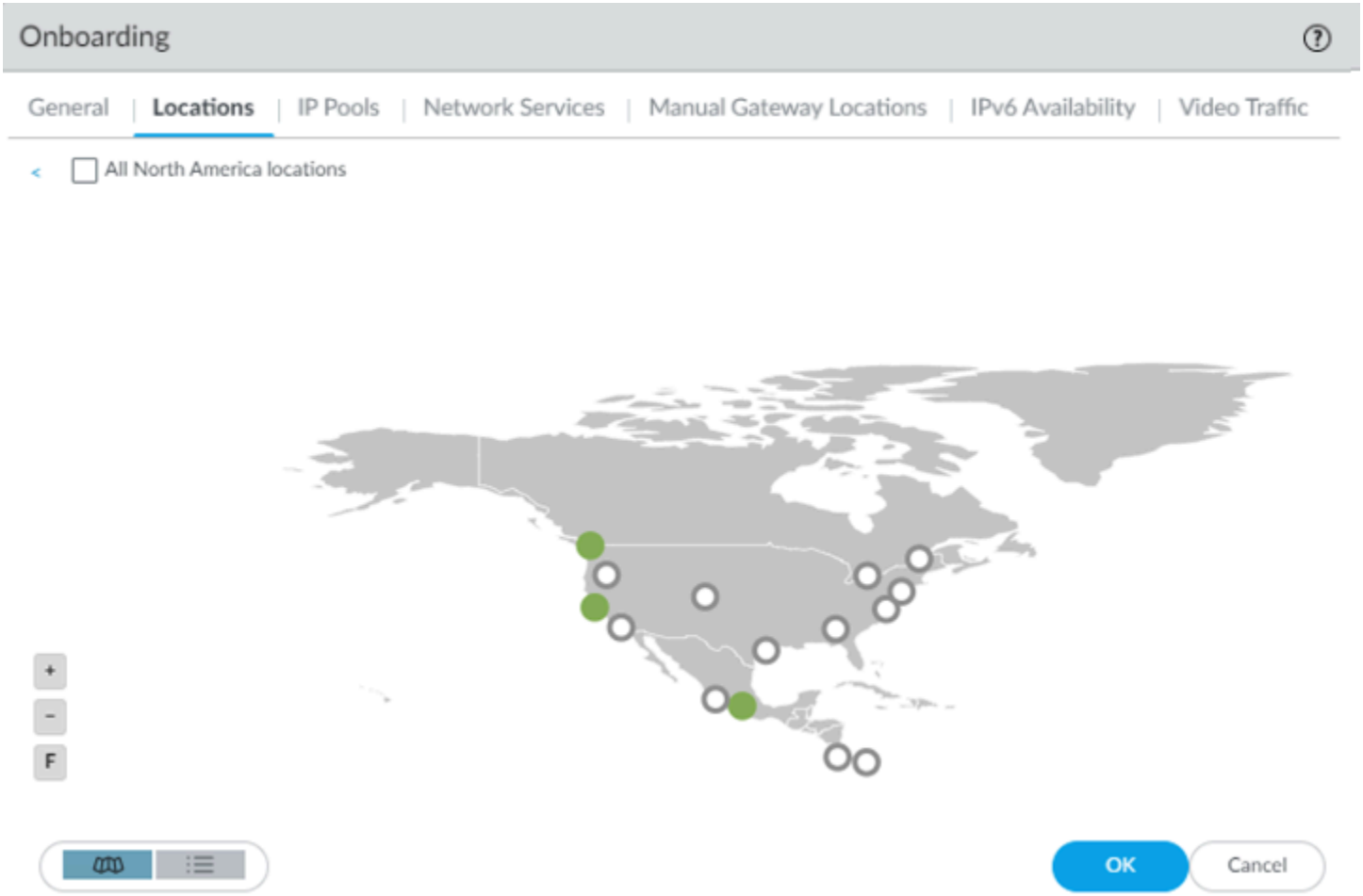
1. **Locations**（ロケーション）タブをクリックして、リージョンを選択します。



 ©2025 Palo Alto Networks, Inc.

2. マップを使って、選択したリージョン内のPrisma Accessゲートウェイを1つまたは複数選択します。

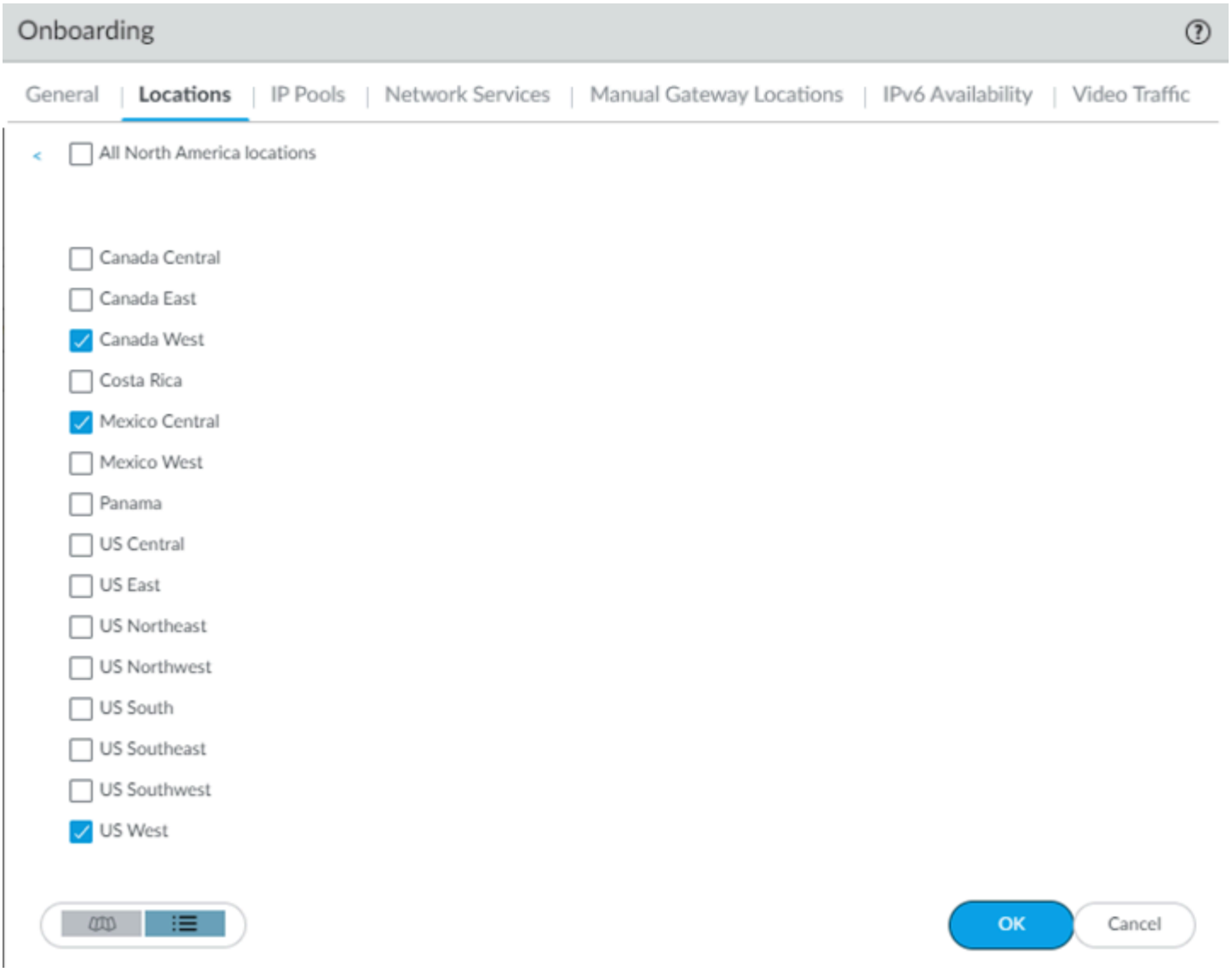
   ロケーション上にカーソルを移動すると、それが強調表示されます。白の円は利用可能なロケーションを、緑の円はそのロケーションが選択されていることを表しています。



   マップビューのほかに、地域とロケーションのリストを表示することができます。左下から、マップビューとリストビューを切り替えられます。リストビューのリストは、地

©2025 Palo Alto Networks, Inc.

域が列でソートされ、すべてのロケーションを地域別にソートされています。リージョン内の**All**（すべて）のサイトを選択できます（ダイアログ上部）。



STEP 9 | **IP Pools**（IPプール）タブを選択して、**Add**（追加）をクリックし、IPアドレスプールを選択して、GlobalProtectエンドポイントへのIPアドレスの割り当てに使用する、IPアドレスプールをセットアップします。

1. IP アドレス プールの リージョン を指定します。

   世界全域のすべてのGlobalProtectエンドポイントに単一のIPアドレス プールを使用することも、モバイル ユーザーがいるシアターごとに個別のプールを使用することも、ロケーション グループ (シアターよりも小さいロケーションのグループ) ごとにプールを指定することもできます。また、世界全域、シアターごと、または場所グループごとのIPプールの組み合わせを指定することもできます。たとえば、特定の場所のグループ

 ©2025 Palo Alto Networks, Inc.

用のプールを追加してから、他のすべての場所で使用する世界全域プールを追加できます。

ユーザーの詳細（位置情報ベースのサービスやユーザーグループまたは機能に基づくサービスなど）を特定するために、ユーザーのソースIPアドレスに依存するサービスがある場合は、ロケーショングループ固有のIPアドレスプールを使用してください。これにより、アクセス制御ポリシーを適用したり、異なるコンピューティングリージョンにある国々に対してルーティングやポリシー操作を実行したりできます。たとえば、異なる コンピューティングロケーションにあるカナダとブラジルに別々のIPアドレス プールを使用して、個別のアクセスおよびセキュリティ制御を提供できます。

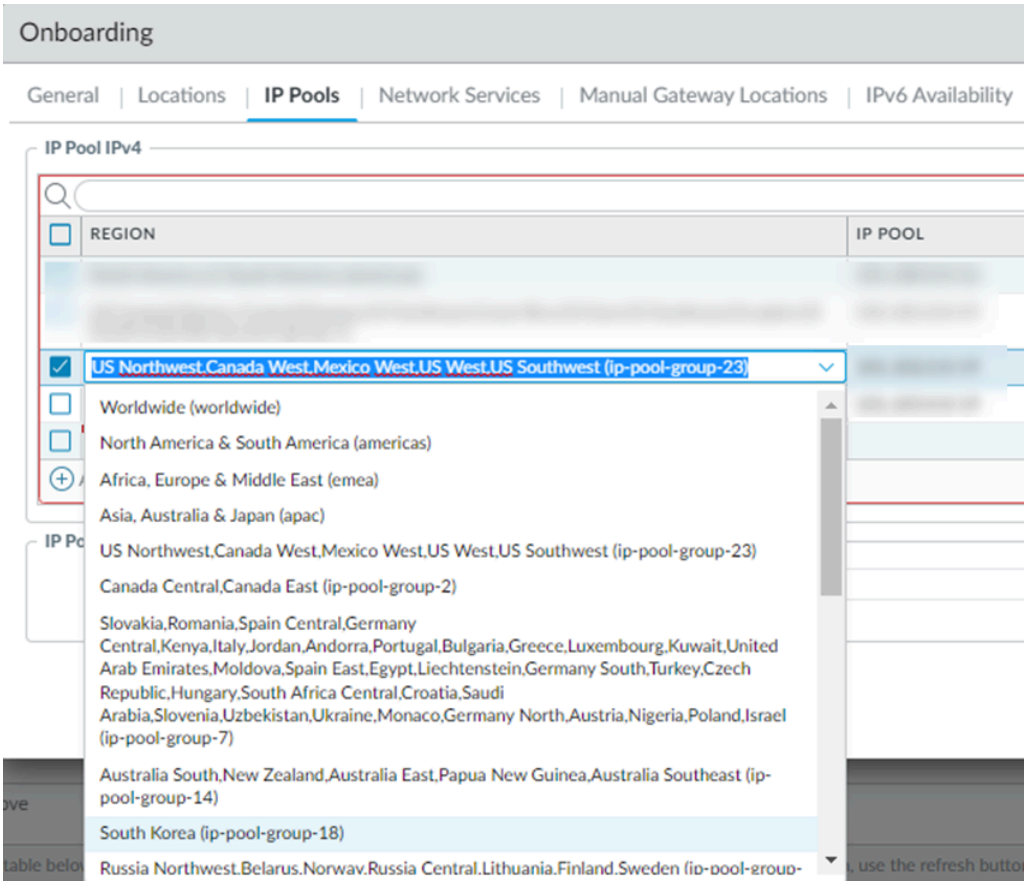
ロケーション グループ固有の*IP*アドレス プールを使用するには、世界全域またはシアター固有のプールも指定する必要があります。

GlobalProtectモバイルユーザーは、まずロケーション グループ内のIPアドレスを使用し、次にシアター固有のIPアドレス、最後に世界全域IPアドレスを使用します。たとえば、ロケーション グループと世界全域のプールを指定し、ロケーション グループ プールで使用可能な IP アドレスを使い果たした場合、Prisma Accessは **Worldwide (**世界全域**)** プールからIPアドレスを取得して、そのロケーション グループで使用します。

- すべての GlobalProtect モバイル ユーザーが使用できる IP プールを指定するには、**[Worldwide (**世界地域**)]**を選択します。
- 特定のシアターでGlobalProtectユーザーが使用できるIPプールを指定するには、シアターを選択してください。

©2025 Palo Alto Networks, Inc.

- ロケーション グループに固有のIPプールを指定するには、リストから選択します。



2. 選択したリージョン内のエンドポイントに割り当てる **IP** プール を入力します。

   - 場所ごとに、/23 (512 IP アドレス) の最小必須サブネットを入力できます。追加するロケーションには、最低「/23」のサブネットが必要になります。Worldwideサブネットを指定した場合、最低必要なサブネットは「/23」ですが、すべてのユーザーが同時にログインしても対応できるように、ライセンスされているモバイルユーザー数以上のIPアドレスを割り当てられるように、GlobalProtectモバイル ユーザー デプロイメントのIPアドレス プールを用意することをお勧めします。

     社内で使用している他のネットワークや、Prisma Accessサービスインフラの設定 (Panorama)の際に割り当てたプールと重複するアドレスを指定しないでください。また、次のIPアドレスとサブネットはPrisma Accessが内部使用のために予約しているため、使用しないでください。

     - 169.254.0.0/16
     - 100.64.0.0/10

     *RFC 1918*準拠の*IP*アドレスプールを使用することをお勧めします。*RFC 1918*非準拠の（パブリック）*IP*アドレスはモバイルユーザー向けにサポートされていますが、インターネットのパブリック*IP*アドレス空間と競合する可能性があるため、これらを使用することはお勧めできません。

©2025 Palo Alto Networks, Inc.

STEP 10 | 内部ドメインと外部 (パブリック) ドメインの DNS 解決設定 を指定するには、[ネットワーク サービス] タブを選択し、設定を追加します。

アクティブなトンネル接続を持つGlobalProtectエンドポイントは、物理的なネットワークアダプタではなく、仮想ネットワークアダプタを使用するため、個別のDNS解決設定が必要になります。

ネットワーク サービス ウィンドウでネットワーク設定を構成します。

- ドロップダウンからリージョンを選択します。

  DNS 設定をグローバルに適用するには、**[Worldwide (全世界)]**を選択するか、シアターを選択するか、場所のグループを選択します。全世界地域、シアターおよびロケーショングループ特有の設定が混在する複数のプロキシ設定を指定した場合、Prisma Accessはロケーション グループ、シアター、全世界地域の順に設定を使用します。Prisma Accessはルールをリストの上から下に評価します。
- 内部ドメインのDNS 設定を構成するルールを1つ以上追加します。
  - ルールの一意のルール名を入力します。
  - Prisma Accessの内部ルーティングの問題が発生する可能性があるため、127.0.0.1アドレスを入力しないでください。
  - 内部DNSサーバーに、指定したドメインのみを解決させる場合は、**Domain List**（ドメインリスト）に解決するドメインを入力します。ドメインの前にアスタリスクを指定します (例:*.acme.com)。最大1,024個のドメインエントリを指定することができます。

    Prisma Accessは、Cloud Default サーバーを使用して **.amazonaws.com*、**.aws.amazon.com*、**.googleapis.com*、および **.google.internal* ドメインを解決するための定義済みルールがあります。内部 *DNS* サーバーでより具体的なドメイン *(*たとえば、**.amazonaws.com* ではなく **.s3.amazonaws.com)* を解決する場合は、 ドメイン リストに *URL* を入力します。 *Prisma Access*はドメイン名を最長から最短の順に、次にリストの上から下の順に評価します。
  - 内部ドメインにアクセスできるカスタム**DNS**サーバーがある場合は、プライマリ**DNS**サーバーとセカンダリ**DNS**サーバーのIPアドレスを指定するか、**[Use Cloud Default (クラウドデフォルトを使用)]**を選択してデフォルトのPrisma AccessDNSサーバーを使用します。
- パブリックドメインのDNS 設定を指定します。
  - クラウドのデフォルトを使用する- デフォルトを使用するPrisma AccessDNS サーバー。
  - **Same as Internal Domains (内部ドメインと同じ)**-内部ドメインの解決に使用するのと同じサーバーを使用する。このオプションを選択すると、パブリックドメインの解決に使

 ©2025 Palo Alto Networks, Inc.

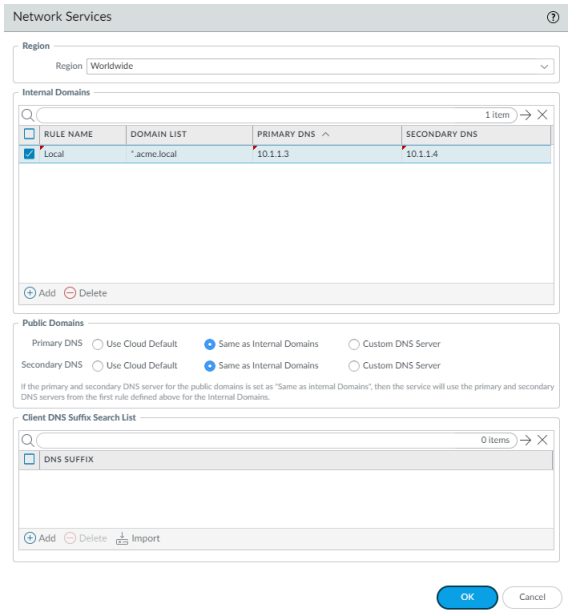
用されるDNSサーバーは、[内部ドメイン]セクションの最初のルールに設定されたサーバーと同じになります。

- **Custom DNS server (**カスタム**DNS**サーバー**)-** パブリック (外部) ドメインにアクセスできるDNSサーバーがある場合は、そのフィールドにプライマリDNSサーバー アドレスを入力します。

(任意) **DNS**サフィックスを追加して、解決できない非修飾ホスト名が入力されたときにクライアントがローカルで使用する必要があるサフィックスを指定できます (例:acme.local)。ドメイン サフィックスの前にワイルドカード (*) 文字を入力しないでください (例: acme.com)。複数のサフィックスを追加できます。

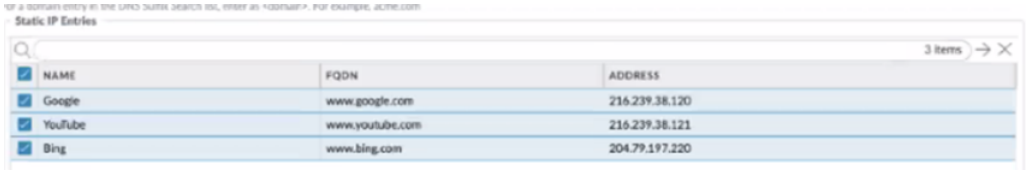
- Prisma AccessにDNSリクエストをプロキシさせたい場合は、UDPクエリ再試行（クエリを再試行する間隔（秒）、および再試行の試行回数（秒））の値を設定します。

  Prisma AccessがDNS要求をプロキシする方法の詳細については、「モバイル・ユーザーのためのDNS解決-GlobalProtectのデプロイメント」を参照してください。



STEP 11 | (任意) スタティック**IP**エントリを使用して、FQDNを特定のIPアドレスに解決します。

この機能は、組織内にゲスト インターネット サービスがあり、ゲストが検索エンジンを安全に使用して、会社のポリシーに違反する可能性のある不適切または不快なコンテンツを検索しないようにしたい場合に役立ちます。これを行うには、スタティックエントリ ルールの一意の 名前 、**FQDN**、およびFQDN 要求を送信するIPアドレスを入力します。



STEP 12 | （任意）デプロイ環境でWindowsインターネットネームサービス（WINS）を使用している場合、**WINS Configuration**（**WINS**設定）を選択してNetBIOS名からIPアドレスへのマッピングを解決するWINSサーバーを指定することができます。 WINSサーバーのリージョ

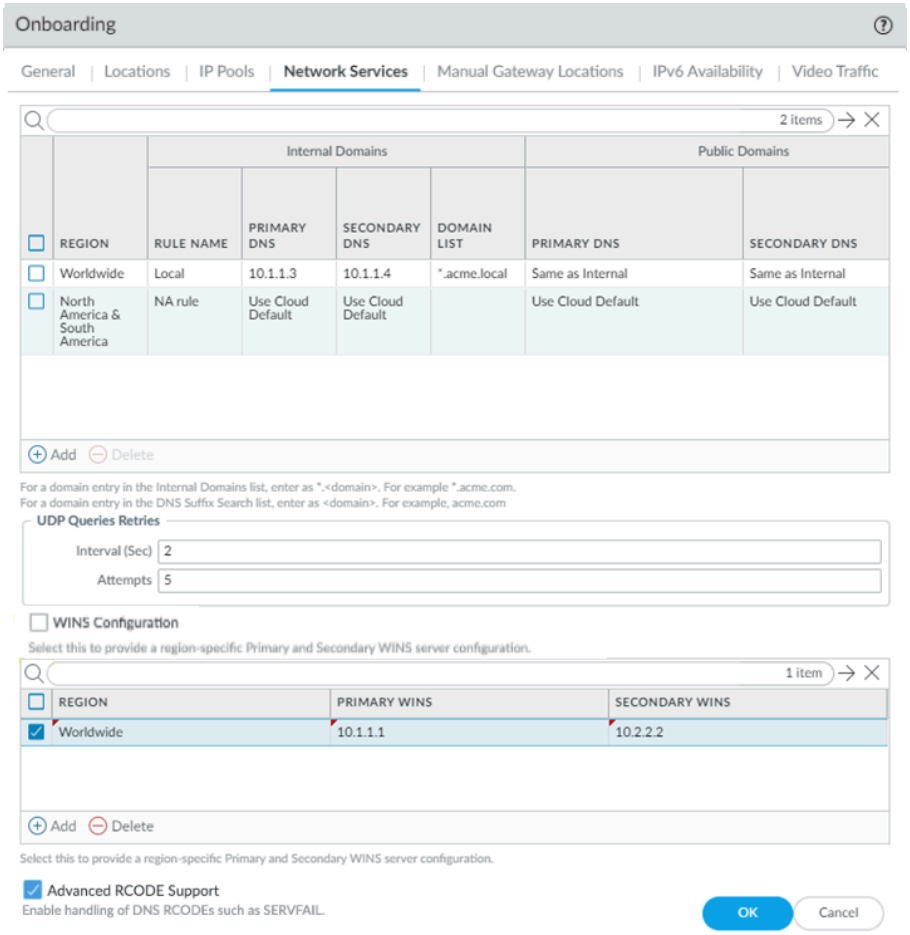
 ©2025 Palo Alto Networks, Inc.

ンを選択するか、またはWorldwideを選択して全世界にWINS設定を適用し、次に**Primary WINS**（プライマリ**WINS**）および必要に応じて**Secondary WINS**（セカンダリ**WINS**）サーバーのアドレスを指定します。

WINSを有効にすると、Prisma AccessはGlobalProtect経由で、WINS設定をモバイルユーザーにプッシュ配信できるようになります。

STEP 13 | (任意) 高度なRCODEサポートを選択すると、RCODE 2 (SERVFAIL) およびRCODE 5 (REFUSED) のDNS戻りコードを受信した場合にプライマリDNSサーバーがセカンダリDNSサーバーにフェイルオーバーできるようになります。

SERVFAILのDNS応答コードはプライマリDNSサーバとの通信エラーを指し、REFUSEDのDNS応答コードはプライマリDNSサーバが要求された情報の提供を拒否したことを意味します。どちらの場合も、サービスはセカンダリDNSサーバーにフェイルオーバーします。



©2025 Palo Alto Networks, Inc.

STEP 14 | （任意） モバイルユーザーに、GlobalProtectアプリからのゲートウェイの手動選択を許可する場合、ユーザーがGlobalProtectアプリから参照できる、**Manual Gateway Locations**（手動ゲートウェイのロケーション）を選択します。

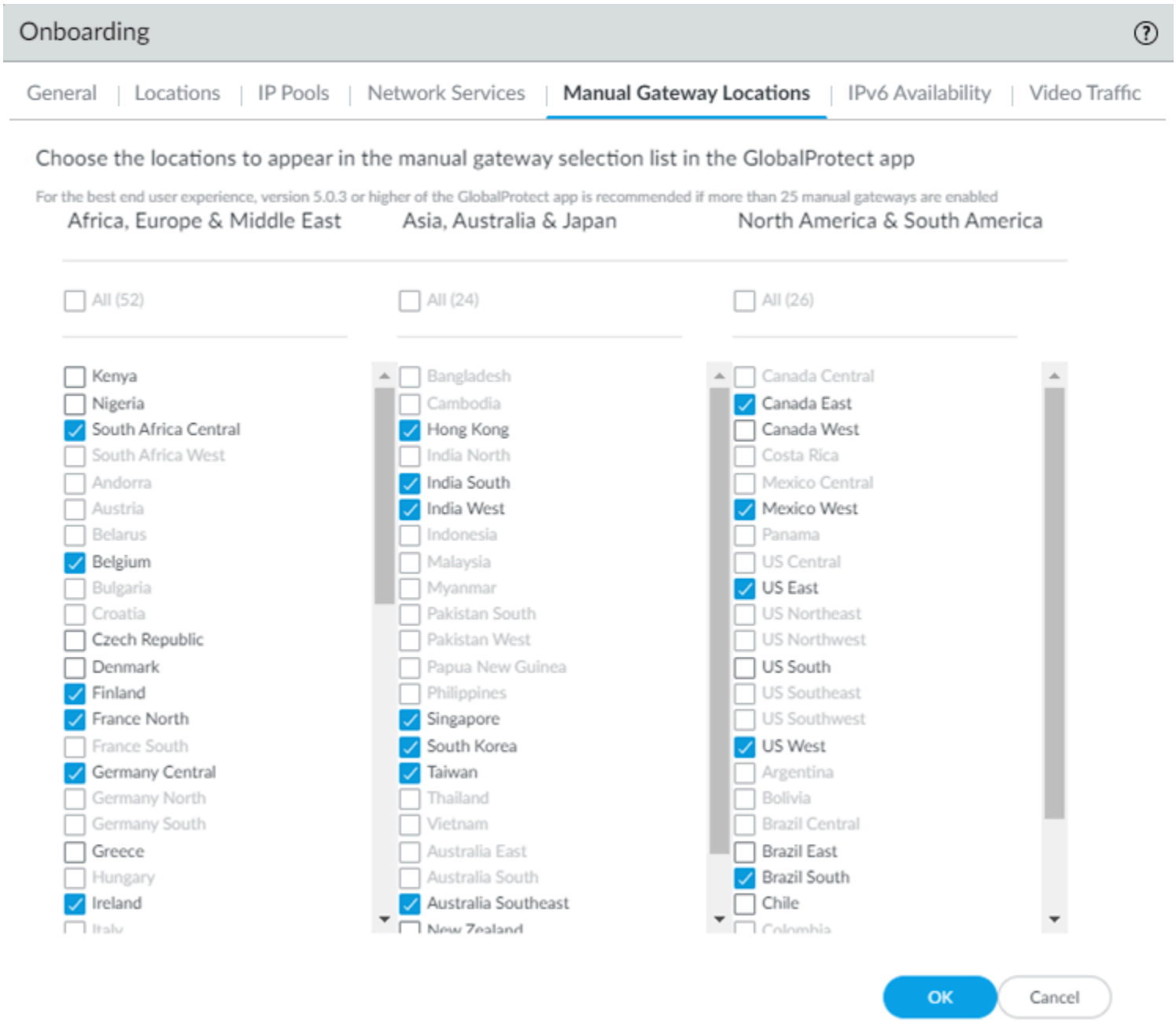
オンボーディングされたロケーションのサブネットを選択すると、モバイルユーザーが手動ゲートウェイ選択のためにGlobalProtectアプリに表示できる、利用可能なゲートウェイ数を減らせます。

このタブで手動ゲートウェイを選択しない場合、Prisma Accessはデフォルトでは次のリストのゲートウェイが選択されます。

- オーストラリア南東部
- ベルギー
- Brazil South（ブラジル南部）
- Canada East（カナダ東部）
- フィンランド
- France North（フランス北部）
- Germany Central（ドイツ中部）
- 香港
- India West（インド西部）
- アイルランド
- イスラエル
- Japan Central（日本中部）
- Netherlands Central（オランダ中部）
- サウジアラビア
- シンガポール
- South Africa Central（南アフリカ中部）
- 韓国
- 台湾
- イギリス
- US East（米国東部）
- US West（米国西部）

Prisma Accessではオンボーディングしたゲートウェイのみが選択できます。たとえば、ロケーションの選択時に**UK**（英国）を選択しなかった場合、**UK**を手動ゲートウェイとして選択できません（ロケーションは灰色表示されます）。

©2025 Palo Alto Networks, Inc.



オンボード後に場所を削除する必要があり、その場所が 手動ゲートウェイの場所の *1* つとして選択されている場合は、ここでも ***Locations (***ロケーション*)* タブでも必ず選択を解除してください。

STEP 15 | **OK**をクリックして、オンボーディング設定を保存します。

STEP 16 | **IPv6** 可用性 オプションを構成します。

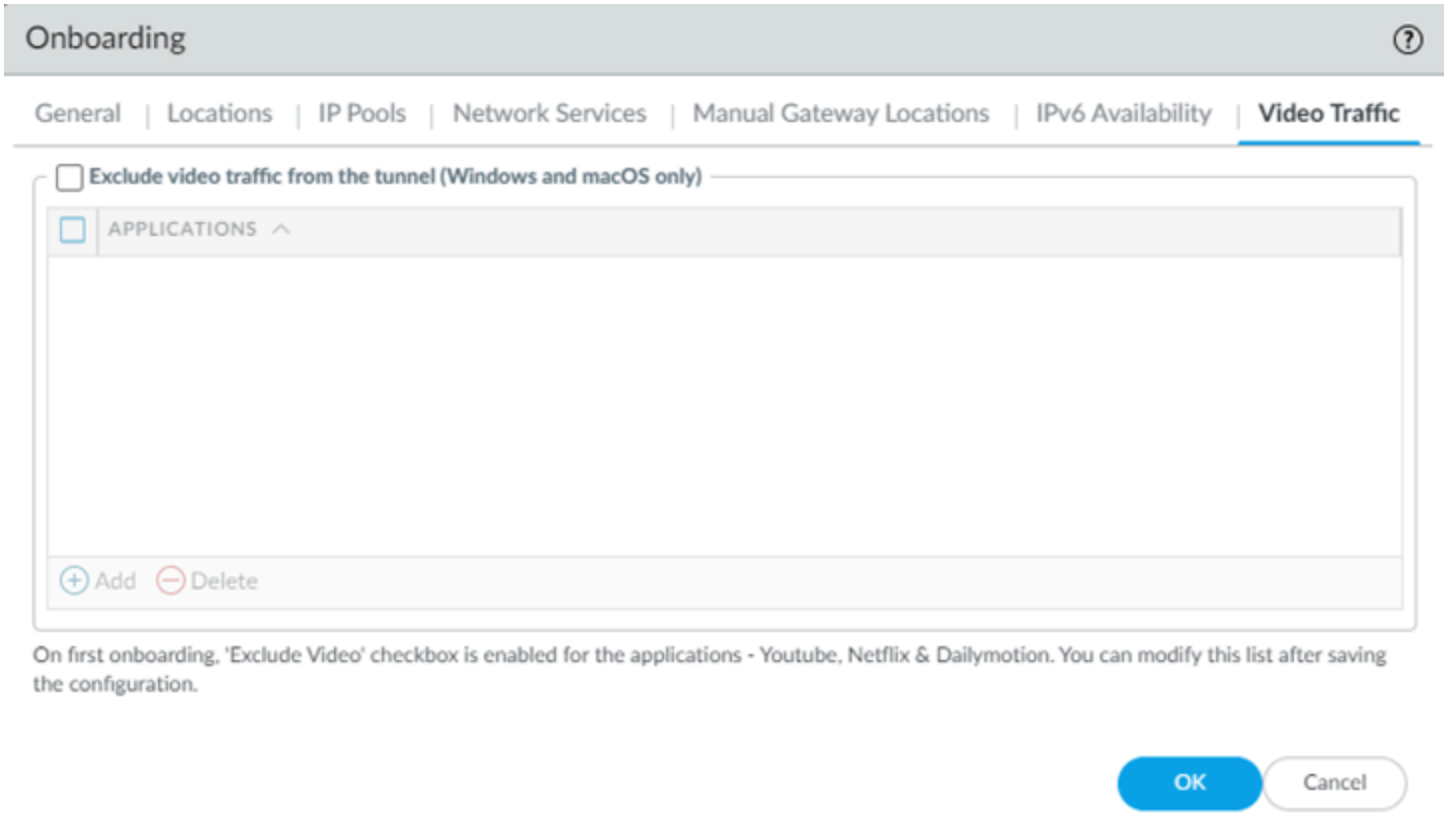
モバイルユーザー - GlobalProtect展開で IPv6ネットワークを 使用する場合は、Prisma Accessを設定することで、モバイル ユーザー ネットワークで IPv6 アドレスを使用できま

©2025 Palo Alto Networks, Inc.

す。また、IPv6アドレッシングを使用する前に、Prisma AccessインフラでIPv6ネットワークをグローバルに有効にする必要があります。

STEP 17 | (任意、Windows および macOS のみ) GlobalProtect トンネルからビデオ トラフィックを除外します。

トンネルからビデオ トラフィックを除外し、GlobalProtect トンネルから除外するビデオ ストリーミング アプリケーションを 追加 または 削除します 。



STEP 18 | モバイル ユーザーのトラフィックを保護するためのセキュリティ ポリシー ルールを作成します。

1. ポリシールールを追加する**Device Group** （デバイス グループ）を選択します。Mobile_User_Device_Groupまたは、モバイルユーザーのPrisma Accessを設定するときに選択した親デバイス グループを選択できます。
2. セキュリティポリシールールを作成します。任意の（Any）ゾーンから任意のゾーンへのトラフィックを許可するセキュリティポリシールールを定義していないことを確認してください。セキュリティポリシールールでは、テンプレー スタック内に定義したゾーンを使用します。

©2025 Palo Alto Networks, Inc.

STEP 19 | ログをStrata Logging Serviceに転送するように設定します。

新しいインストールの完了後、またはPrisma Accessテンプレート ステータスタックからPrisma Access以外のテンプレートを削除した場合、Cloud Servicesプラグインは次のログ設定（**Device**（デバイス） > **Log Settings**（ログ設定））を自動的に追加します：

- Mobile_User_Templateには、システムログ（**system-gpcs-default**）、ユーザーIDログ（**userid-gpcs-default**）およびHIP Matchログ（**hipmatch-gpcs-default**）およびGlobalProtectログ（**gp-prismaaccess-default**）のログ設定が追加されます。
- Remote_Network_Templateには、システムログ（**system-gpcs-default**）、ユーザーIDログ（**userid-gpcs-default**）、およびGlobalProtectログ（**gp-prismaaccess-default**）のログ設定が追加されます。
- Service_Conn_Templateには、システムログ（**system-gpcs-default**）、およびGlobalProtectログ（**gp-prismaaccess-default**）のログ設定が追加されます。

これらのログ設定は、システム、ユーザーID、およびHIP Matchログを自動的にStrata Logging Serviceに転送します。

STEP 20 | （任意） 他のログタイプのログをStrata Logging Serviceに転送します。

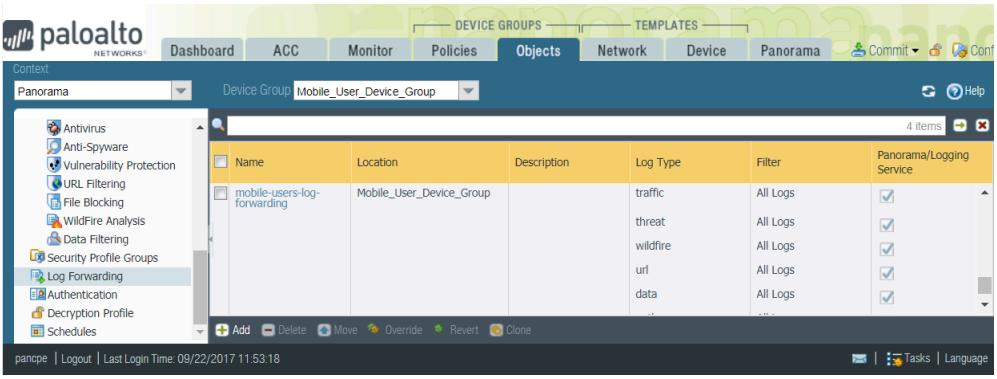
この場合、ログを転送する各ポリシールールに対してログ転送プロファイルを作成して、アタッチする必要があります。

1. ポリシールールを追加した**Device Group**（デバイスグループ）を選択します。
2. **Objects (**オブジェクト**) > Log Forwarding (**ログ転送**)** を選択してプロファイルを **Add (**追加**)** します。Log Forwarding Profile Match List（ログ転送プロファイル一致リスト）で、転送する各ログタイプを**Add**（追加）します。

   Traffic（トラフィック）、Threat Prevention（脅威防御）、WildFire Submission（WildFire送信）、URL Filtering（URLフィルタリング）、Data Filtering（データフィルタリング）、およびAuthentication（認証）ログを転送する例を次に示します。
3. [Forward Method(（転送方法）)]として、**[Panorama/Strata Logging Service]**を選択します。Panoramaを選択すると、ログがStrata Logging Serviceに転送されます。Panoramaからログを監視し、レポートを作成することができます。 Strata Logging Serviceはシームレスな統合を提供し、ログを本社のPanoramaにバックホールすること

©2025 Palo Alto Networks, Inc.

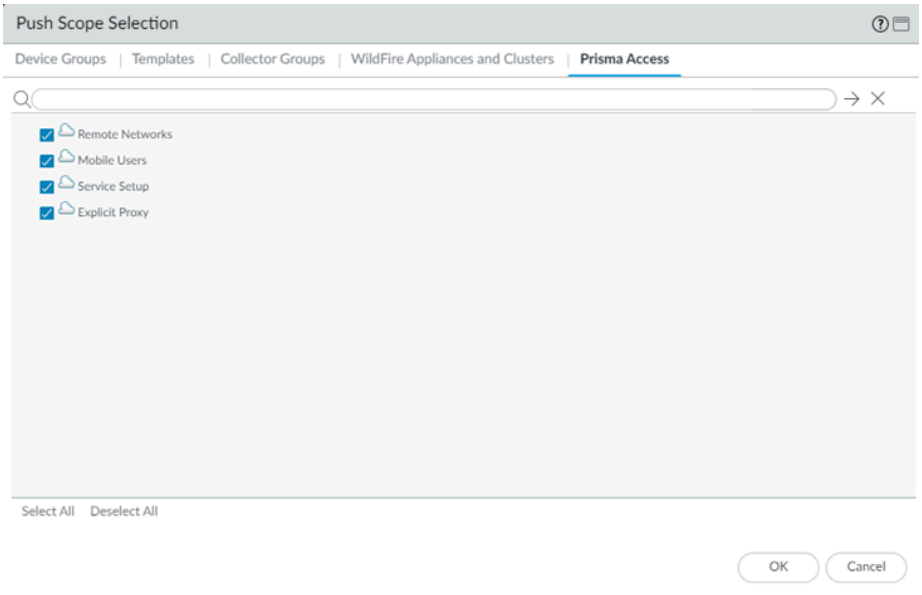
なく保存し、Panoramaは必要に応じてStrata Logging Serviceにクエリを実行することができます。



4. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択して、ポリシールールを編集します。**Actions**（アクション）で、作成した Log Forwarding（ログ転送）プロファイルを選択します。

STEP 21 | Panorama にすべての変更をコミットし、その設定変更をPrisma Accessにプッシュします。

1. **Commit**（コミット） > **Commit and Push**（コミットしてプッシュ）をクリックします。
2. [選択内容を編集]をクリックし、**Prisma Access**タブで[明示型プロキシ]に**[Mobile Users (モバイルユーザー)]**が**[Push Scope (プッシュ範囲)]**内で選択されていることを確認し、**[OK]**をクリックする。



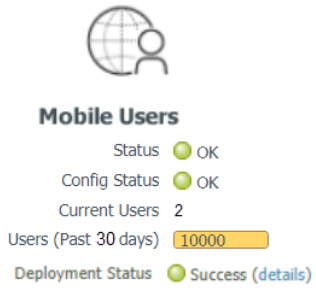
3. [デバイス グループ] タブで、 明示型プロキシ と **GlobalProtect** デバイス グループが選択されていることを確認します。
4. **[Commit and Push (コミットしてプッシュ)]** をクリックします。

©2025 Palo Alto Networks, Inc.

STEP 22 | Prisma Accessfor Usersがデプロイされ、アクティブになっていることを検証するためには、**Panorama** > **Cloud Services** > ステータス > ステータスを選択します。

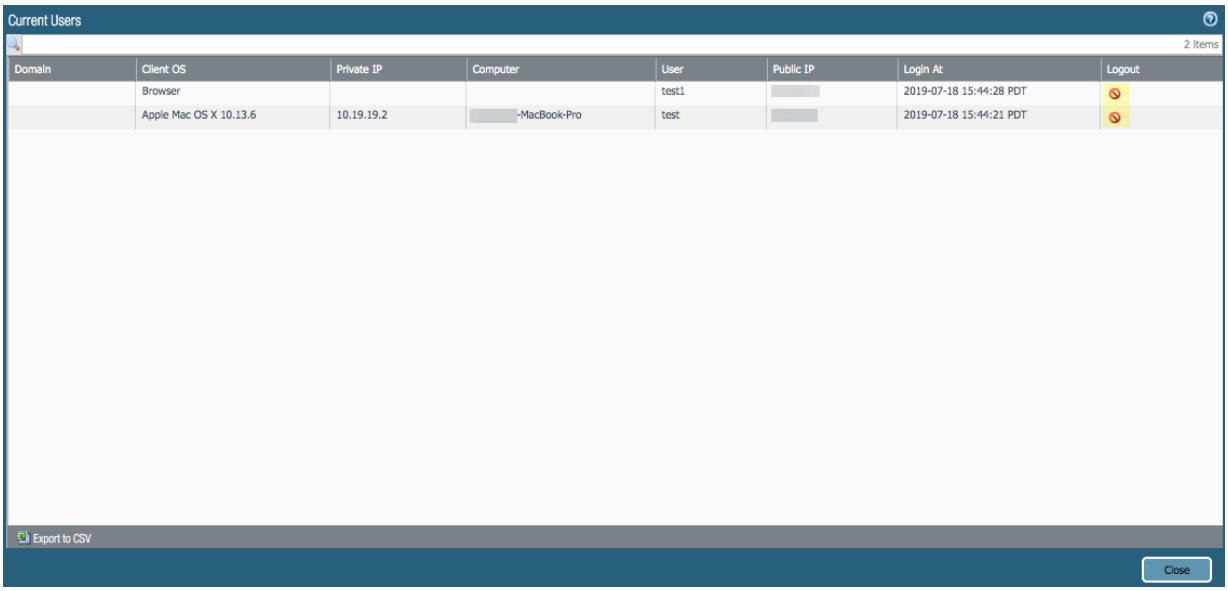
プロビジョニングが完了した後は、モバイルユーザーの**Status**（ステータス）と**Config Status**（設定ステータス）には**OK**が表示されているはずです。

Deployment Status（デプロイステータス）では、オンボーディングおよびデプロイジョブのステータスを参照することができます。また、完了したジョブのステータスに関する詳細情報も参照することができます。



現在ログインしている一意のユーザー数を表示する、またはログインしているユーザーをログアウトさせるには、**Current Users**（現在のユーザー）の隣にあるハイパーリンクされている数字をクリックします。

©2025 Palo Alto Networks, Inc.

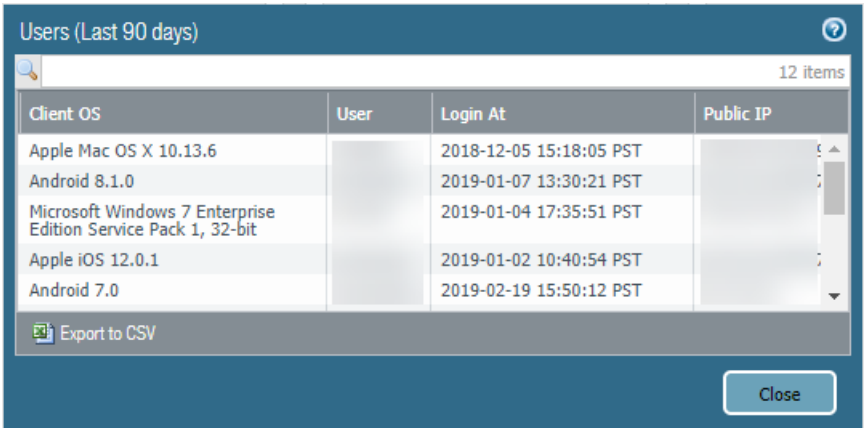


前にログインしたユーザーの履歴情報を90日の期間で表示するには、**Users (Last 90 days)**（過去**90**日間のユーザー）の隣にある数字をクリックします。

「ユーザー (過去 90 日間)」フィールドのユーザー数がライセンス総数の 80% に達すると、その数は赤色で表示されます。

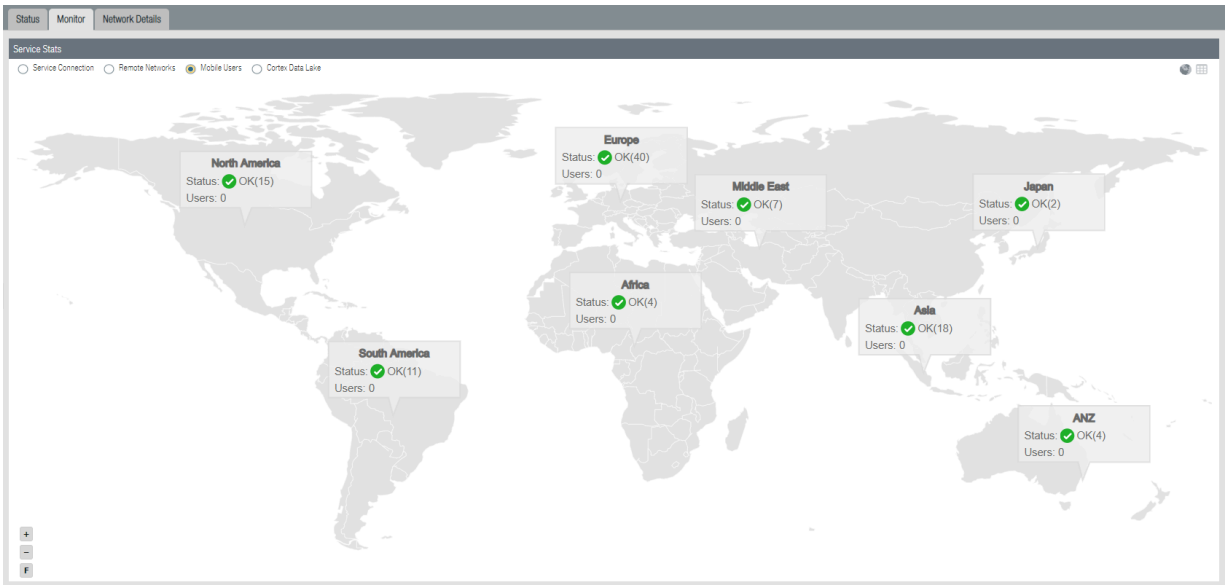
ユーザーのリストをcsvファイルにエクスポートするには、**Export to CSV**（**CSV**にエクスポート）を選択します。1つのCSVファイルには、最大45,000人のユーザーをエクスポートできます。

©2025 Palo Alto Networks, Inc.



選択した地域で動作しているPrisma Accessポータルおよびゲートウェイの、ロケーションを示すマップを表示するには、**Monitor**（監視）を選択して、次に**Mobile Users**（モバイルユーザー）を選択します。

 ©2025 Palo Alto Networks, Inc.



地域を選択すると、その地域の詳細情報が表示されます。

- **Location (**ロケーション**)**- ネットワーク上のモバイル ユーザーを保護するためにクラウド サービス インフラストラクチャがデプロイされている場所。

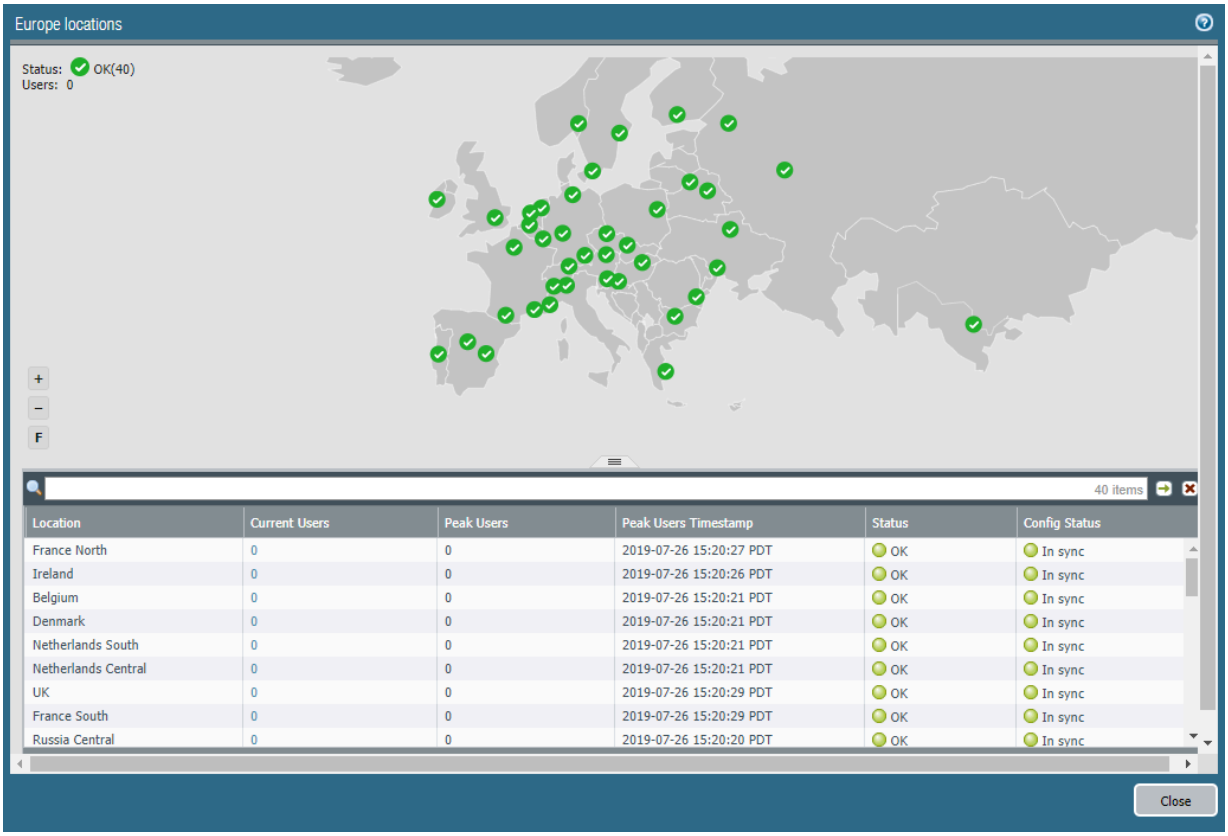
 ©2025 Palo Alto Networks, Inc.

- 現在のユーザー- サービスに接続され、保護されているユーザーの数。

  現在のモバイル ユーザー数がライセンス総数の 80% に達すると、この数値は赤で表示されます。
- ピーク ユーザー数 - 同時ユーザーの最大数。
- ピーク ユーザー タイムスタンプ- ピーク ユーザー データが最後に取得されたときのタイムスタンプ。
- **Status**（ステータス）– Prisma Accessとモバイルユーザー間の接続の動作状況。
- **Config Status**（設定ステータス）–サービスへの設定の最後のプッシュのステータス。ローカルで変更を行ったけれども、まだクラウドに設定をプッシュしていない場合、ステータス**Out of sync**（非同期）が表示される可能性があります。ステータスインジケータ

©2025 Palo Alto Networks, Inc.

上にカーソルを移動すると、詳細情報が表示されます。設定をPrisma Accessにコミットしてプッシュすると、Config Statusが**In sync**になります。



STEP 23 | ポータルホスト名に対して、**Use Company Domain**（会社のドメインを使用）を選択した場合、定義したポータルホスト名を**Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Mobile Users**（モバイルユーザー） > **Onboarding**（オンボーディング） > **General**（全般）タブに表示されているポータルDNS CNAMEにマップするDNSエントリを、内部DNSサーバーに追加する必要があります（`<portal_hostname>.gpcloudservice.com`）。

©2025 Palo Alto Networks, Inc.

STEP 24 | エンドユーザーにGlobalProtectアプリソフトウェアを配布します。

Mac OSまたはWindowsユーザーの場合、ユーザーをPrisma Accessポータルのアドレスにリダイレクトして、そこからGlobalProtectアプリをダウンロードさせることができます。

*Prisma Access*がポータル上で*GlobalProtect*アプリのバージョンを管理し、*Prisma Access*がホストするバージョンからアクティブなバージョンを選択し、ユーザーがダウンロードできるようにコントロールすることができます。

あるいは、Mac OS および Windows ユーザー向けに、GlobalProtectアプリケーション ソフトウェアを Web サーバー上でホストする こともできます。 Prisma Accessはサポート終了として記載されていないGlobalProtectアプリケーションのバージョンと互換性があります。

モバイルアプリのユーザーは、各自のオペレーティングシステムに合わせた適切なアプリストアから、GlobalProtectモバイルアプリをダウンロード、インストールすることができます。

GlobalProtect — トンネル設定のカスタマイズ

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

GlobalProtectアプリケーションがPrisma Accessに接続するために確立するVPNトンネルの設定をカスタマイズします。トンネル設定には、アプリケーションがPrisma Accessに送信するトラフィックと、代わりにローカルにルーティングできるトラフィック（業務で使用する必要のない帯域集約型アプリケーションなど）を定義するために使用できる分割トンネリングオプションが含まれています。

トンネル設定に定義する一致条件は、Prisma Accessに設定を受信するユーザー、デバイス、またはシステムを示します。たとえば、特定のリージョン内のGlobalProtectアプリケーションのすべてのインスタンスにトンネル設定ルールが適用されるように指定できます。Prisma Access (Managed by Panorama)では、アクセスルートまたはドメインとアプリケーションに基づいてスプリットトンネル設定を構成できます。

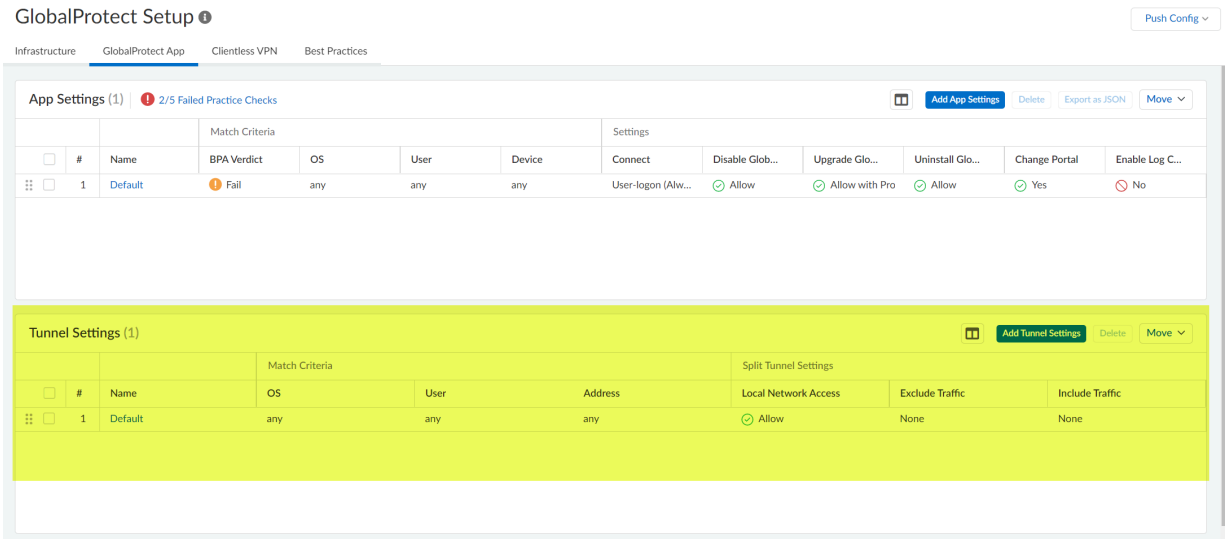
- Strata Cloud Manager
- Panorama

GlobalProtect — トンネル設定のカスタマイズ (Strata Cloud Manager)

 ©2025 Palo Alto Networks, Inc.

STEP 1 | [管理] > [サービス設定] > [モバイル ユーザー] > **[GlobalProtect** 設定] > **[GlobalProtect**アプリケーション] > [トンネル設定の追加]をクリックします。

*Strata Cloud Managerを使用している場合は、[ワークフロー] > [Prisma Access*セットアップ*] > [*モバイル ユーザー*] > [GlobalProtect* セットアップ*] > [GlobalProtect*アプリケーション*] > [*トンネル設定の追加]をクリックします。



STEP 2 | 名前と一致条件 を入力して、設定を受け取るユーザー、デバイス、またはシステムを指定します。たとえば、特定のリージョン内のGlobalProtectアプリケーションのすべてのインスタンスにトンネル設定ルールが適用されるように指定できます。

STEP 3 | Prisma Accessのための**Authentication Override (**認証オーバーライド**)**が、ユーザー認証のために、安全で暗号化されたクッキーを生成し、 受け取ることができるようにします。この設定により、ユーザーは指定された期間中に1回だけログイン資格情報を提供できるようになります。

- **Generate cookie for authentication override**（認証オーバーライド用**Cookie**を生成） — Prisma Accessが暗号化されたエンドポイント固有のCookieを生成し、その認証用Cookieをエンドポイントに発行できるようにします。
- **Accept cookie for authentication override**（**Cookie** による認証オーバーライドを許可） — Prisma Accessが暗号化された有効な Cookie を使用してユーザーを認証できるようにします。アプリが有効なクッキーを提示すると、Prisma Accessはそのクッキーが元々Prisma

©2025 Palo Alto Networks, Inc.

Accessによって暗号化されていたことを検証し、クッキーを復号化してからユーザーを認証します。

*GlobalProtect*アプリケーションは、ユーザのエンドポイントから関連する認証クッキーを照合して取得するために、接続ユーザのユーザ名を知らなければなりません。*Cookie*を取得した後、アプリはそれを*Prisma Access*に送信してユーザー認証を行います。

STEP 4 | 分割トンネリングを有効にして、GlobalProtectアプリケーションがPrisma AccessへのVPNトンネルを通して許可または制限するトラフィックを定義します。分割トンネリングは、ビジネスクリティカルでない、または生産性を向上させないトラフィックPrisma Accessを除外することで、帯域幅を節約します。

- ローカル ネットワーク アクセス- WindowsユーザーとMacユーザーがPrisma Accessに最初に接続しなくても、ローカル リソースにアクセスできるようにします。

  トラフィックを除外- アプリケーション、ドメイン、ルート（IPアドレスのようなもの）に基づいて、 Prisma Accessポリシーの検査と実施から除外するトラフィックを指定する。

  Customize Include Traffic (トラフィックを含むカスタマイズ**)**–デフォルトでは、GlobalProtectアプリケーションは、除外リストにあるものを除くすべてのトラフィックをPrisma Accessにルーティングします。除外リストの条件を満たす場合でも、GlobalProtectアプリケーションがPrisma Accessに常にルーティングする必要のあるトラフィックを指定します。

STEP 5 | リストされたアプリケーションからのビデオ ストリーミング トラフィックをPrisma Accessに送信しないようにするには、「**Video Stream Traffic (**ビデオ ストリーム トラフィック**)**」を除外します。VPN トンネルから低リスクのビデオ ストリーミング トラフィック（YouTube や Netflixなど）を除外することで、帯域幅消費を減らすことができます。ビデオストリーミングの除外は、このルールに定義した一致条件だけでなく、GlobalProtectアプリケーションがPrisma Accessに送信するすべてのトラフィックに適用される。

STEP 6 | 設定を保存します。上記の手順を繰り返して、さらにトンネル設定を追加します。

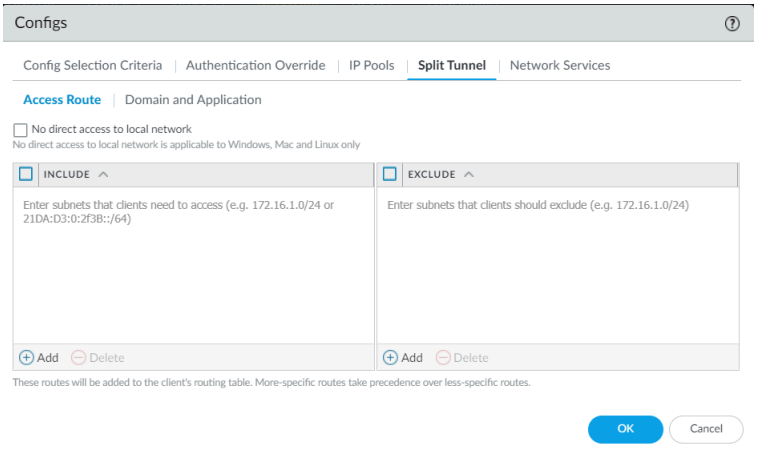
STEP 7 | （任意）Prisma Accessへの接続時に使用される VPN トンネル設定の優先順位を設定するために移動します。

GlobalProtect – トンネル設定のカスタマイズ (Panorama)

アクセスルートまたはドメインとアプリケーションに基づいてスプリットトンネル設定を構成できます。

 ©2025 Palo Alto Networks, Inc.

- アクセスルートに基づいてスプリットトンネル設定を構成します。
  1. **[Panorama] > [**ネットワーク**] > [GlobalProtect] > [**ゲートウェイ**]**をクリックし、カスタマイズしたいゲートウェイを選択します。
  2. **[Agent (**エージェント**)] > [Client Settings (**クライアント設定**)]**をクリックし、設定を選択します。
  3. **[Split Tunnel (**分割トンネル**)] > [Access Route (**アクセスルート**)]**をクリックします。スプリット トンネルの設定は、GlobalProtectアプリケーションがPrisma Accessとトンネルを確立するときに、エンドポイント上の仮想ネットワーク アダプタに割り当てられます。特定の宛先 IP サブネットトラフィックをVPNトンネル経由で送信しないようにしたり、除外したりできます。



  4. GlobalProtectに接続している間、ユーザーがプロキシやローカルリソースに直接トラフィックを送信するのを防ぐために、**[No direct access to local network (**ローカルネットワークへの直接アクセスしない**)]**オプションを有効にしてください。

     不正な*Wi-Fi*アクセスポイントなどの信頼できないネットワークでのリスクを軽減するため、［***No direct access to local network (***ローカルネットワークに直接アクセスしない**)***］設定を有効にします。

  5. LAN宛ての特定のトラフィックのみをGlobalProtectにルーティングするために、［**Include (**含める**)**］を選択し、宛先サブネットまたはアドレスオブジェクト（タイプIPネットマスク）を追加します。IPv6 または IPv4 サブネットを含めることができます。すべての宛先サブネットあるいはアドレス オブジェクトを含めるには、0.0.0.0/0 および ::/0 をアクセス ルートとして**Include (**含有**)**します。
  6. **Excludes**（除外）を選択し、アプリに除外させたい宛先のサブネットまたはアドレス オブジェクト（タイプは IP Netmask（IP ネットマスク））を**Add**（追加）します。除外するルートは、想定外のトラフィックが除外されることのないように、包含するルートよりも細かく指定してください。IPv6またはIPv4サブネットを除外することはできます。

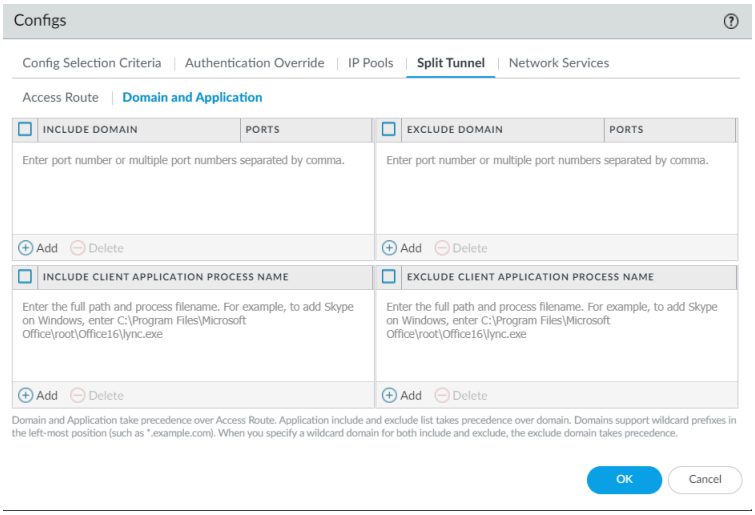
     *Chromebook*で*Android*を実行しているエンドポイントのアクセスルートを除外することはできません。*Chromebook* では *IPv4* ルートのみがサポートされています。

  7. トンネル設定を保存します。

©2025 Palo Alto Networks, Inc.

- ドメインとアプリケーションに基づいて分割トンネル設定を構成します。
  1. **[Panorama] > [**ネットワーク**] > [GlobalProtect] > [**ゲートウェイ**]**をクリックし、カスタマイズしたいゲートウェイを選択します。
  2. **[Agent (**エージェント**)] > [Client Settings (**クライアント設定**)]**をクリックし、設定を選択します。
  3. **[Split Tunnel (**分割トンネル**) > Domain and Application (**ドメインとアプリケーション**)]**タブをクリックして、宛先ドメインに基づいてスプリットトンネル設定を構成します。

     *MacOS*エンドポイントで*Sophos*のようなサードパーティのエンドポイントセキュリティ製品を使用する際に、いくつかの互換性の問題が発生する可能性があります。



  - (任意) **[Include Domain (**ドメインを含む**)]**を選択し、宛先ドメインとポートを使用してVPN接続を介してGlobalProtectにルーティングするSaaSまたはパブリッククラウドアプリケーションを追加します。エントリを最大 200 個まで追加することができます。たとえば、*.gmail.comを追加すると、すべての Gmail トラフィックが VPN トンネルを通過できるようになります。
  - （任意）**[Exclude Domain (**除外ドメイン**)]**を選択し、宛先ドメインとポートを使用して VPN トンネルから除外する SaaS またはパブリック クラウド アプリケーションを追加します。エントリを最大 200 個まで追加することができます。たとえ

©2025 Palo Alto Networks, Inc.

ば、*.target.comを追加すると、すべての Target トラフィックが VPN トンネルから除外されます。

4. アプリケーションに基づいてスプリットトンネル設定を構成します。

   *Safari*トラフィックは、*macOS*エンドポイントのアプリケーションベースのスプリットトンネルルールに追加できません。

   *Windows*および*macOS*エンドポイントでアプリケーションに基づいてスプリットトンネルを構成するために、環境変数を使用できます。

   - (任意) **[Include Client Application Process Name (**クライアントアプリケーションプロセス名を含める**)**］を選択し、アプリケーションプロセス名を使用してVPN接続を介してGlobalProtectにルーティングするSaaSまたはパブリッククラウドアプリケーションを追加します。エントリを最大 200 個まで追加することができます。
   - (任意) **[Exclude Client Application Process Name (**クライアント アプリケーション プロセス名を除外**)]**を選択し、アプリケーション・プロセス名を使用してVPNトンネルから除外するSaaSまたはパブリック クラウド アプリケーションを追加します。エントリを最大 200 個まで追加することができます。

5. トンネル設定を保存します。

GlobalProtect – アプリ設定をカスタマイズ

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

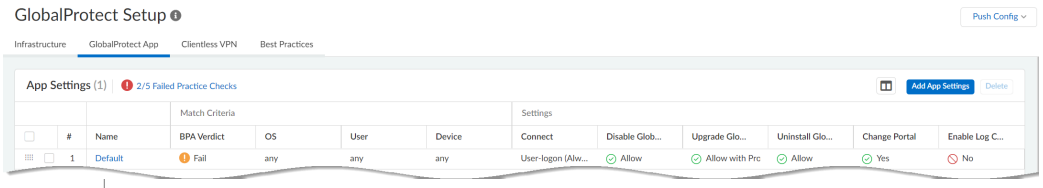
エンドユーザーGlobalProtectアプリケーションとやり取りする方法をカスタマイズします。

グローバルにカスタマイズできる設定がいくつかあります。これらのグローバル アプリ設定は、すべてのデバイスのGlobalProtectアプリケーションに適用されます。GlobalProtectアプリケーションのその他の設定はデフォルトで設定されます。その後、これらのオプションをカスタマイズし、一致条件に基づいて、特定のユーザーやデバイスをターゲットにすることができます。アプリの設定に定義した一致条件は、設定を受け取るべきユーザー、デバイス、またはシステムをPrisma Accessに伝えます。例えば、Active Directoryのエントリと一致するシリアルナンバーを持つデバイスにのみ適用されるルールを指定することができます。

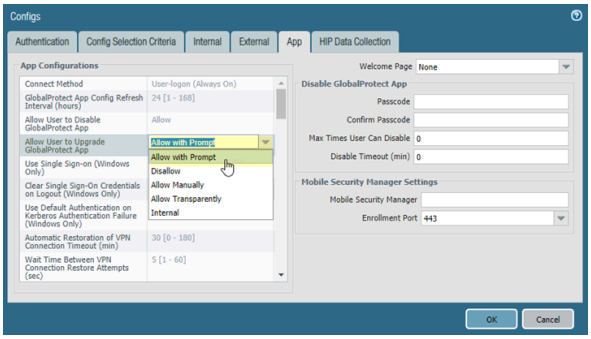
GlobalProtect アプリ設定	
ここでアプリの設定を調べてカスタマイズします (クラウド管理の例を以下に示します) —>	Prisma Access (Managed by Strata Cloud Manager)

©2025 Palo Alto Networks, Inc.

GlobalProtect アプリ設定

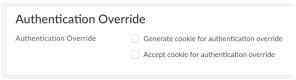


Panorama Managed Prisma Access



認証のオーバーライド

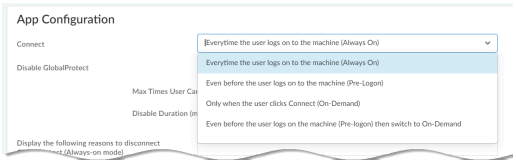
Prisma Accessが、ユーザー認証のために、安全で暗号化されたクッキーを生成し、 受け取ることができるようにします。これをオンにすると、ユーザーは指定された期間中に一度だけログイン認証情報を提供することができます。



- **Generate cookie for authentication override**（認証オーバーライド用 **Cookie** を生成） – Prisma Accessが暗号化されたエンドポイント固有のCookieを生成し、その認証用Cookieをエンドポイントに発行できるようにします。
- **Accept cookie for authentication override**（**Cookie** による認証オーバーライドを許可） – Prisma Accessが暗号化された有効な Cookie を使用してユーザーを認証できるようにします。有効なCookieをアプリが提示した場合、Prisma Accessはポータルまたは Prisma Accessが暗号化したCookieであることを確認し、復号化を行ってユーザーを認証します。

> *GlobalProtect* アプリケーションが関連する認証用 *Cookie* をユーザーのエンドポイントにマッチさせて取得するためには、接続するユーザーのユーザー名を知る必要があります。*Cookie* を取得した後、アプリはそれを*Prisma Access*に送信してユーザー認証を行います。

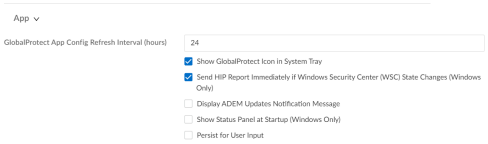
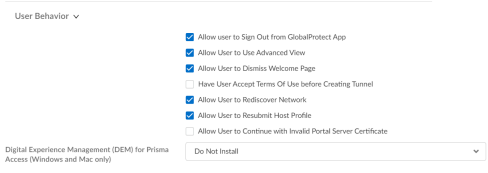
©2025 Palo Alto Networks, Inc.

GlobalProtect アプリ設定	
	• **Cookie Lifetime**（**Cookie** の有効期間） – Cookie が有効な時間数、日数、または週数を指定します（デフォルトは 24 時間）。範囲は、時間が 1～72、週が 1～52、日数が 1～365 です。Cookieが失効した場合、ユーザーはログイン認証情報を再度入力する必要があり、この入力をうけ、Prisma Accessは新しいCookieを暗号化してアプリに送信します。この値は、設定したCookieの有効期間と同じでも異なっていてもかまいません。 • **Certificate to Encrypt/Decrypt Cookie**（**Cookie** 暗号化/復号化時の証明書） – Cookie を暗号化および復号化するために使用する RSA 証明書を選択します。
接続設定	GlobalProtectアプリケーションがPrisma Accessに接続するために使用する方法を指定します。  • ユーザー ログオン (常時オン)- ユーザーがログインするとすぐに、GlobalProtectアプリケーションはPrisma Accessに自動的に接続します。SSO と併用されると（Windows エンドポイントのみ）、ログインはエンドユーザーに透過的になります。 *iOS*エンドポイントでは、*GlobalProtect*アプリケーションがすべてのトラフィックを強制的にトンネル経由にするため、この設定によりワンタイム パスワード *(OTP)* アプリケーションが動作しなくなります。 • プレ ログオン（常時オン）–GlobalProtectアプリケーションはユーザーを認証し、ユーザーがログインする前にPrisma AccessへのVPNトンネルを確立します。このオプションでは、外部PKIソリューションを使用して、これらの設定を受信する各デバイスにマシン証明書を事前にデプロイする必要があります。 • **On-demand (Manual user initiated connection)**（オンデマンド（ユーザーによる手動接続）） – ユーザーは、GlobalProtect に接続するために、アプリを手動で起動する必要があります。 • **Pre-logon then On-demand**（ログオン前、次にオンデマンド） – Pre-logon (Always On)（ログオン前（常時オン））の接続方式と同じく、（コンテンツ リリース バージョン590-3397以降が必要な）この接続方式

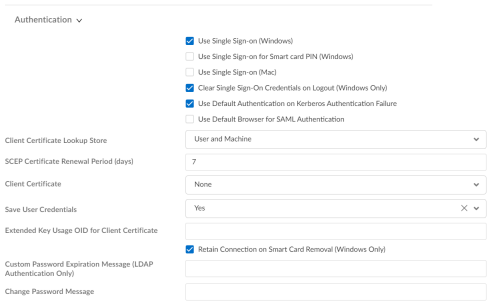
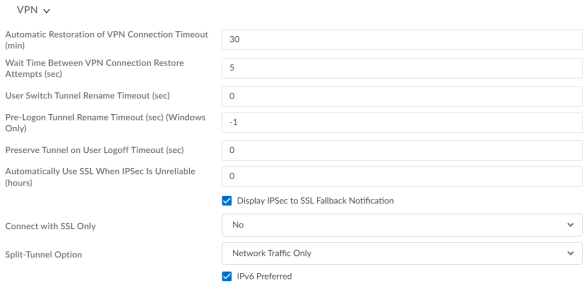
 ©2025 Palo Alto Networks, Inc.

GlobalProtect アプリ設定	
	では、ユーザーがエンドポイントにログインする前にGlobalProtectアプリケーションがユーザーを認証し、Prisma Accessとの VPN トンネルを確立できます。プレ ログオン接続方式と異なり、エンドポイントにログインした後、接続が何らかの理由で切断された場合、ユーザーは手動でアプリを起動してGlobalProtectに接続する必要があります。このオプションの利点は、パスワードの有効期限が切れた後、またはパスワードを忘れた後にユーザーが新しいパスワードを指定できるようにすることができますが、ログイン後にユーザーが手動で接続を開始する必要があることです。
グローバルプロテクト	ユーザーが調整できるGlobalProtectアプリケーション設定を決定します。 • **GlobalProtect**を無効にする- ユーザーがGlobalProtectアプリケーションを無効にできるかどうかを決定します。GlobalProtectアプリケーショ ンを無効にしたユーザーは、アプリをオンに戻すまでPrisma Access（および保護された企業リソー ス）に接続できません。 • **GlobalProtect**のアップグレード- ユーザーが更新を開始できるかどうかなど、アプリのアップグレードの動作方法を指定します。 ユーザーがいつアップグレードできるかを制御するために、設定ごとにアプリのアップグレードをカスタマイズできます。たとえば、あるリリースを全ユーザーにデプロイする前に小規模なユーザー グループでテストする場合、IT グループのユーザーのみに適用される設定を作成できます。これにより、このグループのユーザーにはアップグレードとテストを許可し、他のユーザー/グループ設定にはアップグレードを禁止します。新しいバージョンを完全にテストした後、残りのユーザーのエージェントの設定を変更し、アップグレードを許可できます。 • **Allow with Prompt (**プロンプト付きで許可**)**- アプリの新しいバージョンが利用可能になったときに、ユーザーにアップグレードを促します。 • **Allow Transparently**（メッセージを表示せずに実行）–アップグレードはユーザーの介入なしに自動的に行われます。 • **Internal (**内部**)**- ユーザーがPrisma Accessに接続すると、ユーザーの介入なしに自動的にアップグレードが行われます。

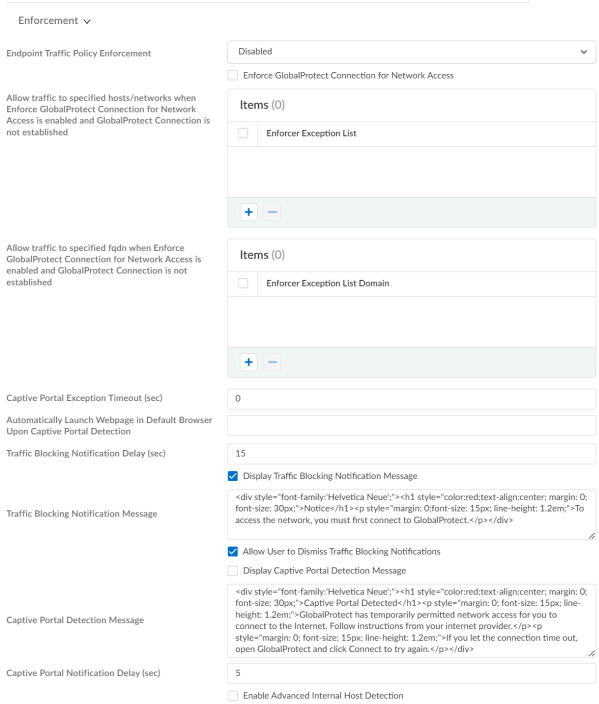
©2025 Palo Alto Networks, Inc.

GlobalProtect アプリ設定	
	• **Disallow (**許可しない**)**- アプリのアップグレードを禁止します。 • **Allow Manually (**手動で許可**)**- ユーザーがGlobalProtectアプリケーション内からアプリのアップグレードを開始できるようにします。 • **Uninstall GlobalProtect (GlobalProtect**のアンインストール**)**–ユーザーがGlobalProtectアプリケーションをアンインストールできるようにするか、ユーザーがGlobalProtectアプリケーションをアンインストールできないようにするか、またはユーザーが作成したパスワードを指定した場合にアンインストールできるようにします。 • **User Can Change Portal (**ユーザーはポータルを変更できます**)**- GlobalProtectアプリケーションがPrisma Accessへの接続に使用するポータルをユーザーが変更できるようにする。
App Configuration (アプリケーション構成**) -** 詳細オプション	
アプリケーション設定	• Send HIP Report Immediately if Windows Security Center (WSC) State Changes（Windows セキュリティーセンター（WSC）の状態が変更された場合にHIPレポートを即座に送信）(Windowsのみ) – Windows セキュリティーセンター（WSC）の状態が変更された際に、GlobalProtectアプリケーションがHIPデータを送信しないようにするには、Noを選択します。WSCの状態が変更された際に即座にHIPデータを送信する場合はYes（デフォルト）を選択します。 
User Behavior (ユーザー振る舞い**)**設定	ユーザー振る舞い設定には以下が含まれます: 
認証設定	認証設定には以下が含まれます。

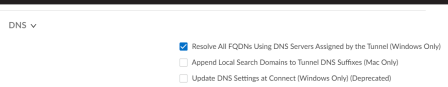
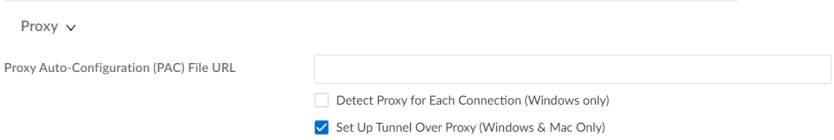
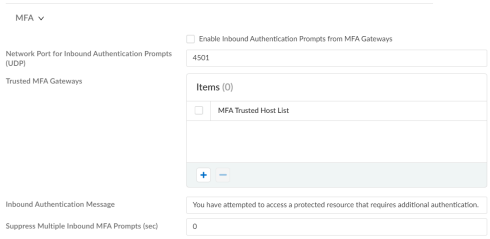
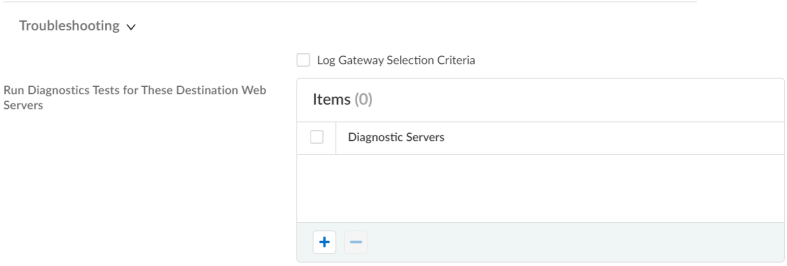
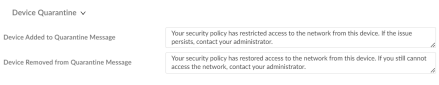
 ©2025 Palo Alto Networks, Inc.

GlobalProtect アプリ設定	
	
VPN設定	VPNタイムアウトとトンネル設定を構成します。 • **Display IPSec to SSL Fallback Notification (IPSec** から **SSL** へのフォールバック通知を表示する**)**- GlobalProtectアプリケーションがIPSecトンネルへの接続を確立できず、SSLトンネルにフォールバックした場合にポップアップ通知が表示され ない ようにするには、**No**を選択します。接続が変更されたときにポップアップ通知を許可するには、**Yes**(デフォルト) を選択します。 
強制設定	指定されたトラフィックの設定を適用します。 • **Enforce GlobalProtect Connection for Network Access** が有効で、**GlobalProtect Connection** が確立されていない場合、指定された **FDQN** へのトラフィックを許可します– 詳細はこちら • **Automatically Launch Webpage in Default Browser Upon Captive Portal Detection (**キャプティブ ポータルの検出時にデフォルトのブラウザで自動的にウェブページを起動する**)** – デフォルトのWebブラウザを自動的に起動して、ユーザが認証ポータルにシームレスにログインできるようにするには、デフォルトのWebブラウザが起動したときにWebトラフィックを開始する最初の接続試行に使用するWebサイトの完全修飾ドメイン名（FQDN）またはIPアドレスを入力します（最大長は256文字）。認証ポータルは、このWebサイト接続の試行を傍受し、デフォルトのWebブラウザを認証ポータルのログインページにリダイレクトします。このフィールドが空の場

 ©2025 Palo Alto Networks, Inc.

GlobalProtect アプリ設定	
	合（デフォルト）、Prisma Accessは認証ポータルの検出時にデフォルトのウェブブラウザを自動的に起動しません。 • **Enable Advance Internal Host Detection (**高度な内部ホスト検出を有効にする**)** - 高度な内部ホスト検出を有効にして、GlobalProtectアプリケーションによる内部ホスト検出中にセキュリティ レイヤーを追加します。高度な内部ホスト検出により、アプリは内部ゲートウェイのサーバー証明書を検証するだけでなく、内部ホストのリバース DNS検索を実行して、アプリが企業ネットワーク内にあるかどうかを判断します。高度な内部ホスト検出を有効にすると、内部ホスト検出中に悪意のある攻撃者がリバースDNSサーバー応答を偽装することを阻止し、企業ネットワーク内のエンドポイントへの不正アクセスを防止します。高度な内部ホスト検出を有効にしない場合は、既存の内部ホスト検出が期待どおりに機能します。 
接続振る舞い設定	接続振る舞いの設定には以下が含まれます。  詳しくはこちらをご覧ください
DNS 設定	DNS設定には以下が含まれます。

©2025 Palo Alto Networks, Inc.

GlobalProtect アプリ設定	
	
プロキシ設定	プロキシ設定を構成するためにエンドポイントにプッシュするプロキシ自動構成 **(PAC)** ファイルの**URL**を指定します。最大長は 256文字です。次のプロキシ自動構成 (PAC) ファイルの URL メソッドがサポートされています。 • Proxy Auto-Config (PAC) 標準 (例: http://pac.<hostname or IP>/proxy.pac)。 • Web Proxy Auto-Discovery Protocol (WPAD) 標準 (例: http://wpad.<hostname or IP>/wpad.dat)。 
MFA設定	MFA設定には以下が含まれます。 
トラブルシューティング設定	トラブルシューティング設定には以下が含まれます。 
デバイスの隔離設定	デバイス隔離設定には以下が含まれます。 
内部ホスト検出	モバイル ユーザーが内部ネットワーク上にいるときにPrisma Accessに接続する必要がない場合は、内部ホスト検出を有効

 ©2025 Palo Alto Networks, Inc.

GlobalProtect アプリ設定	
	にして、GlobalProtectアプリケーションが内部ネットワーク上にあるか外部ネットワーク上にあるかを判断できるようにします。 • 内部ネットワークからのみ解決できるホストのIPアドレス (IPv4 or IPv6) を入力します。 • 入力したIPアドレスに解決されるDNSホスト名を入力します。 モバイルユーザーがPrisma Accessに接続すると、GlobalProtectアプリケーションは指定されたアドレスのDNS逆引きを試みます。検索に失敗した場合、GlobalProtectアプリケーションは外部ネットワーク上にあると判断し、Prisma Accessへの接続を開始します。
内部ホスト検出を有効にする	外部ゲートウェイなしで内部ゲートウェイと内部ホスト検出が設定され、内部ホスト検出が失敗した場合にGlobalProtectアプリケーションがネットワーク検出を再試行するようにするには、「インテリジェント内部ホスト検出を有効にする」 パラメータを「yes」に設定します。
ゲートウェイ	デフォルトでは、Prisma Accessロケーションにあるすべてのゲートウェイがユーザーに利用可能です。ユーザーが接続できるようにしたい追加のGlobalProtectゲートウェイ (内部または外部) がある場合は、ここでそれらのゲートウェイを追加できます。
HIP データ収集	アプリで収集する、または収集から除外するカスタム ホスト情報プロファイル (HIP) データを定義します。このオプションを有効にすると、アプリはWindows、Mac、またはLinuxオペレーティング システムを実行しているデバイスからデータを収集します。 例えば、カスタム・チェックによって、あるアプリケーションがエンドポイントにインストールされているか、あるいは実行されているかを知ることができます。カスタム検査で収集するように定義したデータは、GlobalProtectアプリケーションが収集し、アプリが接続するときにPrisma Accessに送信する生のホスト情報データに含まれます。 カスタム チェックで収集されたデータを監視するには、HIPオブジェクトを作成します。次に、その HIP オブジェクトを HIP プロファイルに追加し、収集したデータとエンドポイント トラフィックを照合して、セキュリティ ルールを適用します。 **[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access] > [オブジェクト] > [HIP]と[HIPオ**

©2025 Palo Alto Networks, Inc.

GlobalProtect アプリ設定	
	ブジェクト]および[HIPプロファイル]へ移動します。**Prisma Access** > モバイル ユーザー コンテナ > **GlobalProtect** 構成スコープを選択します。
タイムアウト設定	• GlobalProtectセットアップ ページで、グローバル アプリ設定領域にある歯車アイコンを選択します。 • 1 回のゲートウェイ ログイン セッションの最大 **Login Lifetime**（ログイン ライフタイム）を変更します（デフォルトのログインの有効期間は 30 日間です）。この期間中、**Inactivity Logout**（アイドル タイムアウト）の期間中にゲートウェイがエンドポイントから HIP チェックを受信する限り、ユーザーのログイン状態は保持されます。この期間が過ぎると、ログインセッションが自動的にログアウトされます。 • ログイン有効期間の期限切れによりアプリ セッションが期限切れになることをユーザーに知らせるための事前通知の量を設定します。デフォルト値は30分です。許容範囲は0 ～ 60分です。 • タイムアウト通知メッセージをカスタマイズします。 • **Inactivity Logout (**非アクティブ ログアウト**)** 期間を変更して、アイドルユーザーが GlobalProtect からログアウトするまでの時間を指定します。セキュリティ ポリシーを適用して、GlobalProtectに接続している間にエンドポイントからのトラフィックを監視し、非アクティブ ログアウト期間を短く設定して非アクティブなGlobalProtectセッションをすばやくログアウトすることができます。GlobalProtect アプリが VPN トンネルを経由してトラフィックをルーティングしていない場合、またはゲートウェイが構成された期間内にエンドポイントから HIP チェックを受信しない場合、ユーザーは GlobalProtect からログアウトされます。 デフォルト値は180分です。許容範囲は5 ～ 43200分です。 • 非アクティブ状態によりアプリ セッションが期限切れになることをユーザーに知らせるための事前通知の量を設定します。デフォルト値は30分です。許容範囲は0 ～ 60分です。 • 非アクティブ通知メッセージをカスタマイズします。 • 管理者がエンド ユーザーにログアウトした場合に通知するかどうかを指定し、表示メッセージを設定します。 • **[Save(**保存**)]**をクリックします。

©2025 Palo Alto Networks, Inc.

GlobalProtect アプリ設定	
認証クッキーの送信元IPアドレスの強制	セキュリティ体制を強化するために、VPN接続設定と認証Cookieの使用制限を構成します。 • GlobalProtectセットアップ ページで、グローバル アプリ設定領域にある歯車アイコンを選択します。 • SSL VPNトンネルの自動復元を構成します。 GlobalProtectポータルでVPN接続の自動復元が有効になっている場合は、**[SSL VPN**の自動復元を無効にする]を選択して、このゲートウェイで無効にすることができます。 • 認証クッキーの送信元IPアドレス強制を設定します。 エンドポイントのIPアドレスがCookieの発効対象である元の送信元 IPアドレスに一致する場合、あるいはエンドポイントの IPアドレスが特定のネットワーク IPアドレス範囲に一致する場合にのみ、エンドポイントからの Cookie を GlobalProtectポータルあるいはゲートウェイが許可するよう、設定を行うことができます。/24 あるいは /32 など、CIDR サブネット マスクを使用してネットワークの IP アドレス範囲を定義できます。たとえば、認証Cookieが最初にパブリック 送信元IPアドレス201.109.11.10を持つエンドポイントに発行され、ネットワークIPアドレス範囲のサブネット マスクが/24に設定されている場合、認証Cookieはその後、201.109.11.0/24ネットワークIPアドレス範囲内のパブリック 送信元IPアドレスを持つエンドポイントで有効になります。 [認証Cookieの使用制限] セクションで、**[認証Cookie**の使用を制限する **(VPN**トンネルの自動復元または認証オーバーライド用**)]** を選択し、次のいずれかの条件を構成します。 • **The original Source IP for which the authentication cookie was issued (**認証用 **Cookie** の元の発効対象である送信元**IP)** を選択すると、Cookieを使用しようとするエンドポイントの公開送信元IPアドレスが、Cookieの元の発効対象であるエンドポイントの公開送信元IPアドレスと同じである場合のみ、認証用 Cookieが有効になります。 • **The original Source IP network range (**元の送信元**IP**ネットワーク範囲**)** を選択すると、Cookieを使用しようとするエンドポイントの公開送信元IPアドレスが、指定されたネットワークのIPアドレス範囲内である場合にのみ、認証用Cookieが有効になります。Source IPv4 Netmask (送信元IPv4ネットマスク)あ

©2025 Palo Alto Networks, Inc.

GlobalProtect アプリ設定	
	るいはSource IPv6 Netmask (送信元IPv6ネットマスク)を入力し、認証用Cookieが有効であるネットワークIPアドレス範囲のサブネット マスクを定義します (例えば、32あるいは128)。

GlobalProtectを無効にするチケットリクエスト

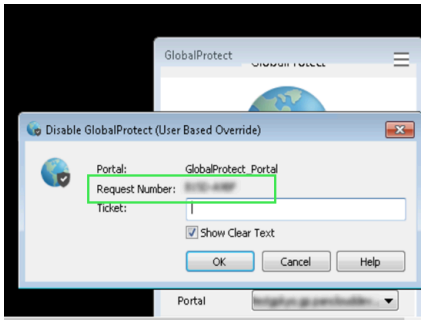
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

ユーザーがGlobalProtectを直接無効にできるようにする代わりに、ユーザーがGlobalProtectを無効にするためのチケットを作成できるようにすることができます。GlobalProtectの管理者は、その後、各特定のユーザーがGlobalProtectを無効にすることを許可するかどうかを決定できます。

動作の仕組み

この機能を設定した後、GlobalProtectを無効にするためのチケットリクエストのワークフローは次のとおりです。

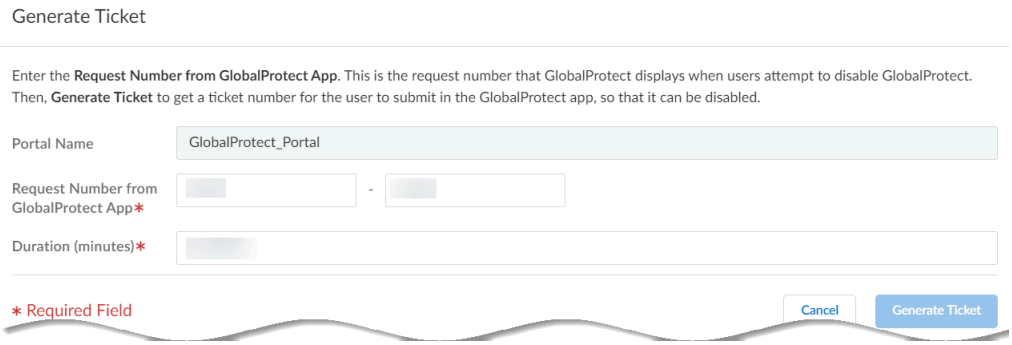
- ユーザーがGlobalProtectアプリケーションでGlobalProtectを無効にしようとしています。GlobalProtectはユーザーにリクエスト番号を表示します。



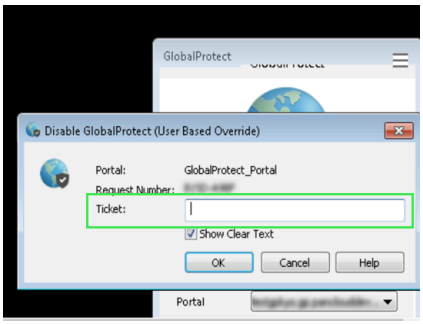
- ユーザーはリクエスト番号をGlobalProtect管理者と共有します。

©2025 Palo Alto Networks, Inc.

- GlobalProtectの管理者はログインし、リクエスト番号を使用してチケットを生成します。



- GlobalProtectプロテクト管理者は、ユーザーとチケット番号を共有します。ユーザーはアプリにチケット番号を入力してGlobalProtectを無効にします。



セットアップ

- Strata Cloud Manager
- Panorama

GlobalProtectを無効にするチケットリクエスト(Strata Cloud Manager)

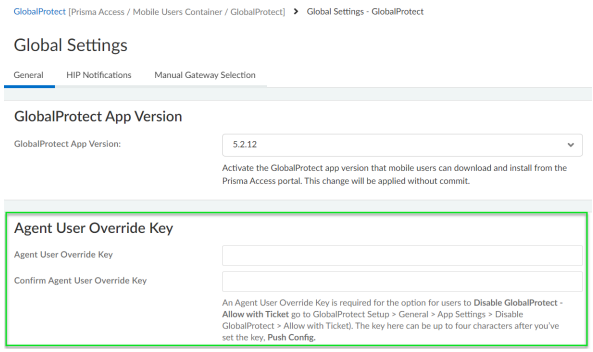
STEP 1 | エージェントオーバーライドキーを設定する

チケット リクエストのオプションを有効にして GlobalProtect を無効にする前に、まずエージェント ユーザー オーバーライド キーを設定する必要があります。

[Workflows (ワークフロー)] > [Prisma Accessセットアップ] > [GlobalProtect] > [GlobalProtect App (GlobalProtectアプリケーション)] > [Global App 設定] をセットアップ

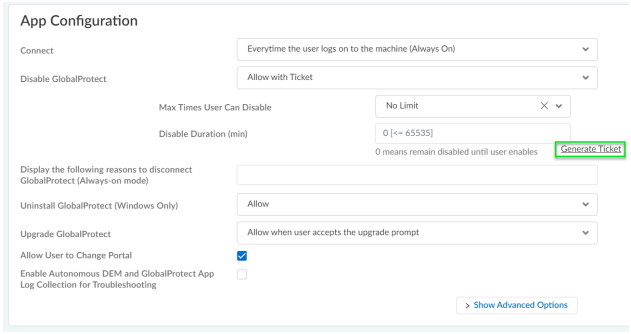
©2025 Palo Alto Networks, Inc.

し、4文字のキーを入力して **[Agent Override Key (エージェント オーバーライド キー)]**を設定します。



STEP 2 | チケットでGlobalProtectを無効にできるようにする

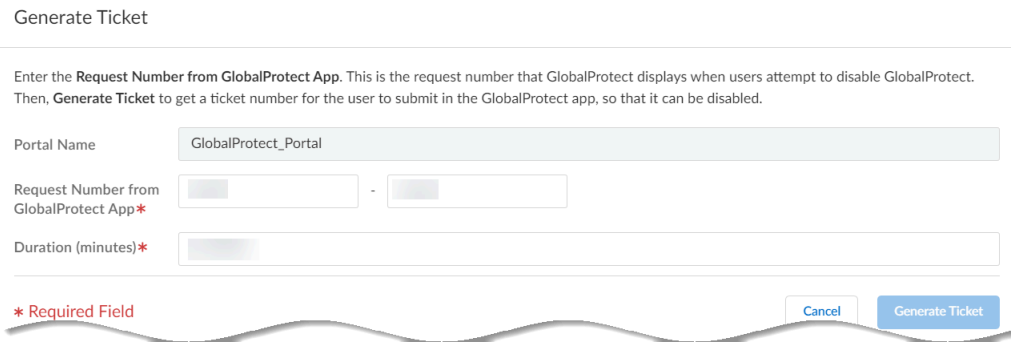
[Workflows (ワークフロー)] > **[Prisma Accessセットアップ]** > **[GlobalProtect]** > **[GlobalProtect App]** > **[App Settings (アプリケーション設定)]** > **[App Configuration (アプリケーション設定)]** > **[Disable GlobalProtect (GlobalProtectを無効にする)]**へと移動し、オプションを**[チケットで許可]**に設定します。



STEP 3 | チケットを生成する

エージェントオーバーライドキー と チケットで許可するオプションを設定すると、 チケットを生成できるようになります。

ユーザーがアプリで GlobalProtect を無効にしようとすると、GlobalProtect はリクエスト番号を表示します。そのユーザーに対して GlobalProtect を無効にするためのチケットを生成するには、ここでそのリクエスト番号を送信してください。



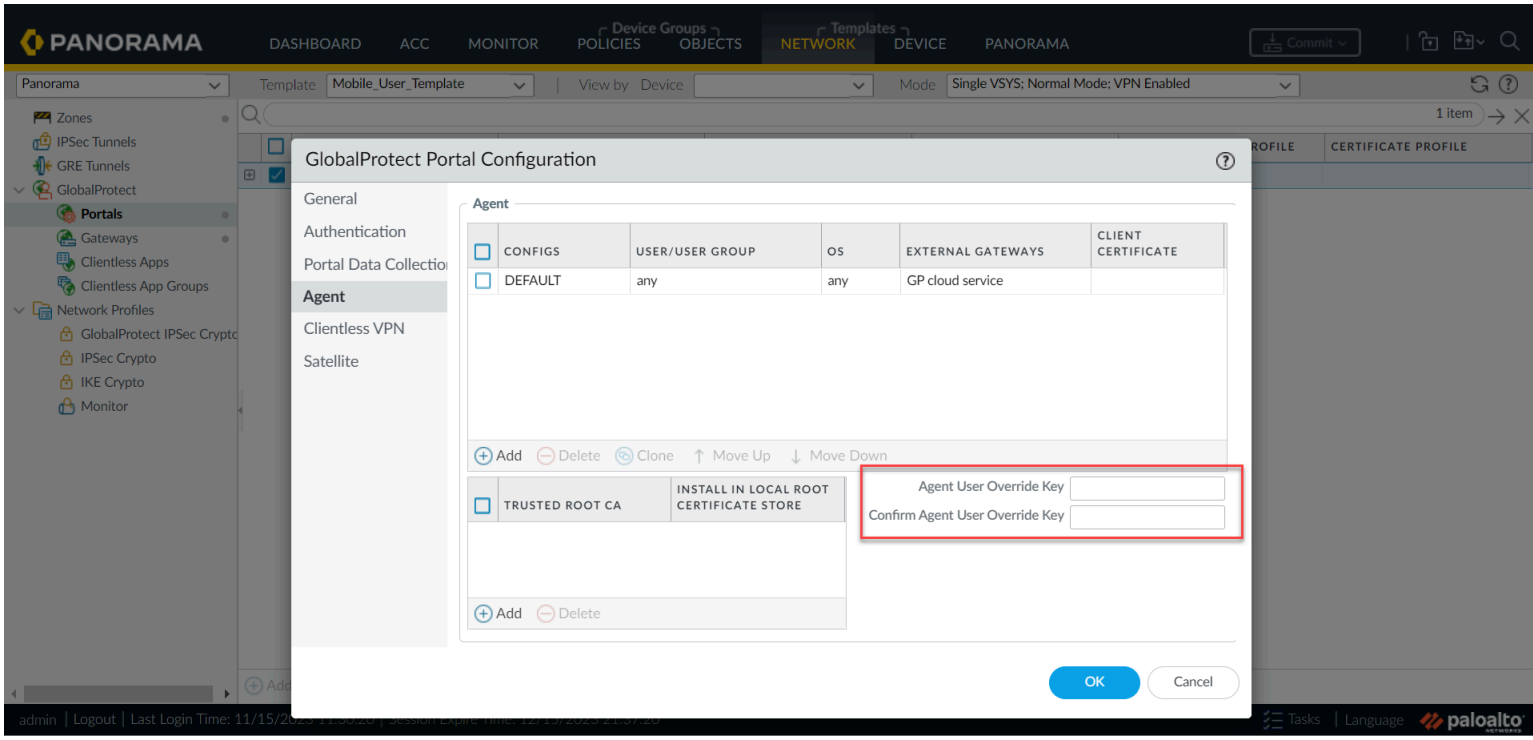
 ©2025 Palo Alto Networks, Inc.

GlobalProtectを無効にするチケットリクエスト(Panorama)

STEP 1 | エージェントオーバーライドキーを設定する

チケット リクエストのオプションを有効にして GlobalProtect を無効にする前に、まずエージェント ユーザー オーバーライド キーを設定する必要があります。

[Network (ネットワーク)] > **[GlobalProtect]** > **[Portals (ポータル)]**へと移動し、オーバーライド キーを設定する接続名を選択します。エージェントを選択し、キーを入力してエージェント オーバーライド キーを設定します。

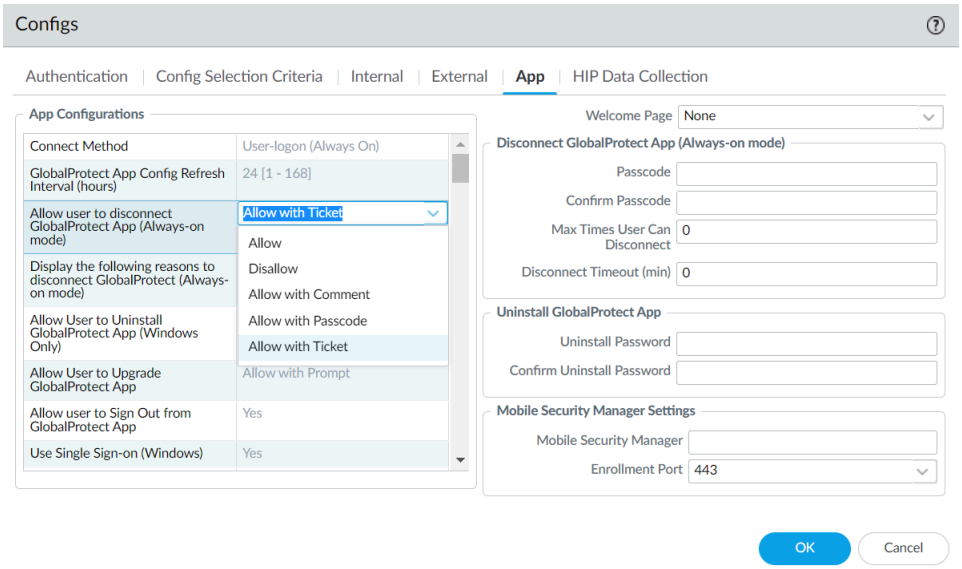


STEP 2 | チケットでGlobalProtectを無効にできるようにする

[Network (ネットワーク)] > **[GlobalProtect]** > **[Portals (ポータル)]**へと移動し、 ユーザーの切断を許可する接続名を選択します。**[Agent (エージェント)]**を選択し、 **[Config (コンフィグ)]**選びます。次に、 **[App (アプリ)]** > **[App Configurations (アプリ構成)]** > **[Allow user to disconnect GlobalProtect App (Always-on mode) (ユーザーがGlobalProtectアプリケーショ**

©2025 Palo Alto Networks, Inc.

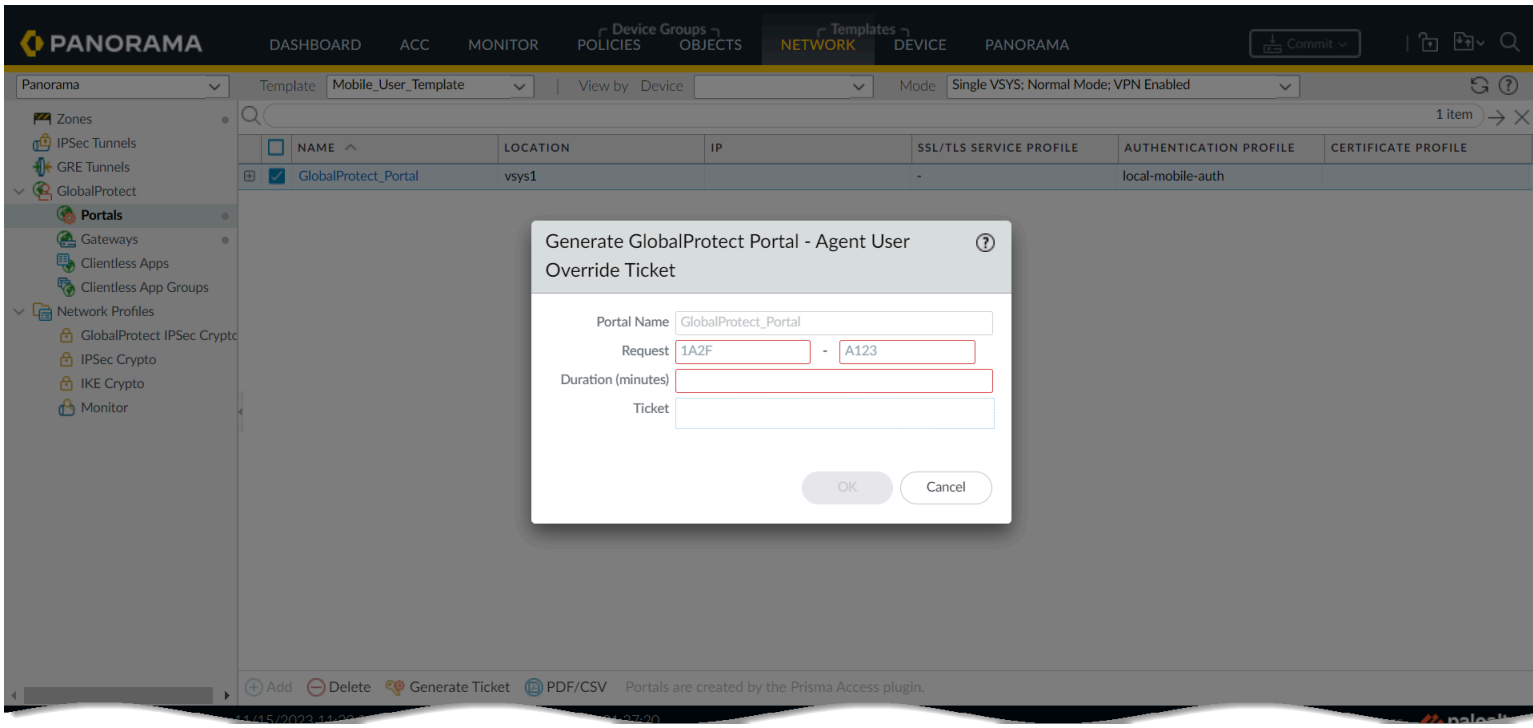
ンを切断できるようにする(常時オンモード)]]を選択し、オプションを **[Allow with Ticket (チケットで許可)]**に設定します。



STEP 3 | チケットを生成する

エージェントオーバーライドキー と チケットで許可するオプションを設定すると、 チケットを生成できるようになります。

ユーザーがアプリで GlobalProtect を無効にしようとすると、GlobalProtect はリクエスト番号を表示します。そのユーザーに対して GlobalProtect を無効にするためのチケットを生成するには、ここでそのリクエスト番号を送信してください。



 ©2025 Palo Alto Networks, Inc.

GlobalProtectプレ ログオン

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Accessのライセンス ❑ マシン証明書をインストールするためのエンドポイントへの管理者アクセス ❑ エンドポイントに導入された信頼できるPKI証明書

プレ ログオンとは、ユーザーがログインする前に VPN トンネルを確立する接続方式のことです。このプレ ログオンの目的は、エンドポイントの電源が入ったらできるだけ早くエンドポイント（ユーザーではなく）を認証し、ドメイン スクリプトや他のタスクを実行することです。マシン証明書により、エンドポイントが GlobalProtect ゲートウェイとの VPN トンネルを確立できるようになります。IT 管理者は一般的に、ユーザーのためにエンドポイントを準備しながらマシン証明書をインストールします。ユーザーがログインしていないため、プレ ログオンVPN トンネルでは一般的なログオン前ユーザー名が使用されます。エンドポイントがリソースにアクセスできるようにするには、プレ ログオンのユーザーに一致するセキュリティ ポリシールールを作成する必要があります。これらのポリシー ルールでは、DHCP、DNS、特定のActive Directory(アクティブ ディレクトリ)サービス、ウイルス対策、その他の更新サービスなど、システムを起動するための基本的なサービスのみへのアクセスを許可する必要があります。ユーザーがゲートウェイに認証されると、GlobalProtectアプリケーションはそのユーザーにVPNトンネルを再割り当てします。Prisma AccessのIPアドレス マッピングは、プレ ログオンのエンドポイントから認証されたユー ザーに変更されます。

プレ ログオン認証に使用される証明書は、エンドポイントの個人証明書ストアに存在します。信頼できるサードパーティCA、自己署名CA、または内部PKI CAを使用して、マシン証明書を発行します。Prisma Accessにログインする前にエンドポイントからトンネルを確立するための認証方法としてマシン証明書を構成し、プレ ログオンのCA証明書を含む証明書プロファイルを作成する必要があります。

- Strata Cloud Manager
- Panorama

GlobalProtectプレ ログオン (Strata Cloud Manager)

サードパーティのルート**CA**証明書をインポートする

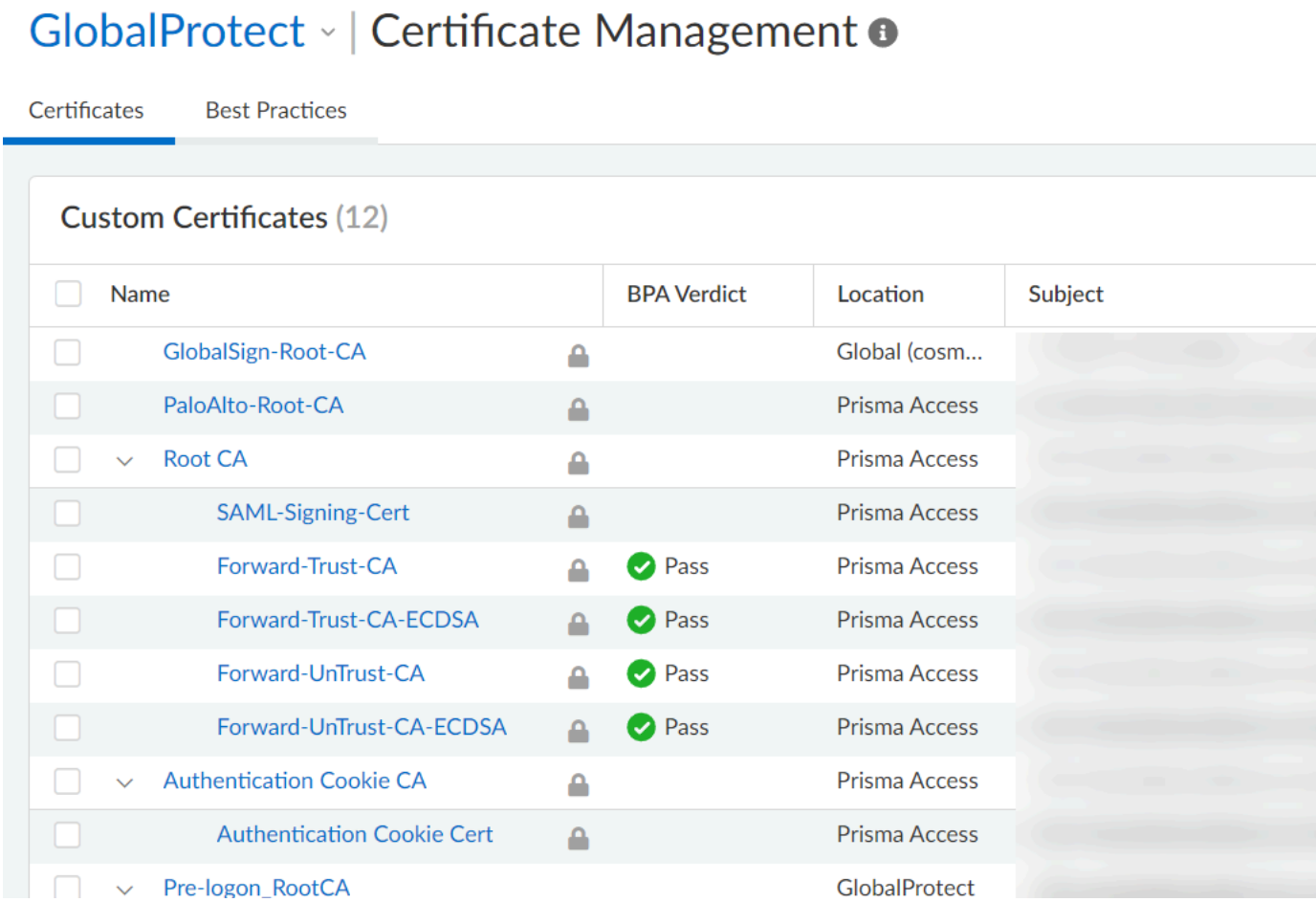
エンドポイントからログインする前にトンネルを確立するための認証方法としてマシン証明書を使用します。Prisma Access

STEP 1 | [管理] > [設定] > **[NGFWとPrisma Access]** > [オブジェクト の証明書 > 管理] を選択します。**Prisma Access**設定スコープを選択します。

GlobalProtectモバイルユーザーのために証明書をインポートしていることを確認してください。

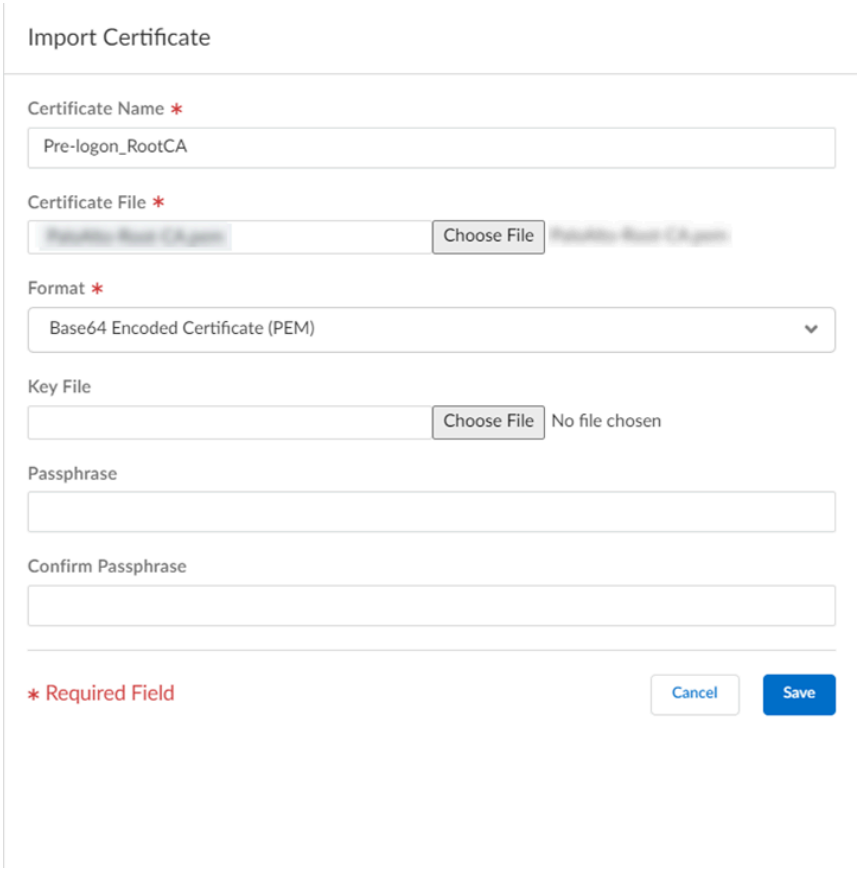
 ©2025 Palo Alto Networks, Inc.

STEP 2 | カスタム証明書をインポートします。



 ©2025 Palo Alto Networks, Inc.

STEP 3 | 値を入力し、証明書設定を保存します。



プレ ログオン証明書プロファイルを作成する

自己署名のルートCAを含む証明書プロファイルを作成します。このCAは、プレ ログオン時にGlobalProtectモバイルユーザーによってマシン証明書を検証します。

STEP 1 | **[管理] > [設定] > [NGFWとPrisma Access] > [オブジェクト の証明書 > 管理]** を選択します。**Prisma Access**設定スコープを選択します。

STEP 2 | プロファイルを追加します。

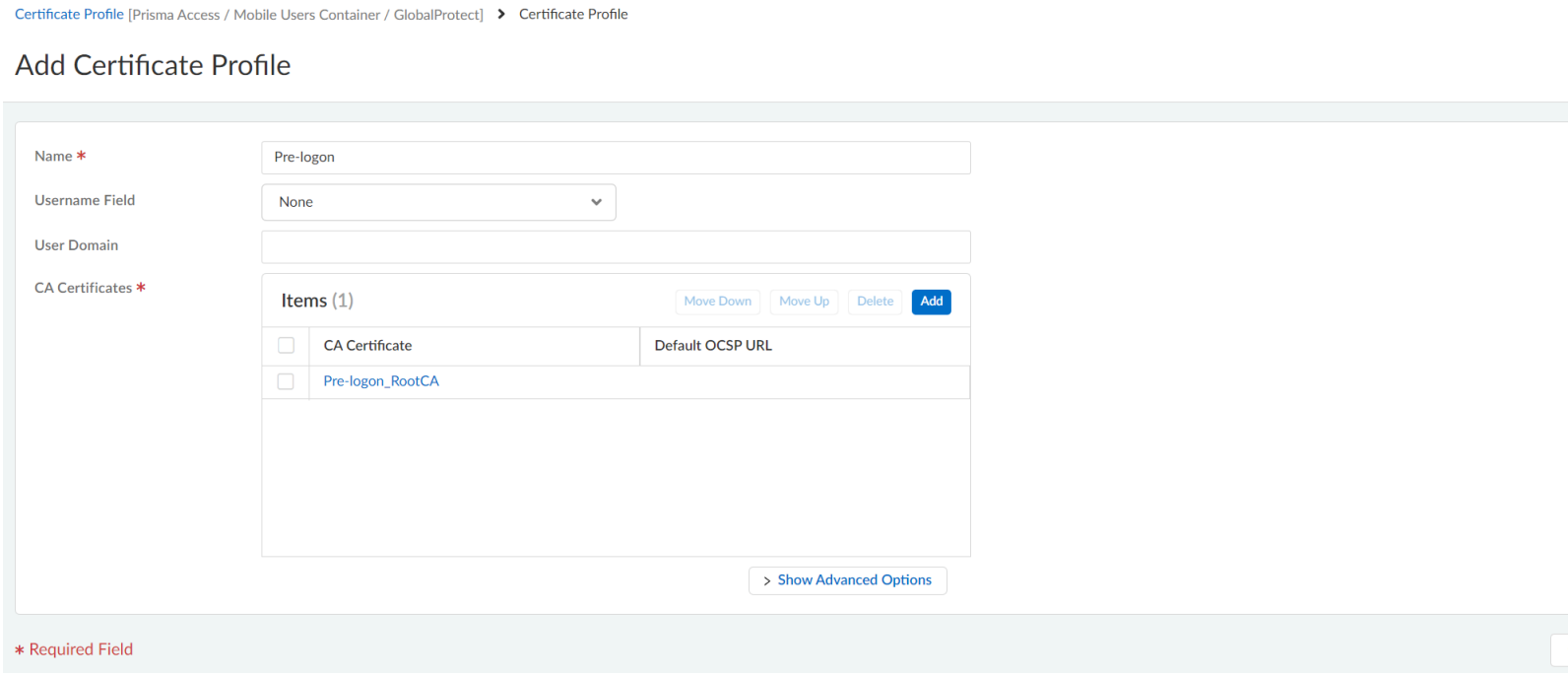
©2025 Palo Alto Networks, Inc.

STEP 3 | 値を入力してください。

1. ユーザー名フィールドが**None**であることを確認して、証明書がユーザーにマッピングされないようにします。

   ユーザー名フィールドは、ステップ2で述べた任意の認証方法またはクライアント証明書によって証明書を認証する場合、***None***にすることはできません。

2. ステップ1でインポートしたルートプレ ログオンCA証明書を追加します。
3. 証明書プロファイル設定を保存します。



プレ ログオンの**GlobalProtect**ポータルの設定

GlobalProtectポータルを構成して、マシン証明書で接続を認証します。

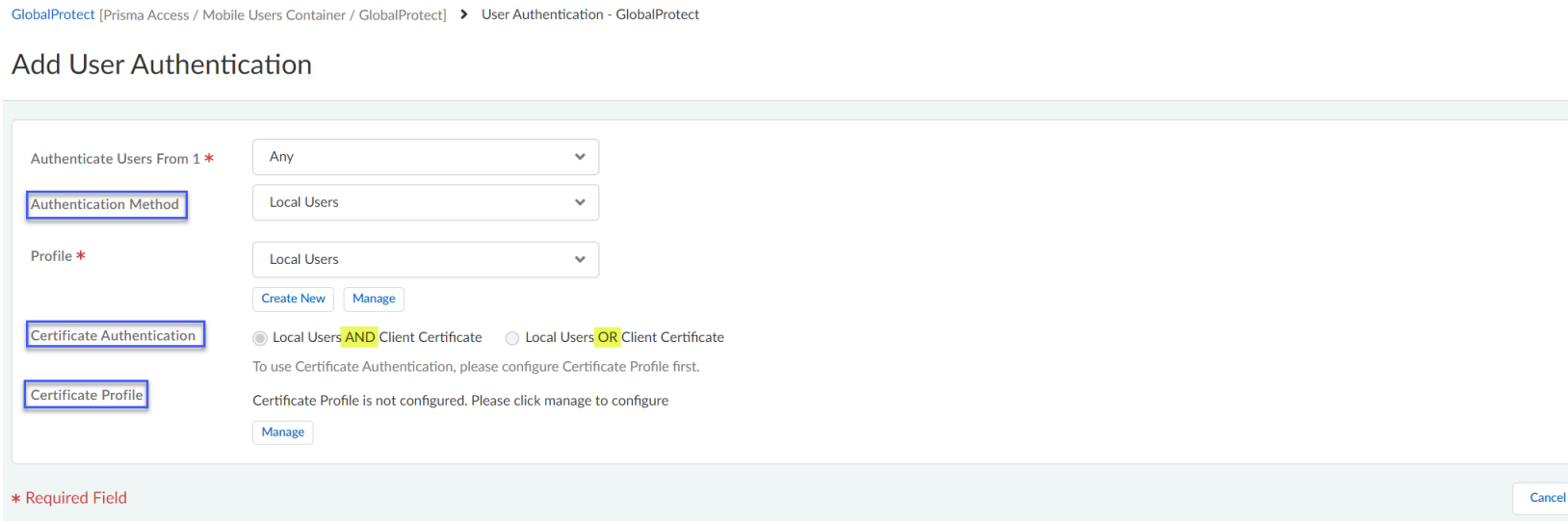
STEP 1 | **[Workflows (ワークフロー)] > [Prisma Accessセットアップ] > [GlobalProtect] > [インフラストラクチャ]**を選択します

 ©2025 Palo Alto Networks, Inc.

STEP 2 | ユーザー認証設定を編集します。

GlobalProtectがサポートする認証方法、あなたが作成したプレ ログオン証明書プロファイル、および証明書認証を選択してください。

*GlobalProtect*がサポートする任意の証明書認証を選択してください。

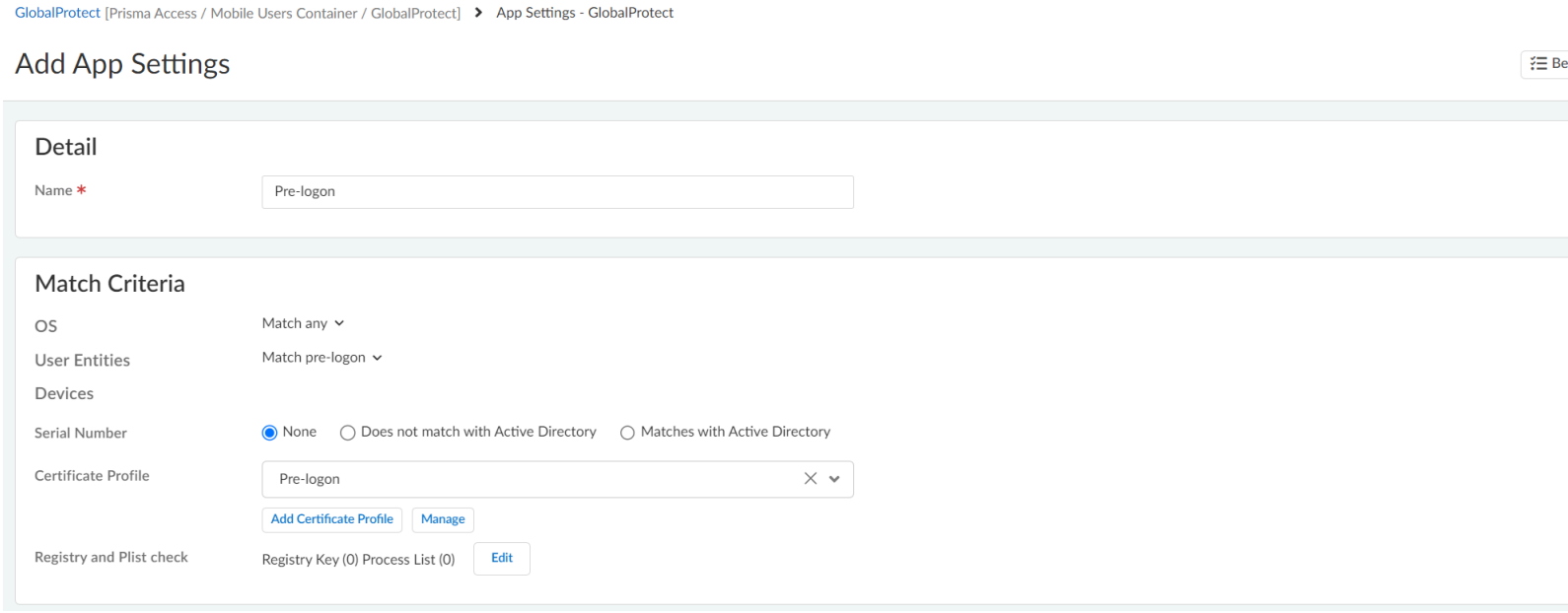


 ©2025 Palo Alto Networks, Inc.

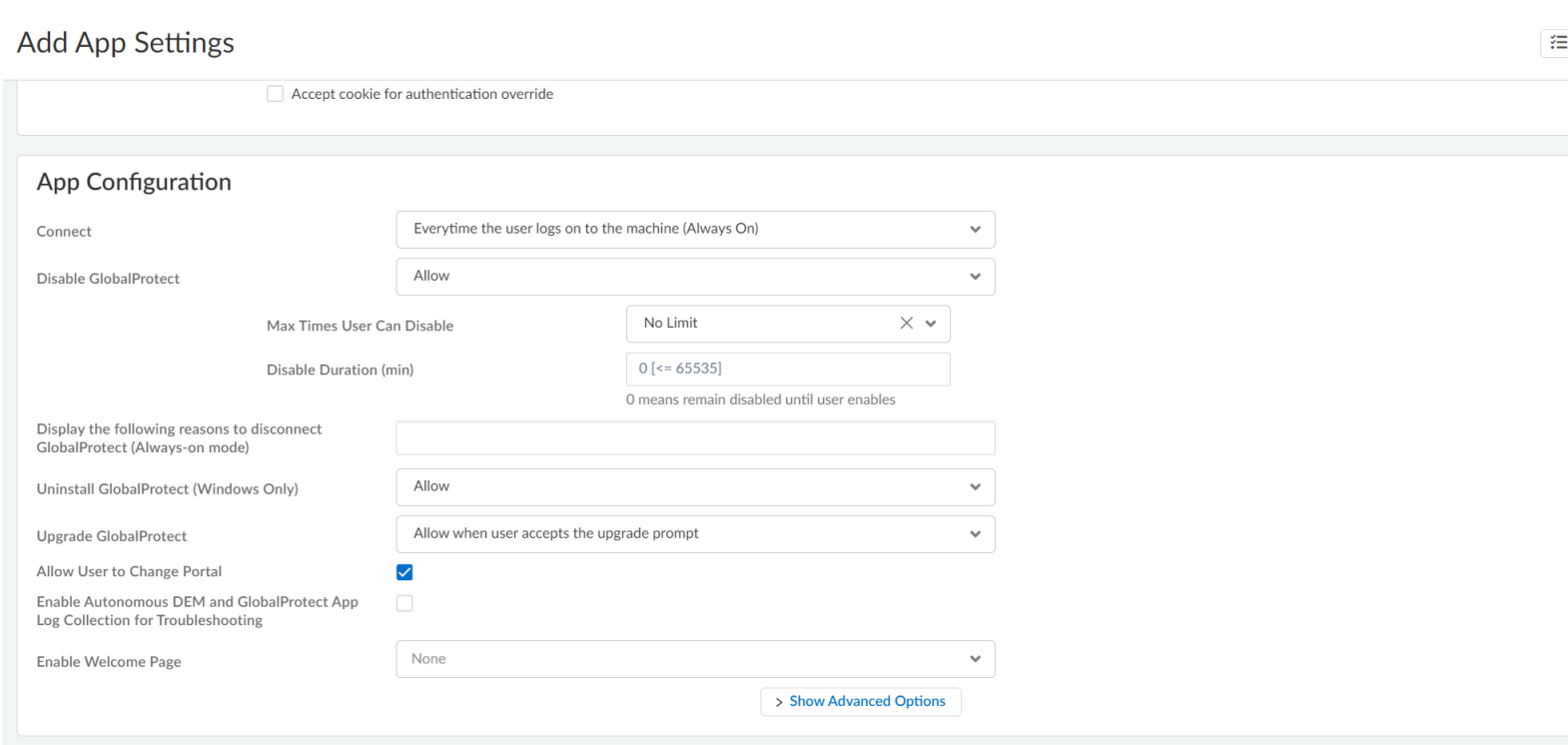
STEP 3 | GlobalProtectアプリケーションの設定をプレ ログオン基準に合わせて構成します。

1. **GlobalProtect**アプリケーションタブに移動します。
2. アプリケーション設定を追加

> 値を入力する際は、プレ ログオンユーザーエンティティとプレ ログオン証明書プロファイルが一致することを確認してください。

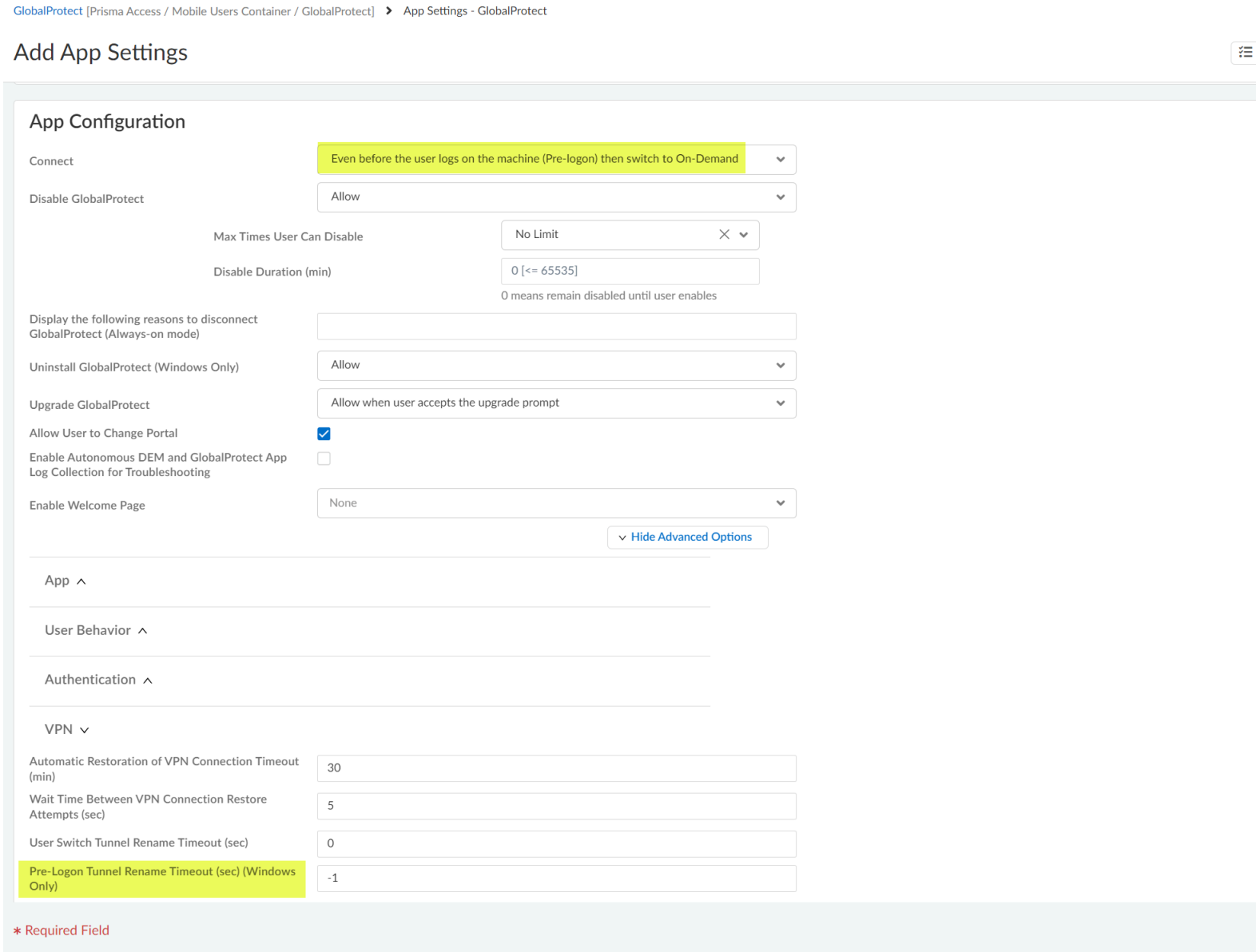


- プレ ログオンの接続方法を選択してください。



 ©2025 Palo Alto Networks, Inc.

- **[Even before the user logs on the machine (Pre-logon) then switch to On-Demand (**ユーザーがマシンにログオンする前でも（プレ ログオン）、オンデマンドに切り替える**)]**を選択した場合は、**[Pre-logon Tunnel Rename Timeout (**プレ ログオン トンネル リネーム タイムアウト**)]** の値を **-1** に設定します。このフィールドを編集するためにVPNの詳細オプションを表示します。



3. プレ ログオンアプリ設定を他のアプリ設定の上に移動します。
4. 認証されたユーザーのために、他のすべてのアプリ設定を編集します。

   接続メソッドと証明書プロファイルを更新します。

STEP 4 | 変更をPrisma Accessにプッシュします。

マシン証明書をインストールする**—Windows**

エンドポイントにマシン証明書をインストールします。これは認証に使用されます。

 ©2025 Palo Alto Networks, Inc.

STEP 1 | PKIから自己署名のルートCA証明書をバイナリエンコード証明書（**DER**）形式でエクスポートします。

STEP 2 | Windowsマシンに証明書ファイルを転送します。

STEP 3 | ローカル マシンの **Trusted Root Certification Authorities (**信頼できるルート認証局**)** ストアに、ルート プレ ログオンCA証明書をインストールします。

STEP 4 | ローカルマシンストアの場所にプレ ログオンマシン証明書をインストールします。

STEP 5 | インストールを進めて、プロンプトが表示されたらパスフレーズを入力し、インストールを完了してください。

STEP 6 | GlobalProtectポータルに接続し、ホストからすべてのクッキーを削除します。

STEP 7 | (任意) マシンからサインアウトし、グローバルプロテクトのログを表示して、プレ ログオン接続を確認します。

GlobalProtectプレ ログオン (Panorama)

プレ ログオンの証明書とプロファイルを設定する

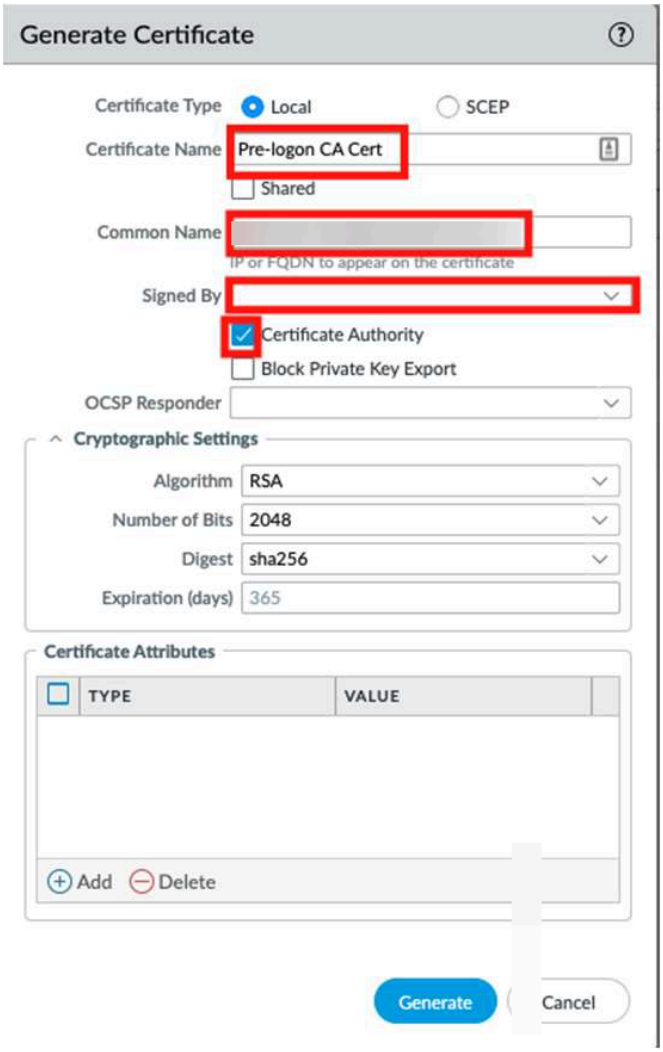
Prisma Accessにログインする前にエンドポイントからトンネルを確立するための認証方法としてマシン証明書を構成し、プレ ログオンのCA証明書を含む証明書プロファイルを作成します。

©2025 Palo Alto Networks, Inc.

STEP 1 | 自己署名CAを設定し、それを使用してモバイル ユーザー テンプレートでマシン証明書を生成します。**[Device (デバイス)]** > **[Certificate Management (証明書の管理)]** > **[Certificates (証明書)]**に移動します。

[Mobile_User_Template]を使用しており、 [ロケーション] が **[Shared (共有)]**に設定されていることを確認してください。

1. 証明書に名前を付けます (例:**Pre-logon CA Cert**)。
2. **Common Name**（共通名）に、「192.168.2.1」などの名前を入力します。
   共通名 (CN) は、証明書で保護するドメイン名 (www.yourdomainname.com など) です。
3. [署名者] フィールドを空白の ままにして、**[Certificate Authority (認証局 - CA)]**チェックボックスをクリックします。
4. プレ ログオン接続で使用する証明書を生成します 。

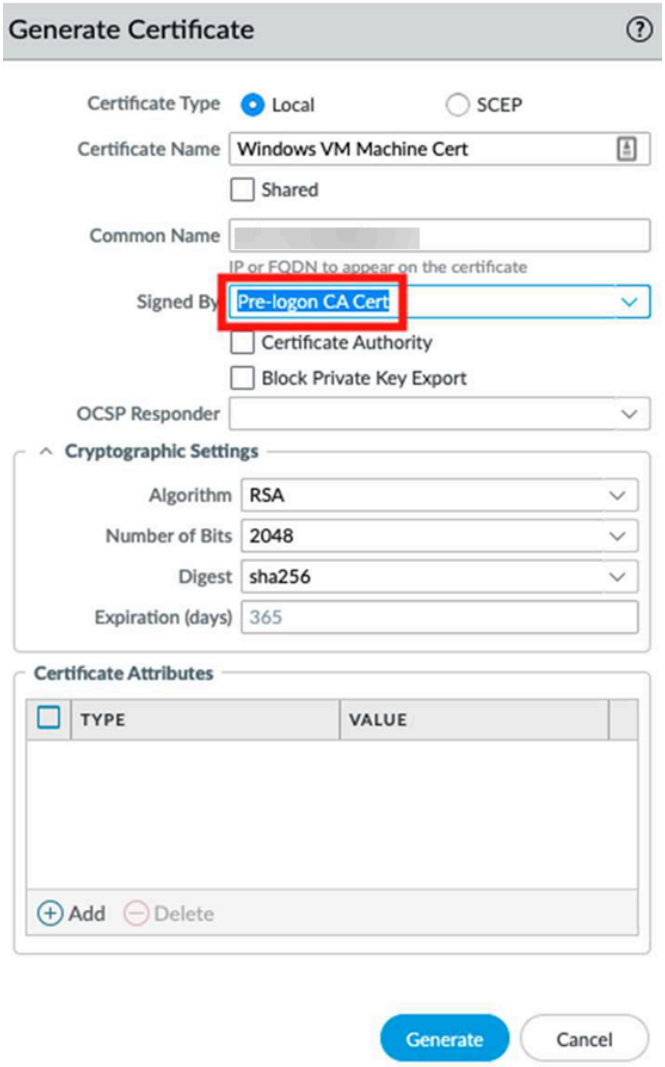


©2025 Palo Alto Networks, Inc.

STEP 2 | 自己署名CAを構成した後、マシン証明書を生成します。

1. 証明書名 と 共通名を入力します。
2. [署名者] ドロップダウンで 、手順 1 で作成した プレ ログオン**CA**証明書 を選択します。
3. 後 Windowsマシンにインストールする **Windows VM**マシン証明書 を生成します 。

   この証明書は、プレ ログオンCAの子です。

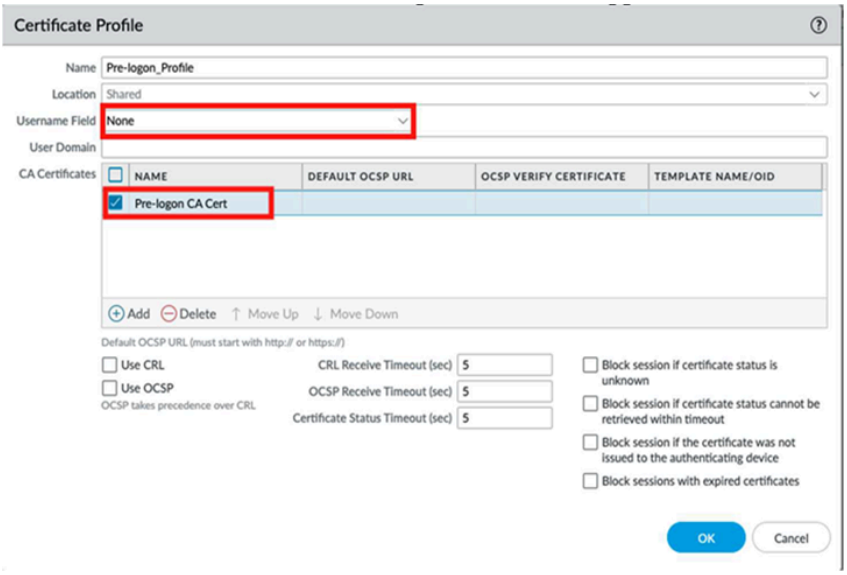


STEP 3 | プレ ログオンのCA証明書を含む証明書プロファイルを作成するには、**[Device (デバイス)] > [Certificate Management (証明書管理)] > [Certificate Profile (証明書プロファイル)]**に移動します。

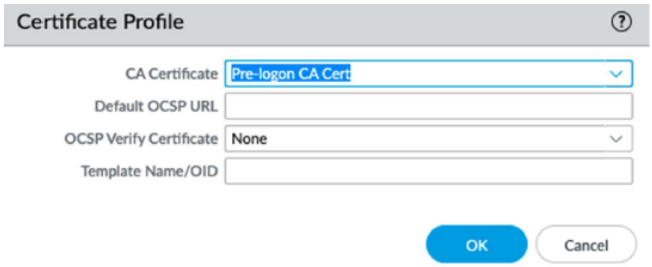
このCAを使用して、プレ ログオンのトンネル初期化中にGlobalProtectクライアントによって提示されたマシン証明書を検証します。

©2025 Palo Alto Networks, Inc.

STEP 4 | プロファイルを作成して名前を付けます。ユーザー名フィールドが**None**であることを確認して、証明書がユーザーにマッピングされないようにします。



STEP 5 | **[CA** 証明書]の下で[追加]を選択し、ドロップダウンから[プレ ログオン**CA**証明書]を選択します。



STEP 6 | **[OK]**を選択し、もう一度 **[OK]** を選択します。

プレ ログオンの**GlobalProtect**ポータルの設定

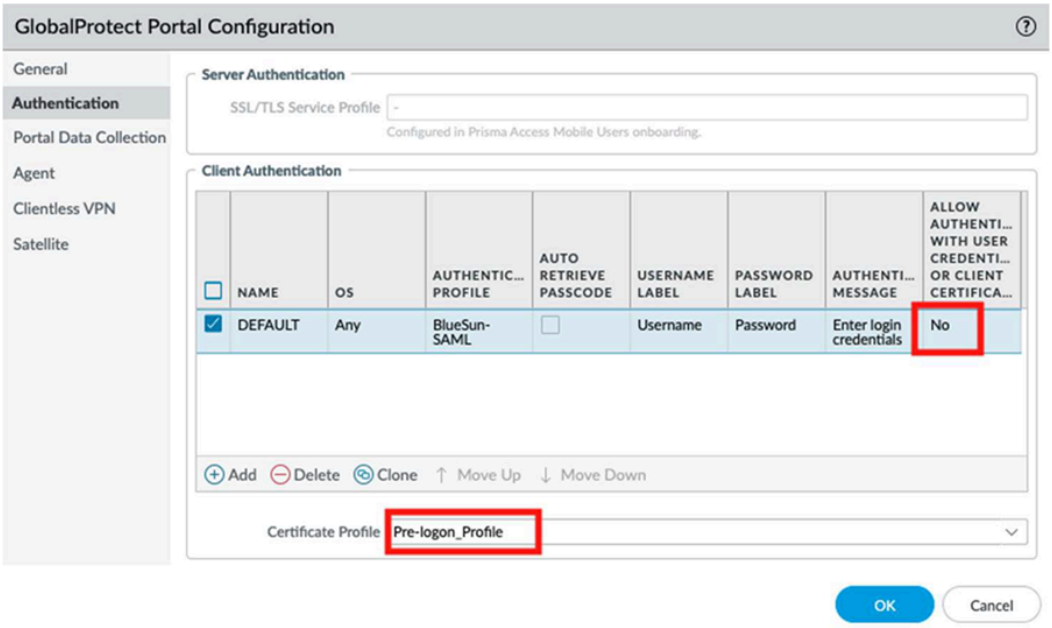
GlobalProtectポータルを構成して、マシン証明書で接続を認証します。

STEP 1 | **[**ネットワーク**] > [GlobalProtect] > [**ポータル**] > [GlobalProtect_Portal] > [Authentication (**認証**)]**に移動します。

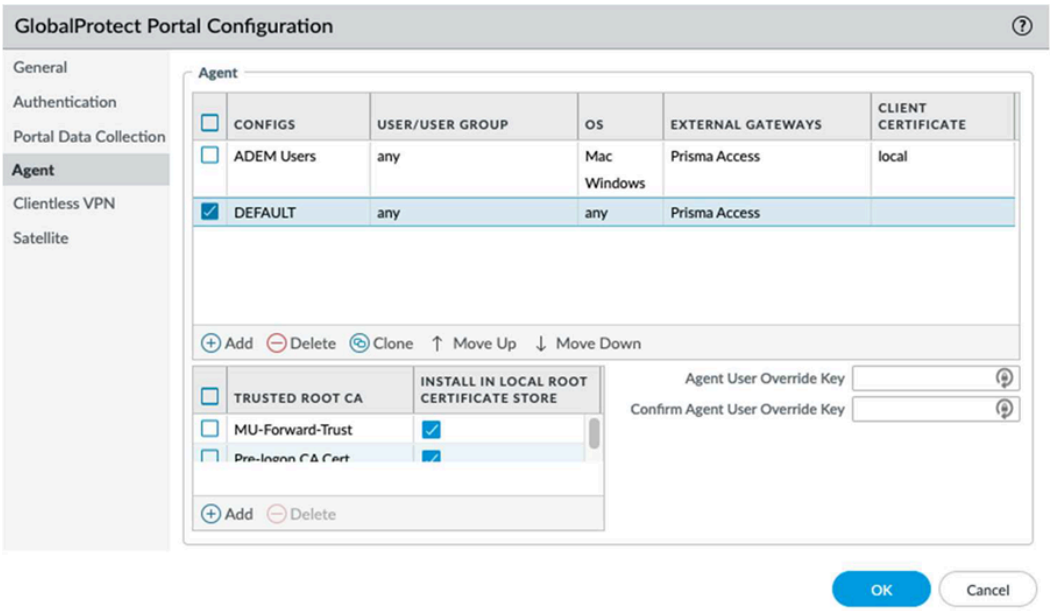
STEP 2 | **[Allow Authentication with User Credentials OR Client Certificate (**ユーザー資格情報またはクライアント証明書による認証を許可する**)]**で **[No]** を選択して、証明書ベースの認証のみを適用します。

©2025 Palo Alto Networks, Inc.

STEP 3 | [証明書プロファイル]で作成した**Pre-logon_Profile** を選択し、**[OK]**をクリックします。



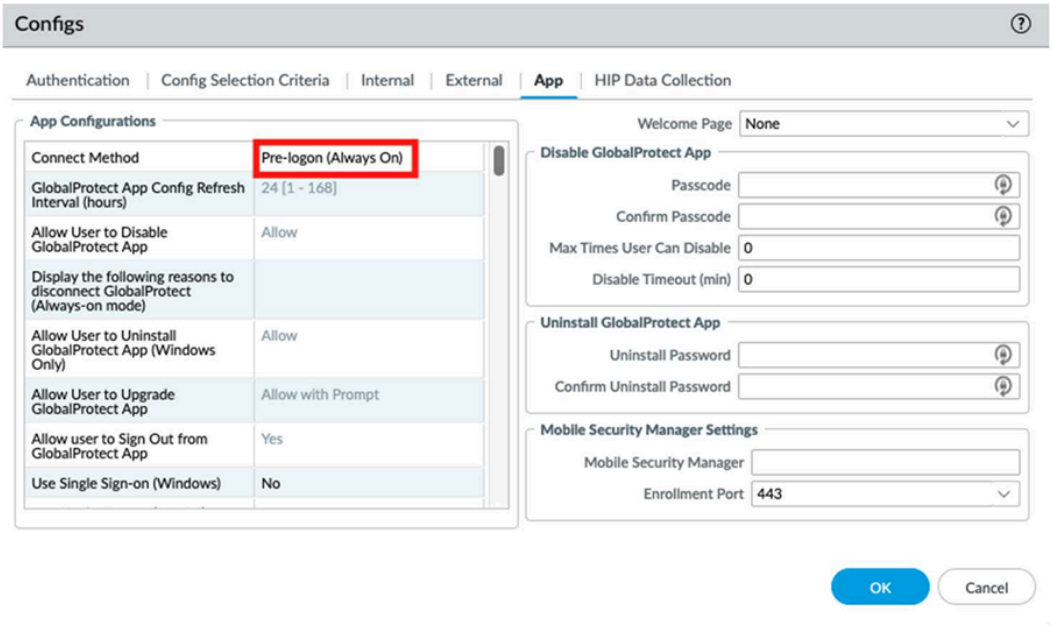
STEP 4 | エージェント を選択し、認証されたユーザーのエージェント構成を開きます。



STEP 5 | **App**（アプリケーション）タブを選択します。

©2025 Palo Alto Networks, Inc.

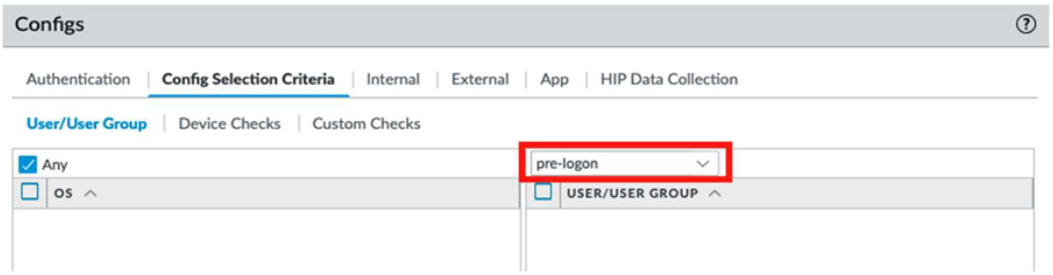
STEP 6 | [プレ ログオン (常にオン)]を選択し、**[OK]** を選択してエージェント領域に戻ります。



STEP 7 | エージェント領域で、デフォルト設定を複製します 。マシン証明書認証の接続方法と一致するように、構成名を [プレ ログオン] に変更します。

STEP 8 | 新しく複製されたエージェント設定を選択します。

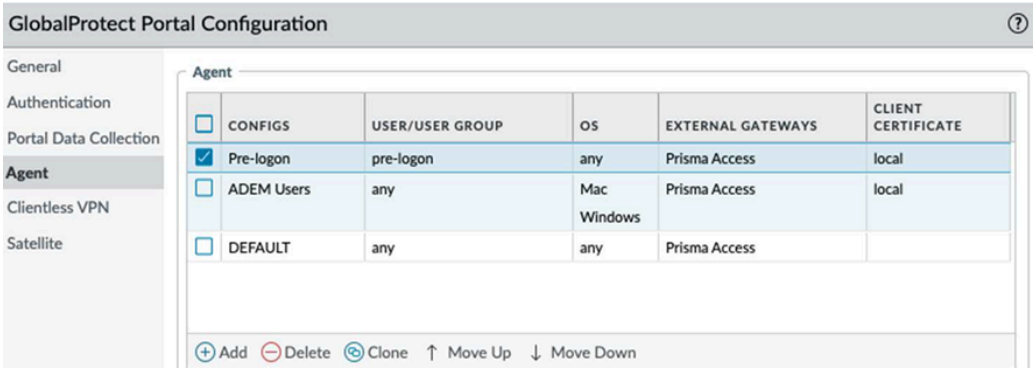
STEP 9 | **Config Selection Criteria** (設定選択条件) を選択します。ユーザー/ユーザー グループ 構成の下で、 ユーザー/ユーザー グループ 構成ボックスの上にあるドロップダウンからプレ ログオンを選択し、構成が[任意]に設定されていることを確認します。



STEP 10 | 必要に応じてアプリの設定を構成し、**OK**を選択します。ログオン前と現在の設定の両方に対して、プレ ログオンの接続方法を選択していることを確認してください。

©2025 Palo Alto Networks, Inc.

STEP 11 | プレ ログオンエージェント構成を **CONFIGS** リストの先頭に移動し、ログオン前の条件と最初に一致するようにします。



STEP 12 | **[OK]** をクリックしてポータルの設定を保存します。

Prisma Access GlobalProtectゲートウェイを構成する

Panorama Managed Prisma AccessでGlobalProtectゲートウェイを構成します。

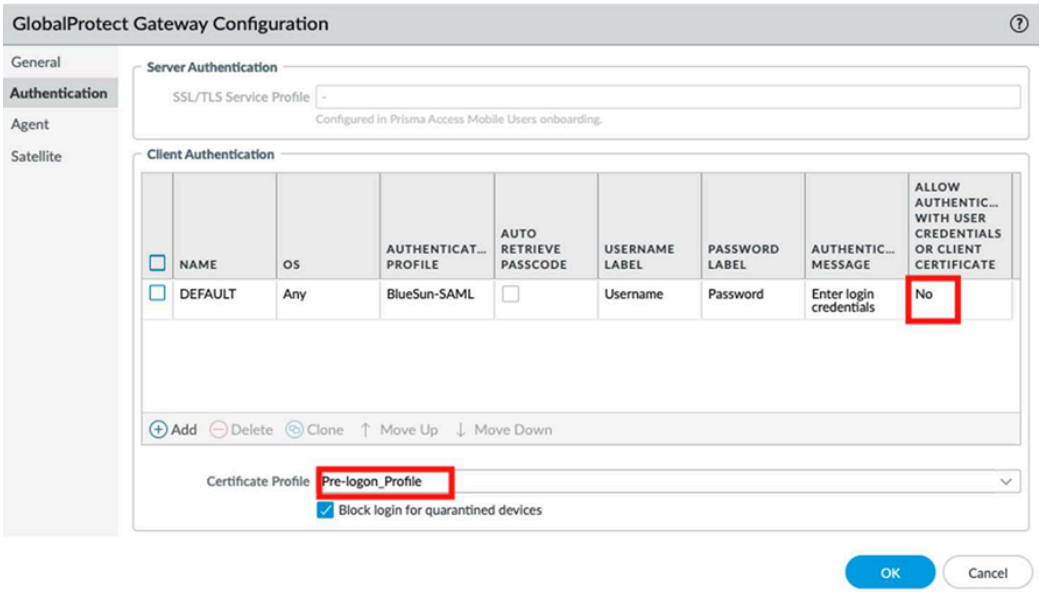
この設定では、証明書ベースの認証のみが適用されます。

STEP 1 | [ネットワーク] > **[GlobalProtect** > ゲートウェイ] > **[GlobalProtect_External_Gateway** > **Authentication (**認証**)]**に移動します。

STEP 2 | デフォルトの 認証方法を選択します。

すでにクライアント認証 (SAML など) が設定されている場合は、**Default**の代わりにそれを選択します。

STEP 3 | **[Allow Authentication with User Credentials or Client Certificate (**ユーザー資格情報またはクライアント証明書による認証を許可する**)]** で [いいえ]を選択し、**[OK]** を選択して構成を保存します。



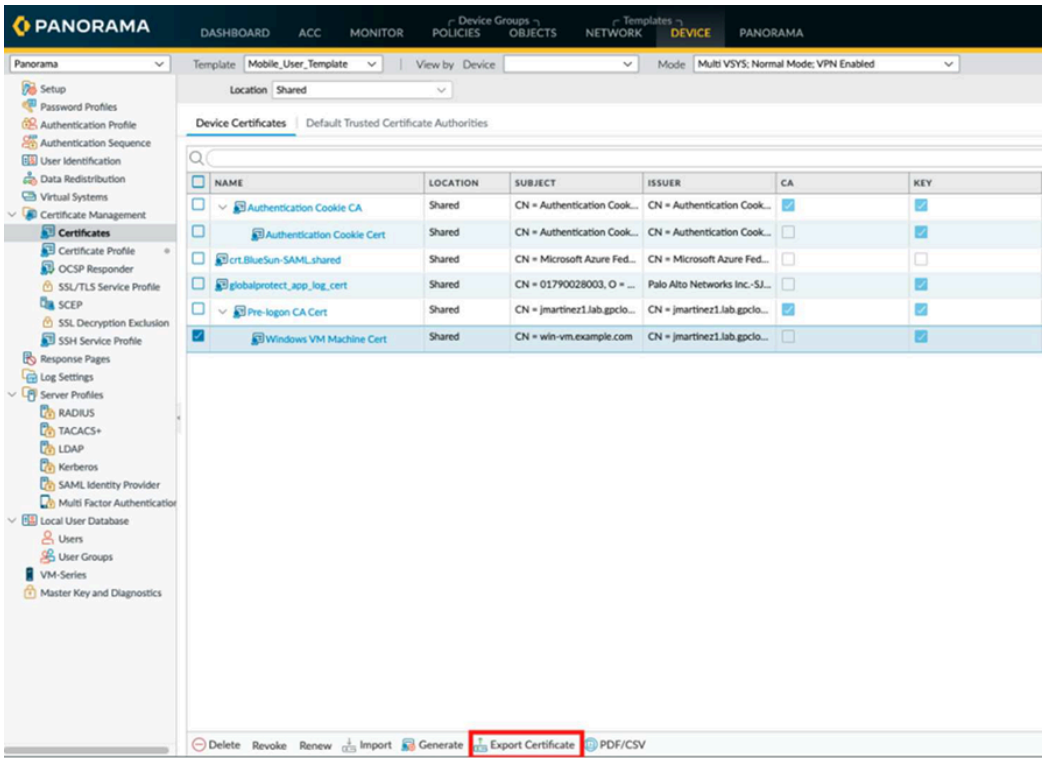
 ©2025 Palo Alto Networks, Inc.

マシン証明書のインストール **- Windows**

認証に使用されるマシン証明書をモバイル ユーザーのエンドポイントにインストールします。

STEP 1 | **[Device (デバイス)]** > **[Certificate Management (証明書の管理)]** > **[Certificates (証明書)]**に移動します。

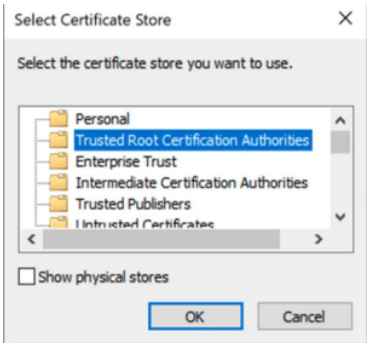
STEP 2 | まだMobile_User_Template内にいることを確認してください。以前に作成した**Windows VM** マシン証明書を選択し、[証明書のエクスポート]を選択して、パスフレーズ付きのPKCS12ファイルとしてダウンロードします。



STEP 3 | ログオン前のCA証明書をbase64でエンコードされた証明書としてエクスポートします。

STEP 4 | Windowsマシンに証明書ファイルを転送します。

STEP 5 | ローカル マシンの **Trusted Root Certification Authorities (信頼できるルート認証局)** ストアに、ルート プレ ログオンCA証明書をインストールします。



 ©2025 Palo Alto Networks, Inc.

STEP 6 | ローカルマシンストアの場所にプレ ログオンマシン証明書をインストールします。権限を完了し、[次へ] を選択してインストールを続行します。

STEP 7 | 証明書のファイル名を検証し、[次へ]を選択します。

STEP 8 | Panoramaからの証明書のエクスポート時に使用したパスフレーズであるパスワードを入力し、[次へ]を選択します。

STEP 9 | [証明書ストア] ダイアログで、[証明書をすべて次のストアに配置する]を選択し、[参照]を選択します。

STEP 10 | マシン証明書をインストールする 個人用フォルダーを選択し、**[OK]**を選択します。

STEP 11 | インストールを続行するには、**[Next (次へ)]** を選択します。

STEP 12 | GlobalProtectポータルに接続し、ホストからすべてのクッキーを削除します。

STEP 13 | (任意) マシンからサインアウトし、グローバルプロテクトのログを表示して、プレ ログオン接続を確認します。

GlobalProtect — クライアントレス VPN

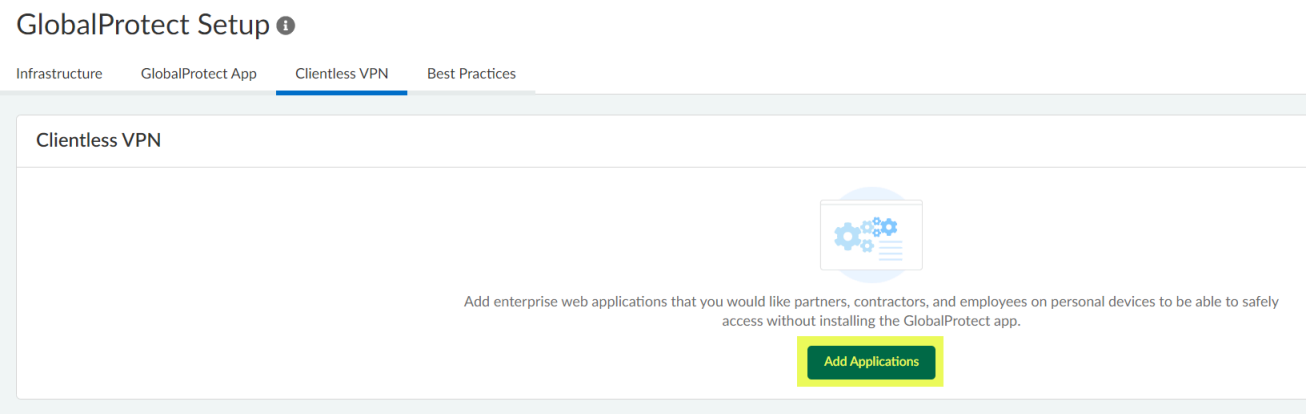
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

クライアントレスVPN を使用 すると、SSL対応のWebブラウザからエンタープライズ アプリケーションに安全にリモートアクセスできます。クライアントレスVPNを使用すると、エンドユーザーはエンドポイントにGlobalProtectアプリケーション ソフトウェアをインストールする必要がありません。これは、パートナーや請負業者によるアプリケーションへのアクセスを有効にし、個人のエンドポイントなどの管理されていない資産を安全に有効にする必要がある場合に役立ちます。

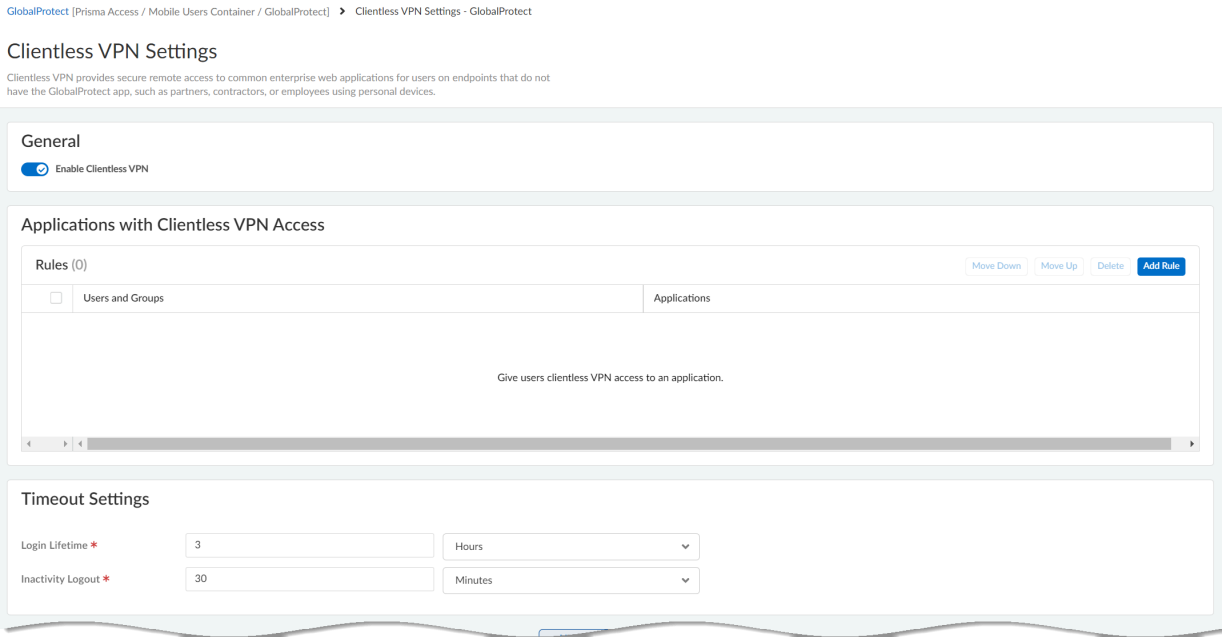
クライアントレスVPNを設定するには、以下の手順に従ってください。 Prisma Access:

©2025 Palo Alto Networks, Inc.

STEP 1 | 設定 > **Prisma Access**セットアップ > **GlobalProtect** > **GlobalProtect**セットアップ > クライアントレス**VPN**へ移動jして、 アプリケーションを追加します。



STEP 2 | クライアントレス**VPN**を有効化します。



STEP 3 | クライアントレスVPNプロファイルを追加します。

クライアントレス VPN を使用できるユーザーとアプリケーションを指定します。

©2025 Palo Alto Networks, Inc.

STEP 4 | ユーザーがプロキシ サーバー経由でアプリケーションにアクセスする必要がある場合は、プロキシを追加します。

プロキシに対しては基本的な認証のみがサポートされています（ユーザー名とパスワード）。ドメインのセットごとに 1 つずつ、複数のプロキシ サーバー設定を追加できます。追加する設定には次のようなものがあります。

- **Domains**（ドメイン） – プロキシ サーバーがサービスを提供するドメインを追加します。複数のドメインを示すためにドメイン名の先頭にワイルドカード文字（*）を使用できます。
- **Enable Proxy**（プロキシを有効化） – ドメインへのアクセスを提供するためにプロキシ サーバーを割り当てる場合に選択します。
- **Server**（サーバー） – プロキシ サーバーのIPアドレスまたはホスト名を指定します。
- **Port**（ポート） – プロキシ サーバーとの通信用ポートを指定します。
- **User and Password (**ユーザーとパスワード**)** – プロキシ サーバーへのログインに必要な認証情報であるユーザーとパスワードを指定します。確認のためにパスワードはもう一度指定します。

STEP 5 | デフォルトの 暗号化設定 を変更して、SSLセッションの認証と暗号化アルゴリズムを指定します。 Prisma Access クライアントレス VPN を使用するアプリケーション。

STEP 6 | 書き換え除外ドメイン リストにドメインを追加します。

クライアントレス VPN はリバース プロキシとして機能し、公開されている Web アプリケーションが返す Web ページが変更されます。すべてのURLを書き換え、書き換えられたページをリモート ユーザーに提示します。これにより、リモート ユーザーがそれらのURLのいずれかにアクセスすると、要求は GlobalProtectポータルを経由します。場合によっては、アプリケーションにポータル経由でアクセスする必要のないページが含まれることがあります (たとえば、アプリケーションに yahoo.finance.comの株価表示ツールが含まれる場合など)。これらのページを除外できます。書き換え除外ドメイン リストに追加したドメインは書き換えルールから除外され、書き換えることはできません。ドメイン名ではパスはサポートされていません。ドメイン名のワイルドカード文字（*）は、名前の最初でのみ使用できます。（*.etrade.com など）。

GlobalProtectモバイルユーザーを監視する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

Prisma Access (Managed by Strata Cloud Manager)

Prisma Access (Managed by Strata Cloud Manager)ユーザーは[ユーザーの > 監視]を使用できます。**GlobalProtect**または**Explicit Proxy**接続方法を選択してください。モバイルユーザーのページは、使用している接続方法に特有です。

©2025 Palo Alto Networks, Inc.

Prisma Access (Managed by Panorama)

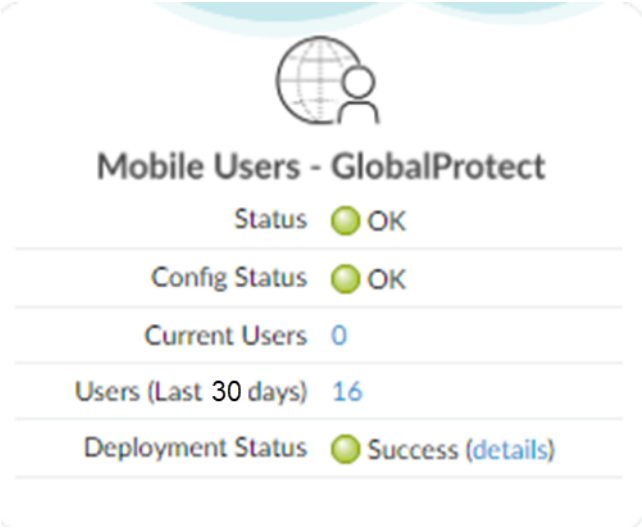
Panoramaでは、さまざまな場所からログインしているユーザーを参照できます。一意のユーザー、ユーザーがログインしているロケーション、および追加情報を記載した表を参照することができます。また、Mobile Users-GlobalProtectのデプロイメントにおいて、Prisma Accessが各ロケーションのユーザー数をどのようにカウントするかを理解することも重要です。

さまざまな場所から、ユーザーの詳細ビューを表示することができます。

- ユーザーの総合的なビューを参照して、ログインしているユーザーを表示、ログアウトできる表を開くには、**Panorama** > **Cloud Services**（クラウドサービス） > **Status**（ステータス） > **Status**（ステータス）を選択します。
- 地図ビューでユーザーのグラフィックビューを参照する、またはリージョンおよびロケーション別にユーザーを表示するには、**Panorama** > **Cloud Services**（クラウドサービス） > **Status**（ステータス） > **Service Stats**（サービスステータス） > **Mobile Users**（モバイルユーザー）**—GlobalProtect**を選択します。
- また、Prisma Accessがどのようにモバイルユーザーをカウントしているかについても、詳しくはこちらをご覧ください。

[Status(ステータス)]タブから**GlobalProtect**モバイルユーザーを表示

すべてのロケーションの中で現在ログインしている一意の合計ユーザー数を表示するには、**Panorama** > **Cloud Services (**クラウドサービス**)** > **Status (**ステータス**)** > **Status (**ステータス**)** > **Mobile Users (**モバイルユーザ**)—GlobalProtect** を選択します。



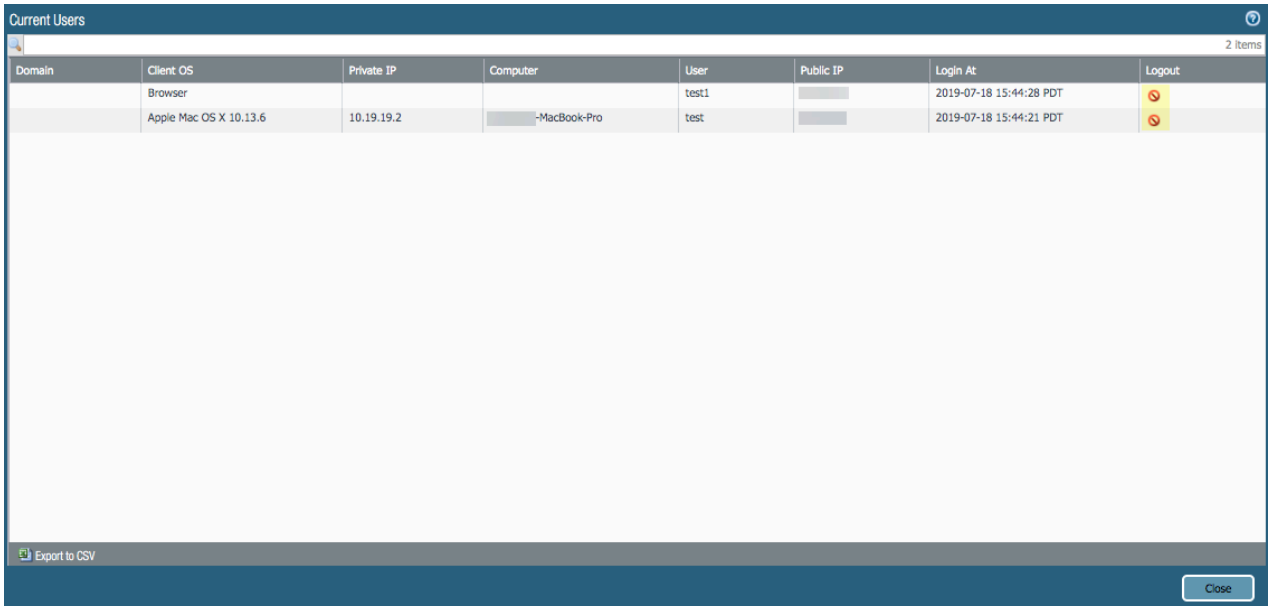
現在ログインしているユーザーの詳細情報を表示するには、**Current Users**（現在のユーザー）の隣にあるハイパーリンクの数字をクリックして、**Current Users**テーブルを表示します。

Status（ステータス）ページに表示されているユーザー数合計、およびポップアップテーブルに表示されているユーザー数が異なっている場合もあります。テーブルに表示されるユーザー数の方が多くなっていることがあります。

©2025 Palo Alto Networks, Inc.

Current Users（現在のテーブル）テーブルから、アクティブなユーザーをログアウトさせることができます。そうするには、ユーザーを選択して**Logout**（ログアウト）をクリックします。画面を一度閉じてから、再び開かないと、ログアウトさせたユーザーが**Current Users**（現在のユーザー）ページから消えない場合があります。

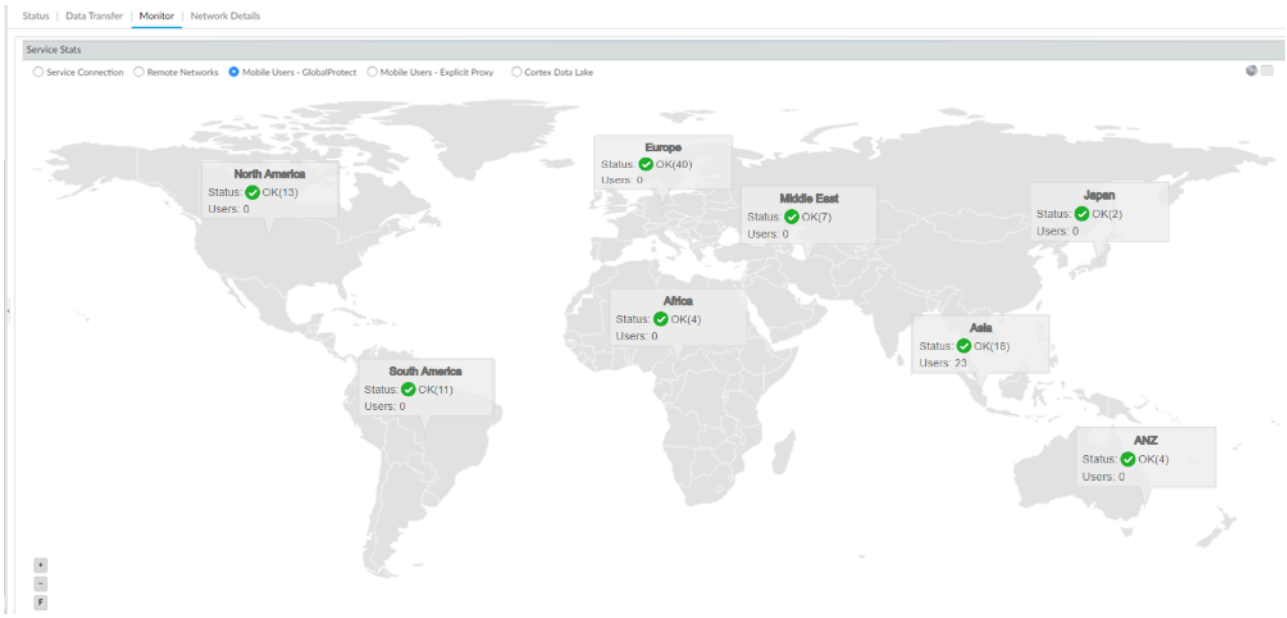
次の画面には、GlobalProtectアプリケーションを使ってログインしているユーザーと、Clientless VPNを使ってログインしているユーザーを表しています。画面には、ユーザーのユーザー名、パブリックIPアドレス、および前回ログイン時刻が表示されています。ユーザーがGlobalProtectアプリを使ってログインしている場合は、クライアントOS、プライベートIPアドレス、およびコンピュータ名も表示されます。



[Monitor(監視)]タブから**GlobalProtect**モバイルユーザーを表示

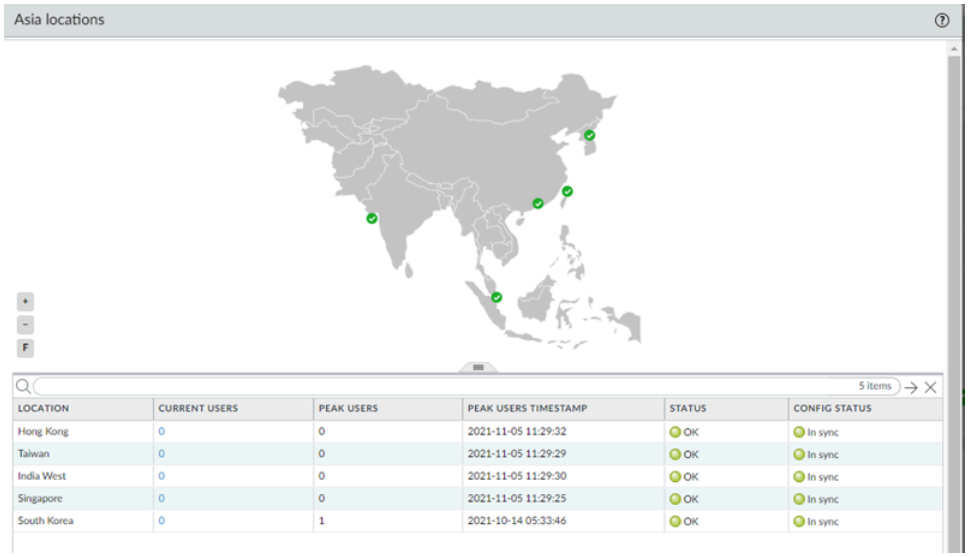
リージョンあたりにログインしている一意のユーザー数を表示するには、**Panorama** > **Cloud Services**（クラウドサービス） > **Status**（ステータス） > **Service Stats**（サービスステータス） > **Mobile Users**（モバイルユーザー）**—GlobalProtect**を選択します。

©2025 Palo Alto Networks, Inc.



リージョン内のロケーションの詳細を表示するには、リージョンをクリックします。

グローバルマップビューに表示されているユーザー数、およびテーブルに表示されているリージョンあたりのユーザー数が異なっている場合もあります。テーブルに表示されるユーザー数の方が多くなっている可能性があります。



Prisma Accessが**GlobalProtect**モバイルユーザーをカウントする方法

ステータスエリアに表示されるユーザー数合計が、対応するテーブルに表示されるユーザー数と異なっている場合があります。この違いについては、次のセクションで説明しています。

- **Status**（ステータス）タブ（**Panorama** > **Cloud Services** > **Status** > **Status**）–メインページの**Mobile Users**（モバイルユーザー）**–GlobalProtect**エリアに表示されるユーザー数が、**Current Users**（現在のユーザー）ハイパーリンクをクリックした時に表示されるテーブルのユーザー数と異なっている場合があります。**Mobile Users**（モバイルユーザー）**–GlobalProtect**エリアに表示される数字は、一意のユーザー数をカウントしています。**Current**

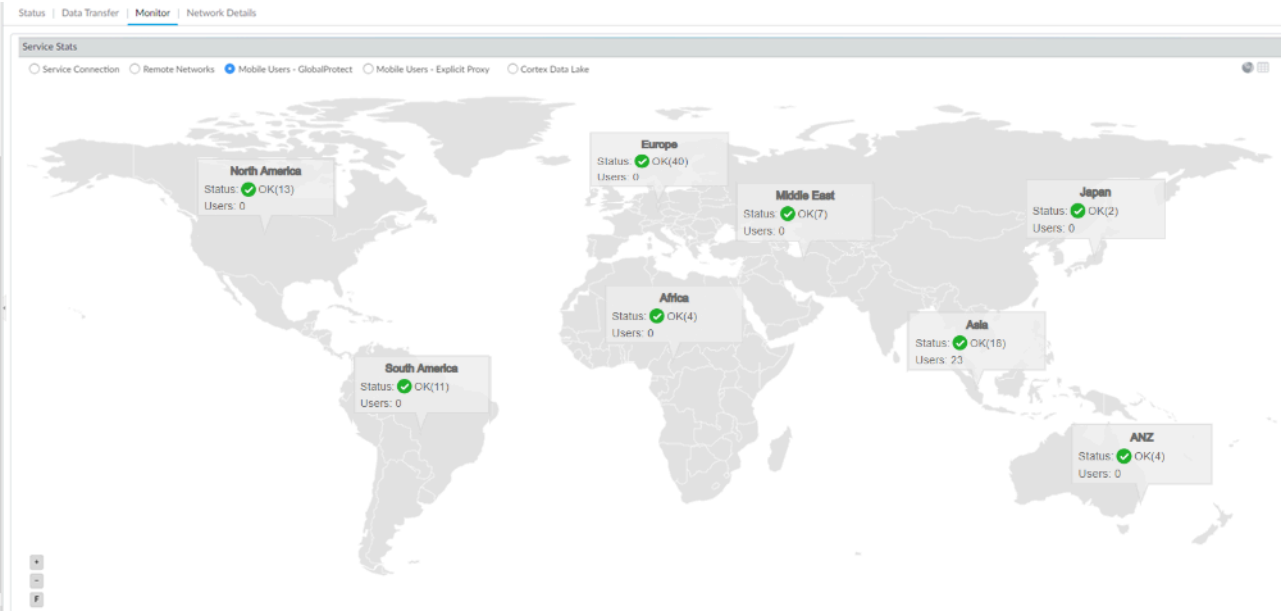
 ©2025 Palo Alto Networks, Inc.

Users（現在のユーザー）テーブルに記載されているユーザー数は、ログインまたは接続あたりのすべてのユーザーをカウントしています。1人のユーザーが複数のゲートウェイにログインしている、または複数のデバイスを使って接続している場合、テーブル内の値が大きくなる可能性があります。

たとえば、ユーザー**user1**が**United Kingdom**（英国）のロケーションに存在している2つのゲートウェイにログインしている場合が考えられます。多数のユーザーが同じロケーションにログインした場合、Prisma Accessは自動的にゲートウェイを追加するため、このような状況が発生する可能性があります。この場合、Prisma Accessは**user1**を**Mobile Users**（モバイルユーザー）**–GlobalProtect**エリアで1回カウントしますが、**Current Users**（現在のユーザー）テーブルでは2回カウントします。

- **Monitor**（監視）タブ（**Panorama** > **Cloud Services (**クラウドサービス**)** > **Status (**ステータス**)** > **Service Stats (**サービスステータス**)** > **Mobile Users (**モバイルユーザー**) – GlobalProtect**）–グローバルマップに表示される**Users**（ユーザー）数が、リージョンを選択した時にテーブルに表示されるユーザー数と異なっている場合があります。複数のゲートウェイにログインしているユーザー、または複数のデバイスを使って接続しているユーザーは、テーブルに複数回表示される可能性があります。

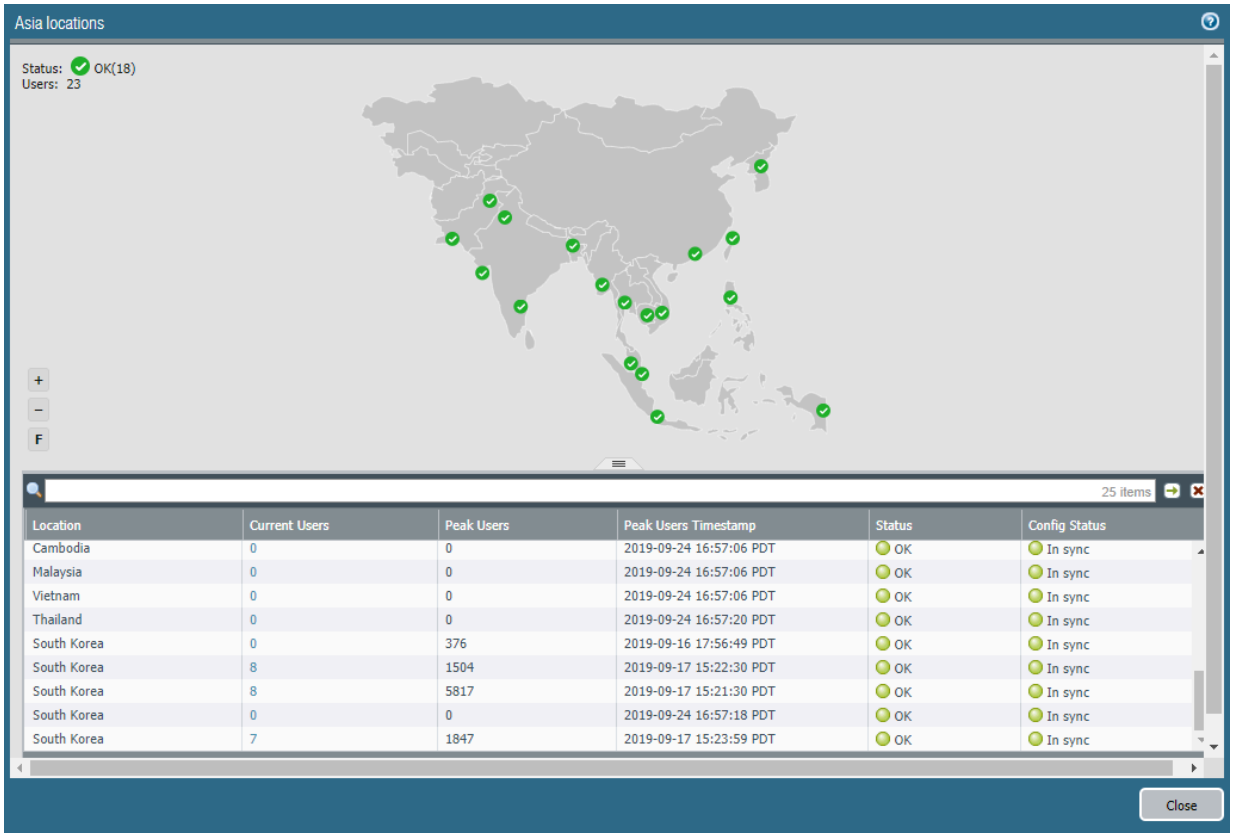
  次の画面に例を示します。グローバルマップに表示されているように、**Asia**（アジア）リージョンには23人の一意のユーザーがログインしています。



Asia（アジア）リージョンを選択した場合、Prisma AccessにはRegion（リージョン）ページの左上に、一意のユーザー数（23）が表示されます。ただし、2人のユーザーが**South Korea**（韓国）ロケーションで複数のデバイスを使って接続しています（例：スマートフォン

©2025 Palo Alto Networks, Inc.

とコンピュータ）。ユーザーは2つの別々の接続を持つため、Prisma Accessはテーブルで2回カウントし、テーブルの合計数は25となります。



 ©2025 Palo Alto Networks, Inc.

GlobalProtectモバイル ユーザーデプロイメントのIPアドレスプール

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

組織内のモバイルユーザーを十分にカバーできる、IP アドレスプールを指定していることを確認してください。一意のユーザーはそれぞれが、複数のデバイスを使ってPrisma Accessに同時に接続でき、接続している各デバイスにはプールからの一意のIPアドレスが必要になることを忘れないようにしてください。このプール内のアドレスは、内部的に使用している他のアドレスプールや、サービスインフラを有効にした時に割り当てたIPサブネットとオーバーラップしてはいけません。

プール内のIPアドレス数は、Prisma Accessに接続するモバイルユーザーデバイス数の2倍にすることをお勧めします。組織がBYODポリシーを採用している場合、または1人のユーザーが複数のユーザーアカウントを保有している場合は、IPプールの割り当て時にそれらの余分なデバイス数も考慮に入れてください。プール空間が限られている場合は、より小さなアドレスプールを指定することができます。ただし、IPアドレスプールが限度に達すると、その他のモバイルユーザーデバイスは接続できなくなります。

有効なIPサブネットが入力されたかどうかが検証されます（たとえば、/23未満のサブネットを持つプールを入力した場合、入力内容の変更を要求するメッセージが表示されます）。ただし、ご利用なデプロイ環境に対して十分な数のIPアドレスが割り当てられているかどうかは検証されません。

*CLI*を使ってロケーションを設定した場合、この検証機能は利用できません。すべてのロケーションを*CLI*を使ってデプロイする場合、モバイルユーザー向けの*Worldwide*プールに「*/18*」アドレスを追加することをお勧めします。

次の最低IPアドレスプールを指定していることを確認するために、Prisma Accessは設定内容をチェックします。

- Worldwideまたは地域的アドレスプールには、最低/23（512件のIPアドレス）が必要になります。
- 既存の場所をコンピューティング場所に変換する場合、変換後にその場所には最低限 /23 サブネットが必要です。
- 地域内にオンボーディングしているPrisma Accessゲートウェイがない場合、その地域にIPアドレスプールは不要です。たとえば、US East（米国東部）、US Northwest（米国北西部）、およびUS Northeast（米国北東部）のロケーションにゲートウェイを指定した場合、North America& South America（北米と南米）リージョンにのみIPアドレスプールを指定する必要があります。逆に、WorldwideアドレスプールまたはAfrica, Europe, & Middle East（アフリカ、欧州、中東）にIPアドレスプールを指定せずに、Europe（欧州）のモバイルユーザーロケーションを有効にした場合、デプロイ環境は失敗してしまいます。

©2025 Palo Alto Networks, Inc.

- GlobalProtectモバイルユーザーは、まずロケーション グループ内のIPアドレスを使用し、次にシアター固有のIPアドレス、最後に世界全域IPアドレスを使用します。たとえば、ロケーション グループと世界全域のプールを指定し、ロケーション グループ プールで使用可能なIP アドレスを使い果たした場合、Prisma Accessは **Worldwide (世界全域)** プールからIPアドレスを取得して、そのロケーション グループで使用します。

  IPアドレスプールのブロックを複数指定した場合、Prisma Accessは、モバイルユーザーセットアップ時に入力した順序でプールを使用します。

モバイル ユーザー向けの静的 IP アドレス割り当て - GlobalProtectのデプロイメント

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	• Prisma Access バージョン 5.2.1 • PAN-OS データプレーン バージョン 11.2.4 には アクティビティ インサイト、ユーザー グループ、ロケーション グループのサポートが含まれます • GlobalProtect バージョン 6.1.4 これは限定提供リリースです。この機能を有効にするには、テナントを有効にした後、*Palo Alto Networks* のアカウント担当者に連絡してください。

一部の従来のネットワークでは、IP アドレスベースの認証を使用して、ユーザーの内部または外部のリソースへのアクセスを制限します。Prisma Access モバイル ユーザー: GlobalProtect のデプロイメントにより、オンボーディング時に割り当てたモバイル ユーザーの IP アドレス プールから IP アドレスがユーザーに割り当てられ、このユーザーと IP アドレスのマッピングは、以降のログインで変更される可能性があります。ユーザと IP アドレスのマッピングを維持するために、Prisma Accessではユーザに静的 IP アドレスを割り当てることができます。

この機能は、新規*Prisma Access*デプロイメントでのみ利用可能です。

IP プール プロファイルを作成するには、次の 1 つ以上の基準を使用します。

- シアター- ユーザーがいるシアターに基づいて IP アドレスを割り当てます。たとえば、特定の劇場用に /30 サブネットを作成できます。これらの IP アドレスはそのシアターに対して静的です。シアターに指定した IP アドレスを使用してセキュリティ ポリシー ルールを作成することにより、シアターに基づいてリソースへのアクセスを適用できます。
- ユーザー- モバイル ユーザーの IP アドレス プールに /30 または /32 アドレスを設定し、一致基準を使用してそのユーザーを IP アドレスに関連付けることで、ユーザー ID に基づいて IP アドレスを割り当てます。このように、Prisma Accessが特定のユーザに対して保持する静

 ©2025 Palo Alto Networks, Inc.

的 IP アドレスを割り当てることで、現在の IP アドレスベースのセキュリティ・ポリシー・ルールを維持し、ユーザのリソースへのアクセスを制御することができます。

- ユーザー グループ- ユーザー グループに基づいて IP アドレスを割り当てます。ユーザーが設定されたユーザー グループに属している場合、定義された IP プール サブネットから IP アドレスを取得します。
- ロケーション グループ - IP プール プロファイルで定義されたロケーション グループに基づいて IP アドレスを割り当てます。

静的 IP アドレスを割り当てるときは、次のガイドラインに従ってください。

- 複数のIPプールを指定する場合、 Prisma Accessはルールを上から下に評価し、ルールのリストの最初の一致に基づいて IP アドレスを割り当てます。
- ユーザーID またはユーザーグループを IP プールのマッチング基準として使用する場合は、Prisma AccessデプロイメントをCloud Identity Engineと統合します。
- テナントごとに次の最大割り当てがサポートされます。
  - 20,000 ユーザー
  - 5,000 ユーザー グループ (ユーザー グループあたり 50,000 ユーザー)
  - 10,000 IP アドレス プール プロファイル
  - 10,000 IP アドレス プール
- /23 から /32 までのプレフィックス長を入力します。
- 作成するモバイル ユーザー クライアント **IP** プール プロファイルごとに、次の操作を行います。
  - 最大 10 個の IP プレフィックスがサポートされます。
  - 最大 256 人のユーザーがサポートされます。
- 静的 IP アドレス設定では、Prisma Access がユーザと IP アドレスの関連付けを維持する期間を指定するた めに、リース期間とグレース期間を使用します。
  - リース期間 とは、ユーザーと IP アドレスのマッピングを割り当てた後に有効となる期間です。

    デフォルトのリース期間は 86400 秒 (24 時間) です。

    最小リース期間は 3600 秒 (1 時間) です。

    最大リース期間は 7776000 秒 (90 日) です。
  - 猶予期間とは、リース期間が終了した後、Prisma AccessがそのユーザとIPアドレスのマッピングを他のユーザに割り当てずに保持する期間です。

    デフォルトの猶予期間は 14400 秒 (4 時間) です。

    最小猶予期間は 60 秒です。

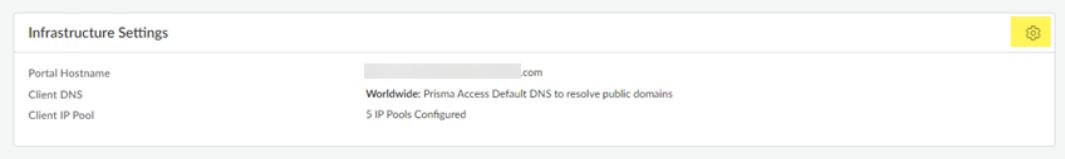
    最大猶予期間は 7776000 秒 (90 日) です。

静的**IP**アドレスの割り当てを構成する

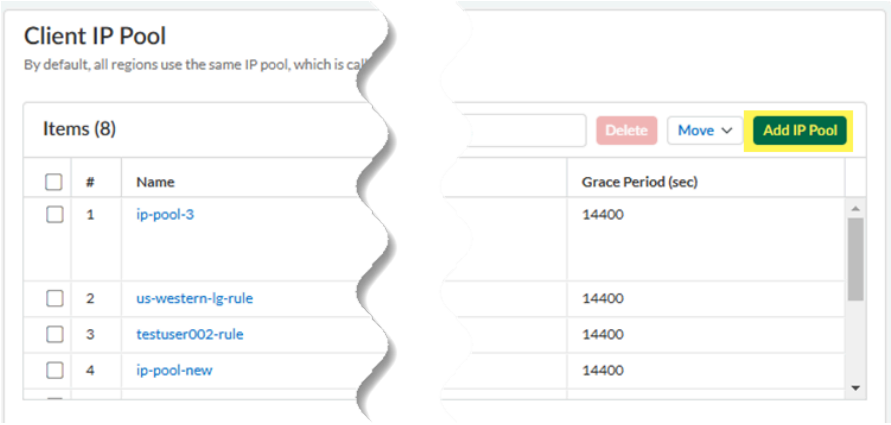
デプロイメントで静的 IP アドレスの割り当てを構成するには、次の手順を実行します。

 ©2025 Palo Alto Networks, Inc.

STEP 1 | [ワークフロー] > **[Prisma Access セットアップ] > [GlobalProtect]** へと移動し、歯車をクリックしてインフラストラクチャ設定を強調表示します。



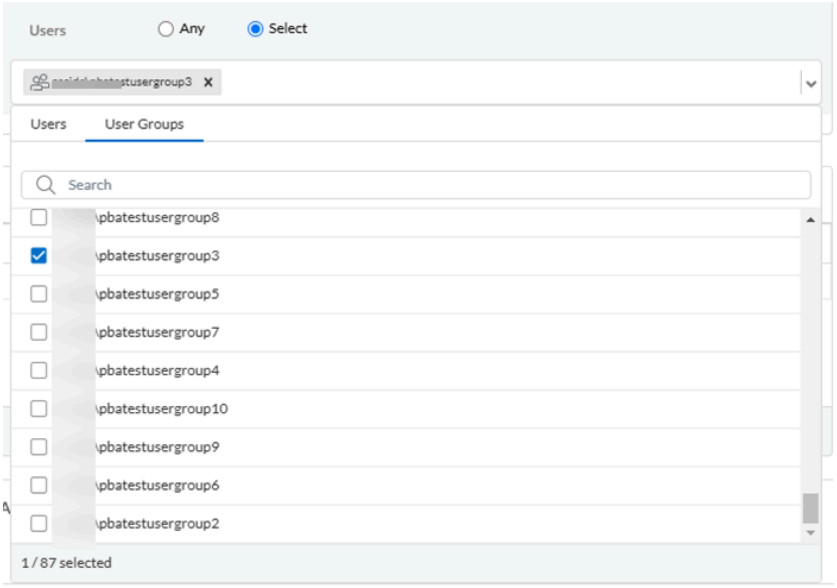
STEP 2 | [クライアント IP プール] 領域で、静的 IP アドレスの **IP** プールを追加します 。



 ©2025 Palo Alto Networks, Inc.

STEP 3 | シアター、Prisma Accessロケーショングループ、またはユーザに静的 IP アドレスを割り当てます。

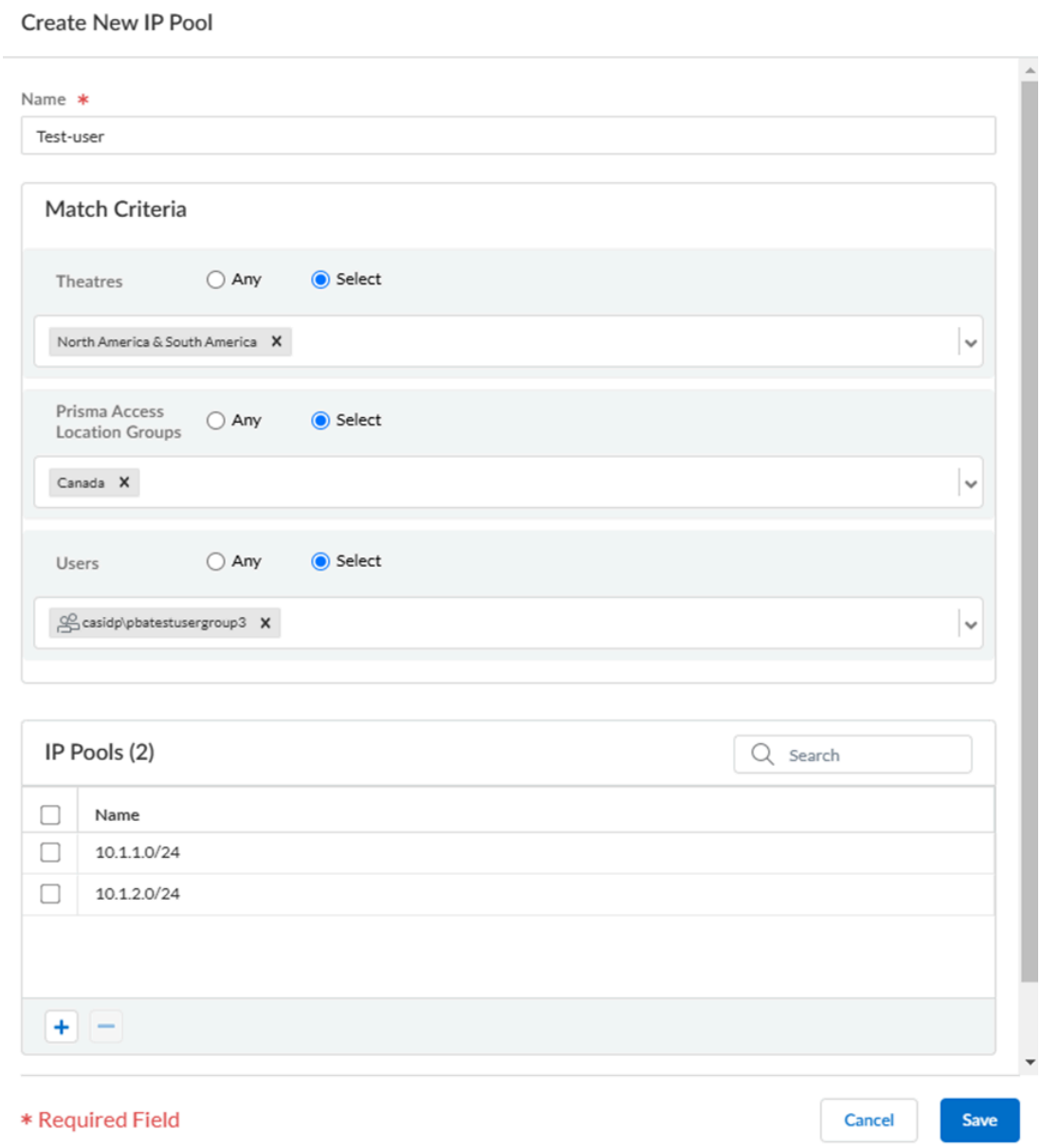
1. IP アドレス プールに一意の 名前を付けます。
2. 1 つ以上の シアター を選択して、 それらのシアターでプールを使用できるようにするか、[任意] を選択して、すべての劇場でプールを使用できるようにします。
3. 1 つ以上の **Prisma Access** ロケーション グループを 選択して 、そのロケーション グループでプールを使用できるようにするか、[任意] を選択して、すべてのロケーション グループでプールを使用できるようにします。
4. ユーザーまたはユーザー グループを選択する か、[任意] を選択して、プールを任意のユーザーまたはユーザー グループで使用できるようにします。
   - 1 人以上のユーザーを IP アドレス プールに割り当てるには、[ユーザー] タブでユーザーを選択します。
   - 1 つ以上のユーザー グループを IP アドレス プールに割り当てるには、[ユーザー グループ] タブでユーザーを選択します。



5. **[IP プール]** 領域に、IP アドレス プールを入力します。

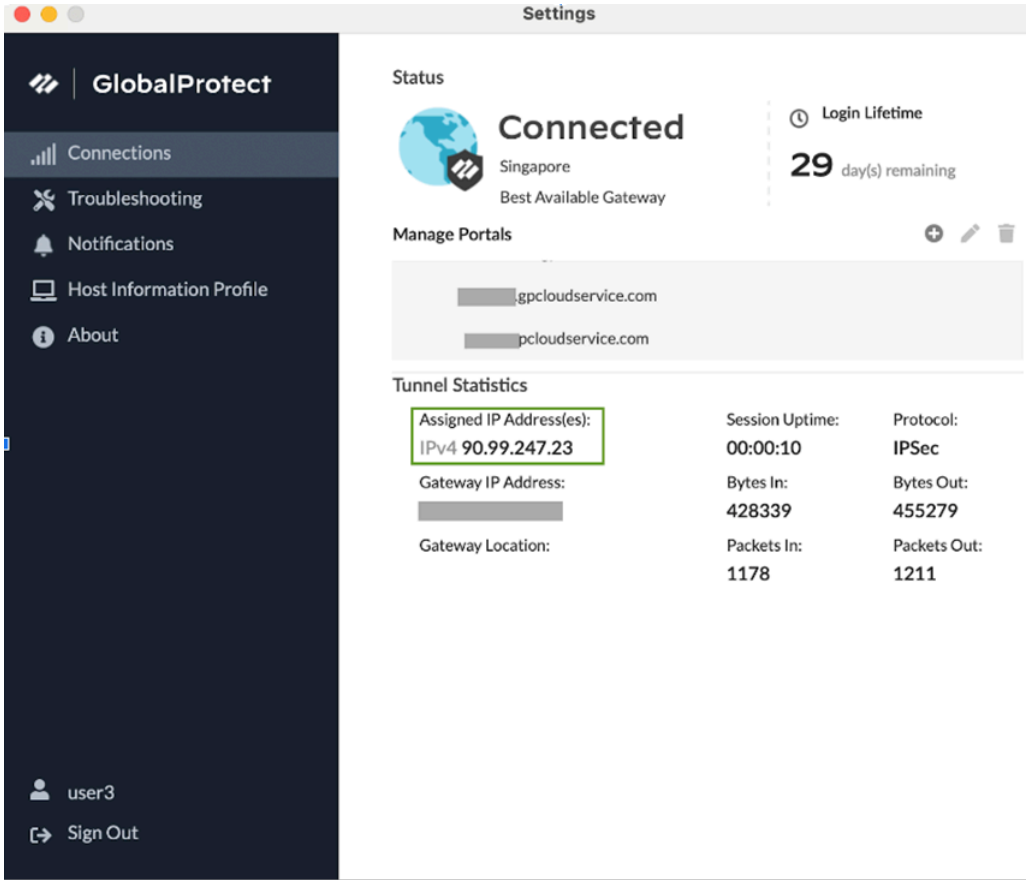
   ユーザーを単一の *IP* アドレスに制限するには、*/30* または */32 IP* アドレスを指定します。 *Prisma Access*はユーザーをそのアドレスに割り当てます。*/32* では *1* つの *IP* アドレスしか提供されないため、最小サブネットを */30* にして、ユーザーをそのサブネットに制限することをお勧めします。
6. (任意) ユーザーと IP アドレスのマッピングの リース期間 と 猶予期間 を入力します。
7. 変更を保存します。

©2025 Palo Alto Networks, Inc.



©2025 Palo Alto Networks, Inc.

STEP 4 | クライアント マシンの **[GlobalProtect]** > **[設定]** に移動し、 **[トンネル統計]**を表示して、 割り当てられた **IP** アドレスを確認して、変更を確認します。



GlobalProtectアプリケーションがモバイルユーザーのためにPrisma Accessロケーションを選択する方法

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

モバイルユーザーがPrisma Accessロケーションに接続する場合、アプリは次の選択手続きを使って接続するロケーションを決定します。

モバイルユーザーのオンボーディング時に、*Prisma Access*を配置するモバイルユーザーのロケーションを有効にします。オンボーディング時にロケーションを選択しなかった場合、*Prisma Access*はデプロイメント環境でそれを使用しません。

- Prisma Accessロケーションが存在している国にモバイルユーザーが接続する場合、ユーザーはその国のロケーションに接続します。

©2025 Palo Alto Networks, Inc.

- モバイルユーザーが何らかの理由で国内のロケーションに接続できない場合、Prisma Accessはリージョンに基づいてユーザーを接続するために、次のうちから 1 つモバイルユーザーロケーションを選択します。
  - **Asia, Australia & Japan**（アジア、オーストラリア、日本）:Hong Kong, Japan Central, or Japan South(香港、日本中部、または日本南部)
  - **Africa, Europe & Middle East**（アフリカ、欧州、中東）:Netherlands Central（オランダ中部）
  - **North America & South America**（北米、南米）:US Northwest（米国北西部）

  Palo Alto Networksでは、冗長性を確保するために、モバイル ユーザーのオンボーディング中に、それぞれのリージョンでこれらの場所の少なくとも1つを有効にすることをお勧めしています。Prisma Accessロケーションを持たない国からPrisma Accessに接続するモバイル ユーザーがいる場合、前述のリストにあるフォールバック ロケーションの少なくとも1つを有効にする必要があります。

  香港、日本中部、日本南部、オランダ中部、米国北西部のロケーションは、どこからでもクライアント接続を受け入れることができ、 グローバル フォールバック ロケーションと呼ばれています。これらの場所に加えて、グローバル フォールバックの場所としても機能する次の場所を1つ以上有効にすることができます。
  - バーレーン
  - France North（フランス北部）
  - アイルランド
  - South Africa West（南アフリカ西部）
  - 韓国
- Palo Alto Networksでは、冗長性を確保するために、複数の コンピューティング場所 で場所を有効にすることをお勧めします。
- Prisma Accessロケーションとオンプレミスゲートウェイを使用している場合、Prisma Accessで優先度を設定して、モバイルユーザーを特定のオンプレミスGlobalProtectゲートウェイに接続、またはPrisma Accessロケーションに接続させることができます。詳細については、[Prisma Accessおよびオンプレミス ゲートウェイの優先順位の管理]を参照。
- モバイルユーザーの接続時、GlobalProtectアプリケーションは自動ゲートウェイ選択プロセスにおいて、次のPrisma Accessロケーションを使用しません。これは、オンボーディング時にプラグインでPrisma Accessロケーションを選択した場合でも同様です。ただし、モバイルユーザーのオンボーディング時に、 それらのロケーションの手動選択を許可した場合、モバイルユーザーは手動でこれらのロケーションのいずれかを選択して、それを優先するロケーション（ゲートウェイ）として設定することができます。
  - Australia（オーストラリア）:オーストラリア東部
  - Brazil（ブラジル）:Brazil East（ブラジル東部）およびBrazil Central（ブラジル中央部）
  - フランス：France South（フランス南部）
  - Germany（ドイツ）:Germany North（ドイツ北部）およびGermany South（ドイツ南部）
  - India（インド）:India South（インド南部）
  - Mexico（メキシコ）:Mexico West（メキシコ西武）

©2025 Palo Alto Networks, Inc.

- Netherlands（オランダ）:Netherlands South（オランダ南部）
- Pakistan（パキスタン）:Pakistan West（パキスタン西部）
- Russia（ロシア）:Russia Northwest（ロシア北西部）
- Spain（スペイン）:スペイン東部は

モバイル ユーザーがゲートウェイに手動で接続するには、 接続方法をオンデマンド に変更する必要がある場合があります。

GlobalProtectモバイルユーザーのリスト表示を許可する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス ❑ Minimum Required Prisma Access Version:3.0 Preferred

既存のモバイル ユーザーに対して出口IP許可リストを有効にする方法について説明します。

GlobalProtectのパブリック(出口)IPアドレスを追加するには、以下の手順に従います。–組織内で使用する任意のSaaSアプリケーション許可リストにモバイル ユーザーをデプロイすると、Prisma AccessによってIPアドレスが提供され、環境内で使用する前に許可リストに追加されていることを確認できます。既存のPrisma Accessデプロイメントに対して出口IP許可リストを有効にすると、Prisma Accessは、すでにロケーションに割り当てられているすべての出口IPアドレスを出口IP許可リストに移行します。新しいPrismaデプロイメントの場合、Global Protect モバイル ユーザーをオンボードするときに、出口IP許可リストを有効にします。

組織の許可リストに出口IPアドレスを追加したら、Prisma AccessUIで、GlobalProtectの出口IPアドレスが許可リストに登録されていることを確認し、変更を プッシュします 。 次に、Prisma Accessはこれらの出口IPアドレスをリリースし、デプロイメントに追加します。自動スケール イベントの結果として、初期構成後にPrisma AccessがIPアドレスを追加した場合、Prisma Accessがデプロイメントに新しい出口IPアドレスを追加する前に、新しい出口IPアドレスが追加されたことを確認します。

有効にすると、出口IP許可リストテーブルには、確認済みまたはまだ確認されていな IPアドレスと、そのプロビジョニング ステータスに関する情報が表示されます。

- Strata Cloud Manager
- Panorama

GlobalProtectモバイルユーザーのリスト表示を許可する（Strata Cloud Manager）

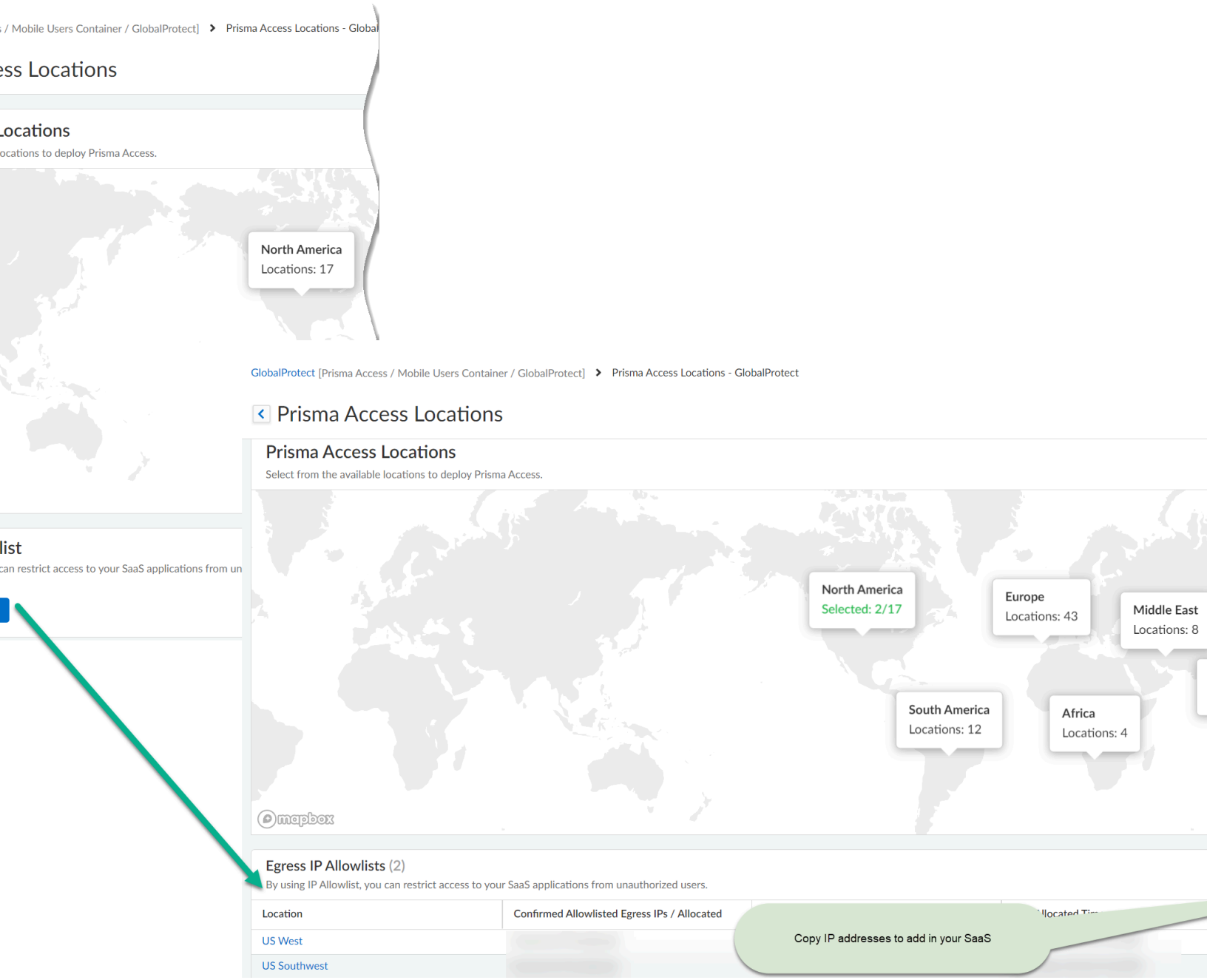
Prisma Accessを有効にして、Prisma Accessトラフィックの出口IPアドレスを表示します。承認されたユーザーまたはソースのみの使用を制限するSaaSアプリケーションのIP許可リストでこれらのIPアドレスを使用します。

STEP 1 | [ワークフロー] > **[Prisma Access**セットアップ] > **[GlobalProtect]** > [インフラストラクチャ]**[Prisma Access**ロケーション]設定を編集します。

©2025 Palo Alto Networks, Inc.

STEP 2 | Prisma AccessロケーションのIPアドレスを表示します。

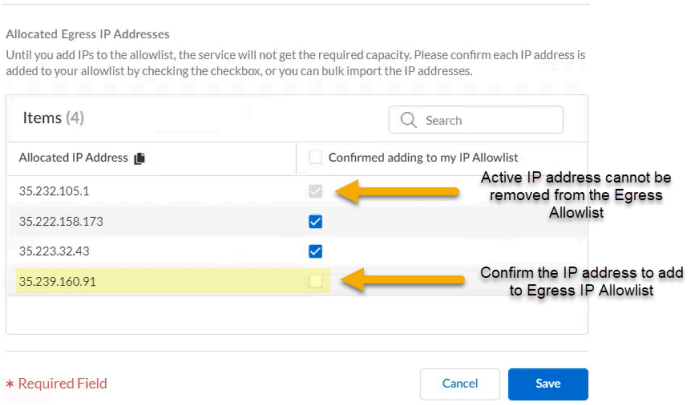
1. 出口IP許可リストを有効にすると、オンボードされたPrisma Accessのロケーションのアドレスが表示されます。
2. 割り当てられたIPアドレスをコピーして、SaaSアプリケーションの許可リストに追加します。
3. 移行して、Prisma Accessでオンボードされた場所に割り当てられたIPアドレスを確認します。



©2025 Palo Alto Networks, Inc.

STEP 3 | 新しくオンボードされた場所または自動スケーリング イベント中にIPアドレスを取得します。

1. ロケーション名を選択して、その場所に割り当てられた新しい出口IPアドレスを見つけます。
2. Prisma Accessで確認する前に、これらのIPアドレスをSaasアプリケーションの許可リストに追加するには、**[IP** 許可リストへの追加を確認**]** を選択します。



IPv6アドレスをお持ちの場合は、**[IPv6** 許可リストへの追加を確認**]**を選択します。



STEP 4 | Prisma Accessへの変更をプッシュします。

割り当てられた出口**IP**アドレスのステータス

出口IP許可リストのステータス列には、場所に割り当てられたすべてのIPアドレスがデプロイメント用にプロビジョニングされているかどうかが示されます。各ステータスの詳細については、以下をお読みください。

プロビジョニング済み - SaaSアプリケーションの許可リストに出口IPアドレスを追加し、Prisma AccessでIPアドレスを確認し、変更をプッシュして完全にプロビジョニングしました。

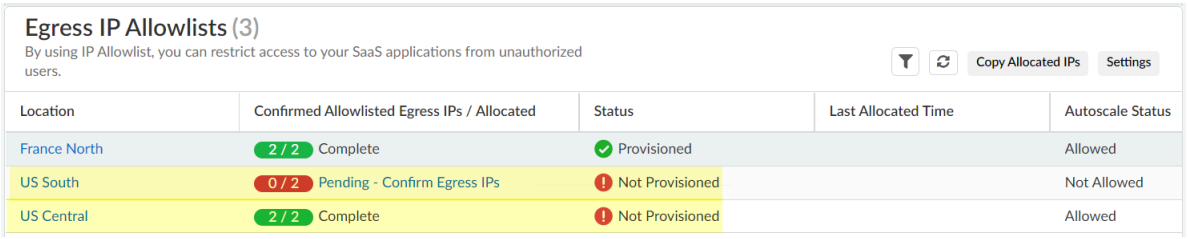
部分的にプロビジョニング済み - 最初の出口IPアドレス セットを追加し、Prisma Accessで確認して、変更をプッシュしました。ただし、Prisma Accessは自動スケール イベントの一環として別のIPアドレス セットを追加しており、それらのIPアドレスはPrisma Accessでは確認されていません。

プロビジョニングされていません - Prisma AccessはロケーションにIPアドレスを割り当てており、出口IPアドレスをSaaSアプリケーションの許可リストに追加してPrisma Accessで確認しましたが、このロケーションはまだオンボードされていません。

©2025 Palo Alto Networks, Inc.

プロビジョニングできません - このロケーションをオンボードしましたが、まだPrisma Accessで確認して変更をプッシュしていません。

出口IP許可リスト テーブルには、Prisma Accessで確認済みのIPアドレスとまだ確認されていないIPアドレスの数も示されます。たとえば、1/2は、その場所に割り当てられた2つのIPアドレスのうち1つがPrisma Accessで確認されていることを意味します。



GlobalProtectモバイルユーザーのリスト表示を許可する（Panorama）

GlobalProtectのパブリック(出口)IPアドレスを追加するには、以下の手順に従います。–組織内で使用する任意のSaaSアプリケーション許可リストにモバイル ユーザーをデプロイすると、Prisma AccessによってIPアドレスが提供され、環境内で使用する前に許可リストに追加されていることを確認できます。

この出口IPアドレス割り当て方法には、次の利点があります。

- これにより、Prisma Accessは許可リストに載っているIPアドレスのみをプロビジョニングするようになります。
- これにより、モバイル ユーザーが組織のネットワークによってブロックされているIPアドレスからPrisma Accessに接続しようとするのを防ぎます。 Prisma Accessは許可リストに登録されていることを確認するまで、IPアドレスはデプロイメントにリリースされません。
- APIを使用せずに現在の出口IPアドレスを取得する方法を提供します。

Prisma Accessは、次の状況で出口IPアドレスを割り当てます。

- モバイル ユーザーのオンボーディング中に場所をオンボーディングする場合。

  Prisma Accessは、オンボードする場所ごとに2つのゲートウェイIPアドレスを割り当てます。

  ある場所をオンボードし、同じコンピューティング場所内の他の場所で自動スケール イベントが発生している場合、*Prisma Access*は新しい場所に*2*つ以上の*IP*アドレスを割り当てることがあります。このような状況では、これらの *IP*アドレスをすべて許可リストに追加し、すべてのアドレスが *[*許可リストに追加*]* されていることを確認してください。

- 大規模なスケーリングイベントの場合。

  モバイルユーザーの数が、事前に割り当てられた2つのIPアドレスの容量を超えた場合、Prisma Accessは2つのIPアドレスのセットをさらに1つ割り当てます。

  自動スケール イベントは、コンピューティング ロケーション内のすべてのオンボード ロケーションに影響します。ある場所で自動スケール イベントが発生し、アドレスが許可リス

 ©2025 Palo Alto Networks, Inc.

トに追加されていることをまだ確認していない場合、そのコンピューティング場所のすべての場所で、 自動スケール ステータス が **[Not Allowed (未許可)]**と表示されます。

自動スケール ステータスには、*Prisma Access* の自動スケールのステータスが表示されます。

- 許可済み- *IP*アドレスを許可リストに追加しました。多数のモバイル ユーザーが*1*つの場所にログインして自動スケール イベントをトリガーすると、*Prisma Access*は自動スケール イベントに許可されたリストされた*IP*アドレスを使用します。
- 許可されていません- *Prisma Access UI*ですべての*IP*アドレスを許可リストに追加するように指定していないか、変更を追加済みとしてマークした後にコミットしてプッシュしていません。*Prisma Access*が自動スケール イベントをトリガーした場合、*Prisma Access*は、その場所に容量を追加するために追加の*IP*アドレスをプロビジョニングしません。

  場所を追加するたび、または自動スケール イベントの結果として*Prisma Access*が*IP*アドレスを追加するたびに、出口*IP*許可リスト テーブルを含むページを更新し、*[許可リストに追加済み]* を指定して*IP*アドレスが組織の許可リストに追加されていることをマークし、変更をコミットしてプッシュする必要があります。

自動スケール イベントの結果として*Prisma Access*が追加する*IP*アドレスを常に把握できるように、*Prisma Access IP*アドレスの変更を通知する URLをセットアップできます。

この機能を有効にする必要はありません。 UIにリストされているIPアドレスが許可されていることを確認するまで、Prisma AccessにIPアドレスを解放させるかどうかを選択します。

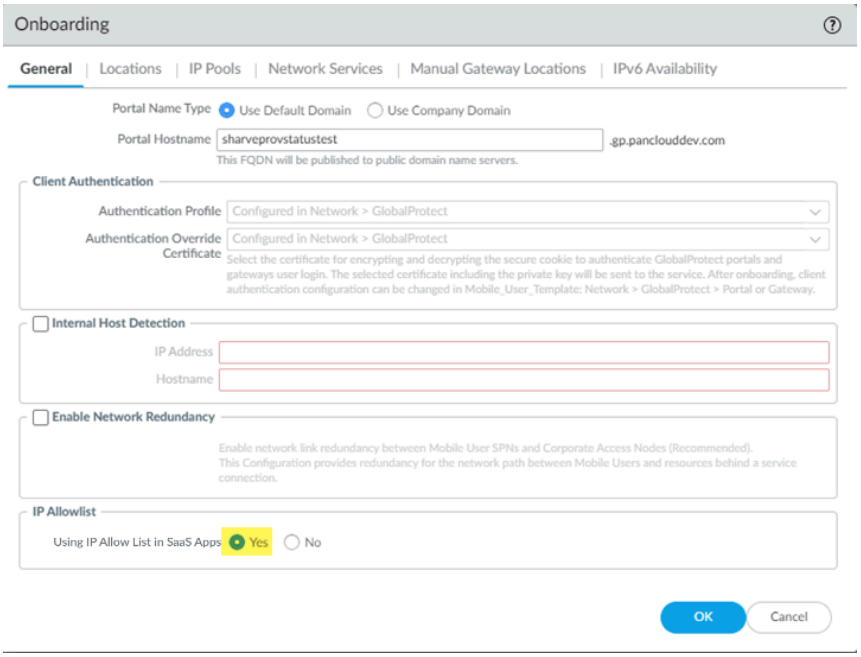
Prisma Accessが、GlobalProtectのパブリック (出口) IPアドレスを許可リストに追加するまでデプロイメントにプロビジョニングしないようにするには、モバイル ユーザー - GlobalProtectオンボーディング中に、**SaaS**アプリでの**IP**許可リストの使用設定で **[はい]** を指定します。次のタスクを完了して、Prisma AccessUIに追加されたことを確認します。

STEP 1 | **[Panorama]** > **[クラウド サービス]** > **[構成]** > **[モバイル ユーザー - GlobalProtect]**を選択します。

STEP 2 | ホスト名 を選択して構成します (既存のデプロイメントの場合)、またはデプロイメントを初めて構成します (新しいデプロイメントの場合)。

©2025 Palo Alto Networks, Inc.

STEP 3 | **SaaS**アプリでの**IP**許可リストの使用を**Yes**に指定します。



STEP 4 | モバイル ユーザー - GlobalProtectデプロイメントで使用するロケーションの選択など、Prisma Accessオンボーディングを続行し、変更をコミットしてプッシュします。

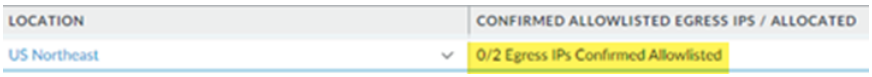
変更がUIに反映されるまでに最大1分かかる場合があります。変更をコミットしてプッシュする前に 出口**IP**許可リスト を表示すると、**0/0 Egress IPs Confirmed Allow Listed**というステータスが表示されます。 これは、Prisma Accessがデプロイメントに送信IPアドレスを割り当てていないからです。

©2025 Palo Alto Networks, Inc.

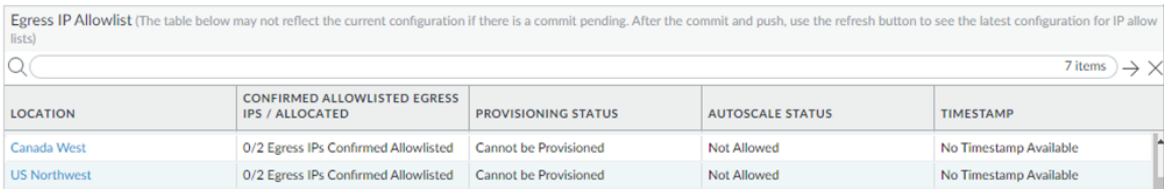
STEP 5 | 出口**IP**許可リストテーブルを表示し、許可リストに追加する必要がある出口IPアドレスをメモします。

出口IPアドレスは、出口**IP**許可リストテーブルの**[**確認済みの許可リスト出口**IP /** 割り当て済み**]** フィールドで確認できます。最初の数字は、IPアドレスが許可リストに追加されていることが確認されているかどうかを示します。

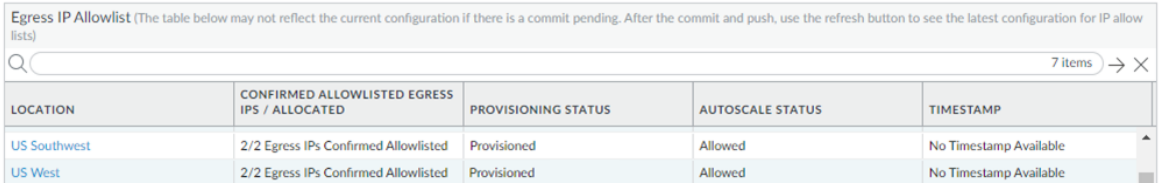
次の例は、米国北東部のIPアドレスを示しています。`0/2`出口`IP`が許可リストに登録済みと確認されている という説明は、2つの出口IPアドレスのうち0つが許可リストに追加済みとしてマークされており、それらを追加する必要があることを示しています。



新しいPrisma Accessデプロイメントが行われていない場合、または場所を追加した場合や自動スケール イベントが発生した場合、表には、出口IPアドレスが組織の許可リストに追加されていないことが示されます。

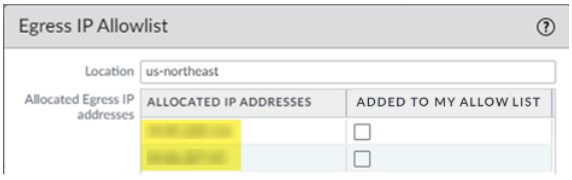


既存のPrisma Accessデプロイメントでは、テーブルに プロビジョニングステータス が プロビジョニング済み 、 オートスケールステータス が 許可済みと表示され、 Prisma Accessが出口IPアドレスを追加済みとしてマークします。



Prisma Accessは新しく追加された場所ごとに2つのアドレスを割り当てます。既存の場所で、多数のモバイル ユーザーが同時に1つの場所にログインしたときに自動スケール イベントが発生したことがある場合は、Prisma Accessは2の倍数で追加の出口IPアドレスを割り当て、既存の場所に4つ以上のアドレスが存在する可能性があります。

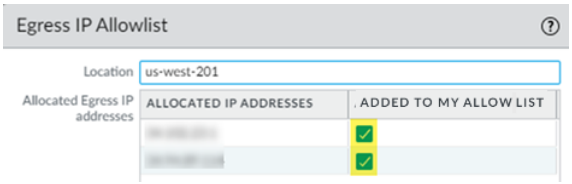
STEP 6 | 表内のロケーション 名を選択して、組織の許可リストに追加する必要がある新しい出口IPアドレスを見つけます。



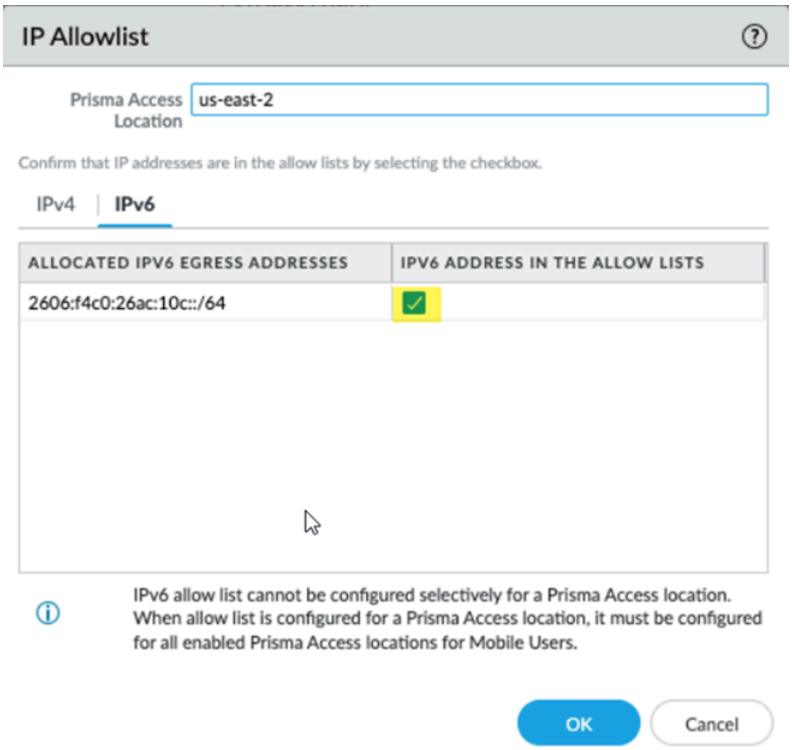
STEP 7 | これらの出口IPアドレスを組織の許可リストに追加します。

©2025 Palo Alto Networks, Inc.

STEP 8 | 出力 IPアドレスを許可したら、出口IP領域に戻り、[許可リストに追加]を選択して、許可リストに追加したことを示します。

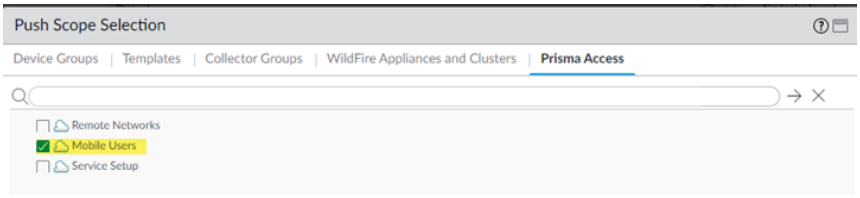


IPv6アドレスがある場合は、 許可リストで**IPv6**アドレスを選択します。



STEP 9 | 変更をコミットしてプッシュし、Prisma Accessでアクティブにします。

1. **Commit**（コミット） > **Commit and Push**（コミットしてプッシュ）の順に選択し、Push Scope（プッシュ スコープ）で **Edit Selections**（選択内容の編集）を行います。
2. **Prisma Access**を選択し、モバイル ユーザーが選択されていることを確認します。

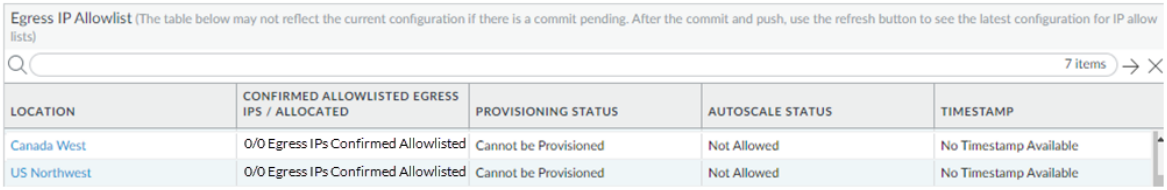


3. **OK** をクリックして、プッシュ スコープに対する変更を保存します。
4. 変更をコミットしてプッシュします。

変更をコミットしてプッシュする前に 出口**IP**許可リスト テーブルを表示すると、**0/0 Egress IPs Confirmed Allow Listed**というステータスが確認済コラムに表示されます。 これは、コ

 ©2025 Palo Alto Networks, Inc.

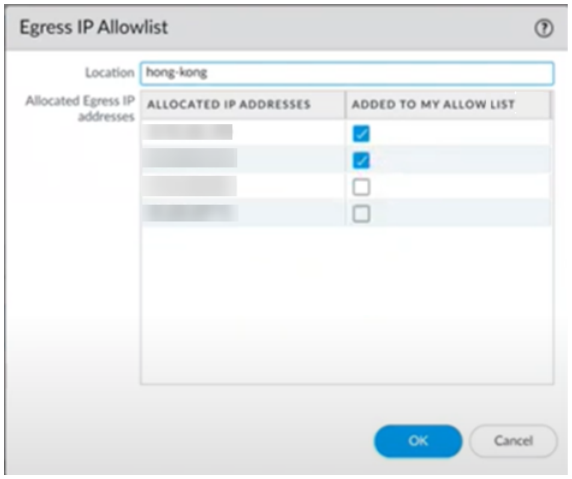
ミットしてプッシュするまで、Prisma Accessがデプロイメントに送信IPアドレスを割り当てていないからです。



出口**IP**許可リスト テーブルには、次の追加フィールドが含まれています。

項目	詳説
場所	オンボードされたモバイル ユーザーの場所。
確認された許可リストに登録された出口**IP** / 割り当て済み	許可リストに登録されていることが確認された出口IPアドレスの数と、割り当てられた出口IPアドレスの数。
プロビジョニングの状態	出口IPアドレスの許可リストステータス。 • プロビジョニング済み- 組織の許可リストに出口IPアドレスを追加し、 Prisma AccessUIで[許可リストに追加]をチェックし、変更をコミットしてプッシュし、完全にプロビジョニングされるようにします。 • プロビジョニングされていません- Prisma Accessによってその場所にIPアドレスが割り当てられており、出口IPアドレスが組織の許可リストに追加され、Prisma Access UIで追加されたことが確認されていますが、この場所はまだオンボードされていません。 • プロビジョニングできません- この場所をオンボードしましたが、「許可リストに追加」をまだチェックしておらず、変更をコミットしてプッシュしていません。 Prisma Accessでこれらの出口IPを組織の許可リストに追加したことを指定し、変更をコミットしてプッシュするまで、Prisma Accessはこれらの IPアドレスをデプロイメントにプロビジョニングしません。 • 部分的な容量でプロビジョニング済み- 最初の出口IPアドレスセットを追加し、Prisma AccessUIで追加されたことを確認して、変更をコミットしてプッシュします。ただし、Prisma Accessは自動スケール イベントの一環として別のIPアドレス セットを追加

 ©2025 Palo Alto Networks, Inc.

項目	詳説
	しましたが、それらのIPアドレスはPrisma AccessUIの許可リストに追加されるように指定されていません。 次のスクリーンショットは、 部分的な容量でプロビジョニング済みとしてマークされるデプロイメントの例を示しています。2つのIPアドレスが「許可リストに追加」としてマークされています。ただし、Prisma Accessはこの場所にさらに2つのIPアドレスを追加しましたが、それらの場所はUIには追加されていません。 
オートスケールの状態	Prisma Accessで自動スケーリングのステータスを表示します 。 • 許可済み- IPアドレスを許可リストに追加しました。多数のモバイル ユーザーが1つの場所にログインして自動スケール イベントをトリガーすると、Prisma Accessは自動スケール イベントに許可されたリストされたIPアドレスを使用します。 • 許可されていません- Prisma AccessUIですべてのIPアドレスを許可リストに追加するように指定していないか、変更を追加済みとしてマークした後にコミットしてプッシュしていません。Prisma Accessが自動スケール イベントをトリガーした場合、Prisma Accessは、その場所に容量を追加するため

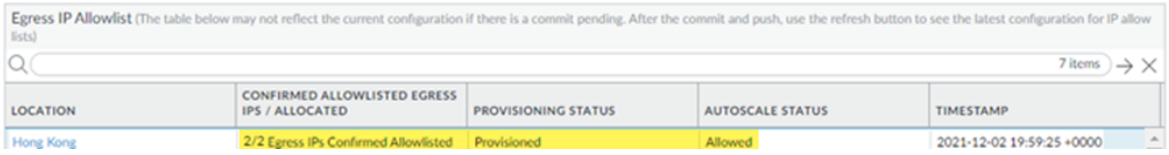
 ©2025 Palo Alto Networks, Inc.

項目	詳説
	に追加のIPアドレスをプロビジョニングしません。 場所を追加するたび、または自動スケールイベントの結果としてPrisma AccessがIPアドレスを追加するたびに、出口IP許可リストテーブルを含むページを更新し、[許可リストに追加済み] を指定してIPアドレスが組織の許可リストに追加されていることをマークし、変更をコミットしてプッシュする必要があります。 自動スケール イベントの結果としてPrisma Accessが追加するIPアドレスを常に把握できるように、Prisma AccessのIPアドレスの変更を通知するURLをセットアップできます。
タイムスタンプ	協定世界時 (UTC) でこの地域にIPが割り当てられた最後の既知の時刻。

コミットしてプッシュした後、IPアドレスがPrisma AccessUIで許可リストに登録されていることをまだ確認していないため、[確認済み] 列に**0/2 Egress IPs Confirmed Allow Listed**というステータスが表示されます。

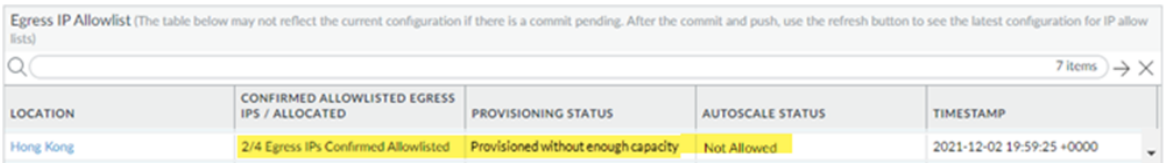
モバイル ユーザーのロケーションをオンボードすると、Prisma Accessは2つの出口IPアドレス (アクティブなIPアドレス1つと、自動スケール イベントの場合に使用するアドレス1つ) を提供します。以下は、自動スケール イベント後にPrisma Accessが出口IPアドレスを割り当ててプロビジョニングする方法の例を示しています。

自動スケールイベント- 多数のモバイル ユーザーが同時にモバイル ユーザーのロケーションにログインすると、そのイベントにより、Prisma Accessは多数のユーザーに対応するために2つの出口 IPアドレスの追加セットを割り当てることがあります。最初の2つの出口IPアドレスを許可リストに登録すると、自動スケール イベント前のステータスには、次のスクリーンショットの香港の場所に示すように、2つの出口IPアドレスが許可リストに登録され、確認ステータスが**[2/2 Egress IPs Confirmed Allow Listed]**、プロビジョニング ステータスが [プロビジョニング済]、自動スケール ステータスが[許可済]として表示されます。

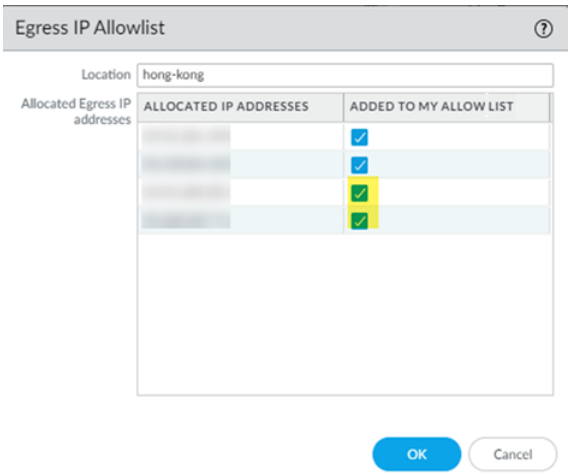


 ©2025 Palo Alto Networks, Inc.

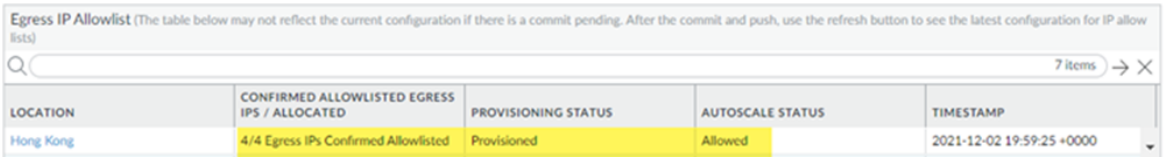
多数のモバイルユーザーが同時に香港のロケーションにログインすると、 Prisma Accessはバックアップ出口IPアドレスをアクティブにし、さらに2つのIPアドレスを割り当てて、そのうちの1つをアクティブにします。自動スケール イベントが発生すると、出口IPアドレスは割り当てられていますがプロビジョニングされておらず、確認ステータスは **[2/4 Egress IPs Confirmed Allow Listed]**となり、プロビジョニング ステータスは **[Provisioned without enough capacity (**十分なキャパシティのないプロビジョニング**)]**と表示されます。さらに、自動スケールのステータスには 「未許可」と表示されます。これは、自動スケール イベントが発生した場合、Prisma Accessはデプロイメントに追加の出口IPアドレスをプロビジョニングしないことを意味します。



新しい出口IPアドレスを許可リストに追加したら、場所名を選択し、追加された2つのIPアドレスに対して **[**許可リストに追加**]** を選択し、変更を コミットしてプッシュします 。



完了すると、香港のロケーションでは、4つの出口IPアドレスがすべて確認およびプロビジョニングされ、自動スケーリングがアクティブになっていることが示されます。



GlobalProtectアプリケーションのアップグレード

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	• Prisma Accessライセンス

©2025 Palo Alto Networks, Inc.

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	

Prisma AccessがホストするGlobalProtectアプリケーションのバージョンは、組織のMacOSおよびWindowsユーザーがPrisma Accessポータルからダウンロードできます。Prisma AccessはGlobalProtectアプリケーションの複数のバージョンを提供しており、そのうちの1つをアクティブ バージョンにすることができます。モバイルユーザーによるGlobalProtectアプリケーションへのアクセスを管理したり、段階的なアップグレードを実施することも可能です。

- Prisma Access用のアクティブなGlobalProtectアプリケーションのバージョンを選択する
- ユーザーがGlobalProtectアプリケーションをアップグレードできるようにする
- GlobalProtectアプリケーションのアップデートを段階的に実施

Prisma Access用のアクティブなGlobalProtectアプリケーションのバージョンを選択する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

Prisma Accessは、WindowsおよびMac OSユーザーの、GlobalProtectアプリケーションのバージョンを管理しています。さまざまなバージョンのGlobalProtectアプリケーションが用意されていますが、Prisma Accessでは1つのバージョンしかアクティブにすることはできません。モバイル ユーザーが Prisma Access ポータルにログインすると、アクティブなバージョンは、モバイル ユーザーが Windows および macOS デバイスにダウンロードしてインストールできるバージョンになります。

マルチテナント デプロイメントでは、複数のバージョンのGlobalProtectを選択することができます。GlobalProtectアプリケーションのバージョン設定はテナント単位で適用されます。全体的な設定ではありません。アプリケーションのバージョン管理は、テナント単位に行います。

IP 最適化などの一部の機能を使用するには、ユーザーが GlobalProtect の十分に更新されたバージョンを使用している必要があります。Prisma AccessでアクティブなGlobalProtectアプリケーションのバージョンを選択する方法については、続きをお読みください。

- Strata Cloud Manager
- Panorama

Prisma Access (Managed by Strata Cloud Manager)用のアクティブなGlobalProtectアプリケーションのバージョンを選択する

Service Setup（サービス設定）ページで、現在のアクティブなバージョンを別のバージョンに変更するには、以下の手順に従ってください。

STEP 1 | [ワークフロー] > **Prisma Access**[セットアップ] > [モバイル ユーザー] を設定し、**[GlobalProtect**接続]パネルを見つけます。

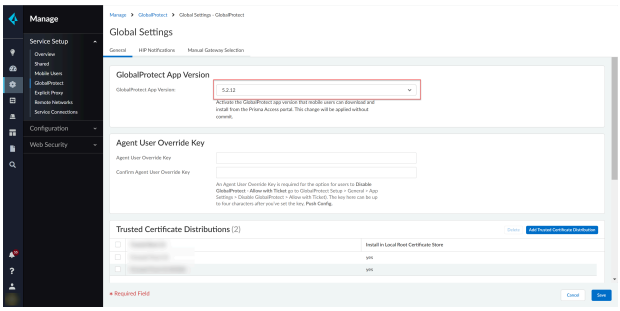
©2025 Palo Alto Networks, Inc.

STEP 2 | GlobalProtectがまだ有効になっていない場合は、**[GlobalProtect** セットアップ**]** を選択するか、**[GlobalProtect** セットアップ**]** > 有効にします 。

STEP 3 | **GlobalProtect**アプリケーションタブを選択し、 **Global**アプリ設定を編集します。

STEP 4 | **Global Settings (Global**設定**)** ページの 一般 タブで、モバイルユーザーがPrisma Access ポータルからダウンロードしてインストールできるようにする**GlobalProtect**アプリケーションのバージョンを選択します。

アクティブなバージョンはドロップダウン リストに表示されます。



Prisma Access (Managed by Panorama)用のアクティブな**GlobalProtect**アプリケーションのバージョンを選択する

現在アクティブになっているバージョンのサポートが終了すると、Prisma Accessよりその旨を知らせてサポートされているバージョンをアクティベートするように要求するメッセージが表示されます。

Service Setup（サービス設定）ページで、現在のアクティブなバージョンを別のバージョンに変更するには、以下の手順に従ってください。

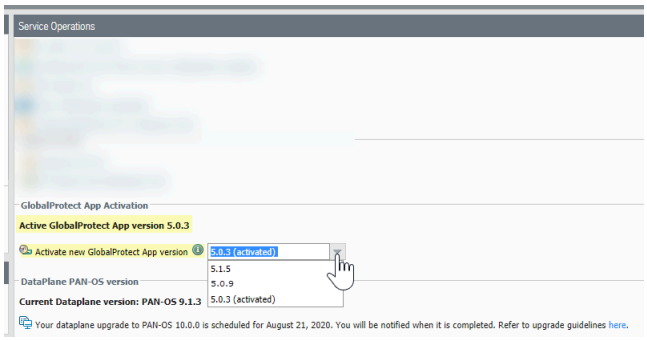
FedRAMP 環境で*Prisma Access*を使用する場合、*GlobalProtect*の*FIPS*認証バージョン（バージョン *5.1.4*）を使用する必要があります。デフォルトのGlobalProtectバージョンを5.1.4から変更した 場合、*Panorama UI*からバージョン*5.1.4*を選択することはできません。再度追加するには、*Palo Alto Networks*テクニカル サポートにサポート ケースを発行してください。

STEP 1 | **Panorama** > **Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Service Setup**（サービスのセットアップ）を選択します。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | [新しい**GlobalProtect**アプリケーションバージョンをアクティベートする]を選びます。

アクティブなバージョンがドロップダウンリストに表示されます。

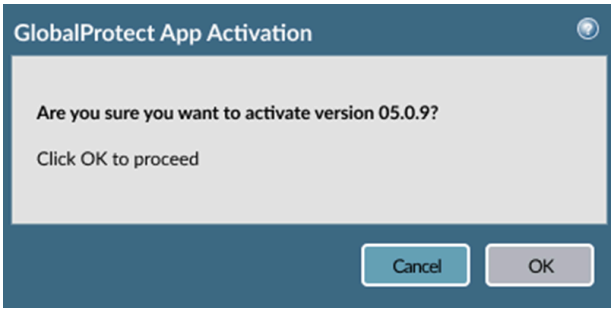


現在のバージョンの*GlobalProtect*が期限切れ（*EoL*）になると、*Service Setup*（サービス設定）ページのこの領域にメッセージが表示されます。このメッセージが表示されたら、次の手順に進んで*GlobalProtect*アプリケーションのバージョンをアップグレードしてください。

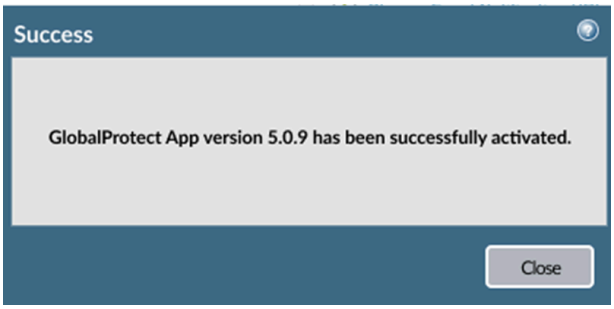


STEP 3 | アップグレードするバージョンを選択します。

選択内容を確認するウィンドウが表示されます。



アプリケーションをアクティブ化したら、正常に処理が完了したことを示すメッセージが表示されます。



 ©2025 Palo Alto Networks, Inc.

STEP 4 | [システムステータス]ページを表示して、 アクティブな**GlobalProtect**アプリケーションのバージョンを検証します。

ユーザーが**GlobalProtect**アプリケーションをアップグレードできるようにする

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

GlobalProtectデプロイメントのためのGlobalProtectアプリケーション バージョンへのモバイル ユーザーのアクセスを制御する方法について学習します。

- Strata Cloud Manager
- Panorama

ユーザーが**GlobalProtect**アプリケーションをアップグレードできるようにする（**Strata Cloud Manager**）

Prisma Accessによってホストされているアクティブな**GlobalProtect**アプリケーション バージョンへのモバイル ユーザー アクセスを管理できます。Prisma Access (Managed by Strata Cloud Manager)でこれを行うには、アップグレード グローバル保護設定を構成します。Prisma Access (Managed by Strata Cloud Manager)にむけて、次の手順を実行します。

STEP 1 | [ワークフロー] > **Prisma Access**[セットアップ] > [モバイル ユーザー] を設定し、**[GlobalProtect**接続]パネルを見つけます。

STEP 2 | GlobalProtectがまだ有効になっていない場合は、**[GlobalProtect** セットアップ] を選択するか、**[GlobalProtect** セットアップ] > 有効にします 。

STEP 3 | **GlobalProtect**アプリケーションタブを選択し、 アプリ設定を追加します。

STEP 4 | **App Configurations**（アプリ設定）エリアで、**[GlobalProtect**アプリケーションのアップグレード]で選択を行い、Prisma Accessが提供しているアクティブなバージョンのGlobalProtectアプリをモバイルユーザーがアップグレードできるかどうか、またできる場合にアップグレード時期を選択できるかどうかを指定します。

- **Allow with Prompt**（プロンプト付きで許可）（デフォルト） – ファイアウォールで新しいバージョンが起動された場合にプロンプトを表示し、ユーザーは任意のタイミングでアップグレードを行うことができます。
- **Disallow**（無効） – ユーザーはアプリのアップグレードを行うことができません。
- **Allow Manually**（手動を許可） – ユーザーはGlobalProtectアプリケーションで **Check Version**（バージョンの確認）を選択することで、アップグレードの確認と実行を手動で行うことができます。
- **Allow Transparently (**透過を許可**)** – ポータルで新しいバージョンが使用可能になるとアプリのソフトウェアを自動的にアップグレードします。

 ©2025 Palo Alto Networks, Inc.

- ユーザーが企業ネットワーク内にいるときに許可する–新しいバージョンがポータルで利用可能になると、アプリ ソフトウェアを自動的にアップグレードしますが、エンドポイントが社内ネットワークに接続されるまで待ちます。これにより、低帯域幅の接続を使用したアップグレードによる遅延を防ぎます。

ユーザーが**GlobalProtect**アプリケーションをアップグレードできるようにする（**Panorama**）

Prisma Accessによってホストされているアクティブな GlobalProtectアプリケーション バージョンへのモバイル ユーザー アクセスを管理できます。Prisma Access (Managed by Strata Cloud Manager)でこれを行うには、アップグレード グローバル保護設定を構成します。Prisma Access (Managed by Panorama)にむけて、次の手順を実行します。

STEP 1 | **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル）を選択します

STEP 2 | **Template**（テンプレート）ドロップダウンから**Mobile_User_Template**を選択します。

STEP 3 | Prisma Accessポータル設定を編集するには、**GlobalProtect_Portal**を選択します。

STEP 4 | **Agent (**エージェント**)**タブを選択して、設定を選択します。

STEP 5 | **App**（アプリケーション）タブを選択します。

STEP 6 | **App Configurations**（アプリ設定）エリアで、**Allow User to Upgrade GlobalProtect App**（ユーザーに**GlobalProtect**アプリケーションのアップグレードを許可）で選択を行い、Prisma Accessが提供しているアクティブなバージョンのGlobalProtectアプリケーションをモバイルユーザーがアップグレードできるかどうか、またできる場合にアップグレード時期を選択できるかどうかを指定します。

- **Allow with Prompt**（プロンプト付きで許可）（デフォルト） – ファイアウォールで新しいバージョンが起動された場合にプロンプトを表示し、ユーザーは任意のタイミングでアップグレードを行うことができます。
- **Disallow**（無効） – ユーザーはアプリのアップグレードを行うことができません。
- **Allow Manually**（手動を許可） – ユーザーは GlobalProtect アプリで **Check Version**（バージョンの確認）を選択することで、アップグレードの確認と実行を手動で行うことができます。
- **Allow Transparently**（メッセージを表示せずに実行） – ポータルで新しいバージョンが使用可能になるとアプリのソフトウェアを自動的にアップグレードします。
- **Internal**（内部） – ポータルで新しいバージョンが使用可能になるとアプリのソフトウェアを自動的にアップグレードしますが、エンドポイントが企業ネットワークに内部接続するまで待機します。これにより、低帯域幅の接続を使用したアップグレードによる遅延を防ぎます。

GlobalProtectアプリケーションのアップデートを段階的に実施

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

©2025 Palo Alto Networks, Inc.

大規模な組織を管理している場合、段階的にモバイルユーザーを最新バージョンのGlobalProtectアプリに更新させることができます。たとえば、まず小規模なグループにGlobalProtectアプリを更新させ、その後組織内の全員にアップデートを公開することができます。そのためには、次の作業を行ってください。

STEP 1 | まだ作成していない場合は、GlobalProtectアプリケーションのアップデートを公開する、最初のユーザーグループを作成します。

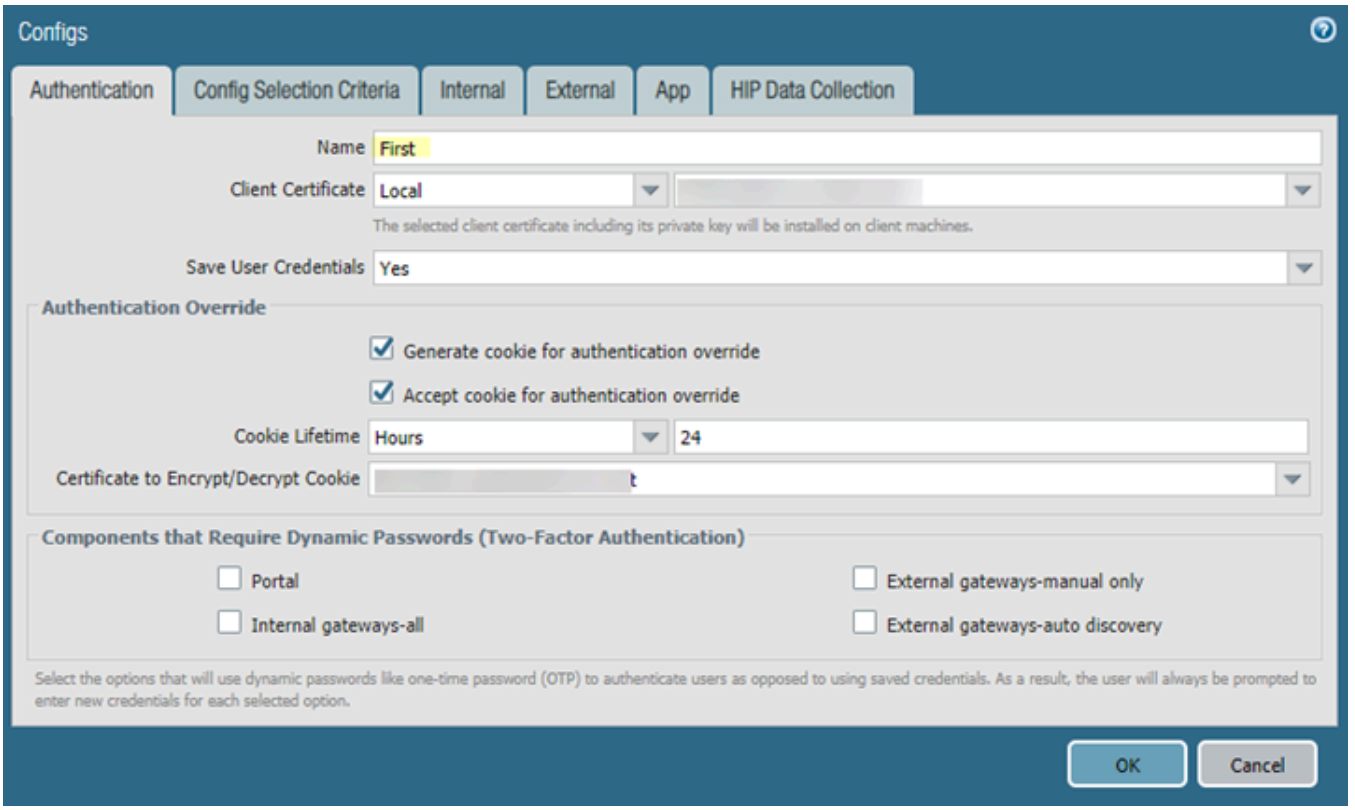
を使ってユーザーをグループにマップする、または**Device**（デバイス） > **Local User Database**（ローカルユーザーデータベース） > **User Groups**（ユーザーグループ）を選択して、手動でグループを作成することができます。

©2025 Palo Alto Networks, Inc.

STEP 2 | 最初のユーザーグループに対して使用する、新たなGlobalProtectエージェント設定を作成します。

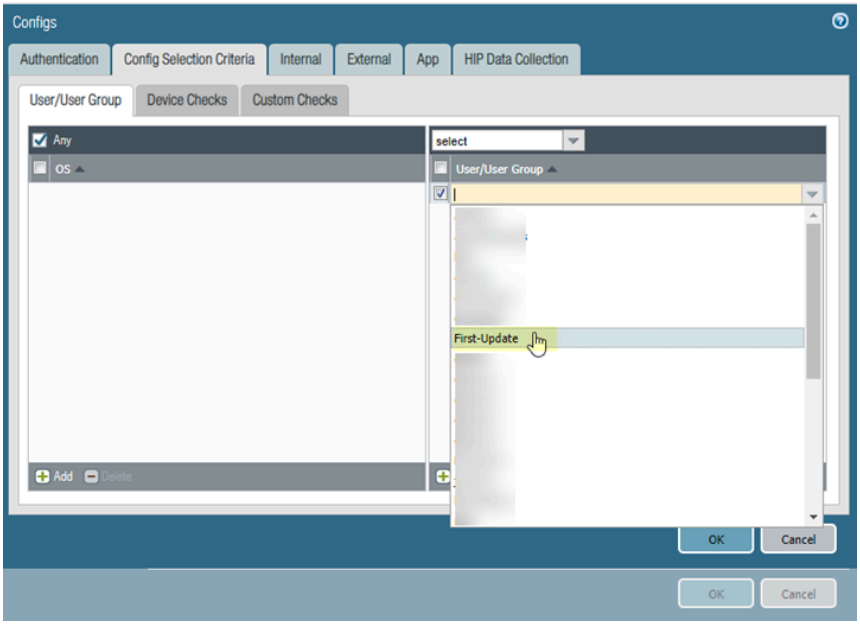
1. Panoramaで、**Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル）を選択します。
2. **Template**（テンプレート）ドロップダウンから**Mobile_User_Template**を選択します。
3. Prisma Accessポータル設定を編集するには、**GlobalProtect_Portal**を選択します。
4. **[エージェント]** タブを選択します。
5. **DEFAULT**（デフォルト）設定を選択して、それを**Clone**（複製）します。

   また、新たな設定を**Add**（追加）することもできます。ただし、既存の設定を複製すると、新しい設定の必須情報にコピーされます。
6. 設定の**Name**（名前）を指定します。



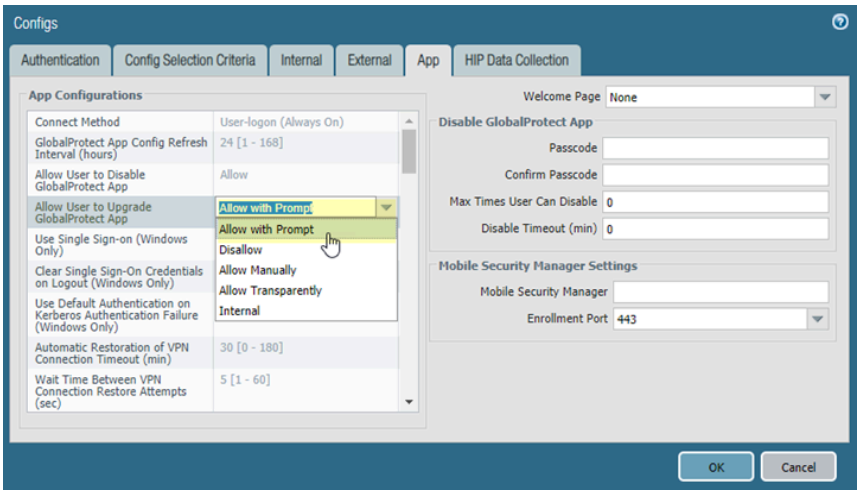
7. **Config Selection Criteria**（選択条件の設定）タブを選択します。
8. **User/User Group**（ユーザー/ユーザーグループ）で、ステップ1で作成したユーザーを選択します。

 ©2025 Palo Alto Networks, Inc.



9. **App**（アプリケーション）タブを選択します。
10. **Allow User to Upgrade GlobalProtect App**（**GlobalProtect**アプリケーションのアップグレードをユーザーに許可）を**Allow with Prompt**（メッセージを表示して許可）または**Allow Transparently**（そのまま許可）に変更します。

    Allow with Prompt（メッセージを表示して許可）では、新しいバージョンがアクティブになった時にユーザーにメッセージが表示され、任意の時点でのソフトウェアのアップグレードを可能にします。**Allow Transparently**（そのまま許可）は、ポータルで新しいバージョンが利用できるようになると、自動的にソフトウェアをアップグレードします。

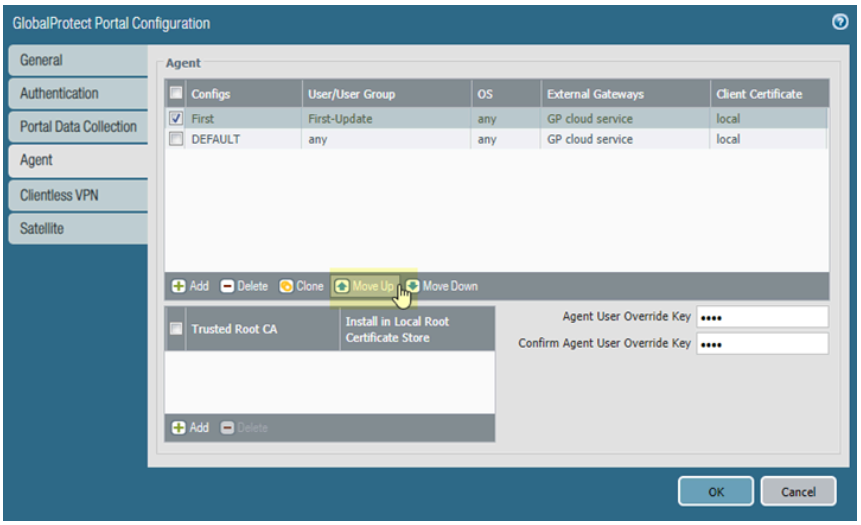


11. **OK** をクリックして変更内容を保存します。

©2025 Palo Alto Networks, Inc.

STEP 3 | 自分の設定をデフォルトの設定よりも優先させるには、**Move Up**（上に移動）を選択します。

アプリに接続すると、ポータルは、パケットの送信元の情報を、定義したエージェント設定と比較します。セキュリティ ルール評価によって、ポータルはリストの先頭から一致を検索します。一致が見つかると、ポータルは対応する設定をアプリに配信します。



STEP 4 | **DEFAULT**（デフォルト）の設定に対してこれらの手順を繰り返します。ただし、ユーザーが最新のGlobalProtectアプリケーションにアップデートすることを防止するために、**Allow User to Upgrade GlobalProtect App**（ユーザーに**GlobalProtect**アプリケーションのアップグレードを許可）を**Disallow**（許可しない）に変更してください。

STEP 5 | 残りのユーザーにアプリケーションをアップデートさせたい場合は、**DEFAULT**設定の**Allow User to Upgrade GlobalProtect App**を、アップデートを許可する設定に変更します（**Allow with Prompt**または**Allow Transparently**）。

Prisma AccessをオンプレミスのGlobalProtectゲートウェイと統合する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	• Prisma Accessライセンス

Prisma Accessを利用すれば、独自のグローバルセキュリティインフラを構築して運用の手間を増加させることなく、Palo Alto Networksセキュリティプラットフォームをリモートネットワークのロケーションおよびモバイルユーザーにまで拡張することができます。GlobalProtectゲートウェイを管理するためのインフラをすでに持っている地域に、GlobalProtectゲートウェイをすでに導入している場合、適切なときにモバイルユーザーを既存の外部ゲートウェイに誘導するようにPrisma Accessを設定することで、この投資を活用することができます。

©2025 Palo Alto Networks, Inc.

Prisma Accessゲートウェイとオンプレミスゲートウェイの優先順位を管理することができ、オンプレミ スゲートウェイとPrisma Accessゲートウェイの優先順位を指定することができます。管理者は、モバイルユーザーが特定のPrisma Accessゲートウェイに接続するように指定することはできませんが、GlobalProtectアプリケーションを使用して、モバイルユーザーが特定のPrisma Accessゲートウェイを手動で選択できるようにすることはできます。

*Prisma Access*で独自のポータルを使用することはできません。モバイルユーザー向け*Prisma Access*のプロビジョニング時にデプロイされていたポータルのみが使用できます。

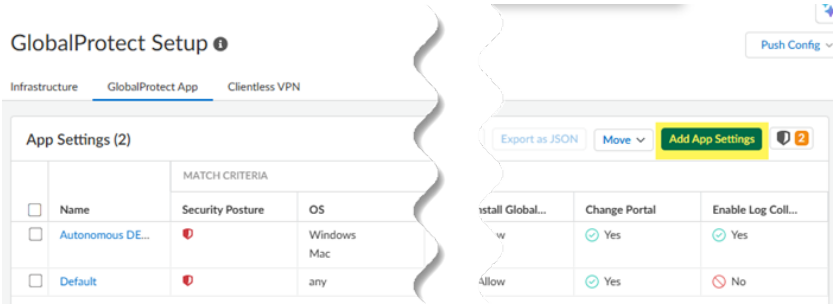
- Strata Cloud Manager
- Panorama

オンプレミスのGlobalProtectゲートウェイとPrisma Accessを統合する (Prisma Access (Managed by Strata Cloud Manager))

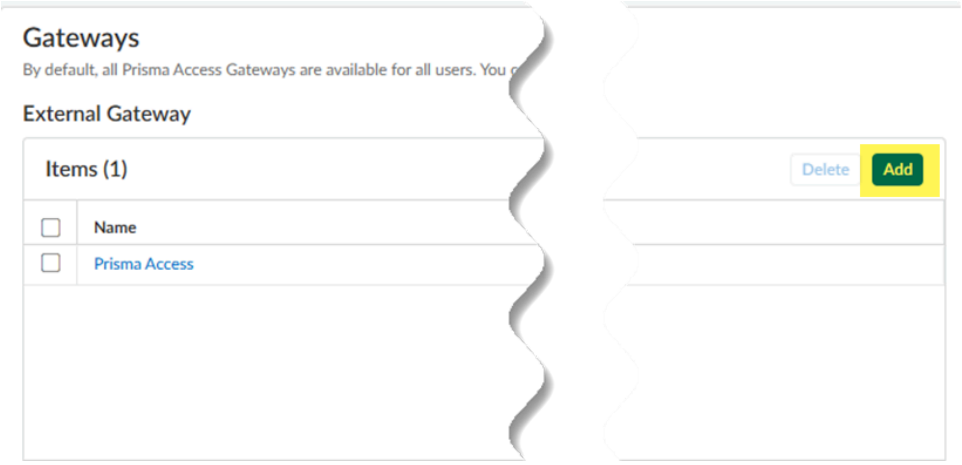
©2025 Palo Alto Networks, Inc.

STEP 1 | オンプレミスゲートウェイを、エージェント設定のゲートウェイのリストに追加します。

1. **[ワークフロー]** > **[Prisma Access セットアップ]** > **[GlobalProtect]**へと移動し**[GlobalProtect**アプリケーション**]**タブを選択します。
2. アプリケーション設定を追加します。



3. 外部ゲートウェイを追加します。



新しいエージェントを追加して、その設定の外部ゲートウェイのリストに*Prisma Access*ゲートウェイを追加したい場合、***Name***（名前）に***GP cloud service***（***GP***クラウドサービス）、***Address***（アドレス）に***gpcloudservice.com***を設定する必要があります。これらの値を表示されている通りに入力します。*Prisma Access*以外のゲートウェイにこれらの値を使用することはできません。

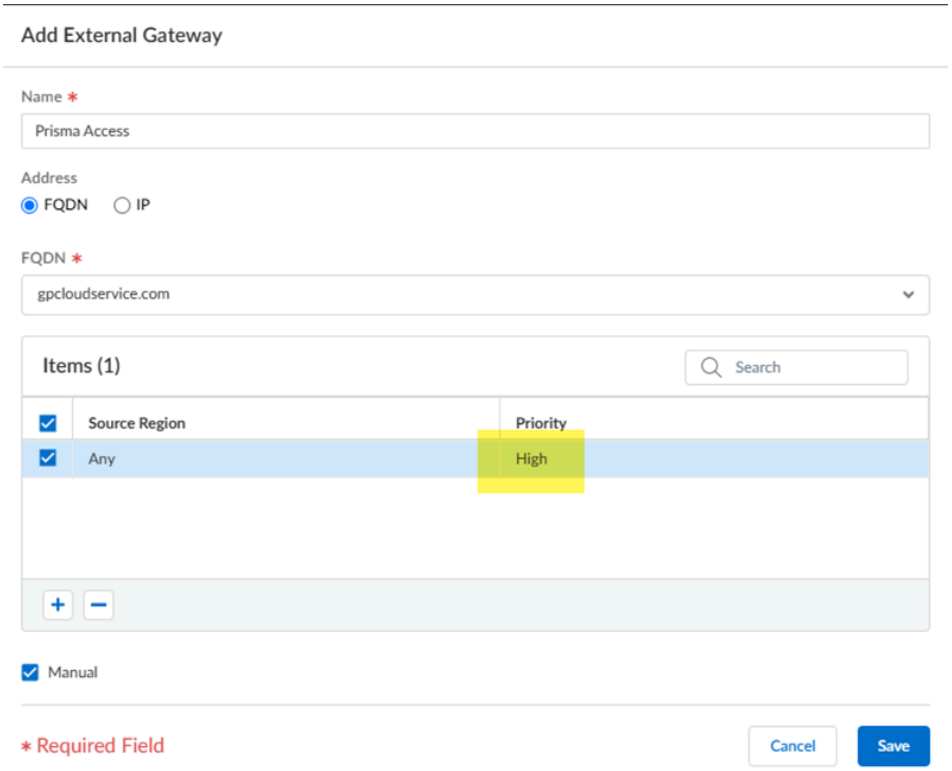
4. ゲートウェイの**Name**（名前）を入力して、ゲートウェイの**FQDN**または**IP**アドレスを**Address**（アドレス）フィールドに入力します。この値は、ゲートウェイ証明書の共通名（CN）と完全に一致させる必要があります。
5. （任意） モバイルユーザーが対応する地域にいる時にのみ当該ゲートウェイに接続させたい場合は、ゲートウェイを制限する**Source Region**（ソース地域）を**Add**（追加）します。たとえばゲートウェイがフランスにある場合は、FR（フランス）を選択

 ©2025 Palo Alto Networks, Inc.

します。スウェーデンにゲートウェイがある場合は、SE（スウェーデン）を選択します。

この方法の利点の1つとして、ユーザーは各自の言語に対応したインターネットリソースにアクセスできるゲートウェイを利用できることが挙げられます。

6. (任意) ゲートウェイ設定で優先順位を指定します。
   オンプレミスゲートウェイは、より高い優先度に設定することも、より低い優先度に設定することもできます。
   - オンプレミスゲートウェイをデフォルトPrisma Accessゲートウェイよりも低い優先度に設定するには、優先度を**[High (高)]**または**[Medium (中)]**に設定します。
     ゲートウェイをさらに追加し、ゲートウェイごとに異なる優先順位を設定したい場合は、優先度を**[High (高)]**、**[Medium (中)]**、**[Low (低)]**、または**[Lowest (最低)]**に設定できます。
   - オンプレミスゲートウェイをデフォルトよりも高い優先度に設定するには、優先度を**[Highest (最高)]**に設定します。
     オンプレミスゲートウェイをより高い優先度に設定する場合は、デフォルトの**Prisma Access**ゲートウェイも編集し、優先度を**[Highest (最高)]**よりも低い優先度に設定する必要があります。

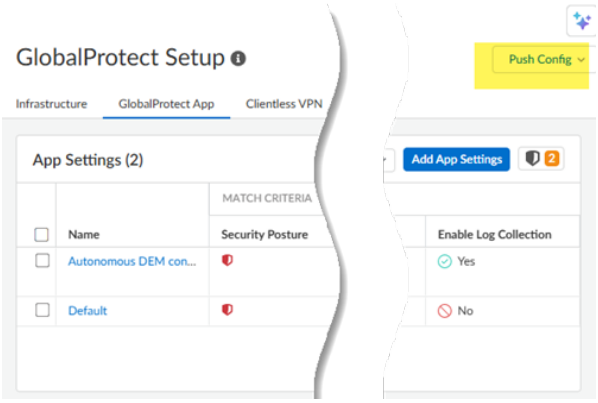


7. **[Manual (手動)]**を選択します。
   このチェック ボックスを選択すると、GlobalProtectユーザーはGlobalProtectアプリケーションでこの外部ゲートウェイを手動で選択できます。

STEP 2 | 変更を保存します。

©2025 Palo Alto Networks, Inc.

STEP 3 | 構成をプッシュします。



Prisma AccessをオンプレミスのGlobalProtectゲートウェイと統合する （Prisma Access (Managed by Panorama)

これらのハイブリッドPrisma Accessデプロイメント環境を設定するには、Mobile_User_Template内のGlobalProtect_Portal設定を編集して、適切な地域にオンプレミスゲートウェイを追加する必要があります：

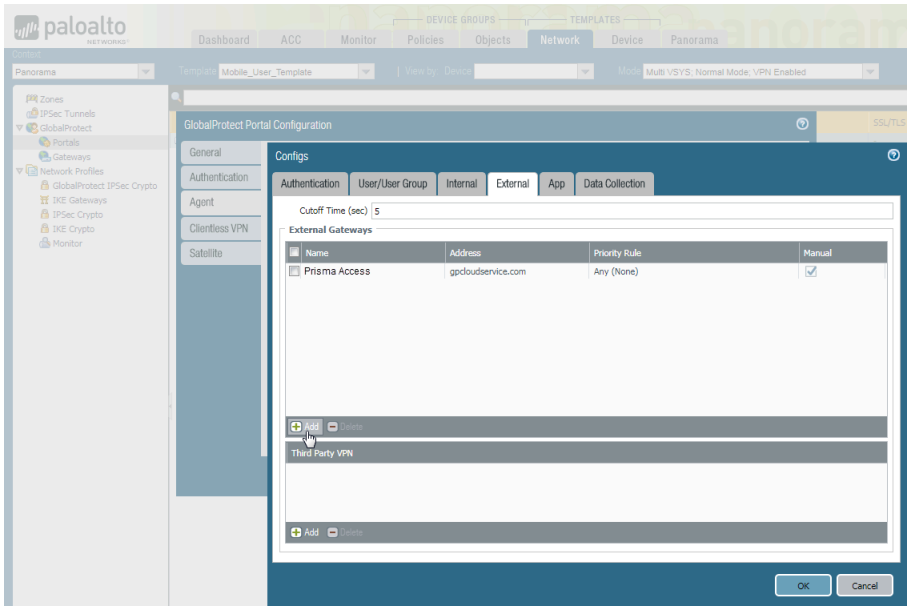
STEP 1 | Prisma Accessポータル設定を編集します。

1. 既存のゲートウェイを利用可能なゲートウェイのリストに追加するには、**Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル）の順に選択します。
2. **Template**（テンプレート）ドロップダウン リストから**Mobile_User_Template**を選択します。
3. Prisma Accessポータル設定を編集するには、**GlobalProtect_Portal**を選択します。

©2025 Palo Alto Networks, Inc.

STEP 2 | オンプレミスゲートウェイを、エージェント設定のゲートウェイのリストに追加します。

1. **Agent**（エージェント）タブを選択し、**DEFAULT**（デフォルト）エージェント設定を選択するか、または新しい設定を**Add**（追加）します。
2. **External**（外部）タブを選択し、オンプレミスゲートウェイを**Add**（追加）します。



新しいエージェントを追加して、その設定の外部ゲートウェイのリストに*Prisma Access*ゲートウェイを追加したい場合、***Name***（名前）に***GP cloud service***（***GP***クラウドサービス）、***Address***（アドレス）に***gpcloudservice.com***を設定する必要があります。これらの値は表示されている通りに入力する必要があります。また、*Prisma Access*以外のゲートウェイにこれらの値を使用することはできません。

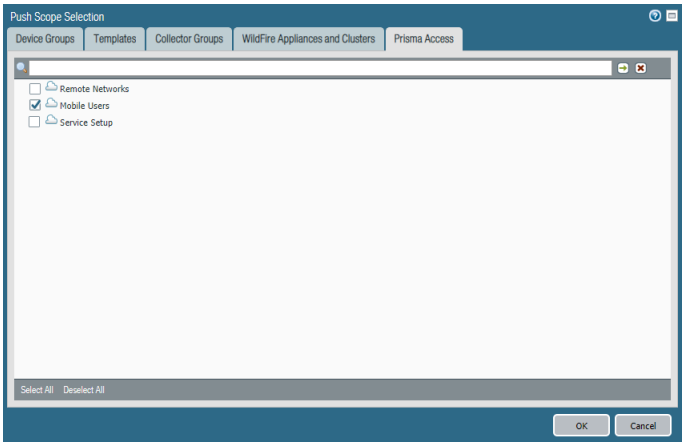
3. ゲートウェイの**Name**（名前）を入力して、ゲートウェイの**FQDN**または**IP**アドレスを**Address**（アドレス）フィールドに入力します。この値は、ゲートウェイ証明書の共通名（CN）と完全に一致させる必要があります。
4. （任意） モバイルユーザーが対応する地域にいる時にのみ当該ゲートウェイに接続させたい場合は、ゲートウェイを制限する**Source Region**（ソース地域）を**Add**（追加）します。たとえばゲートウェイがフランスにある場合は、FR（フランス）を選択します。スウェーデンにゲートウェイがある場合は、SE（スウェーデン）を選択します。

   この方法の利点の1つとして、ユーザーは各自の言語に対応したインターネットリソースにアクセスできるゲートウェイを利用できることが挙げられます。
5. (任意) ゲートウェイの優先度を設定します。
6. 必要に応じて他のエージェント設定を編集し、エージェント設定作業を完了します。
7. **[OK]** をクリックしてポータルの設定を保存します。

©2025 Palo Alto Networks, Inc.

STEP 3 | Panorama にすべての変更をコミットし、その設定変更をPrisma Accessにプッシュします。

1. **Commit**（コミット） > **Commit to Panorama**（**Panorama** へのコミット）をクリックします。
2. **Commit**（コミット） > **Push to Devices**（デバイスへのプッシュ）をクリックして、**Edit Selections**（選択内容の編集）をクリックします。
3. **Prisma Access**タブ上で、ユーザー向けの**Prisma Access**が選択されているのを確認して、**[OK]**をクリックします。



4. **Push**（プッシュ）をクリックします。

Prisma Accessとオンプレミス ゲートウェイの優先順位設定

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

モバイルユーザーと物理的にもっとも近い場所にあるオンプレミスゲートウェイを選択しておき、モバイルユーザーが別の場所に移動した場合でも安全なアクセスを行えるように、別のゲートウェイへの接続（オンプレミスまたはクラウド）を許可することができます。また、同じ国またはモバイルユーザーと同じ言語圏内にあるゲートウェイの優先度を指定することもできます。

ユーザーに特定のPrisma Accessゲートウェイへの接続を要求する場合、モバイルユーザーが特定のPrisma Accessゲートウェイを手動で選択できるようにすることができます。モバイルユーザーは、各自のエンドポイントにインストールされているGlobalProtectアプリを使って、いずれかのPrisma Accessゲートウェイを選択します。

Prisma Accessでゲートウェイの優先度を設定するには、次のワークフローを完了してください。

- オンプレミスゲートウェイとPrisma Accessゲートウェイの優先度を等しく設定する
- 1つのオンプレミスゲートウェイに対する高い優先度の設定
- 複数のオンプレミスゲートウェイに対する高い優先度の設定
- Prisma Accessおよびオンプレミス・ゲートウェイの優先順位を構成する

©2025 Palo Alto Networks, Inc.

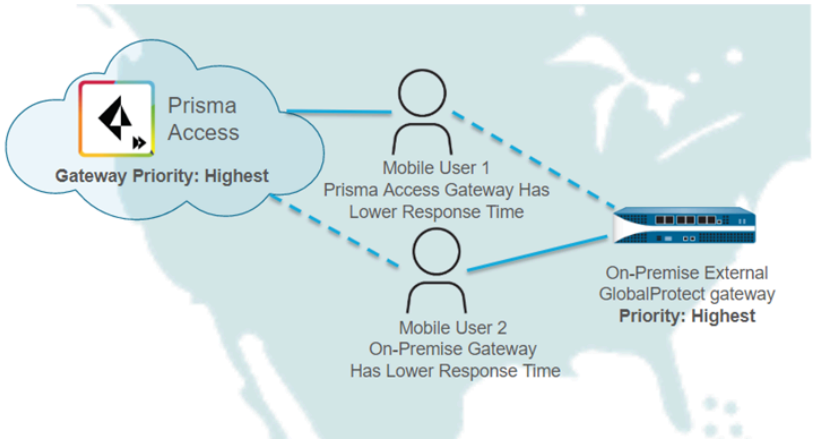
オンプレミスゲートウェイと**Prisma Access**ゲートウェイの優先度を等しく設定する

モバイルワーカーがどこにいる場合でも安全にアクセスできるように、オンプレミスGlobalProtectゲートウェイとPrisma Accessゲートウェイに等しい優先度を設定できます。GlobalProtectアプリは「複数ゲートウェイ設定でのゲートウェイの優先度」を利用して、使用するゲートウェイを判断します。

モバイルユーザーがオンプレミスゲートウェイにもっとも近いことが多い場合に、この設定を使用することができます。ユーザーがロケーションを変更すると、GlobalProtectアプリケーションはもっとも高い優先度およびもっとも短い応答時間を基準に、別のゲートウェイ（オンプレミスまたはPrisma Accessゲートウェイ）を選択します。

North America（北米）の2人のモバイルユーザーを持つ設定の例を以下の図に示します。Prisma Accessゲートウェイとオンプレミスゲートウェイの両方のゲートウェイの優先度を**Highest**（最高）に設定します。

この例で、ユーザー1のGlobalProtectアプリはPrisma Accessゲートウェイがオンプレミスゲートウェイより応答時間が短いと判断します。ユーザー2のGlobalProtectアプリは、オンプレミスゲートウェイがもっとも応答時間が短いと判断します。すべてのゲートウェイが同じ優先度を持っているため、応答時間の短さを基準にユーザー1はPrisma Accessゲートウェイに、ユーザー2はオンプレミスゲートウェイに接続します。



1つのオンプレミスゲートウェイに対する高い優先度の設定

モバイルユーザーにPrisma Accessゲートウェイではなくオンプレミスゲートウェイを使用させたい場合、Prisma Accessゲートウェイよりも優先度が高い、ソース地域が設定されているオンプレミスゲートウェイを指定します。

Indonesia（インドネシア）のモバイルユーザーに対する設定の例を以下の図に示します。モバイルユーザーがSingapore（シンガポール）にあるもっとも近いPrisma Accessゲートウェイに接続することを防止するために、Indonesiaのオンプレミスゲートウェイの優先度を**Highest**（最高）に設定し、Prisma Accessゲートウェイの優先度を**Medium**（中）に設定します。

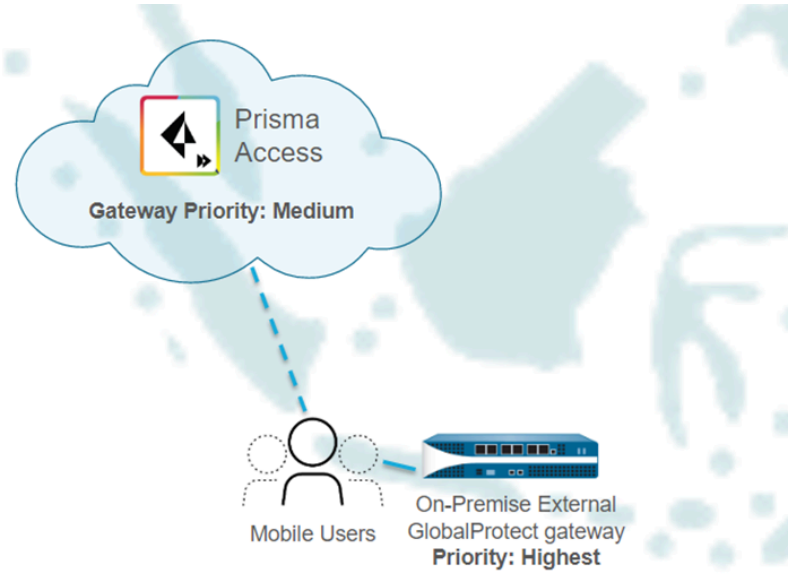
この例では、オンプレミスゲートウェイ向けに、Indonesiaのソース地域も指定します。次の理由から、ソース地域を指定することをお勧めします。

- オンプレミスゲートウェイのソース地域を指定すると、その地域内のユーザーはそのゲートウェイにアクセスし、その地域外のユーザーがそのゲートウェイに接続することを防止できます。この例では、Indonesiaのモバイルユーザーのみが、ソース地域がIndonesiaのオンプ

©2025 Palo Alto Networks, Inc.

レミスゲートウェイに接続できます。また優先度の高さにより、オンプレミスゲートウェイがPrisma Accessゲートウェイよりも優先されます。

- Indonesia内のオンプレミスゲートウェイに対してソース地域**Any**（任意）を設定した場合、組織内の各モバイルユーザーに対してIndonesiaのオンプレミスゲートウェイが優先されます（優先度が高く、ワールドワイドにアクセス可能なため）。この設定を行うと、モバイルユーザーはPrisma Accessゲートウェイに接続しなくなる可能性があります。



複数のオンプレミスゲートウェイに対する高い優先度の設定

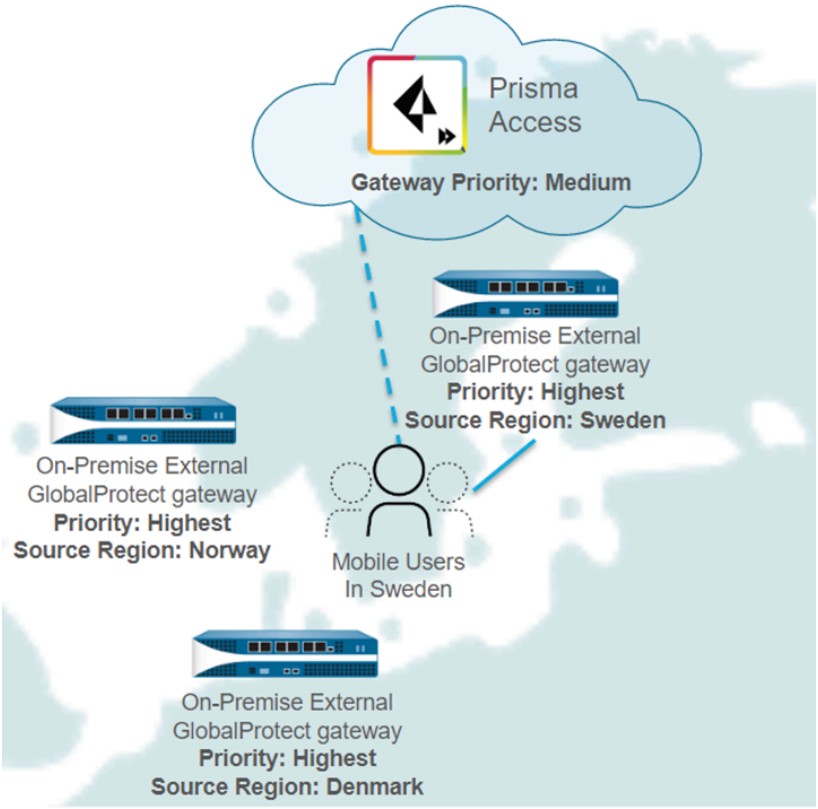
インターネットへのトラフィックを言語固有の地域に限定するために、各ソース地域内の複数のゲートウェイの設定を編集して、オンプレミスゲートウェイの優先度を**Highest**（最高）に、Prisma Accessゲートウェイの優先度を**Medium**（中）に設定することができます。

Scandinavia（スカンジナビア）のモバイルユーザーに対する設定の例を以下の図に示します。この設定を使って、モバイルユーザーがインターネットのWebサイトにアクセスする場合、Webサイトはその言語固有の文字エンコードセットを使用します。

この例では、Denmark（デンマーク）、Norway（ノルウェー）、Sweden（スウェーデン）内のソース地域のオンプレミスゲートウェイの設定を編集します。それらの地域のゲートウェイの優先度を**Highest**（最高）に、Prisma Accessゲートウェイの優先度を**Medium**（中）に設定します。オンプレミスゲートウェイのソース地域を指定することで、それらの地域のユーザーをそのゲートウェイにアクセスさせ、地域外のユーザーによるそれらのゲートウェイへの接続を防止できます。

この例では、ソース地域とゲートウェイの優先度の高さにより、GlobalProtectアプリケーションはスウェーデンのモバイルユーザーに対して、スウェーデンのオンプレミスゲートウェイを選択します。

©2025 Palo Alto Networks, Inc.



Prisma Accessおよびオンプレミス・ゲートウェイの優先順位を構成する

Prisma Accessでオンプレミスゲートウェイを使用しているデプロイ環境の優先度を設定するには、このワークフローを使用してください。

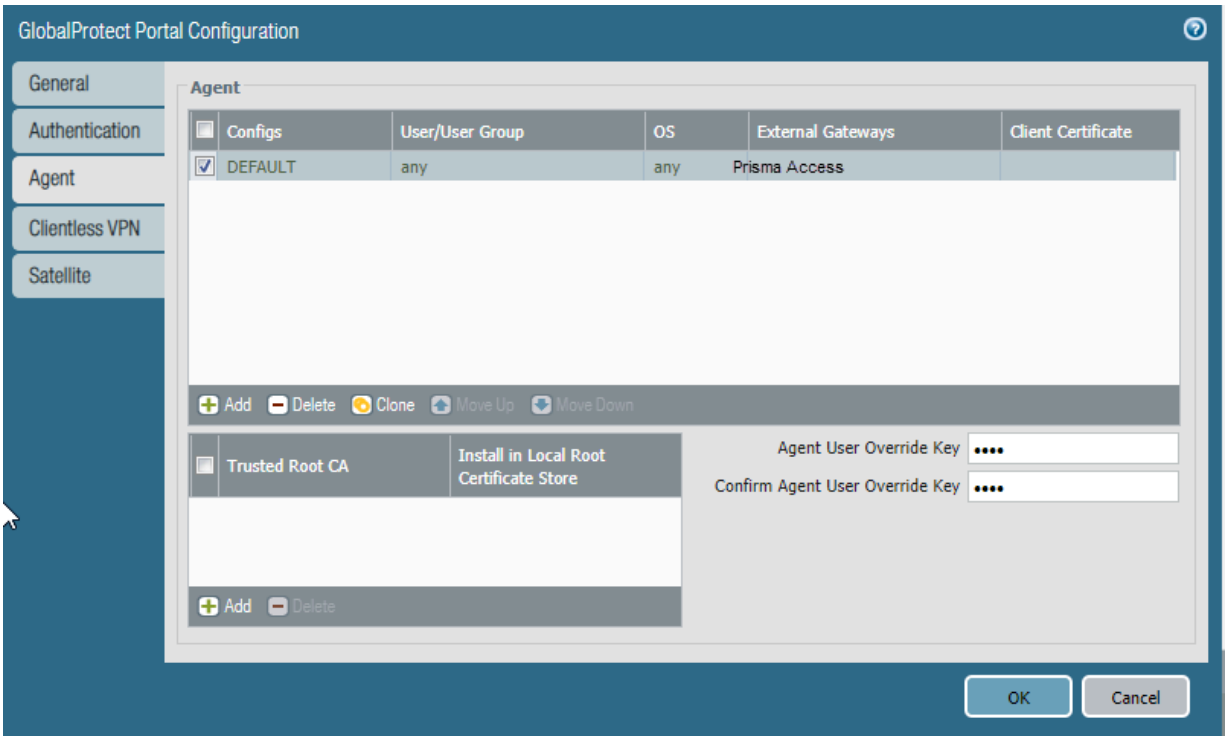
STEP 1 | Prisma Accessにログインします。

STEP 2 | **Mobile_User_Template**テンプレート内で、**Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル）の順に選択します。

STEP 3 | **Name**（名前）フィールドのポータル名をクリックします。

©2025 Palo Alto Networks, Inc.

STEP 4 | **Agent**（エージェント）タブをクリックします。



STEP 5 | 設定するエージェントの名前をクリックします。

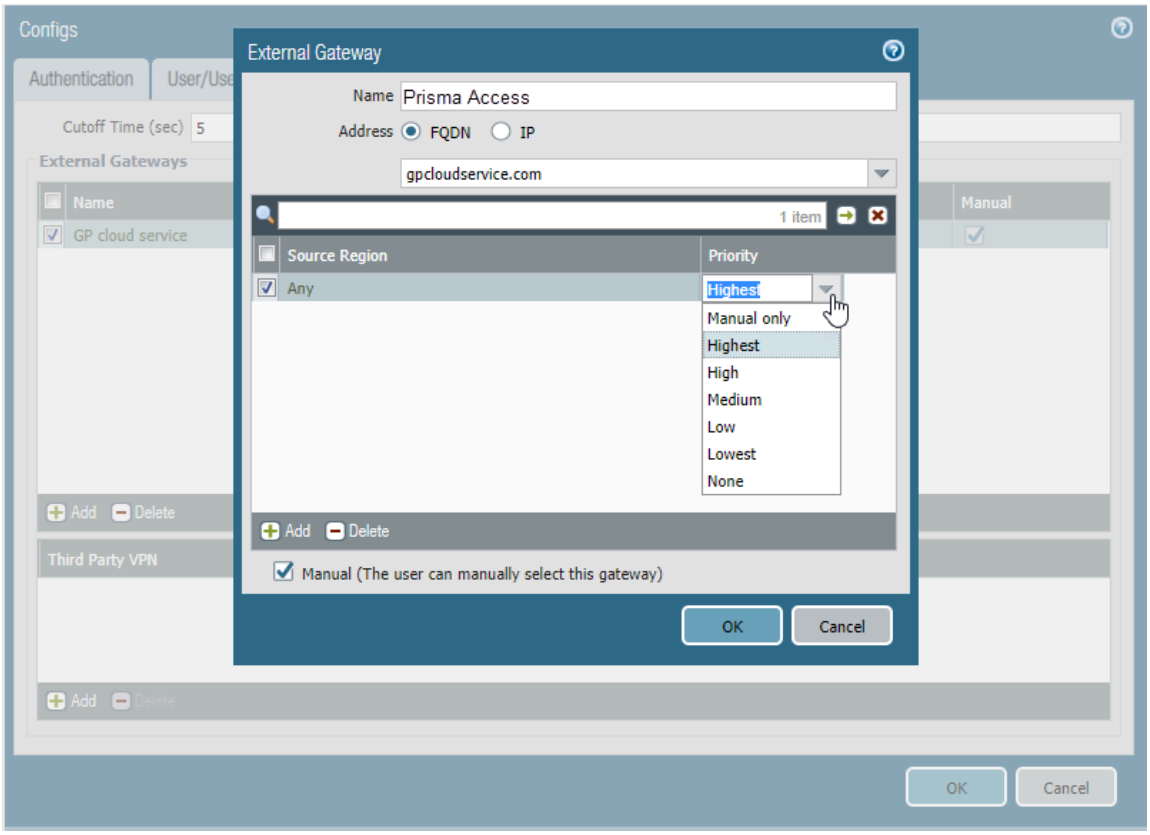
デフォルトのエージェント名は、**DEFAULT**となっています。

STEP 6 | **External**（外部）タブをクリックします。

©2025 Palo Alto Networks, Inc.

STEP 7 | Prisma Accessゲートウェイの優先度を設定します。

1. **GP cloud service**（**GP**クラウドサービス）をクリックします。
2. 優先する環境設定の優先度を設定します。
   - オンプレミスとPrisma Accessゲートウェイに同じゲートウェイ優先度を設定するには、優先度を「なし」から「最高」に変更します。
   - オンプレミスゲートウェイに高いゲートウェイ優先度を設定するか、複数のオンプレミスゲートウェイに高い優先順位を設定するには、優先度を「なし」から「中」に変更します。



3. **Manual**（手動）チェックボックスが選択されていることを確認します。

   Manual（手動）チェックボックスを選択すると、モバイルユーザーは必要に応じて特定のPrisma Accessゲートウェイを選択できるようになります。

©2025 Palo Alto Networks, Inc.

*Prisma Access*ゲートウェイのソース地域を追加しないでください。指定した地域は、設定には適用されません。

4. **OK** をクリックします。

©2025 Palo Alto Networks, Inc.

STEP 8 | 設定に、1つまたは複数の外部ゲートウェイを**Add**（追加）します。

1. **Name**（名前）フィールドに分かりやすいゲートウェイ名を入力します。

   入力する名前は、ゲートウェイを設定したときに定義した名前と一致している必要があります。また、ユーザーが接続するゲートウェイのロケーションを理解できるように、分かりやすい名前にする必要があります。

2. ゲートウェイが設定されているインターフェイスのFQDNまたはIPアドレスを、Address（アドレス）フィールドに入力します。

   IPv4アドレスを設定できます。指定するアドレスは、ゲートウェイ サーバー証明書に記載された共通名（CN）と完全に一致する必要があります。

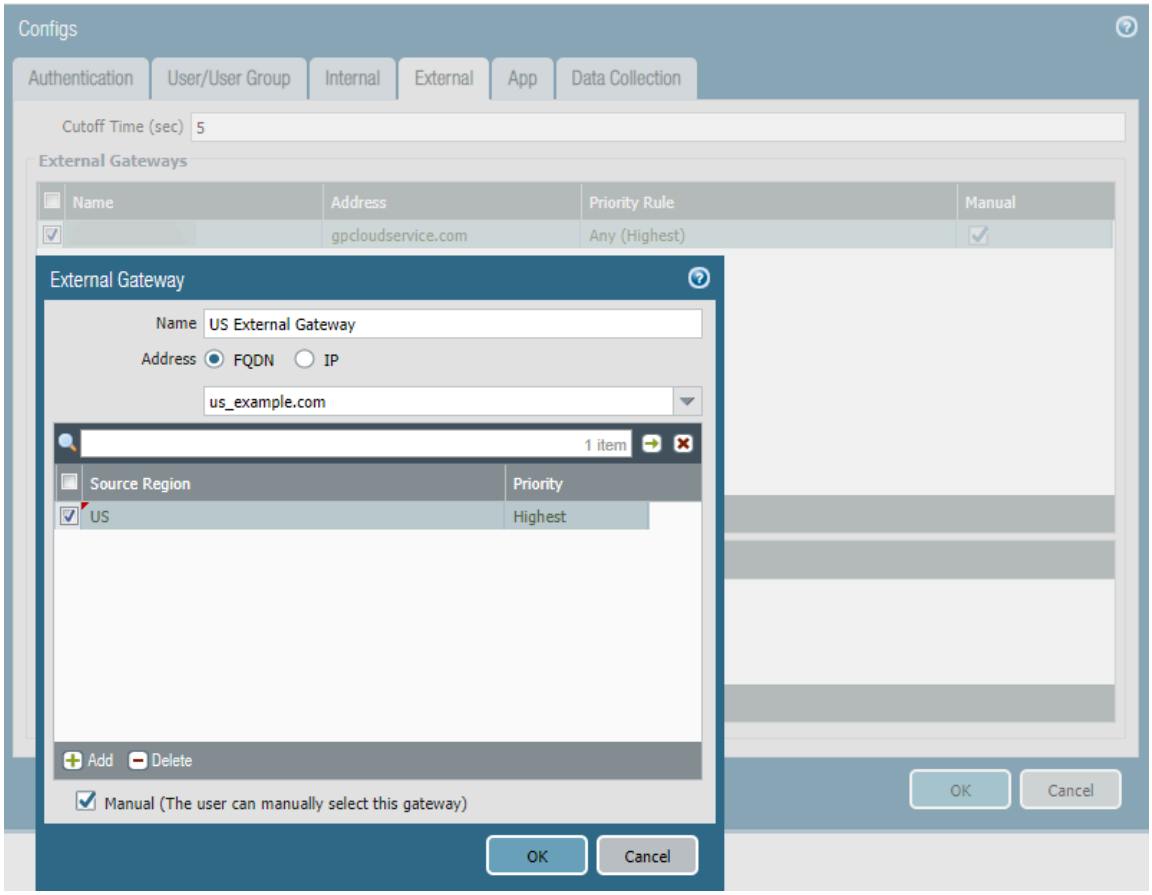
3. オンプレミスゲートウェイ用に1つ以上の**Source Regions**（送信元地域**)**）を Add（追加）するか、**Any**（任意）を選択してゲートウェイをすべての地域で使用できるようにします。

   外部オンプレミスゲートウェイの優先度を、*Prisma Access*ゲートウェイよりも高く設定した場合、外部ゲートウェイの送信元地域を指定することをお勧めします。地域に対して***Any***（任意）を指定した場合、オンプレミスゲートウェイの優先度が高いため、*GlobalProtect*アプリケーションがオンプレミスゲートウェイではなく*Prisma Access*ゲートウェイを選択することはありません。

4. **Manual**（手動）チェック ボックスをオンにして、ゲートウェイに手動で切り替えることをユーザーに許可します。

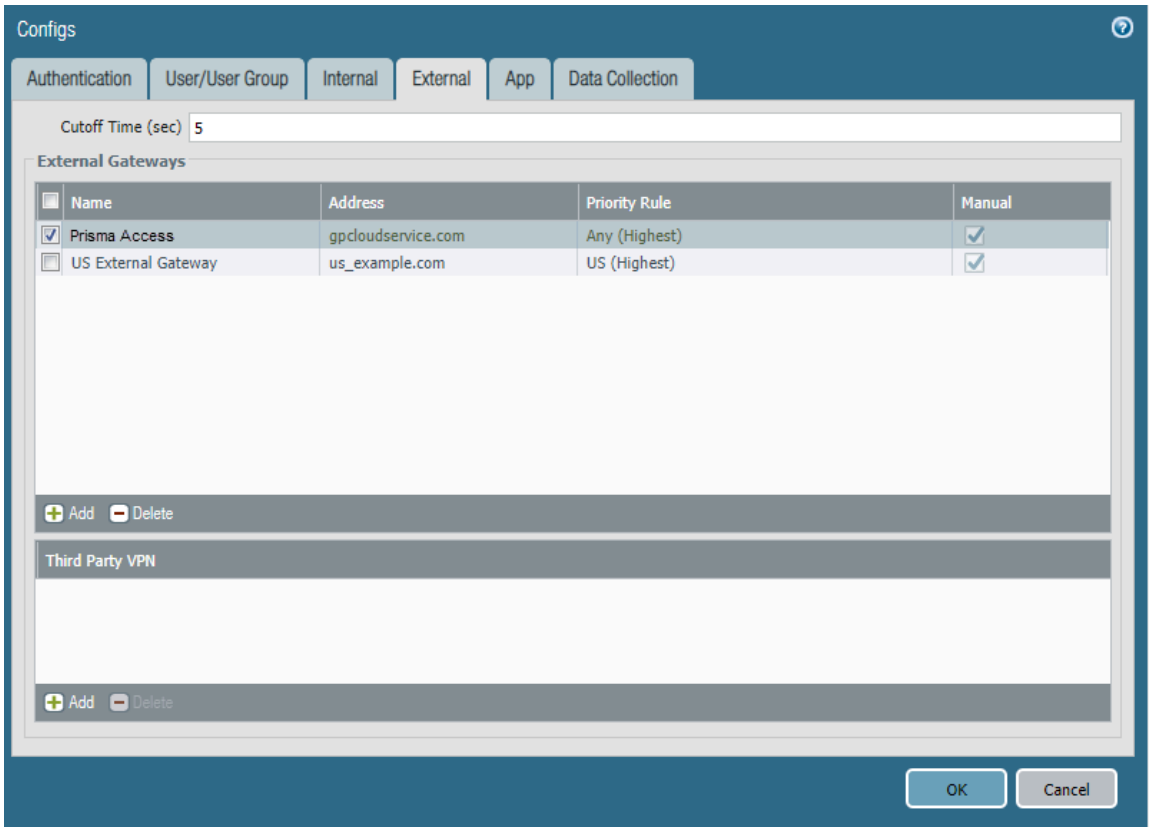
5. オンプレミスゲートウェイの**Priority**（優先度）を、**Highest**（最高）（デフォルト）に設定します。

©2025 Palo Alto Networks, Inc.



6. **OK** をクリックします。

©2025 Palo Alto Networks, Inc.



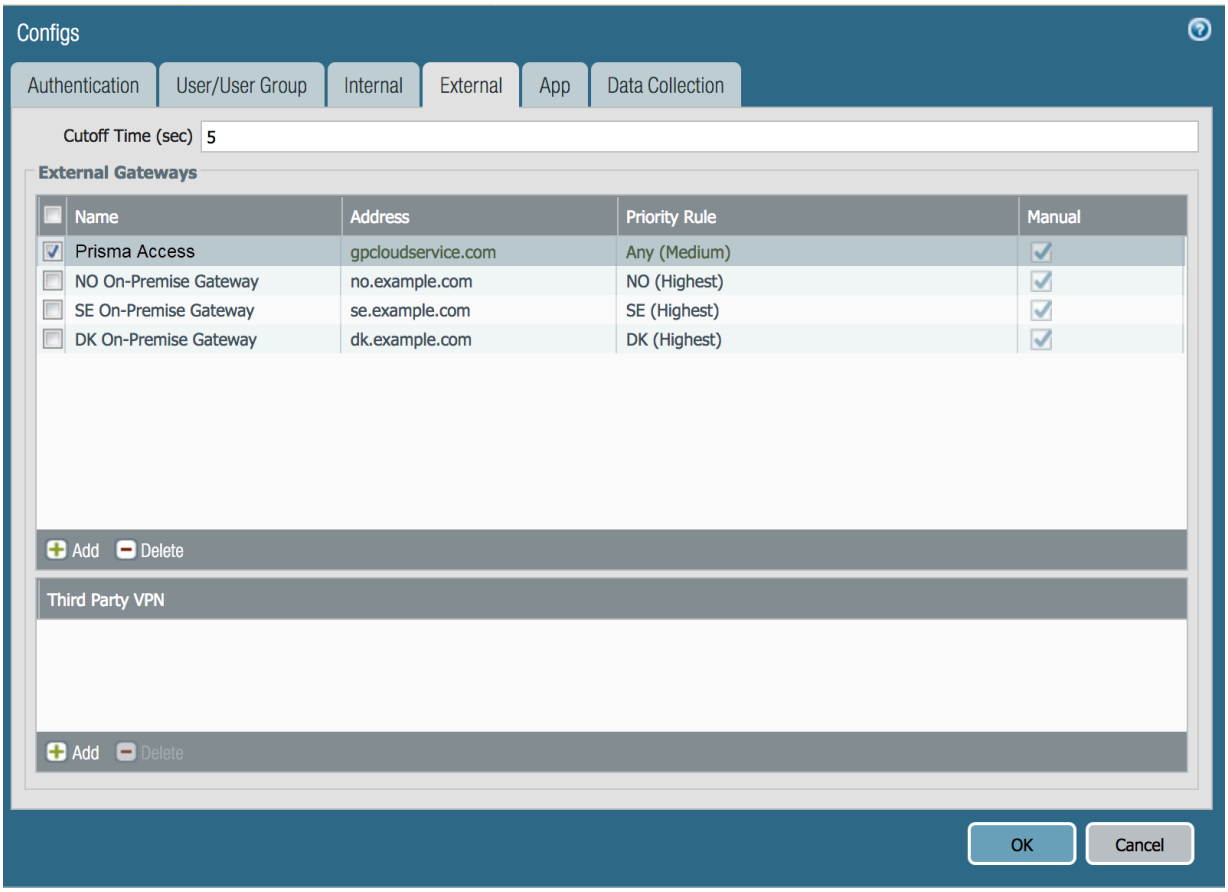
STEP 9 | （任意） ステップ8を繰り返して、他のゲートウェイの優先度を設定します。

正しい送信元地域を指定するようにしてください。

送信元地域がNorway（ノルウェー）、Sweden（スウェーデン）、およびDenmark（デンマーク）である、複数のゲートウェイのサンプル設定を次の図に示します。**Manual**（手

©2025 Palo Alto Networks, Inc.

動）チェックボックスが選択されていることに注目してください。この場合、モバイルユーザーはこれらのゲートウェイを手動で選択できます。



©2025 Palo Alto Networks, Inc.

モバイルユーザー:明示型プロキシ

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

Palo Alto NetworksのPrisma Accessは、高度なURLフィルタリング、SSL復号化、SaaSアプリケーション制御、高度な脅威防御など、クラス最高のクラウドSWG機能を提供するセキュリティ サービス エッジ（SSE）ソリューションです。Prisma Accessは、Palo Alto Networks が完全に管理する広範かつ常時接続のクラウド ネイティブ インフラストラクチャによって、次世代セキュリティのデプロイメントを運用します。モバイル ユーザーとリモート サイトは、企業ポリシーに従ってインターネットとSaaSアプリケーションに安全にアクセスできます。 Prisma Accessは柔軟な接続オプションを提供します。PAC Files、Agent、Agentless、サイト間IPSECにより、レガシーまたは代替のクラウド プロキシ アーキテクチャが最小限のネットワーク変更でPrisma Accessに移行できるようにします。

明示型プロキシ

Prisma Accessはクラウド ベースの明示的なプロキシ接続方法を含む、完全なクラウド セキュアWebゲートウェイ (SWG) 機能を提供します。既存のネットワークですでに明示的なプロキシを使用し、クライアント エンドポイントにPACファイルをデプロイしている場合、レガシー プロキシ ベースのSWGソリューションからPrisma Accessにスムーズに移行し、モバイル・ユーザーのアウトバウンドインターネット トラフィックを保護することができます。コンプライアンスのためにプロキシを使用する必要がある場合は、明示型プロキシを使用することもできます。明示型プロキシはモバイル ユーザー ライセンスを使用します。

複数のPACファイルを使用して、異なるユーザーやシステムへのWebトラフィックの転送方法を定義する場合、 Prisma AccessはこれらのPACファイルを転送プロファイルに関連付けることができるため、複数のPACファイルを同時に使用できるようになります。さらに、PACファイルを作成する代わりに、転送プロファイルを使用すると、Webトラフィックの方向を定義する簡単な転送ルールを構成できます。

- サポートされているロケーション
- GlobalProtectアプリケーションによる明示型プロキシ
  - プロキシモードでのGlobalProtect
  - トンネルおよびプロキシモードのGlobalProtect
- PACファイルを使用した明示型プロキシ
  - SAMLのセットアップ
  - Kerberosのセットアップ

©2025 Palo Alto Networks, Inc.

- 転送プロファイル
  - 複数のPACファイルのサポート
  - 転送ルール
  - GlobalProtectによるプロファイルの転送

Prisma Access明示型プロキシ機能

機能	詳説
App-ID	ポート、TLS/SSL 暗号化、または攻撃者が検出を回避するために使用する手法に関係なく、すべてのアプリケーションを継続的に分類します。アプリケーションの分類が適用される前に、レイヤー3とレイヤー4を最初の制御レイヤとして使用するレガシーソリューションとは異なり、Prisma Accessは、ユーザーIDなどの他のレイヤー7の制御とともにApp-IDを適用します。
User-ID	幅広いユーザーIDリポジトリと統合することで、場所に関係なくユーザーとグループにポリシーを適用できます。
SSL 復号化	TLS/SSLで暗号化されたトラフィックを検査し、ポリシーを適用します。プライバシーと規制遵守のため、URL、ソース、宛先、ユーザー、ユーザー グループ、ポートに基づいて、復号化を柔軟に有効または無効にすることができます。
AI/MLベースの検出	インラインのシグネチャレス攻撃検出とゼロデイ攻撃防止を実現します。 Prisma Accessはスケジュールされた更新に対して、瞬時にリアルタイム保護を適応して提供します。10秒未満のシグネチャ配信により、未知の脅威の最大 95% を即座に防止し、感染したシステムを99.5%削減します。
DNS セキュリティ	リアルタイム保護とインライン機械学習を適用して、C2コールバックやDNSを使用するその他の攻撃を阻止します。Prisma Accessにネイティブに統合されたAdvanced DNS Securityは、自動化された保護を提供し、攻撃者がセキュリ ティ対策をバイパスすることを防ぎ、独立したツールやDNSルーティングの変更を不要にします。
高度な URL フィルタリング	フィッシング、マルウェア、C2などのWebベースの脅威に対する優れた保護機能。強力なデータベース保護と、新しい悪意のあるURLをリアルタイムで分類してブロックするMLベースのWebセキュリティ エンジンを組み合わせます。業界をリードするフィッシング対策は、侵害の最も一般的な原因に対処し、ユーザー、リスク評価、コンテンツ カテゴリに基づいてセキュリティ アクションを自動化するきめ細かい制御とポリシー設定を通じて、Web トラフィックの制御を取り戻します。
高度な脅威防御	業界をリードする脅威防御機能により、ゼロデイ脅威、既知のエクスプロイト、マルウェア、スパイウェア、悪意のあるコマンド アン

 ©2025 Palo Alto Networks, Inc.

機能	詳説
	ド コントロール (C2) を阻止します。従来の侵入防御システムに比べて、未知のインジェクション攻撃を60%多く、回避性の高いC2 トラフィックを48%多く防止します。
アドバンスド WildFire	業界最大の脅威インテリジェンスとマルウェア防止エンジンにより、既知、未知、および回避能力の高いマルウェアを60倍の速さで自動的に防止し、ファイルの安全性を確保します。
NG-CASB*	プロアクティブなSaaSの可視性、誤った構成からの保護、リアルタイムのデータ保護を実現し、クラス最高のSaaSセキュリティを実現します。
データ損失防止 (DLP)*	機密情報を不正アクセス、誤用、抽出、共有から保護するための一連のツールとプロセスが含まれています。Prisma Access上のDLPは、データ セキュリティ ポリシーを実施し、モバイル・ユーザーとリモート ネットワークにまたがる機密データの損失を防ぐことができます。
リモートブラウザ分離のサポート	CloudBladesを通じて、既存のNGFW URL分類およびURL書き換え機能を活用してサードパーティのRBIクラウドと統合し、選択した/すべてのインターネット接続トラフィックをRBIクラウドに転送します。この機能は、特定のトラフィック（未知または高リスクのカテゴリー）を追加検査のためにRBIに転送する一方で、残りのトラフィックはPrisma Accessによって検査され、インターネットに直接イグジットすることができ、シームレスなユーザーエクスペリエンスを提供します。
レポート作成	標準として、ネットワーク上のすべてのSaaSトラフィック (承認済みおよび未承認) に関する洞察を提供する、詳細でカスタマイズ可能なSaaSアプリケーション使用状況レポートが含まれています。また、ニーズに応じてカスタム レポートを作成し、簡単にスケジュール設定、ダウンロード、組織内の他のユーザーと共有することもできます。
ユーザー認証	Kerberos、RADIUS、SAML、LDAP、クライアント証明書、ローカル ユーザー データベースなど、既存のすべてのPAN-OS認証方法に対応しています。PACのみで、KerberosとSAMLをサポートします。
サイト間IPsec VPN	互換性を確保するために、IPv4およびIKEv1/IKEv2経由のサイト間トンネルをサポートします。複数の接続サイトの場合、ECMPルーティングは、利用可能なインターネット接続を介してセッションのバランスをとることで、追加の冗長性とコスト効率を提供できます。
ロギング	全体的なトラフィック、アプリケーション、ユーザー、脅威、URL、およびデータ フィルターのログ記録を表示し、クラウドベースのStrata Logging Serviceを介したデータの整理を容易にします。

©2025 Palo Alto Networks, Inc.

機能	詳説
転送プロファイル	異なるユーザー グループまたはシステムに対して複数のPACファイルの使用を有効にします。また、Web トラフィックの方向を定義する転送ルールの作成もサポートしており、PACファイルの作成と管理に代わるよりシンプルな方法を提供します。

* アドオンライセンスが必要です。

製品の特徴と機能の詳細については、Prisma Accessデータシートを参照してください。

明示型プロキシの設定ガイドライン

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

システム要件とサポートされる機能

これらは、明示型プロキシで使用できるさまざまな接続方法のシステム要件とサポートされている機能です。

	エージェントレスSAML	エージェントレス Kerberos	エージェントのプロキシ モード (GP 6.2 以降が必要)	リモートネットワークのプロキシモード
アプリケーションとOSのサポート				
トラフィックの種類	インターネットとパブリックSaaSトラフィックのみ	インターネットとパブリックSaaSトラフィックのみ	インターネットとパブリックSaaSトラフィックのみ	インターネットとパブリックSaaSトラフィックのみ
プロトコル サポート	プロキシ対応HTTPまたはHTTPS	プロキシ対応HTTPまたはHTTPS	プロキシ対応HTTPまたはHTTPS	プロキシ対応HTTPまたはHTTPS
Prisma Accessへの転送チャネル	HTTP接続	HTTP接続	TLS 内のHTTP接続	ブランチからリモート ネットワーク セキュリティ処理ノード (SPN)

©2025 Palo Alto Networks, Inc.

				へのIPSec内のHTTP接続
サポートされている環境	Windows、Mac、Linux、ChromeOS、VDI	Windows、Mac、Linux、ChromeOS、VDI	WindowsとMac	Windows、Mac、Linux、ChromeOS、VDI
アプリケーション サポート	プロキシ対応HTTP(s) アプリ	PACファイルまたはシステムプロキシ設定を尊重し、Kerberosをサポートするアプリ	プロキシ対応HTTP(s) アプリ	プロキシ対応HTTP(s) アプリ
ブラウザのサポート	Chrome#、Edge、Firefoxバージョン115以降	Chrome#、Edge、Firefoxバージョン115以降	Chrome#、Edge、Firefoxバージョン 115以降*	Chrome#、Edge、Firefoxバージョン115以降
O365サポート†	ブラウザとクライアントアプリ	ブラウザとクライアントアプリ	ブラウザとクライアントアプリ	ブラウザとクライアントアプリ
ID				
ユーザー**ID‡**	復号化された非HTTP CORSトラフィック	サポートされているすべてのトラフィック	サポートされているすべてのトラフィック	SAMLまたはKerberosのどちらを使用しているかによる: 復号化/非CORS X-Authenticated-Userトラフィック
認証サポート	SAML (任意のSAML 2.0 IDPまたはCIE 経由)	Kerberos	GlobalProtectでサポートされているすべての認証	SAML、Kerberos、X認証ユーザーベース
認証をスキップ	ドメイン別および送信元IP別	ドメイン別および送信元IP別	ドメイン別	ドメイン別および送信元IP別
ユーザー グループ ディレクトリ	CIEがサポートされているすべてのディレクトリ	CIEがサポートされているすべてのディレクトリ	CIEがサポートされているすべてのディレクトリ	CIEがサポートされているすべてのディレクトリ

©2025 Palo Alto Networks, Inc.

ライセンス	ユーザーあたりのモバイル ユーザー ユニット	ユーザーあたりのモバイル ユーザー ユニット	ユーザーあたりのモバイル ユーザー ユニット	ユーザーまたはヘッドレスデバイスごとのモバイルユーザー単位と、リモートネットワークの帯域幅のNET単位
管理				
マルチテナントPanorama	ファースト テナントをサポート	ファースト テナントをサポート	ファースト テナントをサポート	ファースト テナントをサポート
マルチテナントクラウド管理	サポート	サポート	サポート	サポート
セキュリティ サービス				
SaaS インライン	サポート	サポート	サポート	サポート
DLP	サポート	サポート	サポート	サポート
DNSセキュリティ§	サポート	サポート	サポート	サポート
高度な URL フィルタリング	サポート	サポート	サポート	サポート
アドバンスド WildFire	サポート	サポート	サポート	サポート
高度な脅威防御	サポート	サポート	サポート	サポート
リモートブラウザ分離	サポート	サポート	サポート	サポート
プライベートIPの可視性と適用	サポートされていません	サポートされていません	既知のサイトまたはブランチでサポート	サポート
出口NAT	サポート	サポート	サポート	サポート
プライベート アプリケーション アクセス	サポートされていません	サポートされていません	サービス接続を介してサポート	サポートされていません

©2025 Palo Alto Networks, Inc.

すべての**TCP**トラフィック	サポートされていません	サポートされていません	サポートされています (GlobalProtectバージョン 6.3.1を使用)	サポートされていません
ZTNA コネクタ	サポートされていません	サポートされていません	サポート	サポートされていません
Colo Connect	サポートされていません	サポートされていません	サポート	サポートされていません
サービスコネクション	サポート	サポート	サポート	サポート
HIPサポート (トンネルおよびプロキシ モード)	サポートされていません	サポートされていません	サポート	サポートされていません

Chromeブラウザの場合、復号化が有効になっている場合は、以下の手順に従ってTLS 1.3 Kyberを無効にしてください。

1. Chromeブラウザを開きます。
2. アドレスバーに `chrome://flags/#enable-tls13-kyber`を追加して無効にします。
3. [再起動]をクリックします。

* エージェントのプロキシモードの場合、Firefoxは Mobile Device Management(モバイルデバイス管理) を通じてプッシュされた手動のポリシールールを必要とし、システムプロキシを尊重するように指示します。

† 明示型プロキシはHTTPトラフィックのみをサポートし、UDPはサポートしていません。SAMLでは、明示型プロキシはクライアント アプリ フローにユーザーIDを提供しません。エージェント プロキシの場合、PACファイルを使用してクライアント アプリの認証フローをクラウド プロキシに送信する必要があります。

‡ 認証バイパスに使用できるユーザーIDはありません。

§ 明示型プロキシ フローにDNSセキュリティ プロファイルを適用することはできません。代わりにドメインをブロックします。

アプリサポートに関する考慮事項

1. 明示型プロキシは、IPアフィニティを必要とするアプリをサポートしません。アプリは、特定のユーザー セッションに対して複数のIPからのトラフィックをサポートする必要があります。
2. 明示型プロキシは、復号化されたHTTP/2フローをHTTP/1にダウングレードします。
3. 明示型プロキシは、オンプレミスの外部動的リストを取得しません。

©2025 Palo Alto Networks, Inc.

4. エージェントレスSAMLのみ:
   1. SAML Authを使用したエージェントレスPACベースのExplicit Proxyで、ドメインによる認証バイパスを許可するSSL復号ポリシーを設定する

      *Prisma Access*がモバイルユーザーのブラウザで設定した認証状態*Cookie*を読み取るには、復号化が必要です。復号化を強制しないと、明示型プロキシがオープン プロキシとして悪用され、攻撃者がサービス拒否攻撃の転送サービスとして使用できる可能性があります。
   2. トラフィック ログでは、明示型プロキシは、復号化されていないHTTP-CORSモバイルユーザー トラフィック ログをSWG認証済みユーザーとして表示します。
   3. 次のブラウザの要件と使用ガイドラインに注意してください。
      - 明示型プロキシを使用する場合は、ブラウザでCookieを無効にしないでください。無効にすると、Webページを閲覧できなくなります。
      - Microsoft Edgeで明示型プロキシを使用している場合は、 設定の > プライバシー、検索、およびサービスの > 追跡防止 必ず 基本に設定してください。

接続要件

モバイル ユーザーが明示型プロキシを使用してリモート サイト、本社、またはデータセンターの場所から接続する場合、モバイル ユーザーのエンドポイントは、IdP、ACS FQDN、明示型プロキシ URL、およびPrisma Accessによってホストされている PAC ファイルの URL にアクセスしてルーティングできる必要があります。

PACファイルの要件とガイドライン- Explicit Proxy(明示型プロキシ)で使用するPACファイルを設定する際は、PACファイルガイドラインに従ってください。

プロキシ チェーン ガイドライン- サードパーティ プロキシから明示型プロキシへのプロキシ チェーンを使用する場合は、明示的プロキシにトラフィックを転送するためにサードパーティ プロキシで **[Explicit Proxy URL (**明示型プロキシ**URL)]** を指定します。

オンプレミス サポート- 明示型プロキシはクラウドベースのプロキシ ソリューションであり、オンプレミス製品ではありません。オンプレミスのプロキシ ソリューションの場合は、PAN-OS Webプロキシを構成します。

プロキシモードでのGlobalProtect

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager) この機能をPrisma Access環境で使用したい場合は、アカウントチームにお問い合わせください。	• Prisma Access 5.2 • WindowsまたはMacOS用のGlobalProtectアプリケーション バージョン6.2 • コンテンツリリースバージョン 8700-7994 • Prisma Access モバイルユーザーライセンス

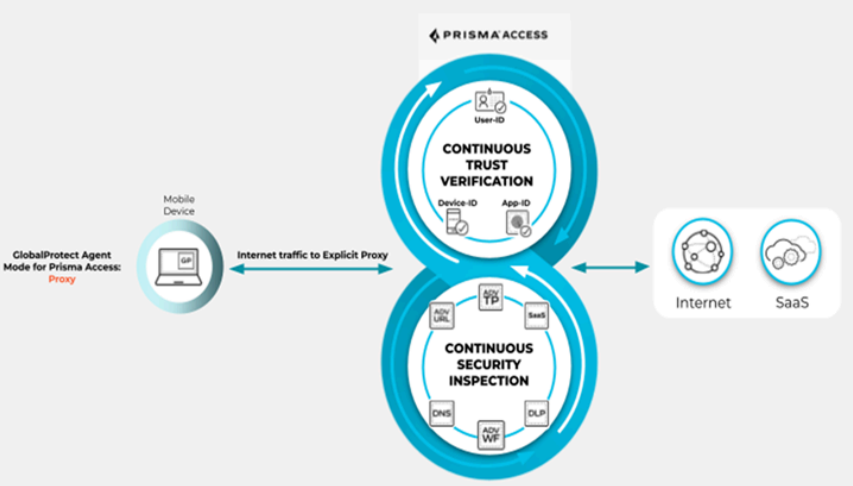
©2025 Palo Alto Networks, Inc.

プロキシモードを使用すると、GlobalProtectアプリケーションは常時インターネット セキュリティを提供します。このモードでは、GlobalProtectアプリケーションは、Prisma Accessまたはお客様の環境でホストされているPACファイルからの転送ルールとロジックに基づいて、Prisma Accessへのトラフィックをプロキシします。これは、既存の（レガシー）プロキシ アーキテクチャがある場合、または規制やコンプライアンス上の理由でプロキシ アーキテクチャを管理する必要がある場合に役立ちます。

エージェントベースのプロキシ機能により、GlobalProtectアプリケーションとサードパーティのVPNの共存と相互運用性が促進され、GlobalProtect アプリから明示的なプロキシまでのモバイル ユーザーのインターネット トラフィックを保護し、任意のサードパーティVPNを使用してプライベート アプリケーション アクセスを保護できます。

プロキシを意識しないトラフィックを含む、すべての*IPv4 TCP*接続をサポートする*GlobalProtect*プロキシチャネルには、*Strata Cloud Manager*と*GlobalProtect*エージェントバージョン*6.3.0*が必要です。シームレスな機能を確保するには、エンドポイントに構成された*DNS*が宛先*FQDN*を解決できる必要があります。

このシナリオでは、GlobalProtectアプリケーションは定義したPACファイルルールに基づいてインターネットトラフィックをPrisma Accessに送信し、エンドポイントはIPSec/TLSトンネルを使用してサードパーティVPNを介してプライベートアプリケーションへのアクセスをルーティングします。



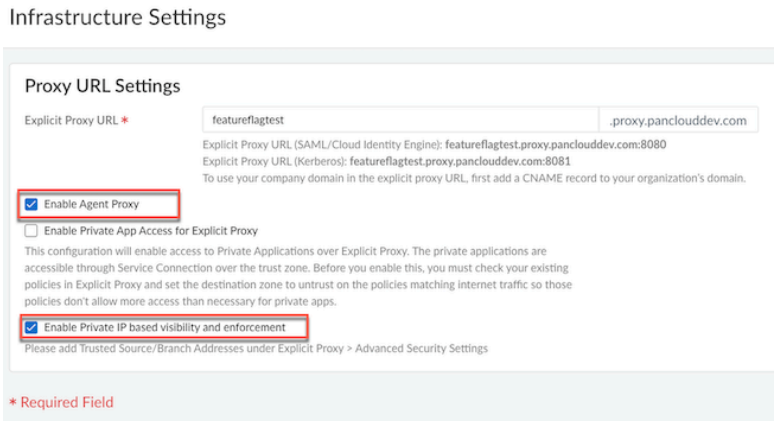
- Strata Cloud Manager
- Panorama

プロキシモードでのGlobalProtect (Strata Cloud Manager)

©2025 Palo Alto Networks, Inc.

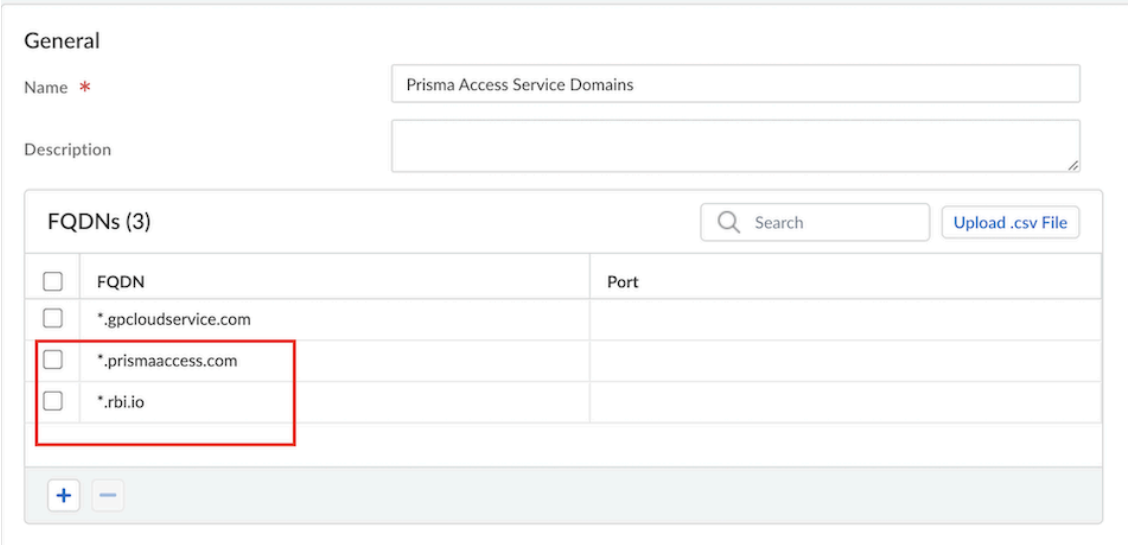
STEP 1 | Prisma Accessのモバイル ユーザー向けにエージェント ベースのプロキシ機能を有効にします。

1. 明示的なプロキシを有効にします。
   1. **[ワークフロー] > Prisma Access[セットアップ] > [モバイルユーザー]**を選択し、**[明示型プロキシのセットアップ]**をクリックします。
   2. インフラストラクチャ設定領域で、**[プロキシ設定のセットアップ]**をクリックし、**[明示的なプロキシURL]**を指定します。
2. エージェント プロキシを有効にし 、オプションでプライベート **IP** ベースの可視性と適用を有効にして、**[保存]**をクリックします。



3. モバイルユーザーをサポートしたいPrisma Accessロケーションを選択します。

   最適なユーザー エクスペリエンスにむけて、場所の数を制限する場合は、エンド ユーザーに最も近いロケーションを選択します。モバイル ユーザーが居住する国で場所が利用できない場合は、モバイル ユーザーに最も近いロケーションを選択します。
4. 転送プロファイルを作成して、 明示的なプロキシ経由で送信するトラフィックを定義します。転送プロファイルを構成する際、*.prismaaccess.com および *.gpcloudservice.com ドメインをバイパスします。



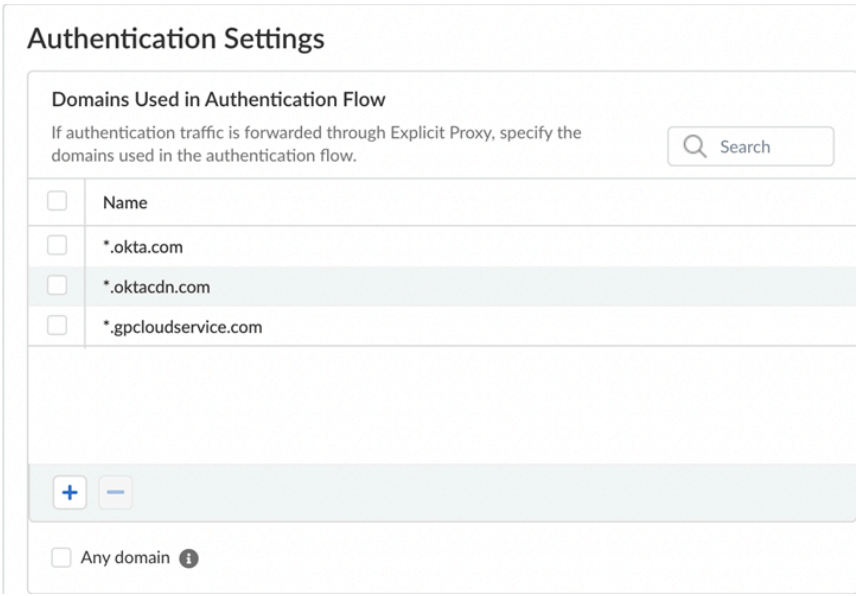
5. 転送プロファイルをGlobalProtectアプリケーション構成に添付します。

 ©2025 Palo Alto Networks, Inc.

6. **[Workflows (ワークフロー)] > [Setup (セットアップ)] > [Explicit Proxy (明示型プロキシ)] > [Advanced Security Settings (詳細セキュリティ設定)] > [Authentication Settings (認証設定)]**を選択し、バイパスする必要があるドメインを追加します。

   プロキシへのすべてのリクエストは認証を受けます。ただし、プロキシを介してIdPフローを渡している場合は、認証を成功させるためにIDPフローをバイパスする必要があります。

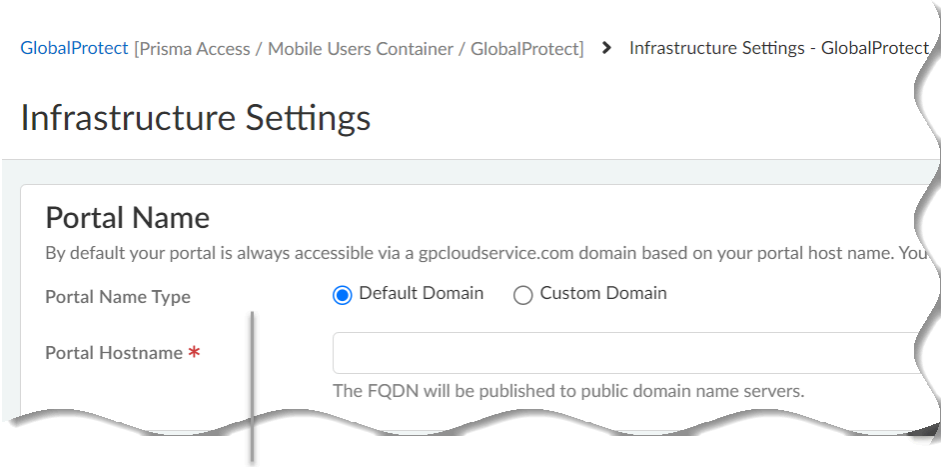
   この例では、GlobalProtectポータルとOktaをバイパスしていますが、使用するIdPに合わせてカスタマイズしてください。



 ©2025 Palo Alto Networks, Inc.

STEP 2 | GlobalProtectポータル、認証を設定し、GlobalProtectアプリケーションのプロキシモードを設定します。

1. [ワークフロー] > **[Prisma Accessセットアップ]** > **[GlobalProtect]** > [インフラストラクチャ] > [インフラストラクチャ設定]を選択し、[ポータル名]を指定します。



GlobalProtect Infrastructure Settings

- **Use Default Domain**（デフォルトドメインを使用）–このオプションを選択した場合、ポータルホスト名はデフォルトのドメイン名「`.gpcloudservice.com`」を使用します。この場合は、デフォルトのドメイン名に追加するポータル ホスト名を入力するだけです。 ユーザー向けPrisma Accessは必要な証明書を自動的に作成し、ホスト名をパブリックDNSサーバーに公開します。
- カスタム ドメイン- ポータル ホスト名のドメインを会社のドメイン名 (たとえば、myportal.mydomain.com) と一致させたい場合は、ポータル アドレスをカスタマイズすることもできます。

2. モバイルユーザーがPrisma Accessに対して認証できるようにします。

©2025 Palo Alto Networks, Inc.

3. GlobalProtectアプリケーションの設定で、Prisma AccessのGlobalProtectプロキシモードを有効にして、インターネットトラフィックをエージェントベースのプロキシに送信します。

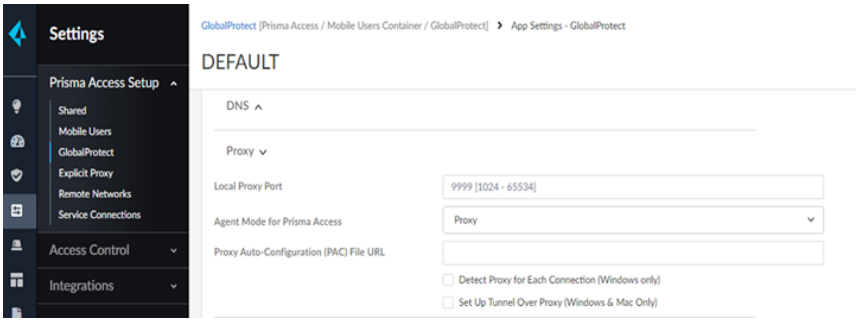
   *GlobalProtect*接続方法は、常にオンになっているため、プロキシ モードでは適用されません。

   - **[ワークフロー] > Prisma Access[セットアップ] > [GlobalProtect]**を選択します。
   - **GlobalProtect**アプリケーションタブで、デフォルトをクリックしてアプリ設定をカスタマイズするか、**[アプリ設定の追加]**をクリックして新しい構成を追加します。
   - 「詳細オプションを表示」 をクリックし、「アプリ構成」 セクションをクリックします。
   - GlobalProtectアプリケーションがインターネットトラフィックをPrisma AccessのExplicit Proxy(明示型プロキシ)に送信するように指示するために、**Prisma Access**のエージェントモードを**Proxy**に設定します。
   - (任意) ローカル プロキシ ポートを設定します。ポート範囲は1024 ～ 65534で、デフォルト ポートは9999です。デフォルトのポートが使用できない場合、GlobalProtect は9999 ～ 10009の範囲にある他の10個のポートを試行し、使用可能なポートを使用します。範囲内で独自のポート番号を選択することもできます。
   - (任意) プロキシ設定の新規PAC URLをエンドポイントにプッシュする場合は、PAC自動設定 (PAC) ファイルURLを構成します。ユーザーが接続すると、PAC URLがエンドポイントにプッシュされます。ユーザーがGlobalProtectアプリケー

 ©2025 Palo Alto Networks, Inc.

ションを切断すると、エンドポイント プロキシ設定は自動的に無効になり、以前の設定に戻ります。

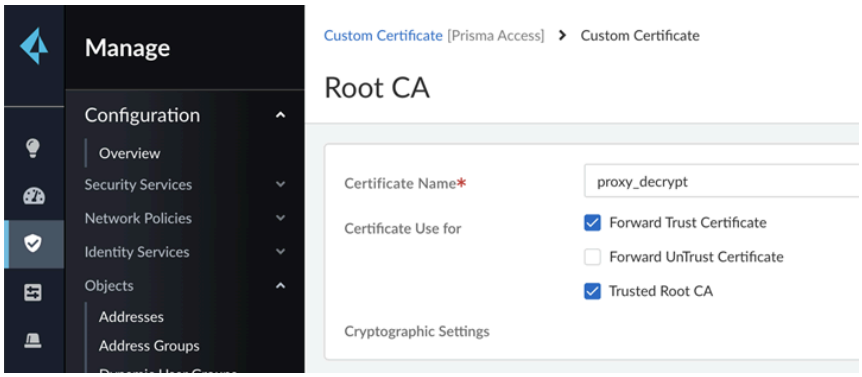
- (任意) ユーザーがポータルで新しい設定を確認できるようにする場合は、[Allow User to Rediscover Network (ユーザーによるネットワークの再検出を許可)] を有効にします。
- (任意)GlobalProtectアプリケーション設定の更新間隔 (時間)を設定します。デフォルトでは、GlobalProtectクライアントはキャッシュされたポータル設定を24時間ごとに更新します。ビジネス要件に応じて更新間隔を変更できます。
- **Tunnel Over Proxy**のセットアップを無効にします（**Windows** および **Mac** のみ）。



4. [ワークフロー] > [**Prisma Access**セットアップ] > [**GlobalProtect**] > [**GlobalProtect**アプリケーション] > [アプリ設定の追加]ページで以下の設定を行い、常時接続のインターネットセキュリティを有効にする：
   1. GlobalProtectを無効にするを 、 **[Disallow (**許可しない**)]**、 **[Allow with Passcode (**パスコードで許可する**)]**、または**[Allow with Ticket (**チケットで許可する**)]**に設定します。
   2. [ユーザーが GlobalProtect アプリからサインアウトできるようにする]を無効にします。

STEP 3 | 明示型プロキシ トラフィックの復号化を設定します。

- **[Manage (**管理**)]** > **[Configuration (**設定**)]** > **[NGFW]** > **[Security Services (**セキュリティ サービス**)]** > **[Decryption (**復号化**)]**を選択します。
- 復号化を有効にする場合は、復号化証明書を信頼できるルートCAとしてセットアップしてください。



 ©2025 Palo Alto Networks, Inc.

STEP 4 | 明示的なプロキシ トラフィックのセキュリティ ポリシー ルールを構成します。

- **[Manage (管理)] > [Configuration (設定)] > [NGFW]Prisma Access > [Security Services (セキュリティ サービス)] > [Security Policy (セキュリティ ポリシー)]**を選択します。
- 「インターネット ゲートウェイ セキュリティ ポリシーのベストプラクティス」に従ってください。

STEP 5 | (任意) デフォルト ルートのないネットワークでGlobalProtectアプリケーションをプロキシモードで構成します。

- （任意）PACファイルを内部でホストし 、 PACファイル内のプロキシとしてPrisma Access明示的なプロキシFQDNを指定するか、 転送プロファイル でPACファイルをホストし、ネットワーク内にPACサービスIPアドレスのルートを追加します。
- PACファイルで、IdP URLとPrisma Accessポータル URLを明示型プロキシに転送します。
- 明示的なプロキシでは、認証設定からIdPとポータルURLを除外します。認証フローで使用されるドメインにIdPとポータルURLを追加します。
- ユーザーが明示的プロキシ経由でインターネットにアクセスできるように、境界デバイス上の明示的プロキシFQDNまたはIPアドレスへのルートを設定します。
- （任意）ユーザーがブランチ ネットワーク内のパブリック ドメインを解決できない場合は、Prisma Access明示的プロキシFQDNを内部IPアドレスに解決するDNSレコードを追加し、内部IPアドレスの宛先NATを明示的プロキシFQDNまたはIPアドレスに追加します。

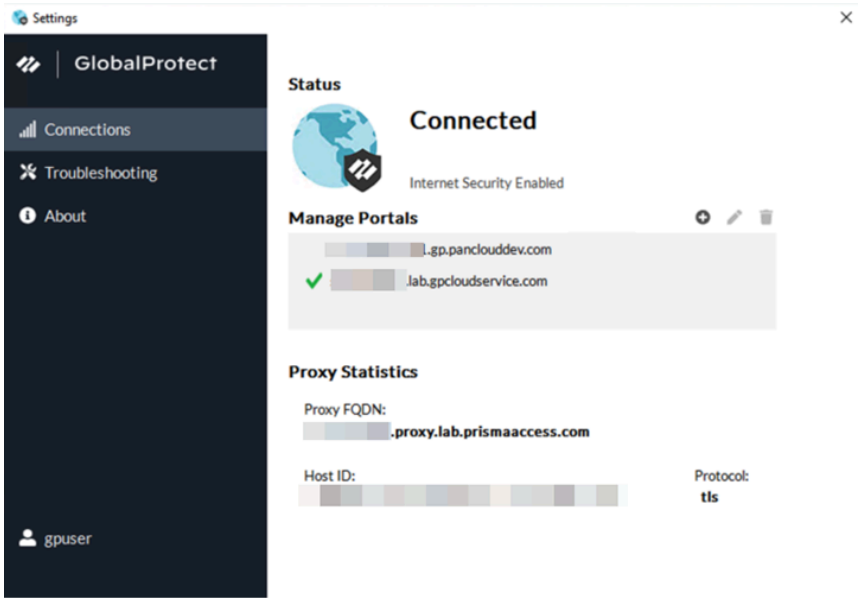
STEP 6 | [保存]をクリック して、**GlobalProtect** と 明示的なプロキシに**[設定をプッシュ]** をクリックします。

©2025 Palo Alto Networks, Inc.

STEP 7 | エージェント プロキシのデプロイメントを確認し、トラブルシューティングを行います。

1. GlobalProtectアプリケーションの[設定]の[接続] タブで、ネットワーク接続に関する情報を確認します。

   1. GlobalProtectアプリケーションを開きます。
   2. [設定] を選択してGlobalProtect設定パネルを開き、[接続]を選択します。



2. GlobalProtectログを表示および収集します。

   PanGPSログを表示して、GlobalProtectポータルのプロキシ モード構成を確認します。

   プロキシモードが設定されているかどうかは、PanGPSのログで以下のイベントを探すことで確認できます。

   `OnProxyAgentMode`：プロキシ専用モード

   で GlobalProtect ログを表示するには、**[Incidents & Alerts (インシデントとアラート)]** > **[Log Viewer (ログ ビューアー)]**を選択します：

   - **GlobalProtect**(認証ログ用)
   - ユーザーアクセスログ用のトラフィック と 復号化

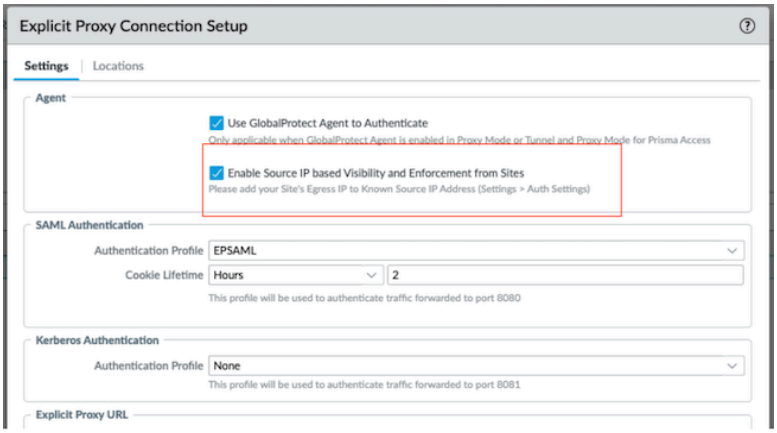
プロキシモードでのGlobalProtect (Panorama)

シングルテナントを変換する場合、マルチテナントへのPrisma Access (Managed by Panorama)デプロイメントでは、最初のテナント (移行したテナント) のみがこの機能をサポートします。また、この最初のテナントでは、カスタム デバイス グループではなく、事前定義済みの *Explicit_Proxy_Device_Group* にポリシー ルールを設定する必要があります。マルチテナントデプロイメント用に最初に作成したテナントの後に作成する後続のテナントでは、この機能はサポートされません。

©2025 Palo Alto Networks, Inc.

STEP 1 | モバイル ユーザー向けにエージェントベースのプロキシ機能を有効にします。

1. 明示的なプロキシを有効にします。
   1. **[Panorama]** > **[クラウド サービス]** > **[構成]** > **[モバイル ユーザー - 明示的なプロキシ]**を選択します。
   2. 明示的なプロキシ**URL**を指定するには、明示的なプロキシ設定を構成します 。
2. エージェントベースのプロキシ機能を有効にするには、**[GlobalProtect**アプリケーションを使用して認証する**]** を選択し、 任意で**[**サイトからのソース**IP**ベースの可視性と適用を有効にする**]**を選択します。



3. **PAC (**プロキシ自動構成**)** ファイルのURLを入力します。PACファイルにポート8080を入力していることを確認してください。
   - PACファイルにポート8080を入力していることを確認してください。
   - PACファイルのプロキシステートメントでは、 上記で設定したPrisma AccessFQDNが使われている必要があります。
   - PACファイルは、サードパーティのVPNトラフィックをバイパスするように設定する必要があります。

   サンプルPACファイル:

```
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. 構成した明示的なプロキシ設定の接続名を選択します。

 ©2025 Palo Alto Networks, Inc.

5. モバイル ユーザー向けの明示的なプロキシをデプロイするロケーションとリージョンを選択します。

   Prisma Accessは、選択した各ロケーションにプロキシノードを追加します。明示的プロキシは、すべてのPrisma Accessロケーションのサブセットをサポートしています。最適なユーザー エクスペリエンスにむけて、場所の数を制限する場合は、エンド ユーザーに最も近いロケーションを選択します。モバイル ユーザーが居住する国で場所が利用できない場合は、モバイル ユーザーに最も近いロケーションを選択します。

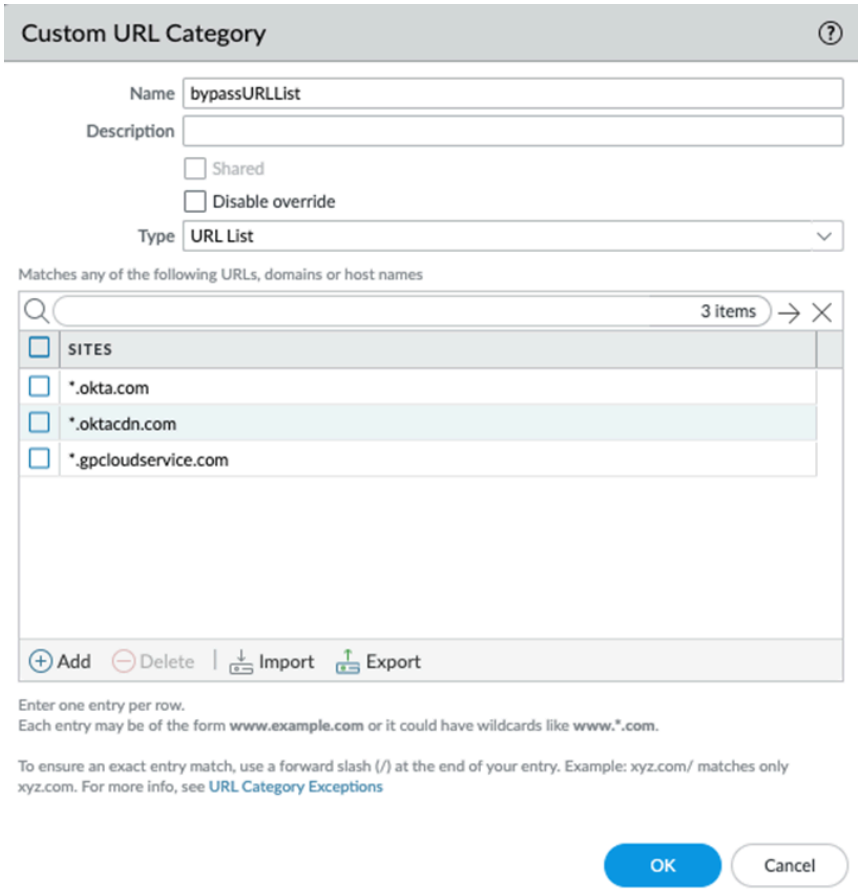
©2025 Palo Alto Networks, Inc.

STEP 2 | IDプロバイダー (IDP) をバイパスします。

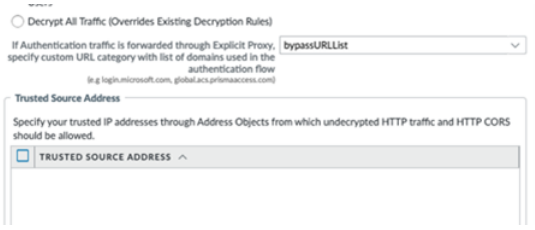
プロキシへのすべての要求が認証されます。ただし、プロキシを介してIDPフローを渡している場合は、認証を成功させるためにIDPフローをバイパスする必要があります。

この例では、GlobalProtectポータルとOktaをバイパスしていますが、使用するIDPに合わせてカスタマイズしてください。

1. **Explicit_Proxy_Device_Group**が選択された状態で、[オブジェクト] > [カスタムオブジェクト] > [**URL**カテゴリ]を選択し、カスタムURLカテゴリーを作成します。
2. カスタムURLカテゴリで、EP認証からバイパスする必要があるすべてのFQDNドメインを追加します。



3. [クラウドサービス] > [構成] > [モバイルユーザー] > [明示型プロキシ] > [設定] > [認証設定]を選択し、カスタムURLカテゴリをアタッチします。



4. コミットして**Explicit_Proxy_Device_Group**にプッシュします。

 ©2025 Palo Alto Networks, Inc.

STEP 3 | GlobalProtectポータルを設定します。

プロキシ モードでは、設定した接続方法によってプロキシ機能の動作は変更されません。オンデマンド接続方法を設定した場合でも、インターネットへのすべてのトラフィックは、常時インターネット セキュリティのためにプロキシされます。

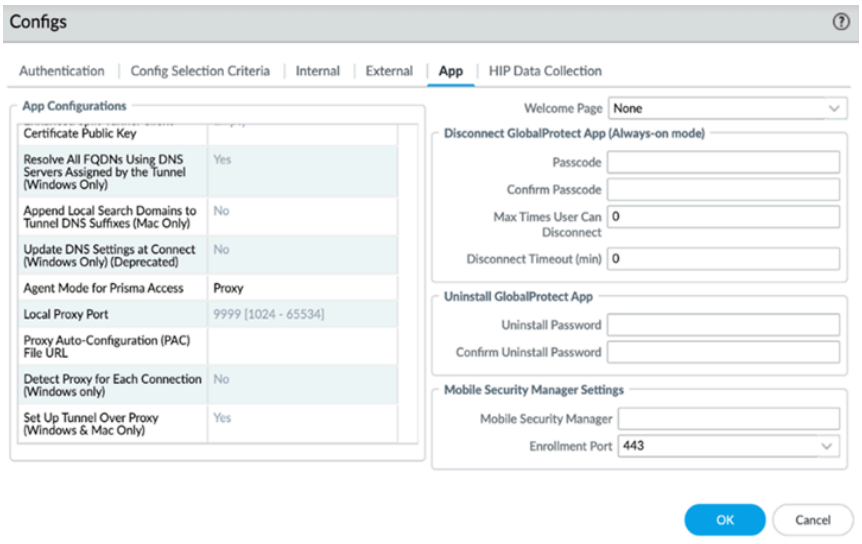
1. Onboarding（オンボーディング）セクションで**Add**（追加）をクリックします。
2. [全般] タブで、 ポータル名のタイプを指定します。

   デフォルト ドメインの使用 - このオプションを選択すると、ポータル ホスト名にはデフォルトのドメイン名 (.gpcloudservice.com) が使用されます。この場合は、デフォルトのドメイン名に追加するポータル ホスト名を入力するだけです。 必要な証明書がPrisma Accessで自動的に作成され、ホスト名がパブリック DNS サーバーに公開されます。

   会社のドメインを使用する - ポータル ホスト名のドメインを会社のドメイン名 (例: myportal.mydomain.com) と一致させる場合は、このオプションを選択します。
3. Prisma Accessがモバイルユーザを認証する方法を指定する認証プロファイルを選択するか、新しいプロファイルを作成します。
4. (任意) モバイル ユーザーがポータルおよびゲートウェイへの認証に使用する安全なCookieを暗号化するには、 認証オーバーライド証明書を選択します。

STEP 4 | GlobalProtectでプロキシ モードを有効にします。

1. [ネットワーク] > [**GlobalProtect** ポータル]を選択します。
2. エージェント設定を追加するポータル設定を選択し、さらに**Agent**（エージェント）タブを選択します。
3. [エージェント]タブで、[アプリ]を選択します。
4. [アプリケーション構成］エリアで、**Prisma Access**用エージェントモードを［**Proxy**］に設定して、インターネットトラフィックをGlobalProtectエージェントベースのプロキシに送信します



 ©2025 Palo Alto Networks, Inc.

STEP 5 | オプションの設定を実行します。

1. (任意) ローカル プロキシ ポートを設定します。ポート範囲は1024 ～ 65534で、デフォルト ポートは9999です。デフォルトのポートが使用できない場合、GlobalProtect は9999 ～ 10009の範囲にある他の10個のポートを試行し、使用可能なポートを使用します。範囲内で独自のポート番号を選択することもできます。
2. (任意) プロキシ設定のカスタムPAC URLをエンドポイントにプッシュする場合は、PAC自動設定 (PAC) ファイルURLを構成します。ユーザーが接続すると、PAC URLがエンドポイントにプッシュされます。ユーザーがGlobalProtectアプリケーションを切断すると、エンドポイント プロキシ設定は自動的に無効になり、以前の設定に戻ります。
3. (任意) ユーザーがポータルで新しい設定を確認できるようにする場合は、[Allow User to Rediscover Network (ユーザーによるネットワークの再検出を許可)] を有効にします。
4. (任意)GlobalProtectアプリケーション設定の更新間隔 (時間)を設定します。デフォルトでは、GlobalProtectクライアントはキャッシュされたポータル設定を24時間ごとに更新します。ビジネス要件に応じて更新間隔を変更できます。

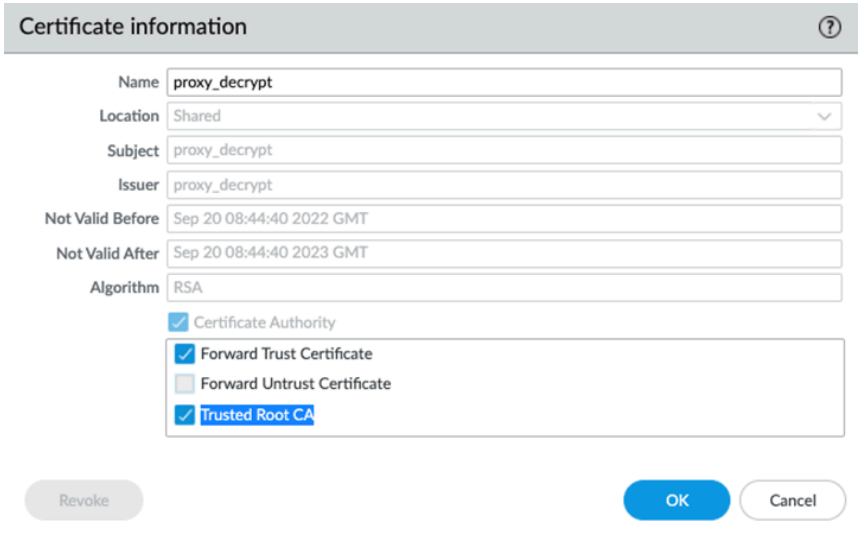
STEP 6 | 次の設定を構成して、常時インターネット セキュリティを有効にします。

1. [GlobalProtectを無効にすることをユーザーに許可する]を 、 **[Disallow (**許可しない**)]**、**[Allow with Passcode (**パスコードで許可する**)]**、または**[Allow with Ticket (**チケットで許可する**)]**に設定します。
2. [ユーザーがGlobalProtectアプリケーションからサインアウトできるようにする]を**No**に設定します。

STEP 7 | (任意) 明示的なプロキシ トラフィックの 復号ポリシーを構成します 。

復号化を有効にする場合は、復号化証明書も信頼できるルートCAとして設定されていることを確認してください。

1. **[デバイス] > [証明書管理] > [証明書]** を選択し、信頼されたルートCAと転送信頼証明書である証明書を作成します。



2. SSLフォワード プロキシを使用して、**Explicit_Proxy_Device Group** の下に復号化ルールを作成します。

 ©2025 Palo Alto Networks, Inc.

STEP 8 | 明示的なプロキシ トラフィックのセキュリティ ポリシー ルールを構成します。

1. **Policies** > **Security**を選択します。
2. デバイス グループを**Explicit_Proxy_Device_Group**に設定します。
3. 「インターネット ゲートウェイ セキュリティ ポリシーのベストプラクティス」に従ってください。

STEP 9 | (任意) デフォルト ルートのないネットワークでGlobalProtectアプリケーションをプロキシモードで構成します。

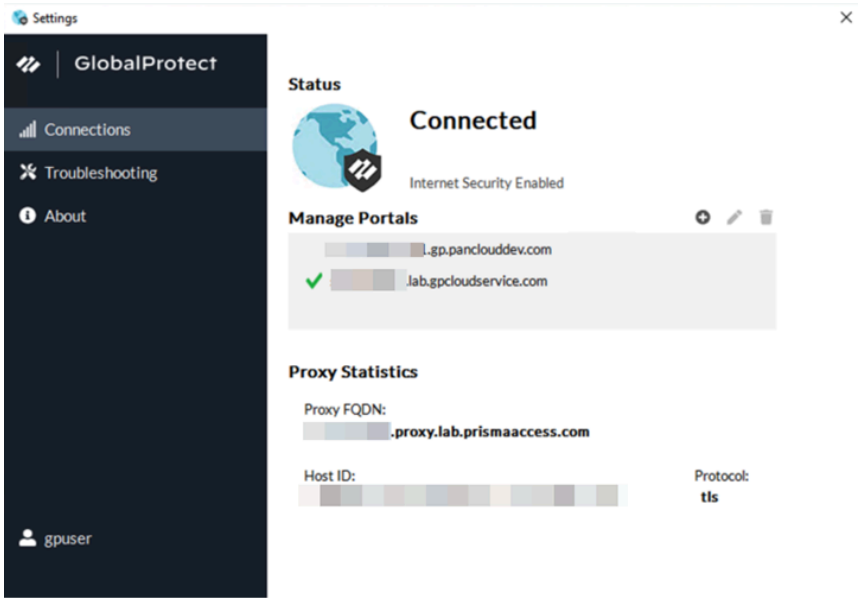
- （任意）PACファイルを内部でホストし 、 PACファイル内のプロキシとしてPrisma Access明示的なプロキシFQDNを指定するか、 転送プロファイル でPACファイルをホストし、ネットワーク内にPACサービスIPアドレスのルートを追加します。
- PACファイルで、IdP URLとPrisma AccessポータルURLを明示型プロキシに転送します。
- 明示的なプロキシでは、認証設定からIdPとポータルURLを除外します。認証フローで使用されるドメインにIdPとポータルURLを追加します。
- ユーザーが明示的プロキシ経由でインターネットにアクセスできるように、境界デバイス上の明示的プロキシFQDNまたはIPアドレスへのルートを設定します。
- （任意）ユーザーがブランチ ネットワーク内のパブリック ドメインを解決できない場合は、Prisma Access明示的プロキシFQDNを内部IPアドレスに解決するDNSレコードを追加し、内部IPアドレスの宛先NATを明示的プロキシFQDNまたはIPアドレスに追加します。

STEP 10 | Panoramaへの変更をコミットし、Prisma Accessモバイルユーザーおよび明示型プロキシへの設定変更をコミットしてプッシュします。

 ©2025 Palo Alto Networks, Inc.

STEP 11 | エージェント プロキシのデプロイメントを確認し、トラブルシューティングを行います。

1. GlobalProtectアプリケーションの[設定]の[接続] タブで、ネットワーク接続に関する情報を確認します。
   1. GlobalProtectアプリケーションを開きます。
   2. [設定] を選択してGlobalProtect設定パネルを開き、[接続]を選択します。



2. GlobalProtectログを表示および収集します。

   PanGPSログを表示して、GlobalProtectポータルのプロキシ モード構成を確認します。

   プロキシモードが設定されているかどうかは、PanGPSのログで以下のイベントを探すことで確認できます。

   `OnProxyAgentMode`：プロキシ専用モード

   Panorama で GlobalProtect ログを表示するには、モニター > ログを選択し、次の操作を行います。

   - **GlobalProtect**、認証ログ用、
   - ユーザーアクセスログ用のトラフィック と 復号化

トンネルおよびプロキシモードのGlobalProtect

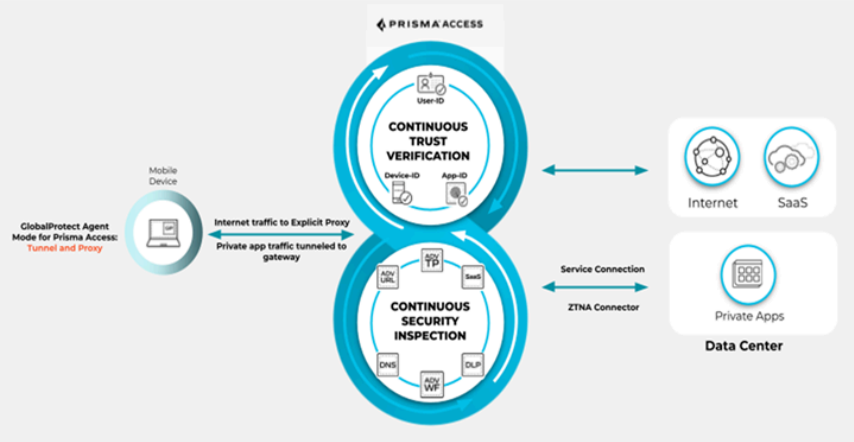
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager) この機能をPrisma Access環境で使用したい場合は、アカウントチームにお問い合わせください。	• Prisma Access 5.2 • WindowsまたはMacOS用のGlobalProtectアプリケーション バージョン6.2 • コンテンツリリースバージョン 8700-7994 • Prisma Access モバイルユーザーライセンス

©2025 Palo Alto Networks, Inc.

トンネルおよびプロキシモードでは、GlobalProtectアプリケーションは、PACファイルで定義したルールに基づいて、インターネット向けのトラフィックを明示的なプロキシに送信します。残りのトラフィックについては、PACファイルで定義されたスプリットトンネリングのルールとロジックを使用して、どのトラフィックをトンネルを通して送信するか、どのトラフィックがトンネルをバイパスできるかを判断します。トンネルルールが定義されていない場合、アプリケーションは残りのすべてのトラフィックをトンネルを通して送信します。

トンネルおよびプロキシモードで*GlobalProtect*アプリケーションを実行する際、ホスト情報プロファイル（*HIP*）機能は*GlobalProtect*トンネルを介したトラフィックのみサポートされています。プロキシを意識しないトラフィックを含む、すべての*IPv4 TCP*接続をサポートする*GlobalProtect*プロキシチャネルには、

と*GlobalProtect*エージェントバージョン*6.3.0*が必要です。シームレスな機能を確保するには、エンドポイントに構成された*DNS*が宛先*FQDN*を解決できる必要があります。



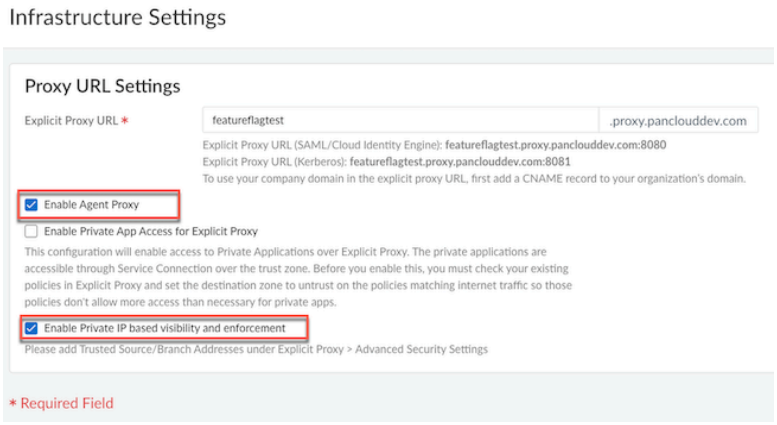
- Strata Cloud Manager
- Panorama

トンネルおよびプロキシモードのGlobalProtect (Strata Cloud Manager)

©2025 Palo Alto Networks, Inc.

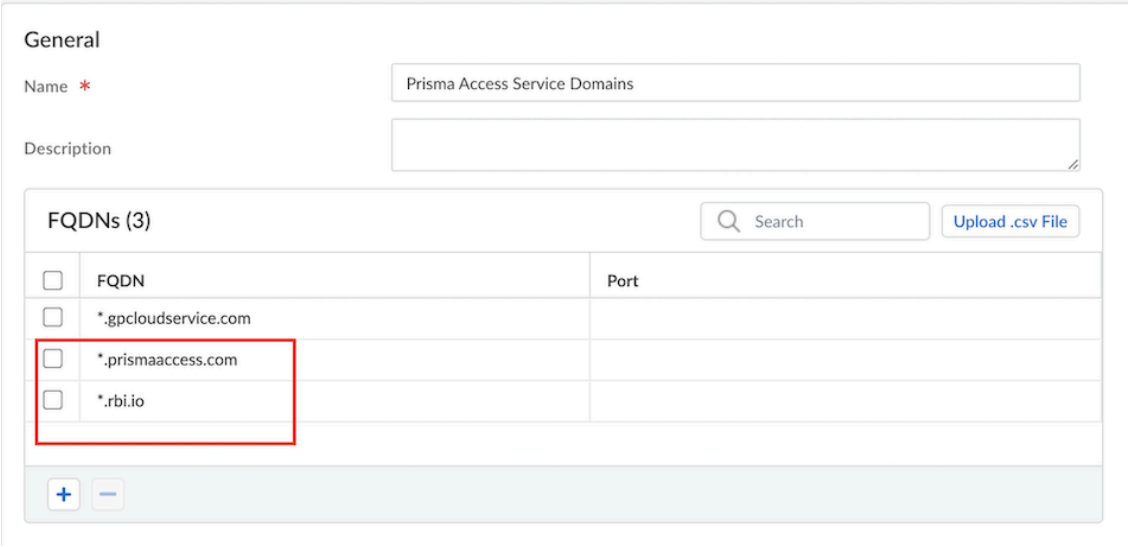
STEP 1 | Prisma Accessのモバイル ユーザー向けにエージェント ベースのプロキシ機能を有効にします。

1. 明示的なプロキシを有効にします。
   1. **[ワークフロー] > [Prisma Accessセットアップ] > [明示的プロキシ]**を選択します。
   2. インフラストラクチャ設定領域で、**[プロキシ設定のセットアップ]**をクリックし、**[明示的なプロキシURL]**を指定します。
2. エージェント プロキシを有効にし 、オプションでプライベート **IP** ベースの可視性と適用を有効にして、**[保存]**をクリックします。



3. モバイルユーザーをサポートしたいPrisma Accessロケーションを選択します。

   最適なユーザー エクスペリエンスにむけて、場所の数を制限する場合は、エンド ユーザーに最も近いロケーションを選択します。モバイル ユーザーが居住する国で場所が利用できない場合は、モバイル ユーザーに最も近いロケーションを選択します。
4. 転送プロファイルを作成して、 明示的なプロキシ経由で送信するトラフィックを定義します。転送プロファイルを構成する際、*.prismaaccess.com および *.gpcloudservice.com ドメインをバイパスします。



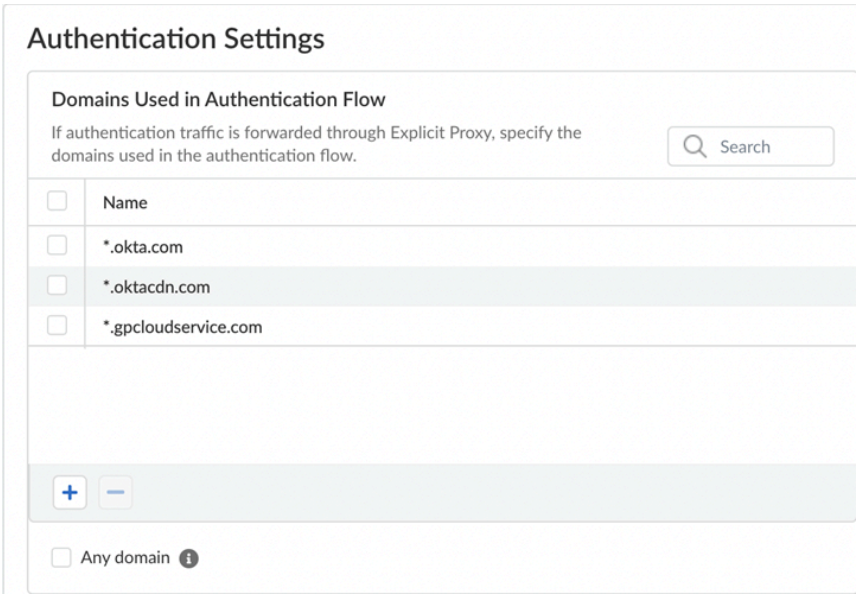
5. 転送プロファイルをGlobalProtectアプリケーション構成に添付します。

 ©2025 Palo Alto Networks, Inc.

6. **[Workflows (ワークフロー)] > [Setup (セットアップ)] > [Explicit Proxy (明示型プロキシ)] > [Advanced Security Settings (詳細セキュリティ設定)] > [Authentication Settings (認証設定)]**を選択し、バイパスする必要があるドメインを追加します。

   プロキシへのすべてのリクエストは認証を受けます。ただし、プロキシを介してIdPフローを渡している場合は、認証を成功させるためにIDPフローをバイパスする必要があります。

   この例では、GlobalProtectポータルとOktaをバイパスしていますが、使用するIdPに合わせてカスタマイズしてください。

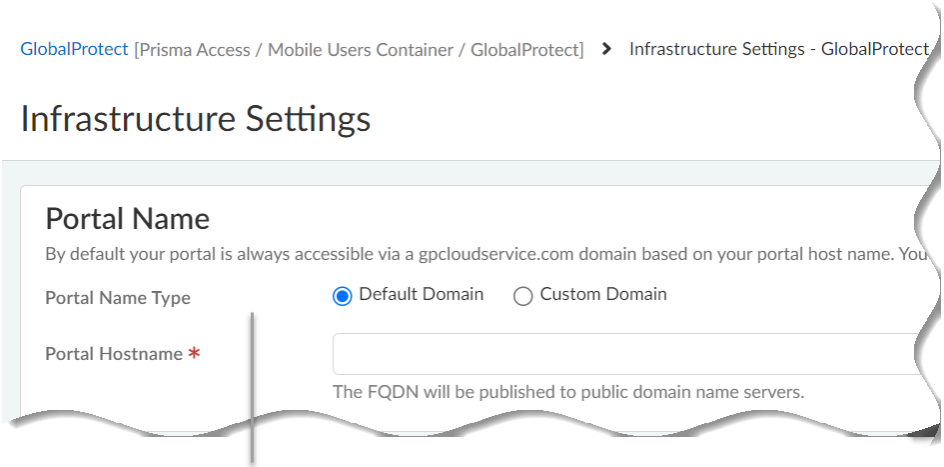


©2025 Palo Alto Networks, Inc.

STEP 2 | Prisma AccessのGlobalProtectアプリケーションのトンネルモードとプロキシモードを設定します。

トンネルおよびプロキシモードでは、設定した接続方法は*GlobalProtect*を介してトンネリングされるトラフィックにのみ適用されます。エージェントベースのプロキシ機能により、常時接続のインターネットセキュリティが提供されます。オンデマンド接続方法を設定した場合でも、ユーザーが*GlobalProtect*アプリケーションを切断しても、インターネット経由のすべてのトラフィックは常時接続のインターネットセキュリティのためにプロキシされます。

1. [ワークフロー] > **[Prisma Access**セットアップ] > **[GlobalProtect]** > [インフラストラクチャ] > [インフラストラクチャ設定]を選択し、[ポータル名]を指定します。



GlobalProtect Infrastructure Settings

- **Use Default Domain**（デフォルトドメインを使用）–このオプションを選択した場合、ポータルホスト名はデフォルトのドメイン名「`.gpcloudservice.com`」を使用します。この場合は、デフォルトのドメイン名に追加するポータル ホスト名を入力するだけです。 ユーザー向けPrisma Accessは必要な証明書を自動的に作成し、ホスト名をパブリックDNSサーバーに公開します。

©2025 Palo Alto Networks, Inc.

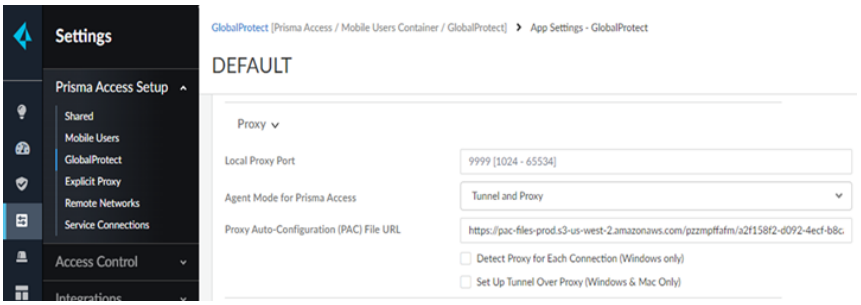
- カスタム ドメイン- ポータル ホスト名のドメインを会社のドメイン名 (たとえば、myportal.mydomain.com) と一致させたい場合は、ポータル アドレスをカスタマイズすることもできます。

2. モバイルユーザーがPrisma Accessに対して認証できるようにします。
3. GlobalProtectアプリケーションの設定で、Prisma AccessのGlobalProtectトンネルとプロキシモードを有効にして、インターネットトラフィックをエージェントベースのプロキシに送信します。

   - [ワークフロー] > **Prisma Access**[セットアップ] > **[GlobalProtect]**を選択します。
   - **GlobalProtect**アプリケーションタブで、デフォルトをクリックしてアプリ設定をカスタマイズするか、 **[**アプリ設定の追加**]**をクリックして新しい構成を追加します。
   - 「詳細オプションを表示」 をクリックし、「アプリ構成」 セクションをクリックします。
   - プロキシセクションで、**Prisma Access**用のエージェントモードを**[**トンネルとプロキシ**]**に設定して、Prisma Accessでインターネットトラフィックを明示的なプロキシに送信し、プライベートアプリケーショントラフィックをVPNに送信するようにGlobalProtectアプリケーションに指示します。Prisma Accessでトンネルおよびプロキシモードを設定すると、GlobalProtectアプリケーションを切断または無効にしても、ユーザーはPrisma Access経由で安全にインターネットにアクセスできます。
   - (任意) ローカル プロキシ ポートを設定します。ポート範囲は1024 ～ 65534で、デフォルト ポートは9999です。デフォルトのポートが使用できない場合、GlobalProtect は9999 ～ 10009の範囲にある他の10個のポートを試行し、使用可能なポートを使用します。範囲内で独自のポート番号を選択することもできます。
   - (任意) プロキシ設定の新規PAC URLをエンドポイントにプッシュする場合は、PAC自動設定 (PAC) ファイルURLを構成します。ユーザーが接続すると、PAC URLがエンドポイントにプッシュされます。ユーザーがGlobalProtectアプリケーションを切断すると、エンドポイント プロキシ設定は自動的に無効になり、以前の設定に戻ります。
   - (任意) ユーザーがポータルで新しい設定を確認できるようにする場合は、[Allow User to Rediscover Network (ユーザーによるネットワークの再検出を許可)] を有効にします。
   - (任意)GlobalProtectアプリケーション設定の更新間隔 (時間)を設定します。デフォルトでは、GlobalProtectクライアントはキャッシュされたポータル設定を24時間ごとに更新します。ビジネス要件に応じて更新間隔を変更できます。

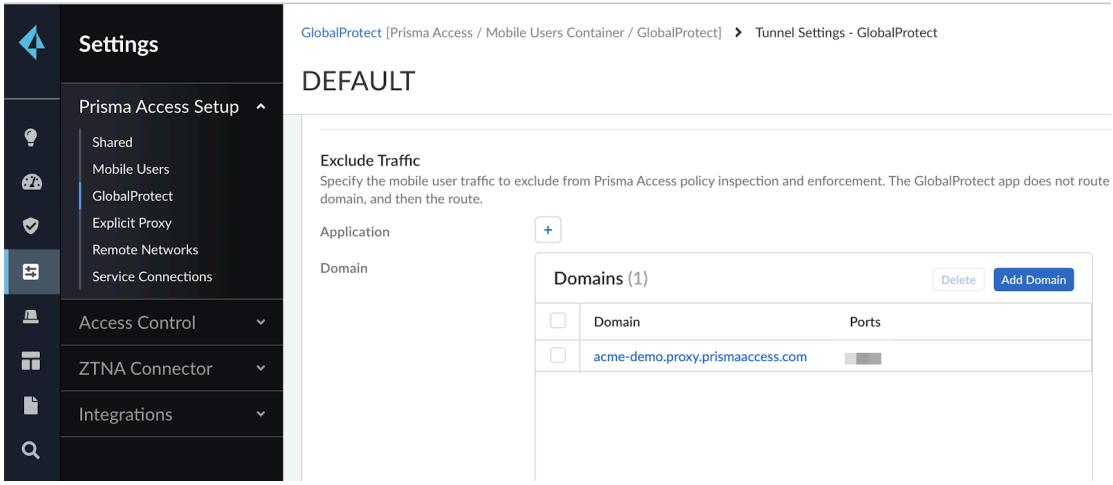
©2025 Palo Alto Networks, Inc.

- **Tunnel Over Proxy**のセットアップを無効にします（**Windows** および **Mac** のみ）。



©2025 Palo Alto Networks, Inc.

4. スプリットトンネル設定で、明示的プロキシFQDNとPACファイルFQDNを除外します。
   - [ワークフロー] > **Prisma Access**[セットアップ] > **[GlobalProtect]**を選択します。
   - **GlobalProtect**アプリケーションタブで、デフォルトをクリックしてトンネル設定をカスタマイズするか、 [トンネル設定の追加]をクリックして新しい構成を追加します。
   - [トラフィックを除外] で [ドメインを追加] をクリックします。



 ©2025 Palo Alto Networks, Inc.

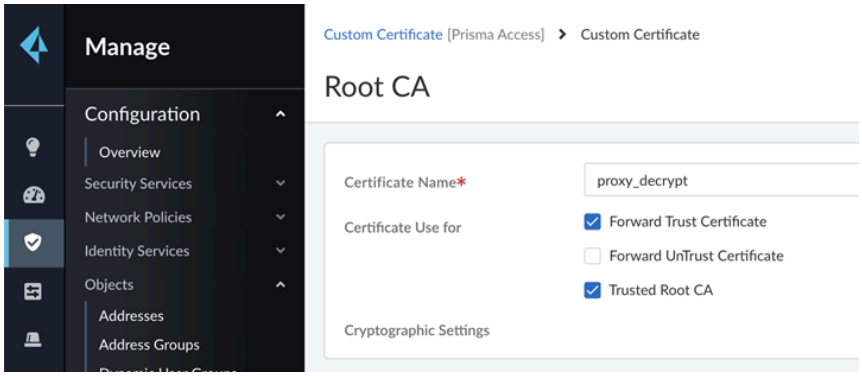
イメージ内の *FQDN*をプロキシ*FQDN*に置き換えます。

STEP 3 | [ワークフロー] > **[Prisma Access**セットアップ] > **[GlobalProtect]** > **[GlobalProtect**アプリケーション] > **[**アプリ設定の追加]ページで以下の設定を行い、常時接続のセキュリティを有効にする：

1. GlobalProtectを無効にするを 、 **[Disallow (**許可しない)]、 **[Allow with Passcode (**パスコードで許可する)]、または**[Allow with Ticket (**チケットで許可する)]に設定します。
2. [ユーザーがGlobalProtectアプリケーションからサインアウトできるようにする]を無効にします。

STEP 4 | 明示型プロキシ トラフィックの復号化を設定します。

- **[Manage (**管理)] > **[Configuration (**設定)] > **[NGFW]** > **[Security Services (**セキュリティ サービス)] > **[Decryption (**復号化)]を選択します。
- 復号化を有効にする場合は、復号化証明書を信頼できるルートCAとしてセットアップしてください。



STEP 5 | 明示的なプロキシ トラフィックのセキュリティ ポリシー ルールを構成します。

- **[Manage (**管理)] > **[Configuration (**設定)] > **[NGFW]Prisma Access** > **[Security Services (**セキュリティ サービス)] > **[Security Policy (**セキュリティ ポリシー)]を選択します。
- 「インターネット ゲートウェイ セキュリティ ポリシーのベストプラクティス」に従ってください。

©2025 Palo Alto Networks, Inc.

STEP 6 | (任意) デフォルト以外のルートネットワークのプロキシモードとトンネルモードでGlobalProtectアプリケーションを設定します。

- （任意）PACファイルを内部でホストし 、 PACファイル内のプロキシとしてPrisma Access明示的なプロキシFQDNを指定するか、 転送プロファイル でPACファイルをホストし、ネットワーク内にPACサービスIPアドレスのルートを追加します。
- ポータルとゲートウェイのFQDNとIdP URLの認証要求をインターネットに転送します。
- ユーザーが明示的プロキシ経由でインターネットにアクセスできるように、境界デバイス上の明示的プロキシFQDNまたはIPアドレスへのルートを設定します。
- （任意）ユーザーがブランチ ネットワーク内のパブリック ドメインを解決できない場合は、Prisma Access明示的プロキシFQDNを内部IPアドレスに解決するDNSレコードを追加し、内部IPアドレスの宛先NATを明示的プロキシFQDNまたはIPアドレスに追加します。
- ユーザーがオフィスにいるときにプライベートアプリに直接アクセスできるようにするには:
  - ダイレクトアクセス:内部ホスト検出を有効にし、内部ゲートウェイリストを空のままにします。

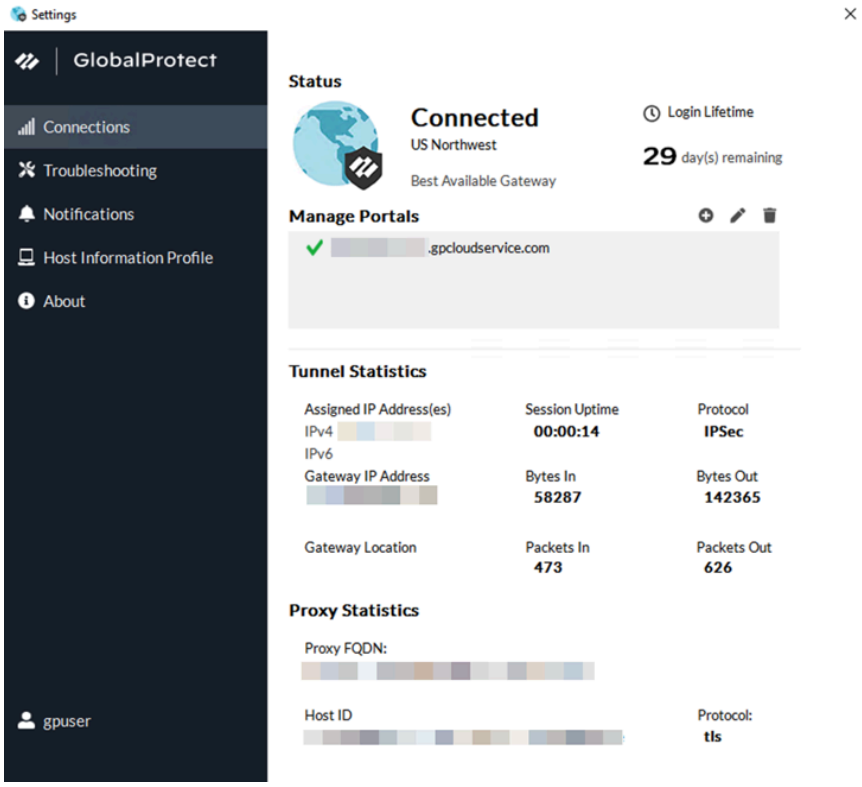
STEP 7 | [保存]をクリック して、**GlobalProtect** と 明示的なプロキシに[設定をプッシュ] をクリックします。

©2025 Palo Alto Networks, Inc.

STEP 8 | エージェント プロキシのデプロイメントを確認し、トラブルシューティングを行います。

1. GlobalProtectアプリケーションの[設定]の[接続] タブで、ネットワーク接続に関する情報を確認します。

   1. GlobalProtectアプリケーションを開きます。
   2. [設定] を選択してGlobalProtect設定パネルを開き、[接続]を選択します。



2. GlobalProtectログを表示および収集します。

   PanGPSログを表示して、GlobalProtectポータルのプロキシ モード構成を確認します。

   プロキシモードが設定されているかどうかは、PanGPSのログで以下のイベントを探すことで確認できます。

   `OnProxyAgentMode:` ハイブリッドモード

   で GlobalProtect ログを表示するには、**[Incidents & Alerts (**インシデントとアラート**)]** > **[Log Viewer (**ログ ビューアー**)]**を選択します：

   - **GlobalProtect**(認証ログ用)
   - ユーザーアクセスログ用のトラフィック と 復号化

常時接続方式によるトンネルとプロキシモードの切断と無効化

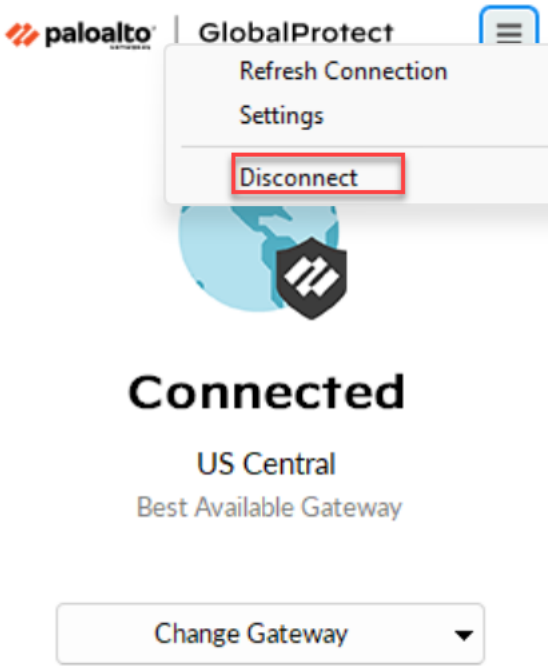
GlobalProtectバージョン6.3.1以降、GlobalProtectアプリケーションのトンネルモードとプロキシモードを接続方法として**Always-On**モードとともに構成し、トンネルとプロキシモードを切断する場合は、次の手順を実行する必要があります。

 ©2025 Palo Alto Networks, Inc.

1. GlobalProtectアプリケーションを切断して、トンネル (VPN) 接続を切断します。アプリを切断すると、トンネル (VPN) 接続が切断され、アプリは引き続きプロキシモードで接続されます。
2. GlobalProtectアプリケーションを無効にして、トンネルモードとプロキシモードの両方を切断します。アプリを無効にすると、トンネルモードとプロキシモードの両方が切断され、アプリは接続されなくなります。

トンネルとプロキシ (ハイブリッドモード) と**Always-On** (常時オン)接続方法で設定されたGlobalProtectアプリケーションを切断して無効にするには、次の操作を行う必要があります。

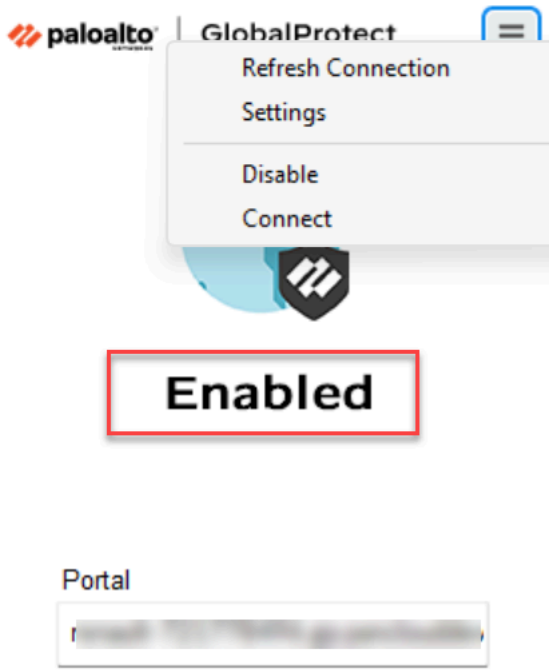
1. ハンバーガーメニューから切断オプションを使用して、GlobalProtectアプリケーションを切断します。アプリを切断すると、トンネル (VPN) 接続が切断されます。



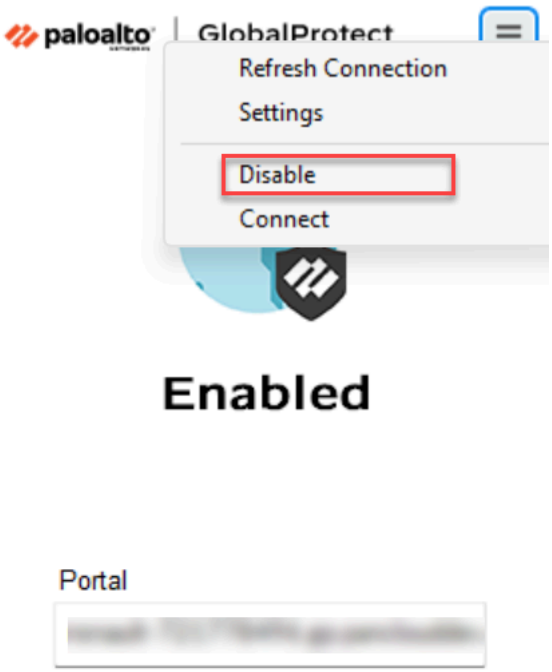
アプリを切断すると、VPN 接続は切断されますが、プロキシモードは有効になります。アプリは引き続きプロキシモードで接続され、アプリにはステータスが[有効] と表示されます。

トンネル *(VPN)* 接続を再接続する場合は、ハンバーガーメニューの*[*接続*]*オプションを使用できます。

©2025 Palo Alto Networks, Inc.

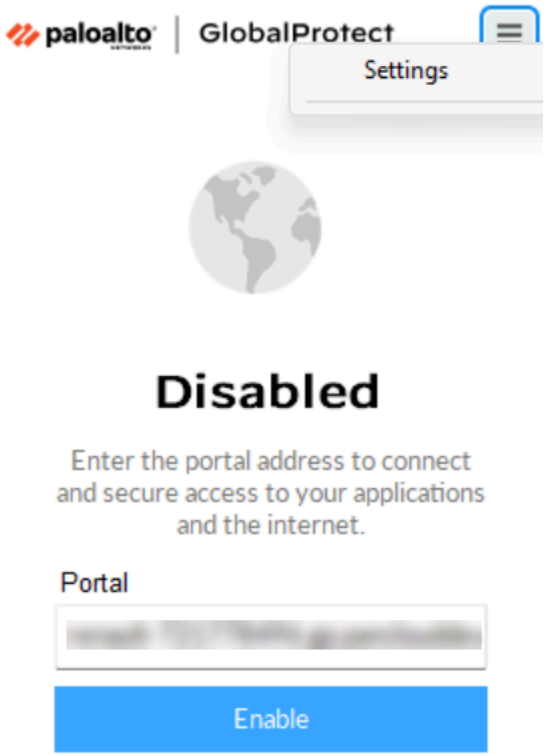


2. ハンバーガーメニューの無効化オプションを使用して、GlobalProtectアプリケーションを無効にします。アプリを無効にすると、トンネル接続とプロキシ接続の両方が切断されます。



アプリが無効になり、ステータスが[無効]と表示されます。

©2025 Palo Alto Networks, Inc.



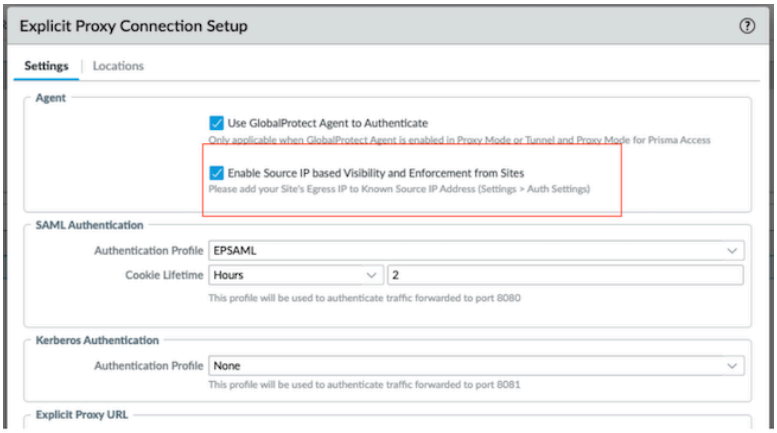
トンネルおよびプロキシモードのGlobalProtect (Panorama)

シングルテナントを変換する場合、マルチテナントへの*Prisma Access (Managed by Panorama)*デプロイメントでは、最初のテナント (移行したテナント) のみがこの機能をサポートします。また、この最初のテナントでは、カスタム デバイス グループではなく、事前定義済みの *Explicit_Proxy_Device_Group* にポリシー ルールを設定する必要があります。マルチテナントデプロイメント用に最初に作成したテナントの後に作成する後続のテナントでは、この機能はサポートされません。

©2025 Palo Alto Networks, Inc.

STEP 1 | モバイル ユーザー向けにエージェントベースのプロキシ機能を有効にします。

1. 明示的なプロキシを有効にします。
   1. **[Panorama]** > **[クラウド サービス]** > **[構成]** > **[モバイル ユーザー - 明示的なプロキシ]**を選択します。
   2. 明示的なプロキシ**URL**を指定するには、明示的なプロキシ設定を構成します 。
2. エージェントベースのプロキシ機能を有効にするには、**[GlobalProtect**アプリケーションを使用して認証する**]** を選択し、 任意で**[**サイトからのソース**IP**ベースの可視性と適用を有効にする**]**を選択します。



3. **PAC (**プロキシ自動構成**)** ファイルのURLを入力します。PACファイルにポート8080を入力していることを確認してください。
   - PACファイルのプロキシステートメントでは、 上記で設定したPrisma AccessFQDNが使われている必要があります。
   - PACファイルは、GlobalProtectゲートウェイ (*.gp.gpcoudservice.com) を除外するように構成する必要があります。
4. 構成した明示的なプロキシ設定の接続名を選択します。
5. モバイル ユーザー向けの明示的なプロキシをデプロイするロケーションとリージョンを選択します。

   Prisma Accessは、選択した各ロケーションにプロキシノードを追加します。明示的プロキシは、すべてのPrisma Accessロケーションのサブセットをサポートしています。最適なユーザー エクスペリエンスにむけて、場所の数を制限する場合は、エンド ユーザーに最も近いロケーションを選択します。モバイル ユーザーが居住する国で場所が利用できない場合は、モバイル ユーザーに最も近いロケーションを選択します。

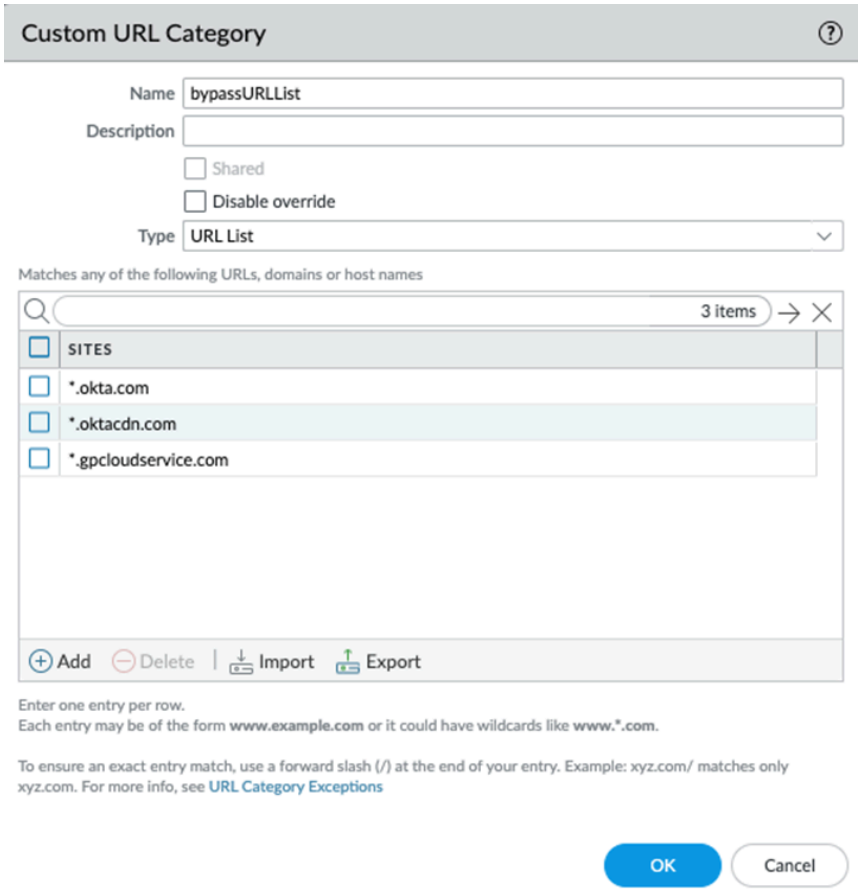
©2025 Palo Alto Networks, Inc.

STEP 2 | IDプロバイダー (IDP) をバイパスします。

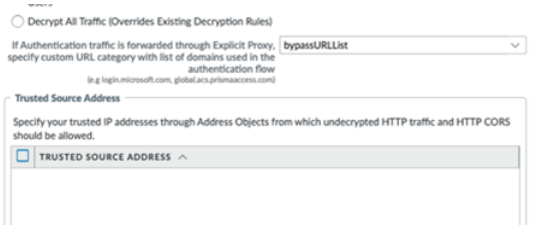
プロキシへのすべての要求が認証されます。ただし、プロキシを介してIDPフローを渡している場合は、認証を成功させるためにIDPフローをバイパスする必要があります。

この例では、GlobalProtectポータルとOktaをバイパスしていますが、使用するIDPに合わせてカスタマイズしてください。

1. **Explicit_Proxy_Device_Group**が選択された状態で、[オブジェクト] > [カスタムオブジェクト] > [**URL**カテゴリ]を選択し、カスタムURLカテゴリーを作成します。
2. カスタムURLカテゴリで、EP認証からバイパスする必要があるすべてのFQDNドメインを追加します。



3. [クラウドサービス] > [構成] > [モバイルユーザー] > [明示型プロキシ] > [設定] > [認証設定]を選択し、カスタムURLカテゴリをアタッチします。



4. コミットして**Explicit_Proxy_Device_Group**にプッシュします。

 ©2025 Palo Alto Networks, Inc.

STEP 3 | GlobalProtectポータルを設定します。

トンネルおよびプロキシモードでは、設定した接続方法は*GlobalProtect*を介してトンネリングされるトラフィックにのみ適用されます。エージェントベースのプロキシ機能により、常時接続のインターネットセキュリティが提供されます。オンデマンド接続方法を設定した場合でも、ユーザーが*GlobalProtect*アプリケーションを切断しても、インターネット経由のすべてのトラフィックは常時接続のインターネットセキュリティのためにプロキシされます。

1. Onboarding（オンボーディング）セクションで**Add**（追加）をクリックします。
2. [全般] タブで、 ポータル名のタイプを指定します。

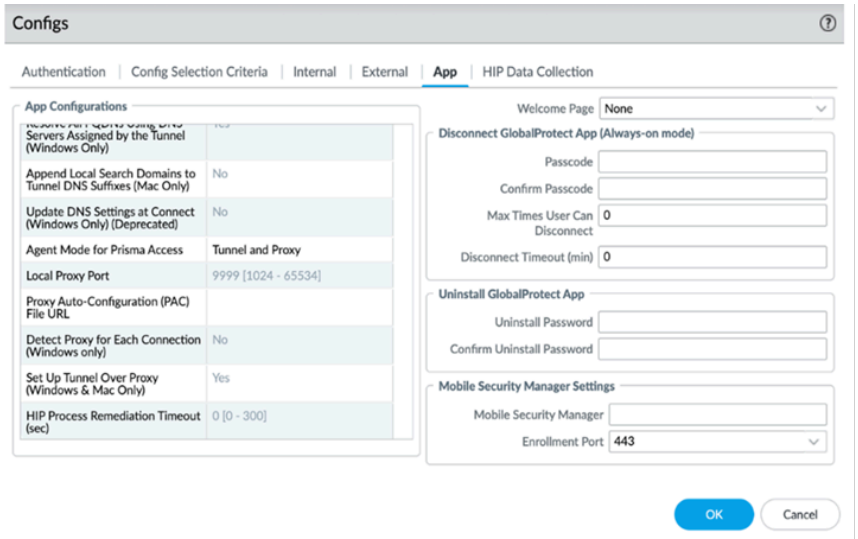
   デフォルト ドメインの使用 - このオプションを選択すると、ポータル ホスト名にはデフォルトのドメイン名 (.gpcloudservice.com) が使用されます。この場合は、デフォルトのドメイン名に追加するポータル ホスト名を入力するだけです。 必要な証明書

©2025 Palo Alto Networks, Inc.

がPrisma Accessで自動的に作成され、ホスト名がパブリック DNS サーバーに公開されます。

会社のドメインを使用する - ポータル ホスト名のドメインを会社のドメイン名 (例: myportal.mydomain.com) と一致させる場合は、このオプションを選択します。

3. Prisma Accessがモバイルユーザを認証する方法を指定する認証プロファイルを選択するか、新しいプロファイルを作成します。
4. (任意) モバイル ユーザーがポータルおよびゲートウェイへの認証に使用する安全なCookieを暗号化するには、 認証オーバーライド証明書を選択します。
   1. GlobalProtectでトンネルとプロキシ モードを有効にします。
      1. **[ネットワーク] > [GlobalProtect** ポータル**]**を選択します。
      2. エージェント設定を追加するポータル設定を選択し、さらに**Agent**（エージェント）タブを選択します。
      3. **[エージェント]**タブで、**[アプリ]**を選択します。
      4. [アプリ構成]エリアで、**Prisma Access**のエージェント モードを**[トンネルとプロキシ]**に設定し、インターネット トラフィックをPrisma Accessの明示的なプロキシに送信し、プライベート アプリ トラフィックをVPNに送信します。



   2. オプションの設定を実行します。
      1. (任意) ローカル プロキシ ポートを設定します。ポート範囲は1024 ～ 65534で、デフォルト ポートは9999です。デフォルトのポートが使用できない場合、GlobalProtect は9999 ～ 10009の範囲にある他の10個のポートを試行し、使用可能なポートを使用します。範囲内で独自のポート番号を選択することもできます。
      2. (任意) プロキシ設定のカスタムPAC URLをエンドポイントにプッシュする場合は、PAC自動設定 (PAC) ファイルURLを構成します。ユーザーが接続すると、PAC URLがエンドポイントにプッシュされます。ユーザーがGlobalProtectアプリケーションを切断すると、エンドポイント プロキシ設定は自動的に無効になり、以前の設定に戻ります。

©2025 Palo Alto Networks, Inc.

3. (任意) ユーザーがポータルで新しい設定を確認できるようにする場合は、[Allow User to Rediscover Network (ユーザーによるネットワークの再検出を許可)] を有効にします。
4. (任意)GlobalProtectアプリケーション設定の更新間隔 (時間)を設定します。デフォルトでは、GlobalProtectクライアントはキャッシュされたポータル設定を24時間ごとに更新します。ビジネス要件に応じて更新間隔を変更できます。

3. スプリットトンネル設定で、明示的プロキシFQDNとPACファイルFQDNを除外します。

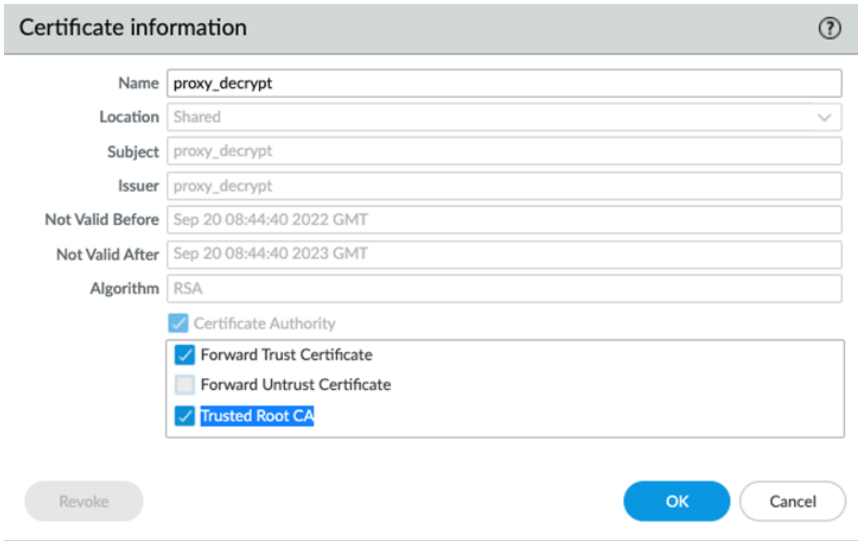
STEP 4 | 次の設定を構成して、常時インターネット セキュリティを有効にします。

1. [GlobalProtectを無効にすることをユーザーに許可する]を 、**[Disallow (許可しない)]**、**[Allow with Passcode (パスコードで許可する)]**、または**[Allow with Ticket (チケットで許可する)]**に設定します。
2. [ユーザーがGlobalProtectアプリケーションからサインアウトできるようにする]を**No**に設定します。

STEP 5 | (任意) 明示的なプロキシ トラフィックの 復号ポリシーを構成します 。

復号化を有効にする場合は、復号化証明書も信頼できるルートCAとして設定されていることを確認してください。

1. **[デバイス] > [証明書管理] > [証明書]** を選択し、信頼されたルートCAと転送信頼証明書である証明書を作成します。



2. SSLフォワード プロキシを使用して、**Explicit_Proxy_Device Group** の下に復号化ルールを作成します。

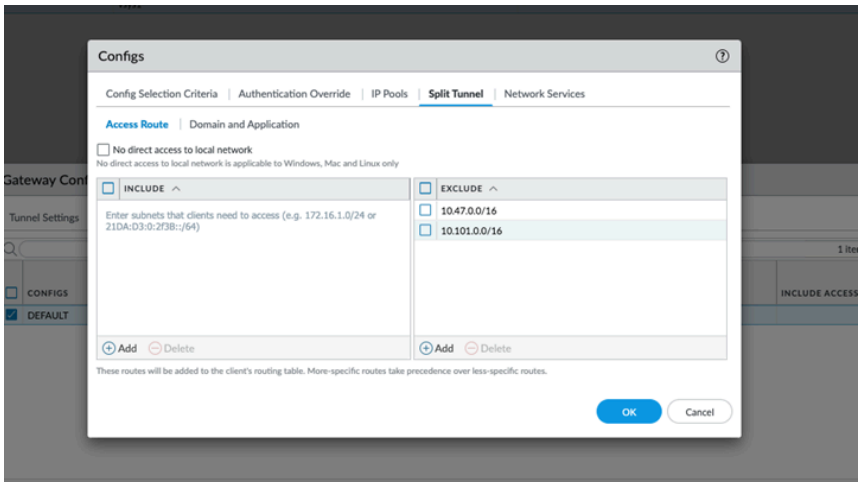
STEP 6 | 明示的なプロキシ トラフィックのセキュリティ ポリシー ルールを構成します。

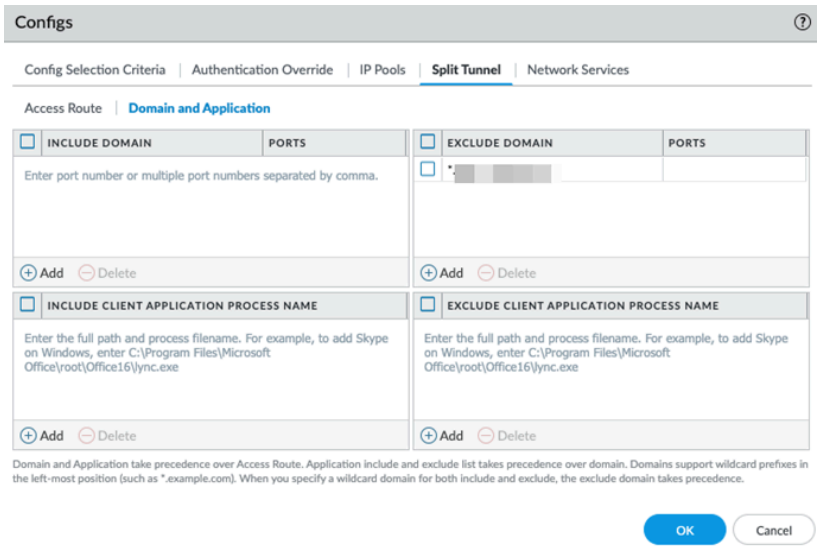
- **[Manage (管理)] > [Security Services (セキュリティサービス)] > [Security (セキュリティ)] >** を選択します。
- 「インターネット ゲートウェイ セキュリティ ポリシーのベストプラクティス」に従ってください。

©2025 Palo Alto Networks, Inc.

STEP 7 | Panoramaでスプリット トンネルを構成します。

1. **[ネットワーク] > [モバイル ユーザー テンプレート] > [ゲートウェイ] > [GlobalProtect_ExternalGateway] > [エージェント] > [クライアント設定] > [Split (分割)]**を選択します。
2. ルートとドメインに基づいてトンネルを構成します。





 ©2025 Palo Alto Networks, Inc.

STEP 8 | (任意) デフォルトルートでないネットワークで、GlobalProtectアプリケーションをトンネルおよびプロキシモードで構成します。

- （任意）PACファイルを内部でホストし 、 PACファイル内のプロキシとしてPrisma Access明示的なプロキシFQDNを指定するか、 転送プロファイル でPACファイルをホストし、ネットワーク内にPACサービスIPアドレスのルートを追加します。
- GlobalProtectポータルURLとIDP URLがPrisma Access明示型プロキシに転送されていることを確認します。
- ユーザーが明示的プロキシ経由でインターネットにアクセスできるように、境界デバイス上の明示的プロキシFQDNまたはIPアドレスへのルートを設定します。
- （任意）ユーザーがブランチ ネットワーク内のパブリック ドメインを解決できない場合は、Prisma Access明示的プロキシFQDNを内部IPアドレスに解決するDNSレコードを追加し、内部IPアドレスの宛先NATを明示的プロキシFQDNまたはIPアドレスに追加します。
- ユーザーがオフィスにいるときにプライベートアプリに直接アクセスできるようにするには:
  - ダイレクトアクセス–内部ホスト検出を有効にし、内部ゲートウェイリストを空のままにします。

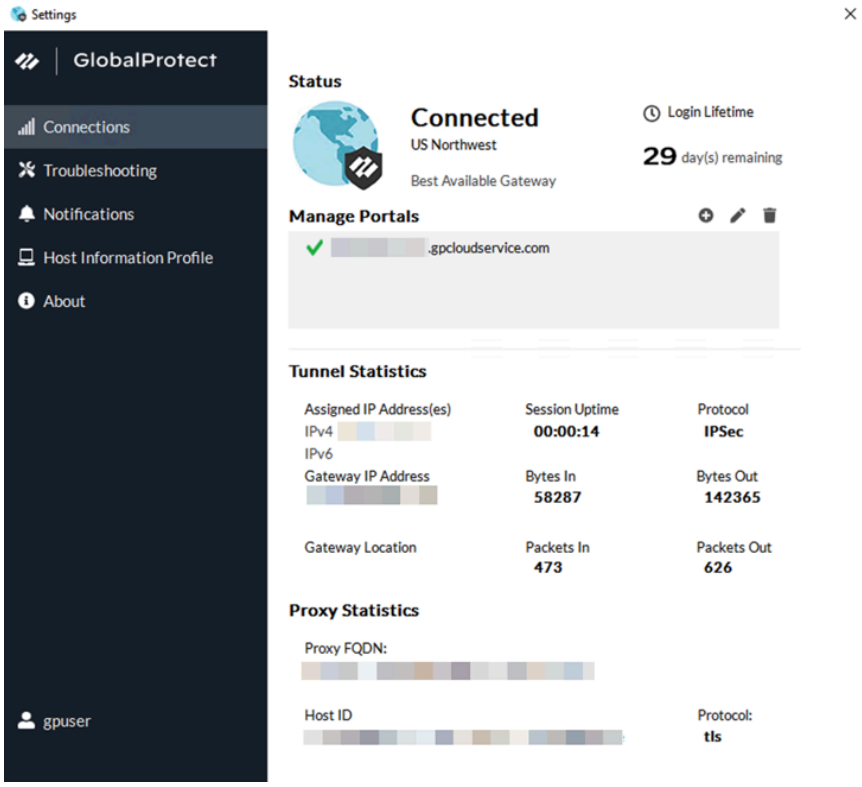
STEP 9 | Panoramaへの変更をコミットし、Prisma Accessモバイルユーザーおよび明示型プロキシへの設定変更をコミットしてプッシュします。

©2025 Palo Alto Networks, Inc.

STEP 10 | エージェント プロキシのデプロイメントを確認し、トラブルシューティングを行います。

1. GlobalProtectアプリケーションの[設定]の[接続] タブで、ネットワーク接続に関する情報を確認します。

   1. GlobalProtectアプリケーションを開きます。
   2. [設定] を選択してGlobalProtect設定パネルを開き、[接続]を選択します。



2. GlobalProtectログを表示および収集します。

   PanGPSログを表示して、GlobalProtectポータルのプロキシ モード構成を確認します。

   プロキシモードが設定されているかどうかは、PanGPSのログで以下のイベントを探すことで確認できます。

   `OnProxyAgentMode:` ハイブリッドモード

   Panorama で GlobalProtect ログを表示するには、モニター > ログを選択し、次の操作を行います。

   - **GlobalProtect**、認証ログ用、
   - ユーザーアクセスログ用のトラフィック と 復号化

常時接続方式によるトンネルとプロキシモードの切断と無効化

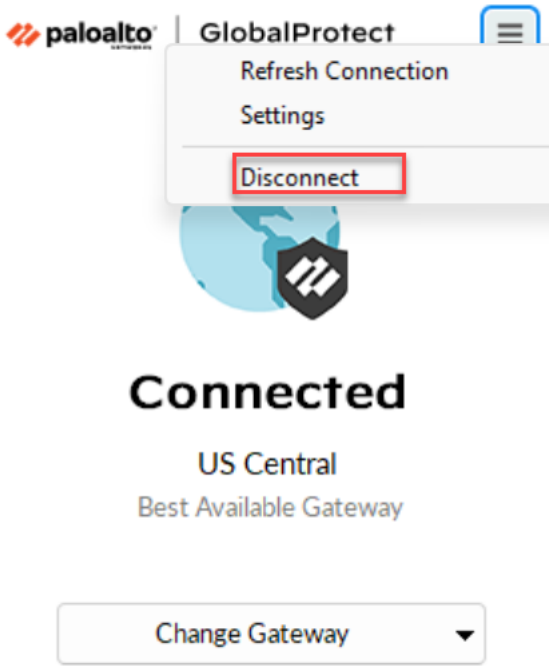
GlobalProtectバージョン6.3.1以降、GlobalProtectアプリケーションのトンネルモードとプロキシモードを接続方法として**Always-On** (常時オン)モードとともに構成し、トンネルとプロキシモードを切断する場合は、次の手順を実行する必要があります。

©2025 Palo Alto Networks, Inc.

1. GlobalProtectアプリケーションを切断して、トンネル (VPN) 接続を切断します。アプリを切断すると、トンネル (VPN) 接続が切断され、アプリは引き続きプロキシモードで接続されます。
2. GlobalProtectアプリケーションを無効にして、トンネルモードとプロキシモードの両方を切断します。アプリを無効にすると、トンネルモードとプロキシモードの両方が切断され、アプリは接続されなくなります。

トンネルとプロキシ (ハイブリッドモード) と**Always-On** (常時オン)接続方法で設定されたGlobalProtectアプリケーションを切断して無効にするには、次の操作を行う必要があります。

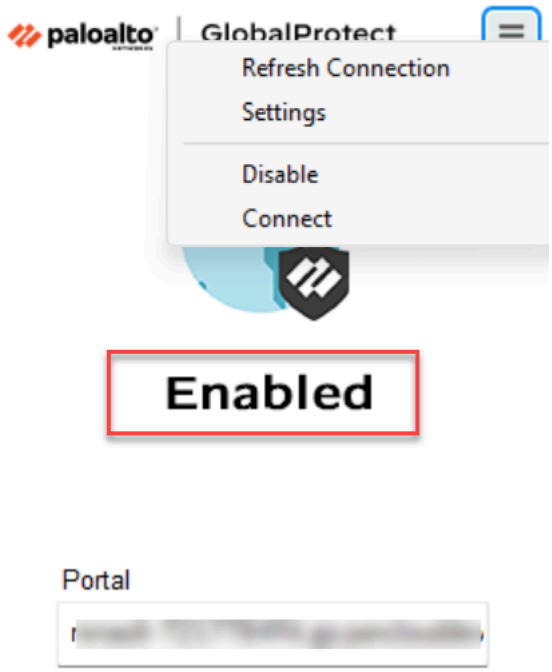
1. ハンバーガーメニューから切断オプションを使用して、GlobalProtectアプリケーションを切断します。アプリを切断すると、トンネル (VPN) 接続が切断されます。



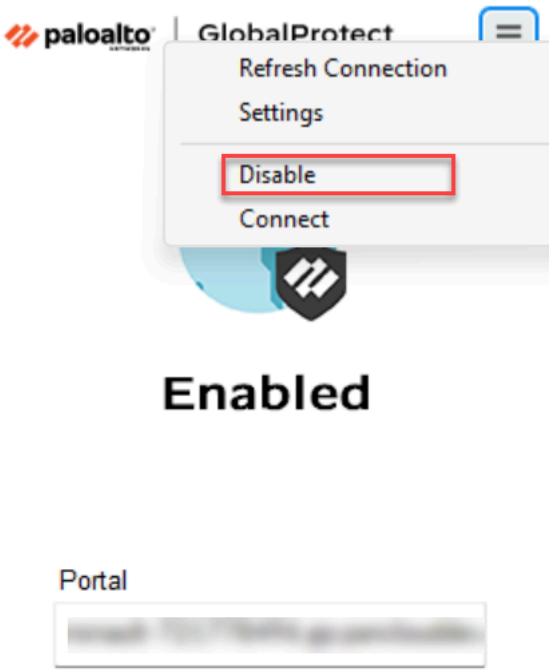
アプリを切断すると、VPN 接続は切断されますが、プロキシモードは有効になります。アプリは引き続きプロキシモードで接続され、アプリにはステータスが[有効] と表示されます。

トンネル *(VPN)* 接続を再接続する場合は、ハンバーガーメニューの*[*接続*]*オプションを使用できます。

©2025 Palo Alto Networks, Inc.

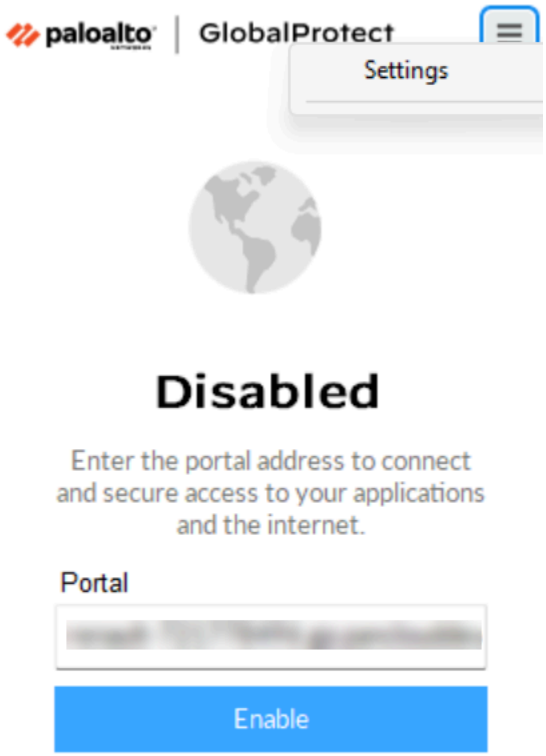


2. ハンバーガーメニューの無効化オプションを使用して、GlobalProtectアプリケーションを無効にします。アプリを無効にすると、トンネル接続とプロキシ接続の両方が切断されます。



アプリが無効になり、ステータスが[無効]と表示されます。

©2025 Palo Alto Networks, Inc.



エージェント ベースのプロキシ トラフィックに対するプライベートIPアドレスの可視化と適用

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	• Prisma Access 5.2 • WindowsまたはMacOS用のGlobalProtectアプリケーション バージョン6.3.1 • Prisma Access データプレーン 10.2.4 • Prisma Access モバイルユーザーライセンス • Panoramaプラグイン バージョン 5.2.0

ブランチからGlobalProtectエージェントを介してPrisma Access明示型プロキシに接続するユーザーは、エンドポイントのプライベートIPアドレスをログに利用したり、IPアドレス ベースの実施を適用したりできます。

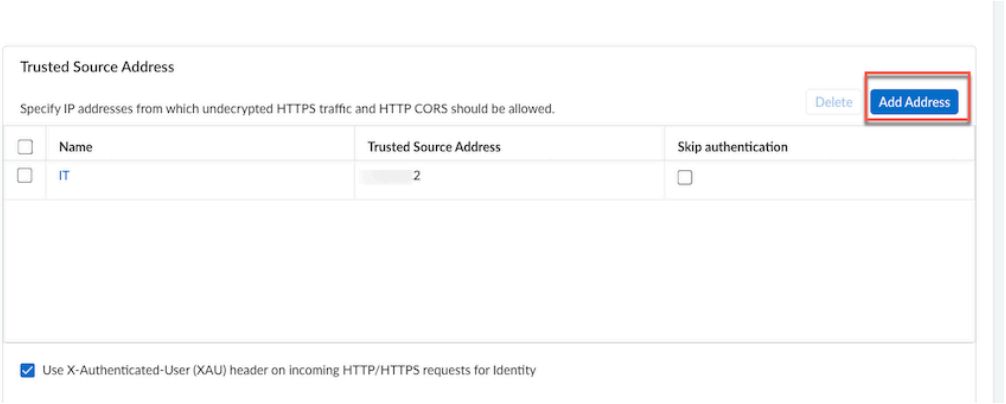
- Strata Cloud Manager
- Panorama

©2025 Palo Alto Networks, Inc.

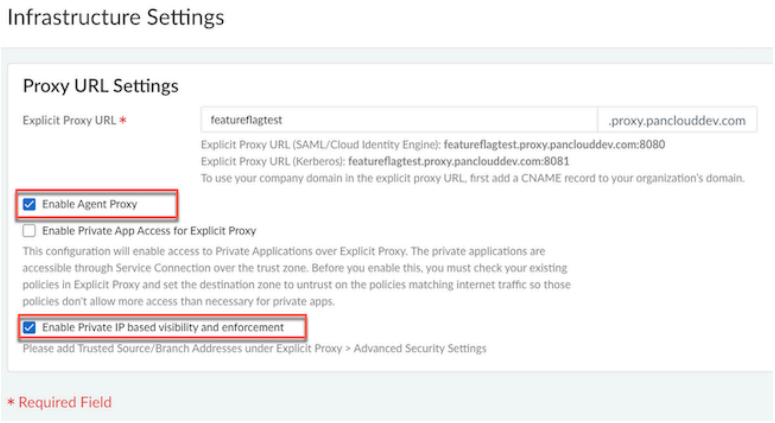
エージェント ベースのプロキシ トラフィックに対するプライベートIPアドレスの可視化と適用 (Strata Cloud Manager)

STEP 1 | モバイル ユーザー向けにエージェントベースのプロキシ機能 (プロキシ モードまたは トンネルとプロキシ モード) を有効にします。

STEP 2 | [ワークフロー] > [Prisma Access セットアップ] > [明示的なプロキシ] > [高度なセキュリティ設定]に移動し、設定アイコンをクリックします。[信頼できるソース アドレス]の下に、ブランチの出口IPアドレスを追加します。



STEP 3 | [ワークフロー] > [Prisma Access セットアップ] > [明示的なプロキシ] > [インフラストラクチャ設定]へ移動します。[プロキシURL設定]で、[ソースIPベースの可視性と適用を有効にする]を有効にし、[保存]をクリックします。



STEP 4 | (オプション) エンドポイントの送信元IPアドレスを使用してセキュリティ ルールを構成します。

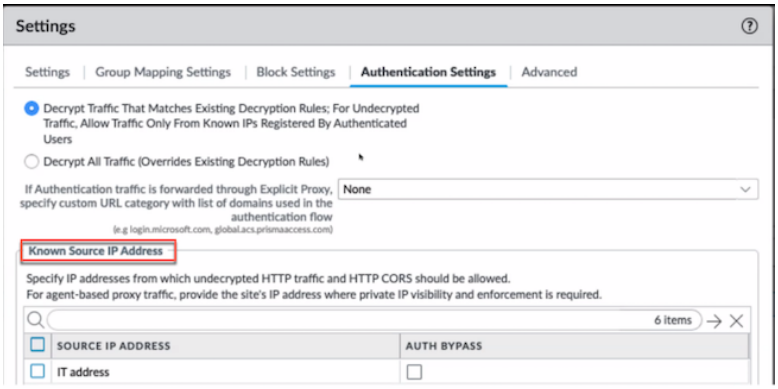
STEP 5 | 明示的なプロキシに設定をプッシュします 。

エージェント ベースのプロキシ トラフィックに対するプライベートIPアドレスの可視化と適用 (Panorama)

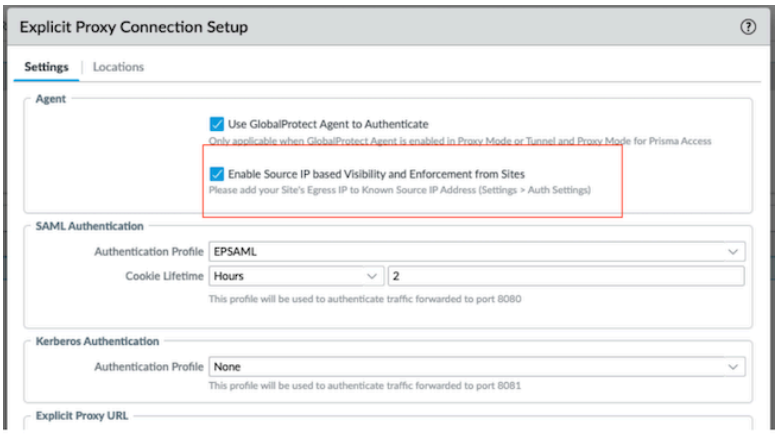
STEP 1 | モバイル ユーザー向けにエージェントベースのプロキシ機能 (プロキシ モードおよびトンネルとプロキシ モード) を有効にします。

©2025 Palo Alto Networks, Inc.

STEP 2 | [クラウド サービス] > [構成] > [モバイル ユーザー] > [明示的なプロキシ > 設定] > [認証設定]に移動し、[既知のソース**IP**アドレス]の下にブランチの出口IPアドレスを追加します。



STEP 3 | [クラウド サービス] > [構成] > [モバイル ユーザー - 明示的なプロキシ]に移動します。[エージェント]の下で、[サイトからのソース**IP**ベースの可視性と適用を有効にする]を有効にし、**[OK]**をクリックします。



STEP 4 | (オプション) エンドポイントの送信元IPアドレスを使用してセキュリティ ルールを構成します。

STEP 5 | コミットして**Explicit_Proxy_Device_Group**にプッシュします。

明示型プロキシのSAML認証

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

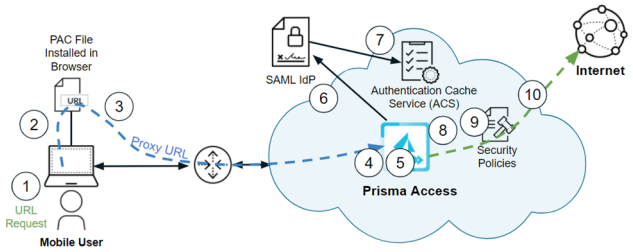
SAMLを使用した明示型プロキシのしくみと設定方法について説明します。

- SAMLを使用した明示型プロキシによるトラフィックの処理方法
- SAMLを使用した明示型プロキシの設定

©2025 Palo Alto Networks, Inc.

SAMLを使用した明示型プロキシによるトラフィックの処理方法

SAML を使用した明示型プロキシの仕組みは次のとおりです。トラフィックがたどるパスを確認するために、一緒に見ていきます。



STEP 1 | モバイルユーザーは、Webブラウザを使用してURLまたはIPアドレスを入力して、インターネットを参照するか、SaaSアプリケーションにアクセスします。

STEP 2 | モバイル ユーザーのエンドポイント上のブラウザーは、PACファイルをチェックします。

このPACファイルは、URLまたはSaaSリクエストが明示型プロキシに送られることを指定します。

STEP 3 | HTTPSクライアント (モバイル ユーザーのエンドポイント上のブラウザー) は、URL要求をプロキシURLに転送します。

STEP 4 | トラフィックは明示型プロキシにリダイレクトされ、プロキシはトラフィックを復号化します。

STEP 5 | プロキシはトラフィックを検査し、Prisma Access明示型プロキシが設定した認証クッキーを確認します。

このCookieには、モバイルユーザーを識別する情報が含まれており、そのCookieを使用してユーザーを認証します。

STEP 6 | もし、クッキーの検査の結果、 Prisma Accessはユーザーが認証されていないと判断した場合、認証のためにユーザーをリダイレクトします。

STEP 7 | IdPがユーザーを認証すると、Prisma Accessはユーザーの認証状態を認証キャッシュ サービス (ACS) に保存します。認証の有効期間は、 **Cookie**の有効期間 明示型プロキシ構成時に指定する値。

STEP 8 | 明示型プロキシは、Cookieの存在と有効性を確認します。Cookieが存在しないか無効な場合、ユーザーはACSにリダイレクトされます。ACSがユーザーの認証を確認した後、ユーザーはトークンを使用して明示型プロキシにリダイレクトされます。その後、プロキシはそのトークンを検証し、そのユーザーのそのドメインの Cookie を設定します。

STEP 9 | Prisma Access は、管理者が構成したセキュリティ ポリシールールに基づいてセキュリティ適用を適用します。

STEP 10 | URLがセキュリティ ポリシールールによってブロックされていない場合、Prisma AccessはURLリクエストをインターネットに送信します。

©2025 Palo Alto Networks, Inc.

STEP 11 | (任意) [Explicit Proxy Connectivity in GlobalProtect for Always-On Internet Security (lobalProtectの明示型プロキシ接続による常時接続のインターネットセキュリティ)]を設定します。この機能を有効にすると、インターネットトラフィックの常時接続セキュリティを実現すると同時に、GlobalProtectまたはサードパーティのVPNを介してプライベートアプリへのオンデマンドアクセスを提供できます。

SAMLを使用した明示型プロキシの設定

次の手順に従って、SAML認証を使用して明示型プロキシを構成します。

- Strata Cloud Manager
- Panorama

SAMLを使用した明示的なプロキシの設定 (Strata Cloud Manager)

STEP 1 | 明示型プロキシを有効にしますセットアップします。

STEP 2 | (任意) 明示型プロキシ用にCloud Identity Engine認証を設定します。

STEP 3 | セキュリティ ポリシー ルールを設定します。

1. **[Manage (管理)] > [Configuration (構成)] > [(NGFWとPrisma Access)] > Configuration (構成)]**を選択します。明示型プロキシ > セキュリティサービス > セキュリティ ポリシー。
2. あなたのニーズとインターネットゲートウェイのセキュリティ ポリシーのベストプラクティスに従って、デフォルトのポリシールールをカスタマイズします。

   *Prisma Access 5.1とPAN-OS 10.2.10またはそれ以降のバージョンのデータプレーンでは、セキュリティ ポリシー ルール「**Allow Web Access to Known Users** (既知のユーザーにウェブアクセスを許可する)」のみが必要です。*

STEP 4 | 設定変更をプッシュします。

SAMLを使用した明示型プロキシの設定（Panorama）

STEP 1 | 明示型プロキシを有効にしますセットアップします。

STEP 2 | (任意) 明示型プロキシ用の認証Cloud Identity Engineを設定します。

STEP 3 | お使いのPrisma Accessバージョンとデータプレーンのバージョンに応じて、単一のポリシー ルールまたは複数のポリシールールを設定します。

バージョン要件	設定
Prisma Access5.1 またはそれ以降のバージョン、及びPAN-OS 10.2.10またはそれ以降のバージョンのデータプレーン。	認証前のユーザートラフィックのためのセキュリティ ポリシー ルールを構成します。 1. **Explicit_Proxy_Device_Group**を選択してください。

©2025 Palo Alto Networks, Inc.

バージョン要件	設定
	2. **Web App**タグを使用したアプリケーション フィルタを作成します。 3. **[Policies**（ポリシー）**] > [Pre Rules (**事前ルール**)] > [**追加**]**を選択します。 4. ルールを作成する。 1. ルールを追加します。 2. 分かりやすい名前を付けてください。 例えば、**`allow-pre-auth`** 3. アプリケーションタブの下に、**Web**アプリケーションアプリケーション フィルターを追加します。 4. ソースタブの下で、既知のユーザーを追加します。
すべての他のPrisma Accessとデータプレーンバージョン。	あなたのニーズとインターネットゲートウェイのセキュリティポリシーのベストプラクティスに従って、セキュリティ ポリシー ルールを構成します。

STEP 4 | 設定を **Commit**（コミット）します。

明示型プロキシのセットアップ

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) Prisma Access環境の明示型プロキシでプライベート ソースIPベースの可視性と適用を有効にする場合は、アカウント チームに連絡して詳細を確認してください。	• Prisma Accessライセンス

明示型プロキシを使用して、ブラウザトラフィックを Prisma Accessへリダイレクトすることでモバイルユーザーを保護します。

オンボーディング ガイドライン- 明示型プロキシ デプロイメントのライセンスを取得してオンボーディングする場合は、次のガイドラインに従います。

- 明示型プロキシは、すべてのPrisma Accessロケーションのサブセットをサポートしています。

©2025 Palo Alto Networks, Inc.

- 2つのアスタリスクで示される場所は追加できません。これらはローカルゾーンであり、Prisma Accessでサポートされていません。
- Prisma Access for Users のローカルまたは評価版ライセンスがあり、Mobile Users-GlobalProtectデプロイメントと Mobile Users-Explicit Proxyデプロイメントがある場合、それぞれ最大 5 つのロケーションにデプロイできます（Mobile Users-GlobalProtect では最大 5 つ、Mobile Users-Explicit Proxy では最大 5 つ）。Worldwide(ワールドワイド)ライセンスをお持ちの場合、場所の最大数に制限はありません。
- 明示型プロキシは、以下の条件でマルチテナントをサポートします。既存の Prisma Access 非マルチテナント デプロイメントをマルチテナント デプロイメントに変換する場合、最初のテナント (移行したテナント) のみが明示的プロキシをサポートします。最初のテナントの後にマルチテナント デプロイメント用に作成する後続のテナントは、明示型プロキシをサポートしません。
- 明示型プロキシ展開をオンボードする場合、Palo Alto Networks では、すべての構成を 1 つのブラウザで実行することをお勧めします。ただし、複数のブラウザまたはブラウザ セッションからセキュリティ ポリシーを追加できます。
- 続行 または オーバーライド の URLフィルタリング アクションはサポートされておらず、明示型プロキシでは機能しません。

明示型プロキシを設定する方法を学びます。

- Strata Cloud Manager
- Panorama

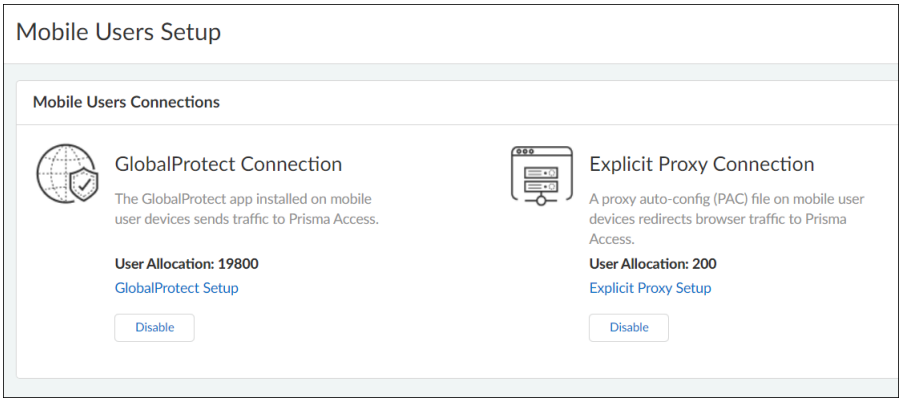
Cloud Management

モバイル ユーザの明示的なプロキシ接続を設定します。明示的なプロキシを使用すると、モバイル ユーザー デバイス上のプロキシ自動設定（PAC）ファイルがブラウザのトラフィックをPrisma Accessにリダイレクトします。

始める前に、明示型プロキシのガイドラインを確認してください。

STEP 1 | 明示型プロキシを有効にし、ユーザーを割り当てる

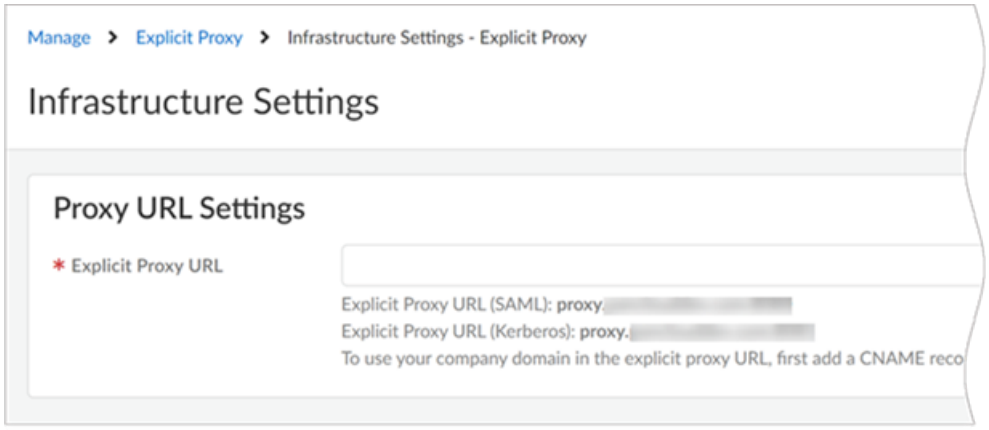
[Workflows (ワークフロー)] > [Prisma Access Setup (セットアップ)] > [Mobile Users (モバイルユーザー)]に移動して、明示的なプロキシの設定を開始します。明示型プロキシを有効にすると、この接続タイプを使用するモバイルユーザーの数を指定するよう求められます。



 ©2025 Palo Alto Networks, Inc.

STEP 2 | モバイルユーザーが**Prisma Access**への接続に使用するプロキシ設定を追加します

インフラストラクチャ設定を編集します 。



1. 明示型プロキシURLを指定します。

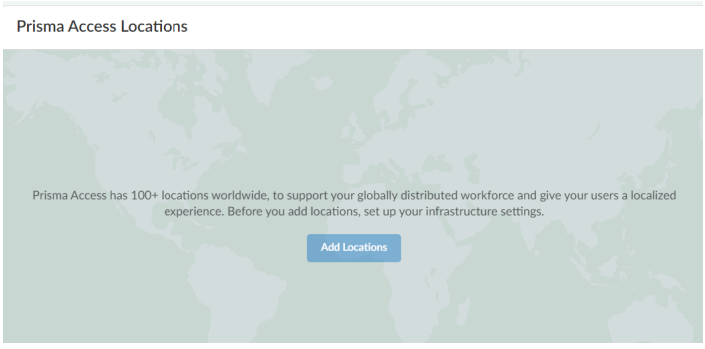
   デフォルトでは、名前は*proxyname*.proxy.prismaaccess.comです。*proxyname*は指定したサブドメインで、ポート8080を使用します。明示型プロキシ URL で会社のドメインを使用するには、CNAMEレコードを組織のドメインに追加します。

   SAMLまたはKerberos認証タイプを使用してモバイルユーザーを認証できます。
2. (任意) [エージェントプロキシを有効にする]を選択して、エージェントベースのプロキシ機能を有効にします。

   プロキシモードまたはトンネルとプロキシモードで明示型プロキシを設定するには、この機能を有効にします。
3. 転送ルールを使用して、要件を満たす PAC ファイルを作成したり、独自の PAC ファイルを転送プロファイルにアップロードしたりできます。

STEP 3 | モバイルユーザーが接続する**Prisma Access**場所を選択する

モバイルユーザーをサポートするPrisma Accessロケーションを追加します。



マップにのPrisma Accessロケーションが表示されます。

場所の数を制限する場合、最適なユーザー エクスペリエンスを実現するために、ユーザーに最も近い場所、またはユーザーと同じ国にある場所を選択してください。モバイル ユーザー

©2025 Palo Alto Networks, Inc.

が居住する国で場所が利用できない場合は、最高のパフォーマンスを得るために、ユーザーに最も近い場所を選択してください。

地域の冗長性を確保するためには、少なくとも2つの地域で明示的なプロキシ ロケーションを有効にする必要があります。

STEP 4 | モバイルユーザーを認証します。

正当なユーザーのみがサービスやアプリケーションにアクセスできるように、ユーザー認証をセットアップします。

サポートされている認証プロトコルはSAMLとKerberosです。 Prisma AccessはSAML認証プロバイダとしてPingOne、Azure AD、Oktaをサポートしていますが、SAML IDプロバイダ（IdP）としてSAML 2.0をサポートしているベンダーであれば、どれでも使用できます。モバイルユーザーがPrisma Accessに対して認証できるようにする方法の詳細をご確認ください。

STEP 5 | デフォルトでオンになっているベストプラクティスのセキュリティルールを確認する

Prisma Accessは、デフォルトでベストプラクティスセキュリティ ポリシー ルールを適用します。これらの規則により、ユーザーは一般のインターネットサイトを安全に閲覧できます。ユーザー：

- URLに基づいて既知の不正なウェブサイトへのアクセスをブロック
- 悪意のあることがわかっているファイルのアップロードやダウンロードをブロック
- 未知の未知の脅威から保護
- ウイルス、スパイウェア（コマンド/コントロール攻撃）、脆弱性から保護

初期設定を行った後に、これらのデフォルトルールを確認して更新し、企業のニーズを満たすことができます。

STEP 6 | モバイルユーザのロケーションがアクティブであることを確認します。

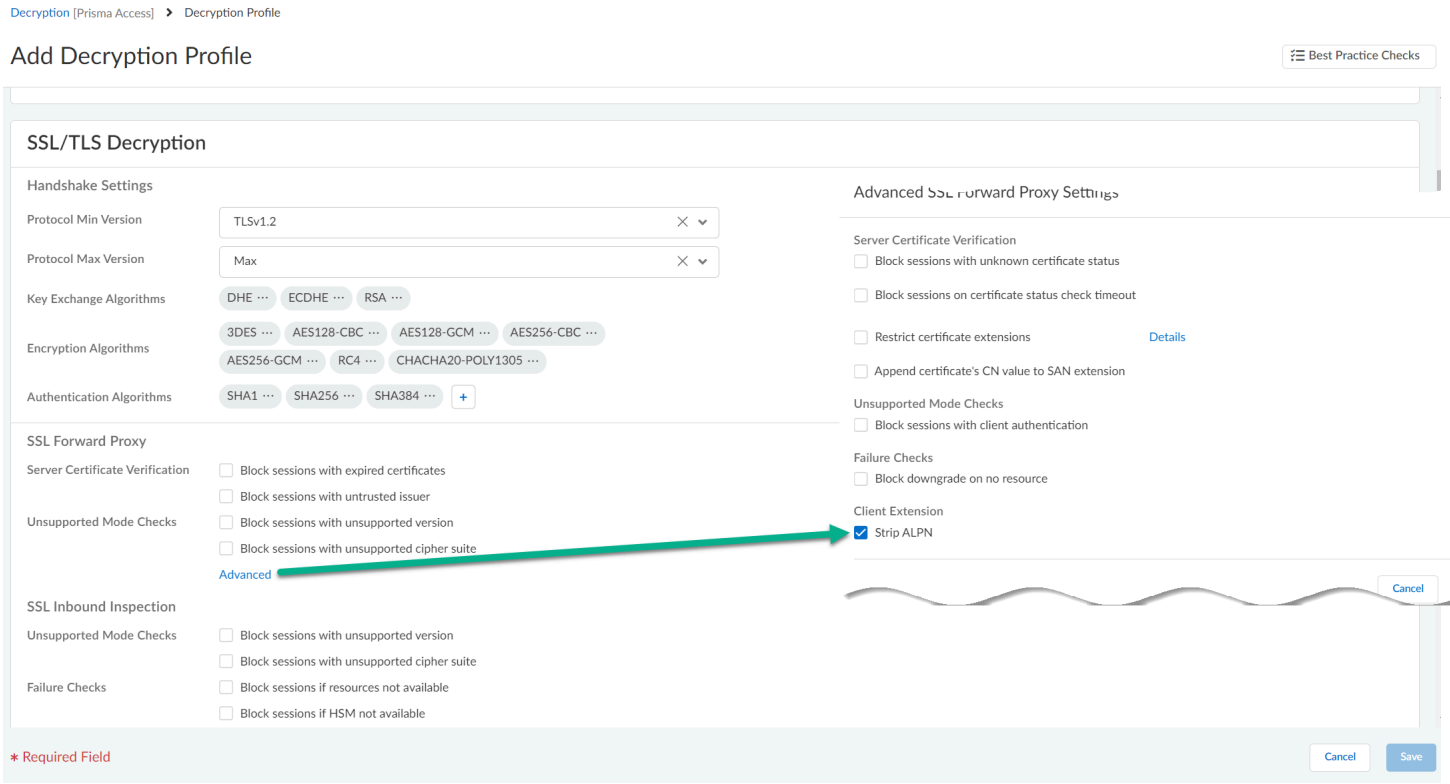
初期設定をPrisma Accessにプッシュすると、Prisma Accessはモバイル ユーザー環境のプロビジョニングを開始する。これには最大15分かかる場合があります。モバイルユーザーのロケーションを設定すると、モバイルユーザーのセットアップ ページ、概要ページ、インサイト内で確認できるようになります。

***[Manage** (管理)] > [**Service Setup** (サービスのセットアップ)] > [**Mobile Users** (モバイルユーザー)]*を選択し、*[*インフラストラクチャ設定*]*を編集して、プロビジョニングした各ロケーションにゲートウェイが設定されていることを確認することで、セットアップを検証することもできます。

©2025 Palo Alto Networks, Inc.

STEP 7 | 明示型プロキシ トラフィックの復号化を有効にする

- TLSの最大サポートバージョンを1.2に設定します。
- 明示型プロキシはネイティブHTTP/2をサポートしていないため、**Strip ALPN**（SSLフォワード プロキシの詳細設定）を設定し、ALPNヘッダーを削除する必要があります。



STEP 8 | ルートCAをダウンロードし、SSL復号化のためにエンドポイントにインストールします。

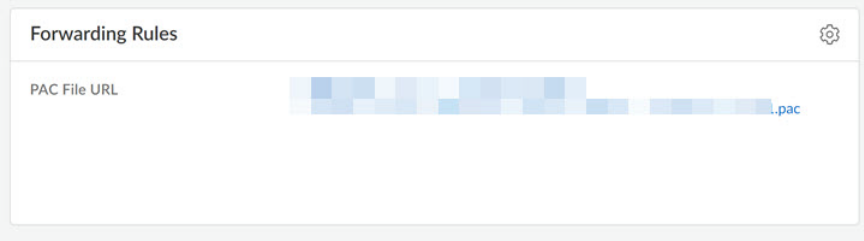
©2025 Palo Alto Networks, Inc.

STEP 9 | **PAC**ファイルの内容を編集します。

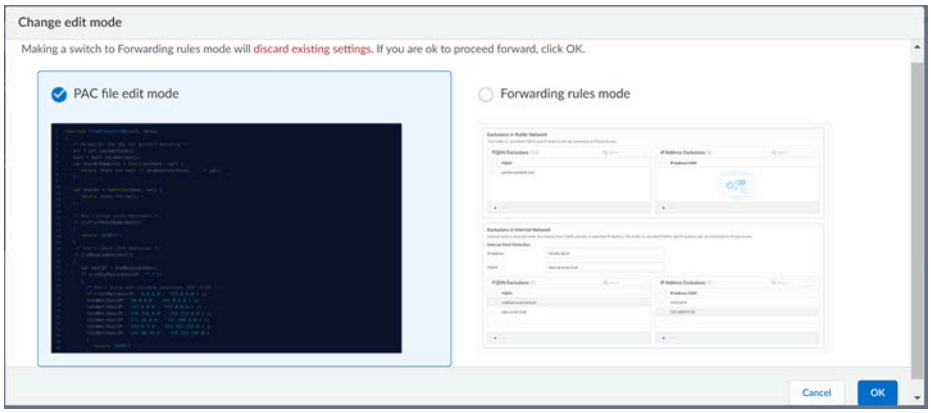
*PAC*ファイルを管理するために転送プロファイルを使用します。

要件を満たす明示的なプロキシ用のプロキシ自動構成(PAC)ファイルを編集します。GlobalProtectアプリケーションは、PACファイルからの転送ルールとロジックに基づいてPrisma Accessへのトラフィックをプロキシします。

転送ルールに移動します。



1. PACファイルをダウンロードし、ニーズに合わせてカスタマイズします。その後、再びここにインポートすると、Prisma AccessがこのPAC ファイルをホストするロケーションの URL が提供されます。
2. **PAC**ファイル エディタ モードまたは転送ルール モードを使用して、PACファイルを編集します。
3. **PAC**ファイルエディタモードはデフォルトで選択されています。PAC ファイル編集モードで編集するには、［**OK**］ をクリックします。
4. 転送ルールモードを選択し、**[OK]**をクリックして転送ルールモードで編集します。転送ルールモードに切り替えると、既存の設定が破棄されます。

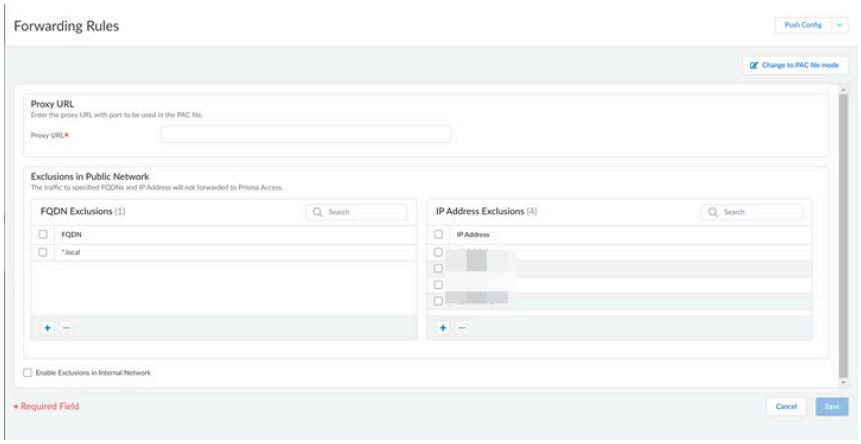


- PAC ファイルで使用するポートとともに明示型プロキシ**URL** を指定します。

  デフォルトでは、名前はproxyname.proxy.prismaaccess.comです。proxynameは指定したサブドメインで、ポート8080を使用します。
- 明示型プロキシモバイルユーザーがパブリックネットワークからPrisma Accessに接続する場合、パブリックネットワークの除外を設定します。
  - **FQDN**除外と**IP**アドレス除外を設定します。除外されたFQDNとIPアドレスはPrisma Accessから転送されません。

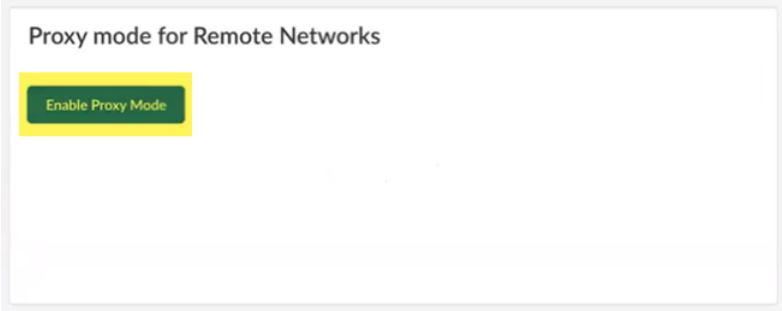
©2025 Palo Alto Networks, Inc.

- ［内部ネットワークの除外］を有効にして、明示的なプロキシモバイルユーザーが内部ネットワーク上のPrisma Accessに接続するときに、特定のIPアドレスまたはFQDNの除外を設定します。
  - ユーザーが内部ネットワーク上にあるときに、異なるトラフィック除外を設定するには、次の除外を指定します。
    - 内部ネットワークからのみ解決できるホストの**IP**アドレスを入力します。
    - が入力したIPアドレスに解決する**FQDN**を入力します。
  - 特定のFQDNとIPアドレスの除外を設定します。指定したFQDNやIPアドレスへのトラフィックはPrisma Accessから転送されません。
- 変更を保存します。



STEP 10 | セキュリティの詳細設定の設定を行います。

- セキュアなIPSecトンネルを介してブランチから明示型プロキシにトラフィックを転送する場合は、プロキシモードを有効にし、明示型プロキシをPrisma Accessリモートネットワークと組み合わせて使用する場合はエニーキャストIPアドレスを取得します。



このソリューションは、リモートネットワークIPSecトンネルでエニーキャストアドレスを使用して、リモートネットワークサイトまたはブランチロケーションのユーザーおよびデバイスに明示プロキシを使用できるようにします。

- プロキシモードデプロイメントのみ プロキシモードがリモートネットワークで有効になっている場合は、リモートネットワーク上のエニーキャストおよびユニキャストIPにバインドされたトラフィックを許可するポリシーを追加します。送信元**IP**の可視性と適用を有効にしている場合は、明示型プロキシのセキュリティ ポリシーの送信元**IP** フィールドを使

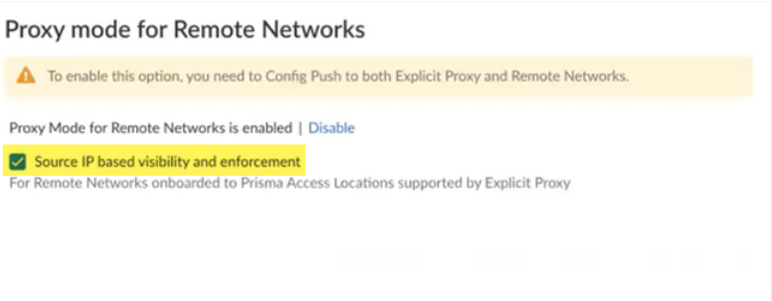
©2025 Palo Alto Networks, Inc.

用してトラフィックを保護します。リモート ネットワークには追加のポリシーが必要です。

- (任意) プロキシモードを有効にする場合、明示型プロキシにトラフィックを転送しているブランチ ロケーションのシステムのプライベートIPアドレスを活用するには、[送信元IPベースの可視性と適用]を選択します。

  この機能には次の要件があります:

  - 最低10.2.4のPrisma Accessデータプレーン
  - 最低4.1のクラウドサービスプラグインを使用したPrisma Access (Managed by Panorama)デプロイメント
  - 送信元IPアドレスは、明示型プロキシでサポートされているリモートネットワークロケーションに対してのみ表示されます。



- ブロックソースを指定します。

  ブロックする必要がある送信元IPアドレスのトラフィックをブロック送信元アドレスリストに追加します。

  アドレス、アドレスグループ、またはEDLを指定します。

  IPアドレスリストエントリを強制適用から除外するには、［例外を追加]をクリックし、ブロックから除外するIPアドレスを選択します。

- 「ブロックドメイン]を指定します。

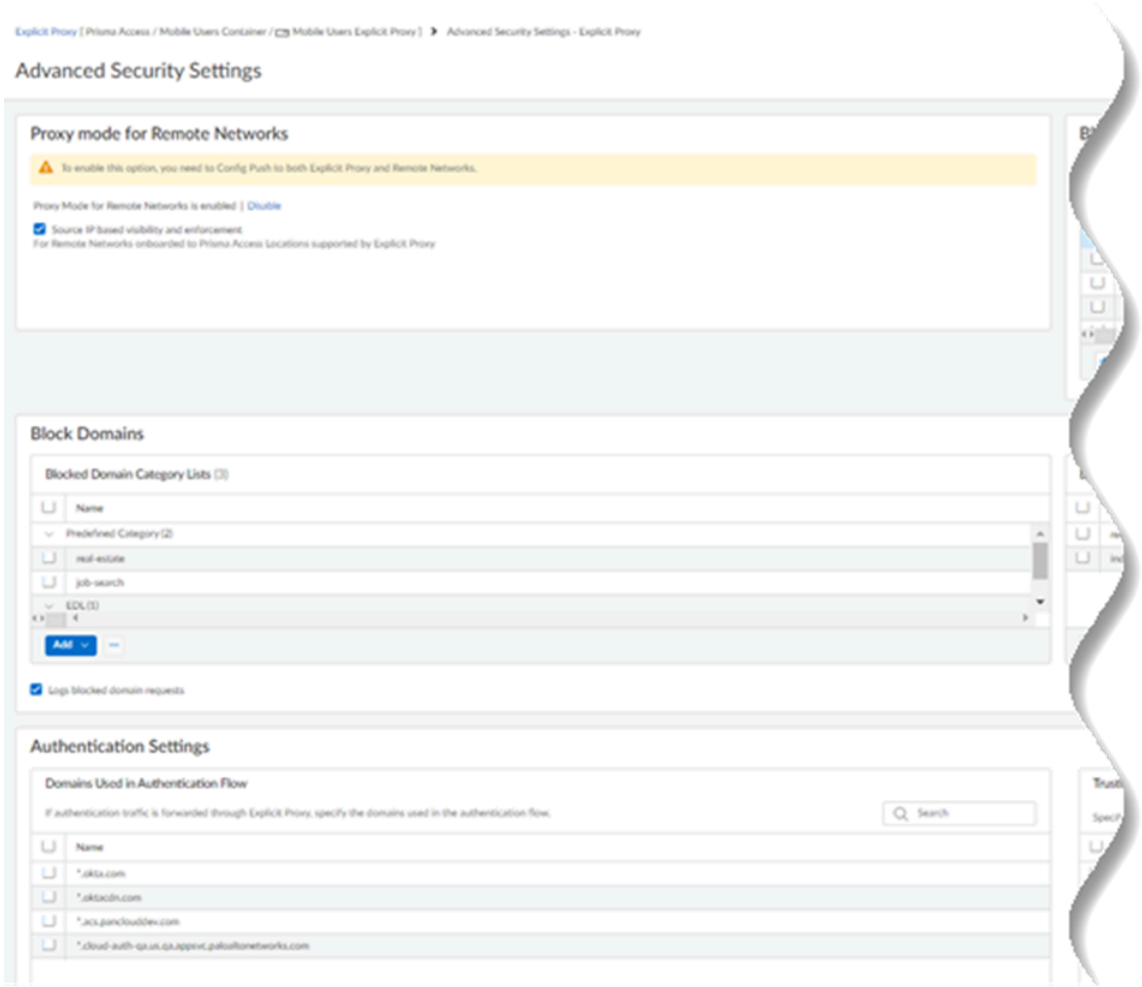
  悪意のあるウェブサイト、またはユーザーにアクセスさせたくないウェブサイトのドメインまたはドメインカテゴリを指定します。Prisma Accessは、ユーザーがHTTP GET（暗号化されていないリクエストの場合）またはHTTP CONNECT（暗号化されたリクエストの場合）を開始するときに、ユーザーがこの領域で指定したURLおよびIPアドレスにアクセ

©2025 Palo Alto Networks, Inc.

スするのを防ぎます。ユーザーがブロックされたウェブサイトにアクセスしようとすると、ブロックページが表示されます。

- ブロックされているドメインカテゴリリストに含まれるドメインを除外する場合は、除外リストでドメインを指定します。

  入力されたドメインは、ブロックしたドメイン カテゴリに表示されていても、ブロックが免除されます。
- 明示型プロキシでは、ユーザーを認証するために復号化が必要です。認証フローで使用するドメインを入力します。
-



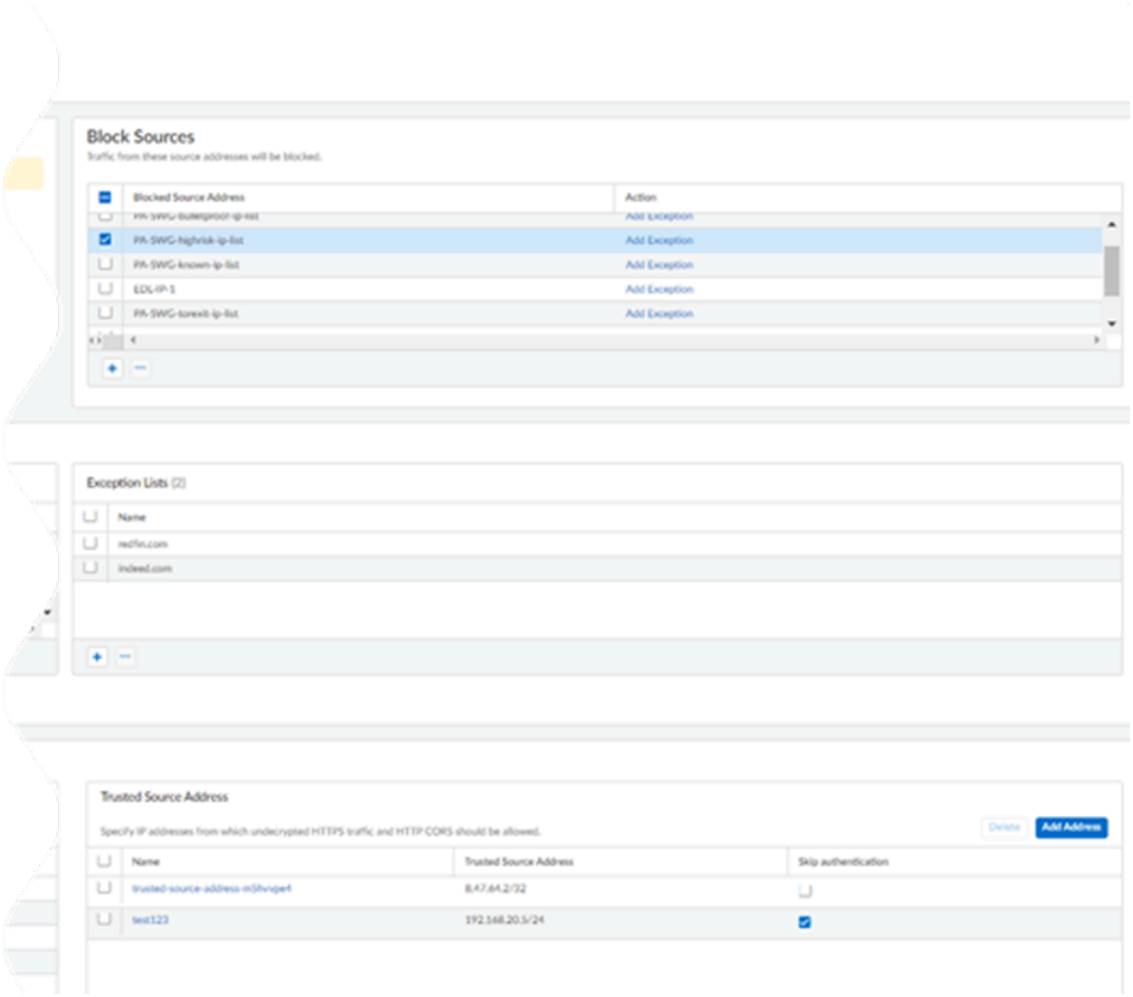
- 復号化されていないHTTPSまたはHTTPクロスオリジンリソース共有（CORS）トラフィックが信頼できる送信元アドレスに対して許可されるIPアドレスを入力します。
- 入力した信頼できる送信元アドレスの認証をバイパスするには、[認証をスキップ]を選択します。

  [送信元IPベース]の可視性と適用で[認証をスキップ]を使用すると、認証できないヘッドレスシステムの認証をスキップし、セキュリティポリシーを設定し、Prisma Access明示型プロキシでトラフィックの可視性を得ることができます。

©2025 Palo Alto Networks, Inc.

*IP*アドレスまたはサブネットのいずれかを追加できます。サブネットの拡張後に最大 *100,000* の *IP* アドレスがサポートされます。

アドレス オブジェクトの認証をスキップするために**[Skip authentication (認証をスキップ)]**を選択し、後でそのアドレス オブジェクトの**[Skip authentication (認証をスキップ)]**の選択を解除して認証を有効にする場合、変更を行ってから変更をコミットおよびプッシュして変更が有効になるまで最大24時間かかることがあります。

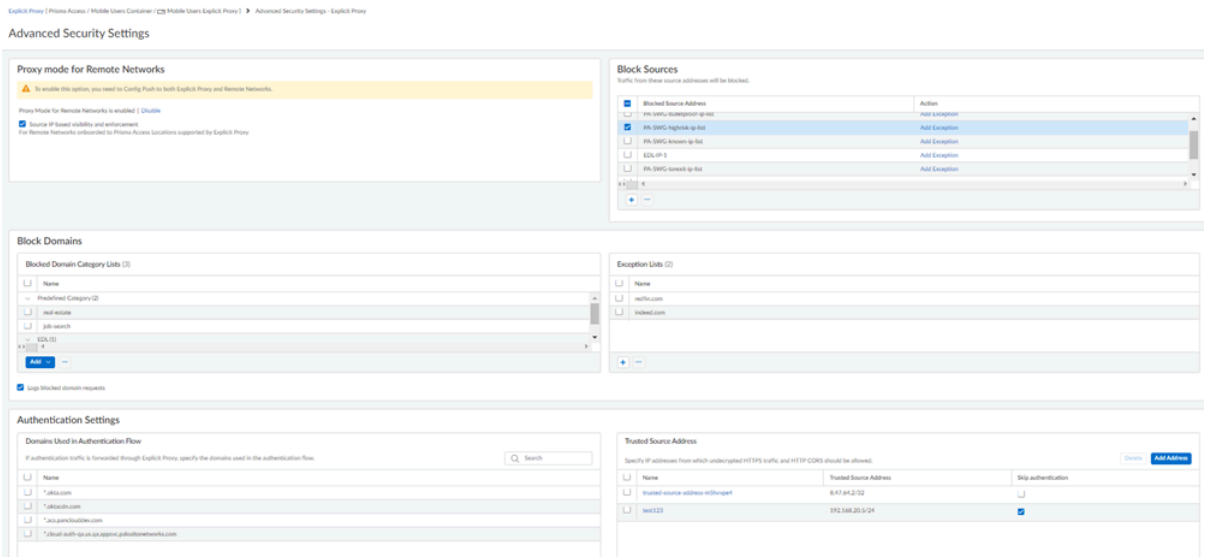
- 

- 明示型プロキシ デプロイメントがあり、信頼できる送信元 IP アドレスのリストが追加されている場合は、着信 HTTP/HTTPS 要求の **X-Authenticated-User**（XAU）ヘッダーを使

©2025 Palo Alto Networks, Inc.

用して識別できます。この機能を使用して、認証にXAUヘッダーを使用する別のプロキシからログインしているユーザーを許可します。

*XAU*設定を有効にするには、［保存］をクリックする必要があります。



明示型プロキシのセットアップ (Panorama)

明示型プロキシを使用してモバイル ユーザーを保護するには、次の手順を実行します。

明示型プロキシを構成する前に、計画チェックリスト を確認して、明示型プロキシ PAC ファイルの設定方法を学習してください。

©2025 Palo Alto Networks, Inc.

STEP 1 | 明示型プロキシの認証を設定します。

サポートされている認証タイプはSAML と Kerberos です。

IdP および Panorama で SAML 認証を構成するときは、次のガイドラインに従ってください。

- **Panorama**ガイドライン:
  - Prisma Access の **SAML ID** プロバイダー と 認証プロファイルを構成します。後の手順で作成する認証プロファイルを指定します。
  - **Explicit_Proxy_Template**の下で認証プロファイルを必ず設定してください。
  - IdP サーバー プロファイルおよび Panorama の 認証プロファイル で、 メール をユーザー属性として使用します。
  - 明示型プロキシは、SAML アイデンティティ プロバイダー サーバー プロファイルで **IdP** への **SAML** メッセージの署名 をサポートしていません。
  - ユーザーとグループのマッピング情報を取得するように Cloud Identity Engine を構成する場合は、グループ マッピングの **SamAccountName** として **mail** または **userPrincipalName** を使用します。
  - 明示型プロキシ設定中に グループマッピング設定 を構成する場合は、プライマリユーザー名と電子メールに同じディレクトリ属性を使用するか、 Prisma Accessはユーザー数を正確に反映していません。たとえば、次のユーザー プロファイルがあるとします。

    ```
    sAMAccountName: muser Netbios: example userPrincipalName:
     muser@example.com mail: mobile.user@example.com
    ```

    Cloud Identity Engineの設定で、 プライマリユーザー名 に `userPrincipalName`、メール アドレスに `mail`を使用した場合、 Strata Logging Service トラフィック ログに返される情報と、ACS が認証ログに返すユーザー情報は異なります。この例では、ACSは メール 属性（mobile.user@example.com）を認証ログに送信し、 Strata Logging Service は**userPrincipalName** 属性 (muser@example.com) をトラフィック ログに送信します。この不一致の結果、ステータス (**Panorama** > **Cloud Services** > ステータス > ステータス ページ) で明示型プロキシ ステータスを確認するときに、**[**現在のユーザー**]** フィールド と **[**ユーザー **(**過去 **90** 日間**)]** フィールドのユーザー数が正確ではなくなります。このため、 グループ マッピング設定を指定するときは、 プライマリ ユーザー名 と 電子メール に同じディレクトリ属性 (たとえば、**mail**) を使用します。

©2025 Palo Alto Networks, Inc.

- Panoramaを使用してPrisma Accessを管理する場合 Cloud Identity Engineは 、セキュリティ ポリシー ルールにユーザーとグループの情報を自動入力しません。

- **IdP** ガイドライン:
  - SAML を構成するときは、次の URL を使用します。

    SAML アサーション コンシューマー サービス URL:**`https://global.acs.prismaaccess.com/saml/acs`**

    エンティティ **ID**URL:**`https://global.acs.prismaaccess.com/saml/metadata`**
  - Okta を IdP として使用する場合は、 名前 **ID** 形式 の設定に **EmailAddress** を使用します。
  - シングル サインオン URL`https://global.acs.prismaaccess.com/saml/acs`を入力します。
  - シングル ログアウト (SLO) はサポートされていません。
  - IdP 認証の問題をトラブルシューティングするには、IdP の監視およびトラブルシューティング機能を使用します。ACS は IdP 認証の失敗を記録しません。
  - SAML IdP の 認証プロファイル を作成するときに、[詳細] タブで [許可リスト]の すべてを 選択しないと、明示型プロキシはグループ マッピングを取得できなくなります。

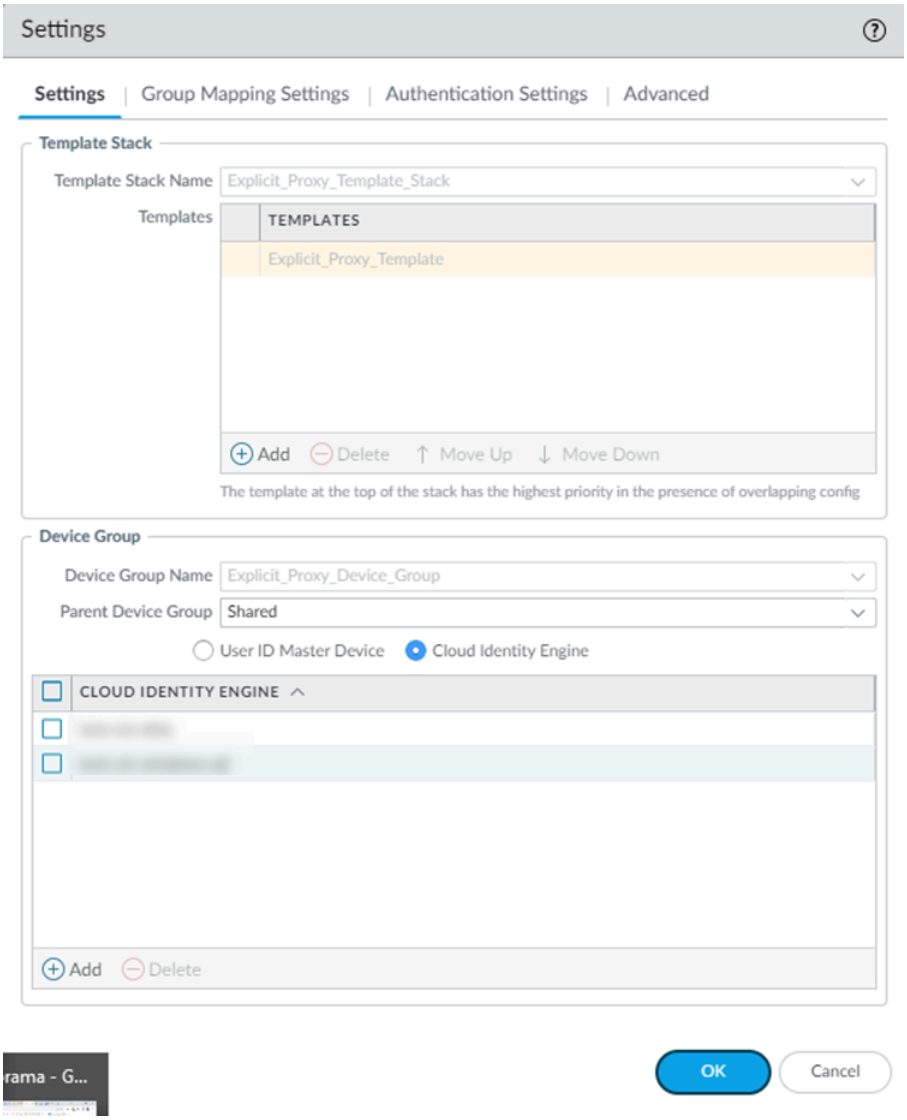
STEP 2 | 明示型プロキシの設定

1. **[Panorama]** > **[Cloud Services (**クラウドサービス**)]** > **[Configuration (**構成**)]** > [モバイルユーザー - 明示型プロキシ] を選択し、歯車アイコンをクリックして明示型プロキシ設定を編集します。
2. [設定] タブで、次の設定を編集します。
   - (任意) テンプレートとテンプレート スタックの名前を確認します。

     デフォルトでは、 Prisma Accessは新しいテンプレート スタック **Explicit_Proxy_Template_Stack** と新しいテンプレート **Explicit_Proxy_Template**を作成します。Panorama で デバイス 設定を作成および編集するときは、必ずこのテンプレートを使用してください。
   - デバイスグループセクションで、明示型プロキシにプッシュするコンフィギュレーション設定を含む親デバイスグループを選択するか、Prisma Accessデバイスグループの共有階層を使用するために親デバイスグループを**Shared (**共有**)**のままにします。デバイス グループ名 は変更できません。
   - (任意) 次世代ファイアウォールをマスターデバイスとして構成した場合、または Cloud Identity Engine プロファイルを追加してセキュリティポリシールールにユーザーおよびグループ情報を入力した場合は、User-ID Master Device または Cloud Identity Engine を選択し、作成したマスターデバイスまたは Cloud Identity Engine プロファイルのいずれかを選択します。

©2025 Palo Alto Networks, Inc.

- [ライセンス割り当て] セクションで、明示型プロキシに割り当てるモバイル ユーザーの数を指定します。



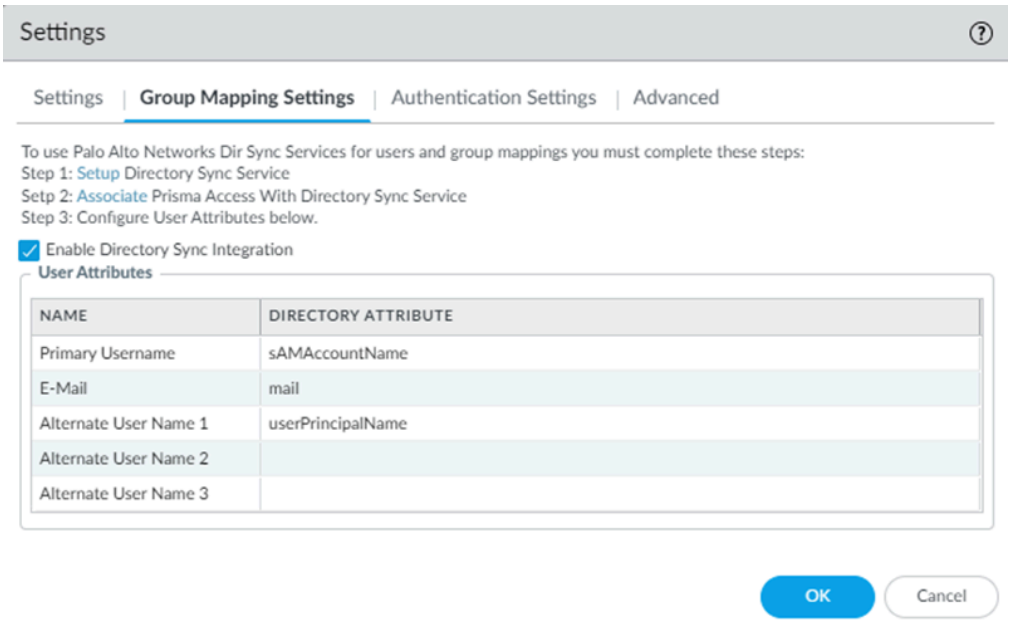
3. **Group Mapping Settings (**グループ マッピング設定**)**タブで、**Enable Directory Sync Integration (**ディレクトリ同期を有効にする**)**現在は「Cloud Identity Engine」と呼ばれ

©2025 Palo Alto Networks, Inc.

る）を選択して、Prisma Accessが Cloud Identity Engine を使用してユーザとグループ情報を取得するように構成します。

Cloud Identity Engine を使用して、明示型プロキシデプロイメントのユーザーとグループマッピング情報を入力します。

プライマリ ユーザー名 フィールドのディレクトリ属性に **mail** と入力し、 電子メール フィールドに **mail** と 入力します。



4. 完了したら **OK** をクリックします。

STEP 3 | (任意) ブロック設定を構成します。

ブロック設定を使用して、DNS 解決段階でインターネットの宛先へのアクセスをブロックします。

明示型プロキシへのアクセスを特定の送信元 *IP* アドレスに制限するには、 特殊なオブジェクトを使用することもできます。特定の名前を使用するこれらのアドレス オブジェクト、アドレス グループ、および外部動的リスト *(EDL)* は、インターネット トラフィックに指定した *IP* アドレスを許可し、その他の *IP* アドレスをブロックします。

STEP 4 | [認証設定] タブで、復号化、X-Authenticated-User (XAU)、および認証設定を構成します。

1. 復号化されたトラフィックの設定を構成します。
   - **[Decrypt Traffic That Matches Existing Decryption rules; For Undecrypted Traffic, Allow Traffic Only From Known IPs Registered By Authenticated Users** (既存の復号化ルールに一致するトラフィックを復号化し、復号化されていないトラフィックに

©2025 Palo Alto Networks, Inc.

ついては、認証されたユーザーによって登録された既知の**IP**からのトラフィックのみを許可する**)]**を選択して、以下の復号化ルールを設定します：

- 復号化 または 復号化して転送するアクション で設定した復号化ポリシー ルールに一致するトラフィックは復号化されます。

  ユーザーが復号化されていない HTTPS サイトにアクセスし、その IP アドレスから明示型プロキシにまだ認証されていない場合、そのユーザーはブロックされます。ただし、ユーザーは復号化されたサイトにアクセスし、認証を完了してから、復号化されていないサイトにアクセスすることはできます。
- モバイル ユーザーがすでに認証されている IP アドレスからの暗号化されていないトラフィックは許可されます。

明示型プロキシでは、ユーザーを認証するために復号化が必要です。カスタム URL カテゴリで復号化できるドメインを入力し、それらのカテゴリを 「認証トラフィックが明示型プロキシ経由で転送される場合は、認証フローで使用されるドメインを指定します」で指定します。

すべての *ACS* および *IdP FQDN* を含め、認証に必要なドメインのみを、指定したカスタム *URL* カテゴリに追加します。認証 *URL* を復号化ポリシーに追加した場合でも、カスタム *URL* カテゴリに追加する必要があります。

©2025 Palo Alto Networks, Inc.

- すべてのトラフィックの復号化を許可するには、**[すべてのトラフィックを復号化(既存の復号化ルールを上書き)]**を選択します。

  このラジオ ボタンを選択する場合は、次の点を確認してください。

  - 復号化ポリシーに例外はありません。
  - セキュリティ ポリシーで送信元 IP アドレス ベースの制限を適用しています。

  これらの推奨事項に従わないと、明示型プロキシがオープン プロキシとして悪用され、サービス拒否攻撃を実行するための転送サービスとして広く悪用される可能性があります。

- 少なくとも 1 つの SSL フォワード プロキシ証明書が フォワード信頼証明書として指定されています。

  転送信頼証明書がない場合は、Panoramaで作成し、変更を Prisma Accessにコミットしてプッシュします。転送信頼証明書がないと、明示型プロキシの変更をコミットするときにコミット エラーが発生します。

2. (任意) 暗号化されていないHTTPまたはHTTP Cross-Origin Resource Sharing (CORS)トラフィックが**Trusted Source Address Auth Bypass (**信頼できる送信元アドレス認証バイパス**)**に許可されるべきIPアドレスを入力します。

   IPアドレスをIPアドレスベースのアドレスオブジェクトに追加し、 フィールド内の Address オブジェクトを追加します。

   最大100,000 個のアドレスを入力します。アドレスオブジェクトがIPアドレスのみを使用していることを確認してください。

3. (任意) 入力した信頼できる送信元アドレスの認証をバイパスするには、 **Auth Bypass (**認証バイパス**)**を選択します。

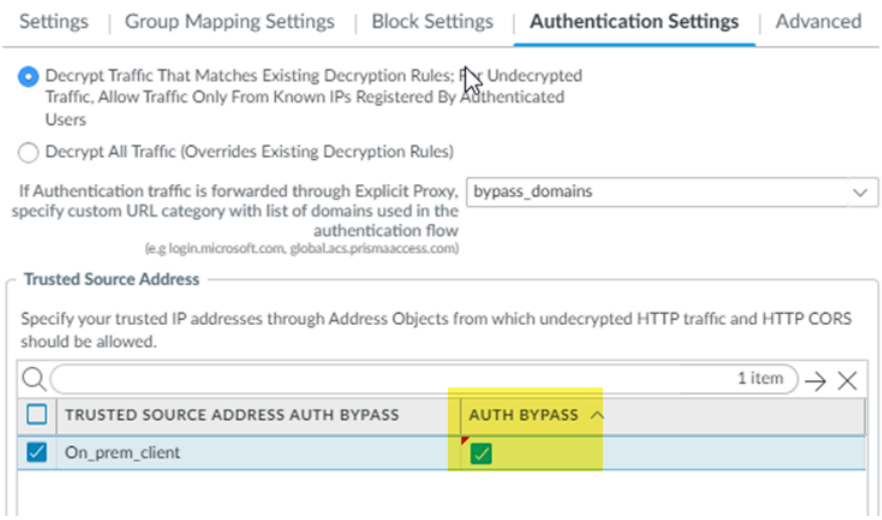
   ソース**IP**ベースの可視性と強制による**Auth Bypass (**認証バイパス**)** を使用すると、認証できないヘッドレスシステムの認証をスキップし、セキュリティポリシーを設定し、明示型プロキシのトラフィックの可視性を得ることができます。

   *IP*アドレスまたはサブネットのいずれかを追加できます。サブネットを拡張すると、最大*100,000*個の*IP*アドレスがサポートされます。

   アドレス オブジェクトの認証をスキップするために **Auth Bypass** を選択し、その後そのアドレス オブジェクトの **Auth Bypass** の選択を解除して認証を有効にする場合、変

©2025 Palo Alto Networks, Inc.

更を加えて変更をコミットおよびプッシュしてから変更が有効になるまでに最大 24 時間かかることがあります。



4. (任意) 信頼できるソース アドレス IP アドレスが ID に XAU を使用できるようにするには、**[ID** に着信 **HTTP/HTTPS** 要求で **X-Authenticated-User (XAU)** ヘッダーを使用する**]**を選択します。

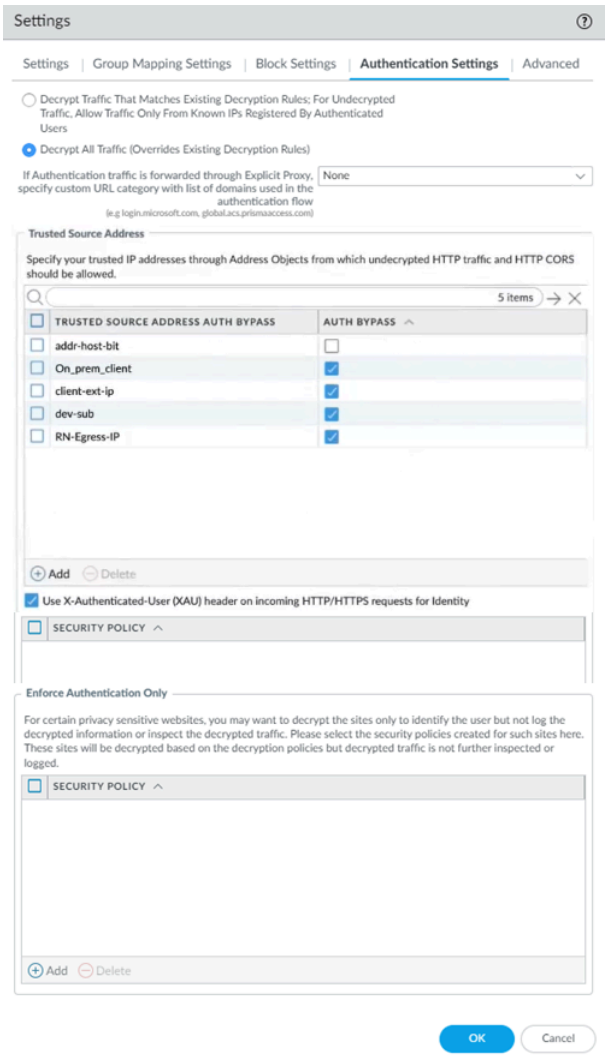
   サードパーティのプロキシから明示型プロキシへのプロキシ チェーンを使用しており、ユーザーがそのプロキシで認証されており、プロキシが XAU ヘッダーを使用している場合は、このオプションを選択します。

   XAU ヘッダーは、明示型プロキシ ヘッダーの取り込みでサポートされる唯一の HTTP ヘッダーです。X-Forwarded-For (XFF) ヘッダーはサポートされていません。

5. (任意) プライバシーに配慮した Web サイトの設定を指定するには、それらのサイトのセキュリティ ポリシー ルールを作成し、**[**認証のみを強制**]** 領域でそれらのサイトの セキュリティ ポリシーを指定します。

   セキュリティ ポリシー または追加したポリシーで指定した Web サイトの場合、明示型プロキシは復号化ポリシーに基づいて Web サイトを復号化しますが、復号化されたトラフィックを検査したりログに記録したりすることはありません。

©2025 Palo Alto Networks, Inc.



©2025 Palo Alto Networks, Inc.

STEP 5 | (任意) 詳細 設定を構成します。

1. セキュアなIPSecトンネルを介してブランチから明示型プロキシにトラフィックを転送する場合は、プロキシモードを有効にし、明示型プロキシをPrisma Accessリモートネットワークと組み合わせて使用する場合はエニーキャストIPアドレスを取得します。

   このソリューションは、リモートネットワークIPSecトンネルでエニーキャストアドレスを使用して、リモートネットワークサイトまたはブランチロケーションのユーザーおよびデバイスに明示プロキシを使用できるようにします。

2. (任意) 明示型プロキシにトラフィックを転送しているブランチ ロケーションのシステムのプライベートIPアドレスを活用するには、**[送信元IP**ベースの可視性と適用]を選択します。

   この機能には次の要件があります:

   - 最低限 Prisma Access 10.2.4
   - のデータプレーン 最小の Cloud Services プラグイン 4.1 を使用したPrisma Access (Managed by Panorama)デプロイメント
   - リモート ネットワーク - 明示型プロキシ デプロイメント を構成した後、ソース IP アドレスはリモート ネットワークからの IP アドレスに対してのみ表示され、 明示型プロキシでサポートされているリモート ネットワークの場所のソース アドレスのみが表示されます。

3. プロキシモードデプロイメントのみ プロキシモードがリモートネットワークで有効になっている場合は、リモートネットワーク上のエニーキャストおよびユニキャストIPにバインドされたトラフィックを許可するポリシーを追加します。送信元**IP**の可視性と適用を有効にしている場合は、明示型プロキシのセキュリティ ポリシーの送信元**IP** フィールドを使用してトラフィックを保護します。リモート ネットワークには追加のポリシーが必要です。

4. **OK** をクリックします。

STEP 6 | 明示型プロキシ設定を構成するには、**[Configure (構成)]** をクリックします。

1. 明示型プロキシ **FQDN**を指定します。

   デフォルトでは、名前は*proxyname*.proxy.prismaaccess.comです。*proxyname*は指定したサブドメインで、ポート8080を使用します。明示型プロキシ URL で組織のドメイン名 (thisproxy.proxy.mycompany.com など) を使用する場合は、組織のドメインの CNAME レコードを入力します。

   たとえば、thisproxy.prismaaccess.com という名前のプロキシ URL を thisproxy.proxy.mycompany.com という名前のプロキシにマップするには、組織のド

 ©2025 Palo Alto Networks, Inc.

メインの CNAME レコードに thisproxy.proxy.prismaaccess.com の CNAME を追加します。

2. (任意) エージェントベースのプロキシ機能を有効にするには、**[GlobalProtect** エージェントを使用して認証する**]** を選択します。

   プロキシモードまたはトンネルとプロキシモードで明示型プロキシを設定するには、この機能を有効にします。ソース **IP** ベースの可視性と適用を有効にするには、このチェック ボックスもオンにする必要があります。

3. 認証プロファイル と **Cookie** の有効期間を指定します。

   - ステップ 1で使用したSAML 認証プロファイル を指定するか、Prisma Accessで使用する新しい 認証プロファイルを追加します。

     明示型プロキシを使用するには、**SAML** アイデンティティ プロバイダー (IdP) と 認証プロファイルの構成を含む SAML 認証を構成する必要があります。

   - (任意) ユーザーの認証資格情報を保存する **Cookie** の有効期間 を指定します。

     Prisma Access はユーザーの資格情報をキャッシュし、Cookie の形式で保存します。値を変更するには、使用する時間の長さを秒、分、時間、または日単位で指定します。

     > クッキーの有効期間が切れる前にユーザーが大きなファイルをダウンロードできない、またはユーザーが *1* つの *Web* サイトに長時間アクセスしているときにクッキーが期限切れになるなどの問題を回避するために、*Palo Alto Networks* ではクッキーの有効期間を少なくとも *1* 日に設定することをお勧めします。明示型プロキシ ユーザーに*Cookie*の有効期限の問題がある場合は、別の*Web*サイトを参照して*ACS*に再認証し、*ACS Cookie*を更新できます。

     ファイルをダウンロードしていて、ファイルのダウンロードに **Cookie** の有効期間よりも長い時間がかかる場合、有効期間の値が期限切れになるとファイルのダウンロードは終了します。このため、ダウンロードに時間のかかる大きなファイルをダウンロードする場合は、**Cookie** の有効期間を 長くすることを検討してください。

STEP 7 | モバイル ユーザー向けの明示型プロキシを展開する 場所 と、それらの場所に関連付けられたリージョンを選択します。 Prisma Accessは選択した各場所にプロキシ ノードを追加します。

明示型プロキシは、すべてのPrisma Accessロケーションのサブセットをサポートしています。場所のリストについては、明示型プロキシの設定ガイドラインをご覧ください。

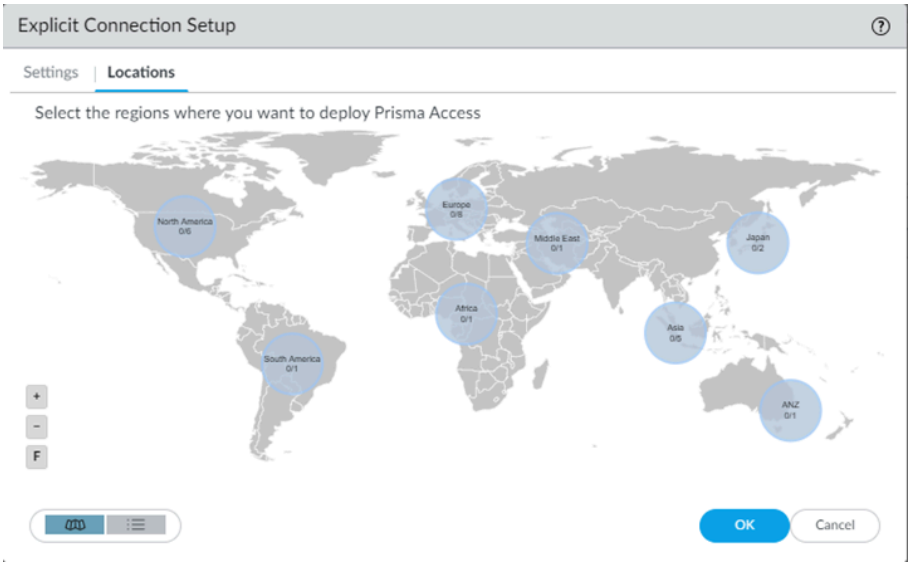
Locations（ロケーション）タブにはマップが表示されます。マップを強調表示すると、グローバルな地域（Americas（アメリカ）、Europe（欧州）、およびAsia Pacific（アジア太平

©2025 Palo Alto Networks, Inc.

洋））および各地域内で利用できるロケーションが表示されます。地域を選択して、次に各地域で展開するロケーションを選択します。

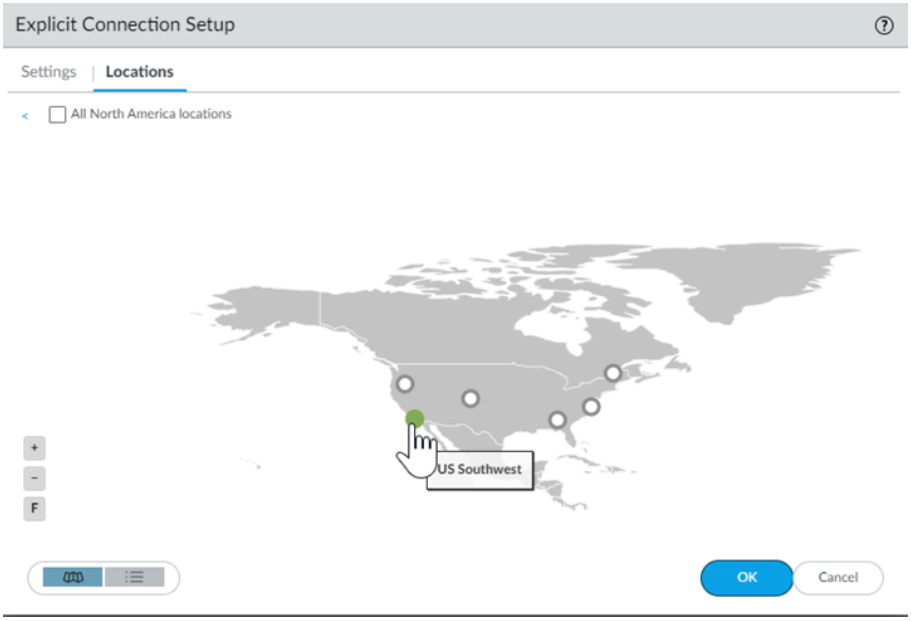
地域の冗長性を確保するためには、少なくとも2つの地域で明示型プロキシ ロケーションを有効にする必要があります。

1. **Locations**（ロケーション）タブをクリックして、リージョンを選択します。



2. マップを使用して、選択した地域内の 1 つ以上の明示型プロキシの場所を選択します。

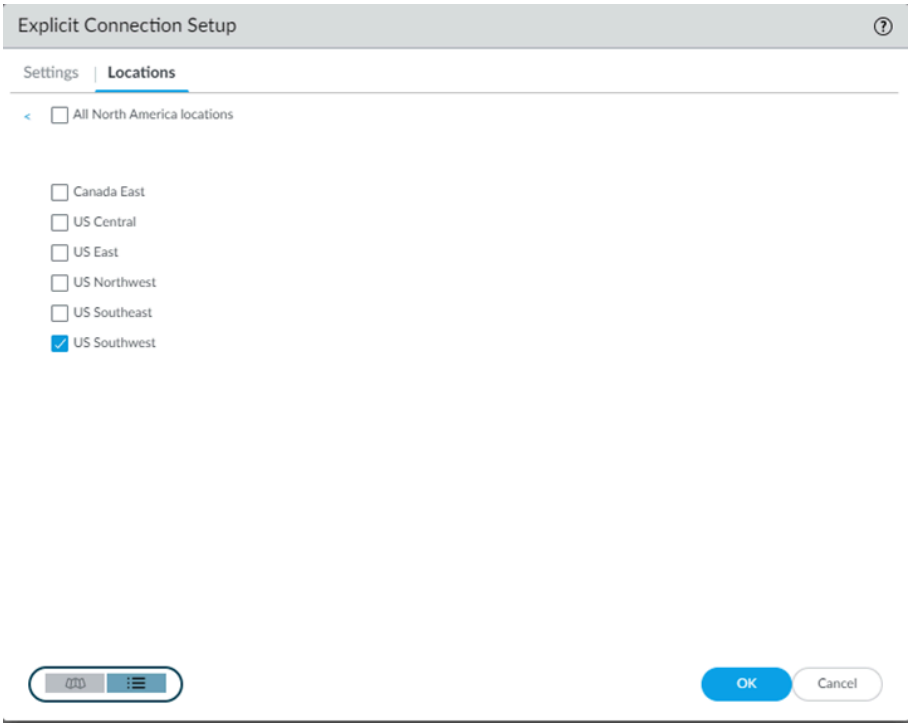
   ロケーション上にカーソルを移動すると、それが強調表示されます。白の円は利用可能なロケーションを、緑の円はそのロケーションが選択されていることを表しています。



   マップビューのほかに、地域とロケーションのリストを表示することができます。左下から、マップビューとリストビューを切り替えられます。リストビューのリストは、地

©2025 Palo Alto Networks, Inc.

域が列でソートされ、すべてのロケーションを地域別にソートされています。リージョン内の**All**（すべて）のサイトを選択できます（ダイアログ上部）。



3. 場所を追加するには、「**OK**」 をクリックします。

STEP 8 | 組織のセキュリティ ポリシーを適用するために、セキュリティ ポリシー ルールを構成します。

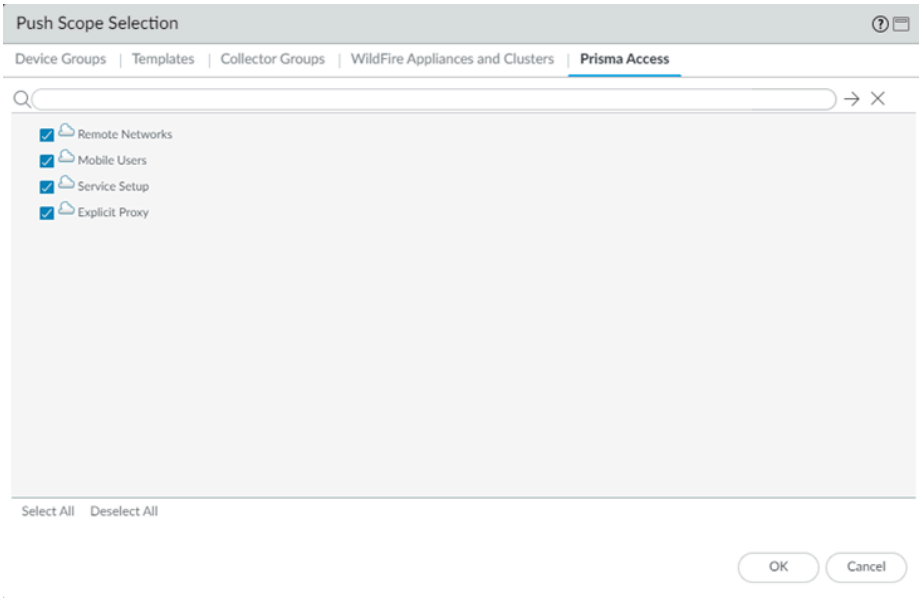
必要な構成変更を行い、モバイル ユーザーが明示型プロキシからアクセスできる URL を制御するには、セキュリティ ポリシーを使用します。セキュリティ ポリシーを構成するときは、次のガイドラインと要件に従ってください。

- ビジネス目標に基づいて、App-ID とそれらのアプリケーションへのアクセスを必要とするユーザー グループを使用して、承認されたインターネットおよび SaaS アプリのセキュリティ ポリシーを作成します。
- セキュリティ プロファイルのベスト プラクティスに従って既知と未知の両方の脅威を防止できるように、すべてのセキュリティ ポリシー ルールにセキュリティ プロファイルを添付します。

©2025 Palo Alto Networks, Inc.

STEP 9 | Panorama に変更をコミットし、その変更をデバイスにプッシュします。

1. **Commit**（コミット） > **Commit and Push**（コミットしてプッシュ）をクリックします。
2. 選択内容を編集し 、**Prisma Access** タブの プッシュ スコープで 明示型プロキシ が選択されていることを確認してから、**[OK]**をクリックします。



3. **[Commit and Push (**コミットしてプッシュ**)]** をクリックします。

STEP 10 | 明示型プロキシで使用する PAC ファイルを選択します。

1. **[Panorama] > [Cloud Services**（クラウドサービス）**] > [Configuration**（設定）**] > [Mobile Users**（モバイルユーザー）**]**を選択します。

   PAC ファイルにポート 8080 を必ず入力してください。
2. 先ほど構成した明示型プロキシ設定の 接続名 を選択します。
3. 明示型プロキシに使用する **PAC (**プロキシ自動構成**)** ファイル を入力します。

   *PAC*ファイルの仕組みと変更方法を必ず理解してから*Prisma Access*にアップロードしてください。

   ファイルを参照して アップロードします。

   Prisma Accessはサンプル PAC ファイルを提供します。 サンプル **PAC** ファイルをダウンロードし、値を変更して、そのファイルをアップロードできます。PAC ファイルの要件とガイドライン、およびサンプル PAC ファイルの内容の説明については 、「明示型プロキシ PAC ファイルの設定」 を参照してください。

 ©2025 Palo Alto Networks, Inc.

明示型プロキシデプロイメント用のKerberos認証

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

Prisma Access Mobile—Explicit Proxy (明示型プロキシ) のデプロイメントはKerberos認証をサポートしています。サーバー、IoTデバイス、またはSAMLを使用して認証できないヘッドレスマシンがある場合は、代わりにKerberos認証を使用できます。

デプロイメントが認証にSAMLとKerberosの両方を使用する場合、単一の明示型プロキシデプロイメントで両方の認証タイプを設定できます。このようにして、SAMLを使用してモバイルユーザーを認証し、Kerberosを使用してサーバー、IoTデバイス、またはヘッドレスマシンを認証できます。Prisma Access明示型プロキシは、認証トラフィックに使用されるポートに応じて認証を処理します。

- 認証トラフィックがポート8080を使用する場合、明示型プロキシはSAML認証を使用します。
- 認証トラフィックがポート8081を使用する場合、明示型プロキシはKerberos認証を使用します。

もし1つのポートのみが構成されている場合、構成されていないポートは構成されたポートと同じ認証プロファイルを使用します。

*Kerberos SSO*は、あなたの*Kerberos*インフラストラクチャにアクセスできるエンドポイントとシステムにのみ利用可能です。エンドポイントとシステムは、*Kerberos*インフラストラクチャへのアクセスがない場合、*SAML SSO*を使用しなければなりません。

- 明示型プロキシのデプロイのためのKerberosのデプロイメントに関する要件と推奨事項
- Kerberos キータブを作成する
- 明示型プロキシデプロイメント用のKerberos認証を構成する

明示型プロキシのデプロイのための**Kerberos**のデプロイメントに関する要件と推奨事項

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Accessのライセンス ❑ 最低限必要なデータプレーンバージョン:PAN-OS 10.1.3 以降のバージョン

©2025 Palo Alto Networks, Inc.

明示型プロキシデプロイメントでKerberosを実装するためにKerberosキータブを作成する前に、Kerberosデプロイメントに次の要件と前提条件があることを確認してください。

- データプレーンをPAN-OS 10.1.3以降のバージョンに更新します。
- サーバーまたはデバイスを認証するためにPrisma Accessで使用できるKerberosアカウントがあることを確認します。

  Kerberosキータブ (プリンシパル名と暗号化されたKerberosパスワードを含むファイル) を作成するにはアカウントが必要です。
- サーバーとエンドポイントがドメインに参加していることを確認します。これにより、ユーザーとマシンは職場のネットワーク資格情報を使用して職場のドメインに安全に接続できるようになります。
- モバイル ユーザーのPACファイルまたはエンドポイントまたはサーバーのプロキシ設定で、Kerberos認証トラフィックをポート8081に転送するようにしてください。

  明示型プロキシは、Kerberos認証にポート8081を使用し、SAML認証にポート8080を使用します。
- Kerberos管理者がキータブを作成およびエクスポートする権限を持っていることを確認してください。
- サーバー、IoTデバイス、またはヘッドレス マシンが配置されているブランチまたはキャンパスのロケーションの出力IPアドレスがあることを確認します。

  これらのIPアドレスを、明示型プロキシによって信頼されるアドレスのリストに追加します。

©2025 Palo Alto Networks, Inc.

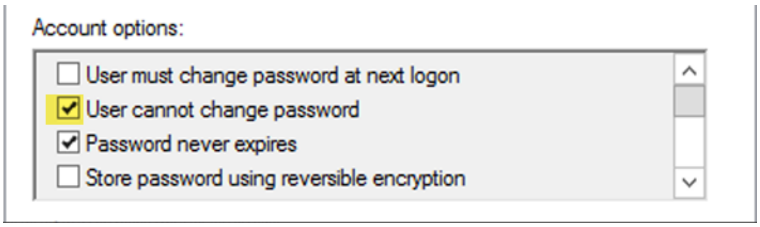
- Kerberosユーザー認証と作成に関するベストプラクティスに従ってください。

  Kerberos環境を保護し、パスワードが侵害されるのを防ぐためのベストプラクティスに従うのは、Kerberos アカウント管理者の責任です。ユーザー アカウント、パスワード、およびServicePrincipalNames (SPN) を作成するときは、次のベストプラクティスを使用します。

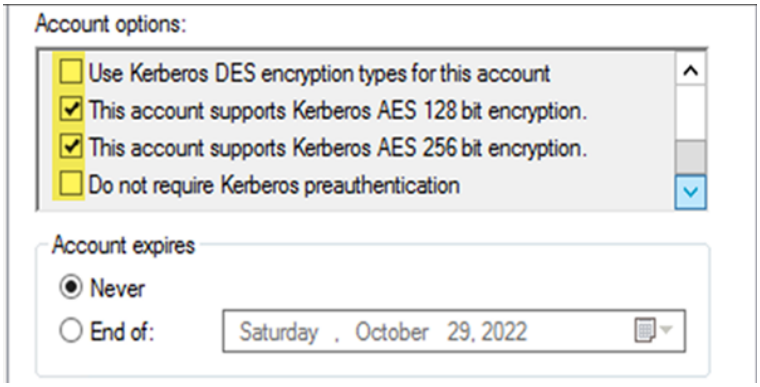
  Kerberosユーザー アカウント作成のベストプラクティス:

  - 管理者ユーザー アカウントを再利用しないでください。

    Explicit Proxy (明示型プロキシ)で使用するKerberosアカウントに一意のアカウント名を作成します。
  - このアカウントを他のサービスと共有しないでください。Prisma Access明示型プロキシ専用のユーザーアカウントを使用してください。
  - ユーザーがKerberosアカウントのパスワードを変更できないことを確認します。

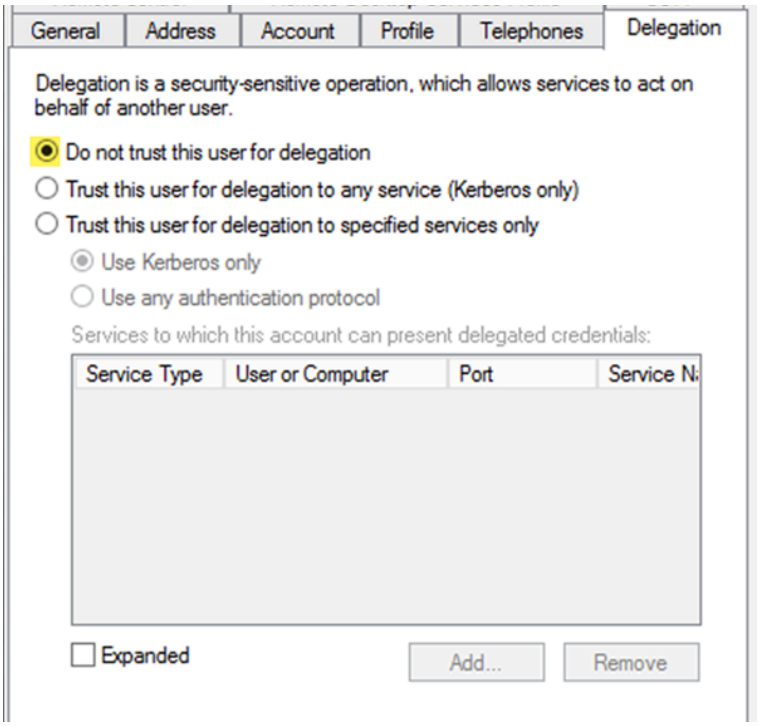
    

  - Kerberosアカウント オプションを選択するときは、[このアカウントに**Kerberos DES**暗号化タイプを使用する] と **[Kerberos**事前認証を必要としない] の選択を解除します。
  - AES-128およびAES-256ビット暗号化を有効にします。

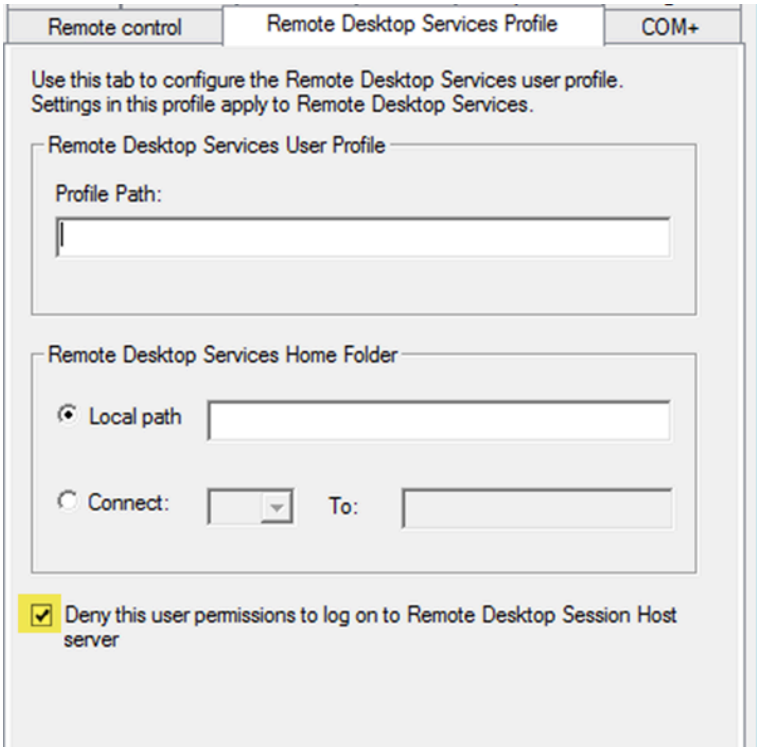
    

  - ユーザーの委任を無効にします。

©2025 Palo Alto Networks, Inc.

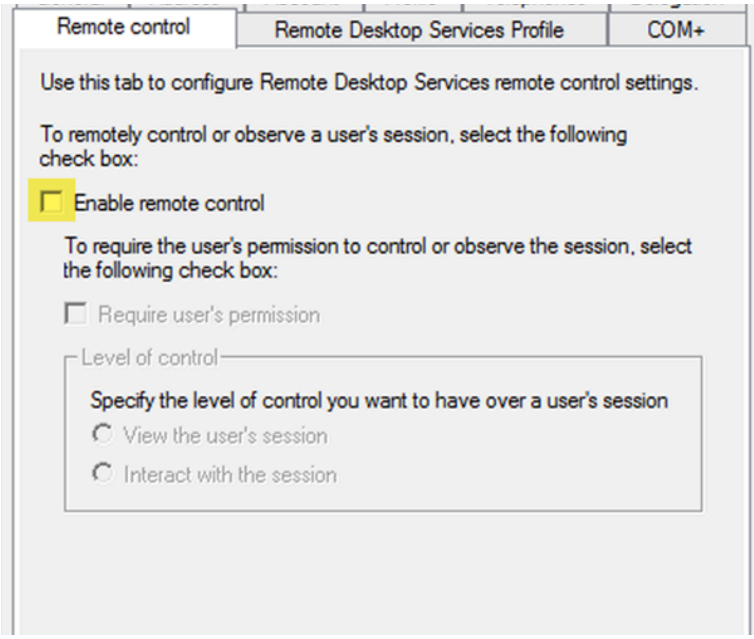


- リモート デスクトップ セッションにログインする機能を拒否します。

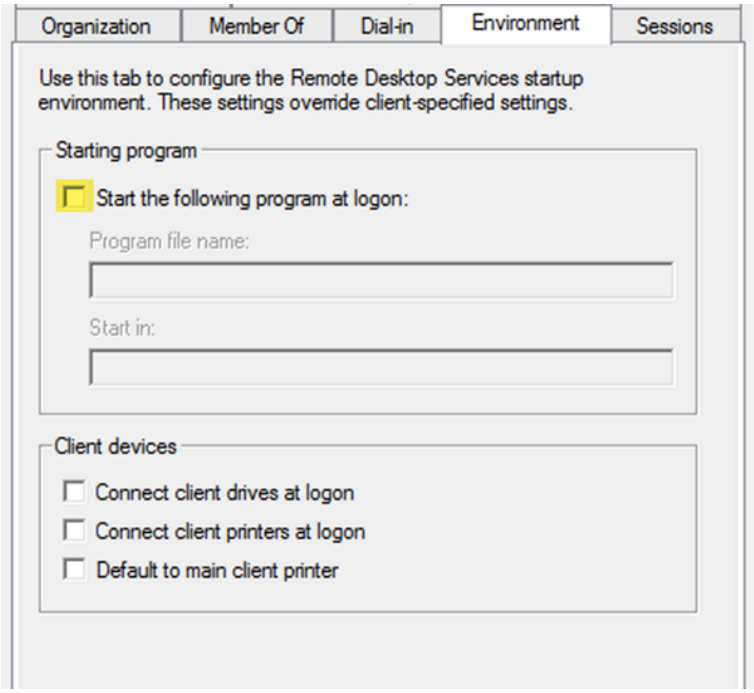


- リモートコントロールを有効にしないでください。

©2025 Palo Alto Networks, Inc.



- ユーザーがログオン時にプログラムを起動することを許可しません。



- 作成する認証プロファイルの許可リストにユーザーまたはユーザー グループを指定して、正当なビジネス ニーズを持つユーザーまたはマシンのみに認証を制限できます。

SPNと**Keytab**のベスト プラクティス:

- SPNが複数のユーザー アカウントに関連付けられていないことを確認してください。関連付けられていると、重複したSPN障害が発生する可能性があります。
- RC4-HMAC-NTは弱いNTMLハッシュを使用します。RC5暗号を含めるか除外するかについては、組織のセキュリティ ポリシーとガイドラインに従ってください。

©2025 Palo Alto Networks, Inc.

- DES-CBC-CRCおよびDES-CBC-MD5暗号は非推奨であり、Prisma Accessではサポートされていません。
- SPNのパスワードを定期的に変更します。パスワードのローテーションについては、組織のセキュリティ ポリシーとガイドラインに従ってください。
- パスワードの複雑さに関する組織の慣行に従います (たとえば、人間が判読したり推測したりできない、完全にランダムな形式でSPNパスワードを作成します)。
- サービスユーザーのパスワードを変更したり、その他の属性を変更したりする場合は、新しいキータブを更新して再生成し、Prisma Accessにアップロードしてください。
- 新しいPAリージョンをオンボードする場合は、次の手順に示すように、そのリージョンの新しいキータブを生成する必要があります。

次の出力例は、Kerberosのベスト プラクティスを使用して作成されたアカウントを示したものです。

```
PS C:\Users\Administrator> Get-ADUser example -Properties "*"
 AccountNotDelegated :True AllowReversiblePasswordEncryption :False
 CannotChangePassword :True CN : example
 Deleted :DoesNotRequirePreAuth :False Enabled :True
 GivenName :PrismaAccess EP Service User KerberosEncryptionType :
 {AES128, AES256} msDS-SupportedEncryptionTypes :24 Name :
 example PasswordExpired :False PasswordNeverExpires :True
 PasswordNotRequired :False PrincipalsAllowedToDelegateToAccount :
 {} ProtectedFromAccidentalDeletion :True SamAccountName :
 example servicePrincipalName : {HTTP/us-west-2.prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM, HTTP/us-east-2.prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM, HTTP/us-south-1.prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM} ServicePrincipalNames :
 {HTTP/us-west-2.prisma-abcde12345.proxy.prismaaccess.com@EXMP.COM,
 HTTP/us-east-2.prisma-abcde12345.proxy.prismaaccess.com@EXMP.COM,
 HTTP/us-south-1.prisma-abcde12345.proxy.prismaaccess.com@EXMP.COM}
 SmartcardLogonRequired :False TrustedForDelegation :False
 TrustedToAuthForDelegation :False UseDESKeyOnly :False
 UserPrincipalName :HTTP/us-south-1.prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM
```

Kerberos キータブを作成する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	☐ Prisma Accessのライセンス ☐ 最低限必要なデータプレーン バージョン:PAN-OS 10.1.3 以降のバージョン

明示型プロキシ用にKerberosをデプロイするための要件と推奨事項を確認したら、Kerberosキータブを作成する準備が整います。

©2025 Palo Alto Networks, Inc.

最適なパフォーマンスを得るには、キータブ ファイルのサイズを*60 KB*未満にする必要があります。

STEP 1 | 明示型プロキシのデプロイメントをセットアップします。

STEP 2 | Kerberos認証を設定するために必要なFQDN、プロキシFQDN、およびDNS CNAMEを取得します。

Kerberos認証では、Prisma AccessAPIスクリプトから取得した情報を使用して、Kerberosキータブを作成および構成します。API スクリプトは次の情報を取得します。

- **ep_geo_lb_fqdn**—明示型プロキシ ネットワーク ロード バランサ構成で使用される明示型プロキシDNS FQDN。このFQDNは、明示型プロキシの 明示型プロキシ**URL** と同じです。 これは、**[Workflows (ワークフロー)]** > **[Prisma Accessセットアップ]** > **[Explicit Proxy (明示型プロキシ)]** > **[Infrastructure Settings (インフラストラクチャ設定)]** > **[Explicit Proxy URL (明示型プロキシURL)]**におけるPrisma Access UIにあるものです。
- **ep_geo_lb_cname**—明示型プロキシ テナントのDNS CNAME。
- **ep_regional_fqdn**—オンボードされた明示型プロキシの場所に使用されるFQDN。

  明示型プロキシは、各場所にネットワーク ロード バランサーのパブリック IP アドレスを提供します。ep_regional_fqdn はその IP アドレスに関連付けられた FQDN です。複数の場所で同じパブリックIPアドレスを共有している場合、それらの場所では同じ地域FQDNが使用されます。

1. curlコマンドの一部として使用するAPIキーを生成します。
   - Prisma Access (Managed by Strata Cloud Manager)上で、 **[Workflows (ワークフロー)]** > **[Prisma Accessのセットアップ]** > **Prisma Access** > **[Infrastructure Settings (インフラストラクチャの設定)]** > **[Generate New API Key (新しいAPIキーの生成)]**を選択します。
   - Panorama Managed Prisma Access上で、 **[Panorama]** > **[Cloud Services (クラウドサービス)]** > **[Configuration (設定)]** > **[Service Setup (サービスセットアップ)]** > **[Generate API Key (APIキーの生成)]**を選択します。
2. .txt ファイルを作成し、ファイルに次のコマンド オプションを入力します。

   ```
   { "serviceType": "swg_proxy", "location": "deployed",
    "addrType": "network_load_balancer" }
   ```
3. Kerberos 認証を使用するために必要な FQDN を取得するには、次のコマンドを入力します。

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

   ここで、`option.txt` は前の手順で作成した .txt ファイルであり、`Current-API-Key`はPrisma Access API キーです。

 ©2025 Palo Alto Networks, Inc.

4. FQDNをメモします。

   オンボードされた場所ごとに、少なくとも 1 つの **ep_geo_lb_fqdn**、 1 つの **ep_geo_lb_cname**、および1つの**ep_regional_fqdn**が存在します。

STEP 3 | 以下のコマンドを入力して、組織の Active Directory (アクティブディレクトリ - AD)にPrisma AccessExplicit Proxyサービス用の新しいユー ザを作成します：

```
New-ADUser -Name "USER_NAME" -GivenName "USER_GIVEN_NAME"
 -SamAccountName "USER_SAMACCOUNTNAME" -UserPrincipalName
 "USER_NAME@DNS_DOMAIN_NAME" -Path "X_500_PATH" –AccountPassword
 (ConvertTo-SecureString “PASSWORD” -AsPlainText -force) -Enabled
 $true -KerberosEncryptionType RC4、AES128、AES256
```

ここで:

- *USER_NAME* はユーザー オブジェクトの名前です。
- *USER_GIVEN_NAME* はユーザーの名です。
- *USER_SAMACCOUNTNAME* は、ユーザーのセキュリティ アカウント マネージャー (SAM) 名です。
- *USER_NAME@DNS_DOMAIN_NAME* は、ユーザーのユーザー プリンシパル名 (UPN) です。
- *X_500_PATH* は新しいオブジェクトが作成される OU またはコンテナの X.500 パスです (例:DC=EXAMPLE,DC=COM)。
- *PASSWORD* は アカウントに使用するパスワードです。

次の CLI の例では、ユーザー名は example、SAM 名は example、名は PrismaAccess EP Service User、UPN は example@exmp.com、パスは DC=EXMP,DC=COM、パスワードは Ex@mple123 です。

```
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
```

前述のコマンドは、弱い*NTLM*ハッシュを使用する*RC4*の暗号化タイプを指定します。このコマンドに*RC4*を含めるか除外するかについては、組織のセキュリティ ポリシーとガイドラインに従ってください。

©2025 Palo Alto Networks, Inc.

STEP 4 | パスワードの有効期限が切れないようにし、変更されないようにするには、次のコマンドを入力します。

```
Get-ADUser USER_NAME|Set-ADUser -PasswordNeverExpires:$True -
CannotChangePassword:$true
```

パスワードの有効期限とローテーション ポリシーについては、組織のセキュリティ ポリシーとガイドラインに従ってください。

STEP 5 | 新しく作成されたユーザー アカウントを表示するには、次のコマンドを入力します。

```
Get-ADUser USER_NAME -property msDS-KeyVersionNumber
```

STEP 6 | SPNを関連付け、Windows ADのKerberos認証で使用するキータブ ファイルをエクスポートします。

キータブ ファイルを使用すると、明示型プロキシは、ユーザー、サーバー、IoT デバイス、またはその他のヘッドレス マシンからのトラフィック フロー中に提供されるKerberos認証トークンを検証できます。キータブ ファイルの作成中、明示型プロキシでは、前の手順

©2025 Palo Alto Networks, Inc.

で API を使用して取得した値が、その手順の後の手順で作成したユーザー アカウントに ServicePrincipalNames (SPN) として関連付けられる必要があります。

ep_geo_lb_fqdn、**ep_geo_lb_cname**、および **ep_regional_fqdn** の 値を使用します。これらの値により、明示型プロキシはいずれかのプロキシ ドメインへのトラフィック フローを認証できるようになります。

1. 次のコマンドを入力して、**ep_geo_lb_fqdn** 値をサービス プリンシパル名 (SPN) として使用してキータブを生成し、エクスポートします。

   ```
   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
   ```

   ここで:

   - *ep_geo_lb_fqdn* は、明示型プロキシAPI スクリプトから返される **ep_geo_lb_fqdn** 値です。
   - *REALM* は領域です (例:EXMP.COM)。

     ほとんどの場合、大文字を使用して領域を入力します。
   - *DOMAIN\USER_NAME* は ドメイン レベルのログオン名です (例:EXMP\example)。
   - *PASSWORD* は 、キータブに使用するパスワードです。このパスワードはユーザー パスワードと一致する必要はありませんが、次の手順で **ep_geo_lb_cname** および **ep_regional_fqdn**SPN に作成する値と一致する必要があります。
   - *KEYTAB_NAME_1*は キータブの名前です。キータブ名はこの SPN に対して一意である必要があります。

   SPN とパスワードを作成する場合は、必ずベスト プラクティスに従ってください。

   次の CLI の例では、*ep_geo_lb_fqdn* は example.proxy.prismaaccess.com、*REALM* は

©2025 Palo Alto Networks, Inc.

EXMP.COM、*DOMAIN\USER_NAME* は EXMP\example、*PASSWORD* は Ex@mple123、エクスポートされたキータブ名は exmp1.keytabです。

```
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. 次のコマンドを入力して、**ep_geo_lb_cname**値をSPNとして使用してキータブを生成し、エクスポートします。

```
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
```

ここで:

- *ep_geo_lb_cname* は、明示型プロキシAPIスクリプトから返される**ep_geo_lb_cname**値です。
- *REALM*は領域です。例:EXMP.COM
- *DOMAIN\USER_NAME* は ドメイン レベルのログオン名です (例:EXMP\example)。
- *PASSWORD* は 、キータブに使用するパスワードです。このパスワードは、**ep_geo_lb_fqdn** および**ep_regional_fqdn**SPNパスワードと一致する必要があります。
- *KEYTAB_NAME_2* はエクスポートするキータブの名前です。この名前は、作成する他のSPNキータブ名とは異なる必要があります。

次の CLI の例では、*ep_geo_lb_cname* は prisma-abcde12345.proxy.prismaaccess.com、*REALM* は EXMP.COM、*DOMAIN\USER_NAME* は EXMP\example、*PASSWORD* は Ex@mple123、エクスポートされたキータブ名は exmp2.keytabです。

```
ktpass -princ HTTP/prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM -mapuser EXMP
```


©2025 Palo Alto Networks, Inc.

```
\example -ptype KRB5_NT_PRINCIPAL -crypto all -pass Ex@mple123
 -out exmp2.keytab
```

3. 次のコマンドを入力して、**ep_regional_fqdn** 値をSPNとして使用してキータブを生成し、エクスポートします。

```
ktpass -princ HTTP/ep_regional_fqdn@REALM -
mapuser DOMAIN\USER_NAME -ptype KRB5_NT_PRINCIPAL -crypto all
 -pass PASSWORD -out KEYTAB_NAME_3.keytab
```

ここで:

- *ep_regional_fqdn* は、明示型プロキシ API スクリプトから返される **ep_regional_fqdn** 値です。
- *REALM* は領域です (例:EXMP.COM)。
- *DOMAIN\USER_NAME* は ドメイン レベルのログオン名です (例:EXMP\example)。
- *PASSWORD* は 、キータブに使用するパスワードです。このパスワードは、**ep_geo_lb_fqdn** および **ep_geo_lb_cname**SPN パスワードと一致する必要があります。
- *KEYTAB_NAME_3* は、エクスポートするキータブの名前です。この名前は、作成する他のSPNキータブ名とは異なる必要があります。

次の CLI の例では、*ep_regional_fqdn* は us-west-2.prisma-abcde12345.proxy.prismaaccess.com、*REALM* は EXMP.COM、*DOMAIN\USER_NAME* は EXMP\example、*PASSWORD* は Ex@mple123、エクスポートされたキータブ名は exmp3.keytabです。

```
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. （任意）異なる **ep_regional_fqdn** 値を使用する追加のロケーションがあり、それらのロケーションのキー タブを作成したい場合は、ステップ6.cを繰り返して、それらのロケーションの **ep_regional_fqdn** 値を使用して、1 つ以上の追加のキー タブを生成し、エクスポートする。

一意の **ep_regional_fqdn**ごとに一意のキータブ名を作成します。
たとえば、別の場所の **ep_regional_fqdn** が us-east-2.prisma-abcde12345.proxy.prismaaccess.comの場合、一意のエクスポートされたキータブ ファイル名を使用して次のサンプル CLI を入力します。

```
ktpass -princ HTTP/us-east-2.prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM -mapuser EXMP
\example -ptype KRB5_NT_PRINCIPAL -crypto all -pass Ex@mple123
 -out exmp4.keytab
```


©2025 Palo Alto Networks, Inc.

STEP 7 | Ubuntu で次の `ktutil` コマンドを入力して、作成されたキータブ内のサポートされていない暗号を削除します。

次のシステム出力は、さまざまな暗号をクリーンアップする例を示しています。

```
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
```

ここで、*KEYTAB_NAME_1*.keytab、*KEYTAB_NAME_2*.keytab、および *KEYTAB_NAME_3*.keytab は、前の手順で作成したキータブです。

STEP 8 | (任意) 他のリージョン用にさらにキータブを作成した場合は、前の `ktutil` コマンドを入力し、*KEYTAB_NAME_1*.keytab をリージョンに使用したキータブ名に置き換え、別の出力ファイル (`new4.keytab`、`new5.keytab`など) を指定して、それらのキータブでサポートされていない暗号を削除します。

STEP 9 | 次の `ktutil` コマンドを入力して、作成したキータブをマージします。ここで、new1.keytab、new2.keytab、および new3.keytab は、前の手順で作成したキータブです。このコマンドには、リージョン固有のキータブをすべて含めるようにしてください。

```
ktutil rkt new1.keytab rkt new2.keytab rkt new3.keytab # 追加の地域
固有のキータブファイルを作成した場合は、ここに追加します。 wkt papxv1.keytab
 quit
```

完了したら、作成したキータブ (この例では`papxv1.keytab`) を明示型プロキシで使用するキータブとして使用します。

©2025 Palo Alto Networks, Inc.

明示型プロキシデプロイメント用のKerberos認証を構成する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

- Strata Cloud Manager
- Panorama

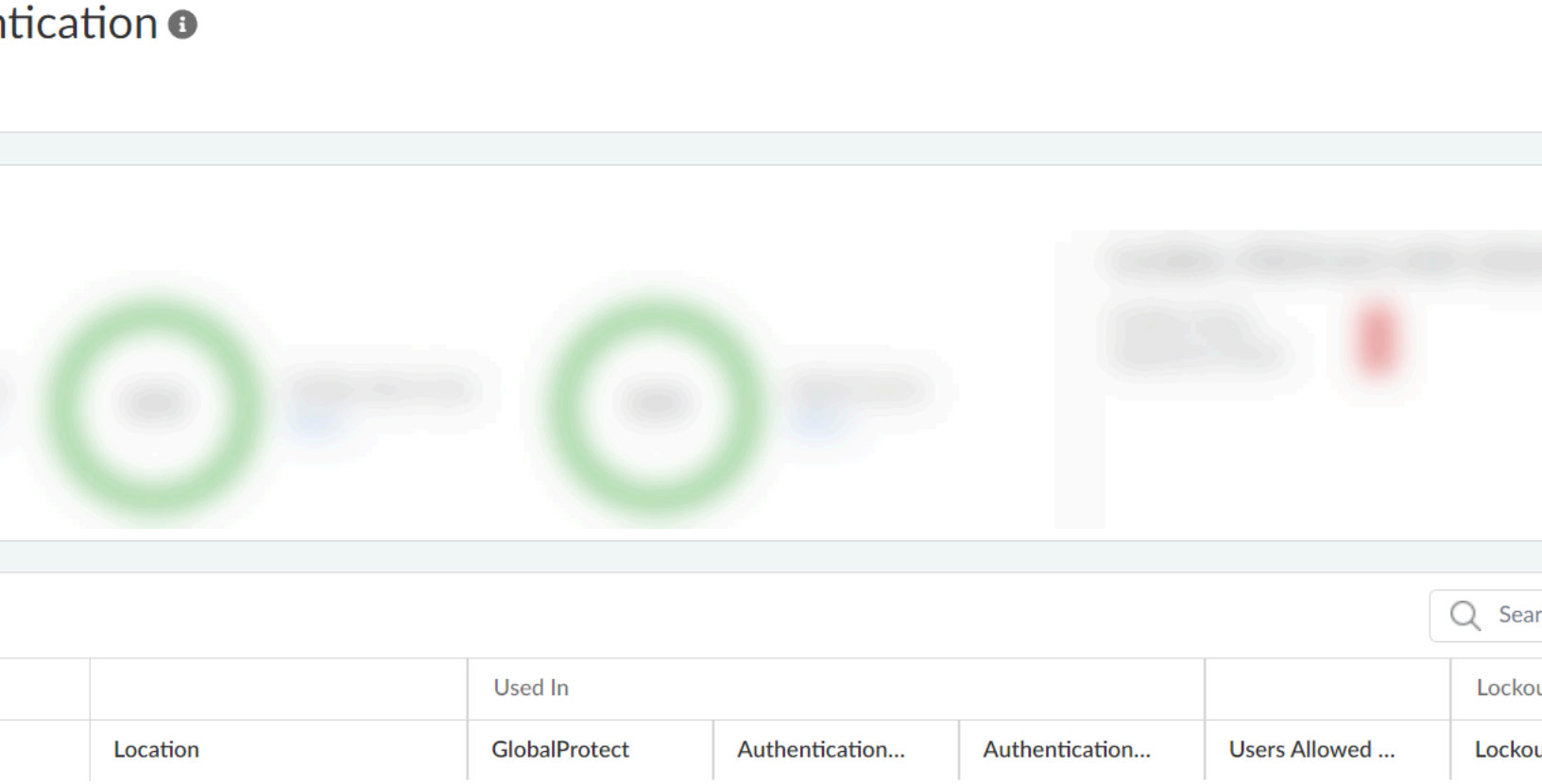
©2025 Palo Alto Networks, Inc.

明示型プロキシデプロイメント用の**Kerberos**認証を構成する（**Strata Cloud Manager**）

STEP 1 | Kerberos 認証プロファイルをセットアップします。

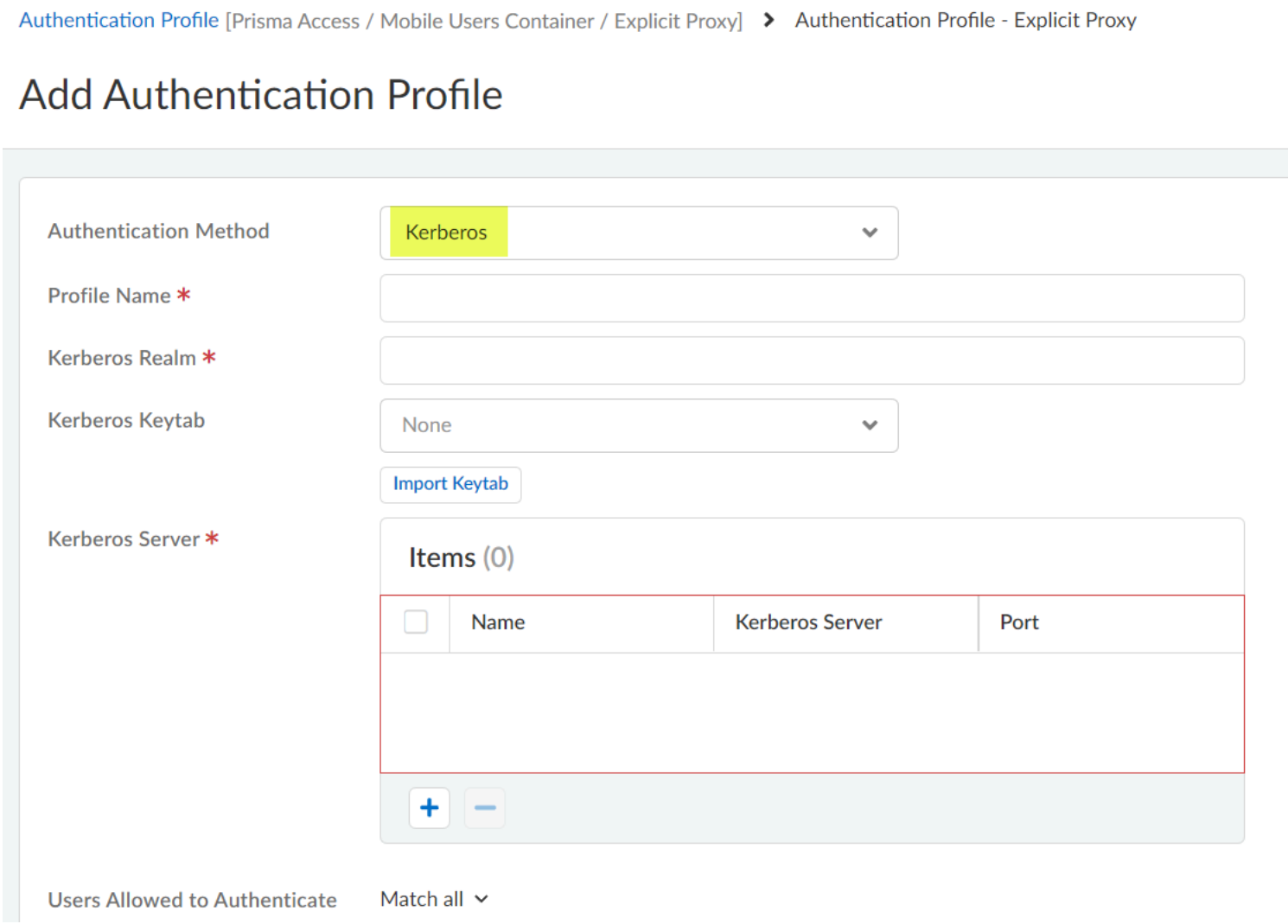
このプロファイルは、モバイル ユーザーの認証のために明示的なプロキシがKerberosサーバーに接続する方法を定義します。

1. **[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access] > [Identity Services (IDサービス)] > [Authentication (認証)] > [Authentication Profiles (認証プロファイル)]** および**[Add Profile (プロファイルを追加)]**に移動します。



2. **[Authentication Method (認証方法)]**の方法を選択します:**Kerberos**。

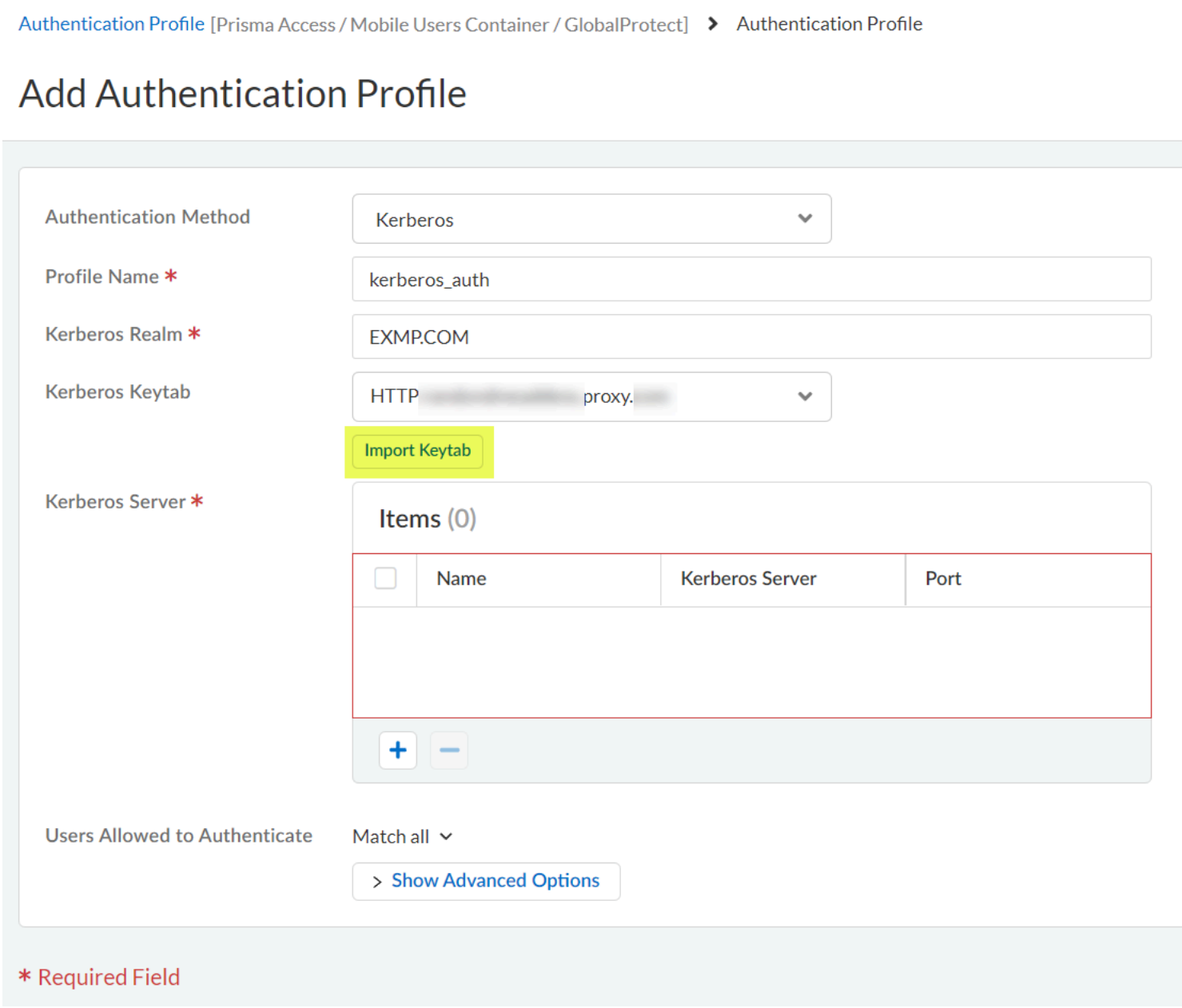
©2025 Palo Alto Networks, Inc.



3. サーバープロファイルを識別する**[Profile Name**（プロファイル名）**]**を入力します。

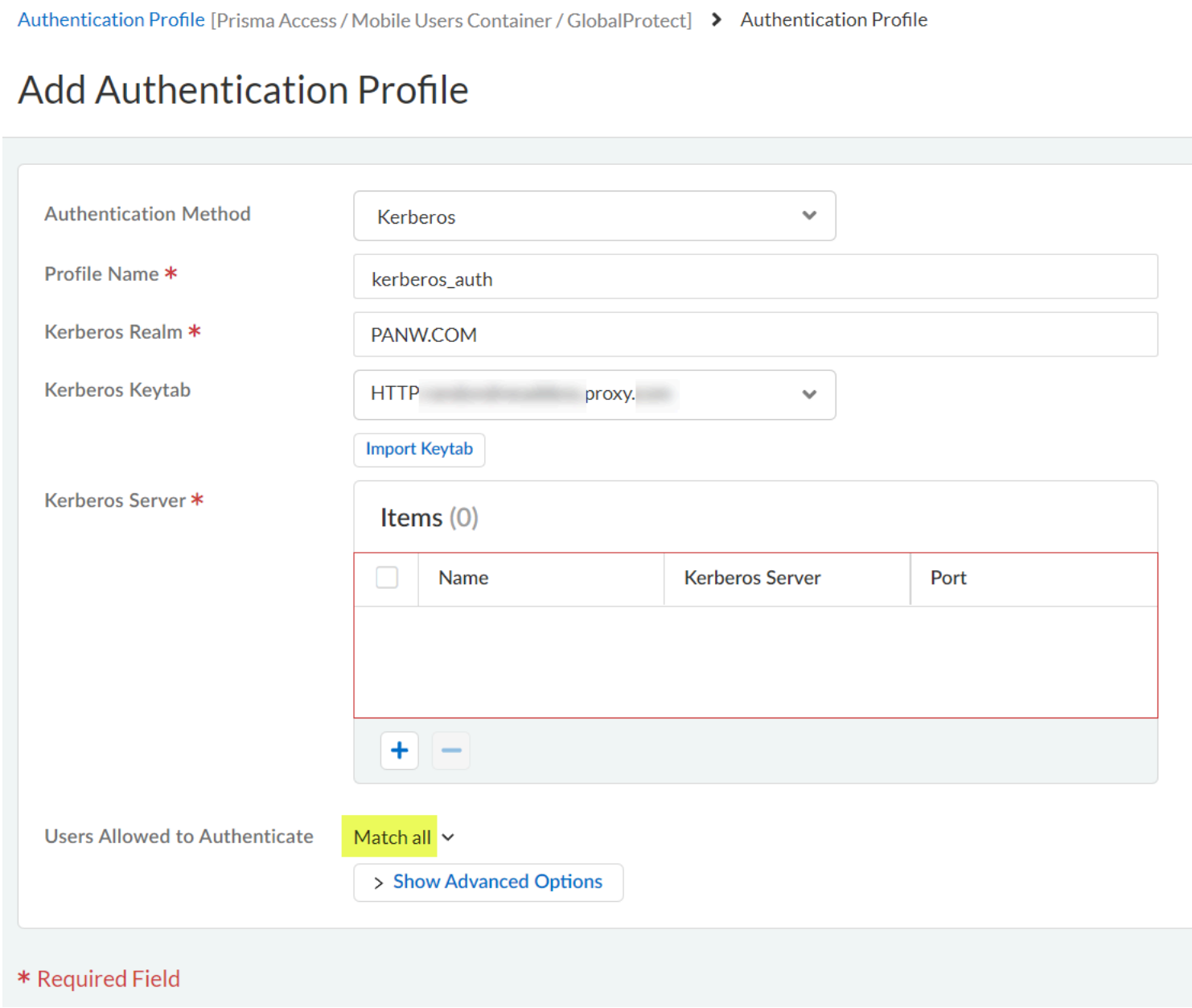
   認証プロファイルは、ポータルまたはゲートウェイがユーザーを認証する際に使用するサーバー プロファイルを指定します。
4. **Kerberos Realm**（**Kerberos** レルム）を入力して（最大 127 文字）、ユーザーのログイン名のホスト名部分を指定します。たとえば、ユーザー アカウント名 user@EXMP.COM には、realm EXMP.COM があります。
5. 先ほど作成した**Kerberos Keytab(Import Keytab)** をインポートします。

©2025 Palo Alto Networks, Inc.



6. このプロファイルで 認証を許可されたユーザー を追加します。
   - すべてのユーザーを選択するには、 **Match all (**すべて一致**)**を選択します。
   - Cloud Identity Engineを使用してユーザーのリストを作成する場合は、リストからユーザーを選択するか、 すべて を選択してすべてのユーザーの認証を許可します。
   - Kerberos を使用してログインできるローカル ユーザーを追加するには、 ローカル ユーザーを追加し、 名前を追加して、 パスワードを作成します。
     - ユーザー認証とユーザー マッピングを構成するときは、userPrincipalName (UPN) の形式を使用します。他の形式 (samAccountName など) はサポートされていません。
     - Unicode文字のユーザー名はサポートされていません。

©2025 Palo Alto Networks, Inc.

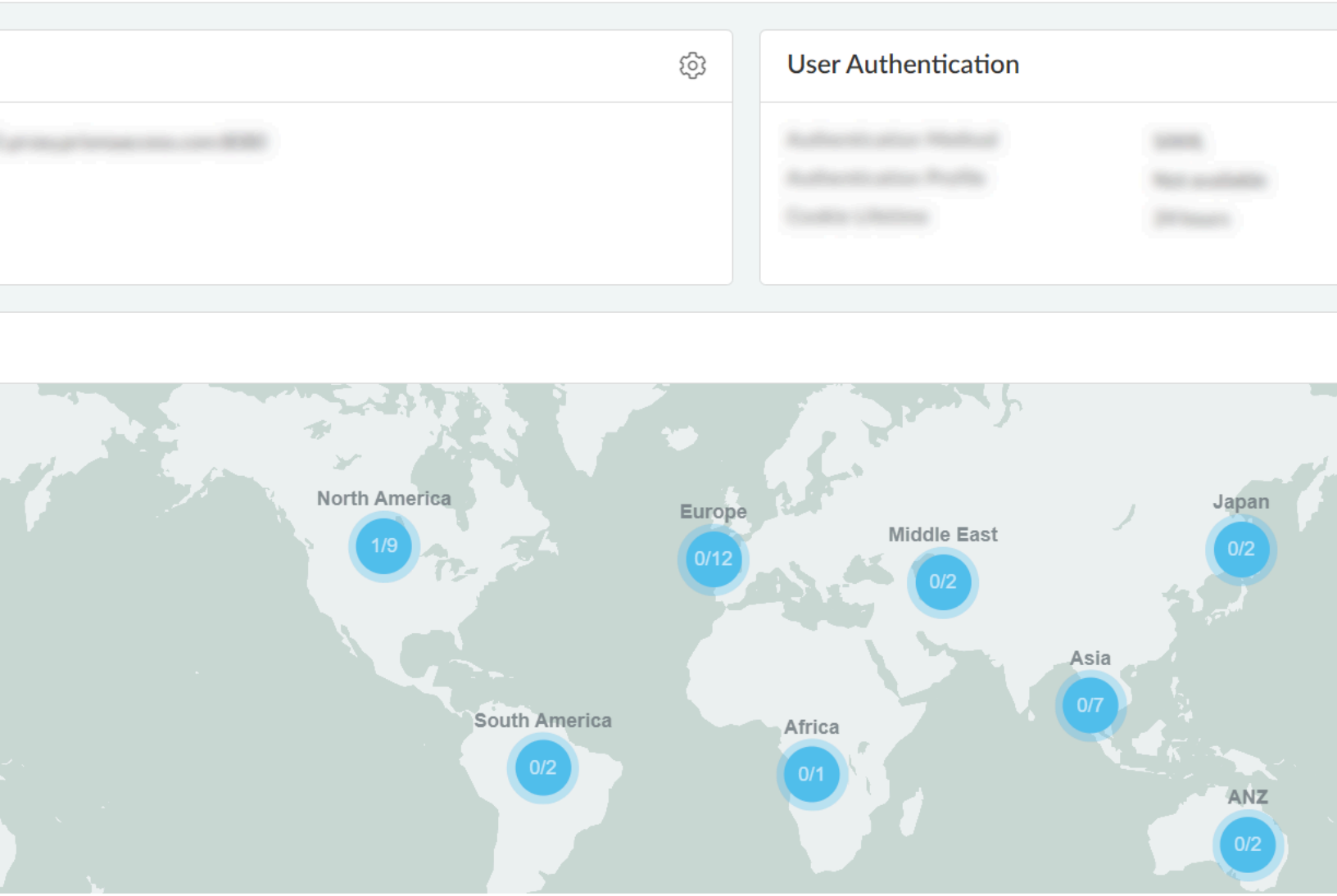


7. 変更を保存します。

©2025 Palo Alto Networks, Inc.

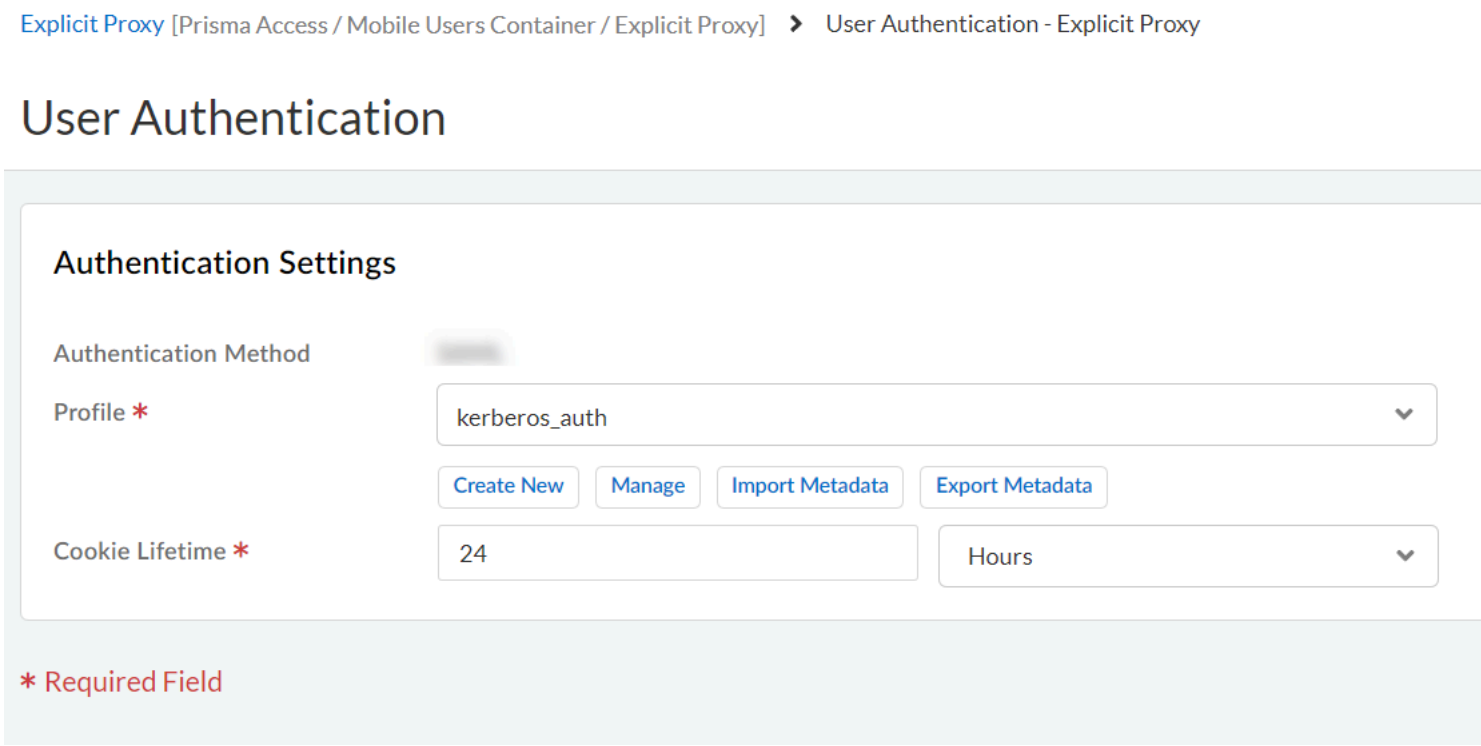
STEP 2 | 認証プロファイルを認証方法に関連付けます。

1. **[ワークフロー] > [Prisma Accessのセットアップ] > [明示型プロキシ] > [ユーザー認証]**に移動します。



2. **[Connection Name (接続名)]**を選択します。
3. **Kerberos** の認証方法を選択し、作成したKerberosプロファイルを選択します。

©2025 Palo Alto Networks, Inc.



4. 変更を保存します。

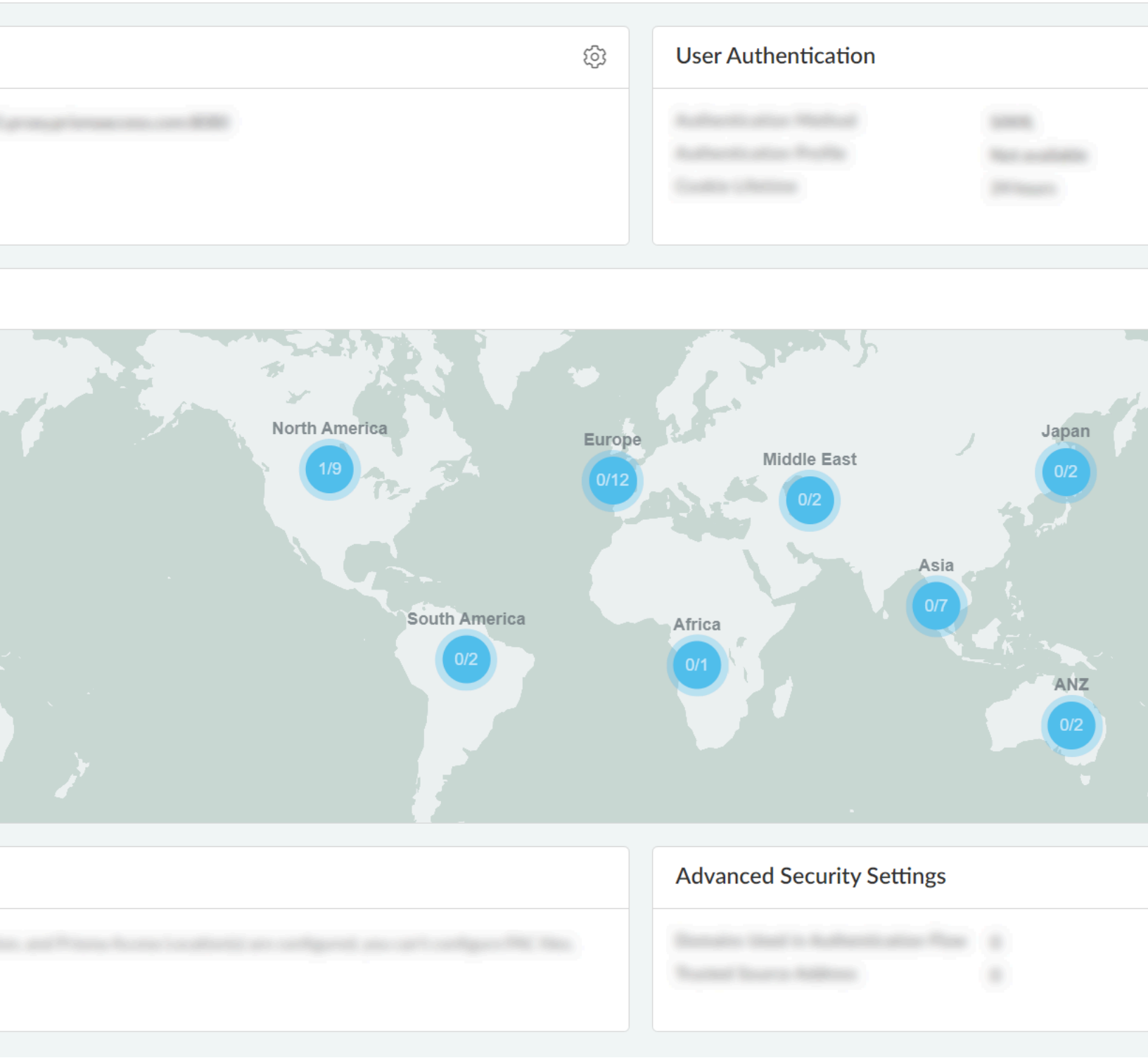
©2025 Palo Alto Networks, Inc.

STEP 3 | (任意) ユーザー、サーバー、IoT デバイス、またはヘッドレス マシンが配置されているブランチまたはキャンパスの場所の出力IPアドレスを、信頼できる明示的プロキシ アドレスのリストに追加します。

特定のIPアドレスの 認証をスキップ する場合、または **ID** の受信 **HTTP/HTTPS** 要求で **X-Authenticated User (XAU)** ヘッダーを使用する場合にのみ、これを実行する必要があります。

1. [ワークフロー] > **[Prisma Access**セットアップ] > **[Explicit Proxy (**明示型プロキシ**)]** > **[Advanced Security Settings (**詳細セキュリティ設定**)]**に移動します。

©2025 Palo Alto Networks, Inc.

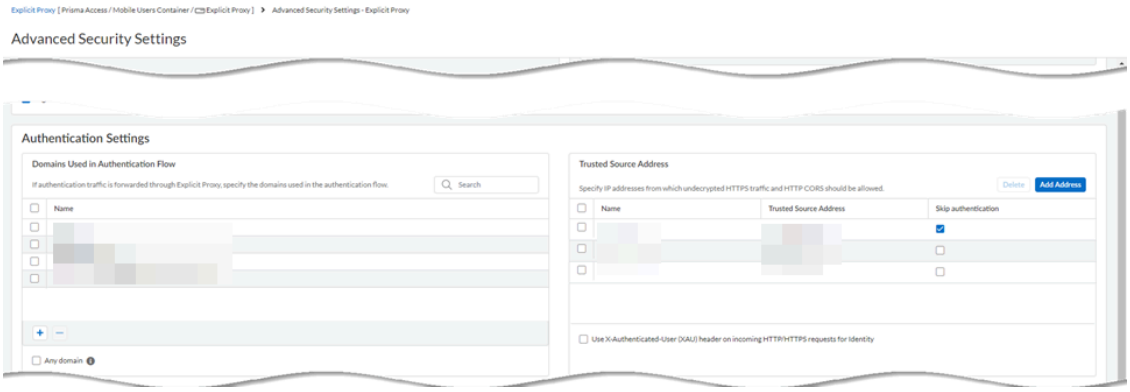


2. **Trusted Source Address** (信頼できるソース アドレス) フィールドにアドレス (**1** つ以上) を追加します 。

©2025 Palo Alto Networks, Inc.

出力エンドポイントIPアドレスを信頼リストに追加しない場合、明示的プロキシはユーザーとマシンにSAMLとKerberosによる認証を強制します。

最大100,000 個のIPアドレスを入力します。



3. 変更を保存します。

STEP 4 | ユーザー認証用のすべて許可ポリシー ルールを作成します。

1. **[Manage (管理)]** > **[Configuration (設定)]** > **[NGFW]Prisma Access** > **[Security Services (セキュリティ サービス)]** > **[Security Policy (セキュリティ ポリシー)]** > **[Add Rule (ルールの追加)]** > **[Pre Rules (事前ルール)]** > を選択します。
2. ルールに名前を付けます。
3. 必要なすべての一致条件を **[Any (任意)]**に設定します。
4. ユーザーを **[Known (既知)]**に設定する
5. アクションを **[Allow (許可)]**に設定します。
6. ルールを保存します。

STEP 5 | 設定変更をプッシュします。

©2025 Palo Alto Networks, Inc.

STEP 6 | トラフィックと認証ログを表示して、Prisma AccessでKerberos認証が機能していることを確認する。

1. (復号化されたトラフィックのみ) [アクティビティ] > [ログ ビューアー] > [ファイアウォール/トラフィック] に移動し、Kerberos 認証が機能していることを確認します。

   *Strata Cloud Manager*を使用している場合は、*[インシデントとアラート] > [ログ ビューアー] > [ファイアウォール/トラフィック]*に移動します。

   復号化されたトラフィックでは、トラフィック ログにユーザー名が表示されます。

2. (復号化されていないトラフィックのみ) [アクティビティ] > [ログ ビューアー] > [ファイアウォール/認証] に移動し、Kerberos 認証が正しく機能していることを確認します。

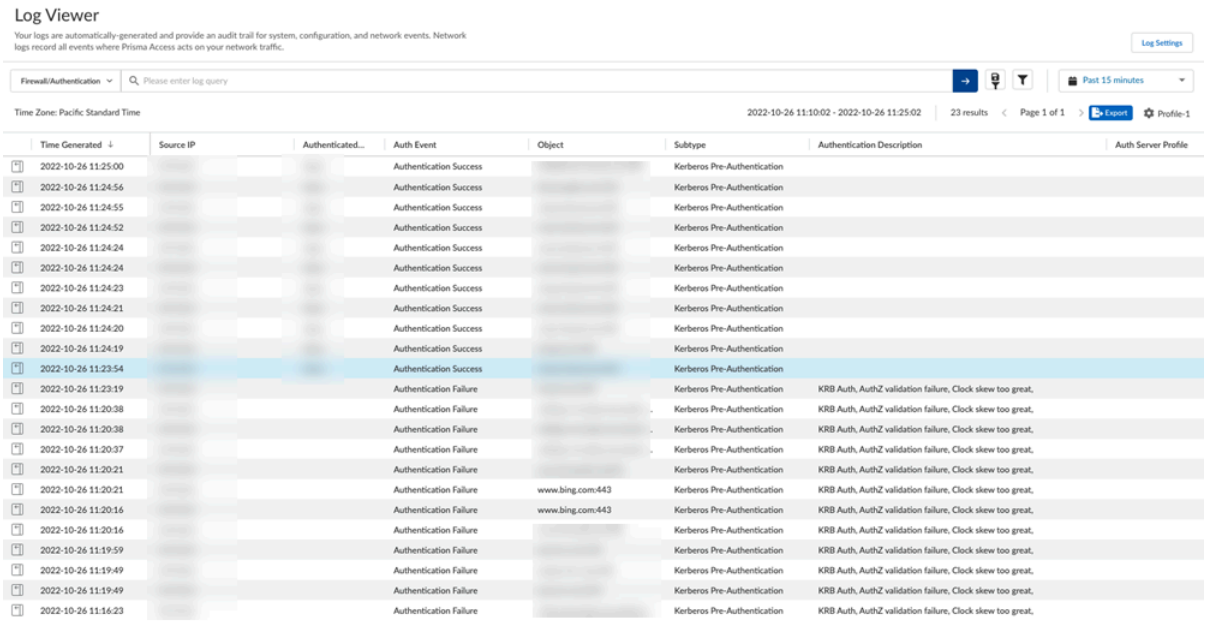
   *Strata Cloud Manager*を使用している場合は、*[インシデントとアラート] > [ログ ビューアー] > [ファイアウォール/認証]*に移動します。

   次のフィールドには、認証イベントに関する詳細情報が提供されます。

   - オブジェクト- 認証のためにKerberosにリダイレクトされる前にユーザーがアクセスしようとしていたWebサイト。
   - 認証イベント- 認証試行のステータス。

     認証成功は、 認証イベントが成功したことを示します。 認証失敗は、 試行が失敗し、ログが生成されたことを示します。
   - 認証の説明- 認証の試行が失敗した場合、失敗の種類に関する追加情報。

     たとえば、「ユーザーは許可されていません」 は、ユーザーまたはグループが認証にKerberosを使用できないことを示します。これは、認証プロファイルの 許可リスト に追加されていないことが原因である可能性があります。



 ©2025 Palo Alto Networks, Inc.

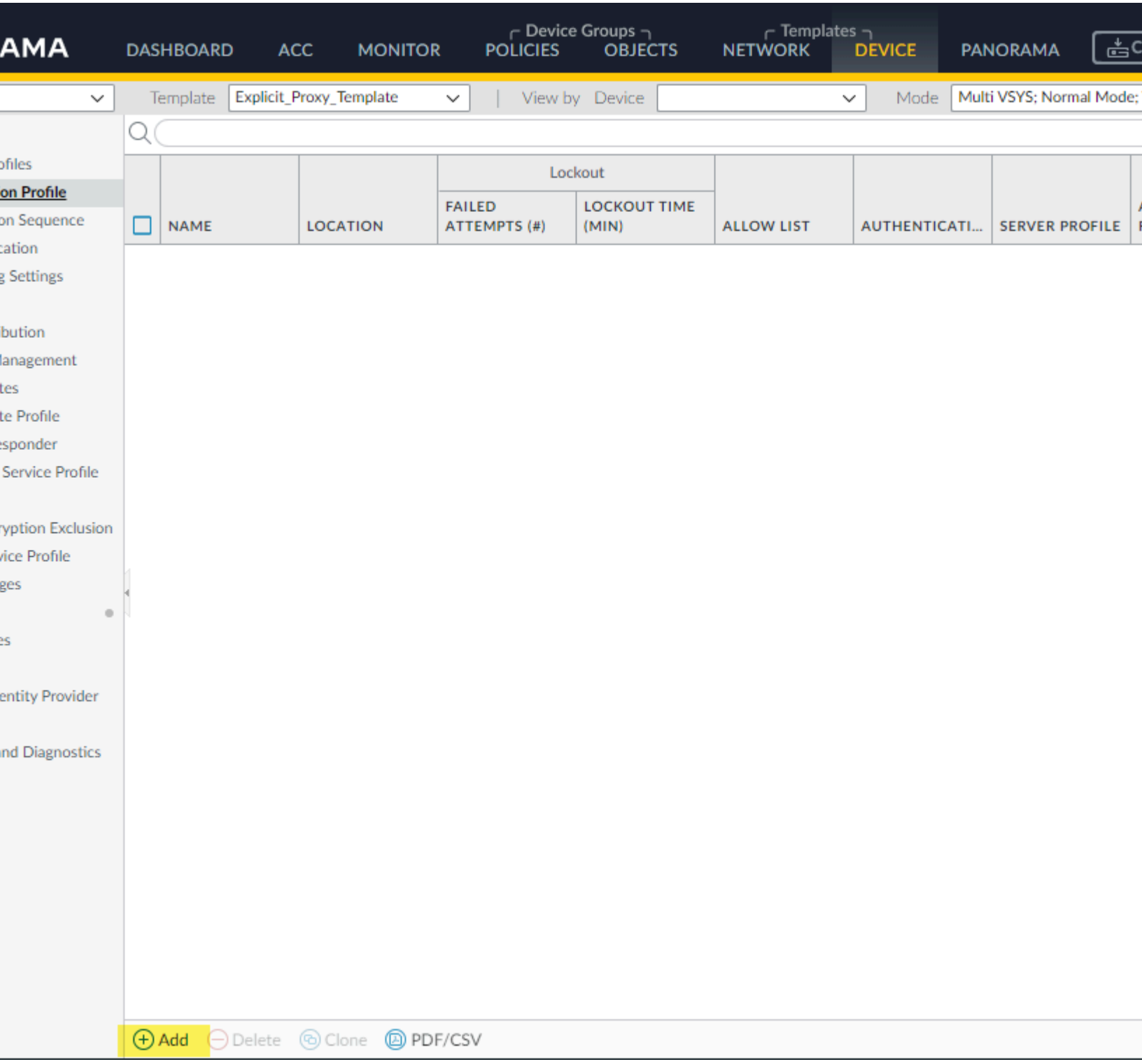
明示型プロキシデプロイメント用の**Kerberos**認証を構成する（**Panorama**）

©2025 Palo Alto Networks, Inc.

STEP 1 | Kerberos認証プロファイルをセットアップします。

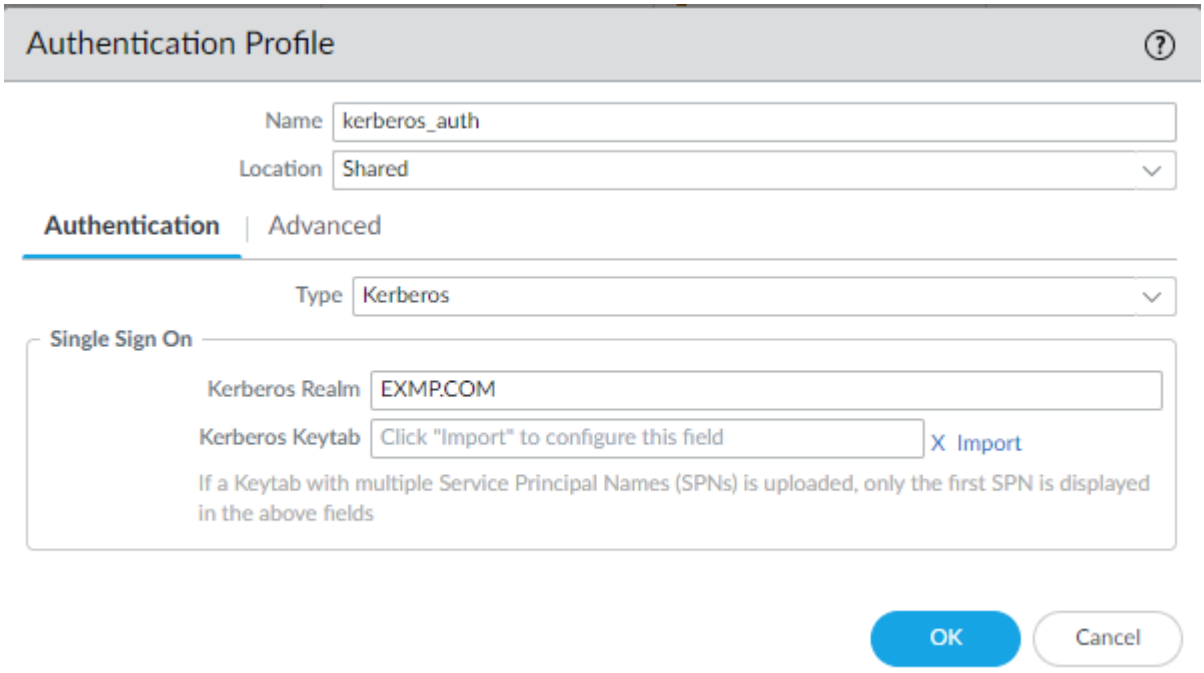
このプロファイルは、モバイル ユーザーの認証のために明示型プロキシがKerberosサーバーに接続する方法を定義します。

1. **Device**（デバイス） > **Authentication Profile**（認証プロファイル） > **+ Add (追加)**に移動します。

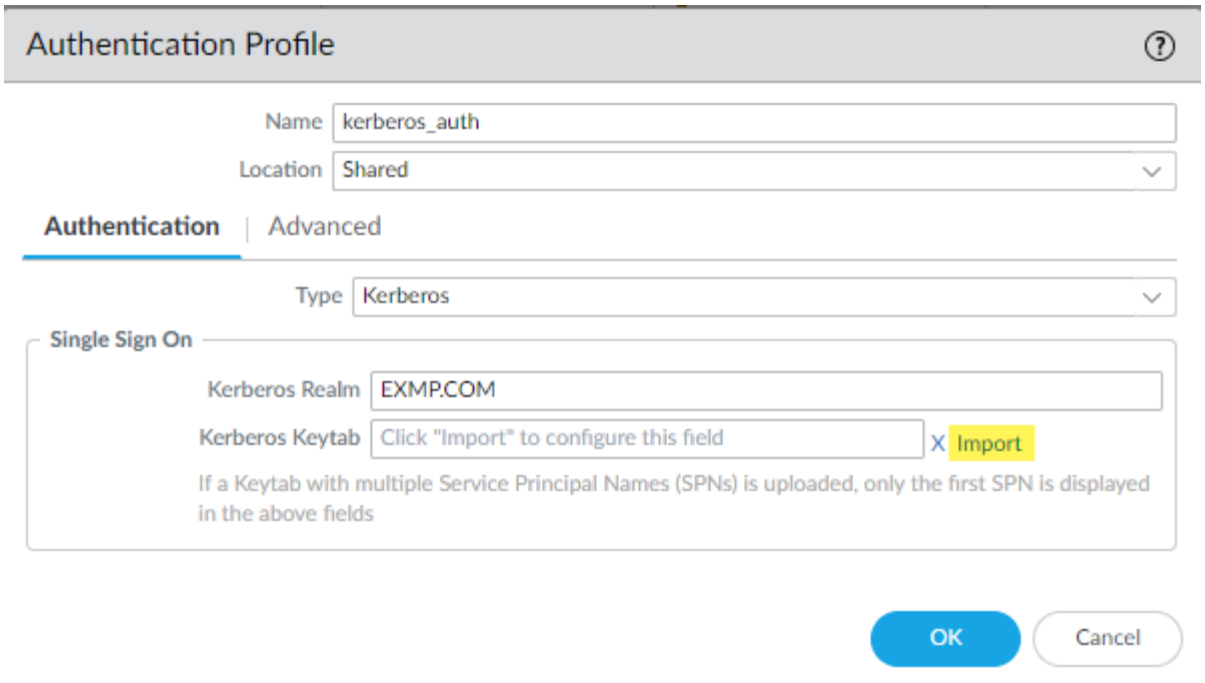


©2025 Palo Alto Networks, Inc.

2. **[Type(タイプ)]** を選択します。**Kerberos**。



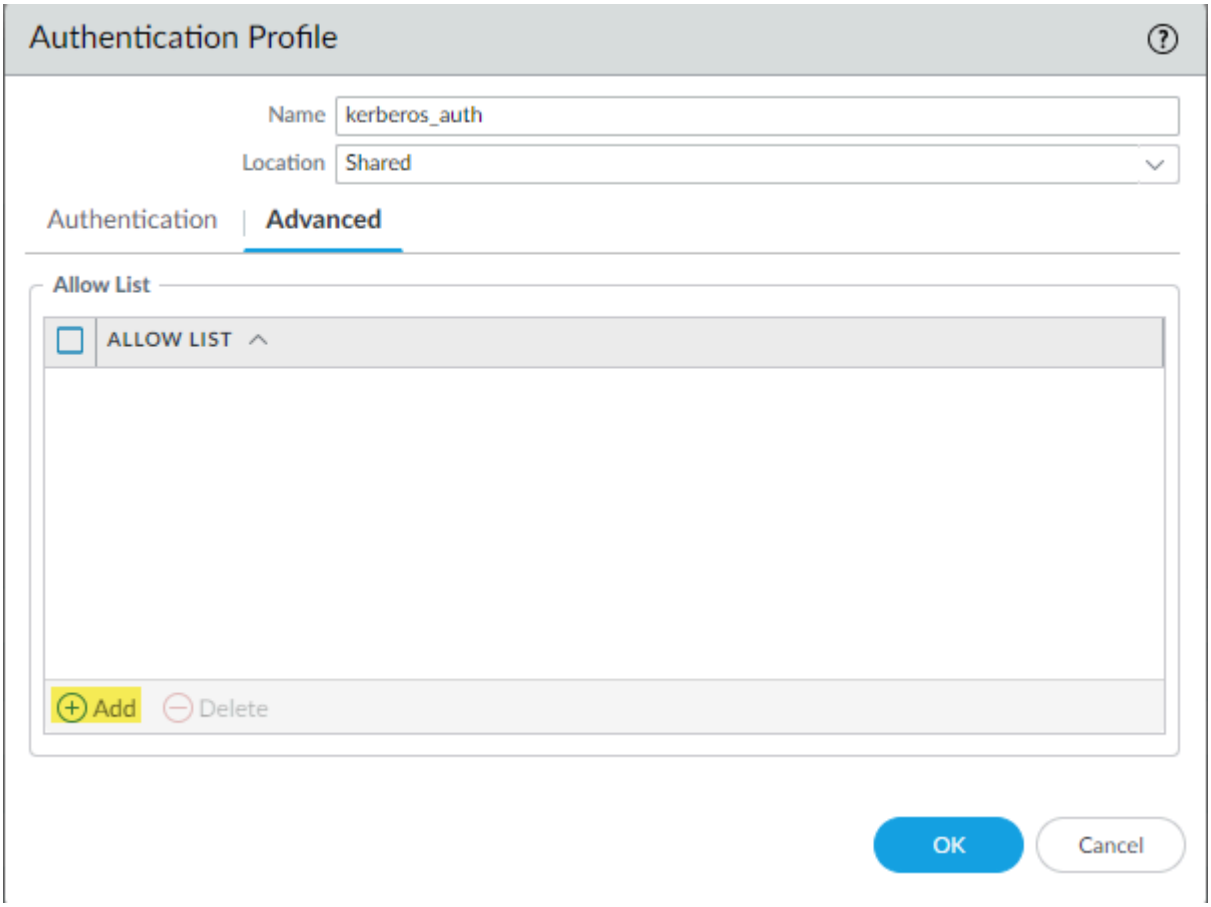
3. 認証プロファイルを識別する **Name**（名前）を入力します。
4. **Kerberos Realm**（**Kerberos** レルム）を入力して（最大 127 文字）、ユーザーのログイン名のホスト名部分を指定します。たとえば、ユーザー アカウント名 user@EXMP.COM には、realm EXMP.COM があります。
5. 先ほど作成したKerberos Keytabをインポートします。



6. このプロファイルで認証できるユーザーを追加します。

©2025 Palo Alto Networks, Inc.

- [詳細設定] > [+追加]を選択します。
- すべてのユーザーを選択するには、 すべてを選択します。
- Cloud Identity Engineを使用してユーザーのリストを作成する場合は、リストからユーザーを選択するか、 すべて を選択してすべてのユーザーの認証を許可します。
- Kerberos を使用してログインできるローカル ユーザーを追加するには、ユーザー名を入力します。
  - ユーザー認証とユーザー マッピングを構成するときは、userPrincipalName (UPN) の形式を使用します。他の形式 (samAccountName など) はサポートされていません。
  - Unicode文字のユーザー名はサポートされていません。



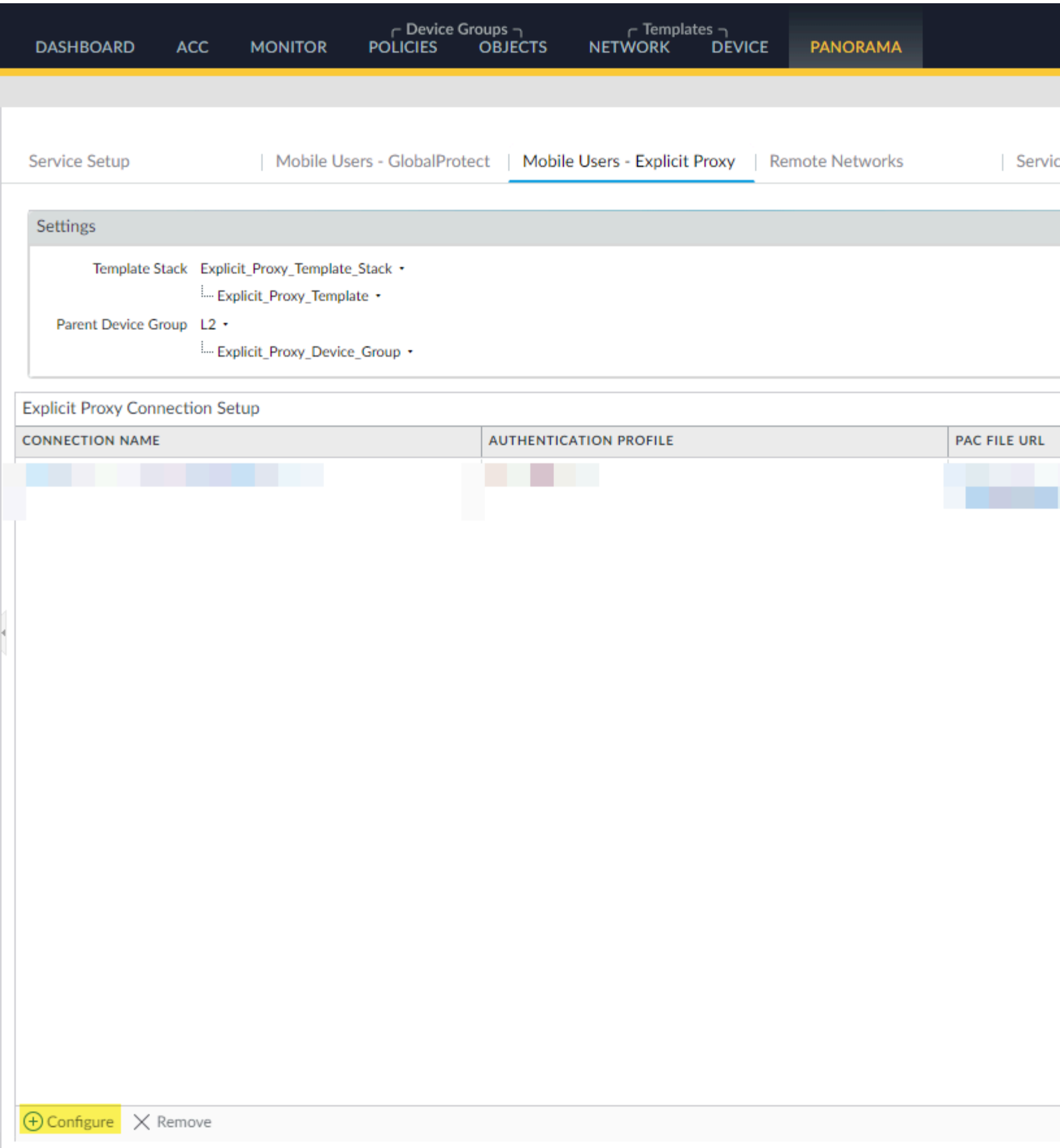
7. 変更を保存します。

©2025 Palo Alto Networks, Inc.

STEP 2 | 認証プロファイルを認証方法に関連付けます。

1. **[Panorama] > [Cloud Services**（クラウドサービス）**] > [Configuration**（設定）**] > [+ Configure**（+設定）**]**へと移動します。

©2025 Palo Alto Networks, Inc.



©2025 Palo Alto Networks, Inc.

2. 明示型プロキシ **FQDN**を設定します。
3. 作成したKerberosプロファイルを選択します。
4. 変更を保存するには、**[OK]**を選択します。

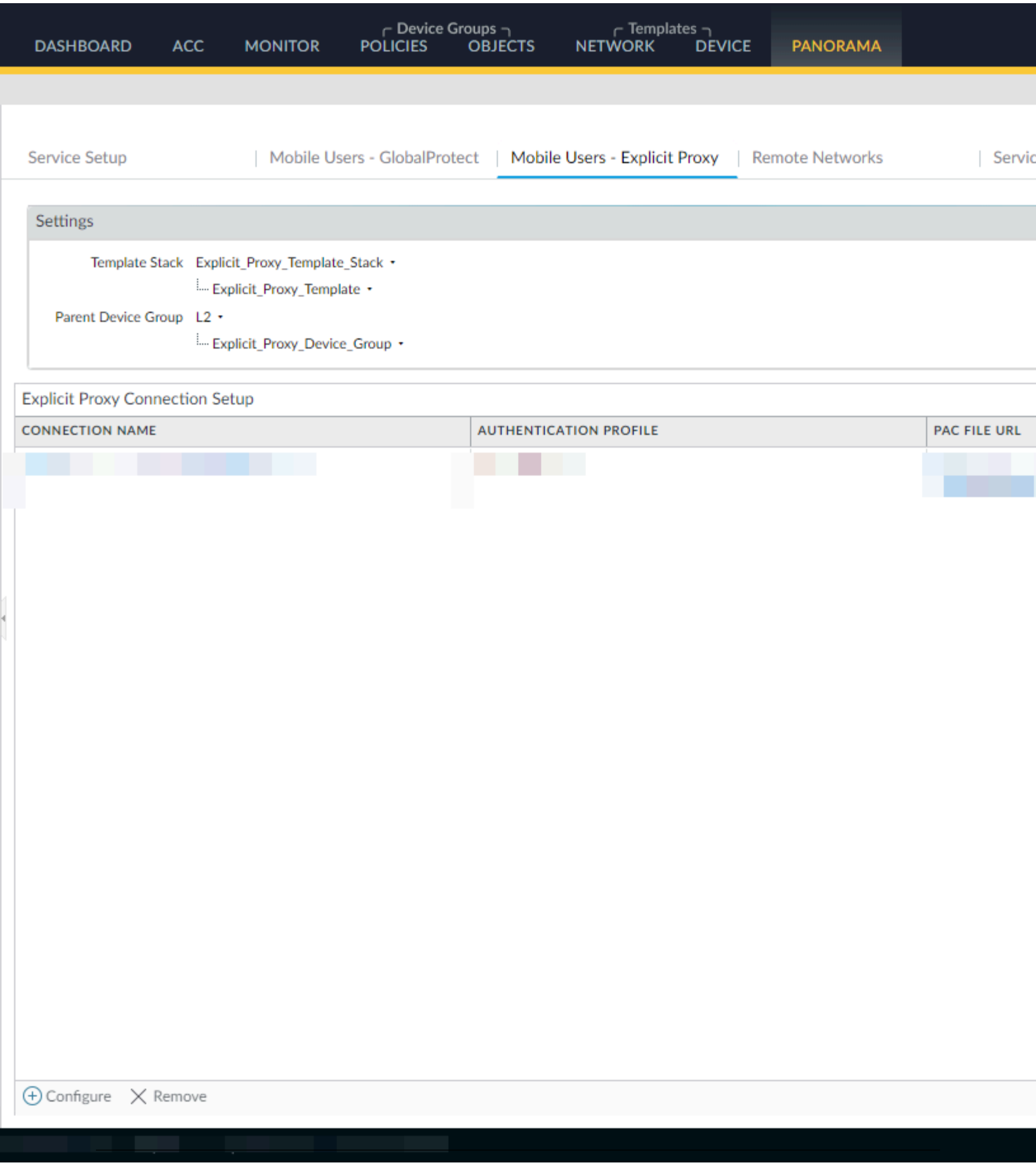
©2025 Palo Alto Networks, Inc.

STEP 3 | (任意) ユーザー、サーバー、IoT デバイス、またはヘッドレス マシンが配置されているブランチまたはキャンパスの場所の出力IPアドレスを、信頼できる明示型プロキシ アドレスのリストに追加します。

特定のIPアドレスの 認証をスキップ する場合、または **ID** の受信 **HTTP/HTTPS** 要求で **X-Authenticated User (XAU)** ヘッダーを使用する場合にのみ、これを実行する必要があります。

1. **[Panorama]** > **[Cloud Services]** > **[Configuration (構成)]** > **[Settings gear (ギアの設定)]** > **[認証設定]**に移動します。

©2025 Palo Alto Networks, Inc.



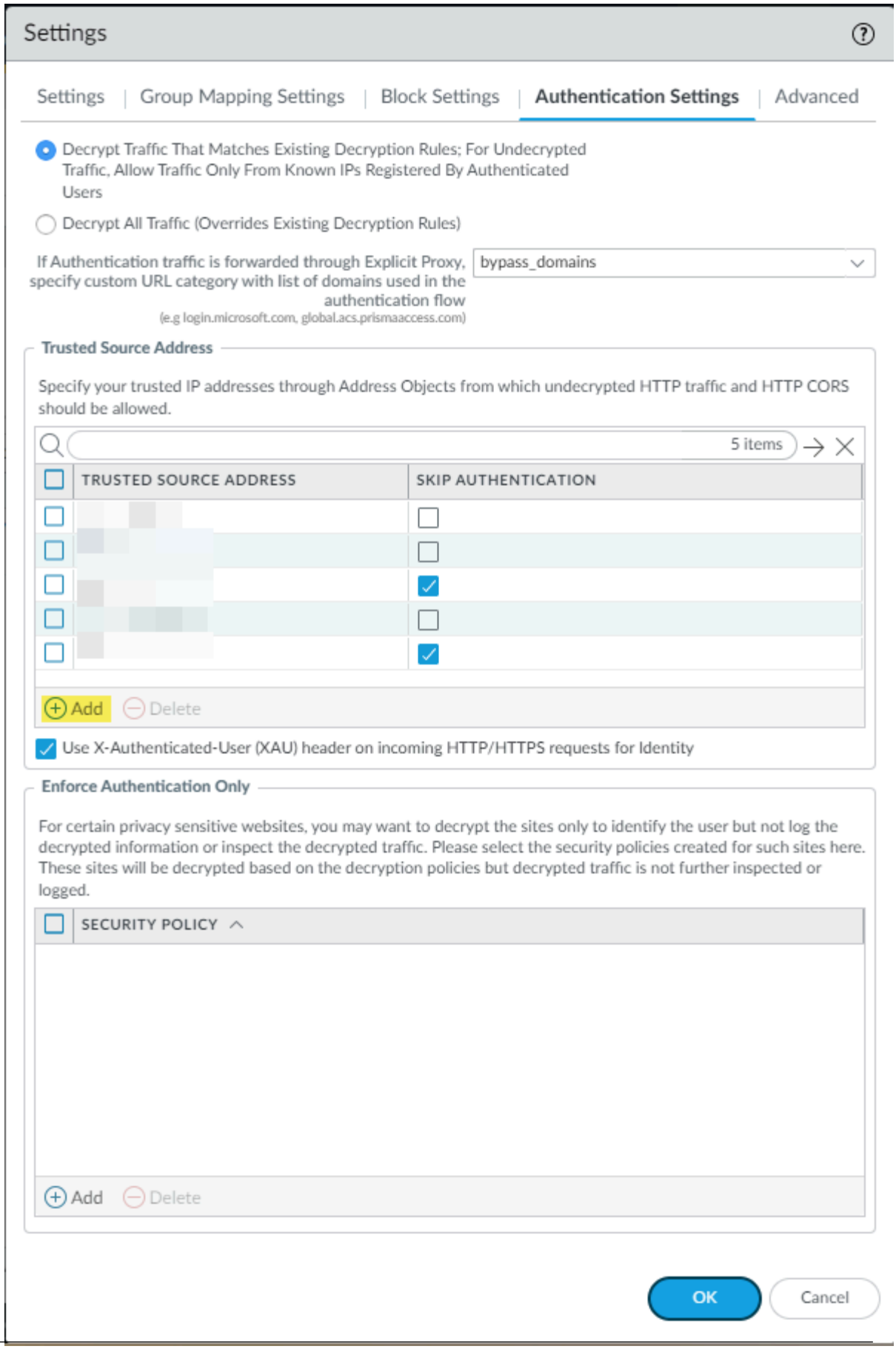
©2025 Palo Alto Networks, Inc.

2. **Trusted Source Address (**信頼できるソース アドレス**)** フィールドにアドレス を追加します 。

   出力エンドポイントIPアドレスを信頼リストに追加しない場合、明示型プロキシはユーザーとマシンにSAMLとKerberosによる認証を強制します。

   最大100,000 個のIPアドレスを入力します。

©2025 Palo Alto Networks, Inc.



©2025 Palo Alto Networks, Inc.

3. 変更を保存するには、**[OK]**を選択します。

STEP 4 | ユーザー認証用のすべて許可ポリシー ルールを作成します。

1. **[Policies**（ポリシー）**]** > **[Pre Rules (**事前ルール**)]** > **[+**追加**]**を選択します。
2. ルールに名前を付けます。
3. ソースを選択します
4. ソースユーザーを **known-user (**既知のユーザー**)**に設定します
5. その他すべての必要な値を **Any (**任意**)**に設定します。
6. **OK** を選択してルールを保存します。

STEP 5 | 設定変更を Commit and Push(コミットおよびプッシュ) します。

STEP 6 | トラフィックと認証ログを表示して、Prisma AccessでKerberos認証が機能していることを確認する。

1. (復号化されたトラフィックのみ)**[Monitor (**監視**)]** > **[Logs (**ログ**)]** > **[Traffic (**トラフィック**)]** に移動して、Kerberos 認証が機能していることを確認します。

   復号化されたトラフィックでは、トラフィック ログにユーザー名が表示されます。

2. (復号化されていないトラフィックのみ)**[Monitor (**監視**)]** > **[Logs (**ログ**)]** > **[Authentication (**認証**)]** に移動し、Kerberos認証が正しく機能していることを確認します。

   次のフィールドには、認証イベントに関する詳細情報が提供されます。

   - オブジェクト- 認証のためにKerberosにリダイレクトされる前にユーザーがアクセスしようとしていたWebサイト。
   - 認証イベント- 認証試行のステータス。

     認証成功は、 認証イベントが成功したことを示します。 認証失敗は、 試行が失敗し、ログが生成されたことを示します。
   - 認証の説明- 認証の試行が失敗した場合、失敗の種類に関する追加情報。

     たとえば、「ユーザーは許可されていません」 は、ユーザーまたはグループが認証にKerberosを使用できないことを示します。これは、認証プロファイルの 許可リスト に追加されていないことが原因である可能性があります。

Cloud Identity Engine 明示型プロキシ(Explicit Proxy)デプロイメントの認証

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

©2025 Palo Alto Networks, Inc.

Cloud Identity Engine (CIE) を使用して、Prisma Access - Explicit Proxy(明示型プロキシ)のデプロイメントにおいてモバイル ユーザーに対してユーザー識別とユーザー認証の両方を提供します。

Cloud Identity Engineは、オンプレミス、クラウドベース、またはハイブリッド ネットワーク環境における集中型クラウドベース ソリューションのユーザー識別とユーザー認証を提供します。Cloud Identity Engineを使用すると、ユーザーとグループに基づいてセキュリティ ポリシーを記述し、動作ベースのセキュリティ アクションを適用してネットワークを保護できます。

オンプレミス、クラウドベース、ハイブリッドのいずれのディレクトリからでも情報を継続的に同期することで、クラウドIDプロバイダーが一時的に利用できなくなった場合でも、ユーザー情報が正確かつ最新の状態に保たれ、マッピングに基づいてポリシーの適用が継続されます。

- 明示的なプロキシデプロイメントのためのCloud Identity Engine認証 (Strata Cloud Manager)
- 明示的なプロキシデプロイメントのためのCloud Identity Engine認証 (Panorama)

明示的なプロキシデプロイメントのための**Cloud Identity Engine**認証 **(Strata Cloud Manager)**

Cloud Identity Engine (CIE) は、Prisma Access - Explicit Proxyのデプロイメントにおいてモバイル ユーザーに対してユーザー識別とユーザー認証の両方を提供します。Cloud Identity Engineは、Explicit Proxy認証キャッシュ サービス(ACS)と統合され、SAML IDプロバイダ(IdP)を使用してExplicit Proxyモバイル ユーザーに認証を提供します。

Cloud Identity Engineを使用してモバイル ユーザー - 明示的プロキシ デプロイメントの認証を構成するには、次の手順を実行します。

STEP 1 | Prisma Access (Managed by Strata Cloud Manager)でテナントに明示的なプロキシをセットアップします 。

明示的プロキシを構成する前に、明示的プロキシの動作と、構成時に使用するガイドラインを理解しておいてください。

複数のテナントがある場合は、必要なテナントごとに明示的なプロキシを構成します。

©2025 Palo Alto Networks, Inc.

STEP 2 | ハブにログインし、Cloud Identity Engineアプリから認証タイプと認証プロバイダを設定します。

ハブ内のアプリは 、テナント別またはサポート アカウント別に表示できます。

1. Cloud Identity EngineでSAML認証タイプを構成します 。

   Cloud Identity Engineスタート ガイドには、Cloud Identity EngineでSAML IdPを構成するために必要な手順が記載されています。

   - Cloud Identity EngineでAzureをIdPとして設定する
   - Cloud Identity EngineでOktaをIdPとして設定する
   - Cloud Identity EngineでPingOneをIdPとして設定する
   - Cloud Identity EngineでPingFederateをIdPとして設定する
   - Cloud Identity EngineでGoogleでIdPとして設定する

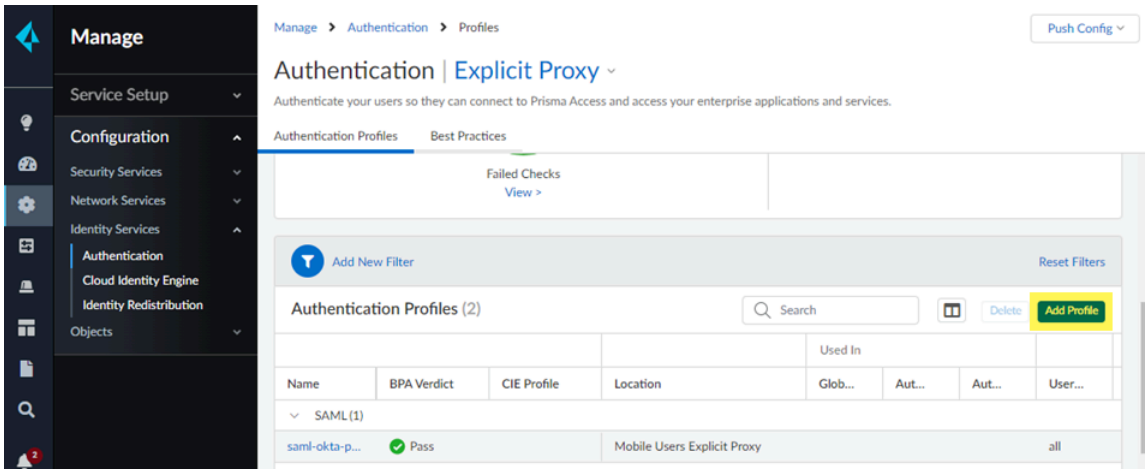
   シングル ログアウトはサポートされていないため、設定しないでください。
2. Cloud Identity Engineで認証プロファイルを設定し 、この認証方法を使用できるユーザーとグループを選択します。

   このプロファイルは、後の手順でPrisma Access (Managed by Strata Cloud Manager)で認証プロファイルを作成するときに指定します。

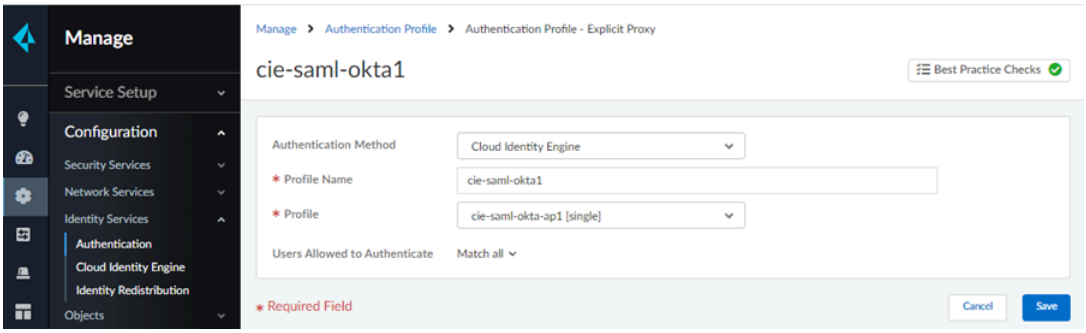
©2025 Palo Alto Networks, Inc.

STEP 3 | Prisma Access (Managed by Strata Cloud Manager)に戻り、クラウド認証エンジンで使用する認証プロファイルを作成します。

1. **[Manage (管理)] > [Configuration (構成)] > [NGFWとPrisma Access] > [Identity Services (IDサービス)] > [Authentication (認証)]**に移動します。次に、スコープを[明示的なプロキシ]に設定し、認証プロファイルを追加します (プロファイルの追加)。



2. **Cloud Identity Engine**の認証方法を選択します。
3. プロファイルに プロファイル名を付けます。
4. 前の手順で作成したCloud Identity Engine認証プロファイルを選択します。

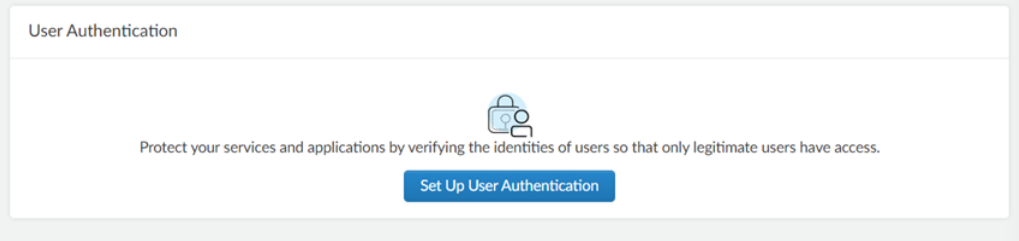


5. 変更を保存します。

©2025 Palo Alto Networks, Inc.

STEP 4 | 明示的プロキシでユーザー認証を設定します。

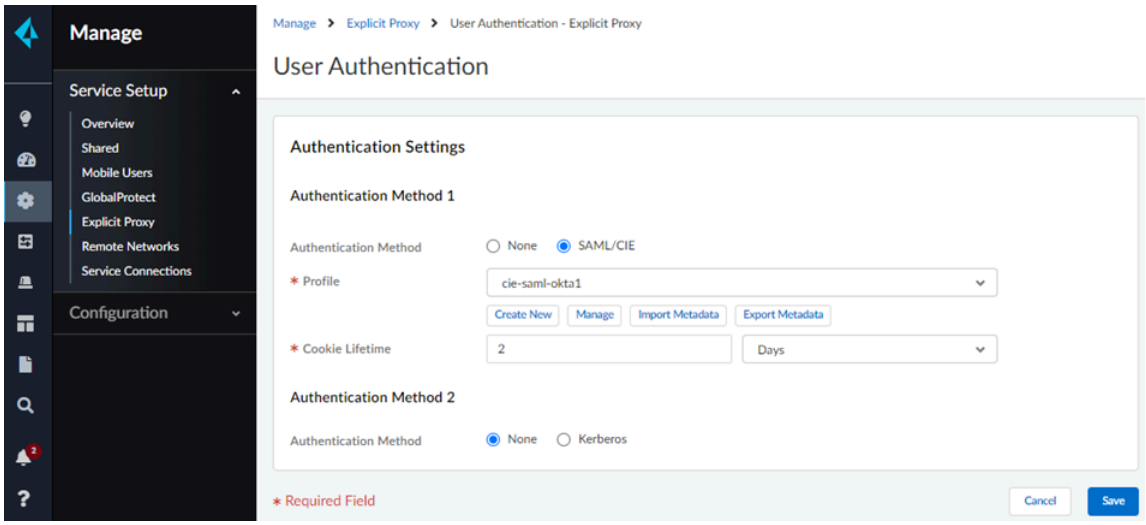
1. [ワークフリー] > [**Prisma Access**のセットアップ] > [明示型プロキシ] および[ユーザー認証の設定]に移動します。



2. **SAML/CIE**の認証方法を選択します。
3. Cloud Managed Prisma Accessで作成した認証プロファイルを選択します。
4. ユーザーの認証資格情報を保存する**Cookie** の有効期間を指定します。

   IdPがユーザーを認証すると、Prisma Accessはユーザーの認証状態を認証キャッシュサービス (ACS) に保存します。認証の有効期間は、ここで指定したCookieの有効期間の値に基づきます。

   Cookieの有効期間が切れる前にユーザーが大きなファイルをダウンロードできない、またはユーザーが 1 つのWebサイトに長時間アクセスするとクッキーが期限切れになるなどの問題を回避するために、Palo Alto Networks では、**Cookie**の有効期間を少なくとも 1 日に設定することをお勧めしています。明示的プロキシ ユーザーにCookieの有効期限の問題がある場合は、別のWebサイトを参照してACSに再認証し、ACS Cookieを更新できます。

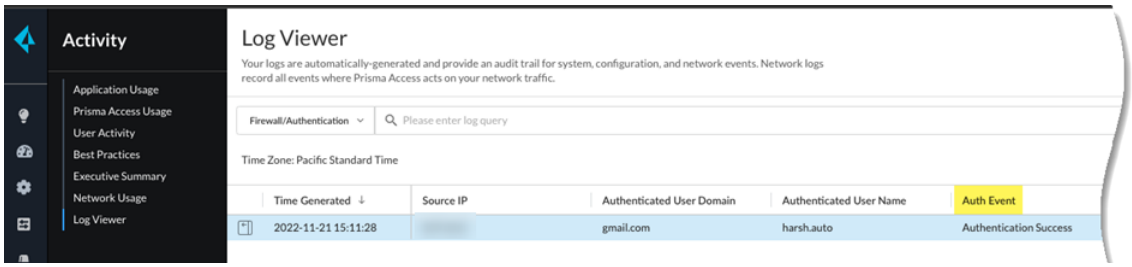


5. 変更を保存します。

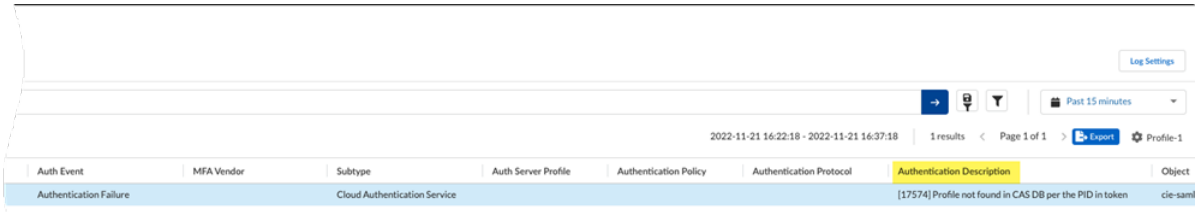
©2025 Palo Alto Networks, Inc.

STEP 5 | Cloud Identity Engineが明示的プロキシ モバイル ユーザーを正常に認証していることを確認します。

1. Prisma Access (Managed by Strata Cloud Manager)から、[インシデントとアラート] > [ログ ビューア] > [ファイアウォール/認証]を選択します。
2. 認証イベントのステータスを表示します。

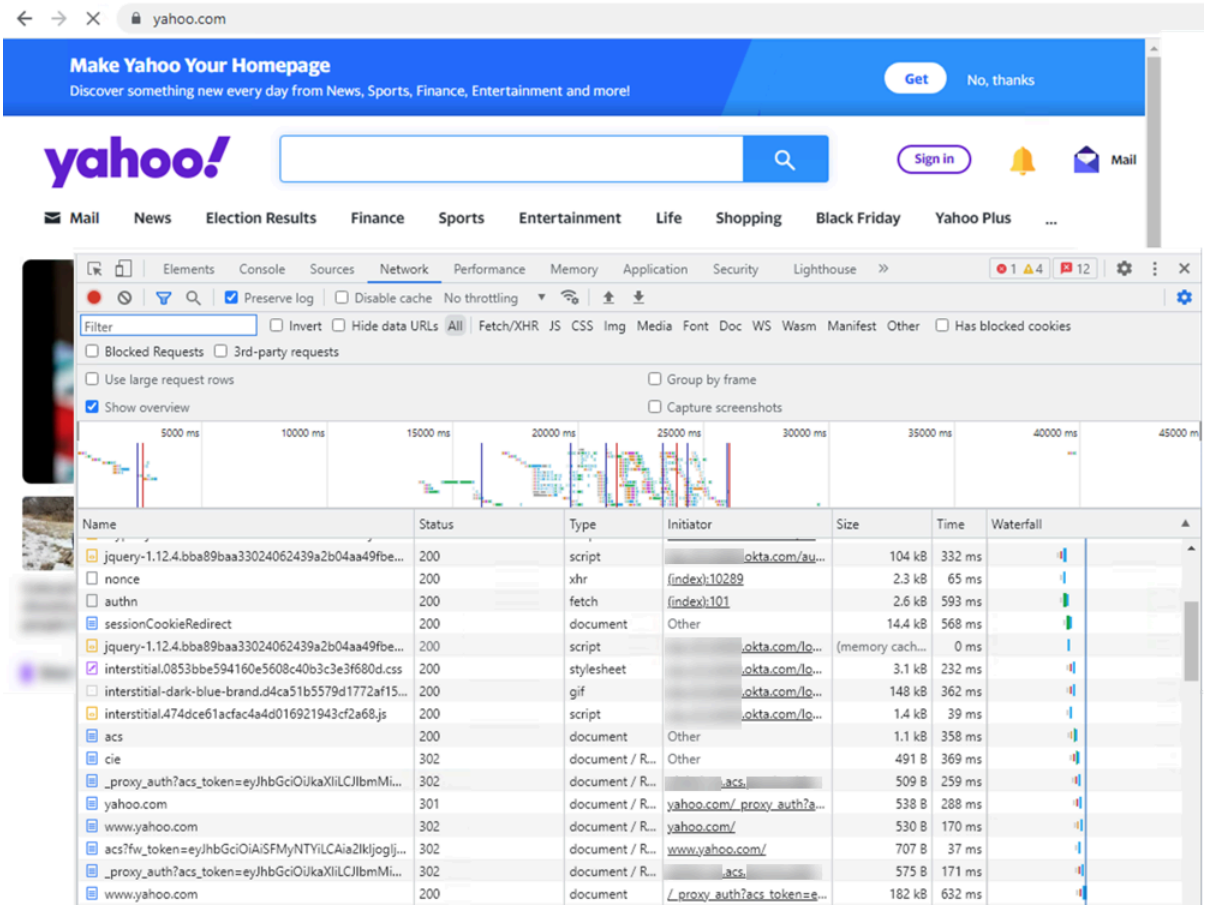


認証が失敗した場合は、認証の説明を参照して失敗の詳細を確認してください。



3. モバイル ユーザーのエンドポイントから、開発ツールを使用してCloud Identity Engine認証フローを表示します。

 ©2025 Palo Alto Networks, Inc.



明示的なプロキシデプロイメントのための**Cloud Identity Engine**認証 **(Panorama)**

Cloud Identity Engineを使用してPrisma Access (Managed by Panorama)明示プロキシ モバイルユーザーを認証する

リモートネットワークのプロキシモード

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) Prisma Access 環境の明示型プロキシでプライベート ソースIPベースの可視性と適用を有効にする場合は、アカウント チームに連絡して詳細を確認してください。	• Prisma Accessライセンス リモートネットワーク用のプロキシモードには、Prisma Accessモバイルユーザーライセンスと Prisma Accessリモートネットワークライセンスが必要です。

リモート ネットワーク上のプロキシ モードは、ネットワークまたはコンプライアンス上の理由により PAC ベースの接続方法を必要とするブランチ内のユーザーとサーバーのアウトバウンド インターネット トラフィックを保護するのに役立ちます。

リモート ネットワークのプロキシモードを使用すると、次のことが可能になります。

©2025 Palo Alto Networks, Inc.

- デフォルト以外のルートを使用するブランチ サイトからのインターネットへのトラフィックを保護します。
- データ センターや本社サイトにバックホールすることなく、ブランチからインターネットへのトラフィックを保護します。
- プライベート IP アドレス経由でPrisma Access明示型プロキシに接続します。

  Prisma Access は、トラフィックを明示型プロキシに転送するために使用する、グローバルに 4 つのエニーキャスト IP アドレスと、リモート ネットワークごとに 1 つのユニキャスト IP アドレスを提供します。
- セキュリティ制御を実施し、ブランチ内のシステムのソースIPに基づいて可視性を獲得します。
- 送信元 IP アドレスに基づいてサーバーの認証をスキップします。
- IPSecトンネルを通して、ブランチからPrisma Accessに接続します。
- 1000 Mbps を超える帯域幅が必要な場合は、複数のリモート ネットワーク接続を使用して高帯域幅のリモート ネットワーク接続を作成し、各接続で明示型プロキシ エニーキャスト アドレスとユニキャスト アドレスを指定できます。

次の図は、デフォルト ルートが構成されていないサイト用に構成されたリモート ネットワークを示しています。明示型プロキシを使用してサイトのユーザーとヘッドレス デバイスを保護するために、管理者は次の構成変更を行いました。

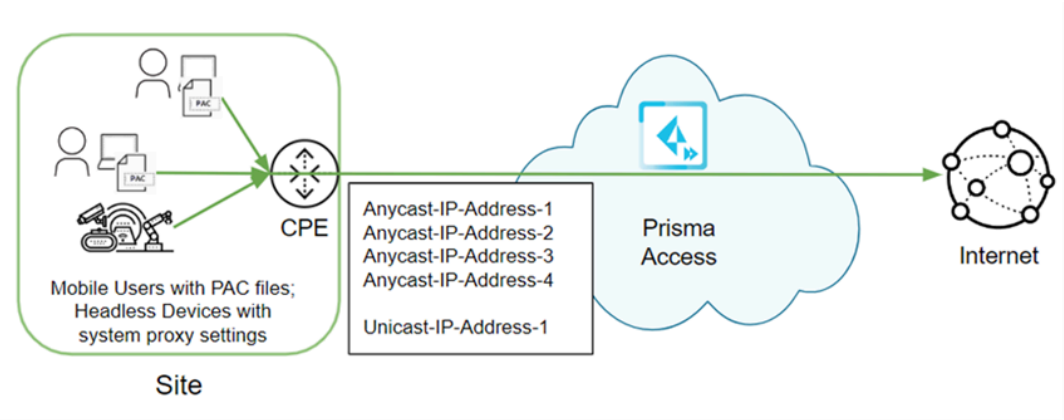
- オンボード リモート ネットワークと明示型プロキシのロケーションで、Prisma Accessがインフラストラクチャ・サブネットから取得するエニーキャストとユニキャストのIPアドレスを取得しました。

  明示型プロキシ向けトラフィックのホスト名を作成し、そのホスト名に明示型プロキシのユニキャストおよびエニーキャスト *IP* アドレスを追加することもできます。
- 明示型プロキシ トラフィックをこれらのエニーキャスト アドレスとユニキャスト アドレスに転送するように CPE を構成しました。

  PAC ファイル内のエニーキャスト IP アドレスを使用して、Prisma Accessに、オンボーディングされているリモートネットワーク トンネルから明示型プロキシにトラフィックを転送するように選択させます。Prisma Accessに特定のリモート ネットワーク トンネルを経由してトラフィックを転送させるには、ユニキャストアドレスを使用します。この例では、トラフィックは 1 つのリモート ネットワーク IPSec トンネルのみを通過するため、エニーキャスト アドレスまたはユニキャスト アドレスのいずれかを使用できます。
- これらの IP アドレスを、ユーザーのエンドポイントの PAC ファイルとヘッドレス デバイスのシステム プロキシ設定で指定します。

設定が完了したら、 Prisma Accessはリモート ネットワーク トンネルからのトラフィックを明示型プロキシに転送します。

©2025 Palo Alto Networks, Inc.



- Strata Cloud Manager
- Panorama

リモートネットワークのプロキシモード（Strata Cloud Manager）

Cloud Managed Prisma Accessの明示型プロキシを使用してリモート ネットワークのユーザーを保護するには、次の手順を実行します。

STEP 1 | 明示型プロキシ設定を構成し、追加する明示型プロキシの場所をオンボードします。

STEP 2 | まだリモート ネットワークをオンボードしていない場合はオンボードします。

*Prisma Access*明示型プロキシがサポートされている場所では、リモート ネットワークを有効にする必要があります。

STEP 3 | 構成をプッシュして、 **[Push (プッシュ)]** スコープで **Mobile Users—Remote Workforce (**モバイル ユーザー - リモート ワークフォース**)** と リモート ネットワーク が選択されていることを確認します。

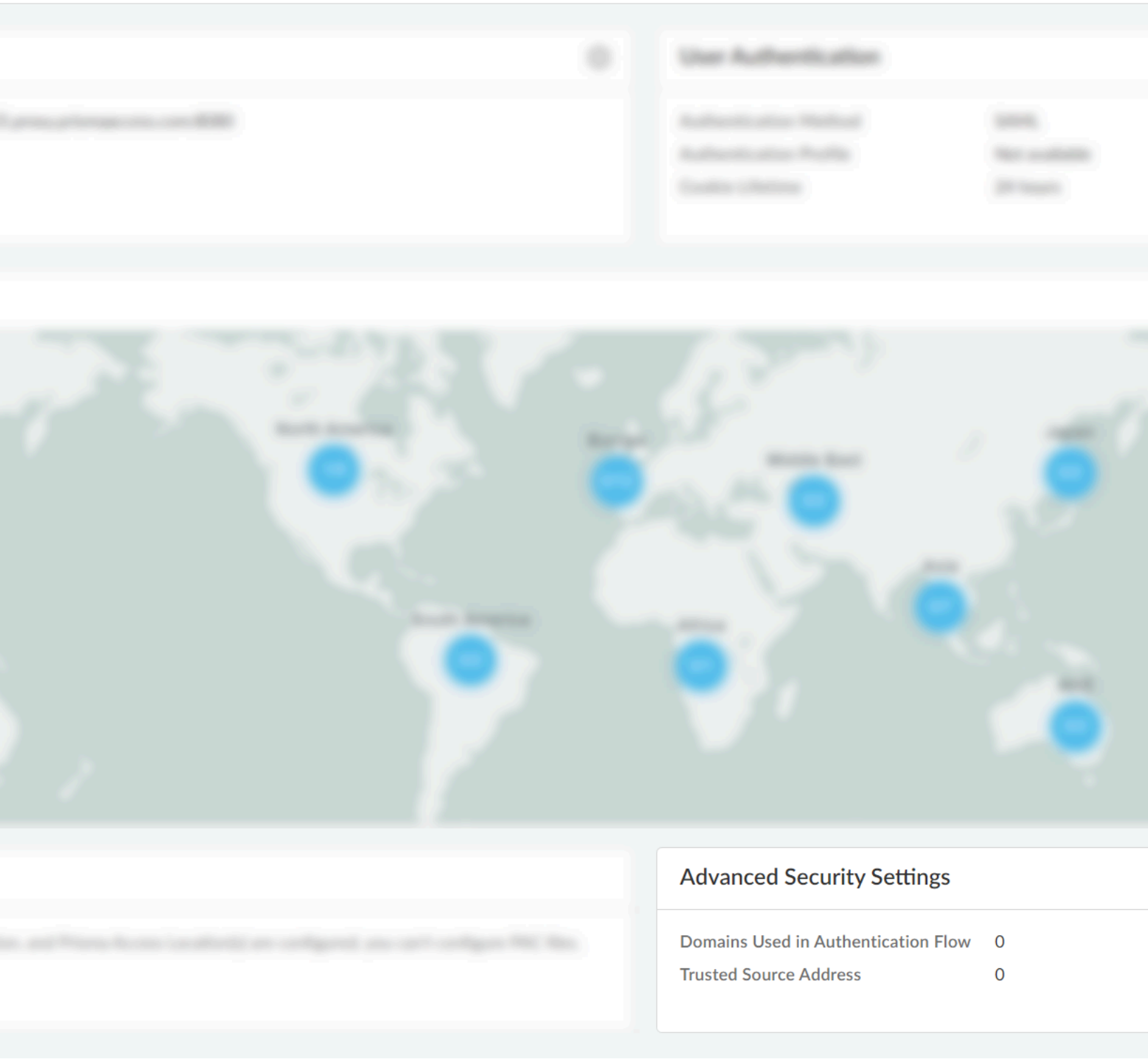
プッシュ操作は、明示型プロキシをリモート ネットワークに統合するために必要なエニーキャスト アドレスを取得します。

©2025 Palo Alto Networks, Inc.

STEP 4 | 明示型プロキシ/リモート ネットワークの展開に使用するエニーキャストIPアドレスを取得します。

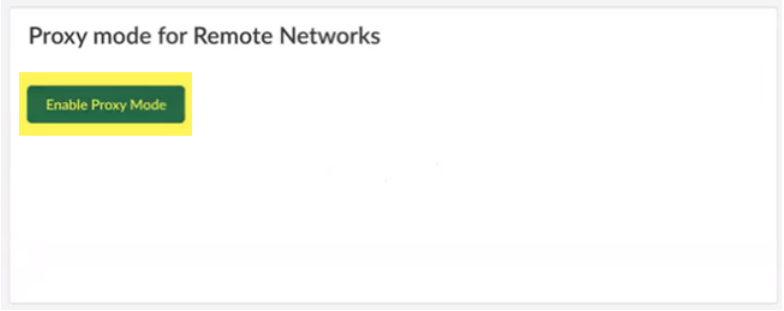
1. **[ワークフロー] > [Prisma Accessセットアップ] > [Explicit Proxy (明示型プロキシ)] > [Advanced Security Settings (詳細セキュリティ設定)]**に移動します。

©2025 Palo Alto Networks, Inc.

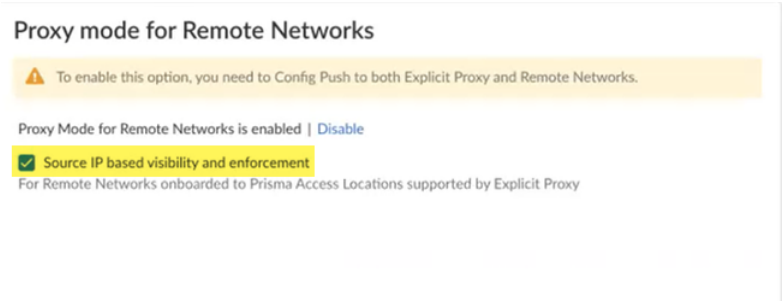


2. プロキシモードを有効にします。

©2025 Palo Alto Networks, Inc.



3. 明示型プロキシにトラフィックを転送しているブランチ ロケーションのシステムの送信元IPアドレスを活用するには、[送信元**IP**ベースの可視性と適用]を選択します。
   この機能には次の要件があります:
   - 最低限 Prisma Access 10.2.4 のデータプレーン
   - 明示型プロキシでサポートされているリモート ネットワークのロケーションのみを使用する必要があります。



4. リモート ネットワーク上のエニーキャストおよびユニキャスト**IP**にバインドされたトラフィックを許可するポリシーを追加します。送信元**IP**の可視性と適用を有効にしてい

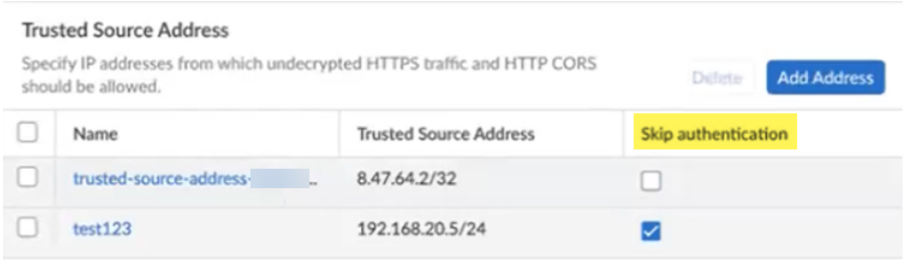
©2025 Palo Alto Networks, Inc.

る場合は、明示型プロキシのセキュリティ ポリシーの送信元IP フィールドを使用してトラフィックを保護します。リモート ネットワークには追加のポリシーが必要です。

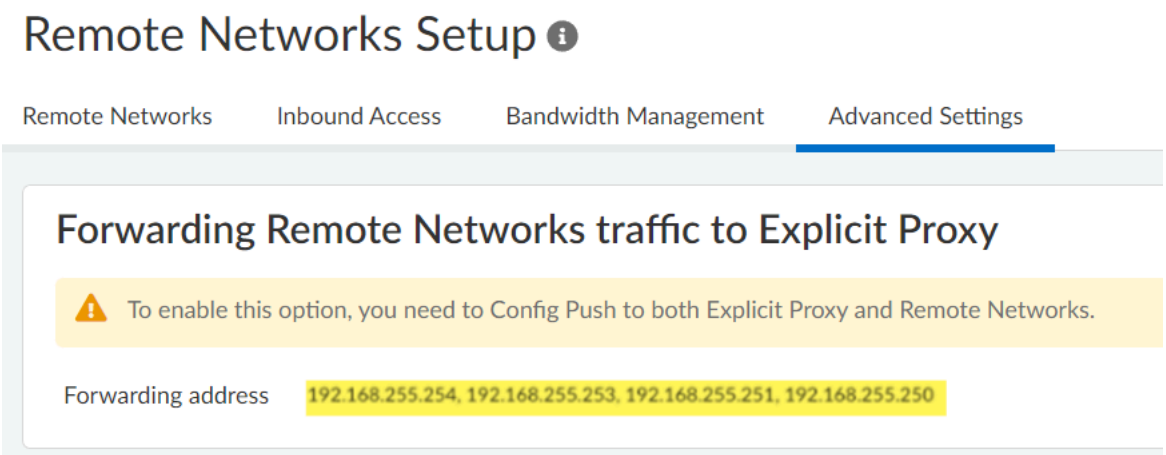
5. (任意) 入力した信頼できるソース アドレスの認証をバイパスするには、**[Trusted Source Address (信頼できる送信元アドレス)]** 領域で認証をスキップするIPアドレスを指定し、**[Skip authentication (認証をスキップ)]**を選択します。

   ソースIPベースの可視性と強制による認証スキップ を使用すると、認証できないヘッドレスシステムの認証をスキップし、セキュリティポリシーを設定し、Prisma Access明示型プロキシのトラフィックの可視性を得ることができます。

   *IP*アドレスまたはサブネットのいずれかを追加できます。サブネットを拡張すると、最大*100,000*個の*IP*アドレスがサポートされます。



6. **[Workflows (ワークフロー)]** > **[Prisma Accessセットアップ]** > **[Remote Networks (リモートネットワーク)]**へ移動します。
7. 構成をプッシュして、 **[Push (プッシュ)]** スコープで **Mobile Users—Remote Workforce (モバイル ユーザー - リモート ワークフォース)** と リモート ネットワーク が選択されていることを確認します。
8. リモート ネットワーク設定の 詳細設定 に移動し、明示型プロキシにトラフィックを転送するために使用されるエニーキャストIPアドレスを見つけます。



STEP 5 | (任意) 明示型プロキシ/リモート ネットワークのデプロイメントに使用するユニキャスト アドレスを検索します。

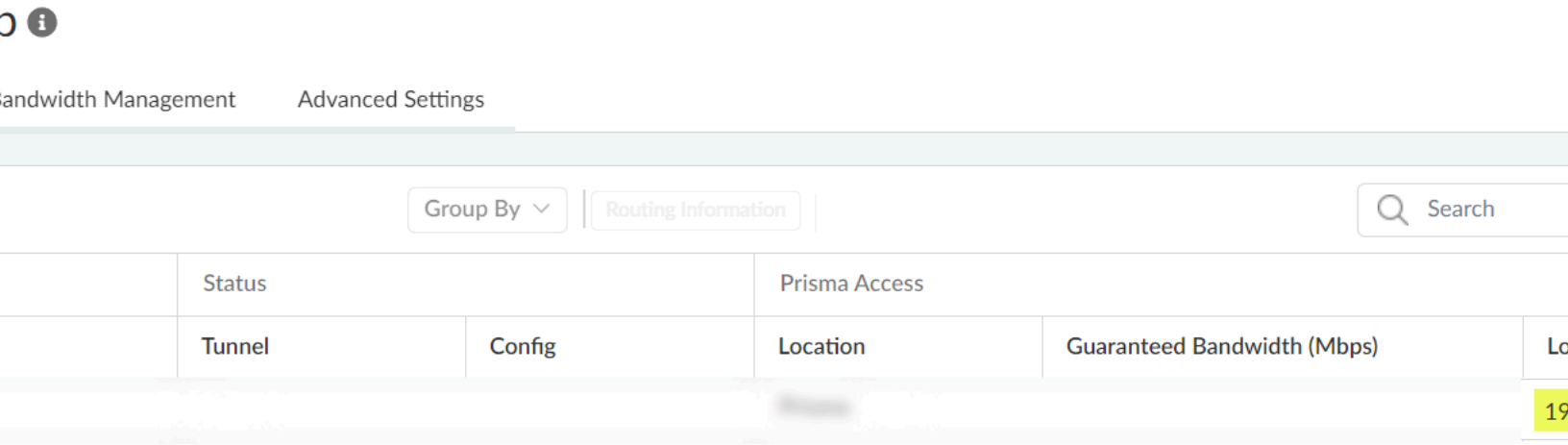
特定のリモート ネットワークをターゲットにしてトラフィックを明示的プロキシに転送する場合にのみ、PACファイル内のユニキャストIPアドレスを使用します。デプロイされたすべ

©2025 Palo Alto Networks, Inc.

てのリモート ネットワークを使用してトラフィックを明示型プロキシに転送する場合は、エニーキャスト アドレスを使用します。

1. **[Workflows (ワークフロー)] > [Prisma Accessセットアップ] > [Remote Networks (リモートネットワーク)]**へ移動します。
2. ループバック **IP**アドレスをメモします。

   IPv4アドレスとIPv6アドレスがある場合は、IPv4アドレスをメモしてください。



リモートネットワークのプロキシモード（Panorama）

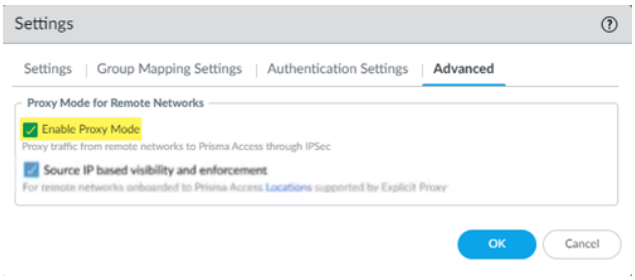
Prisma Access (Managed by Panorama) Accessの明示型プロキシを使用してリモート ネットワークのユーザーを保護するには、次の手順を実行します。

STEP 1 | 明示型プロキシデプロイメントを設定し、追加する明示型プロキシの場所をオンボードします。

©2025 Palo Alto Networks, Inc.

STEP 2 | 明示型プロキシ/リモート ネットワークのデプロイメントに使用するエニーキャストIPアドレスを取得します。

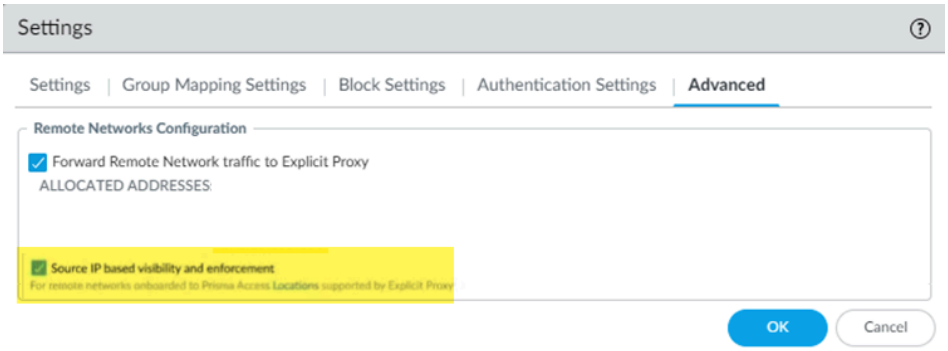
1. **[Panorama]** > **[クラウド サービス]** > **[構成]** > **[モバイル ユーザー - 明示的なプロキシ]**を選択します。
2. **Settings**（設定）を編集するには、歯車型アイコンを選択します。
3. **[プロキシモードを有効にする]**を選択します。



4. 明示型プロキシにトラフィックを転送しているブランチ ロケーションのシステムのプライベートIPアドレスを活用するには、**[送信元IPベースの可視性と適用]**を選択します。

   この機能には次の要件があります:

   - 最小値 10.2.4のPrisma Accessデータプレーン
   - Cloud Servicesプラグイン4.1以上を使用したPrisma Access (Managed by Panorama)デプロイメント
   - 明示型プロキシでサポートされているリモート ネットワークのロケーションのみを使用する必要があります。



5. リモート ネットワーク上のエニーキャストおよびユニキャストIPにバインドされたトラフィックを許可するポリシーを追加します。送信元IPの可視性と適用を有効にしてい

©2025 Palo Alto Networks, Inc.

る場合は、明示型プロキシのセキュリティ ポリシーの送信元**IP** フィールドを使用してトラフィックを保護します。リモート ネットワークには追加のポリシーが必要です。

6. (任意) 認証設定の下 で、暗号化されていないHTTPまたはHTTP Cross-Origin Resource Sharing (CORS)トラフィックが**Trusted Source Address Auth Bypass (**信頼できる送信元アドレス認証バイパス**)**に許可されるべきIPアドレスを入力します。

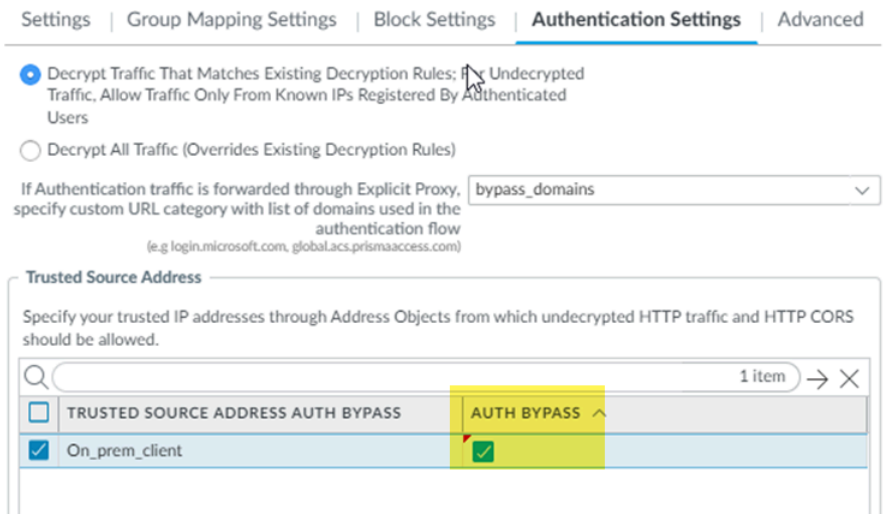
   IPアドレスをIPアドレスベースのアドレスオブジェクトに追加し、 フィールド内の Address オブジェクトを追加します。

   最大100,000 個のアドレスを入力します。アドレスオブジェクトがIPアドレスのみを使用していることを確認してください。

7. (任意) 入力した信頼できる送信元アドレスの認証をバイパスするには、 **Auth Bypass (**認証バイパス**)**を選択します。

   ソース**IP**ベースの可視性と強制による**Auth Bypass (**認証バイパス**)** を使用すると、認証できないヘッドレスシステムの認証をスキップし、セキュリティポリシーを設定し、明示型プロキシのトラフィックの可視性を得ることができます。

   *IP*アドレスまたはサブネットのいずれかを追加できます。サブネットを拡張すると、最大*100,000*個の*IP*アドレスがサポートされます。



8. **[Panorama] > [Cloud Services**（クラウドサービス）**] > [Configuration**（設定）**] > [Remote Networks**（リモートネットワーク）**]**を選択します。
9. リモート ネットワーク ロケーションにオンボードします (していない場合)。

   *Prisma Access*明示型プロキシがサポートされている場所では、リモートネットワークを有効にする必要があります。

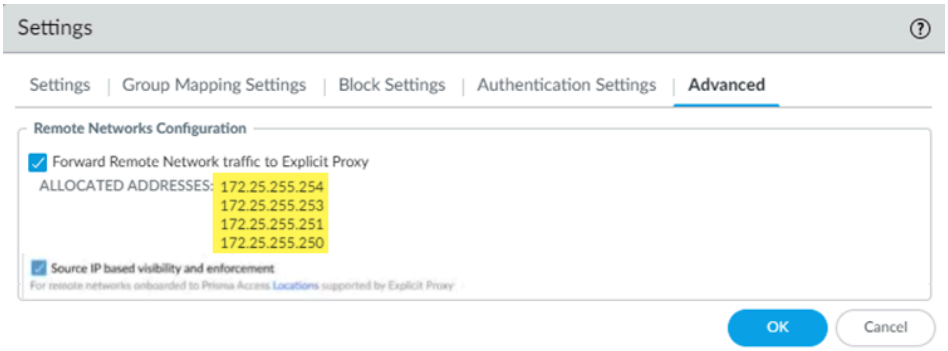
10. **Commit**（コミット） **> Commit and Push**（コミットしてプッシュ）をクリックします。
11. [選択内容を編集]をクリックし、**[Prisma Access]**タブで**[Push Scope (**スコープをプッシュ**)]**に[ネットワーク用**Prisma Access]**が選択されていることを確認し、**[OK]**をクリックする。

©2025 Palo Alto Networks, Inc.

12. 変更を **Commit and Push**（コミットしてプッシュ）します。

    明示型プロキシ／リモートネットワークのデプロイメントで使用されるIPアドレスをPrisma Accessが取得するには、リモート・ネットワークのコミットとプッシュを実行する必要があります。

13. 明示型プロキシの設定に戻ります (**[Panorama]** > **[Cloud Services (クラウドサービス)]** > **[Configuration (構成)]** > [モバイル ユーザ - 明示型プロキシ] > **[Settings (設定)]** > **[Advanced (詳細設定)]**)。次に、リモートネットワークの設定で確認することができる割り当てられたアドレスをメモします。



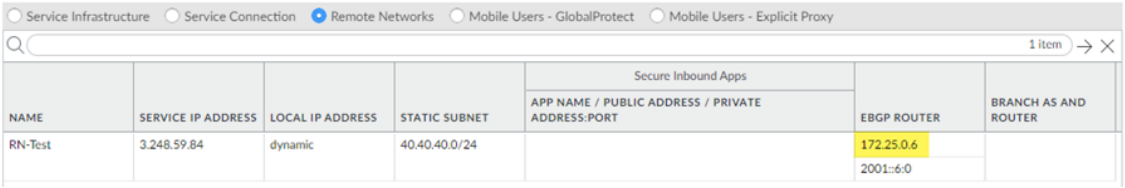
STEP 3 | (任意) 明示型プロキシ/リモート ネットワークのデプロイメントに使用するユニキャスト アドレスを検索します。

特定のリモート ネットワークをターゲットにしてトラフィックを明示的プロキシに転送する場合にのみ、PACファイル内のユニキャストIPアドレスを使用します。デプロイされたすべてのリモート ネットワークを使用してトラフィックを明示型プロキシに転送する場合は、エニーキャスト アドレスを使用します。

1. **[Panorama]** > [クラウドサービス] > [ステータス] > [ネットワークの詳細] > [リモートネットワーク]を選択します。
2. **EBGP**ルータのアドレスをメモしてください。

   IPv4 アドレスと IPv6 アドレスがある場合は、IPv4 アドレスをメモします。

   このアドレスは、ループバック アドレスとも呼ばれます。設定を変更して*EBGP*ルーターのアドレスが変更された場合は、*Prisma Access*レガシーAPIを使用してループバック*IP*アドレスを取得できます。



STEP 4 | エンドポイントがエニーキャストおよびユニキャストIPアドレスを介して明示型プロキシにトラフィックを転送できるように、ネットワーク内のCPEが正しく設定されていることを確認します。

©2025 Palo Alto Networks, Inc.

明示型プロキシがユーザーを識別する方法

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

明示型プロキシは、次の表に示すように、ユーザーがプロキシで認証する方法に応じて、トラフィック ログ内のユーザーを識別します。

認証タイプ	トラフィック ログにおけるユーザー識別
SAML認証と復号化を使用してログインするユーザー	ユーザー名。
X-Authenticated-User (XAU) ヘッダーを使用する別のプロキシからログインするユーザー	XAUヘッダー情報。 明示型プロキシでは、特定のIPアドレスからのトラフィックのみが認証にXAUを使用できます。アドレス オブジェクトを作成し、XAUの認証を許可するIPアドレスを指定します。次に、明示型プロキシのセットアップ中に、 信頼できる送信元アドレス フィールドにアドレス オブジェクトを追加します。
認証されたクロスオリジンリソース共有（CORS）リクエスト	`swg-authenticated-ip-user`ユーザー。 一部のトラフィックは、ブラウザがCookieを送信したり、CORSリクエストなどの認証リダイレクトを実行したりできない認証済みユーザーから発生します。このような場合、明示型プロキシは `swg-authenticated-ip-user`を トラフィック ログに追加します。
復号化されていないトラフィック（ユーザーが以前に認証したIPアドレスからの復号化されていないトラフィックを明示的なプロキシで許可している場合）	`swg-authenticated-ip-user`ユーザー。 明示型プロキシを指定して、ユーザーが認証したIPアドレスからの暗号化されていないトラフィックを許可することができる。これを行うには、明示型プロキシを設定するときに**[Decrypt traffic that matches existing decryption rules; for undecrypted traffic, allow traffic only from known IPs registered by authenticated users (**既存の復号化ルールに一致するトラフィックを復号化する。復号化されていないトラフィックについては、認証されたユーザーが登録した既知の**IP**からのトラフィックのみを許可する**)]**を指定します。これらの設定では、明示型プロキシによって `swg-`

©2025 Palo Alto Networks, Inc.

認証タイプ	トラフィック ログにおけるユーザー識別
	`authenticated-ip-user` が トラフィック ログに追加されます。
認証をバイパスすることを選択したドメインのトラフィック	*swg-known-auth-bypass* ユーザー。 明示型プロキシを設定するときに、特定のドメインからの認証をバイパスすることを選択できます。これらのドメインからのトラフィックのユーザー名は、ログに *swg-known-auth-bypass*として表示されます。

明示型プロキシ転送プロファイル

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Accessモバイルユーザー ライセンス

明示型プロキシ転送プロファイルを使用すると、複数のPACファイルを使用して、 Prisma Accessに転送するトラフィックを定義できます。転送プロファイルを使用すると、PACファイルの作成と管理の複雑さに対処する代わりに、使いやすい転送ルールを作成するオプションも提供されます。

- 転送プロファイルを使用して複数のPACファイルを定義する
- 転送ルールを使用して明示型プロキシに転送するトラフィックを定義する
- GlobalProtect アプリ設定に転送プロファイルを添付する

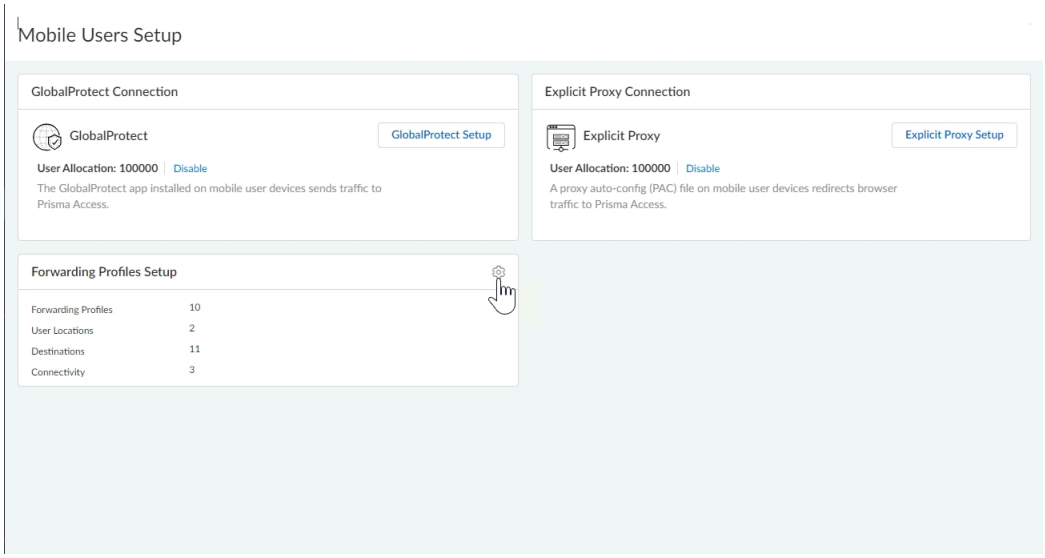
転送プロファイルを使用して複数のPACファイルを定義する

転送プロファイルを使用すると、デプロイメントで複数のPACファイルを同時に使用できるため、どのトラフィックをPrisma Accessに転送するかを定義できます。

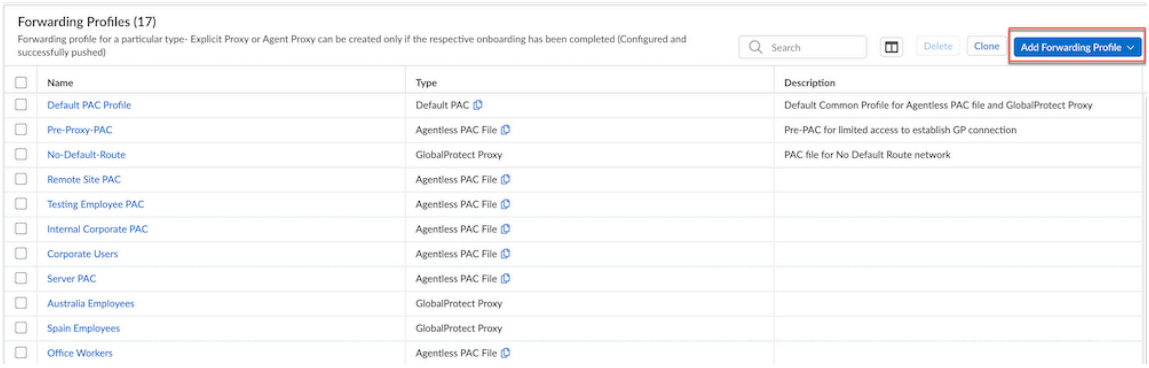
©2025 Palo Alto Networks, Inc.

STEP 1 | ログ転送プロファイルを作成します。

1. Strata Cloud Managerから、**[Workflows (ワークフロー)]** > **[Prisma Accessセットアップ]** > **[Mobile Users (モバイルユーザー)]** > **[Forwarding Profiles Setup (転送プロファイルセットアップ)]**を選択します。



2. 転送プロファイルの追加。



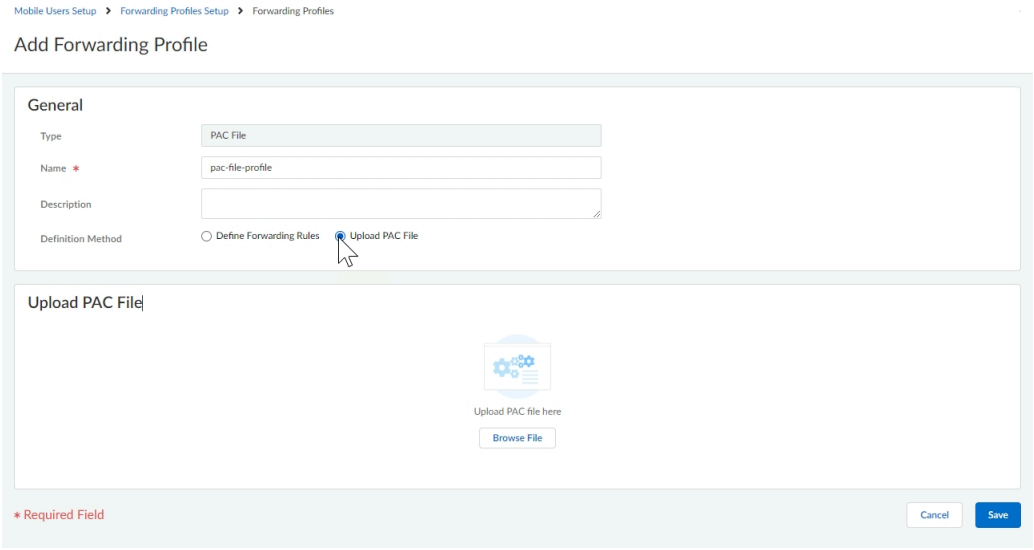
STEP 2 | **PAC**ファイルを選択します。

PACファイル は Prisma Access明示型プロキシのためのものです。**GlobalProtect Proxy**はGlobalProtect をプロキシ モードで使用するためのものです。

©2025 Palo Alto Networks, Inc.

STEP 3 | PACファイルをアップロードします。

1. 既存の PACファイルをアップロードするか、PAC ファイル ガイドラインを使用してPACファイルを作成するには **[PACファイルのアップロード]** を選択します。



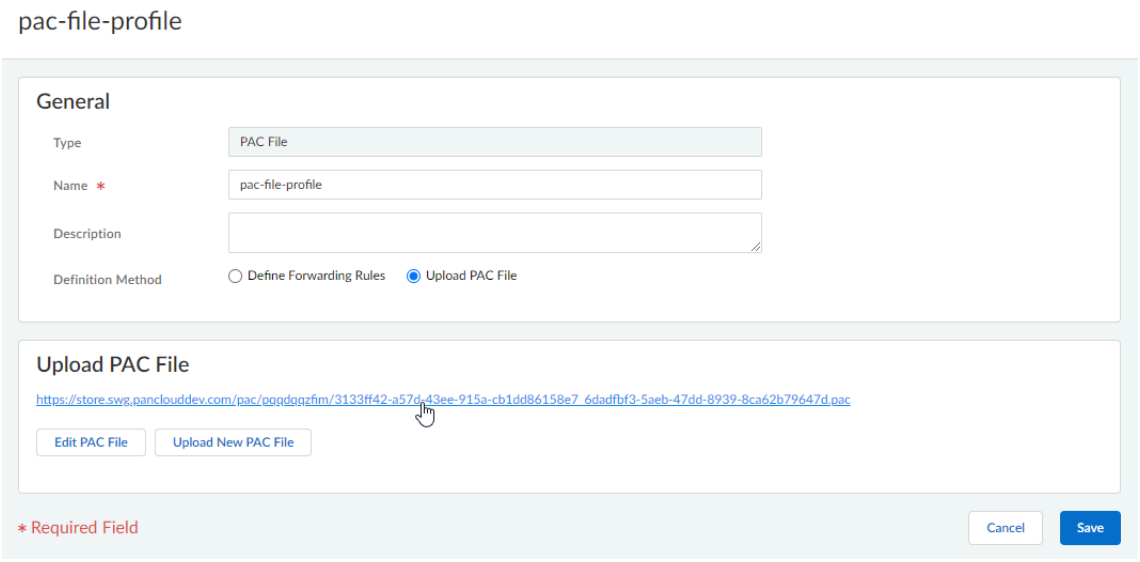
2. ファイルを参照して 、ファイル システムでPACファイルを参照します。
3. プロファイルを保存します。

STEP 4 | 前の2つの手順を繰り返して、別のPACファイルを使用して別の転送プロファイルを作成します。

両方のPACファイルがデプロイメント内で同時に動作するようになりました。

STEP 5 | PACファイルのURLを取得します。

1. PACファイルをアップロードしたプロファイルに戻ります。
   PACファイルがホストされているURLが表示されます。



©2025 Palo Alto Networks, Inc.

STEP 6 | (任意) PACファイルを編集します。

PACファイルを素早く変更するには、Webインターフェース内で直接編集することができます。

1. 転送プロファイル内から、**PAC**ファイルを編集します。
2. 変更を加えて保存します。



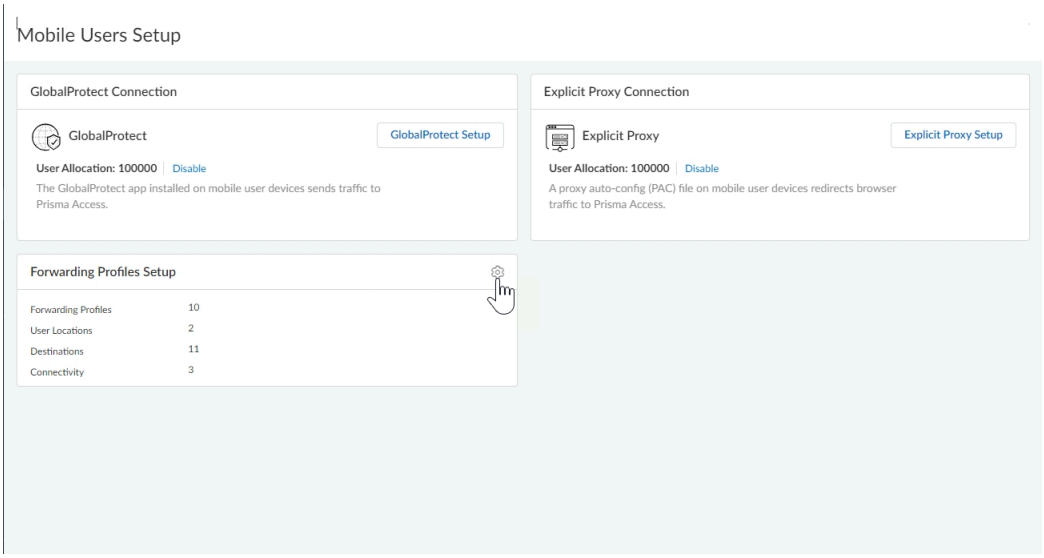
転送ルールを使用して明示型プロキシに転送するトラフィックを定義する

独自のPACファイルを最初から作成する代わりに、簡単な転送ルールを作成してPACファイルを生成できます。

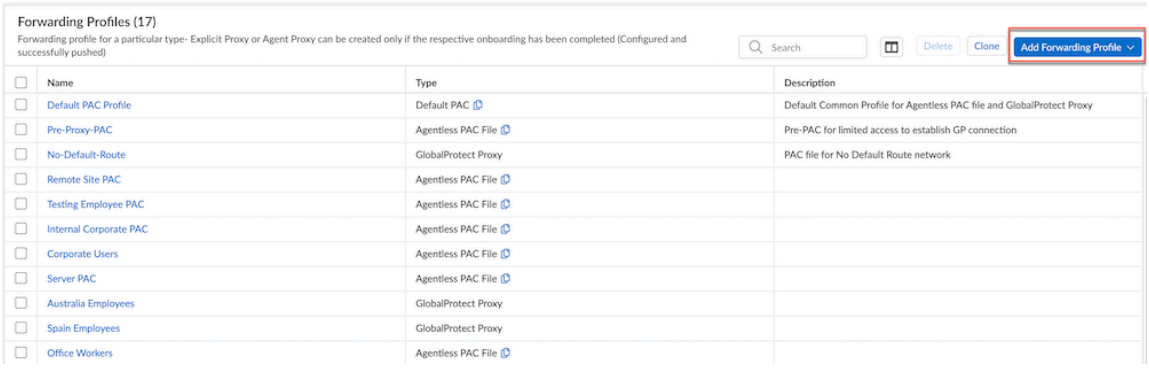
©2025 Palo Alto Networks, Inc.

STEP 1 | ログ転送プロファイルを作成します。

1. Strata Cloud Managerから、**[Workflows (ワークフロー)]** > **[Prisma Accessセットアップ]** > **[Mobile Users (モバイルユーザー)]** > **[Forwarding Profiles Setup (転送プロファイルセットアップ)]**を選択します。



2. 転送プロファイルの追加。



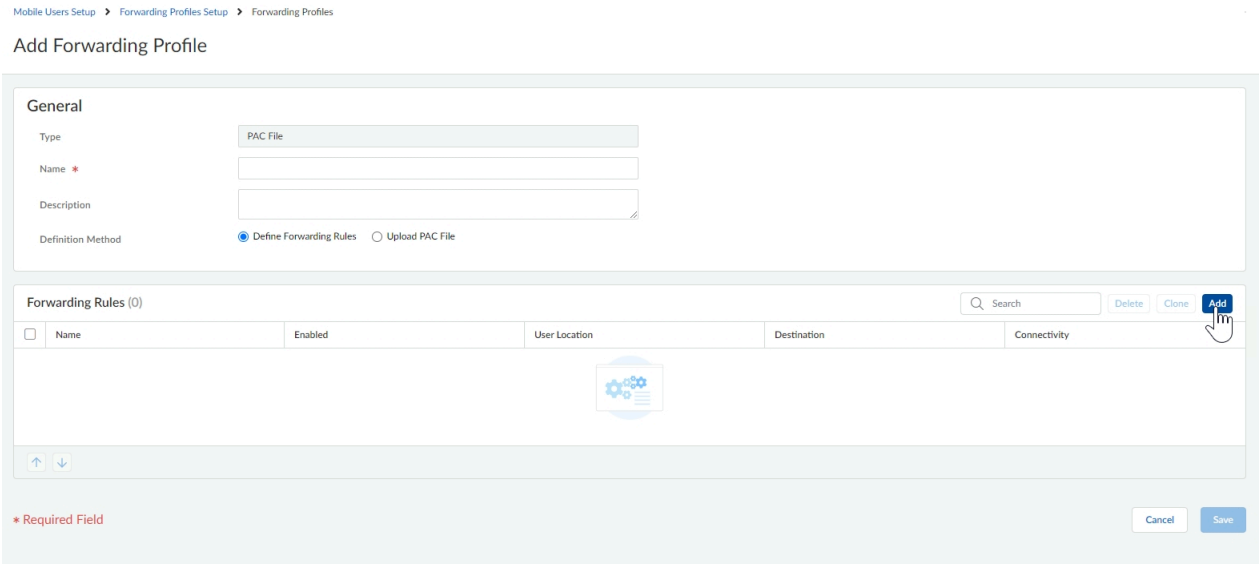
STEP 2 | **PAC**ファイルを選択します。

PACファイル は Prisma Access明示型プロキシのためのものです。**GlobalProtect Proxy**はGlobalProtect をプロキシ モードで使用するためのものです。

©2025 Palo Alto Networks, Inc.

STEP 3 | 転送ルールを追加します 。

1. **Add**（追加）を選択します。



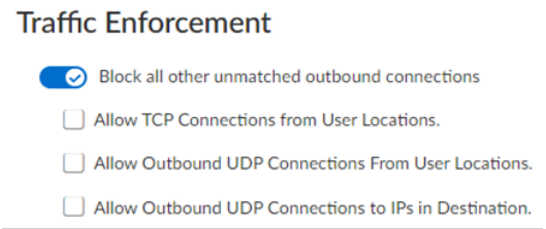
2. 必須フィールドに入力します:

氏名	プロファイルの名前。
ユーザーのロケーション	転送ルールを作成するユーザーの場所。カスタムロケーションの作成は以下より行えます。**[Workflows (ワークフロー)]** > **[Prisma Accessセットアップ]** > **[Mobile Users (モバイルユーザー)]** > **Forwarding Profiles Setup (転送プロファイルセットアップ)** > **[User Locations (ユーザーロケーション)]**。 *IP*アドレスに基づいてカスタムユーザーの場所を設定する場合、ワイルドカード文字は使用できません。
宛先	Web トラフィックの宛先。カスタム宛先の作成は、事前定義済みの宛先から選択するか、 **[Workflows (ワークフロー)]** > **[Prisma Accessセットアップ]** > **[Mobile Users (モバイルユーザー)]** > **[Forwarding Profiles Setup (転送プロファイルセットアップ)]** > **[Destinations (宛先)]**から行えます。

©2025 Palo Alto Networks, Inc.

接続	**Direct (直接)** では、トラフィックはプロキシをバイパスします。 グローバル プロキシ により、トラフィックはプロキシをパススルーします。

3. 完了したら 「追加」 を選択します。
4. 転送ルールに一致しないすべてのアウトバウンド トラフィック (UDP など) をブロックする場合は、 **[Traffic Enforcement (トラフィックの適用)]** を有効にします。このオプションにはGlobalProtectエージェント バージョン 6.3.1が必要であり、デフォルトでは無効になっています。UDP 接続を許可する必要のあるアプリケーションがある場合は、 **[User location (ユーザーのロケーション)]** または **[Destination (宛先)]** オブジェクトを使用してこれらの例外を追加できます。
   ブロックアクションは次のようにカスタマイズできます。
   - エンドポイントからのすべてのUDPアウトバウンド接続をブロックします。
   - 特定のロケーションからのTCPを許可します。たとえば、オフィスからのすべての TCP トラフィックを許可できます。
   - 特定のロケーションからのUDPを許可します。たとえば、オフィスからのすべての TCP トラフィックを許可できます。
   - 特定のアプリケーションでUDP接続が必要な場合は、特定の宛先へのアウトバウンドUDP接続を許可できます。

5. 作成した転送ルールを含むプロファイルを保存します 。
   プロファイルが転送プロファイルのリストに表示されます。開くと、ルールから生成されたPACファイルへのURLが表示されます。**PAC**ファイルを表示してその内容を確認します。

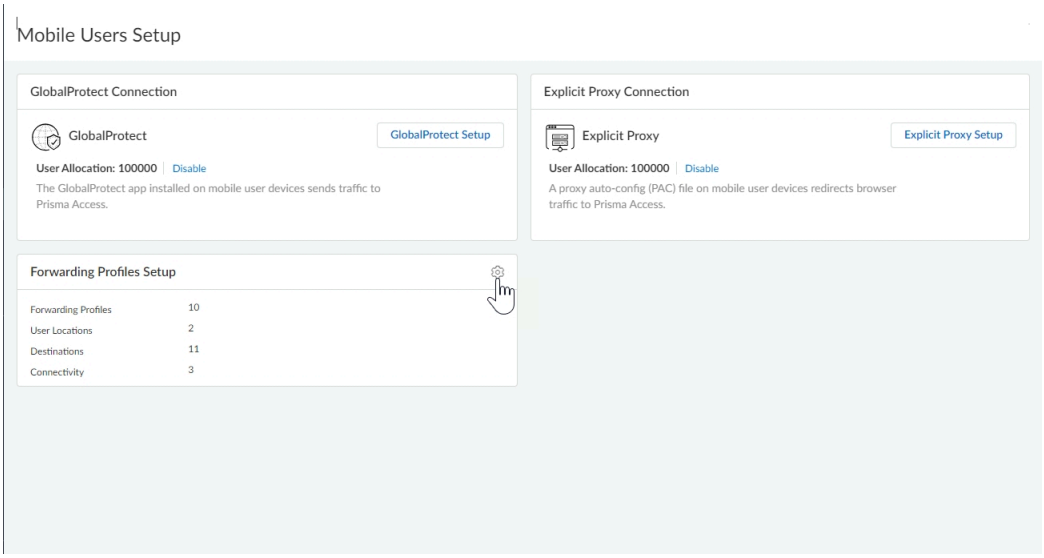
GlobalProtect アプリ設定に転送プロファイルを添付する

転送プロファイルを使用すると、GlobalProtectアプリケーション プロキシの設定を簡素化できます。

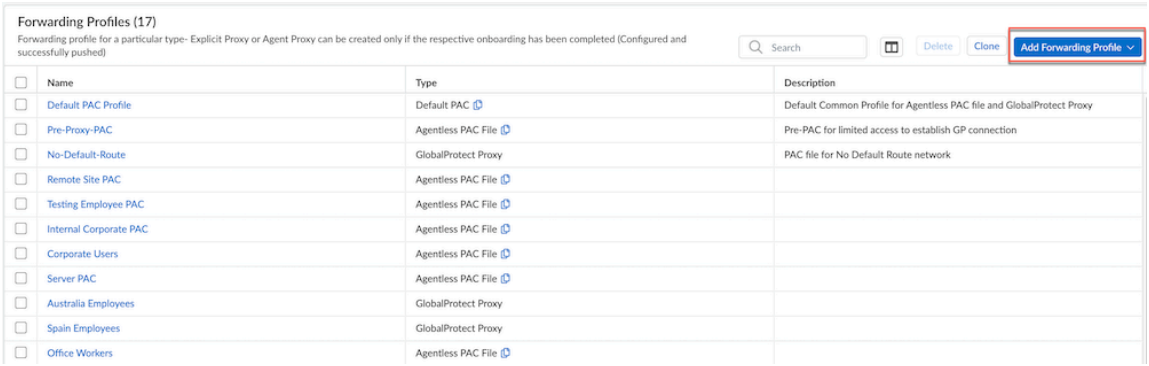
©2025 Palo Alto Networks, Inc.

STEP 1 | ログ転送プロファイルを作成します。

1. Strata Cloud Managerから、**[Workflows (ワークフロー)]** > **[Prisma Accessセットアップ]** > **[Mobile Users (モバイルユーザー)]** > **[Forwarding Profiles Setup (転送プロファイルセットアップ)]**を選択します。



2. 転送プロファイルの追加。



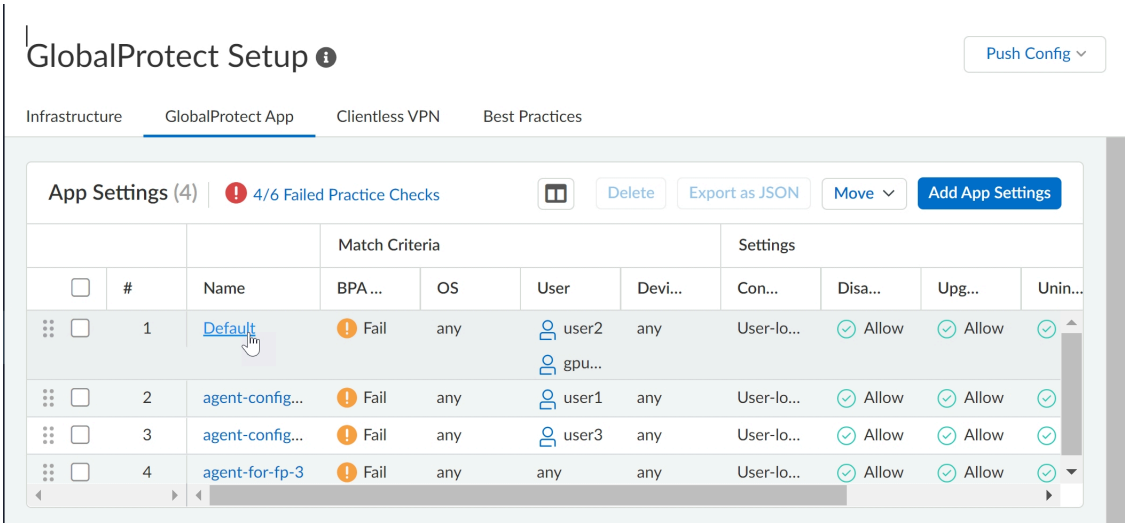
STEP 2 | **GlobalProtect Proxy**を選択します。

STEP 3 | PACファイルをアップロードする か、 転送ルールを作成して、転送プロファイルを設定します。

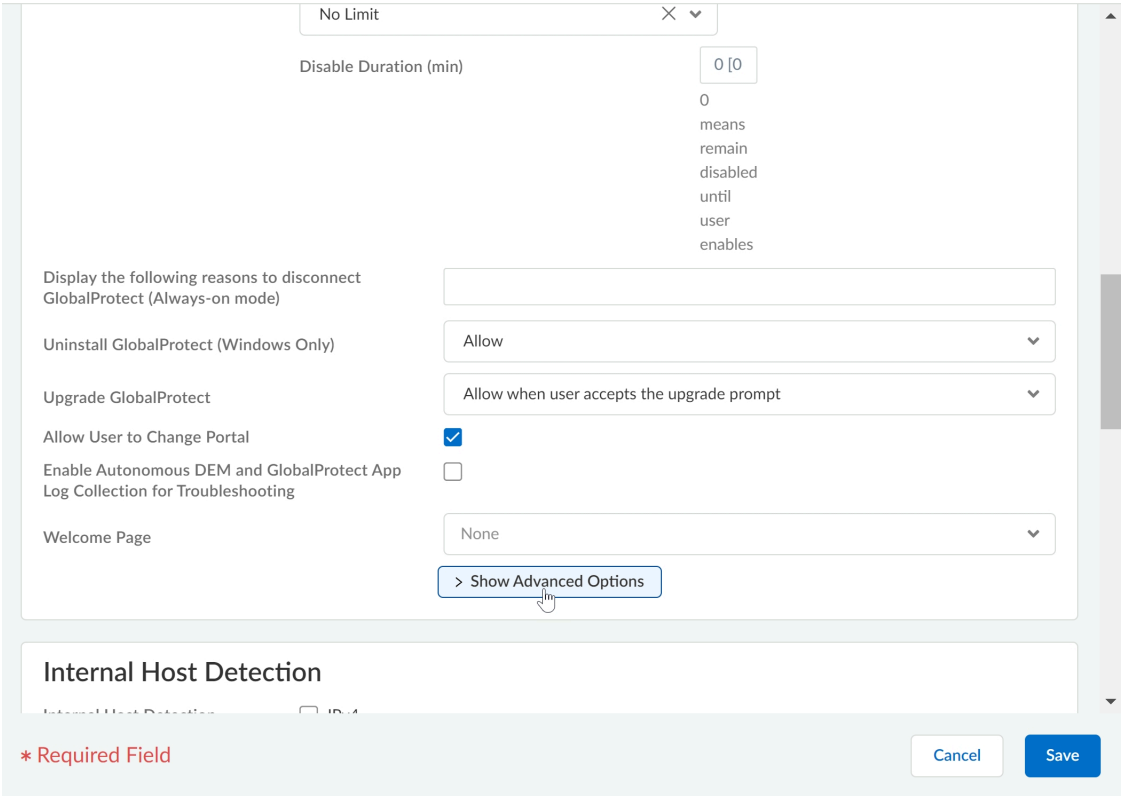
©2025 Palo Alto Networks, Inc.

STEP 4 | 転送プロファイルをGlobalProtect appプロキシ設定に追加します。

1. **[Workflows (ワークフロー)] > [Prisma Accessセットアップ] > [GlobalProtect] > [GlobalProtectアプリケーション]** を選択します。
2. 設定ファイルを選択します。



3. [App Configuration (アプリ設定)]で、 詳細オプションを表示します。

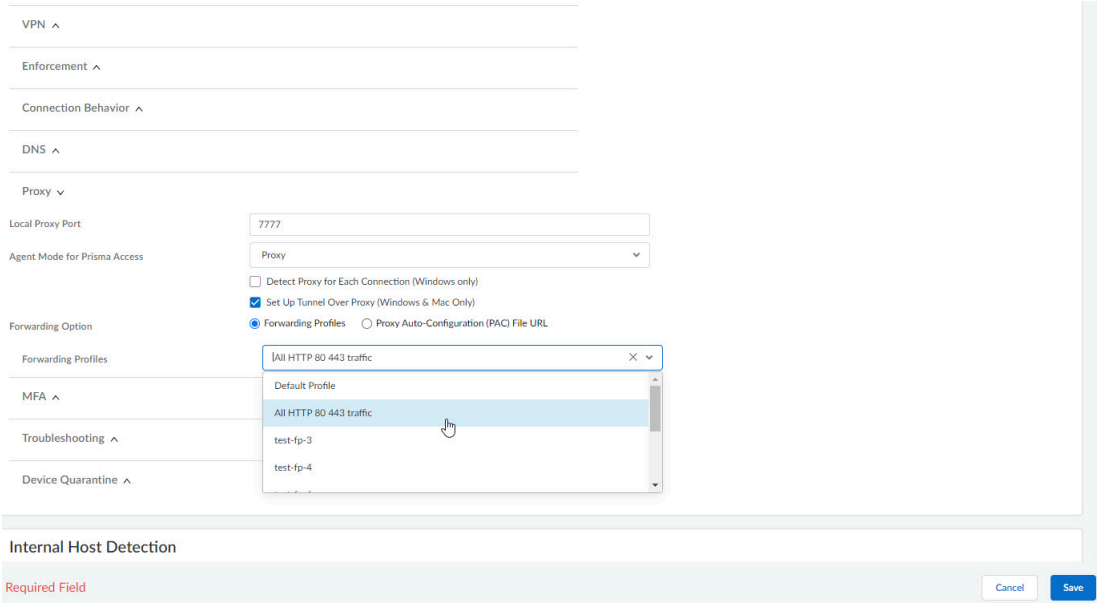


4. プロキシ 設定を展開します。
5. GlobalProtectエージェントモードに応じて、 プロキシ または トンネルとプロキシのいずれかを選択します。

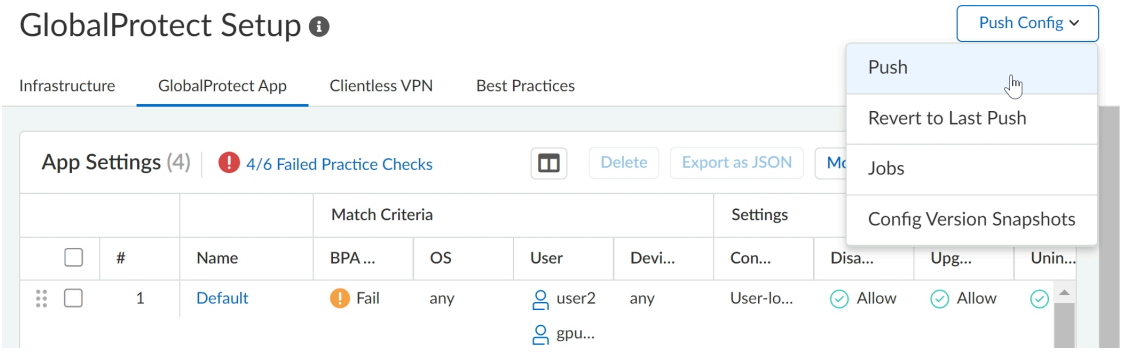
©2025 Palo Alto Networks, Inc.

トンネルモードを選択した場合、転送プロファイルを追加することはできません。

6. 転送プロファイル を選択し、使用する転送プロファイルを選択します。



7. 変更を保存します。
8. **[Push Config (設定のプッシュ)]** > **[Push (プッシュ)]**を選択します。



PACファイルガイドライン

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

- Strata Cloud Manager
- Panorama

©2025 Palo Alto Networks, Inc.

PACファイルガイドライン（Strata Cloud Manager）

明示型プロキシで使用するPACファイルを構成するときは、次のガイドラインと要件に従います。

- GlobalProtectエージェントをプロキシ モードで使用している場合、エージェントはPACファイルをホストに配信することに注意してください。エージェントはHTTPS経由でPACファイルにアクセスします。PACファイルは公開されています。
- PACファイルはユーザー トラフィックを明示型プロキシに誘導します。
- Prisma Accessで使用するためにホストできるPACファイルは1つだけであり、Explicit Proxy PACファイルは米国でホストされます。米国外で代替のPACファイル アクセスが必要な場合は、企業内でPACファイルをホストできます。
- PACファイルにアクセスするには、エンドポイントが次のIPアドレスにアクセスできることを確認してください。
  - 34.111.7.85
  - 34.160.172.204
  - 34.110.206.116
  - 34.95.107.244
  - 34.149.8.36

  デフォルト ルートのないネットワークの場合は、これらのIPアドレスがPACファイルにアクセスできるようにルートを追加する必要があります。
- PACファイルではASCIIテキスト形式のみがサポートされています。Palo Alto Networksは、VIやVimなどのテキストエディタでPACファイルを作成して保存することをお勧めします。
- 明示型プロキシ設定を作成し、変更をコミットしてプッシュしたら、PACファイルをアップロードするか、PACファイル エディターでPAC設定を指定します。
- Prisma Accessに流入するトラフィックのために、戻り 「PROXY `foo.proxy.prismaaccess.com:8080`」;ステートメントの先頭に、少なくとも1つの明示的なプロキシURLを持つ必要があります。変更をプッシュするときに使用する構成済みドメインを使用するか、または PROXY `paloaltonetworks-245139.proxy.prismaaccess.com:8080`やPROXY `1.2.3.4:8080`などの有効なIPv4アドレスまたはDIRECTキーワードを使用します。
- プロキシがバイパスされていない場合は、PROXYキーワードを指定する必要があります。プロキシバイパスに`DIRECT`キーワードが設定されていない場合は、有効なプロキシステートメントが必要です。
- 無効なPROXYステートメントの前に有効なPROXYステートメントが見つかった場合、明示型プロキシは、最初のステートメントの後のすべてのPROXYステートメントの有効性チェックをすべてスキップします。たとえば、有効なステートメントPROXY `paloaltonetworks-245139.proxy.prismaaccess.com:8080`の後に無効なステートメントPROXY `foo.proxy.prismaacess.com:8080`が続くPACファイルは、明示型プロキシは`foo.proxy.prismaacess.com:8080`の有効性チェックをスキップするため、有効と見なされます。

©2025 Palo Alto Networks, Inc.

- PROXYステートメントを使用してACSトラフィックをバイパスする場合、Prisma Accessプロキシの場合、PROXY ステートメントでは明示的なプロキシ URL を使用しないでください。この構成では、明示型プロキシによってエラー メッセージが表示されますが、PACファイルのアップロードは許可されます。有効なFQDNまたはIPv4アドレスを使用して ACSトラフィックを他のプロキシに送信したり、DIRECT キーワードを使用してインターネットに直接送信したりできます。
- PROXYステートメントではIPv4アドレスのみがサポートされます。PROXYステートメント内でIPv6アドレスを使用しないでください。
- PAC ファイルの最大ファイルサイズは750KB です。
- ACS/IdPトラフィックが明示型プロキシを経由する必要がある場合は、それらのドメインを認証バイパス リストと復号化なしポリシー ルールに追加します。
- デフォルト ルート環境で明示型プロキシを設定する場合は、ポータル、ゲートウェイ、およびSAML FQDNを除外する必要があります。PACファイルを使用してFQDNをバイパスできます。
- アップロードしたPACファイルを削除することはできません。ただし、新しいPACファイルをアップロードしたり、PACファイル エディターで編集して既存のファイルを上書きしたりすることはできます。

Explicit Proxyには、変更してExplicit ProxyデプロイメントのPACファイルとして使用できるサンプルPACファイルが用意されています。Prisma Accessが提供するサンプルPACファイルには以下のデータが含まれます：

```
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";
```

Prisma Accessが提供するデフォルトのPACファイルを使用する場合、オプションとして、以下の表に説明するようにPACファイルのフィールドを変更することができます。

テキスト	詳説
`var resolved_ip = dnsResolve(host); ... return "DIRECT";`	このファイル内のデータを変更しない場合、次のホスト名とIPアドレスは明示型プロキシをバイパスします。 • `if (isPlainHostName(host)`—ドットを含まないホスト名（例：http://intranet）の明示型プロキシをバイパスします。

©2025 Palo Alto Networks, Inc.

テキスト	詳説
	• `shExpMatch(host, "*.local") ||` –内部ネットワーク (localhost) でホストされているホスト名のプロキシをバイパスします。 • `isInNet(`解決されたIP、「10.0.0.0」、「255.0.0.0」) || isInNet(`解決されたIP、「172.16.0.0」、「255.240.0.0」) || isInNet(`解決されたIP、「192.168.0.0」、「255.255.0.0」) || isInNet(`解決されたIP、「127.0.0.0」、「255.255.255.0」)–プライベートまたはループバック IP アドレス範囲内のIPアドレスに対して明示型プロキシをバイパスします。
`if (url.substring(0,4) == "ftp:" )` の場合、`"DIRECT"` を返します。	FTPセッションの明示型プロキシをバイパスします。
`shExpMatch(host, "*.okta.com") || shExpMatch(host, "*.oktacdn.com"))` の場合は `"DIRECT"` を返します。	SAML IdPの明示型プロキシをバイパスします。IdPで使用されるすべてのFQDNを必ず追加してください。 SAML認証に使用するIdPとしてOktaを使用する場合は、**`*.okta.com`**と**`*.oktacdn.com`**を入力します。
`shExpMatch(host, "*.acs.prismaaccess.com")` の場合、`"DIRECT"` を返します。	Prisma Access認証キャッシュ サービス（ACS）の明示型プロキシをバイパスする。 ワイルドカードを使用する代わりに、デプロイメントに特定の**ACS FQDN** を追加できます。この FQDN は**[Panorama] > [Cloud Services (クラウドサービス)] > [Status (ステータス)] > [Network Details (ネットワーク詳細)] > [Mobile Users—Explicit Proxy (モバイルユーザー—Explicit Proxy)] > [ACS FQDN]**で見つかります。
「`PROXY foo.proxy.prismaaccess.com:8080`」を返します	明示型プロキシURLの明示型プロキシをバイパスします。

©2025 Palo Alto Networks, Inc.

テキスト	詳説
	Prisma Accessに流入するトラフィックのために、戻り 「PROXY foo.proxy.prismaaccess.com:8080」;ステートメントに、少なくとも1つの明示型プロキシURLを持つ必要があります。変更をプッシュするときに使用する構成済みドメインを使用するか、または PROXY paloaltonetworks-245139.proxy.prismaaccess.c 1.2.3.4:8080の有効なIPv4アドレスまたはDIRECTキーワードを使用します。

PACファイルガイドライン（Panorama）

明示型プロキシで使用するPACファイルを構成するときは、次のガイドラインと要件に従います。

- GlobalProtectエージェントをプロキシ モードで使用している場合、エージェントはPACファイルをホストに配信することに注意してください。エージェントはHTTPS経由でPACファイルにアクセスします。PACファイルは公開されています。
- PACファイルはユーザー トラフィックを明示型プロキシに誘導します。
- Prisma Accessで使用するためにホストできるPACファイルは1つだけであり、Explicit Proxy PACファイルは米国でホストされます。米国外で代替のPACファイル アクセスが必要な場合は、企業内でPACファイルをホストできます。
- PACファイルにアクセスするには、エンドポイントが次のIPアドレスにアクセスできることを確認してください。
  - 34.111.7.85
  - 34.160.172.204
  - 34.110.206.116
  - 34.95.107.244
  - 34.149.8.36
- PACファイルではASCIIテキスト形式のみがサポートされています。Palo Alto Networksは、VIやVimなどのテキストエディタでPACファイルを作成して保存することをお勧めします。
- 明示型プロキシ構成を作成し、変更をコミットしてプッシュした後、PACファイルをアップロードします。PACファイルをアップロードした後は、コミットとプッシュの操作は必要ありません。
- Prisma Accessに流入するトラフィックのために、戻り 「PROXY foo.proxy.prismaaccess.com:8080」;ステートメントの先頭に、少なくとも1つの明示的なプロキシURLを持つ必要があります。変更をプッシュするときに使用する構成済みドメインを使用するか、または PROXY paloaltonetworks-245139.proxy.prismaaccess.com:8080やPROXY 1.2.3.4:8080などの有効なIPv4アドレスまたはDIRECTキーワードを使用します。

©2025 Palo Alto Networks, Inc.

- プロキシがバイパスされていない場合は、PROXYキーワードを指定する必要があります。プロキシバイパスにDIRECTキーワードが設定されていない場合は、有効なプロキシステートメントが必要です。
- 無効なPROXYステートメントの前に有効なPROXYステートメントが見つかった場合、明示型プロキシは、最初のステートメントの後のすべてのPROXYステートメントの有効性チェックをすべてスキップします。たとえば、有効なステートメントPROXY paloaltonetworks-245139.proxy.prismaaccess.com:8080の後に無効なステートメントPROXY foo.proxy.prismaacess.com:8080が続くPACファイルは、明示型プロキシはfoo.proxy.prismaacess.com:8080の有効性チェックをスキップするため、有効と見なされます。
- PROXYステートメントを使用してACSトラフィックをバイパスする場合、Prisma Accessプロキシの場合、PROXY ステートメントでは明示的なプロキシ URL を使用しないでください。この構成では、明示型プロキシによってエラー メッセージが表示されますが、PACファイルのアップロードは許可されます。有効なFQDNまたはIPv4アドレスを使用して ACSトラフィックを他のプロキシに送信したり、DIRECT キーワードを使用してインターネットに直接送信したりできます。
- PROXYステートメントではIPv4アドレスのみがサポートされます。PROXYステートメント内でIPv6アドレスを使用しないでください。
- PAC ファイルの最大ファイルサイズは 256KB です。
- ACS/IdPトラフィックが明示型プロキシを経由する必要がある場合は、それらのドメインを認証バイパス リストと復号化なしポリシー ルールに追加します。
- デフォルト ルート環境で明示型プロキシを設定する場合は、ポータル、ゲートウェイ、およびSAML FQDNを除外する必要があります。PACファイルを使用してFQDNをバイパスできます。
- アップロードしたPACファイルを削除することはできません。ただし、新しいPACファイルをアップロードして既存のファイルを上書きすることは可能です。
- 明示型プロキシURLをPrisma Accessで変更しても、その変更を反映するようにPACファイルを変更しなければ、変更は適用されません。新しい明示型プロキシURLを指定する新しいPACファイルをアップロードする必要があります。

Explicit Proxyには、変更してExplicit ProxyデプロイメントのPACファイルとして使用できるサンプルPACファイルが用意されています。Prisma Accessが提供するサンプルPACファイルには以下のデータが含まれます：

```
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.

Prisma Accessが提供するデフォルトのPACファイルを使用する場合、オプションとして、以下の表に説明するようにPACファイルのフィールドを変更することができます。

テキスト	詳説
`var resolved_ip = dnsResolve(host); ... return "DIRECT";`	このファイル内のデータを変更しない場合、次のホスト名とIPアドレスは明示型プロキシをバイパスします。 • `if (isPlainHostName(host)`—ドットを含まないホスト名（例：http://intranet）の明示型プロキシをバイパスします。 • `shExpMatch(host, "*.local") ||`—内部ネットワーク (localhost) でホストされているホスト名のプロキシをバイパスします。 • `isInNet(`解決されたIP、「10.0.0.0」、「255.0.0.0」) || isInNet(解決されたIP、「172.16.0.0」、「255.240.0.0」) || isInNet(解決されたIP、「192.168.0.0」、「255.255.0.0」) || isInNet(解決されたIP、「127.0.0.0」、「255.255.255.0」)`—プライベートまたはループバック IP アドレス範囲内のIPアドレスに対して明示型プロキシをバイパスします。
`if (url.substring(0,4) == "ftp:")` の場合、`"DIRECT"` を返します。	FTPセッションの明示型プロキシをバイパスします。
`shExpMatch(host, "*.okta.com") || shExpMatch(host, "*.oktacdn.com"))` の場合は `"DIRECT"` を返します。	SAML IdPの明示型プロキシをバイパスします。IdPで使用されるすべてのFQDNを必ず追加してください。 SAML認証に使用するIdPとしてOktaを使用する場合は、**`*.okta.com`**と**`*.oktacdn.com`**を入力します。

©2025 Palo Alto Networks, Inc.

テキスト	詳説
`shExpMatch(host, "*.acs.prismaaccess.com")` の場合、`"DIRECT"` を返します。	Prisma Access認証キャッシュ サービス（ACS）の明示型プロキシをバイパスする。 ワイルドカードを使用する代わりに、デプロイメントに特定の**ACS FQDN** を追加できます。この FQDN は**[Panorama] > [Cloud Services (クラウドサービス)] > [Status (ステータス)] > [Network Details (ネットワーク詳細)] > [Mobile Users—Explicit Proxy (モバイルユーザー—Explicit Proxy)] > [ACS FQDN]**で見つかります。
「`PROXY foo.proxy.prismaaccess.com:8080`」を返します	明示型プロキシURLの明示型プロキシをバイパスします。 Prisma Accessに流入するトラフィックのために、戻り 「`PROXY foo.proxy.prismaaccess.com:8080`」;ステートメントに、少なくとも1つの明示型プロキシURLを持つ必要があります。変更をプッシュするときに使用する構成済みドメインを使用するか、または `PROXY paloaltonetworks-245139.proxy.prismaaccess.com 1.2.3.4:8080`の有効なIPv4アドレスまたはDIRECTキーワードを使用します。

明示型プロキシのベストプラクティス

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

推奨されるベストプラクティスを使用して、最適なパフォーマンスと理想的なユーザーエクスペリエンスのために明示的プロキシのデプロイメントを実装してください。

- 一般的な明示型プロキシ デプロイメントのベストプラクティス:
  - 冗長性のために少なくとも2つの地域に明示型プロキシをデプロイします。
  - すべてのユーザーがNATデバイスの背後にいる場合、かつ明示的プロキシがNATデバイスのIPアドレスを送信元IPアドレスとして認識する場合、500人のモバイルユーザーごとに1つのNAT IPアドレスを割り当てる必要があります。
  - は、PACファイルを構成するために転送プロファイルを使用します。

©2025 Palo Alto Networks, Inc.

- **PAC**ファイルのベストプラクティス - 際は、すべてのSAML、CIE、および認証キャッシュサービス（ACS）URLをバイパスしてください。
- **SAML**認証のベストプラクティス:
  - SAML認証クッキーの有効期間を 24 時間に設定すると、認証が中断されることなく、最高のユーザー エクスペリエンスが得られます。
  - GlobalProtectをプロキシモードまたはトンネルおよびプロキシモードで設定した場合、GlobalProtectポータルのクッキーの有効期限を12時間に設定してください。
- **Kerberos**認証のベストプラクティス–keytabファイルのサイズは60 KB未満であるべきです。
- セキュリティポリシールールのベストプラクティス - ポリシーのアクションをドロップやリセットではなく拒否に設定することで、セキュリティポリシールールのベストプラクティスを使用します。このアクションは、最適なパフォーマンスのために、明示的プロキシセキュリティ処理ノード（EP-SPN）内でリソースを迅速に解放するのに役立ちます。
- 復号化のベストプラクティス–少なくとも1つの復号ポリシーと1つの復号化証明書を構成してください。
- **IP**ソースアドレスのベストプラクティス–特定のソースIPアドレスに対して明示型プロキシへのアクセスを制限するには、アドレスオブジェクト、アドレスグループ、および外部ダイナミックリスト（EDL）を含む特別なオブジェクトを使用します。

明示型プロキシの監視とトラブルシューティング

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

Prisma AccessExplicit Proxy (明示型プロキシ) のデプロイメントを監視し、トラブルシューティングを行う方法について説明します。

- Strata Cloud Manager
- Panorama

明示型プロキシの監視とトラブルシューティング (Strata Cloud Manager)

Prisma AccessExplicit Proxy (明示型プロキシ) デプロイメントの詳細を監視して、問題のトラブルシューティングに役立てます

- **[Monitor (監視)]** > **[Users (ユーザー)]**をクリックし、 **[Explicit Proxy (明示型プロキシ)]** connected method (接続方法)を選択します。
- **[Monitor (監視)]** > **[Users (ユーザー)]**を選択し、 **[Explicit Proxy (明示型プロキシ)]**という接続方法を選択すると、Explicit Proxy (明示型プロキシ) を介してPrisma Accessセキュリティ サービスに接続するモバイルユーザーを、そのデバイス上のWebブラウザで表示することができます。

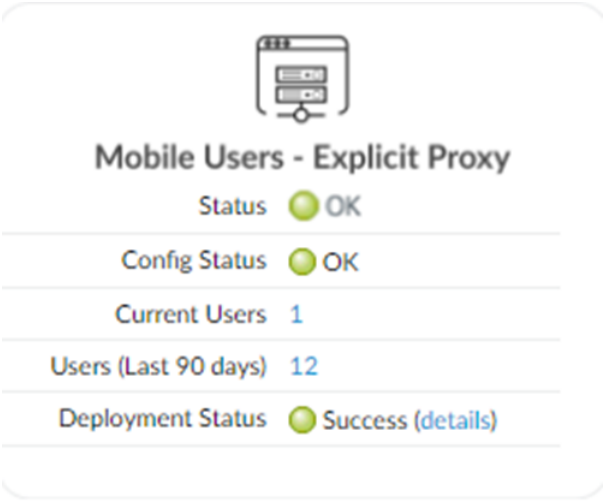
©2025 Palo Alto Networks, Inc.

- **[監視] > [Prisma Accessロケーション] > [明示型プロキシモバイルユーザー]**を選択すると、モバイルユーザーのすべてのPrisma Accessロケーションの状態の概要が表示されます。
- 認証関連の問題のトラブルシューティングを行うには、トラフィック ログ (**[インシデントとアラート] > [ログビューア]** を選択し、ログタイプ **[トラフィック]**) と認証ログ (**[インシデントとアラート] > [ログビューア]** を選択し、ログタイプとして**[認証]**を選択) を確認します。

明示型プロキシの監視とトラブルシューティング (Panorama)

モバイルユーザー向けにExplicit Proxy (明示型プロキシ)を設定したら、Prisma Access Explicit Proxy (明示型プロキシ) デプロイメントのステータスを確認してステータスを監視し、問題をトラブルシューティングします。

- **[Panorama] > [Cloud Services (クラウドサービス)] > [Status (ステータス)] > [Status (ステータス)]**を選択すると、明示型プロキシステータスが表示されます。



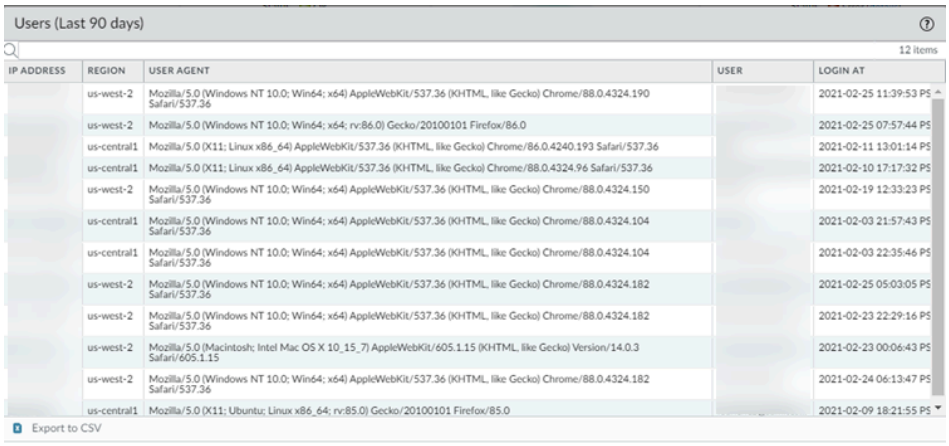
モバイルユーザーの **[Status (ステータス)]** フィールドと **[Config Status (構成ステータス)]** フィールドには、モバイルユーザーとPrisma Accessの接続に問題がないか、トンネルのス

©2025 Palo Alto Networks, Inc.

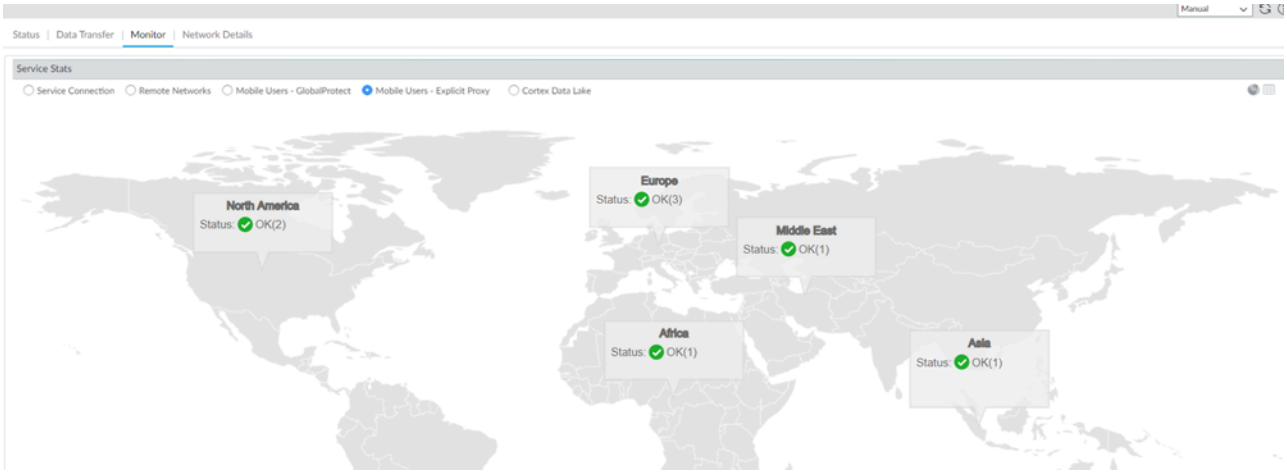
テータスを取得できない (警告)、もしくはモバイルユーザーが明示型プロキシに接続できない (エラー) が示されます。

[現在のユーザー]と[ユーザー(過去**90**日間)]の横にあるハイパーリンクをクリックすると、モバイルユーザーの詳細が表示されます。

- 現在のユーザー—過去5分間にトラフィックを閲覧した認証済みユーザの現在の数。
- ユーザー(過去**90**日間)-過去 90 日間に認証されたユニークな Explicit Proxy ユーザーの数。

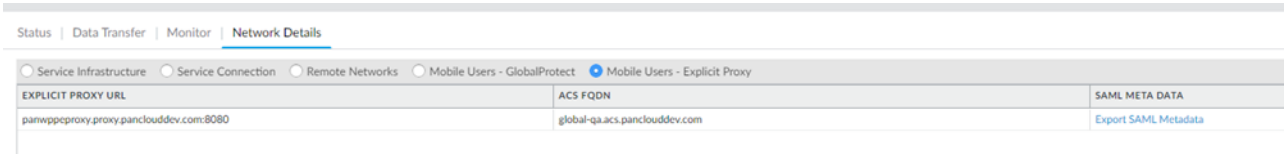


- **[Panorama] > [Cloud Services (クラウドサービス)] > [Status (ステータス)] > [Monitor (監視)] > [Mobile Users—Explicit Proxy (モバイルユーザー-明示型プロキシ)]**を選択すると、デプロイされた明示型プロキシの場所を示すマップが表示されます。



 ©2025 Palo Alto Networks, Inc.

- **[Panorama] > [Cloud Services (クラウドサービス)] > [Status (ステータス)] > [Network Details (ネットワーク詳細)] > [Mobile Users—Explicit Proxy (モバイルユーザー-明示型プロキシ)]**を選択すると、次の詳細が表示されます。



  - 明示型プロキシ**URL** – 明示的なプロキシに使用されるURL。
  - **ACS QDN** – ACSのFQDN。
  - **SAML**メタデータ – SAML で使用される認証プロファイルメタデータ。**SAML** メタデータをエクスポートしてメタデータファイルを保存できます。
- 認証関連の問題のトラブルシューティングを行うには、トラフィック ログ (監視 > ログ > トラフィック) と認証ログ (監視 > ログ > 認証) を確認します。明示型プロキシは、ログに次のIPアドレスと場所を表示します。
  - **IP** アドレス–モバイルユーザがPACファイルのACS FQDNをバイパスした場合、トラフィック ログとトラフィック ログの **[Source (送信元)]** 列と [認証ログ] の [IPアドレス] 列に表示される **IP**アドレスは、**Explicit_Proxy_Device_Group** で表示すると、モバイルユーザのIPアドレスと同じになります。ユーザがPACファイル内のACS FQDNをバイパスしない場合、送信元IPアドレスは、リダイレクトがACSに送信されるExplicit Proxyクラウドファイアウォールのパブリック**IP**アドレスになります。
  - **Locations (ロケーション)**–モバイルユーザがPACファイルのACS FQDNをバイパスした場合、**Authentication Logs (認証ログ)**、**Current Users (現在のユーザー)**、ユーザー（過去 **90** 日間）の**Region (リージョン)**列に表示されるリージョン名は、ACSがデプロイされている5つの5つのリージョン（us-west-2、us-east-1、eu-west-2、eu-west-3、ap-south-1）のいずれかであり、明示型プロキシがクライアントのブラウザからリダイレクトを実行しているリージョンが表示されます。ユーザーがPACファイルのACS FQDNをバイパスした場合、**Authentication Logs (認証ログ)**、**Current Users (現在のユーザー)**、ユーザー（過去 90 日間）の**Region (リージョン)**列に表示されるリージョン名は、ACSがデプロイされている5つの5つのリージョン（us-west-2、us-east-1、eu-west-2、eu-west-3、ap-south-1）のいずれかであり、明示型プロキシが明示型プロキシファイアウォールからリダイレクトを実行しているリージョンが表示されます。

明示的プロキシのブロック設定

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Panorama Managed Prisma Access	• Prisma Accessライセンス

この機能を有効にするには、**Palo Alto Networks**のアカウント担当者またはパートナーに連絡して、サイト信頼性エンジニアリング**(SRE)**チームに連絡してリクエストを送信してください。

©2025 Palo Alto Networks, Inc.

ユーザーがExplicit Proxyを使用してインターネットの宛先にアクセスすると、インターネットの宛先のDNS解決はExplicit Proxyによって実行されます。DNS解決段階でインターネットの宛先へのアクセスをブロックするには、ブロック設定を使用できます。DNSセキュリティカテゴリ、URLフィルタリングカテゴリ、または 外部ダイナミックリスト (EDL).

ブロックするドメインの場合、 Prisma Accessはドメインをブロックし、ユーザーはHTTP GETリクエスト(暗号化されていないWebサイトの場合)またはHTTP Connectリクエスト(暗号化されたWebサイトの場合)中にブロックページを受け取ります。つまり、最初の接続リクエスト中にドメインがブロックされます。サイトへのアクセスをブロックすると、ユーザーは認証フローを通過した後でブロックページが表示され、ユーザー名はフォレンジックやセキュリティオペレーションセンター(SOC)のワークフローのためにキャプチャされます。

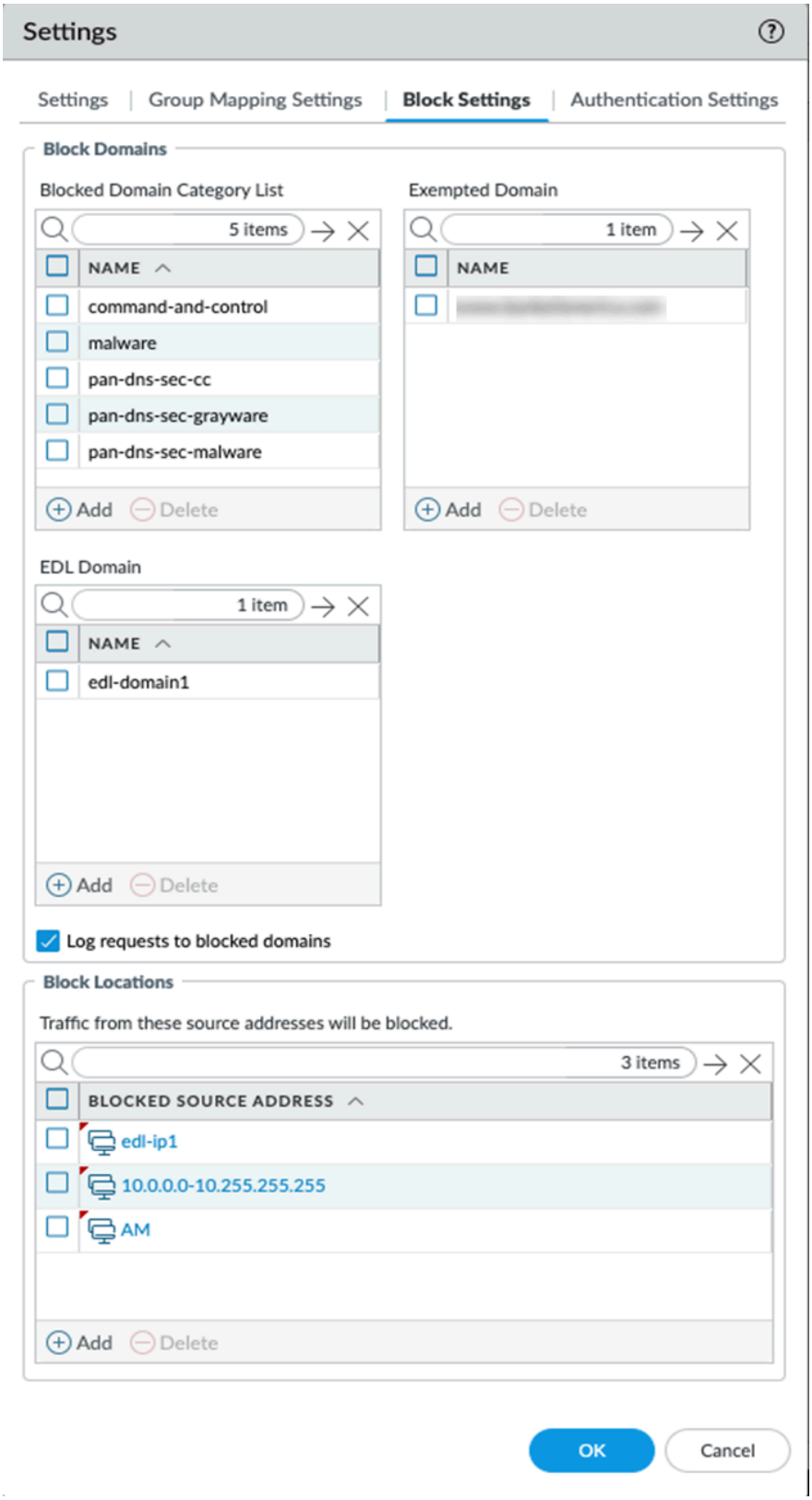
Prisma Access (Managed by Strata Cloud Manager)を使用している場合は、[明示的なプロキシの設定]の手順8を参照してください。Panorama ManagePrisma Accessブロック設定を構成するには、次の手順を実行します。

STEP 1 | ブロック設定 を設定して、ドメインまたはドメイン カテゴリをブロックします。

悪意のあるWebサイト、またはユーザーにアクセスを許可しないWebサイトのドメインまたはドメイン カテゴリを指定します。Prisma Accessは、ユーザーがHTTP GET(暗号化されていないリクエストの場合)またはHTTP CONNECT(暗号化されたリクエストの場合)を開始するときに、この領域で指定したURLとIPアドレスにユーザーがアクセスできないようにします。

©2025 Palo Alto Networks, Inc.

ユーザーがブロックされたウェブサイトにアクセスしようとすると、ブロックページが表示されます。



©2025 Palo Alto Networks, Inc.

1. ブロックされたドメイン カテゴリ リストに、ブロックする定義済みカテゴリを入力します。

   カスタムURLカテゴリ はサポートされていません。
2. **EDL**ドメインに、ブロックするドメインベースの外部ダイナミックリスト（EDL）を入力します。

   選択できるEDLは、EDLタイプがダイナミックドメインリストであるものに限られます。ダイナミックIPリストとダイナミックURLリストは選択できません。
3. ブロックされたドメインカテゴリリストに含まれているドメインを除外したい場合は、除外ドメインとして指定します。

   入力されたドメインは、ブロックしたドメイン カテゴリに表示されていても、ブロックが免除されます。

   - 最大100個のドメインを入力できます。
   - ドメイン レコードの最大長は256文字です。

STEP 2 | ブロックするIPアドレスを［ブロックする送信元アドレス］領域で選択します。

アドレス、アドレス グループ、IPアドレスベースのEDL、または地域および国ベースのIPアドレスを追加できます。

次のIPアドレスのガイドラインを使用してください。

- EDLは、**IP**リストのタイプまたは定義済み**IP**リストでのみ使用します。
- **IP**範囲または**IP**ネットマスクタイプのアドレス オブジェクトのみを使用します。
- 動的オブジェクトメンバーシップを持つアドレス グループはサポートされていません。
- IPアドレス オブジェクトでカスタム領域を使用しないでください。代わりに、定義済みのリージョンを使用します。

STEP 3 | Prisma Accessがブロックされたドメイン リクエストをログに記録するようにするには、**[**ブロックされたドメインへのリクエストをログに記録する**]**を選択します。

ブロックされたドメインログはボットネットから大量のトラフィックを生成する可能性があるため、ログ記録を有効にする場合は注意が必要です。または、トラブルシューティングの目的でのみ使用してください。プロキシの使用を制限する場合 (たとえば、特定のIPアドレスに使用を制限する場合)、制限なくログ記録を有効にできる場合があります。

特別なオブジェクトを使用して、明示型プロキシインターネットトラフィックを特定のIPアドレスに制限する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

©2025 Palo Alto Networks, Inc.

明示型プロキシには、明示型プロキシへのアクセスを特定の送信元IPアドレスに制限するための特別なアドレスオブジェクト、アドレスグループ、および外部動的リスト（EDL）が用意されています。次の正確な名前を使用してこれらの特殊オブジェクトを 1 つ以上作成すると、明示型プロキシは指定した送信元 IP アドレスを許可し、他の IP アドレスはすべてブロックします。

- アドレスオブジェクト – Explicit_Proxy_Device_Group 内のオブジェクト > アドレスを選択し、パロアルトネットワークスの明示型プロキシ許可送信元アドレスという名前のオブジェクトを作成します。
- アドレスグループ – Explicit_Proxy_Device_Group 内のオブジェクト > アドレスグループを選択し、パロアルトネットワークスの明示型プロキシ許可送信元アドレスグループという名前のオブジェクトを作成します。
- 外部ダイナミックリスト **(EDL)** – Explicit_Proxy_Device_Group 内のオブジェクト > 外部ダイナミックリストを選択し、パロアルトネットワークスの明示型プロキシ許可ソースリストという名前の EDL を作成し、**IP**リストというタイプの EDL を作成します。

支社の出口 IP アドレスなどの IP アドレスを指定できます。

ワイルドカード（*.* など）を使用して多数のドメインの明示的プロキシ認証をスキップすることは許可されません。ただし、これらの特別なオブジェクトのいずれかを使用してソーストラフィックを特定の送信元 IP アドレスに制限する場合を除きます。

アドレスオブジェクト、アドレスグループ、または EDL を個別に、または組み合わせて使用します。たとえば、アドレスオブジェクトや EDL を作成せずにアドレスグループのみを作成できます。

明示的なプロキシを使用してデータセンターにアクセスする

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ （ZTNAコネクタおよびColo-Connect用）Prisma Access5.2.1バージョン ❑ （サービス接続用）Prisma Access5.0バージョン ❑ （プライベートおよびパートナーアプリへのアクセス用）GlobalProtect appバージョン6.2（WindowsまたはMacOS用）

サービスコネクション、ZTNAコネクタ、Colo-Connectを使用して、明示的なプロキシ接続のメリットを享受しながら、外部動的リストやプライベートおよびパートナーアプリなどのデータセンター内のリソースにアクセスできます。

©2025 Palo Alto Networks, Inc.

以下の*RFC 6598 IP*アドレスは、サービス接続、*Colo-Connect*、または*ZTNA*コネクタを介した明示プロキシ経由のプライベートアプリケーションアクセスには対応していません。

- *100.64.0.0/15*
- *100.88.0.0/15*
- *100.72.0.0/15*

*ZTNA Connector Application IP*ブロックまたは*Connector IP*ブロックでこれらの*IP*アドレスを使用している既存の*ZTNA Connector*は、明示的なプロキシを介してプロキシモードで*Prisma Access Browser*または*GlobalProtect*エージェントを使用できなくなります。*IP*アドレスを別のブロックに移行するには、*Palo Alto Networks*の担当者に連絡する必要があります。

- Strata Cloud Manager
- Panorama

明示的なプロキシを使用してデータセンターにアクセスする（Strata Cloud Manager）

STEP 1 | サービス接続、Colo-ConnectおよびZTNAコネクタ を要件に応じて設定します。

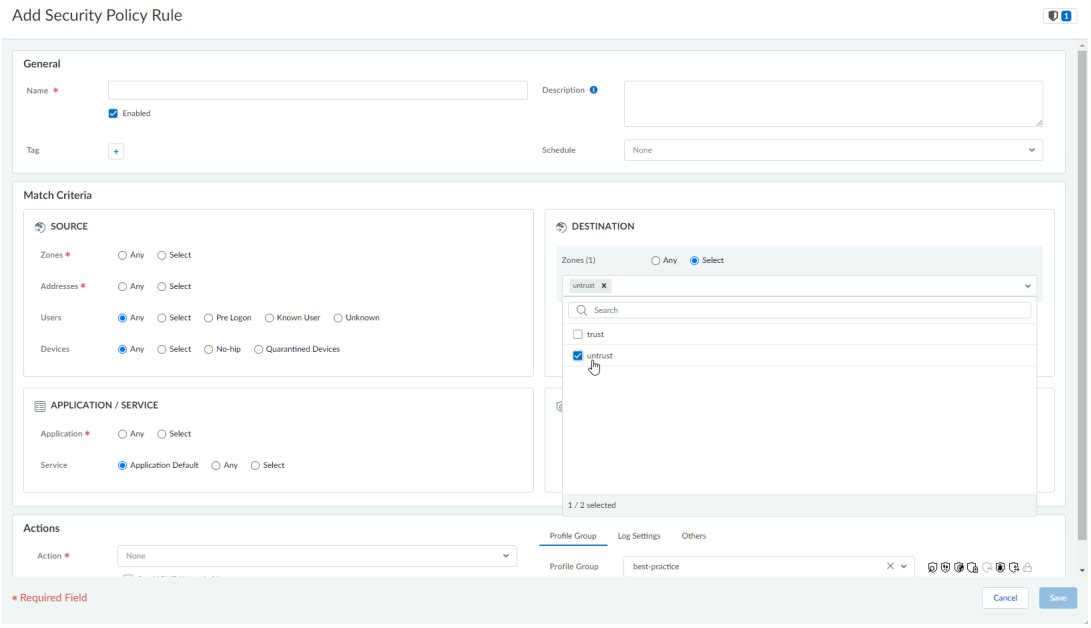
STEP 2 | DNSセキュリティの設定

©2025 Palo Alto Networks, Inc.

STEP 3 | インターネット宛てのトラフィックの 宛先ゾーンが任意ではなくアントラストに設定されていることを確認します。

この手順を実行しないと、データ センターへの意図しないアクセスが発生する可能性があります。

1. [管理] > [構成] > [NGFWとPrisma Access]に移動し、[構成スコープ] を[Prisma Access] > [モバイルユーザー コンテナ] > [明示的プロキシ]に設定して、[セキュリティ ポリシー] > [セキュリティ サービス]を選択します。
2. インターネット宛のトラフィックのルールを開きます。
3. 宛先の下のゾーンがアントラストに設定されていることを確認します。



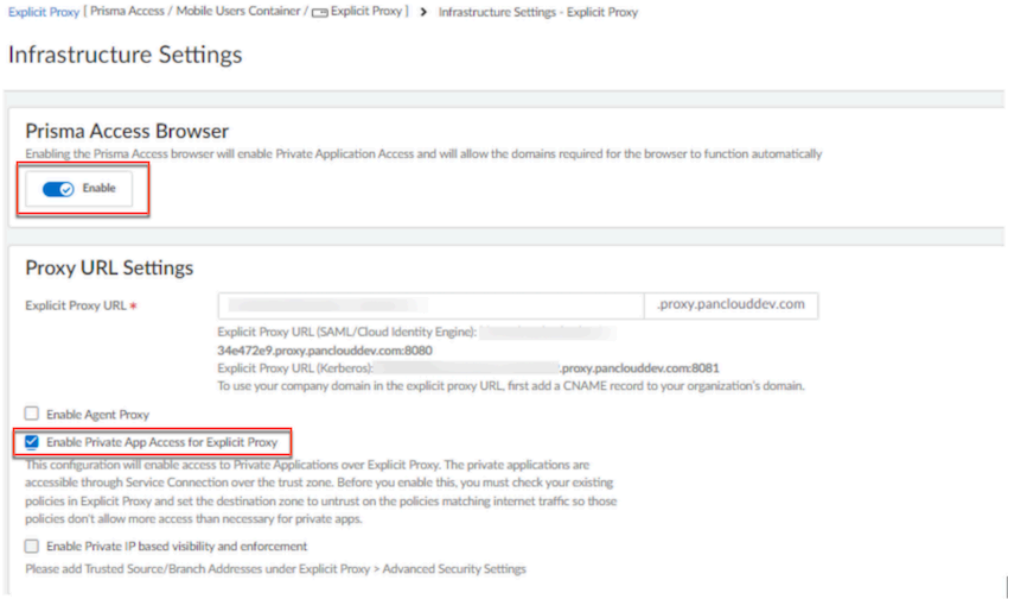
4. インターネットへのすべてのトラフィック ルールでこれを繰り返します。

STEP 4 | プライベートアプリケーションアクセスを有効にします。

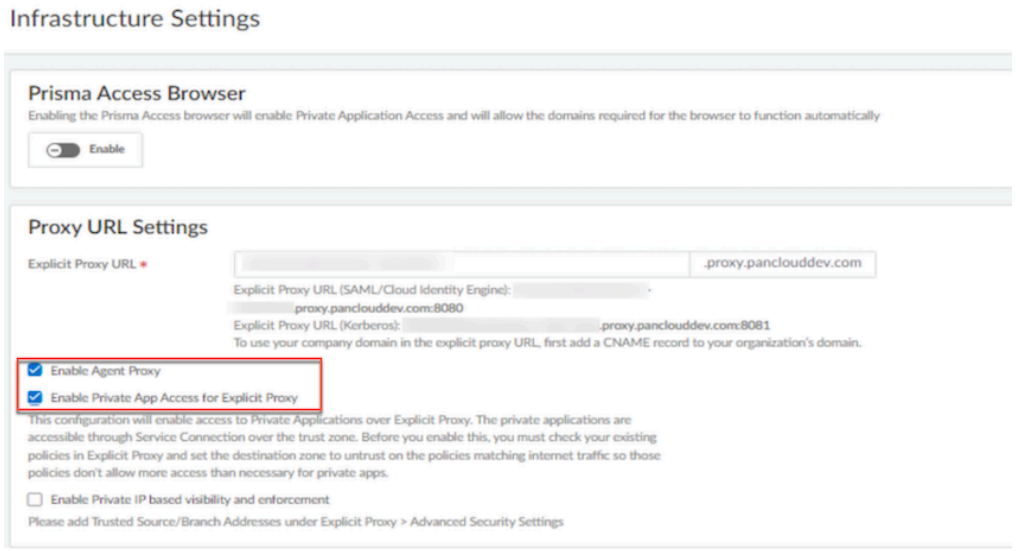
- プライベートアプリケーションアクセスを有効にするにはPrisma Access Browserを使用します。
  1. [ワークフロー] > [Prisma Access セットアップ] > [明示的なプロキシ] > [インフラストラクチャ設定] [を有効にする]Prisma Access Browser を選択します。[プロキ

©2025 Palo Alto Networks, Inc.

シ**URL**設定]で、[明示的なプロキシのプライベート アプリ アクセスを有効にする]を選択します。



- 通常のブラウザを使用してプライベート アプリケーション アクセスを有効にします。
  1. [ワークフロー] > [**Prisma Access** セットアップ] > [明示的なプロキシ] > [インフラストラクチャ設定] > [エージェント プロキシを有効にする] > [明示的なプロキシのプライベート アプリ アクセスを有効にする]を選択します 。

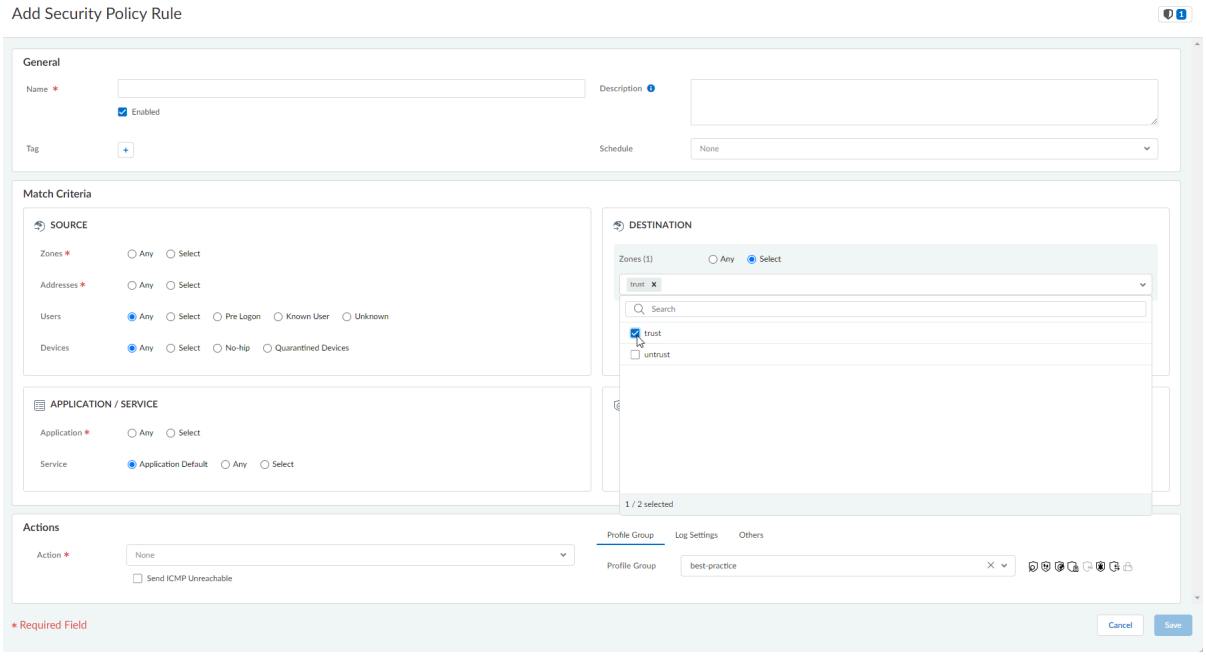


 ©2025 Palo Alto Networks, Inc.

STEP 5 | アクセスするデータセンター リソースのセキュリティ ポリシー ルールを作成します。

1. [管理] > [構成] > **[NGFW**と**Prisma Access]**に移動し、[構成スコープ] を**[Prisma Access]** > [モバイルユーザー コンテナ] > [明示的プロキシ]に設定して、[セキュリティ ポリシー] > [セキュリティ サービス]を選択します。
2. セキュリティ ポリシー ルールを作成します。

データ センター アクセスのルールでは、宛先の下のゾーンがトラストに設定されていることを確認します。



STEP 6 | 明示的なプロキシでプライベート アプリケーション アクセスを有効にする場合は、ZTNA コネクタをオンボードした後、 構成をプッシュして構成の変更を保存します。

明示的なプロキシを使用してデータセンターにアクセスする（Panorama）

STEP 1 | サービス接続、Colo-ConnectおよびZTNAコネクタ を要件に応じて設定します。

STEP 2 | DNSセキュリティの設定

STEP 3 | ゾーン マッピングを構成します。

1. **[Panorama]** > [クラウド サービス] > [構成] > [モバイル ユーザー - 明示的なプロキシ] > [ゾーン マッピング]を選択します。
2. データセンター リソースにアクセスするために使用するゾーンを **Trusted Zones (**トラスト ゾーン)に追加します。

©2025 Palo Alto Networks, Inc.

STEP 4 | インターネット宛てのトラフィックのポリシー ルールの 宛先ゾーンが 、任意のゾーンではなく、アントラスト ゾーンに設定されていることを確認します。

この手順を実行しないと、データ センターへの意図しないアクセスが発生する可能性があります。

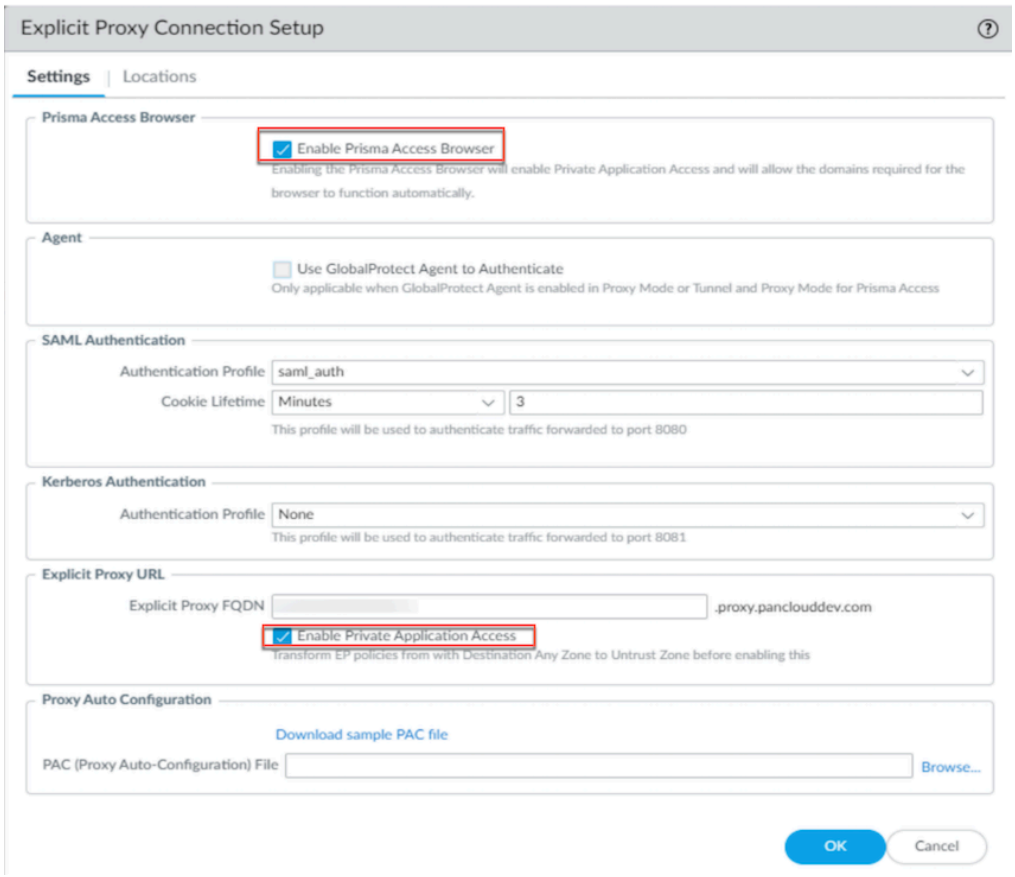
1. ポリシーを選択します。
2. デバイス グループを**Explicit_Proxy_Device_Group**に設定します。
3. 宛先ゾーンを任意から先のステップで設定したアントラスト ゾーンの1つに変更する。

©2025 Palo Alto Networks, Inc.

STEP 5 | プライベートアプリケーションアクセスを有効にします。

- プライベートアプリケーションアクセスを有効にするには Prisma Access Browserを使用します。

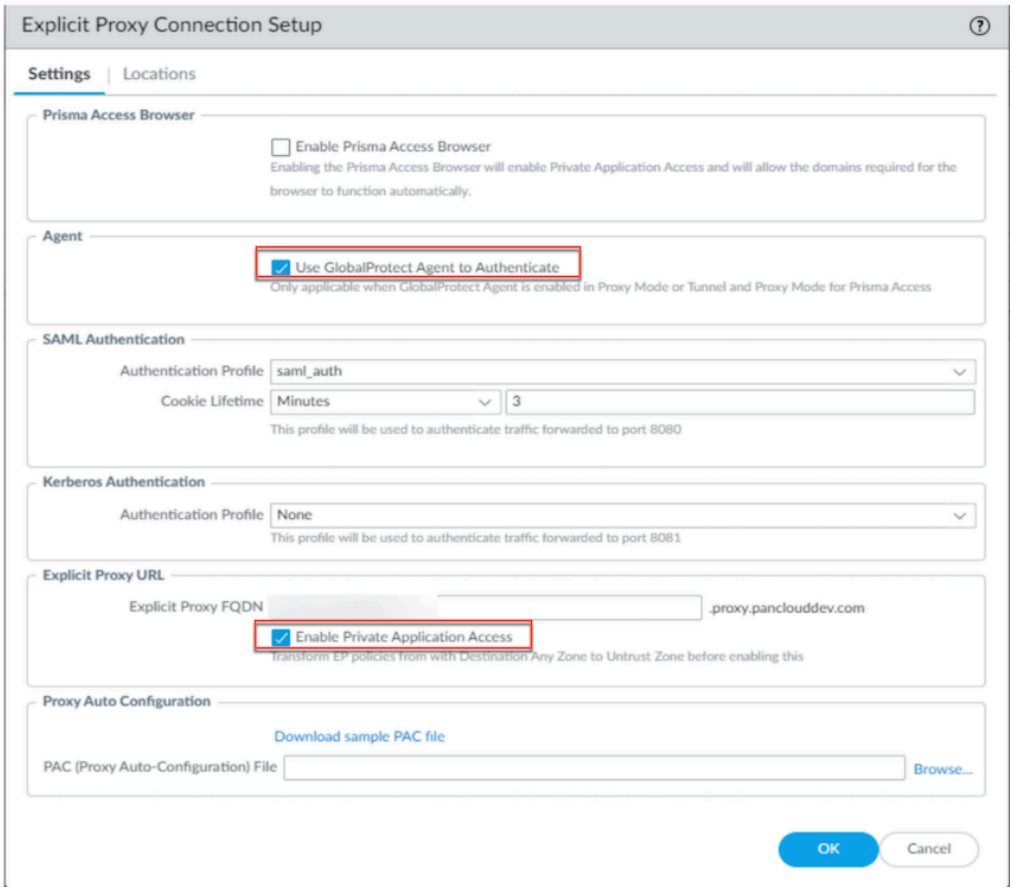
  1. **[Panorama]** > **[Cloud Services]** > [構成] > [モバイル ユーザー - 明示的なプロキシ] > [設定]に移動します > [詳細設定] > **[Prisma Access Browser** を有効にする] > [プライベートアプリケーションアクセスを有効にする]



- 通常のブラウザを使用してプライベート アプリケーション アクセスを有効にします。

  1. **[Panorama]** > **[Cloud Services]** > [構成] > [モバイル ユーザー - 明示的なプロキシ] > [設定] > [詳細設定] > **[GlobalProtect**エージェントを使用して認証] > [プライベートアプリケーションアクセスを有効にする]

©2025 Palo Alto Networks, Inc.



に移動します

STEP 6 | アクセスするデータセンター リソースのセキュリティ ポリシー ルールを作成します。

1. ポリシーを選択します。
2. デバイス グループを**Explicit_Proxy_Device_Group**に設定します。
3. セキュリティポリシールールを作成します。

   データ センター アクセスのルールでは、前の手順で設定したトラストゾーンを使用していることを確認します。

明示型プロキシを使用したアプリケーションベースのOffice 365統合

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• モバイル ユーザー ライセンス

Office 365のブラウザーベースバージョンをExplicit Proxy (明示型プロキシ)と統合する方法について説明します。

©2025 Palo Alto Networks, Inc.

- Strata Cloud Manager
- Panorama

明示型プロキシを使用したアプリベースのOffice 365統合 (Panorama)

Prisma AccessExplicit Proxy (明示型プロキシ)は、Office Online (office.com) を含む、ブラウザーベースのバージョンのOffice 365 (M365) をサポートします。ブラウザーベースのバージョンのOffice 365を明示型プロキシと統合するには 、次の手順に従います。

明示型プロキシはOffice 365のアプリベース バージョンをサポートしていませんが、次のガイドラインに従って、明示型プロキシをOffice 365アプリベース ポリシーで使用できます。

Prisma Access明示型プロキシによるブラウザベースのOffice 365統合のセットアップ

ブラウザベースのバージョンのOffice 365を使用する場合は、次のタスクを実行してOffice 365を明示型プロキシと統合します。

STEP 1 | (任意) テナントベースの制限 (Office 365へのアクセス制御を特定の数のテナントのみに制限する) を使用する場合は、 カスタムURLカテゴリでHTTPヘッダー挿入を 使用して、特定のテナントがOffice 365にアクセスできるようにします。

STEP 2 | Office 365に使用されるURLの復号化ポリシーを追加します。

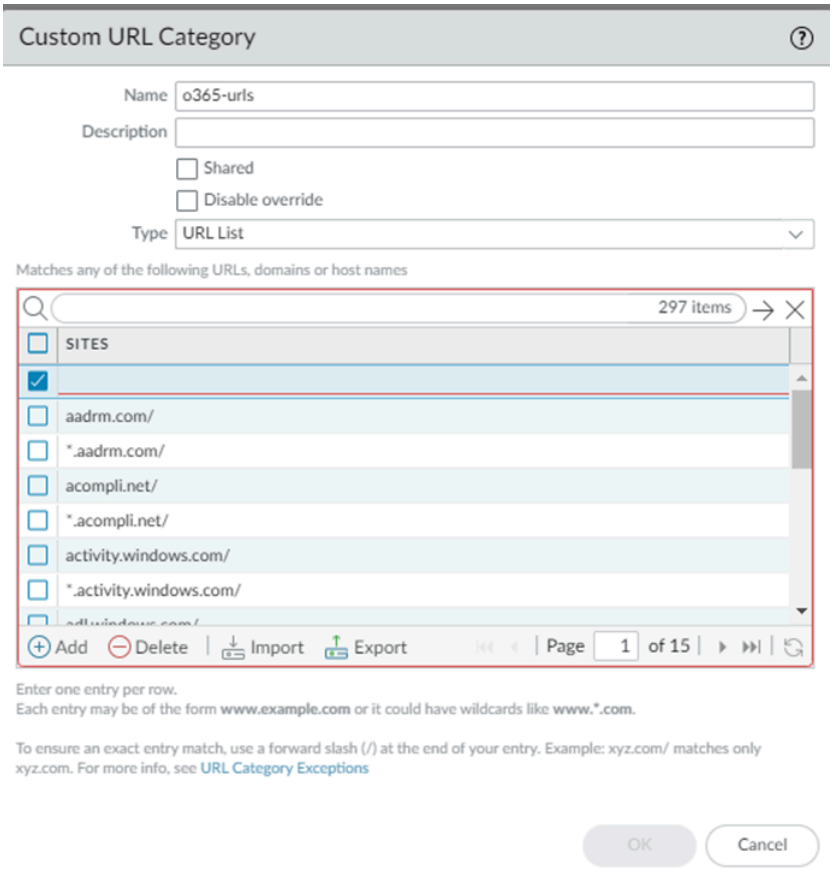
1. **Objects (オブジェクト) > Custom Objects (カスタム オブジェクト) > URL Category (URL カテゴリ)** を選択してカスタムURLカテゴリを **Add (追加)** します。

   Explicit_Proxy_Device_Groupに属していることを確認してください。
2. **URL**リストの タイプ を指定します。
3. Office 365 統合を有効にするサイトのリストを追加します 。

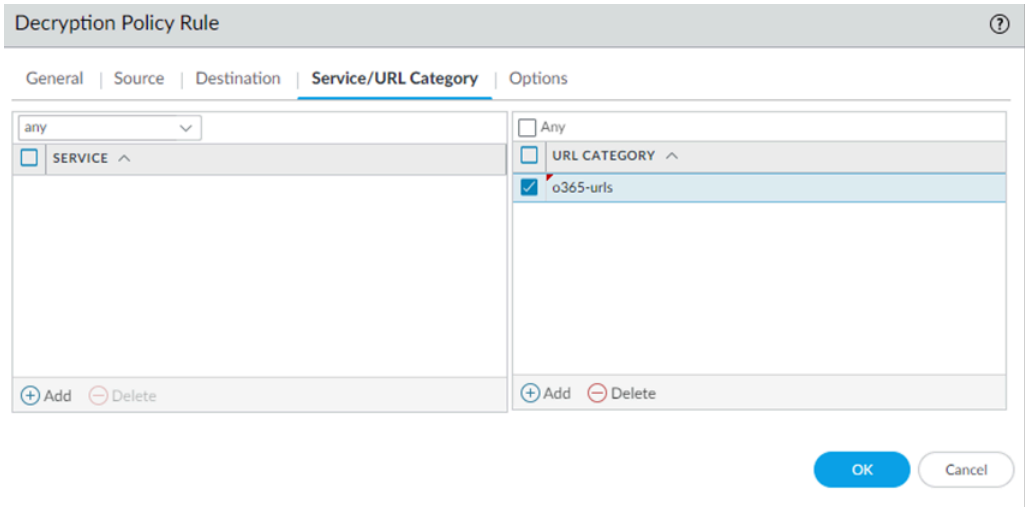
   URL のアップロードを簡素化するには、https://saasedl.paloaltonetworks.com/feeds/m365/worldwide/any/all/urlにある Office 365 URL のリストをコピーし、それらの

©2025 Palo Alto Networks, Inc.

URL をファイルに保存して、そのファイルをカスタム URL カテゴリに インポートします。



4. **Policies** (ポリシー) > **Decryption** (復号化) > **Pre Rules** を選択し、復号ポリシー ルールを **Add** (追加) します。
5. 作成した**URL** カテゴリを指定します。



6.

©2025 Palo Alto Networks, Inc.

STEP 3 | エンタープライズ データ損失防止 (エンタープライズDLP)、WildFire、 脅威防御、SaaSセキュリティなどのデータおよび脅威防止機能の復号化ポリシーを追加します。

STEP 4 | EDL ホスティング サービス を使用して、 外部の動的リストを作成します。

STEP 5 |

明示型プロキシを使用したアプリベースの**Office 365**統合をセットアップする

明示型プロキシは、Office 365の完全なクライアント ベース (アプリ) バージョンをサポートしていません。これは、Office 365がWeb以外のポートとプロトコル、および固定された証明書を使用しており、復号化が使用できないためです。Office 365クライアント アプリからのトラフィックをセキュリティで保護する必要がある場合は、次のいずれかのPrisma Access機能を使用できます。

- 明示型プロキシを使用してモバイル ユーザー - GlobalProtectデプロイメントを デプロイし、GlobalProtect分割トンネルオプションを使用してOffice 365アプリからのトラフィックをGlobalProtectトンネルにルーティングし、PACファイルとGlobalProtectトンネルの含めるオプションと除外オプションに基づいて、その他のインターネット トラフィックをGlobalProtectトンネルに送信するか、インターネットに直接送信するか、明示型プロキシに送信するかを指定します。
- インターネット接続トラフィックが明示的プロキシを経由する必要がある場合、またはネットワークにデフォルトルートがない場合、明示型プロキシを使用したリモートネット トワークデプロイメント明示型プロキシを使用したリモートネット トワークデプロイメントをデプロイできます。このデプロイメントでは、明示型プロキシによってエニーキャスト アドレスとユニキャスト アドレスのリストが提供され、それらのアドレスを介してトラフィックをリモート ネットワークにルーティングし、そこから明示型プロキシとインターネットにルーティングするようにCPEを設定します。

  このデプロイメントの種類でOffice 365を使用するには、非Web Office 365 をインターネットに直接バイパスするPACファイル ルールを指定します。
- GlobalProtectまたは環境内のPrisma Accessリモート ネットワークでは、明示型プロキシPACファイルを設定してOffice 365トラフィックをバイパスできます。バイパスするにはURL リストを使用します。

*Prisma Access*明示型プロキシによる*Office 365*統合を有効にする*URL*のリスト

ブラウザー以外のOffice 365アプリを明示型プロキシと統合するために使用できるオプションの1つは、Office 365関連のURLを指定し、明示型プロキシPACファイルでそれらのURLをバイパスすることです。バイパスするURLのリストを取得するには、次のいずれかの方法を使用します。

- Microsoft 365アプリには、Palo Alto NetworksDL Hosting Service (EDLホスティング サービス)のEDL URLを使用します。

  ホスティング サービスを使用すると、フィードURLをEDLソースとして利用することで、SaaSアプリケーションへのトラフィックを保護するための運用上の負担が軽減されま

 ©2025 Palo Alto Networks, Inc.

す。SaaSプロバイダーがSaaSアプリケーションの新しいエンドポイントを追加すると、対応するフィードURLが更新されます。

世界中のMicrosoft 365 URLについては、https://saasedl.paloaltonetworks.com/feeds/m365/worldwide/any/all/urlURL を使用してください。IPv4およびIPv6、国固有および政府アプリケーション用の他のURLも提供されています。

- https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-rangesでMicrosoftが提供するOffice 365 IPアドレスとURLのリストを取得します。Microsoftはhttps://learn.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-ip-web-serviceで Office 365 IPアドレスとURL Webサービスも提供しています。

Blue Coat Proxyでプロキシ チェーンを構成する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Accessライセンス。

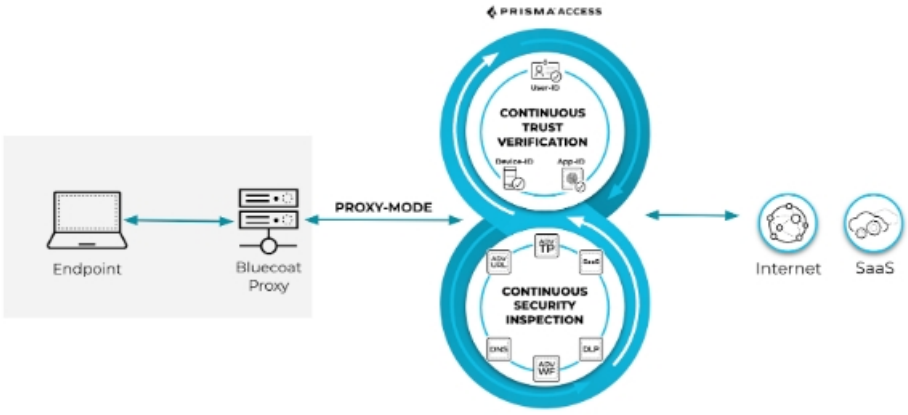
プロキシ チェーンは、セキュリティ層の追加やコンプライアンスのために、複数のプロキシ サーバーをカスケード接続して、マルチホップ インターネット パスウェイを作成します。各サーバーはトラフィックを次のサーバーに転送し、最終的にインターネットに到達します。この手法では、既存のネットワーク インフラストラクチャを使用し、上流プロキシに接続して安全なHTTPおよびHTTPS通信を可能にします。この統合により、ユーザーのブラウザ設定が保持され、セキュリティと制御が強化されます。

企業がプロキシ チェーン機能を使用する理由:

1. 多層保護を提供し、地理的制限を回避することで、プライバシーと匿名性を強化します。
2. ユーザーのブラウジング エクスペリエンスにセキュリティ層を追加することで、悪意のあるコンテンツ、スパム、フィッシング攻撃をフィルタリングし、セキュリティと制御を実現します。
3. 企業はプロキシ チェーンを使用して、ユーザーの役割や場所に基づいて特定のWebサイトやサービスへのアクセスを制限することで、内部ポリシー ルールを適用できます。
4. 新しいシステムを導入する代わりに、プロキシ チェーンを使用すると、特定のタスクのために上流のプロキシ サーバーに接続して、既存のネットワーク インフラストラクチャを利用できます。これは費用対効果が高く効率的なソリューションになります。

Prisma Access Explicit Proxyの仕組みについて詳しく学びます。

©2025 Palo Alto Networks, Inc.



顧客が、オンプレミスのBlue Coatプロキシから Prisma AccessExplicit Proxyにトラフィックをプロキシチェーンしたい場合のシナリオを以下に示します。オンプレミスのBlue Coatプロキシはユーザーを認証し、Blue CoatプロキシにX-Authenticated-User（XAU）ヘッダーを挿入してPrisma AccessExplicit Proxyにユーザー名を渡します。

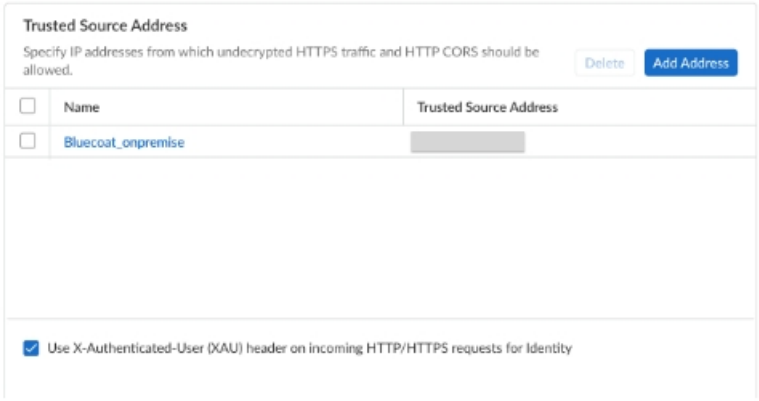
デフォルト ルートのないネットワークでは、明示型プロキシ*IP*アドレスのスタティック ルートと宛先*NAT*が必要です。

STEP 1 | Prisma Accessを構成します。

1. Explicit Proxy (明示型プロキシ)を設定します。
2. Blue Coat Explicit Proxy を信頼できるソース アドレスとして追加します。
   1. [ワークフロー] > **[Prisma Access** セットアップ] > [明示的なプロキシ] > [高度なセキュリティ設定] > **[Add Address (**アドレスを追加**)]**を選択します。
   2. Blue Coat Explicit Proxy の IP アドレスを入力します。

      *IP*アドレスまたはサブネットのいずれかを追加できます。

   3. **[ID**の着信**HTTP/HTTPS**要求で**X-Authenticated-User (XAU)**ヘッダーを使用する]を選択します。

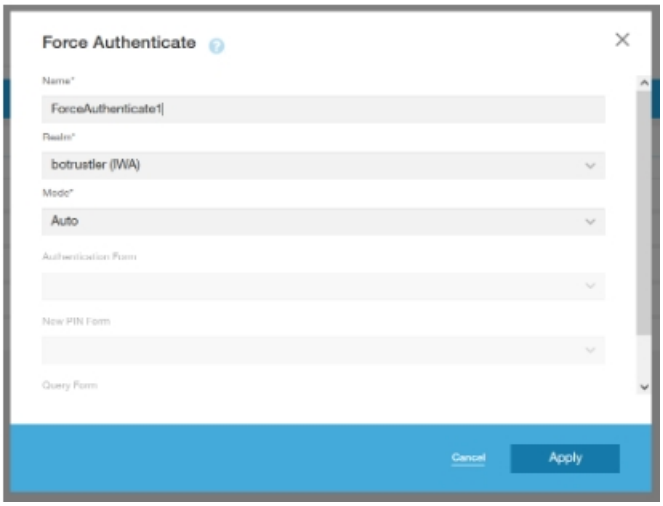


 ©2025 Palo Alto Networks, Inc.

STEP 2 | Blue Coat Proxyで設定を実行します。

1. 認証のみを実施する

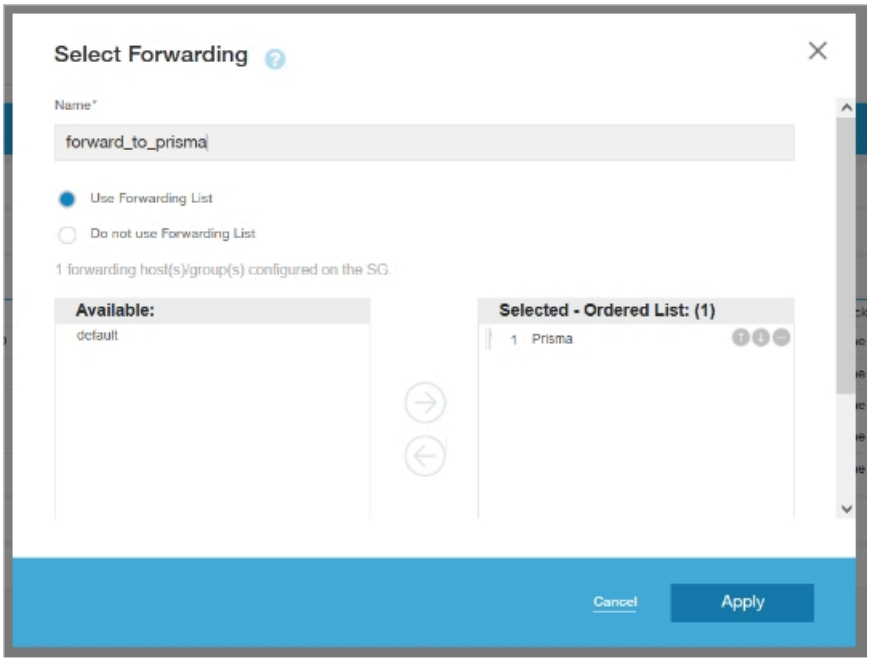




2. 転送層を構成します。



1. Prisma AccessExplicit Proxy の IP アドレスを取得します。
   1. Strata Cloud Managerで、[ワークフロー] > **[Prisma Access** セットアップ] > [明示型プロキシ] > [インフラストラクチャ設定]を選択します。
   2. プロキシ FQDN をコピーします。

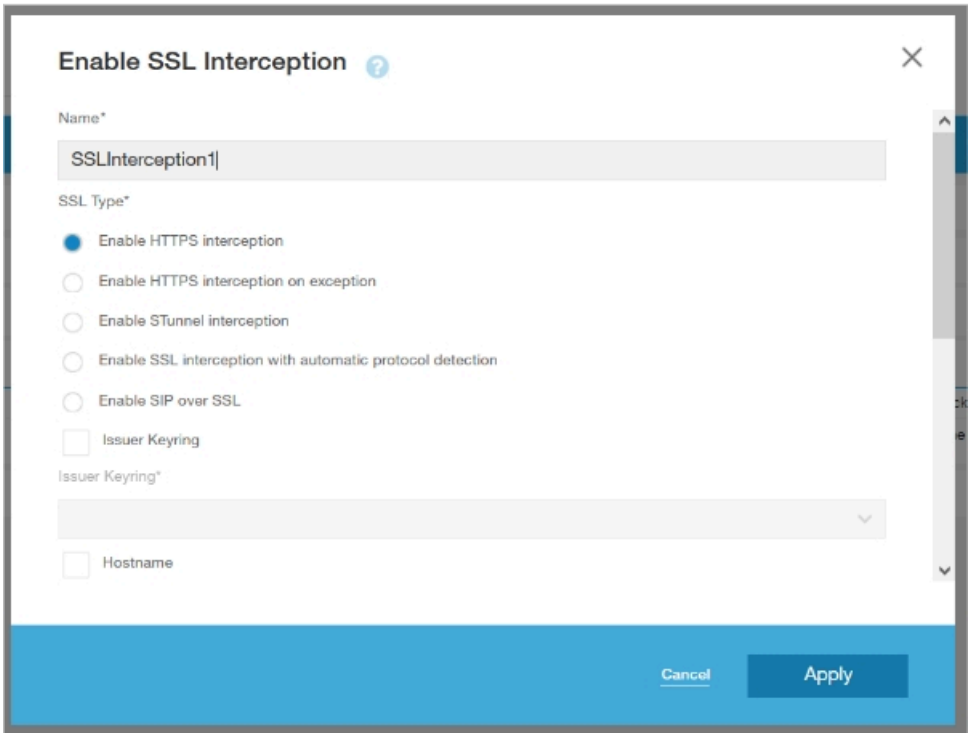


 ©2025 Palo Alto Networks, Inc.



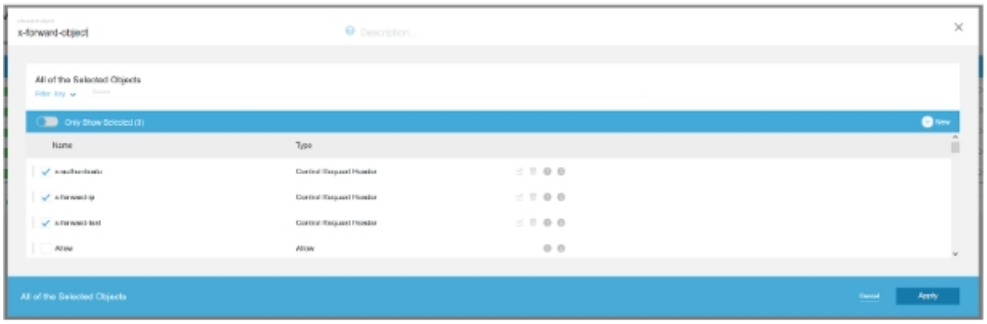
2. ヘッダー挿入のために HTTPS 復号化を有効にします。

   ヘッダー挿入には復号化が必須です。

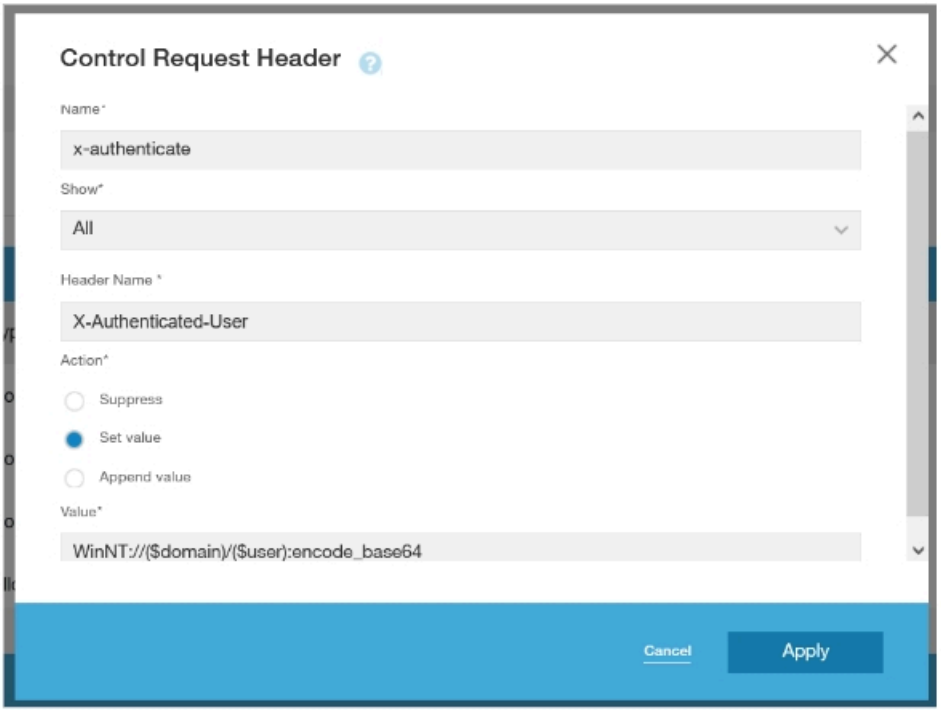


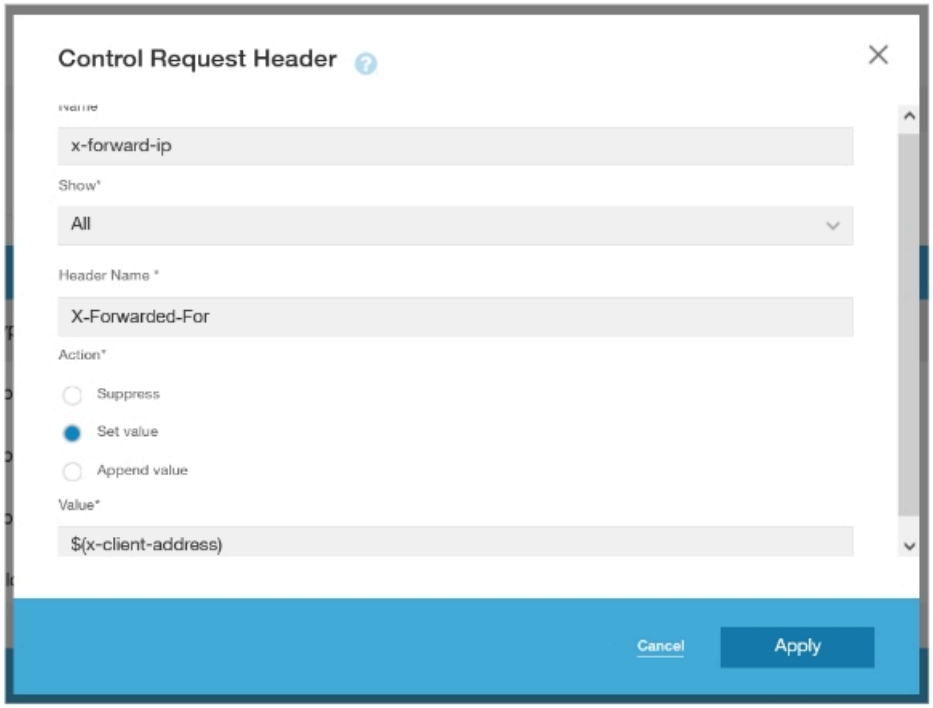


3. ヘッダー転送を設定します。



©2025 Palo Alto Networks, Inc.





XFF ヘッダーを通じて受信されたクライアント *IP* アドレスは単にログに記録されるだけで、ポリシーに活用することはできません。

4. ヘッダー値のエンコードを base64 に設定します:

```
define action Encode_All_XFF set( request.x_header.X-
Authenticated-User, "$(user:encode_base64)" ) end define action
```


©2025 Palo Alto Networks, Inc.

```
x-authenticate set( request.x_header.X-Authenticated-User,
"WinNT://($$domain)/($$user):encode_base64" ) end
```

STEP 3 | 設定を確認します。

1. Strata Cloud Managerで、 [インシデントとアラート] > [ログビューア]を選択します。
2. `X-Forwarded-For` 列と `Users` 列をチェックして、ユーザーと IP アドレス情報がPrisma Accessに表示されていることを確認します。

STEP 4 | 以下の点を考慮してください。

1. Blue Coat プロキシでは、XAU ヘッダー情報を挿入するために認証と復号化が必要です。
2. X-Authenticated-User 認証ヘッダーの値は Base64 形式である必要があります。
3. Prisma AccessExplicit Proxyは、復号化されたトラフィックのユーザー ID を確認できます。

GlobalProtect(またはサードパーティのVPN)で明示型プロキシを使用する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

明示型プロキシをGlobalProtectまたはサードパーティのVPNと組み合わせることができます。

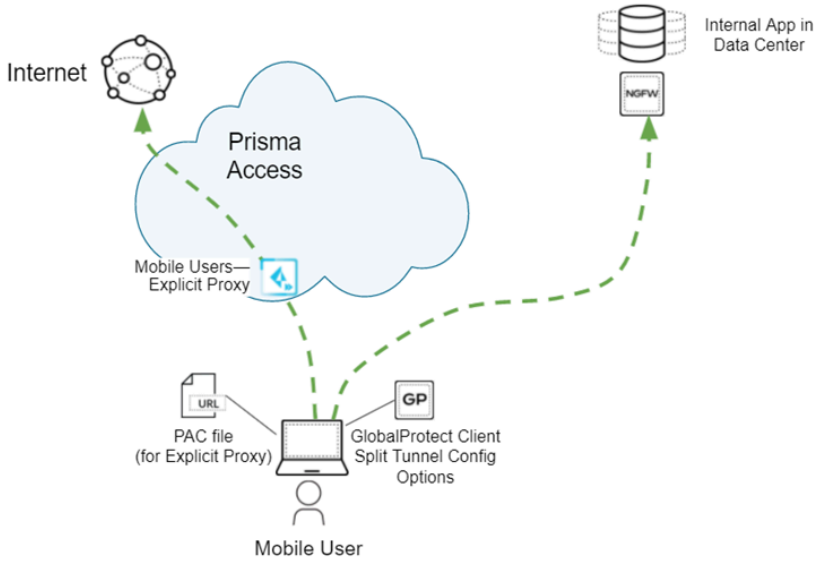
- **Explicit Proxy(明示型プロキシ)とGlobalProtect:**
  - プライベート アプリのみへの安全なアクセスを提供するには、GlobalProtectをスプリット トンネル モードで使用します。
  - 明示型プロキシを使用して、インターネット トラフィックや外部SaaSアプリケーションなどのパブリック アプリを保護します。
- 明示型プロキシとサードパーティの**VPN**

  データセンターやプライベート アプリケーションへのアクセスにVPNクライアントを使用している場合は、明示型プロキシとPACファイルを使用してパブリック アプリへのアクセスを保護しながら、引き続きそのクライアントを使用してプライベート アプリへのアクセスを保護することができます。明示型プロキシをモバイル ユーザーに近い場所にデプロイできるため、Webセキュリティのためにトラフィックをデータセンターにバックホールする必要がなくなります。

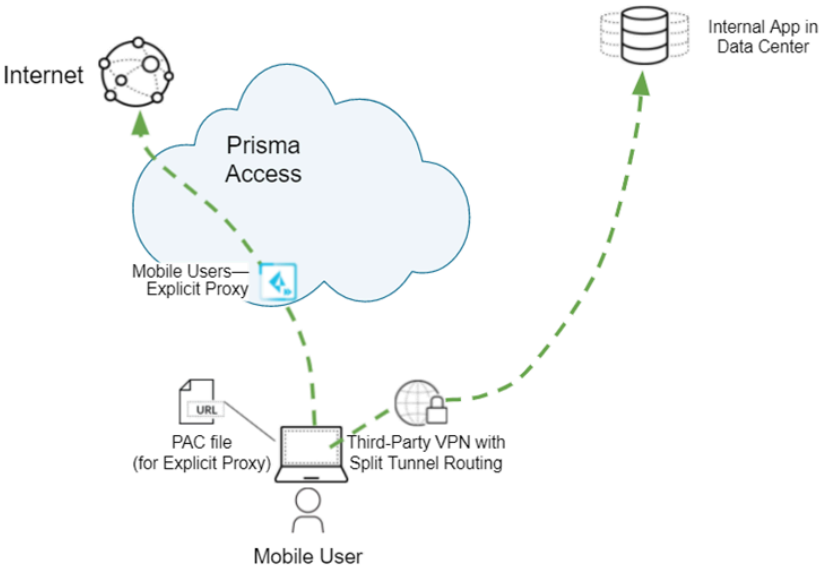
次の図は、GlobalProtectゲートウェイと明示型プロキシを使用したデプロイメントを示したものです。GlobalProtectは、GlobalProtectクライアントを使用してトラフィックをPalo Alto Networks次世代ファイアウォールにルーティングします。このデプロイメントを構成するには、GlobalProtectで分割トンネル構成を作成し、プライベート アプリをGlobalProtectで保護

©2025 Palo Alto Networks, Inc.

し、パブリック アプリを明示型プロキシで保護できるようにします。構成が完了すると、モバイル ユーザーは GlobalProtect を使用して組織のデータセンター内のプライベート アプリに接続し、明示型プロキシを使用してプライベート インターネット ベースのアプリに接続します。



サードパーティの VPN をお持ちの場合は、次の図に示すように、明示型プロキシを使用してパブリック アプリを保護しながら、それを使用してデータセンター内のプライベート アプリに接続できます。



始めましょう：

- 動作の仕組み
- Explicit Proxy(明示型プロキシ) – ガイドライン
- Explicit Proxy(明示型プロキシ)とGlobalProtect:セットアップ
- 明示型プロキシとサードパーティのVPN

©2025 Palo Alto Networks, Inc.

GlobalProtectまたはサードパーティVPNで明示型プロキシを使用するための要件

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

構成を開始する前に、GlobalProtectまたはサードパーティのVPNを使用して明示型プロキシをデプロイするために必要な要件と推奨事項に従っていることを確認してください。

- GlobalProtect で明示型プロキシを使用するには、GlobalProtect (モバイル ユーザー - GlobalProtect デプロイメント、または GlobalProtectゲートウェイとポータルを使用するスタンドアロン GlobalProtectデプロイメント) をデプロイする必要があります。

  GlobalProtectでsplit tunnel(分割トンネル)構成を構成します。このセクションの例では、ドメイン (URL) またはアプリケーションに基づいてトラフィックが分割されていますが、 アクセス ルートに基づいてトラフィックを分割することもできます。

  GlobalProtectで split DNS (分割DNS) オプションを構成して、VPN割り当てDNSサーバーによって解決されるドメインと、ローカルDNSサーバーによって解決されるドメインを構成することもできます。
- 明示型プロキシプロキシをサードパーティのVPNで使用するには、VPNソリューションを展開する必要があります。
- モバイル ユーザー - GlobalProtectまたはサードパーティのVPNデプロイメントで保護するアプリケーションのリストを作成します。

  たとえば、GlobalProtectを使用して明示型プロキシを構成する場合は、プライベート アプリまたはリソースへのすべてのアクセスを保護するようにGlobalProtectを構成し、パブリック アプリまたはSaaSアプリケーションを保護するように明示型プロキシ PACファイルを構成する必要があります。このセクションの構成例では、GlobalProtectが内部ドメインを解決し、Explicit Proxyが外部ドメインを解決します。
- 明示型プロキシとGlobalProtectまたはサードパーティのVPNの認証を構成します。
  - 明示型プロキシの場合は、SAML認証を使用する必要があります。SAMLサインオンに使用するURLを含む、明示型プロキシのデプロイメントでSAMLを構成するためのガイドラインに従います。
  - モバイル ユーザー - GlobalProtectデプロイメントの場合、アイデンティティ プロバイダー (IdP) としてOktaを使用してSAML認証を使用する場合は、「Prisma Access 統合ガイド (Panorama 管理)」で「Okta を使用してSAML認証を構成する」手順を参照してください。
  - スタンドアロンGlobalProtectデプロイメントの場合、PAN-OSでSAML 認証を設定できます。
  - サードパーティのVPNについては、その VPNの製品ドキュメントを参照してください。

  Palo Alto Networksでは、各モバイルユーザのエンドポイント上のデフォルトブラウザをSAML認証に使用することを推奨しているため、明示型プロキシのセットアップに示すようにポータル構成を編集することで、シングル サインオン (SSO) を利用できます。

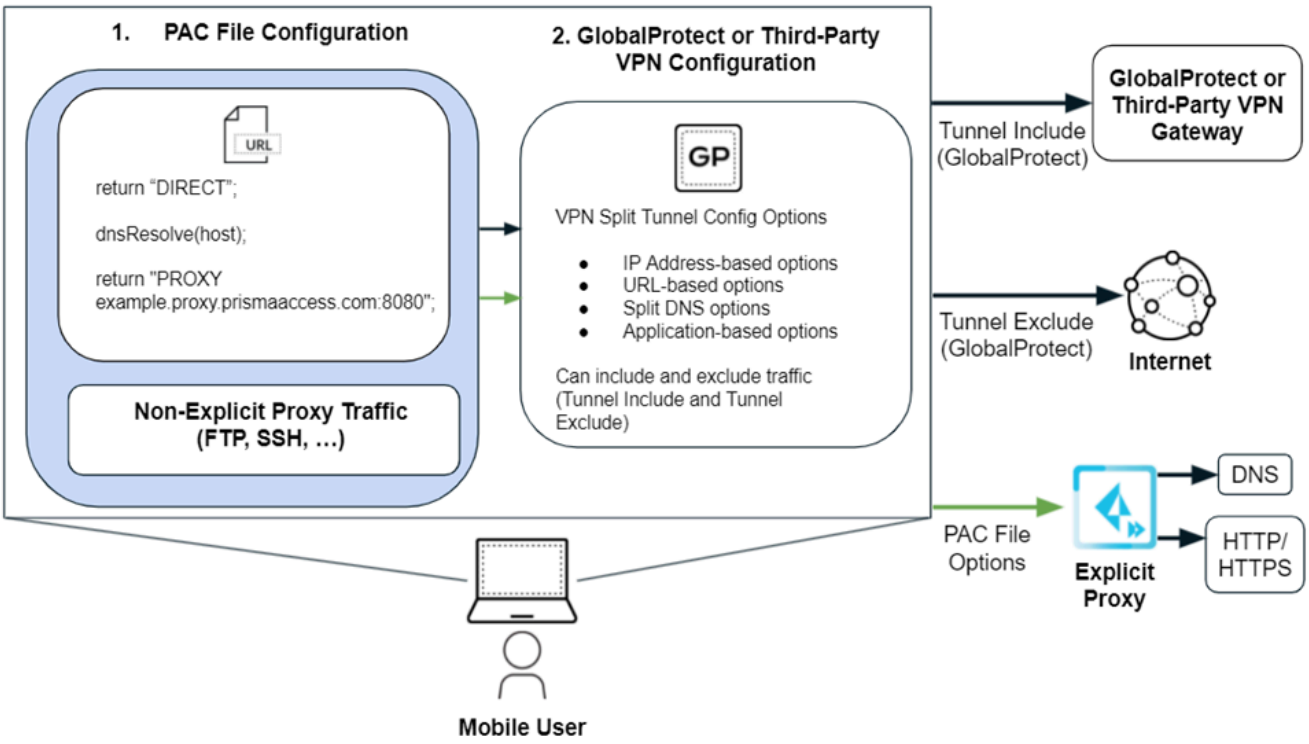
©2025 Palo Alto Networks, Inc.

- モバイル ユーザーが使用するブラウザーがPACファイル内の構成に従っていることを確認する必要があります。

Explicit Proxy(明示型プロキシ)とGlobalProtect:動作の仕組み

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

Explicit Proxyで保護すべきアプリケーションやトラフィックを決定し、GlobalProtectまたはサードパーティ製VPNで保護すべきアプリケーションを決定する前に、GlobalProtectとPrisma AccessがExplicit ProxyとVPN構成に基づいてどのように転送を決定するかを理解しておく必要があります。このセクションの例では、Explicit Proxy(明示型プロキシ)とGlobalProtectを組織のネットワークにすでにデプロイし、GlobalProtect 分割トンネルオプションを設定していることを前提としています。次の図はそのプロセスを示しています。



モバイルユーザーがプライベートまたはインターネットベースのリソースまたはアプリをリクエストすると、そのリクエストはエンドポイントのExplicit Proxy PACファイルによって評価されます。

©2025 Palo Alto Networks, Inc.

- PAC ファイルの `return"DIRECT";` 関数を使用すると、式で指定されたトラフィックはExplicit Proxy(明示型プロキシ)処理をバイパスします。

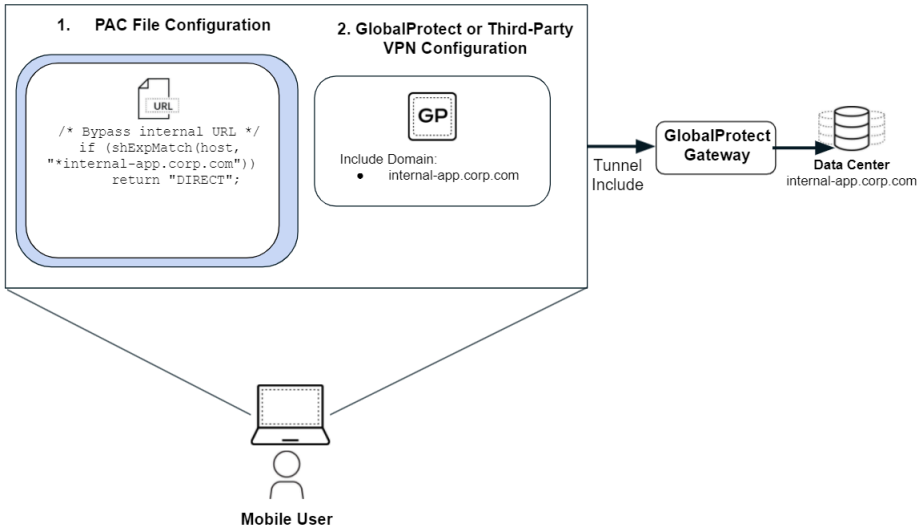
  Explicit Proxyには、IPアドレスとURLを指定した `return"DIRECT";` 関数を使用するサンプルPACファイルが用意されています。PACファイルの内容と使用方法の説明については、」を参照してください。
- PAC ファイルの `dnsresolve (host)` 関数により、エンドポイントはDNSクエリを実行して、ホスト名をIPアドレスに解決します。次に、このクエリはVPNポリシー（スプリットトンネルやスプリットDNSなど）に従ってDNS要求を宛先DNSサーバに転送します。

  Explicit Proxyで提供されるPACファイルでは、`dnsresolve(host)`, `return"DIRECT";`、およびプライベートIPアドレスが1つの式にまとめられています。DNSルックアップ後、返されたIPアドレスが式内のプライベートIPアドレスに含まれる場合、プライベートIPアドレスに関連付けられたトラフィックはExplicit Proxy(明示型プロキシ)処理をバイパスします。
- PACファイルで`return "PROXY sitename :8080";`として指定されたトラフィックは、Explicit Proxyに転送されます。

PACファイルの条件に基づいてウェブリクエストが評価された後、エンドポイントのGlobalProtectまたはサードパーティのVPN構成に送信されて処理され、トラフィックはGlobalProtectアプリケーションでスプリットトンネル構成オプションについて評価されます。ドメイン (URL)、アプリケーション、またはサブネットに基づいてトラフィックを分割できます。GlobalProtectで[split DNS (DNS分割)] オプションを設定した場合、トラフィックもそのDNSオプションに基づいて評価されます。

トラフィックが処理されると、PACファイルとVPN処理に基づいてGlobalProtectに直接送信されるか、インターネットに直接送信されるか、Explicit Proxyに送信されます。

次の図は、**`internal-app.corp.com`**というURLを使用してプライベートリソースにアクセスしようとしているモバイルユーザーを示しています。



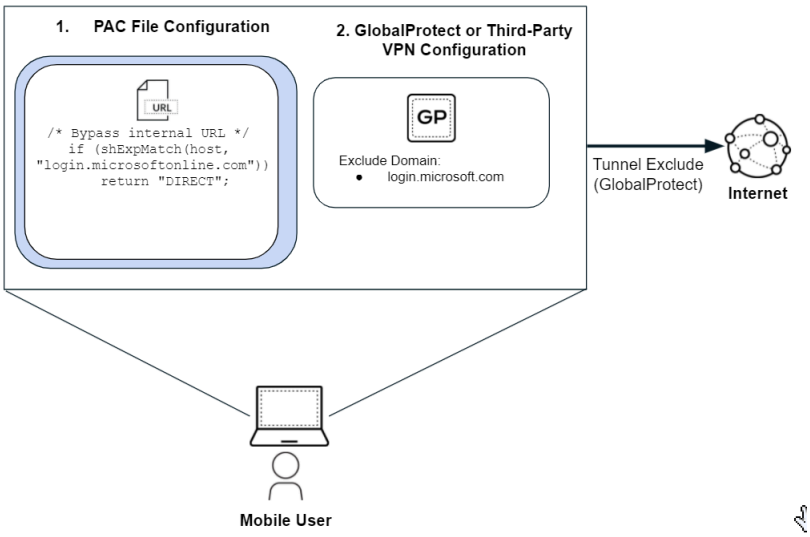
 ©2025 Palo Alto Networks, Inc.

- PACファイルには、**internal-app.corp.com**がExplicit Proxyをバイパスできるようにするための以下の設定があります。

```
    /* Bypass internal URL */ if (shExpMatch(host, "*internal-
app.corp.com")) return "DIRECT";
```

- モバイルユーザーがブラウザから**internal-app.corp.com**をリクエストすると、ブラウザはPACファイル内の条件を評価します。その評価に基づいて、ブラウザはリクエストをプロキシに転送せず、GlobalProtectアプリケーションに直接送信します。
- GlobalProtectは、**internal-app.corp.com**が**[Include Domain (含まれるドメイン)]**にリストされていることを指摘し、それをVPNトンネルを通して送信します。
- GlobalProtectはGlobalProtectの設定オプションに基づいて**internal-app.corp.com**のリソースにリクエストを送信します。

ログインリソースなどの一部のリソースは、Explicit Proxy、GlobalProtect、またはサードパーティのVPNを処理に使用しないように設定したい場合があります。次の図は、ユーザーがブラウザから**login.microsoftonline.com**と入力してマイクロソフトオンラインにログインしているところを示しています。



- PACファイルには、**internal-app.corp.com**がExplicit Proxyトラフィックをバイパスできるようにするための以下の設定があります。

```
    /* Bypass internal URL */ if (shExpMatch(host,
 "login.microsoftonline.com")) return "DIRECT";
```

- モバイルユーザーがブラウザから**login.microsoftonline.com**を要求すると、PACファイルはモバイルユーザーのエンドポイントのPACファイルからの要求を評価し、それをGlobalProtect VPN設定（この場合はGlobalProtect）に送信して処理します。
- GlobalProtectアプリケーションは、**login.microsoftonline.com**が**[Exclude Domain (除外ドメイン)]**にリストされていることを認識しています。

©2025 Palo Alto Networks, Inc.

- GlobalProtectはVPNをバイパスし、GlobalProtectの設定オプションに基づいてリクエストをインターネットに直接送信します。

Explicit Proxy(明示型プロキシ)とGlobalProtect:セットアップ

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

モバイル ユーザーが安全に接続できるようにするには、明示型プロキシとGlobalProtectまたはサードパーティのVPNを組み合わせることができます。

- Explicit Proxy(明示型プロキシ)とGlobalProtect:
  - プライベート アプリのみへの安全なアクセスを提供するには、GlobalProtectをスプリット トンネル モードで使用します。
  - 明示型プロキシを使用して、インターネット トラフィックや外部SaaSアプリケーションなどのパブリック アプリを保護します。
- 明示型プロキシとサードパーティのVPN
  - データセンターやプライベート アプリケーションにアクセスし、プライベート アプリへのアクセスを保護するには、VPN クライアントを使用します。
  - 明示型プロキシとPACファイルを使用して、パブリック アプリへのアクセスを保護します。

明示型プロキシとGlobalProtectまたはサードパーティVPNで保護すべきアプリケーションまたはトラフィックを決定する前に、GlobalProtectとPrisma Accessが明示型プロキシとVPN構成に基づいてどのように転送を決定するかを理解しておく必要があります。

モバイル ユーザーがプライベートまたはインターネット ベースのリソースやアプリを要求すると、その要求はエンドポイントにインストールされている明示型プロキシ PAC ファイルに送信されます。

- PACファイルで return "DIRECT" として指定されたトラフィックは、明示型プロキシ処理をバイパスします。DNS 解決 (ホスト) は、"DIRECT" を返します。指定された IP パスの明示型プロキシ処理を許可します。
- PACファイルで return "PROXY sitename:8080"; として指定されたトラフィックは、明示型プロキシに転送されます。

トラフィックが処理された後、PACファイルとVPN処理に基づいて、GlobalProtectに送信されたり、インターネットに直接送信されたり、明示型プロキシに送信されたりします。

PACファイルには、「internal-app.corp.com」が明示型プロキシをバイパスできるようにする設定があります。モバイルユーザーがブラウザからinternal-app.corp.comをリクエストすると、ブラウザはPACファイル内の条件を評価します。GlobalProtectは、internal-app.corp.comが[Include Domain (含まれるドメイン)]にリストされていることを指摘し、それ

©2025 Palo Alto Networks, Inc.

をVPNトンネルを通して送信します。GlobalProtectはGlobalProtectの設定オプションに基づいてinternal-app.corp.comのリソースにリクエストを送信します。

- Strata Cloud Manager
- Panorama

Explicit Proxy(明示型プロキシ)とGlobalProtect:セットアップ（Strata Cloud Manager）

GlobalProtect - Explicit Proxy(明示型プロキシ)を使用したモバイル ユーザーを実装するには、次の手順を実行します。

これらの設定手順では、ネットワーク環境について次のことを前提としています。ネットワーク環境が異なる場合は、設定も異なる可能性があります。

- モバイル ユーザーは、GlobalProtectポータルのホスト名、ゲートウェイFQDN、Explicit Proxy(明示型プロキシ)URL、およびPACファイルURLにアクセスして解決できます。

  この情報は、次の場所で確認できます。

  - **GlobalProtect**ゲートウェイ**FQDN** と ポータル ホスト名

    # [Workflows (ワークフロー)] > [Prisma Accessセットアップ**] > [GlobalProtect] > [Infrastructure (**インフラストラクチャ**)]**へと移動し、 インフラストラクチャ設定を編集します。

  - 明示型プロキシ**URL** と **PAC**ファイル**URL**

    # [Workflows (ワークフロー**)] > [Prisma Access**セットアップ**] > [Explicit Proxy (**明示型プロキシ**)] > [Infrastructure (**インフラストラクチャ**)]**へと移動し、 インフラストラクチャ設定を編集します。

- モバイル ユーザーはGlobalProtectから内部ドメインを解決できます。

STEP 1 | GlobalProtectに送信するアプリケーションとExplicit Proxyに送信するアプリケーションを決定します。

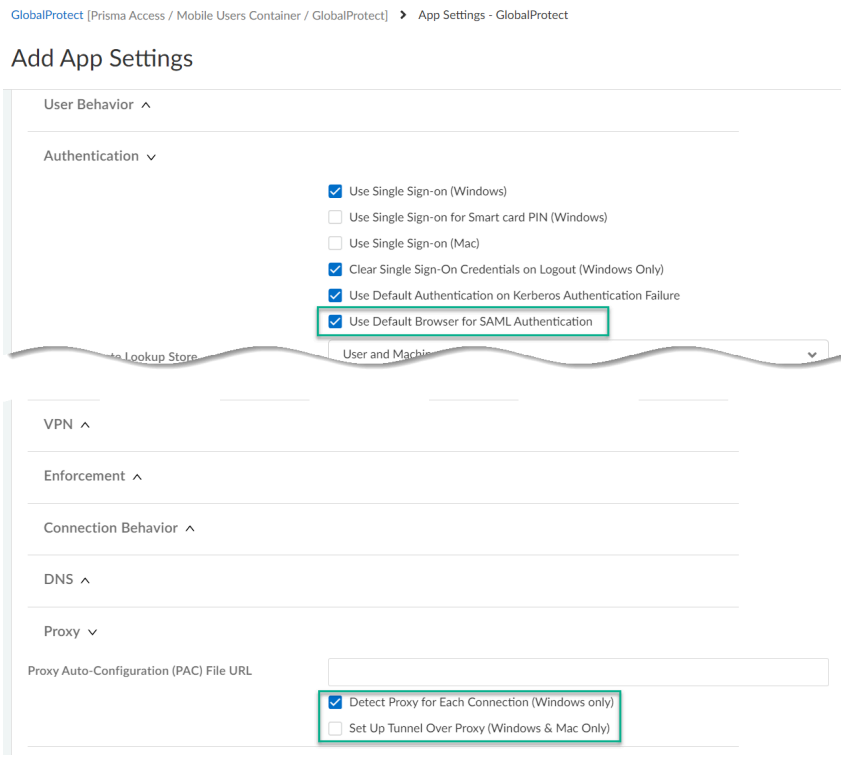
次の手順では、データセンターでホストされているプライベート アプリケーションをGlobalProtectに送信し、インターネットおよびパブリック SaaS アプリケーションへの要求をExplicit Proxyに送信します。

©2025 Palo Alto Networks, Inc.

STEP 2 | GlobalProtectポータルの設定。

[GlobalProtect] > [アプリケーション設定] > **[アプリケーション設定]** > **[詳細設定]**へ移動

1. **Proxy(**プロキシ**)**設定で以下を実施します。
   - **Detect Proxy for Each Connection**（接続ごとにプロキシを検出）をチェック
   - **Tunnel Over Proxy** のセットアップ（**Windows**および**Mac**のみ）をクリア
2. **Authentication(**認証**)**設定で以下を実施します。
   - **Use Default Browser for SAML Authentication (SAML** 認証にデフォルトのブラウザを使用**)**をチェック



STEP 3 | 内部トラフィックをGlobalProtectに誘導できるように、GlobalProtectで分割トンネルを作成します。

[GlobalProtect] > **[Tunnel Settings (**トンネル設定**)]** > **[Split Tunneling (**分割トンネリング**)]**に移動します。ドメイン (FQDN)、アクセス ルート、またはアプリケーションに基づいて分割トンネルを設定します。

STEP 4 | GlobalProtect分割トンネルに指定したドメインを除外するようにPACファイルを設定します。

PACファイルをダウンロードして編集するには、 **[Workflows (**ワークフロー**)]** > **[Prisma Access**セットアップ**]** > **[Explicit Proxy (**明示型プロキシ**)]** > **[Infrastructure (**イン

©2025 Palo Alto Networks, Inc.

フラストラクチャ)] > **[Infrastructure Settings (インフラストラクチャ設定)]** > **[Proxy Auto Configuration (プロキシ自動設定)]**

次の例は、内部プロキシをバイパスしてプライベート アプリ (internal-app.corp.com) をホストするURLを含むPACファイルを示しています。次のPACファイル内のパラメータはすべてサンプル値です。

- ポータルのホスト名は `splittunnel.gpcloudservice.com`です。
- モバイル ユーザー ゲートウェイは、ワイルドカードFQDN`*examplegateways.gw.gpcloudservice.com`に含まれています。
- PACファイルのURLは`https://pacfileurl.pac`です。
- `internal-app.corp.com`は、モバイル ユーザー (GlobalProtect) によって保護されているプライベート アプリをホストしています。
- SAML認証にはOktaが使用されています。
- 明示型プロキシURL は`example.proxy.prismaaccess.com`です。

```
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"; }
```

Explicit Proxy(明示型プロキシ)とGlobalProtect:セットアップ（Panorama）

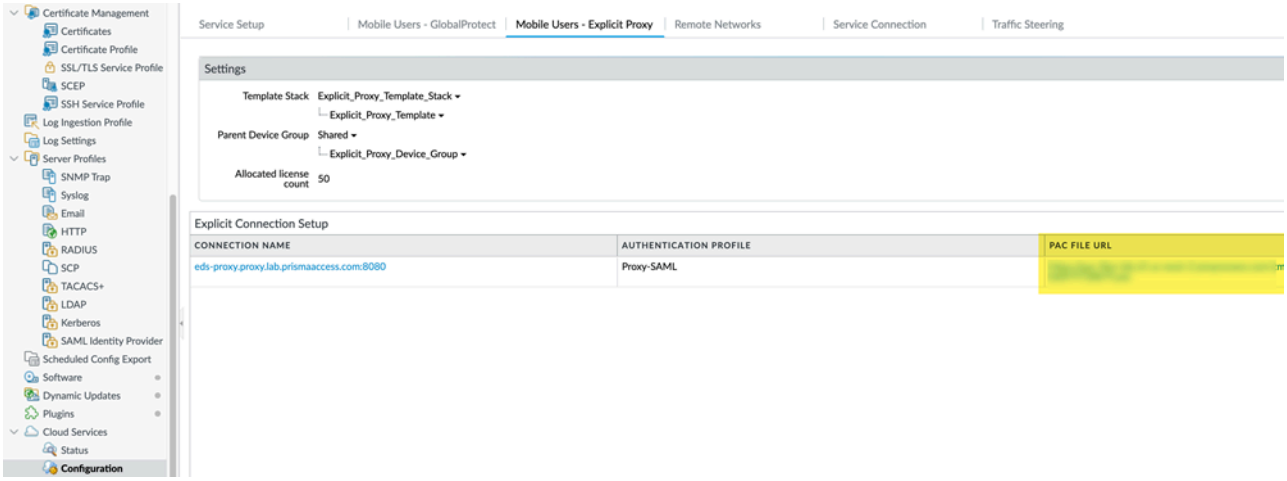
GlobalProtect - Explicit Proxy(明示型プロキシ)を使用したモバイル ユーザーを実装するには、次の手順を実行します。

これらの設定手順では、ネットワーク環境について次のことを前提としています。ネットワーク環境が異なる場合は、設定も異なる可能性があります。

- モバイル ユーザーは、GlobalProtectポータルのホスト名、ゲートウェイFQDN、Explicit Proxy(明示型プロキシ)URL、およびPACファイルURLにアクセスして解決できます。
  - ゲートウェイFQDNを見つけるには、**[Panorama]** > **[Cloud Services (クラウドサービス)]** > **[Status (ステータス)]** > **[Network Details (ネットワーク詳細)]** > **[Mobile Users—GlobalProtect (モバイルユーザー—GlobalProtect)]** > **[Gateways (ゲートウェイ)]**を選択します。

 ©2025 Palo Alto Networks, Inc.

- PACファイルのURLを見つけるには**[Panorama] > [Cloud Services (クラウドサービス)] > [Configuration (設定)] > [Mobile Users—Explicit Proxy (モバイルユーザー—明示型プロキシ)] > [PAC File URL (PACファイルURL)]**を選択します。



- モバイル ユーザーはGlobalProtectから内部ドメインを解決できます。

STEP 1 | Mobile Users-Explicit ProxyのデプロイメントとGlobalProtectのデプロイメント（Mobile Users-GlobalProtectまたはスタンドアロンの GlobalProtectのデプロイメント）を計画します。

STEP 2 | GlobalProtectに送信するアプリケーションとExplicit Proxyに送信するアプリケーションを決定します。

次の手順では、データセンターでホストされているプライベート アプリケーションをGlobalProtectに送信し、インターネットおよびパブリック SaaS アプリケーションへの要求をExplicit Proxyに送信します。

STEP 3 | Prisma Accessを管理するPanoramaで、GlobalProtectポータル設定を設定します。

1. **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル）を選択します

   [Template (テンプレート**)]**ドロップダウンから**[Mobile_User_Template]**になっていることを確認してください。
2. Prisma Accessポータル設定を編集するには、**GlobalProtect_Portal**を選択します。
3. **Agent**（エージェント）タブを選択し、**DEFAULT(**デフォルト**)**設定を選択するか、または新しい設定を**Add**（追加）します。
4. **App**（アプリケーション）タブを選択します。
5. 次のアプリの設定変更を行ってください:
   - **[Detect Proxy for Each Connection**（接続ごとにプロキシを検出）**]**で、**Yes**を選択します。
   - **Tunnel Over Proxy**のセットアップ（**Windows**および**Mac**のみ）で、**No**を選択します。
   - **Use Default Browser for SAML Authentication (SAML**認証にデフォルトのブラウザを使用**)**で、**Yes**を選択します。

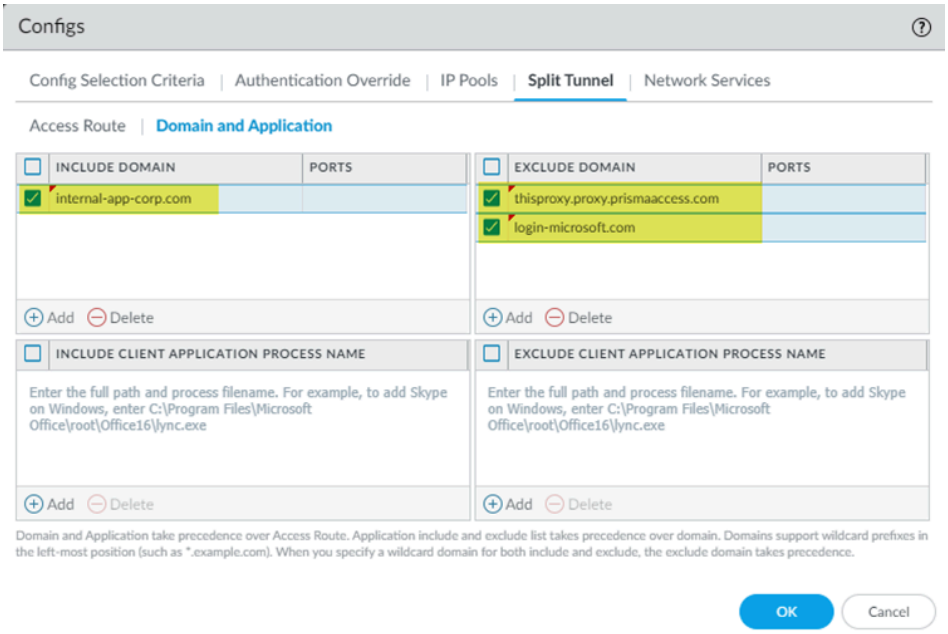
©2025 Palo Alto Networks, Inc.

STEP 4 | 内部トラフィックをGlobalProtectに誘導できるように、GlobalProtectで分割トンネルを作成します。

次の例では、ドメイン（FQDN）に基づいてトラフィックを指示するためにスプリットトンネルを使用しています。トラフィックのアクセスルートに基づいて分割トンネルを構成することもできます。

1. GlobalProtectエージェントの設定（[ネットワーク] > **[GlobalProtect]** > [ゲートウェイ] > **[GlobalProtect**外部ゲートウェイ]）で、エージェント クライアント > 設定を選択します。
2. **DEFAULT**（デフォルト）設定を選択するか、または新しく**Add**（追加）します。
3. [分割トンネル] > [ドメインとアプリケーション]を選択します。
4. **[Include Domain(**ドメインを含める)]と、任意でドメインと一緒に使用するポートを追加します。

   この例では、internal-app.corp.comをデータセンターでアプリをホストするために使用するURLとして使用しています。このURLとSAML認証URLを**Exclude Domain(**除外ドメイン)に追加します。



5. **OK** をクリックして変更内容を保存します。
6. 変更を **Commit and Push**（コミットしてプッシュ）します。

©2025 Palo Alto Networks, Inc.

STEP 5 | 分割トンネル用に入力したドメインを除外するようにPACファイルを設定します。

次の例は、内部プロキシをバイパスしてプライベート アプリ (internal-app.corp.com) をホストするURLを含むPACファイルを示しています。次のPACファイル内のパラメータはすべてサンプル値です。

- ポータルのホスト名は `splittunnel.gpcloudservice.com`です。
- モバイルユーザーゲートウェイ（**Panorama** > **Cloud Services** > **Status** > **Network Details** > **Mobile Users—GlobalProtect** > **Gateways**）は、ワイルドカードFQDN `*examplegateways.gw.gpcloudservice.com` に含まれています。
- **PAC**ファイルの**URL ([Panorama]** > **[Cloud Services (**クラウドサービス**)]** > **[Configuration (**設定**)]** > **[Mobile Users—Explicit Proxy (**モバイルユーザー—明示型プロキシ**)]** > **[PAC File URL (PAC**ファイル**URL)])** は`https://pacfileurl.pac` です。
- `internal-app.corp.com`は、モバイルユーザー（GlobalProtect）によって保護されているプライベートアプリをホストしています。
- SAML認証にはOktaが使用されています。
- 明示型プロキシのURLは`example.proxy.prismaaccess.com`です。

```
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"; }
```

明示型プロキシとサードパーティのVPN

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

サードパーティのVPNを明示型プロキシで使用するには、ネットワークに以下の変更を加える必要があります:

- インターネットトラフィックを明示型プロキシに向けるために、サードパーティのVPNを分割トンネリングを実行するように設定する必要があります。

  サードパーティのVPNの設定に関する支援が必要な場合は、サードパーティのVPNベンダーにお問い合わせください。

©2025 Palo Alto Networks, Inc.

- PACファイルを修正して、明示型プロキシが以下のVPNコンポーネントのいずれかをバイパスするようにします:
  - サードパーティのVPNに関連するIPアドレス
  - サードパーティのVPNに必要なログインURL

次の例では、PACファイルを構成して、明示型プロキシがプライベートIPアドレスを使用して内部リソースをバイパスし、認証トラフィックフローもバイパスするようにしました。

```
++++++++++++++++ function FindProxyForURL(url, host) { if
 (isPlainHostName(host) || shExpMatch(host, "*.local")
 || isInNet(dnsResolve(host), "10.0.0.0", "255.0.0.0") ||
 isInNet(dnsResolve(host), "127.0.0.0", "255.255.255.0"))
 return "DIRECT"; /* Bypass SAML for AnyConnect Azure */
 if (shExpMatch(host, "login.microsoftonline.com")) return
 "DIRECT"; if (shExpMatch(host, "login.windows.net")) return
 "DIRECT"; if (shExpMatch(host, "login.microsoft.com"))
 return "DIRECT"; /* Forward to Prisma Access */ return "PROXY
 example.proxy.prismaaccess.com:8080"; }
```

明示型プロキシ ユーザーのためのIPアドレス最適化 -プロキシ デプロイメント

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) この機能をPrisma Access環境で使用したい場合は、アカウントチームにお問い合わせください。	• Prisma Access 5.2 • Prisma Access データプレーン 10.2.4 • Panoramaプラグイン バージョン 5.2.0

IPアドレス最適化は、デプロイメント環境におけるIPアドレスの全体的な数を削減するアーキテクチャ上の拡張機能のセットです。これにより、許可リスティング ワークフローが簡素化されると同時に、耐障害性が向上し、Prisma Accessテナントの迅速なオンボーディングが可能になります。

IPアドレスの持続性

IPアドレスの持続性により、ユーザー セッションを必要とするSaaSアプリやウェブサイトをセキュリティ保護し、ユーザー セッション全体を通じてPrisma Accessの出力IPアドレスを同じに保つことができます。

SaaSアプリケーションのオンボーディングを簡素化

Prisma Accessロケーションを追加するか、既存のPrisma Accessロケーションでスケーリング イベントが発生すると、明示型プロキシのデプロイメントに新しいIPアドレスが割り当てられる可能性があります。ベストプラクティスは、新しい出力およびゲートウェイのIPアドレスを取

©2025 Palo Alto Networks, Inc.

得し、SaaSアプリケーションの許可リストに追加することです。IPアドレスの最適化により、大規模なデプロイメントで管理しなければならないIPアドレスの数を減らすことができます。

トラブルシューティング

IPアドレスの最適化の対象として特定のアプリケーションを指定する場合は、そのアプリケーションをURLカテゴリまたは外部動的リスト (EDL) に追加できます。特別なオブジェクトを構成すると、これらのオブジェクトに含まれるドメインのみがIPアドレスの最適化を受けます。

Panorama- URL カテゴリを**PANW EP IP**アフィニティ**URL**リスト として、またはEDLを**PANW EP IP**アフィニティ リストとして設定します。ワイルドカードエントリ（例 **.***） や、**.com**などのトップレベルドメインは使用しないでください。

Strata Cloud Manager- URL リスト **PANW EP IP**アフィニティ**URL**リストをサポートします。

モバイル ユーザー向けのDNS解決 - 明示型プロキシのデプロイメント

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • この機能をPrisma Access環境で使用したい場合は、アカウントチームにお問い合わせください。	❑ Prisma Accessライセンス ❑ Prisma Access バージョン 5.2.0

Prisma Accessでは、組織内部のドメインと外部のドメインの両方のドメインを解決する、DNSサーバーを指定することができます。Prisma Accessは、DNSサーバーの設定に基づいて、DNSリクエストのプロキシを行います。明示型プロキシは次の DNS 機能をサポートします。

- 明示型プロキシでサードパーティのブラウザを使用する
- Prisma Access Browser でリージョンごとの DNS サーバーを使用する

- 明示型プロキシ構成の*DNS*プロキシは、***Prisma Access*** セットアップで定義された内部*DNS*サーバー設定よりも優先されます。
- 明示型プロキシの*DNS*プロキシを有効にした後、既存の*DNS*構成を ***Prisma Access***セットアップ*]* > *[*内部***DNS***サーバー*]* から *[*ワークフロー*]* > *[****Prisma Access***セットアップ*]* > *[*明示型プロキシ*]* > *[*インフラストラクチャ設定*]* > *[****DNS***プロキシ*]*に移行する必要があります。

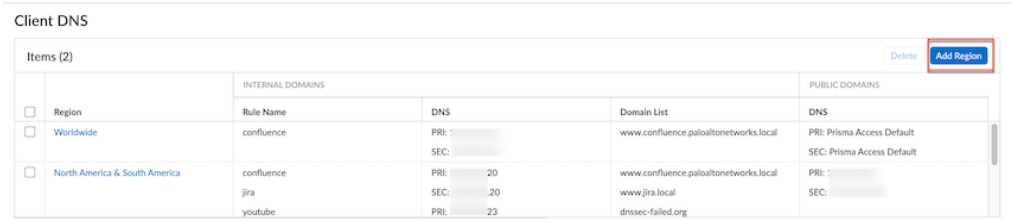
DNSセキュリティの設定

DNSプロキシ設定を構成するには、次の手順を実行します。

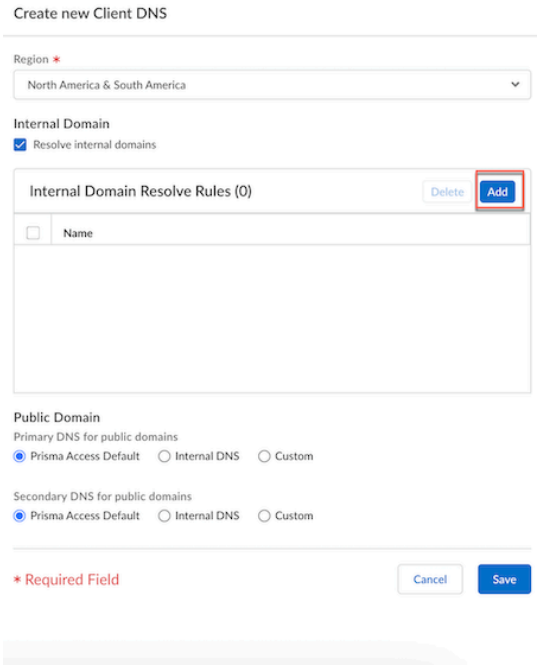
©2025 Palo Alto Networks, Inc.

1. 明示型プロキシDNSサーバー ルールを追加します。
   1. [ワークフロー] > [**Prisma Access**セットアップ] > [明示型プロキシ] > [インフラストラクチャ設定]へ移動します。
   2. 設定アイコンをクリックして、 クライアント**DNS**に移動します。
   3. リージョンを追加し 、一意の名前を付けます。
   4. 地域または場所を選択するか、**[Worldwide (**全世界地域**)]**を選択します。

      全世界地域とシアターの設定が混在する複数のプロキシ設定を指定した場合、*Prisma Access* は、ロケーション グループ、シアター、全世界地域の順に設定を使用します。*Prisma Access* は、リストの上から下に向かってルールを評価します。
   5. DNSサーバーのIPアドレスを追加します。



2. Prisma Accessで 内部ドメインを解決するかどうかを選択します。解決する場合は、1つ以上の 内部ドメイン解決ルールを追加します 。

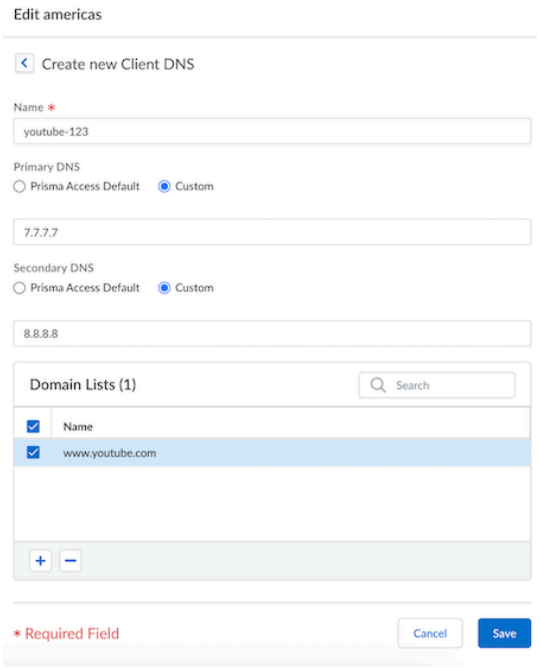


3. 内部ドメイン解決ルールを追加し て定義します。

   現在、 内部ドメイン解決ルールは*Prisma Access Browser*とエージェント プロキシでのみサポートされています。
4. プライマリ **DNS**とセカンダリ**DNS**の下に、ルールの一意の 名前とカスタムIPアドレスを追加します。

©2025 Palo Alto Networks, Inc.

5. デフォルトのPrisma Access DNSサーバーを使用して内部ドメインを解決するには、**[Prisma Access** デフォルト**]** を選択します。内部DNSサーバーに、指定したドメインのみを解決させる場合は、**[Domain List**（ドメインリスト）**]**に解決するドメインを入力します。
6. 内部ドメインにアクセスできる カスタムDNSサーバーがある場合は、 プライマリ**DNS**サーバーとセカンダリ**DNS**サーバーのIPアドレスを指定します。



7. 内部DNSサーバーに、指定したドメインのみを解決させる場合は、**[Domain List**（ドメインリスト）**]**に解決するドメインを入力します。ドメインの前にアスタリスクを指定します(例:*.acme.com)。[保存]をクリックします。
8. 設定の変更を保存してプッシュするには、 **[Push Config (**設定をプッシュ**)]**をクリックします。

©2025 Palo Alto Networks, Inc.

ユーザーと IP アドレスまたはユーザー グループのマッピングを表示する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Panorama Managed Prisma Access	• Prisma Accessライセンス

Prisma Access Insights を使用すると、モバイル ユーザーのユーザーと IP アドレス、またはユーザーとグループのマッピングをリアルタイムで表示できます。リモート ネットワークとサービス接続の場合、ユーザーとユーザー グループのマッピングを表示できます。

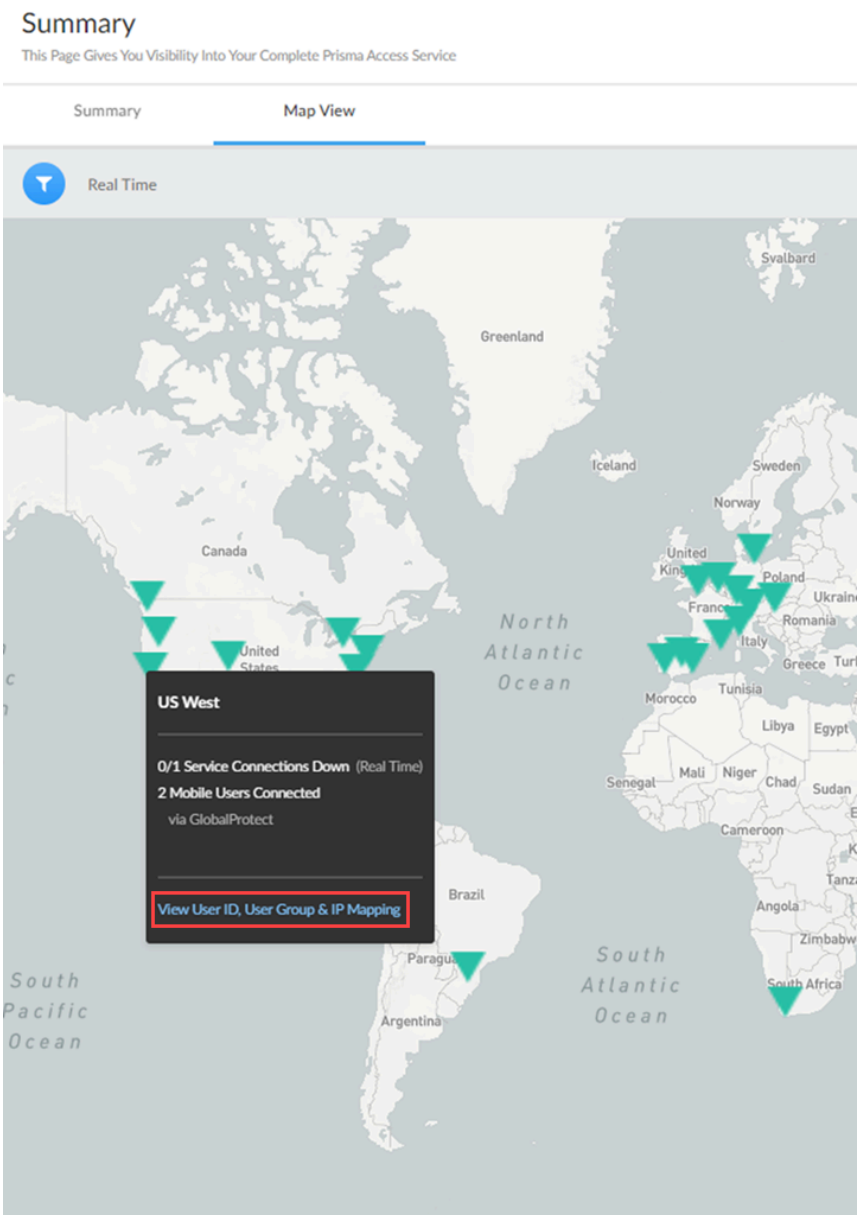
地図上の逆三角形は、Prisma Accessの位置状況を色分けして示したものです：

- 緑:すべてのインスタンスが起動しています。
- 赤:すべてのインスタンスがダウンしています。
- 黄:インスタンスは、アップ、ダウン、不明の組み合わせであり、注意が必要な場合があります。
- 灰:すべてのインスタンスは不明です。

STEP 1 | 概要 ダッシュボードから、 マップ ビューを選択します。

©2025 Palo Alto Networks, Inc.

STEP 2 | ポップアップ ダイアログが表示されるまで、マウス カーソルを場所の上に置きます。



STEP 3 | ダイアログから 「ユーザー **ID**、ユーザー グループ、**IP** マッピングの表示」を 選択します。**UserID and User Group Distribution Check (**ユーザー **ID** とユーザー グループの配信チェック**)** ダイアログが開きます。

STEP 4 | **Prisma AccessLocation (**ロケーション**)** と **Node Type (**ノードタイプ**)** を選択します。**Prisma Access[Location (**ロケーション**)]**は、**[Node Type (**ノードタイプ**)]**が**[Mobile Users**（**GlobalProtect**）**]**の場合は考慮されません。

リモート ネットワークとサービス接続の場合、ユーザー ID とユーザー グループのマッピングのみが表示されます。

1. **Prisma Access** のロケーションを選択します。選択したPrisma Accessロケーションに関連するリモート ネットワークまたはサービス接続がない場合、「No Data Available（データ

©2025 Palo Alto Networks, Inc.

がありません）」というメッセージが**[Remote Networks Site**（リモート ネットワーク サイト）」フィールドまたは「**Service Connections Site**（サービス接続サイト）」フィールドに表示され、**[Show User Groups**（ユー ザーグループを表示）**]**と**[Export to CSV**（**CSV** にエクスポート）**]**ボタンは無効になります。

2. ノード タイプから、リモート ネットワークまたはサービス接続を選択します。
3. [リモート ネットワーク サイト] または [サービス接続サイト] フィールドから、データを取得するサイトを選択します。
4. [View (表示)]で、ユーザー ID がどのユーザー グループに属しているか (ユーザー) を表示するか、サイトに関連付けられている特定のグループに属しているユーザー (グループ) を表示するかを選択します。

   - [ユーザー]を選択した場合は、ユーザーの ユーザー **ID**(たとえば、saas\testuser3) を入力してユーザー ID とユーザー グループのマッピングを取得し、[ユーザー グループの表示]を選択します。ユーザー ID が属するすべてのグループのリストが [ユーザー **ID-IP** マッピング]の下に表示されます。

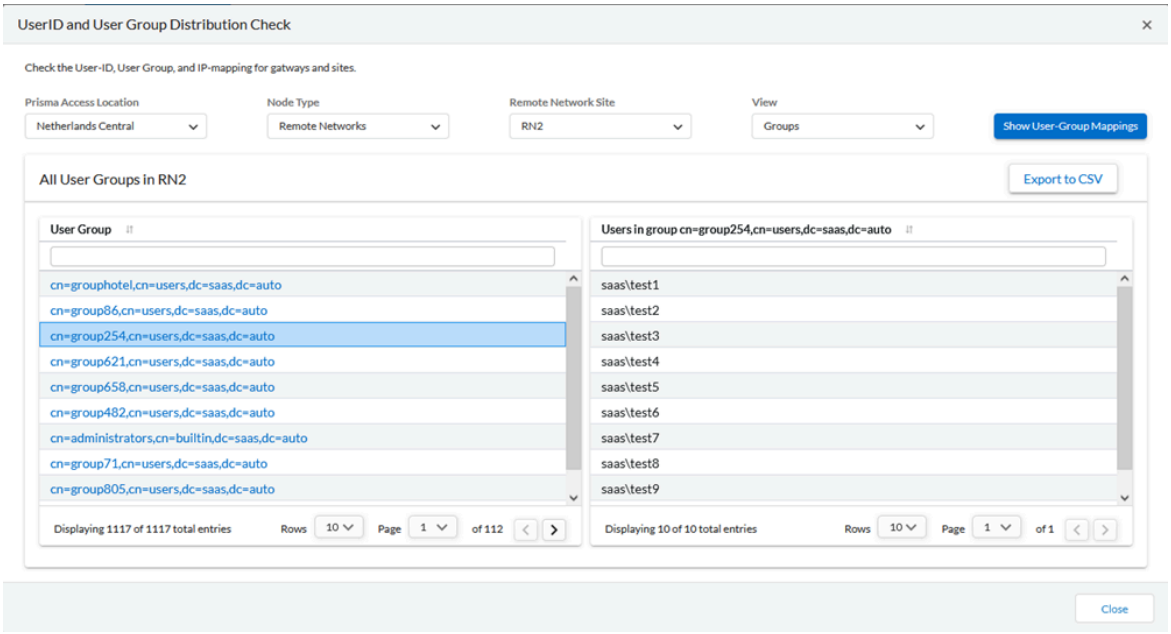
     [ユーザー グループ] テキスト ボックスにグループ名または検索するグループ名に含まれる文字列を入力することで、特定のグループを検索できます。存在しないグループを検索すると、「データがありません」というエラーが表示されます。「ユーザー グループ」の横にある矢印アイコンを切り替えることで、グループのリストを並べ替えることもできます。表示するエントリの数を選択できるほか、進む矢印と戻る矢印をクリックしてページをスクロールすることもできます。

     グループを選択した場合、 ユーザーグループマッピングの表示 を選択すると、サイト内の すべてのユーザーグループの下にある利用可能なすべてのグループが表示されます。 ***<selected_site>***。グループを選択すると、そのグループに属するすべてのユーザーが右側のペインに表示されます。**[CSV** にエクスポート**]** ボタンが有効になり、そのグループに属するすべてのユーザーを CSV ファイルにエクスポートできます。エクスポートされた CSV ファイルには、エクスポート時に UI に表示されない場合でも、グループのすべてのエントリが含まれます。

     [ユーザー グループ] テキスト ボックスにグループ名または検索するグループ名に含まれる文字列を入力することで、特定のグループを検索できます。存在しないグループを検索すると、「データがありません」というエラーが表示されます。「ユーザー グループ」の横にある矢印アイコンを切り替えることで、グループのリストを並べ替える

©2025 Palo Alto Networks, Inc.

こともできます。表示するエントリの数を選択できるほか、進む矢印と戻る矢印を選択してページをスクロールすることもできます。



ノードタイプ:モバイルユーザー **(GlobalProtect)**

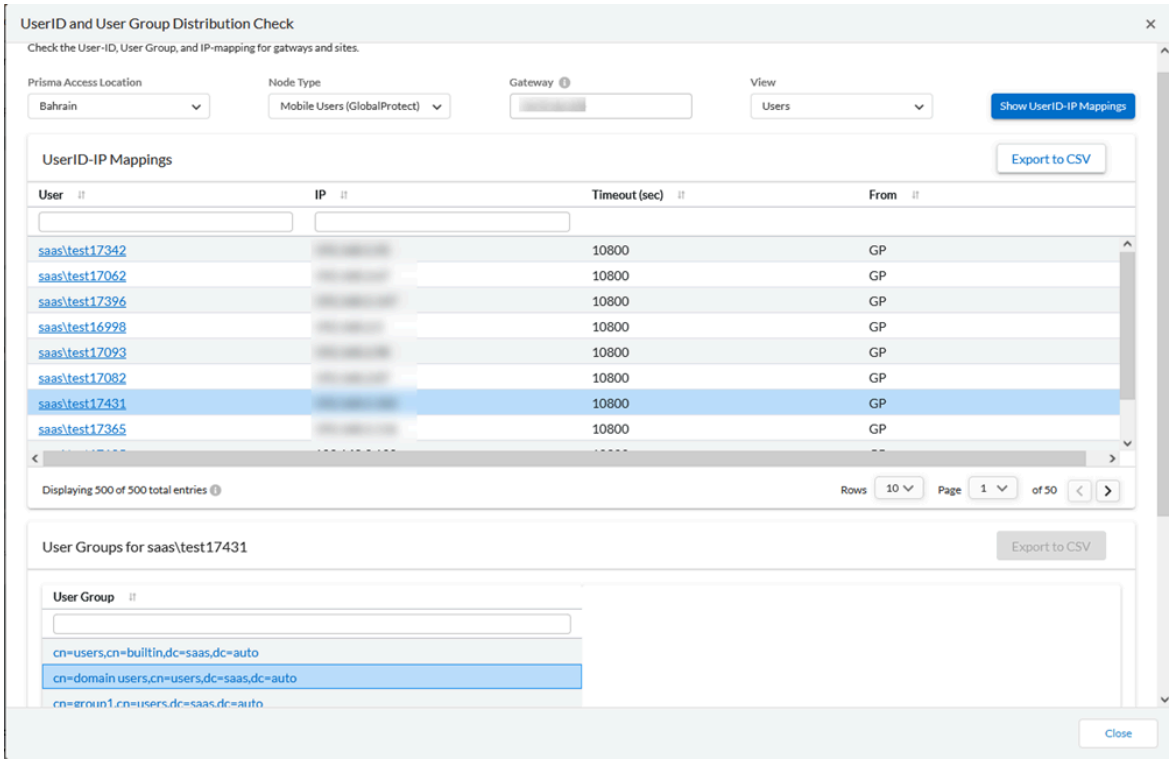
ユーザー ID と IP のマッピング、およびユーザー ID とユーザー グループのマッピングを確認できます。選択したノード タイプがモバイル ユーザー **(GlobalProtect)**の場合、**Prisma Access** ロケーションフィルターは考慮されません。その代わり、 Prisma AccessInsights GlobalProtect ゲートウェイ IP アドレスを使用してデータを検索します。

1. [ゲートウェイ] テキスト ボックスに GlobalProtect IP ゲートウェイ アドレスを入力します。
2. 指定したGlobalProtectゲートウェイに接続されているユーザーのユーザーIDからユーザーIPへのマッピング (ユーザー) のデータを表示する か、ユーザーIDからユーザー グループへのマッピング (グループ) のデータを表示するかを選択します。

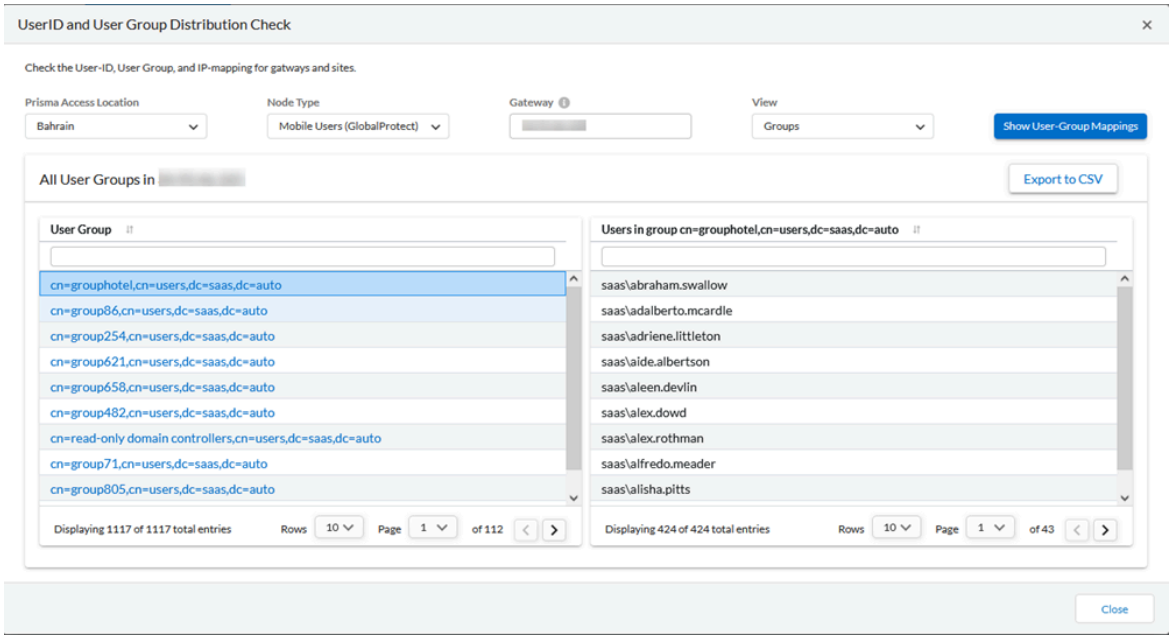
   [ユーザー]を選択した場合は、[ユーザー **ID** と **IP** のマッピングを表示]を選択します。ユーザー ID とユーザー IP のマッピングのテーブルが タイムアウトとともに表示されます。タイムアウトには、ユーザー ID とユーザー IP のエントリの有効期間 (秒単位) が表示されます。特定のユーザーを選択すると、そのユーザーが属するグループが表示されます。グループを選択すると、そのグループに属するすべてのユーザーが表示されます。ま

©2025 Palo Alto Networks, Inc.

た、**[CSV**にエクスポート] ボタンも有効になり、UI に表示されるフィルターされたビューに関係なく、そのグループ内のすべてのユーザーをエクスポートできるようになります。



[グループ] を選択した場合は、[ユーザーとグループのマッピングを表示]を選択します。そのGlobalProtectゲートウェイに属するすべてのユーザー グループのリストが [ユーザー グループ]の下に表示されます。ユーザー グループを選択すると、そのグループに属するすべてのユーザーが右側のペインに表示されます。また、**[CSV**にエクスポート] ボタンも有効になり、UI に表示されるフィルターされたビューに関係なく、そのグループ内のすべてのユーザーをエクスポートできるようになります。



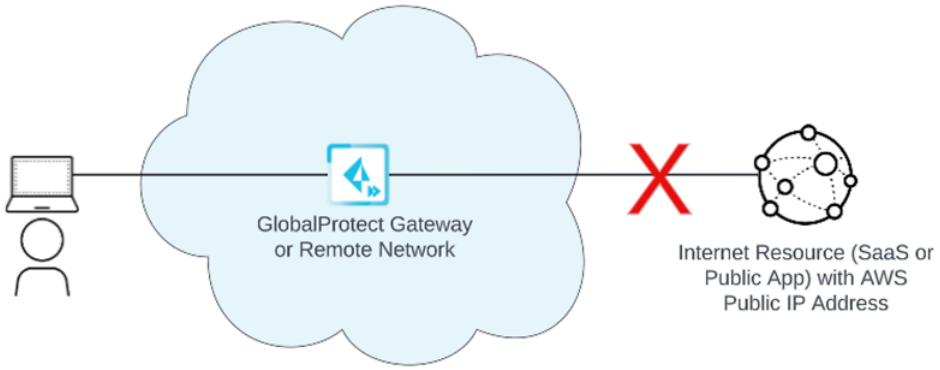
©2025 Palo Alto Networks, Inc.

モバイルユーザーのサイトアクセスの問題を報告する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

stubhub.com、ticketmaster.com、またはdollartree.comなど、一部のWebサイトは、AWSクラウドのIPアドレス範囲からのトラフィックをブロックします。このようなWebサイトにPrisma Accessで保護されているユーザーがアクセスすると、アクセスが拒否されて次のようなメッセージがWebブラウザに表示される可能性があります：

```
Access Denied.サーバーの「http://www.dollartree.com/」にアクセスする権限がありません。Reference #18.7f955b8.1509600370.44eb7c8
```



この問題を報告するには、Webブラウザにhttps://reportasite.gpcloudservice.com/と入力して、アクセスできなかったWebサイトのURLを指定してください。24～48時間経過後にhttps://reportasite.gpcloudservice.com/に戻って、前と同じURLを入力してそのステータスを確認してください。

Palo Alto Networksは、URLで使用されるIPアドレスを提供します。場合によっては、このトラフィックがブラックホール化されないように、このIPアドレスを組織の許可リストに追加する必要があります。リダイレクトされるURLがある場合は、次のIPアドレスを許可リストに追加します。

- 65.154.226.160
- 154.59.126.110
- 66.232.36.110

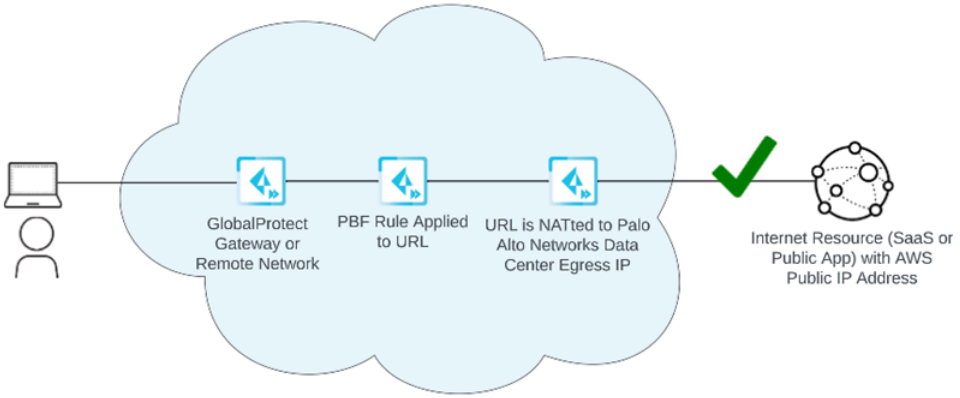
Prisma AccessURL リダイレクト プロセス

©2025 Palo Alto Networks, Inc.

一部のWebサイトでは、クラウドIPアドレス範囲からのトラフィックがブロックされます。Prisma Accessで保護されているユーザーがこれらのウェブサイトにアクセスしようとすると、アクセスを拒否されることがあります。これらのWebサイトへのアクセスが確実に回復されるように、Palo Alto Networksは報告されたすべてのサイトを確認し、アクセスの問題が見つかった場合はサイトを分類し、IPアドレスをアクセス可能なIPアドレスにNATする出力ポリシーを追加します。Palo Alto Networksは、サイトを徹底的にレビューしてその評判を判断し、評判が良好なWebサイトのみを出力ルールに追加すると共にその他のサイトは拒否します。そのプロセスは次のとおりです。

1. アクセスの問題のあるURLをhttps://reportasite.gpcloudservice.com/を使用して通知します。
2. サイト信頼性エンジニアリング (SRE) 自動化によりURLがレビューされます。
3. SREがURLが安全であると判断した場合、Policy-Based Forwarding (ポリシー ベース フォワーディング - PBF)ルールがURLとその親ドメインに適用されます。
4. トラフィックはPrisma Access経由でGlobalProtectゲートウェイまたはリモートネットワークからURL処理ハブにルーティングされ、そこでPBFルールがドメインに適用され、ハブからPalo Alto Networksデータセンターにルーティングされます。
5. トラフィックがデータ センターから出力されると、URLはデータ センターのIPアドレスに送信元NATされます。

これらのアクションの結果、データセンターのIPアドレスの評判が良好であるため、SaaSアプリケーションとの間のトラフィックがドロップされなくなります。



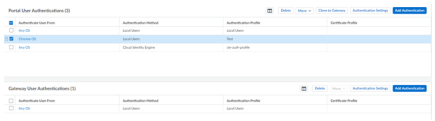
©2025 Palo Alto Networks, Inc.

モバイルユーザーがPrisma Accessに認証できるようにする

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

サポートされている認証タイプのいずれかを使用して、Prisma Accessにモバイルユーザーを認証できます。次の手順に従って、GlobalProtectまたは明示型プロキシのモバイルユーザーの認証を設定します。

STEP 1 | **[Workflows (ワークフロー)]** > **[Prisma Accessセットアップ]**に移動し、モバイルユーザー:グローバルプロテクトまたはExplict Proxyの設定に進み、ユーザー認証を設定します。



STEP 2 | サポートされている認証タイプから認証方法を選択します。

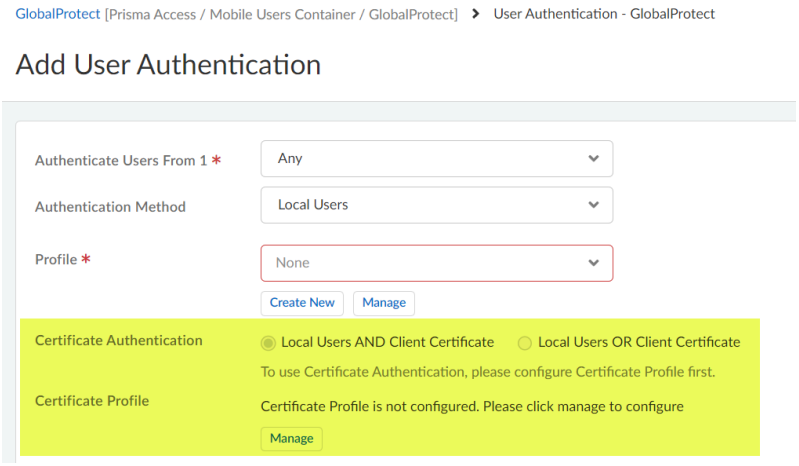
まだPrisma Accessを認証サービスと統合していない場合は、こちらよりその方法を参照してください。

STEP 3 | ユーザー認証に使用するサービスにPrisma Accessを接続できるように構成した認証プロファイルを選択します。

- 手順2でSAMLを使用した場合はSAML認証プロファイルを指定するか、Prisma Accessで使用する新しいSAML認証プロファイルを作成します。
- 手順2でCIEを使用した場合はCIE 認証プロファイルを指定するか、Prisma Accessで使用する新しいCIE認証プロファイルを作成します。
- 手順2でKerberosを使用した場合はKerberos認証プロファイルを指定するか、Prisma Accessで使用する新しいKerberos認証プロファイルを作成します。

©2025 Palo Alto Networks, Inc.

STEP 4 | 証明書認証設定を指定します。



- 証明書の認証

  セキュリティを強化するために、（認証サービスに加えて）証明書を使用して、ユーザー名を取得し、Prisma Accessにユーザを認証します。クライアント証明書に基づいてユーザーを認証するには、Subject Nameフィールドなどの証明書フィールドのいずれかでユーザー名を識別する必要があります。クライアント証明書認証で正常に認証されたモバイルユーザーには、GlobalProtectアプリケーションからサインアウトするオプションはありません。

  Prisma Accessを使用すると、モバイル ユーザーが証明書認証と認証タイプに基づく認証の両方に合格することを要求するか、あるいは、モバイル ユーザーがこれらのチェックの1つだけに合格しさえすれば、モバイル ユーザーにアクセスを許可するかを選択することができます。

- 証明書プロファイル

  オプションの証明書プロファイルを使用して、モバイルユーザーが接続リクエストでPrisma Accessに提示する証明書を確認します。この証明書プロファイルは、ユーザー名およびユーザードメインのフィールドの中身を指定したり、CA 証明書をリストアップしたり、セッションをブロックする基準を指定したりするとともに、CA 証明書の失効状態を判断する方法を提供します。証明書はモバイルユーザーの認証の一部であるため、ユーザーが最初にログインする前に、証明書プロファイルで使用される証明書をユーザーに事前にデプロイする必要があります。証明書プロファイルは、ユーザー名 (Subject または Subject Alt) を含む証明書フィールドを指定します。証明書プロファイルの Username（ユーザー名）フィールドで Subject（サブジェクト）が指定されている場合、エンドポイントから提示される証明書に、そのエンドポイントが接続を行うための共通名が含まれている必要があります。証明書プロファイルでUsername（ユーザー名）フィールドとしてSubject-Alt（サブジェクト代替名）にEmail（電子メール）またはPrincipal Name（プリンシパル名）が指定されている場合、証明書には対応するフィールドが含まれている必要があります。このフィールドは、GlobalProtectアプリケーションがPrisma Accessに対して認証するときにユーザー名として使用されます。

©2025 Palo Alto Networks, Inc.

STEP 5 | ユーザーの認証資格情報を保存する**Cookie** の有効期間を指定します。

IdPがユーザーを認証すると、Prisma Accessはユーザーの認証状態を認証キャッシュ サービス (ACS) に保存します。認証の有効期間は、ここで指定した**Cookie**の有効期間の値に基づきます。

Cookieの有効期間が切れる前にユーザーが大きなファイルをダウンロードできない、またはユーザーが 1 つのWebサイトに長時間アクセスするとクッキーが期限切れになるなどの問題を回避するために、Palo Alto Networks ではCookieの有効期間を少なくとも1日に設定することをお勧めしています。明示的プロキシ ユーザーにCookieの有効期限の問題がある場合は、別のWebサイトを参照してACSに再認証し、ACS Cookieを更新できます。

認証サポートと機能

Prisma Accessが認証を提供するために統合するサービスと、認証のセットアップを計画する際に考慮すべき機能は次のとおりです。

認証サポート：

- Cloud Identity Engine
- SAML
- TACACS+
- RADUIS
- LDAP
- Kerberos
- MFA
- ローカルデータベース認証

認証機能のハイライト：

- SSO
- 認証ポータル
- 認証シーケンス

認証サポート

Cloud Identity Engine	SAML 2.0ベースのIDプロバイダ (IdP)、クライアント証明書と証明局 (CA) チェーン、またはその両方を構成して、ユーザー認証用のCloud Identity Engineをデプロイします。ユーザーの認証方法を指定した後、認証プロファイルを設定して認証セキュリティ ポリシーを定義し、必要に応じてファイアウォールまたはPanoramaで認証ポリシーを構成します。
SAML	ユーザーがネットワーク外のサービスおよびアプリケーションにアクセスする場合、SAML

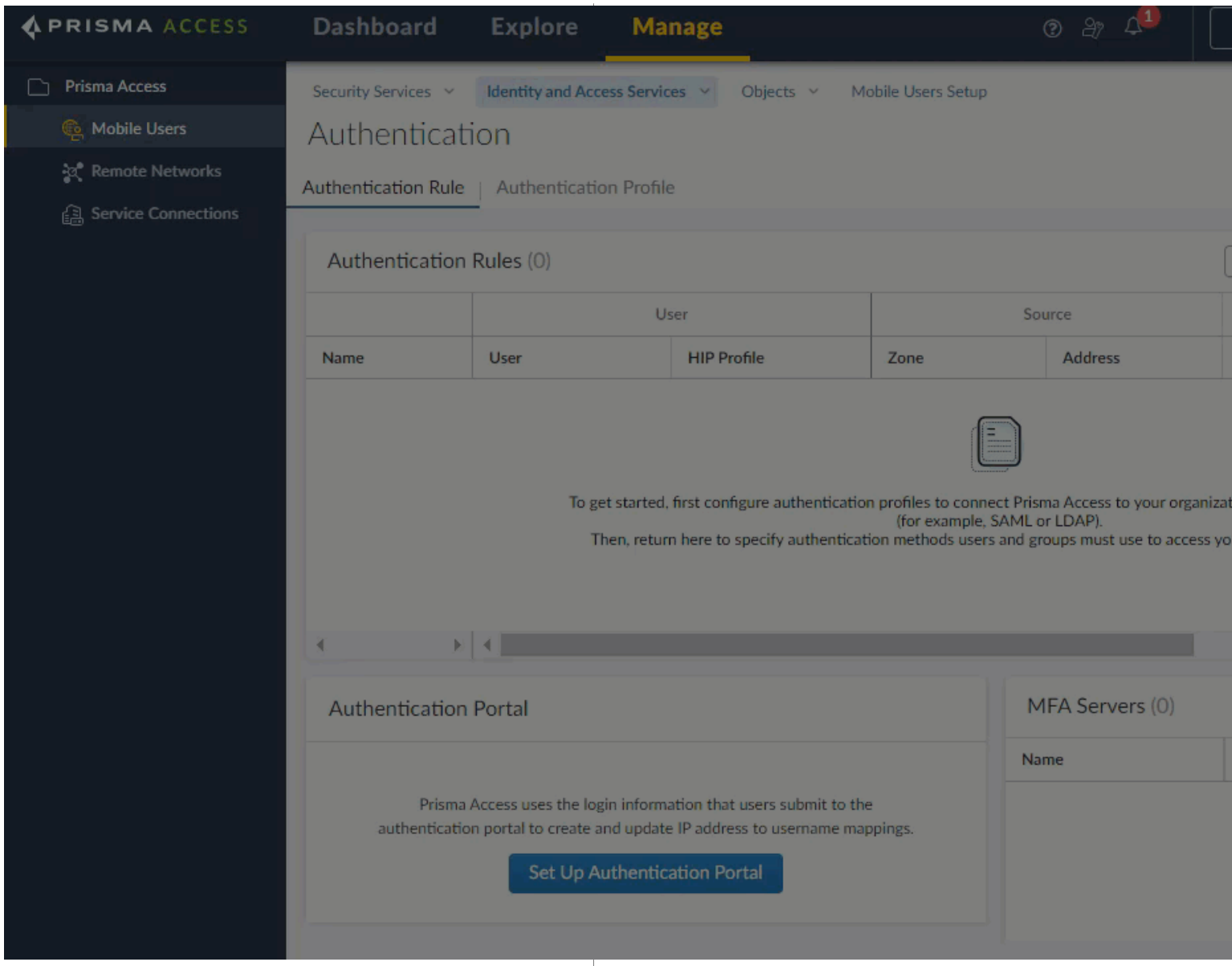
 ©2025 Palo Alto Networks, Inc.

	を使用してPrisma Accessを内外両方のサービスおよびアプリケーションに対するアクセスを制御するアイデンティティ プロバイダ（IdP）と統合できます。SAMLシングル サインオン(SSO)を使用すると、1回のログインで複数のアプリケーションにアクセスできるようになります。これは、各ユーザーが多数のアプリケーションにアクセスし、アプリケーションごとに認証を行うとユーザーの生産性が低下するような環境で役立ちます。この場合、SAML シングル サインオン(SSO)により、1回のログインで複数のアプリケーションにアクセスできるようになります。同様に、SAML シングル ログアウト（SLO）により、ユーザーが一つのセッションからログアウトするだけで複数のアプリケーションのセッションを終了できるようにすることが可能です。SSOは、GlobalProtectアプリを通じてアプリケーションにアクセスするモバイル ユーザー、または認証ポータルを通じてアプリケーションにアクセスするリモート ネットワークのユーザーに対して機能します。SLOはGlobalProtectアプリ ユーザーが利用できます。 認証シーケンスで *SAML* 認証プロファイルを使用することはできません。
TACACS+	Terminal Access Controller Access-Control System Plus（TACACS+）は、中央のサーバーを通して一元的に本人確認および認証を行えるようにするプロトコルの一種です。TACACS+ はユーザー名およびパスワードを暗号化するため、パスワードのみを暗号化する RADIUS よりも安全です。また、UDP を使用する RADIUS と異なり、TACACS+ は TCP を使用するためより安定しています。
RADIUS	Remote Authentication Dial-In User Service（RADIUS）は、広くサポートされているネットワーク プロトコルであり、一元的な本人確認および認証を提供します。Prisma AccessにRADIUSサーバーを追加して、多要素認証を実装することもできます。

©2025 Palo Alto Networks, Inc.

LDAP	Lightweight Directory Access Protocol（LDAP）は、情報ディレクトリにアクセスするための標準的なプロトコルです。LDAPを使用して、認証ポータルを通じてアプリケーションまたはサービスにアクセスするユーザーを認証できます。
Kerberos	Kerberosは、当事者を識別するための固有のキー (チケットと呼ばれる) を使用して当事者間での安全な情報交換を可能にする認証プロトコルです。Kerberosを使用すると、認証ポータルを通じてアプリケーションにアクセスするユーザーを認証できます。Kerberos SSO が有効な場合、ユーザーはネットワークに初めてアクセスした際だけログインを求められます（Microsoft Windows へのログインなど）。この最初のログイン後、ユーザーはSSOセッションの有効期限が切れるまで再度ログインすることなく、ネットワーク内の任意のブラウザベースのサービスにアクセスできます。 Kerberosを使用するには、まずユーザーを認証するPrisma AccessのKerberosアカウントが必要です。Kerberos キータブを作成するためにアカウントが必要です。キータブとは、ファイアウォールあるいはPanoramaのプリンシパル名およびハッシュされたパスワードを含むファイルです。SSO プロセスにはキータブが必要です。 Kerberos SSO は、Kerberos 環境の内部にあるサービスおよびアプリケーションに対してのみ利用できます。外部のサービスおよびアプリケーションに対して SSO を有効化する場合、SAMLを使用します。
MFA	多要素認証(MFA)を使用すると、異なるタイプ(要素と呼ばれる) の複数の認証チャレンジを実装して、最も機密性の高いサービスとアプリケーションを保護できます。例えば、重要な財務文書に対しては、検索エンジンよりも強力な認証が必要になるかもしれません。 Prisma Accessには、サポートされているMFAベンダーのリストが組み込まれており、新しいベンダーが追加されると自動的に更新されます。

©2025 Palo Alto Networks, Inc.



ローカルデータベース認証	Prisma Access上でローカルに実行され、ユーザー アカウント (ユーザー名とパスワード、またはハッシュ化されたパスワード) およびユーザーグループが含まれるデータベースを作成します。このタイプの認証は、プレーンテキストのパスワードを知らず、パスワードのハッシュだけを知っているケースで、既存のUNIX アカウントの認証情報を再利用するユーザーアカウントを作成する際に便利です。プレーンテキストのパスワードを使用するアカウントの場合、パスワードの複雑さおよび有効期限を設定することもできます。この認証方法は、認証ポータルまたはGlobalProtectア

©2025 Palo Alto Networks, Inc.

	プリを通じてサービスやアプリケーションにアクセスするユーザーが利用できます。

認証機能のハイライト

SSO	SAMLまたはKerberos を使用している場合は、シングル サインオン(SSO)を実装できます。これにより、ユーザーは1回認証するだけで複数のサービスやアプリケーションにアクセスできるようになります。SAML および Kerberos が SSO をサポートしています。
認証ポータル	認証ルールに一致するWeb要求をPrisma Accessログイン ページにリダイレクトし、認証を求めます。 Prisma Accessは、ユーザーがこの認証ポータルに送信する情報を使用して、IPアドレスとユーザー名のマッピングを作成または更新します。 これはリモート ネットワークの場合に特に役立ち、ユーザー(またはグループ)に基づいてトラフィックを継続的に監視および適用できます。ユーザーが認証ルールに一致する Web トラフィック (HTTP または HTTPS) を開始すると、Prisma Accessはユーザーに認証ポータルを通じて認証するように要求します。 Prisma Accessは、ユーザーがポータルに送信する情報に基づいて、IPアドレスとユーザー名のマッピングを作成または更新します。これにより、リモート ネットワーク サイトで誰が最も機密性の高いアプリケーションやデータにアクセスしているかを正確に把握できるようになります。
認証シーケンス	複数の種類の認証を異なる目的で使用する場合、認証シーケンスを設定してプロファイルを順位付けすることができます。Prisma Accessは、1つのプロファイルがユーザーの認証に成功するまで、ランキングに基づいて各プロファイルをチェックします。

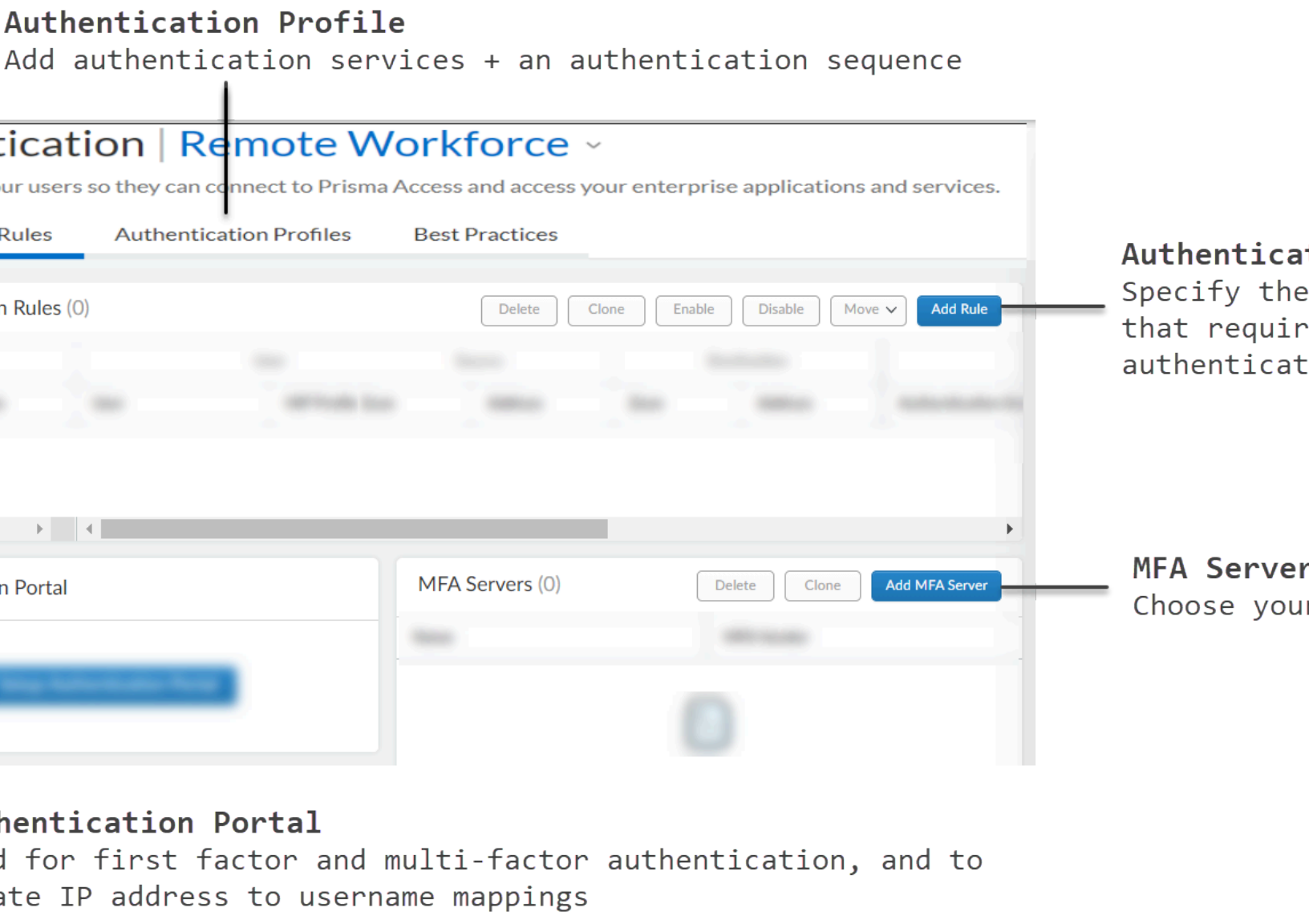
認証のセットアップ

Prisma AccessをPrisma Accessに認証を設定するには、まずPrisma Accessに認証サービスを追加します。次に、認証を要求するトラフィックを指定します。これらの設定に基づいて、MFAや

©2025 Palo Alto Networks, Inc.

認証シーケンスなどの認証機能を追加したり、Prisma AccessでIPアドレス - ユーザー名間マッピングを作成および更新したりできます。

Prisma Accessによる認証を有効にするために必要な設定がすべて一箇所にまとめられています。**[Manage (管理)]** > **[Configuration (設定)]** > **[NGFWとPrisma Access]** > **[Identity Services (IDサービス)]** > **[Authentication]**に進んでください。**Prisma Access**設定スコープを選択します。



認証ルールここでは認証を要求するトラフィックを指定します

認証ルールの設定には、ルールへの認証プロファイルの追加も含まれます。Prisma Accessは、認証ルールに一致するトラフィックを検出すると、認証プロファイルで定義され

©2025 Palo Alto Networks, Inc.

た認証方式と設定を一致するトラフィックに適用します。プロファイルは、ユーザーが認証を受けるために必要な方法を定義するものです。

1. **[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access] > [Identity Services (IDサービス)] > [Authentication (認証)] > [Authentication Rule (認証ルール)]** および**[Add Authentication Rule (認証ルールを追加)]**に移動します。**Prisma Access** の 構成範囲を選択します。
2. 認証を必要とするユーザー、サービス、URLカテゴリを定義します。
3. ルールのアクションを ［**Authenticate (認証)**］ に設定し、このルールに一致するトラフィックに使用する認証方式を定義するプロファイルを選択します。



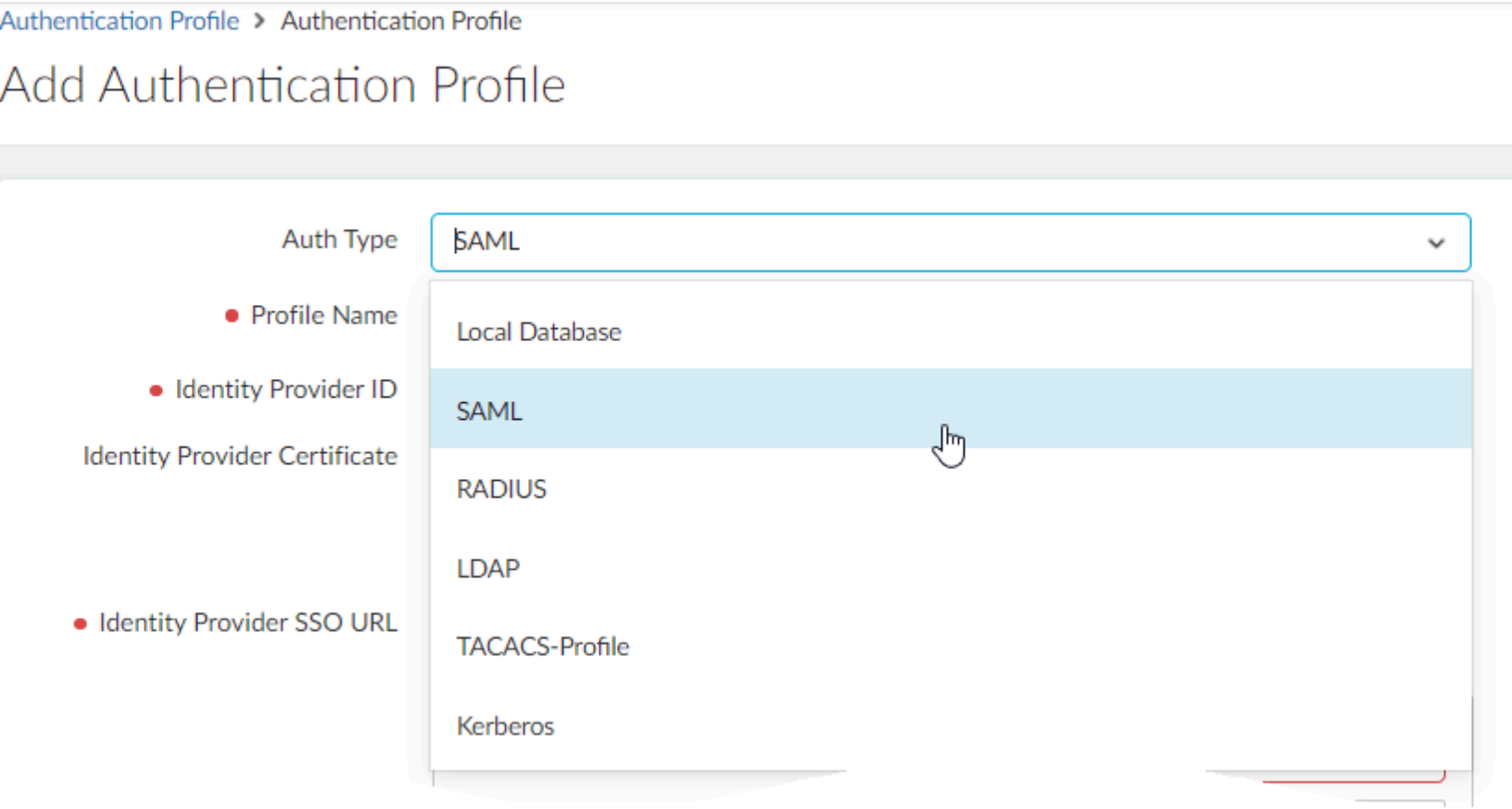
 ©2025 Palo Alto Networks, Inc.

認証プロファイルここに認証サービスを追加し、認証設定を定義します

ユーザーの認証に使用するサービス（SAML、TACACS+、RADIUS、LDAP、Kerberos）にPrisma Accessを接続し、認証設定を定義します（たとえば、ログイン試行の失敗に対する制限を設定します）。

オンプレミス認証サービスを使用している場合は、まずオンプレミス認証サービスを*Prisma Access*に接続するサービス接続を作成する必要があります。次に、ここに戻って認証プロファイルを設定します。

[Manage (管理)] > **[Configuration (設定)]** > **[NGFWとPrisma Access]** > **[Identity Services (IDサービス)]** > **[Authentication (認証)]** > **[Authentication Profile (認証プロファイル)]** > **[Add Profile (プロファイルの追加)]**に移動し、**[Auth Type (認証タイプ)]**プロファイルの設定から始めます。**Prisma Access**設定スコープを選択します。

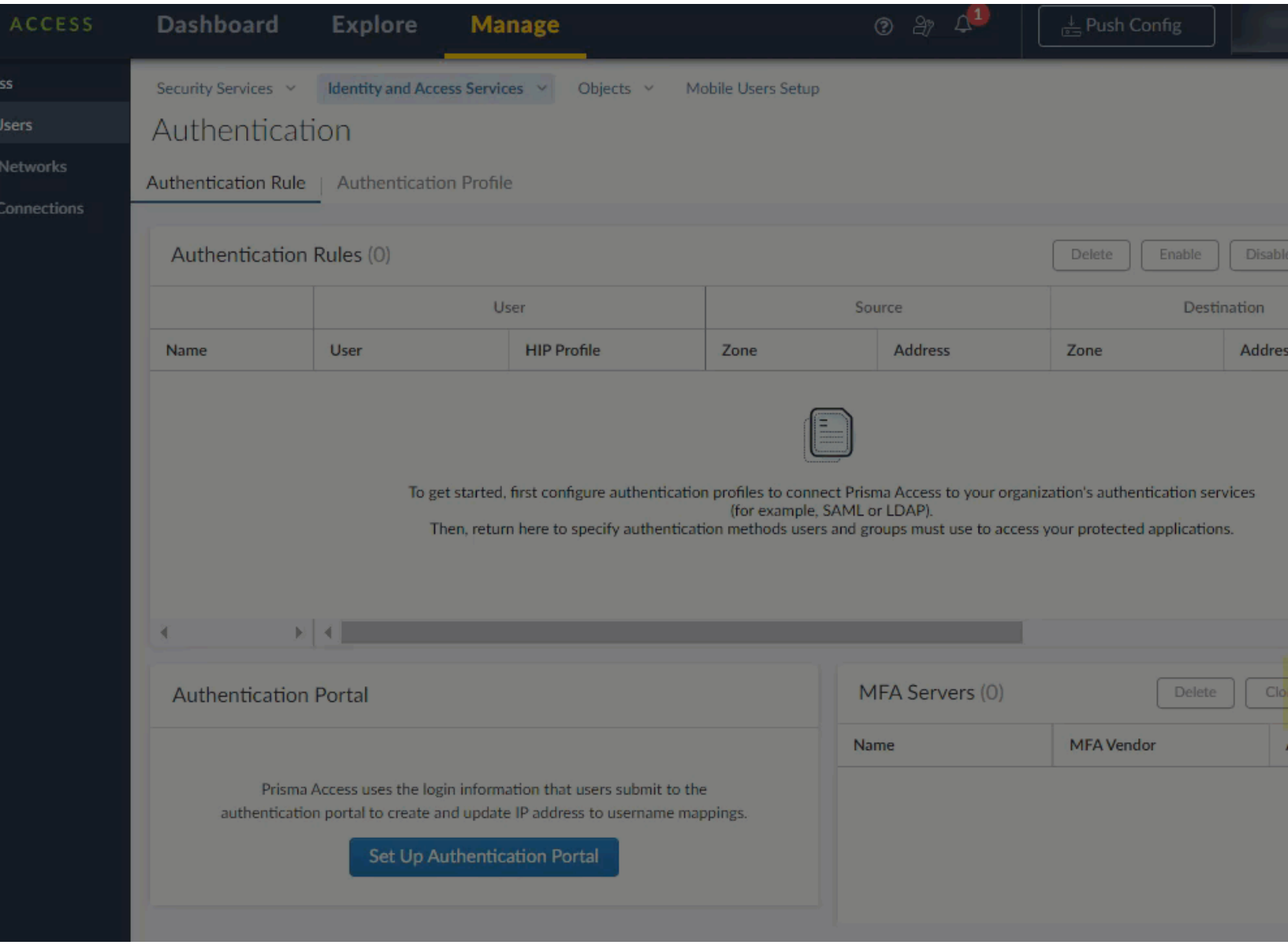


Prisma Accessサービスに接続できるようにする、選択した認証サービスの詳細を追加し、ユーザー資格情報とロール権限を読み取るように求められます。認証をカスタマイズするための追加設定はプロファイルで提供され、設定している認証の種類によって異なる場合があります。

©2025 Palo Alto Networks, Inc.

MFAサーバー使用しているMFAベンダーを指定

機密性の高いアプリケーションに対するユーザー認証に複数の方法を使用するには、使用するMFAベンダーを追加することから始めます(**MFA**サーバーの追加)。 Prisma AccessがMFA業者のリストを提供するので、そこから選ぶことができます。



認証ポータルリモートネットワークサイトのユーザー用の認証ポータル(旧称キャプティブポータル)を設定し、Prisma AccessでIPアドレスとユーザー名のマッピングを作成できるようにする

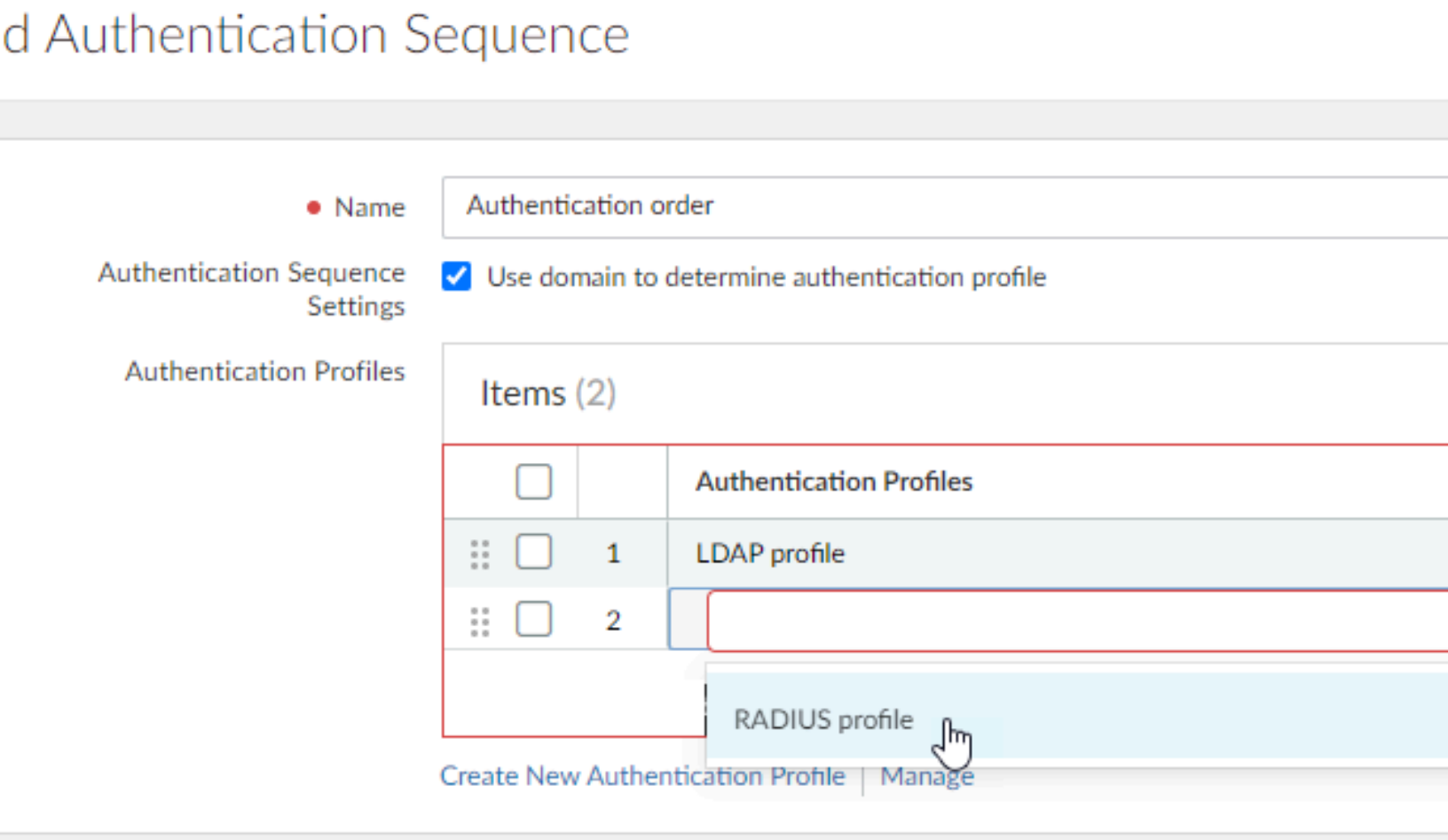
第1要素認証(ログインとパスワード)の場合、リモートネットワークサイトのユーザーは認証ポータルを通じて認証を受ける必要があります。認証が成功した場合、 Prisma Accessは必要な追加の認証要素ごとに MFA ログインページを表示します。 Prisma Accessはユーザーが送信した資格情報を使用して、IPアドレス - ユーザー名間マッピングを作成および更新しま

©2025 Palo Alto Networks, Inc.

す。つまり、リモートネットワークサイトの誰がウェブコンテンツやエンタープライズアプリケーションにアクセスしているかを常に把握できます。

認証シーケンスPrisma Accessで試したい順に認証プロファイルをランク付けする

[Manage (管理)] > **[Configuration (設定)]** > **[NGFWとPrisma Access]** > **[Identity Services (IDサービス)]** > **[Authentication (認証)]** > **[Authentication Profile (認証プロファイル)]** および > **[Add Authentication Sequence (認証シーケンスを追加)]**を選択します。**Prisma Access**設定スコープを選択します。Prisma Accessは、1 つがユーザの認証に成功するまで、それぞれを順番にチェックします。



 ©2025 Palo Alto Networks, Inc.

モバイルユーザーが企業リソースにアクセスできるようにする

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Panorama Managed Prisma Access	• Prisma Accessライセンス

Prisma AccessはデフォルトのIPアドレスプールとクラウド デフォルトのDNSサーバーを提供するので、ユーザーがPrisma Accessを有効にしてインターネット アクセスのみを可能にするうえで、ネットワーク サービスをセットアップする必要はありません。

ただし、モバイル ユーザーが本社、データセンター、またはPrisma Accessにオンボードしたリモート ネットワーク サイトにある社内リソースにアクセスできるようにするには、次の操作を行う必要があります。

- Prisma Access es は、モバイル・ユーザーにIPアドレスを割り当てるために使用するIPアドレス・プールを定義します
- Prisma Accessサービスインフラストラクチャをセットアップします。
- また、本社やデータセンターへのアクセスを可能にするために、オンボード サービス接続も提供します。

モバイル ユーザーがリモート ネットワーク サイトに接続できるようにするには、データ センターまたは HQ の場所へのアクセスを提供するために接続を使用する予定がない場合でも、少なくとも 1 つのサービス接続を構成する必要があります。すべてのブランチは完全にメッシュ化されていますが、モバイル ユーザーの接続はメッシュ化されていません。サービス接続を作成すると、モバイル ユーザー トラフィックをブランチ ネットワークにルーティングするために必要なハブ アンド スポーク アーキテクチャが確立されます。この場合、サービス接続を次のように最小限構成できます。

- サービス接続をオンボードで行う場合は、モバイルユーザーに近いPrisma Accessロケーションを使用します。
- サービス接続用のプライマリIPSecトンネルを設定するときは、プレースホルダー値を使用してIPSecピア認証とトンネル設定を構成します。
- サービス接続のルーティングとQoSを有効にする場合は、プレースホルダーIPサブネットを追加します。

  なぜなら Prisma Accessではこのトンネルを介してトラフィックをルーティングすることはないからです。使用するIPサブネットが、Prisma Accessに接続されている他の設定済みサブネットと衝突したり重複したりしないことを確認してください。

STEP 1 | **[Manage (管理)] > [Mobile Users (モバイルユーザー)] > [Mobile Users Setup (モバイルユーザーセットアップ)]**に移動し、[インフラストラクチャ設]定を編集して、モバイル ユーザーのネットワーク設定を調整します。

©2025 Palo Alto Networks, Inc.

STEP 2 | Prisma Accessがモバイル・ユーザに IP アドレスを割り当てるために使用するクライアントIPプールを確認または調整します。

- デフォルトでは、**Worldwide (**全世界領域)IPプールはすべてのモバイル ユーザーが利用できます。
- 地域ごとにカスタマイズして 、地域またはロケーション専用のIPプールを設定できます。IPプールを指定しない地域または場所については、Prisma Accessはワールドワイドプールを使用します。

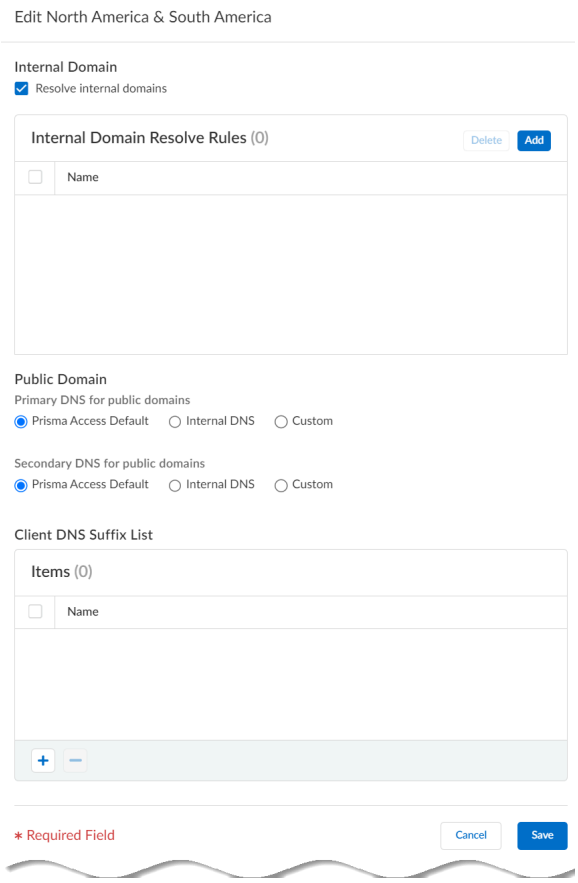
定義するIPアドレス プールは、次の要件を満たしている必要があります。

- ベストプラクティスとして、IPアドレスの競合を防ぐためにRFC 1918準拠のIPアドレス プールを定義します。
- 定義するIPアドレス プールが、内部で使用する他のIPアドレスと重複していないことを確認してください。
- 定義するIPアドレス プールが、Prisma Accessに使用しているインフラストラクチャIPアドレス プールと重複していないことを確認してください。
- Prisma AccessはこれらのIPアドレスとサブネットを内部使用のために予約しているため、169.254.0.0/16および100.64.0.0/10サブネット範囲と重複するサブネットは指定しないでください。
- 次のガイドラインに基づいて、組織内のすべてのモバイル ユーザーに十分なカバレッジを提供するIPアドレス プールを指定してください。
- 1つまたは2つのリージョンに展開されたワールドワイド アドレス プールを使用する予定の場合、最低限必要なIPアドレス プールは /23 (512 IP アドレス) です。
- 3つ以上のリージョンに展開されたワールドワイド アドレス プールを使用する予定の場合、必要な最小IPアドレス プールは /19 (8,192 個の IP アドレス) であり、単一のIPアドレス プール内または複数のプールに分散されます。
- リージョンごとにIPアドレス プールを定義する場合、どのリージョンでも最小プール サイズは /23 (512 IPアドレス) です。
- Prisma Accessをデプロイする予定のない地域では、IPアドレスプールを割り当てる必要はありません。例えば、米国東部（バージニア州北部）、米国東部（オハイオ州）、米国西部（カリフォルニア州北部）の各リージョンを選択し、Prisma Accessをオンボードでユーザーに提供する場合、南北アメリカ地域のみのIPアドレス プールを指定する必要があります。ただし、他の地域のユーザーはPrisma Accessに接続できないことに留意してください。
- 全世界領域プールと地域プールを組み合わせて定義する予定の場合は、地域ごとに少なくとも 512 個の IP アドレスを割り当てるようにしてください。たとえば、3つのリージョンのデプロイメントの場合、ヨーロッパ リージョンで1,024個のアドレスを指定し、全世界リージョンで 512 個のアドレスを指定できます。
- ベストプラクティスとして、組織内の各モバイル ユーザーが同時にログインできるように、少なくとも1つのIPアドレスが割り当てられるようにIPアドレス プールを指定します。ライセンスされたユーザー数よりも少ないIPアドレスを持つIPアドレスプールを指定した場合、 Prisma Accessには警告メッセージが表示されます。ただし、IPアドレス プールが限られており、すべてのユーザーが同時にログインすることが予想されない場合は、メッセージをバイパスして、より小さいプール サイズを使用できます。

 ©2025 Palo Alto Networks, Inc.

STEP 3 | クライアント**DNS** 設定を追加します。 **Worldwide (**全世界領域**)**をデフォルトを使用することも、地域に基づいて設定をカスタマイズすることもできます。

DNS設定をカスタマイズする地域を選択します。



内部ドメインの解決にこれらの**DNS**設定を使用するオプションをチェックし、任意でパブリックドメインの解決にも内部**DNS**サーバーを使用します。このオプションを選択しないと、Prisma Accessはクラウドのデフォルト DNSサーバーを使用してパブリック ドメインの要求を解決します。

*Prisma Access*の*DNS*プロキシは、指定した*DNS*サーバーに要求を送信します。*DNS*要求の送信元アドレスは、リージョンに割り当てた*IP*プールの最初の*IP*アドレスです。*DNS*要求がサーバーに確実に到達できるようにするには、モバイル ユーザー*IP*アドレス プール内のすべてのアドレスから*DNS*サーバーへのトラフィックを許可する必要があります。

STEP 4 | モバイルユーザーが、本社やデータセンター ネットワーク、または他の支社のリソース にアクセスできるようにするには、Prisma Accessインフラストラクチャ設定を構成して、ネッ トワーク バックボーンを有効にする必要があります。

[Manage (管理**)] > [Prisma Access] > [Prisma Access** セットアップ**]**へと進みます。

©2025 Palo Alto Networks, Inc.

STEP 5 | モバイル ユーザーが本社やデータセンターのリソースにアクセスできるようにするには、これらのサイトをPrisma Accessに接続するサービス接続を作成します。

[Manage (管理)] > [Service Connections (サービス接続)] > [Service Connections Setup (サービス接続セットアップ)]に移動します。

STEP 6 | 準備ができたら、Prisma Accessに**Push Config (設定をプッシュ)**して、モバイル ユーザー設定を保存します。

©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

Prisma Accessリモートネットワーク

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

ビジネスが成長し、オフィスのロケーションを世界各地に設置していく中で、リモートネットワークのオンボーディングを素早く行い、最適な組み合わせのセキュリティをユーザーに提供することができます。各リモートロケーションでの、デバイスの設定と管理における複雑性を排除する、役に立つオプションが用意されています。本サービスは、新しいリモートネットワークロケーションを追加し、運用上の課題を最低限に抑える効率的な手段を提供し、各ロケーションのユーザーを常に接続、保護します。また、Panoramaからポリシーを集中管理して、リモートネットワークロケーションのセキュリティの一貫性と整合性を保ちます。

リモートネットワークロケーションからPrisma Accessに接続するために、Palo Alto Networksの次世代ファイアウォール、またはサービスへのIPSecトンネルを確立できるSD-WANなどの、IPSec対応デバイスを使用できます。

Prisma SD-WANでは、IPSecトンネル接続に加えて、 リモート ネットワークとしてオンボードしたCloudBladeを使用して、Prisma SD-WANコントローラーとIONデバイスをPrisma Accessと統合できます。

リモート ネットワークの計画チェックリスト

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

リモート ネットワークのオンボードを開始する前に 、次の構成項目を準備して、リモート ネットワークの場所のユーザーに対してサービスを正常に有効にし、ポリシーを適用できるようにしてください。

- 企業リソースへのアクセスが必要ですか?

  リモート ネットワークが、本社やデータセンターのインフラやリソースにアクセ スする必要がある場合は、企業サイトへのPrisma Access サービス接続を作成します。リモート ネットワークの場所が自律的であり、他の場所のインフラストラクチャにアクセスする必要がない場合は、これを行う必要はありません。

- **Prisma Access**ロケーション

  支店のユーザーがPrisma Accessに接続するとき、選択したPrisma Accessロケーションによって、インターネットからのコンテンツが提供される言語が決定されます。最高のユーザー エクスペリエンスを実現するには、ブランチ オフィスと同じ郡内の地域と場所を選択して、ユーザーに最高のエクスペリエンスを提供できるようにします。支店と同じ国に場所がない場合は、サイトのユーザーの大多数と同じ言語を使用する場所を選択します。

  ローカルゾーンとしてマークされている場所はほとんどありません。これらのロケーションは、人口や産業の中心地に近いPrisma Accessコンピュート ロケーションを提供します。

- **IP** サブネット

  Prisma Accessがトラフィックをリモート ネットワークにルーティングするためには、Prisma Accessを使用してセキュリ ティを確保したいサブネットワークのルーティング情報を提供する必要があります。これには複数の方法があります。リモート ネットワーク ロケーションで各サブネットワークへのスタティック ルートを定義するか、サービス接続ロケーションとPrisma Accessの間でBGPを設定するか、または両方の方法を組み合わせて使用します。スタティックルートを設定し、BGPも有効にした場合、スタティックルートが優先されます。リモートネットワークロケーションのサブネットワーク数がさほど多くない場合、スタティック ルートの使用が便利なことが多いですが、重複するサブネットを持つリモートネットワークが存在する大規模なデプロイ環境では、BGPを使用するとスケーリングが容易になります。

- 集約帯域幅モデル- リモート ネットワーク ロケーションの帯域幅は、コンピューティング ロケーションごとに集約レベルで割り当てられます。オンボードする各ロケーションには、帯域幅が割り当てられる対応するコンピューティング ロケーションがあります。場所ごとでは

©2025 Palo Alto Networks, Inc.

なく、コンピューティング場所ごとに帯域幅を割り当てます。この方法は 集約帯域幅モデルとして知られています。

集約帯域幅モデルは、すべての新しいデプロイメントで利用できます。場所ごとに帯域幅を割り当てる既存のデプロイメントがある場合は、場所ごとの帯域幅の割り当てからコンピューティング場所ごとの帯域幅の割り当てに移行できます。



集約帯域幅モデルに移行する前に、新しいモデルへの移行を計画するを確認する必要があります。

オンボードするすべての場所で、そのコンピューティング場所に割り当てられた帯域幅を共有します。たとえば、シンガポール、タイ、ベトナムの拠点にあるリモート ネットワークを使用して4つのブランチ オフィスをオンボードする必要があるとします。これらすべての場所は、アジア南東部のコンピューティング ロケーションにマップされます。アジア南東部のコンピューティング拠点に200Mbpsの帯域幅を割り当てると、Prisma Accessは200 Mbpsの帯域幅を、その場所にオンボードした4つのブランチ オフィス間で分割します。香港の場所も追加する場合は、香港が香港のコンピューティング ロケーションにマップされ、そのコンピューティング ロケーションに帯域幅を追加する必要があることに注意してください。コンピューティング ロケーションごとに50 Mbpsの最小帯域幅を指定します。

Prisma Accessはロケーションごとの負荷または需要に基づいて帯域幅を動的に割り当てます。4つのサイトが合計で最大200Mbpsを使用している先ほどの例では、1つまたは複数のサイトが他のサイトほど帯域幅を使用していない場合、Prisma Accessでは需要の多いロケーションにより多くの帯域幅を提供し、割り当てられた帯域幅をより効率的に使用できます。さらに、いずれかのサイトがダウンした場合、 Prisma Accessはそのコンピューティング ロケーションでまだ稼働している他のサイト間で帯域幅を再割り当てします。

ローカル ゾーン としてマークされた場所は、リモート ネットワークに対して最大500 Mbpsの帯域幅をサポートします。1 Gbpsの帯域幅をサポートするには、Palo Alto Networksサポートにお問い合わせください。これらのロケーションは、人口や産業の中心地に近いPrisma Accessコンピュート ロケーションを提供するが、いくつかの制限もあります。ローカル ゾーンを追加するには、Palo Alto Networksの担当者にお問い合わせください。

- URLにアクセスする際に問題がある場合は、Palo Alto NetworksサポートにWebサイトの問題を報告してください。
- サイズ設定のガイドラインと帯域幅割り当ての考慮事項

  サイトで必要な帯域幅の量を計算するときは、帯域幅の使用量にリモート ネットワーク接続の出力トラフィックと入力トラフィックの両方が含まれること (つまり、割り当てられた帯域幅は入力と出力の合計) と、オンボードするすべての場所でそのコンピューティング場所に割り当てられた帯域幅を共有することを考慮してください。特定のサイトが必要とする帯域幅の量を判断するために、各ロケーションでお使いのISPから利用できる帯域幅を検討してください。
- 重複するサブネット

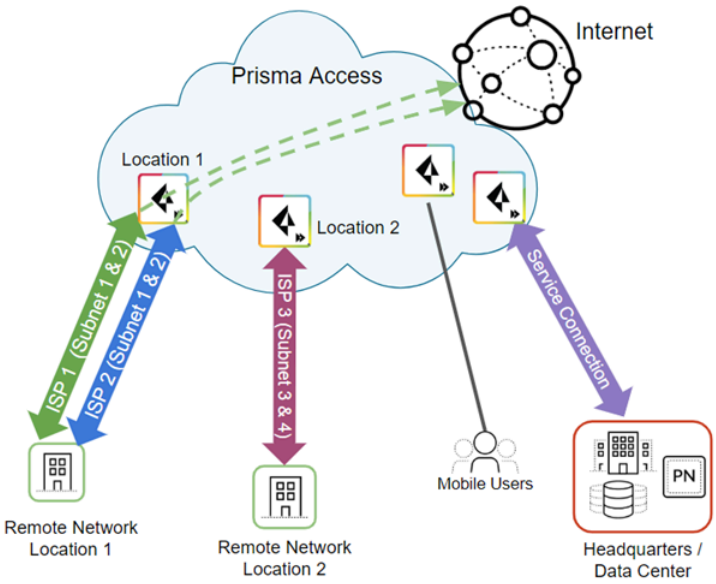
  通常、Prisma Accessインスタンス内で重複するサブネットを持つことはできません。すべてのリモートネットワークロケーション、サービス接続、およびモバイルユーザー向けのPrisma AccessのIPアドレスプールの、サブネットをオーバーラップさせることはできません。ただし、既存のサブネットと重複するサブネットを使用する会社を買収した場合など、状況によってはサブネットの重複を避けることができません。場合によっては、意図的にサ

 ©2025 Palo Alto Networks, Inc.

ブネットが重複する2つのリージョンを構成する必要があります。たとえば、異なるポリシールールを持つ小売店の場所に別のゲスト ネットワークを作成する場合などです。

Prisma Access 重複するサブネットを持つリモート ネットワークの場所をオンボードできますが、重複するサブネットを持つブランチからはインターネットへのトラフィック フローのみがサポートされます。同じテナント内に重複したサブネットを持たないブランチは、Prisma Accessから完全な機能を利用できます。詳細は、次の図の表を参照してください。

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



ただし、サブネットが重複するサイトには次の制限があることに注意してください。

- リモート ネットワークからリモート ネットワークへのインバウンド トラフィックはありません。複数のリモート ネットワークの場所が同じサブネットにルーティングされるため、他のリモート ネットワークの場所ではトラフィックがどこにルーティングされるかわかりません。しかし、どのリモート ネットワーク ロケーションのユーザーとサービスも、サイトに重複するサブネットがなければ、他のリモート ネットワーク・ロケーションのリソースにアクセスすることができ、どのサイトもPrisma Accessインフラを通じてインターネットにアクセスすることができます。
- サービス接続からのトラフィックは、トラフィックをルーティングするリモート ネットワークの場所がわからないため、サブネットが重複しているリモート ネットワークの場所にあるリソースにアクセスできません。ただし、サブネットが重複するリモート ネットワークの場所は、サービス接続からリソースにアクセスできます。

©2025 Palo Alto Networks, Inc.

- モバイル ユーザーは、インバウンド ルーティングの制限により、サブネットが重複しているリモート ネットワークの場所にあるリソースにアクセスできません。

> *Strata Cloud Manager*を使用して*Prisma Access*を管理している場合、***[Workflows (ワークフロー)]*** > ***[Prisma Access Setup (Prisma Access* のセットアップ*)]*** > ***[Remote Networks (*リモート ネットワーク*)]*** > ***[Advanced Settings (*詳細設定*)]***へ移動します。重複サブネットを有効にするには、 ***Overlapped Subnets (*重複サブネット*)*** 設定を編集します。*Panorama*を使用して*Prisma Access*を管理している場合、***[Panorama]*** > ***[Cloud Services (*クラウドサービス*)]*** > ***[Configuration (*構成*)]*** > ***[Remote Networks (*リモート ネットワーク*)]*** に移動して、 ***[Overlapped Subnets (*重複サブネット*)]***を確認します。

- **IPSec** 終端ノード- オンボーディング中にリモート ネットワークに*IPSec*終端ノードを割り当てます。IPSec 終端ノードごとに最大500個のリモート ネットワーク サイト (Prisma Access 5.0以降の場合) または400個のリモート ネットワーク サイト (Prisma Accessリリース5.0より前の場合) を指定できます。許可されるリモート ネットワークの最大数をサポートするには、IPSec終端ノードに対応するコンピューティング ロケーションに500 Mbps以上を割り当てます。

  コンピューティング ロケーションには最大200個のIPSec終端ノードを設定できます。各IPSec終端ノードは最大1,000 Mbpsの帯域幅を提供できます。コンピューティング拠点に1,000Mbps以上の帯域幅を割り当てると、 Prisma Accessは追加のIPSec終端ノードを提供します。

  - **IPSec** 終端ノードと**3.2**より前のリリースからのアップグレード- 3.2より前では、コンピューティング ロケーションの割り当てられた帯域幅500 Mbpsごとに1つの IPSec 終端ノードが割り当てられていました。3.2より前のリモート ネットワーク展開があり、3.2.1以降のリリースにアップグレードし、リモート ネットワークの場所に対応するコンピューティング場所に500 Mbpsを超える帯域幅が割り当てられている場合、IPSec 終端ノードに関連付けられているすべてのリモート ネットワークは最大1,000 Mbpsの帯域幅をサポートできます。3.2以降にアップグレードした後、 Prisma Accessは割り当てられた帯域幅 1,000 Mbps ごとに1つのIPSec終端ノードをデプロイします。既存のリモートネットワークの場合、 Prisma Accessはリモート ネットワークの帯域幅消費量に追加の容量が必要になったときにトリガーされる自動スケーリング メカニズムを使用して、リモート ネットワークの帯域幅を増やすことができます。詳細については、Prisma Access（Panorama Managed）リリースノートの「デフォルト動作の変更」を参照してください。

    3.2へのアップグレード後も、現在の IPSec 終端ノードとリモート ネットワークのマッピングは変更されず、IPSec終端ノードの数も同じままです。IPSec終端ノードは、既存のコンピューティング場所の帯域幅を増減する場合、またはリモート ネットワークの新しいコンピューティング場所をオンボードする場合にのみ追加または削除されます。

- サービス接続–ユーザーを認証する、または重要なネットワークアセットへのアクセスを有効にするなどの目的で、リモートネットワークロケーションが企業本社内のインフラにアクセスする必要がある場合、本社とリモートネットワークロケーションを接続するために、サービス接続を作成する必要があります。リモートネットワークロケーションが自律型で、他のロケーションにあるインフラにアクセスする必要がない場合、サービス接続を設定する必要はありません（モバイルユーザーがアクセスを必要とする場合を除く）。

©2025 Palo Alto Networks, Inc.

- テンプレート–テンプレートスタック（Remote_Network_Template_Stack）、およびPrisma Access for networks用のトップレベルのテンプレート（Remote_Network_Template）はPrisma Accessによって自動的に作成されます。リモート ネットワークの搭載を設定するには、最初からトップレベルのテンプレートを設定するか、またはPalo Alto networksファイアウォールをすでにオンプレミスで実行している場合、既存の設定を活用します。テンプレートには、IPSecトンネルを確立するための設定、およびリモートネットワークロケーションとPrisma Accessfor networks間のプロトコルネゴシエーション用のIKE（Internet Key Exchange）設定、セキュリティ ポリシーを参照できるゾーン、およびリモートネットワーク用のPrisma AccessからStrata Logging Serviceにログを転送するための、ログ転送プロファイルが必要になります。
- **IPSec** トンネル構成-IPSec トンネル、 トンネル監視、および IPSec暗号プロファイル 構成を含む既存のテンプレートがある場合は、そのテンプレートをRemote_Network_Template_Stackに追加して、IPSecトンネルの作成プロセスを簡素化できます。または、自動的に作成されるRemote_Network_Templateを編集し、企業サイトに戻るIPSec トンネルを作成するために必要なIPSec構成を作成することもできます。 また、Prisma Accessより一般的に使用されるネットワーク デバイス用の定義済みIPSecテンプレートのセットと、定義済みテンプレートに含まれていないデバイス用の汎用テンプレートも提供されます。リモート ネットワーク トンネルを構成するときは、必ずIPSecトンネルの推奨事項に従ってください。
- ルーティング方法（静的または動的）を決定する– Prisma Accessがリモート ネットワークにトラフィックをルーティングするには、Prisma Accessを使用してセキュアにしたいサブネットワークのルーティング情報を提供する必要があります。これには複数の方法があります。リモート ネットワーク ロケーションで各サブネットワークへのスタティック ルートを定義するか、サービス接続ロケーションとPrisma Accessの間でBGPを設定するか、または両方の方法を組み合わせて使用します。スタティックルートを設定し、BGPも有効にした場合、スタティックルートが優先されます。リモートネットワークロケーションのサブネットワーク数がさほど多くない場合、スタティック ルートの使用が便利なことが多いですが、重複するサブネットを持つ多数のリモートネットワークが存在する大規模なデプロイ環境では、BGPを使用するとスケーリングが容易になります。
- 親デバイス グループ– ネットワーク用のPrisma Accessでは、セキュリティ ポリシー、セキュリティプロファイル、および他のポリシーオブジェクト（アプリケーショングループとオブジェクト、およびアドレスグループなど）、および認証ポリシーを含める親デバイス グループを指定する必要があります。これにより、Prisma Access for networksへのIPSecトンネル経由でルーティングされるトラフィックに、一貫したポリシーを適用することができます。リモートネットワークロケーションのユーザーを保護するために、Panoramaでポリシールールとオブジェクトを定義するか、または既存のデバイスグループを使用する必要があります。

  ゾーンを参照する既存のデバイス グループを使用する場合、ゾーンを定義した対応するテンプレートを*Remote_Network_Template_Stack*に忘れずに追加してください。これにより、リモートネットワークをオンボードし設定する際に、ゾーンマッピングを完了させることができます。

©2025 Palo Alto Networks, Inc.

リモートネットワーク帯域幅の割り当て

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

リモート ネットワークは、ブランチなどのリモート ネットワークの場所と、そのブランチ内のユーザーを保護するために使用されます。

リモート ネットワークは従量制です。つまり、コンピューティングロケーションには特定の量の帯域幅が割り当てられ、この割り当てられた帯域幅に関連するコストが発生します。

リモート ネットワークをPrisma Accessに接続する準備をする際には、オンボードするサイトの数と、それぞれの帯域幅要件を把握しておく必要があります。

リモート ネットワーク帯域幅を割り当てる方法を学習します。

- Strata Cloud Manager
- Panorama

リモートネットワーク帯域幅の割り当て（Strata Cloud Manager）

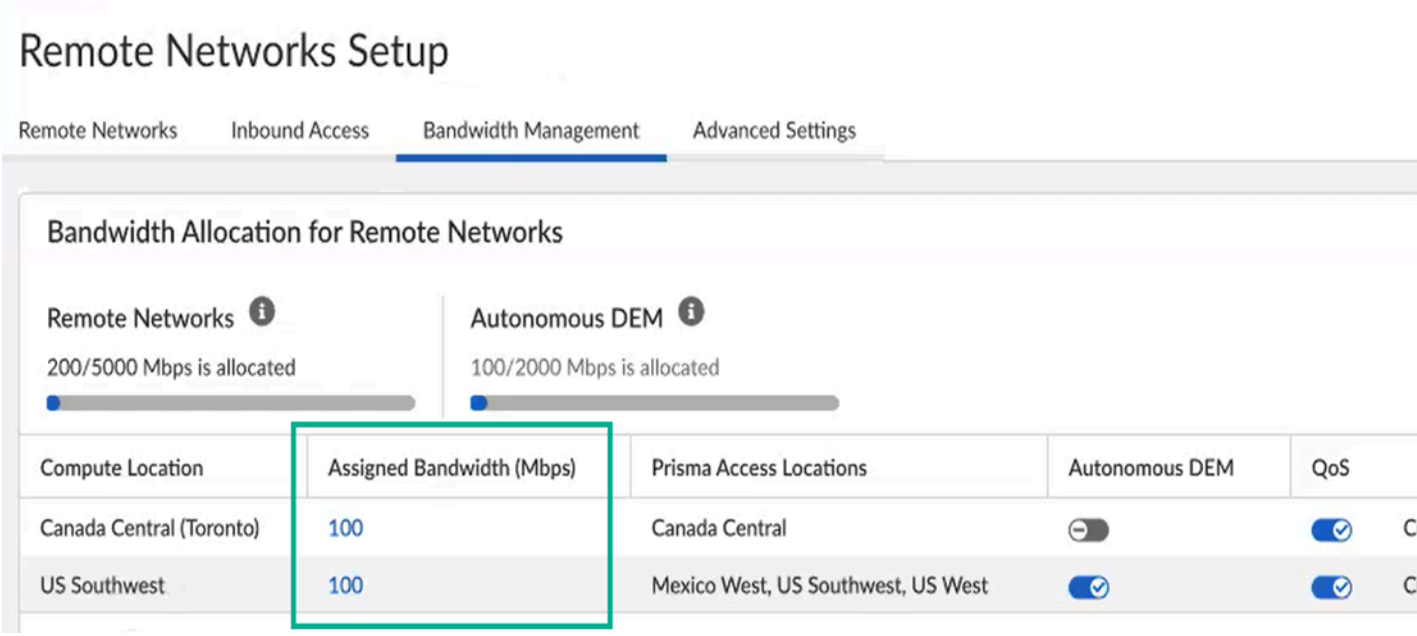
少なくとも2つ（多くの場合はそれ以上）Prisma Access地理的に近いロケーションをグループ化して、 ロケーションを計算します。これは、個々の帯域幅を割り当てるのではなく、帯域幅を割り当てるレベルです。 Prisma Access ロケーションまたは特定のリモート ネットワーク サイト向けです。これは、Prisma Accessや需要に基づいて、コンピュート ロケーションのサイトに動的に帯域幅を割り当てることができることを意味します。

たとえば、シンガポール、タイ、ベトナムの拠点にあるリモート ネットワークを使用して4つのブランチ オフィスをオンボードする必要があるとします。これらすべての場所は、アジア南東部のコンピューティング ロケーションにマップされます。アジア南東部のコンピューティング拠点に200Mbpsの帯域幅を割り当てると、Prisma Accessは200 Mbpsの帯域幅を、その場所にオンボードした4つのブランチ オフィス間で分割します。香港の場所も追加する場合は、香港が香港のコンピューティング ロケーションにマップされ、そのコンピューティング ロケーションに帯域幅を追加する必要があることに注意してください。コンピューティング ロケーションごとに50 Mbpsの最小帯域幅を指定します。

Prisma Accessはロケーションごとの負荷または需要に基づいて帯域幅を動的に割り当てます。4つのサイトが合計で最大200Mbpsを使用している先ほどの例では、1つまたは複数のサイトが他のサイトほど帯域幅を使用していない場合、Prisma Accessでは需要の多いロケーションにより多くの帯域幅を提供し、割り当てられた帯域幅をより効率的に使用できます。さらに、いずれかのサイトがダウンした場合、 Prisma Accessはそのコンピューティング ロケーションでまだ稼働している他のサイト間で帯域幅を再割り当てします。

©2025 Palo Alto Networks, Inc.

開始するには、 [ワークフロー] > **Prisma Access** [セットアップ] > [リモート ネットワーク] > [帯域幅管理]に移動します。



場所に基づいて帯域幅を割り当てる場合は、各サイトに必要な帯域幅を考慮する必要があります。

特定のサイトが必要とする帯域幅の量を判断するために、各ロケーションでお使いのISPから利用できる帯域幅を検討してください。サイトで必要な帯域幅の量を計算するときは、帯域幅の使用量にリモート ネットワーク接続の出口トラフィックと入口トラフィックの両方が含まれることを考慮してください。

複数の場所にわたって帯域幅を割り当てる場合、リモート ネットワーク サイトへの安全な受信アクセスとリモート ネットワークのクオリティ オブ サービス *(QoS)*はサポートされません。

リモートネットワーク帯域幅の割り当て（Panorama）

コンピュート ロケーションごとに帯域幅を割り当てるPrisma Accessリモートネットワーク デプロイメントを構成す るには、以下の手順を実行します。

多数のリモートネットワーク（最大*1,000*）をオンボードする必要がある場合は、次の手順でリモートネットワークをオンボードし、 リモートネットワーク構成をCSVファイルにエクスポートし、オンボードする他のリモートネットワークをCSVファイルに追加し、CSVファイルをインポートして*Prisma Access*に構成を保存します。

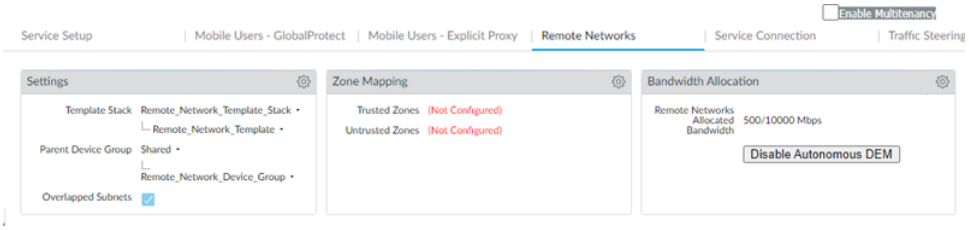
STEP 1 | **[Panorama] > [Cloud Services**（クラウドサービス）**] > [Configuration**（設定）**] > [Remote Networks**（リモートネットワーク）**]**を選択します。

©2025 Palo Alto Networks, Inc.

STEP 2 | 帯域幅割り当て領域の歯車アイコンをクリックして、オンボードする場所に帯域幅を割り当てます。

コンピュート ロケーションごとに集約レベルで帯域幅を割り当てます。詳細は Prisma Accessリモートネットワーク を参照してください。

アドオン ライセンスとして 自律型DEM を削除した場合、またはライセンスからリモート ネットワーク用の自律型*DEM*を削除した場合は、*[*自律型***DEM***を無効にする*]*を選択します。リモート ネットワークの自律型*DEM*を削除し、自律型*DEM*を無効にしないと、コミット時にエラーが発生します。



現在、場所ごとにリモート ネットワークをオンボードしている既存のリモート ネットワーク デプロイメントがある場合は、 集約帯域幅モデルに移行するかどうかを尋ねるポップアップ ウィンドウが表示されます。移行を続行するには [移行] をクリックし、移行をキャンセルするには [キャンセル] をクリックします。

集約帯域幅モデルへの移行は永続的であり、元に戻すことはできません。移行する前に、 移行前チェックリストを確認してください。変更を有効にするには、変更を コミットしてプッシュする 必要があります。

デプロイメントをアグリゲート帯域幅モデルに移行しても、サービス**IP**アドレス (リモート ネットワーク接続のためにPrisma AccessIPSecトンネル側で使用されるまたはパブリック**IP**アドレス）は変更されず、IPSec トンネルの再設定は必要ありません。

STEP 3 | オンボーディングしたい**Prisma Access**ロケーションに関連する、各コンピュートロケーションに必要な帯域幅割り当てを入力します。

入力した帯域幅の量を確認するには、帯域幅の量の横にあるチェックマークを選択します。量をキャンセルするには、**x**を選択します。

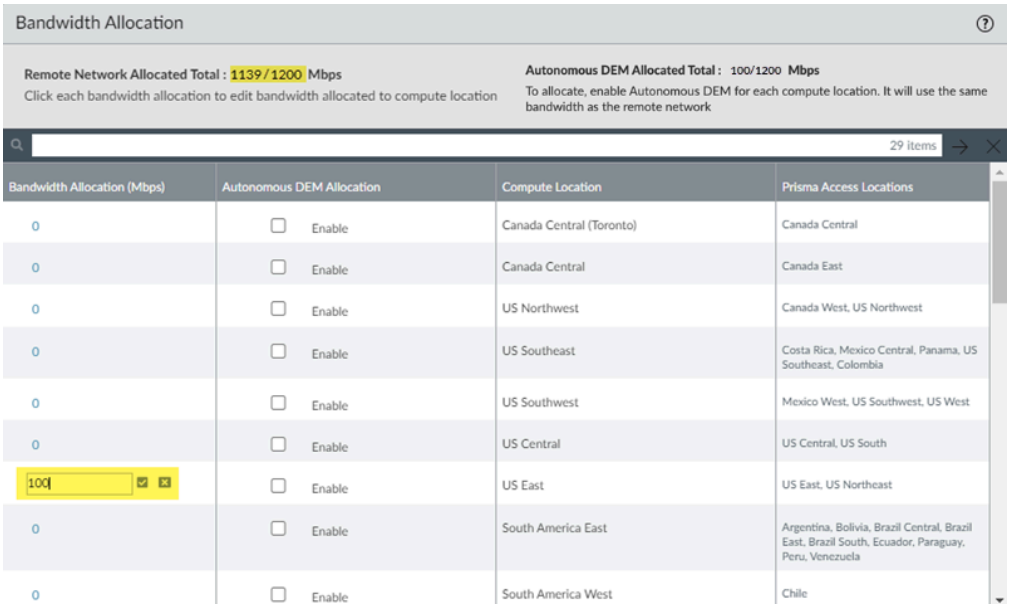
最小帯域幅50 Mbpsと、最大残りのライセンス帯域幅の最大帯域幅を指定します。

STEP 4 | (任意：リモート ネットワーク ライセンスの自律型DEMを使用したデプロイメントのみ) 帯域幅を割り当てたコンピューティングロケーションに対して 自律型**DEM**割り当てを有効にします 。

コンピューティング ロケーションに対して 自律型DEM を有効にすると、自律型DEM ライセンスによって使用される帯域幅の量は、コンピューティング ロケーションに対して指定した帯域幅と同じになります。自律型**DEM** 割り当て合計には、自律型DEMによって使用されている帯域幅と残りの帯域幅が表示されます。詳細については、自律型DEM ガイドを参照してください。

©2025 Palo Alto Networks, Inc.

STEP 5 | ページ上部の [割り当てられた合計]フィールドに帯域幅が反映されるまで待ってから、**[OK]**をクリックします。



STEP 6 | (任意)リモート ネットワークの場所への安全な着信アクセスを提供するようにリモートネットワークを構成する場合は、**[着信アクセス リモート ネットワーク]** タブをクリックし、ワークフローに従って リモート ネットワークの安全な着信アクセスを構成します。

STEP 7 | リモート ネットワークを追加し、名前を指定します。

入力後にリモートネットワークロケーション名を変更することはできません。オンボーディングを開始する前に、リモートネットワークの名前の設定体系を忘れずに確認してください。

STEP 8 | （任意：BGPデプロイ環境のみ）リモートネットワークがそのトラフィックに対して4つまでのIPSecトンネルを使用できるように、設定を作成します（**ECMP**ロードバランシング）。

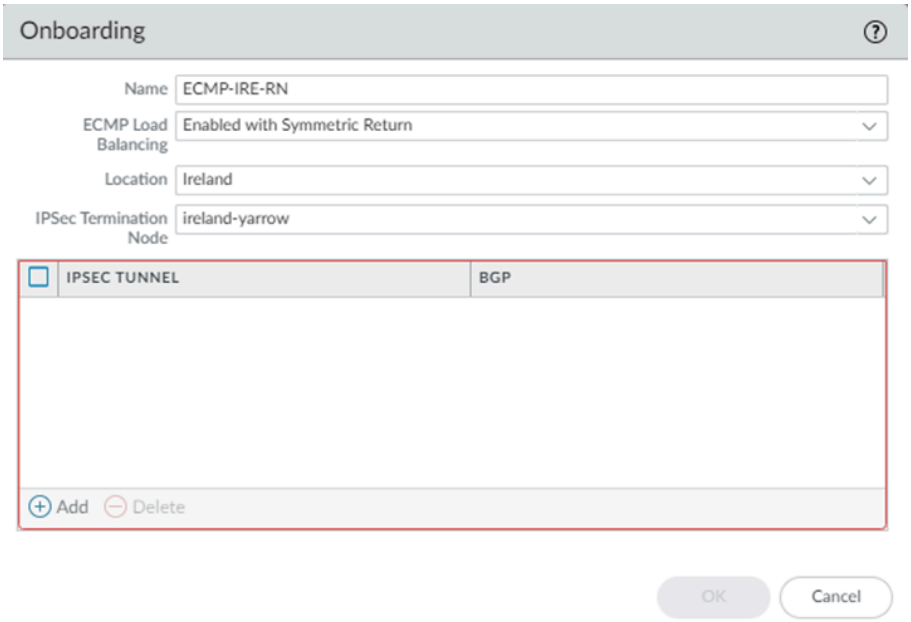
スタティック ルートはサポートされていません (BGPが必要です)。また、QoSが設定されている場合は、ECMPリンクの 割り当て比率を変更することはできません。デプロイ環境でリモートネットワーク接続用にIPSecトンネルを1つ使用している、またはスタティックルートを使用している場合は、**ECMP**ロードバランシングで**None**（なし）を選択して、11ステップに進んでください。

1. ECMPロードバランシングを有効または無効にする選択肢のいずれかを選択します。
   - **None**（なし）–ECMPロードバランシングを使用しません（このリモートネットワーク接続に対して、単一のリモートネットワークトンネルを使用します）。スタティックルートを使用する場合、このオプションしか選択できません。ECMPロードバランシングには、BGPが必要です。
   - **Enabled with Symmetric Return**（対称リターンとともに有効にする）–このリモートネットワーク接続に最大4つのIPSecトンネルを指定し、Prisma Accessがトラ

©2025 Palo Alto Networks, Inc.

フィックの送信に使用したのと同じリンクをリターントラフィックに使用するように強制します。

プライマリトンネルのいずれかがダウンした場合にのみ、1つまたは複数のトンネルをバックアップトンネルとして使用する場合に、このオプションを選択します。リンクに障害が発生した場合、Prisma Accessは他のいずれかのトンネルを使ってトラフィックを対称的に送受信します。



2. **Add**（追加）を選択して、リモートネットワーク接続用のIPSecトンネルを追加して、次の値を指定します。。

   - **Enable**（有効）—IPSecトンネルのBGPを有効にします。

     この選択項目は設定不可能です。ECMPを設定するには、BGPを有効にする必要があります。

   - **Summarize Mobile User Routes before advertising**（アドバタイジングを行う前に、モバイルユーザーのルートを要約）—BGPを介した、顧客構内設備（CPE）への、モバイルユーザーIPサブネットのアドバタイジング数を、それを要約することで減らします。

     デフォルトでPrisma Accessは、モバイルユーザーのIPアドレスプールを、/24サブネットのブロックでアドバタイズします。それを要約すると、Prisma Accessによって指定したサブネットに基づいてプールがアドバタイズされます。たとえば、Prisma Accessは、パブリックユーザーのモバイルIPプールを、アドバタイズ前に10.8.1.0/24、10.8.2.0/24、10.8.3.0/24などのサブネットに分割するのではなく、/20のサブネットを使用して10.8.0.0/20のプールをアドバタイズします。これらのアドバタイズを要約することで、CPEルーティングテーブルに保存されるルート数を削減できる可能性があります。たとえば、限定された数のルートを受け付け

©2025 Palo Alto Networks, Inc.

るクラウドVPNゲートウェイ（仮想プライベートゲートウェイ（VGW）またはトランジットゲートウェイ（TGW））で、IPプールの要約を使用することができます。

*ECMP*を使用するロケーションに対してルート要約を有効にする場合、そのロケーションへのすべてのリンクのルート要約を有効にする必要があります。そうしないと、コミット時にエラーが発生します。

Prisma Accessは、集約されたモバイルユーザールートに対してコミュニティ文字列を`0xFFFE:0xFFF0`に設定します。

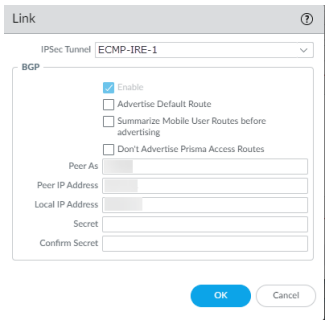
- デフォルトルートをアドバタイズする—Prisma AccessはeBGPを使用してリモートネットワークのデフォルト ルート広告を開始します。

  ネットワークに、*BGP*がアドバタイズしている他のデフォルトルートが存在していないことを確認してください。そうしないと、ネットワークにルーティング上の問題が発生する可能性があります。

- **Prisma Access**ルートをアドバタイズしない—Prisma AccessBGPピアが、組織のネットワークにルートを転送することを防止します。

  デフォルトで、Prisma Accessは、ローカルルート、および他のサービス接続、リモートネットワーク、およびモバイルユーザーサブネットから受信するすべてのプレフィックスを含め、すべてのBGPルーティング情報をアドバタイズします。Prisma AccessによるBGPアドバタイズメントの送信を防止しながら、受信したBGP情報を使って、他のBGPネイバーからルートを学習するには、このチェックボックスを選択します。

  このオプションを選択するとBGPアドバタイズメントは送信されないため、Prisma Accessへのルートを確立するために、オンプレミス機器でスタティックルートを設定する必要があります。



- **Peer AS**—リモートネットワークのファイアウォール、仮想ルーター、またはBGPルーターが所属している自律型システム（AS）を指定します。
- **Peer IP Address**（ピア**IP**アドレス）—この接続を設定しているリモートネットワーク上の、eBGPルーターのルーターID として割り当てるIPアドレスを入力します。
- **Local IP Address**（ローカル**IP**アドレス）（任意）—Prisma AccessがBGPのローカルIPアドレスとして使用するアドレスを入力します。トンネルのPrisma Access側で使用するIPアドレスを指定してください。

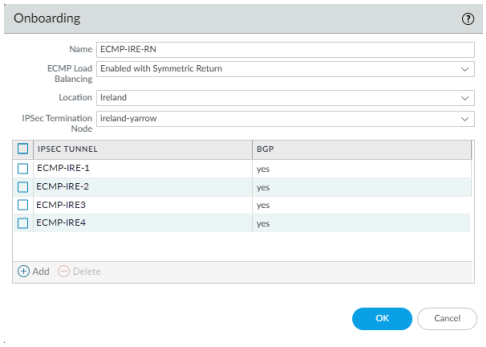
  Local Addressの指定は、接続のもう一方の側にあるデバイス（Amazon Web Service（AWS） Virtual Private Gatewayなど）が、BGPピアリングを正常に行うために、

©2025 Palo Alto Networks, Inc.

特定のローカルIPアドレスを必要としている場合などに役立ちます。指定するIPアドレスは、インフラサブネットまたはリモートネットワーク内のサブネットのIPアドレスと、競合またはオーバーラップしていないことを確認してください。

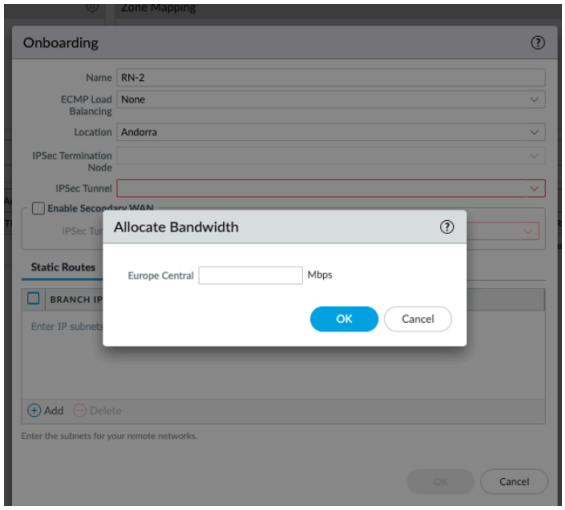
- **Secret**（シークレット）および**Confirm Secret**（シークレットの再入力）（任意）– BGPピア通信の認証のために、パスフレーズを入力して、その内容を確認します。

3. 前のステップを繰り返して、リモートネットワーク接続で使用するトンネルを、最大4つまで追加します。



STEP 9 | リモートネットワークロケーションを保護するために必要なインフラをPrisma Accessが展開する、**Location**（ロケーション）を選択します。この地域は、リモートネットワークロケーションと地理的に近い場所でなければなりません。

ロケーションがマップされている コンピューティングロケーション にまだ帯域幅を割り当てていない場合は、 Prisma Accessはそのコンピューティング場所の帯域幅を入力するように求めます。



STEP 10 | このリモート ネットワークに使用する **IPSec** 終端ノードを選択します。

Prisma Accessはこのノードを使用して、リモート ネットワークの場所とコンピューティングのロケーションを関連付けます。

©2025 Palo Alto Networks, Inc.

STEP 11 | （スタティックルーティングまたは単一トンネルのデプロイのみ）企業のロケーションにあるファイアウォール、ルーター、またはSD-WANデバイスにアクセスするための、新しい**IPSec Tunnel**（**IPSec**トンネル）設定を選択または追加します。

- Remote_Network_Template内の事前定義済みの IPSec テンプレートのいずれかを選択します。または、IPsec トンネル構成を含むテンプレートを Remote_Network_Template_Stack に追加した (または定義済みの Remote_Network_Template を変更した) 場合は、ドロップダウンからその **IPsec** トンネルを選択します。各リモートネットワーク接続用に作成しているトンネルは、Prisma Accessを各支店のロケーションにあるIPSec対応デバイスに接続するものであることに注意してください。

  IPSecトンネルを設定する場合は、以下のガイドラインを使用してください。

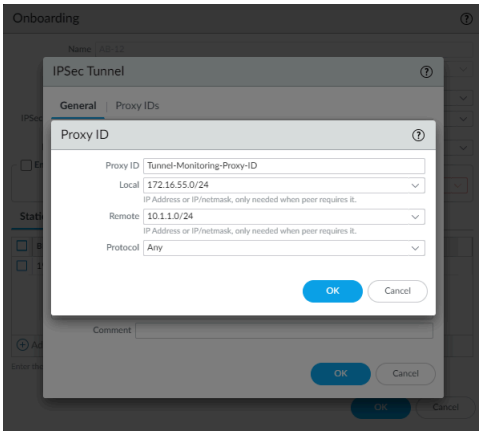
  - IKEゲートウェイ設定のピアアドレスは、各トンネルに対して一意でなければなりません。ただし、Crypto（暗号）プロファイルなど、他の一般的な一部の設定エレメントの再使用は可能です。
  - テンプレートから選択するIPSecトンネルは、Auto Key（自動鍵）交換とIPv4のみを使用する必要があります。
  - IPSec トンネル、IKE ゲートウェイ、および暗号プロファイル名は 31 文字を超えることはできません。
  - ダイナミックIKEピアがある同じロケーションへの、複数のリモートネットワークをオンボーディングする場合、すべてのリモートネットワーク設定で同じIKE暗号プロファイルを使用する必要があります。
- 新しいIPSecトンネル設定を作成するには、**New IPSec Tunnel**（新規**IPSec**トンネル）をクリックして、**Name**（名前）を入力してIKEゲートウェイ、IPSec暗号プロファイル、およびTunnel Monitoringの環境設定を行います。
  - 支店のロケーションにあるIPSec対応デバイスがポリシーベースのVPNを使用している場合、**Proxy IDs**（プロキシ**ID**）タブで、Prisma Accessがローカルデバイスとのの IPSecトンネルを正常に確立できるように、ローカルIPSecデバイスに設定されているプロキシIDと一致するプロキシIDを**Add**（追加）します。
- リプレイ攻撃を検出して無力化するために、**Enable Replay Protection**（リプレイプロテクションを有効にする）は選択された状態のままにしてください。
- 元のTOS情報を保持するため、カプセル化されたパケットの内部IPヘッダーから外部IPヘッダーにTOS（Type of Service）フィールドをコピーするには、**Copy TOS Header**（**TOS**ヘッダーのコピー）を選択します。

©2025 Palo Alto Networks, Inc.

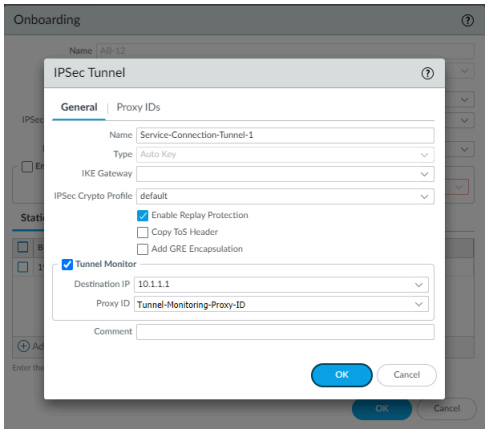
- サービス接続のトンネル監視を有効にするには、**Tunnel Monitor**（トンネル監視）を選択します。
  - **Destination IP**（宛先**IP**）アドレスを入力します。

    Prisma AccessがIPSecトンネル監視のために、ICMP pingリクエストを送信できる、支店のロケーションのIPアドレスを指定します。このアドレスは、Prisma Accessインフラのサブネット全体から、ICMPで到達可能であることを確認してください。
  - 複数のプロキシIDを使用するピアデバイスでトンネル監視をしようする場合、**Proxy ID**（プロキシ**ID**）を指定するか、またはインフラサブネットから支店のロケーションへのアクセスを可能にする、**New Proxy ID**（新しいプロキシ**ID**）を追加します。

    サービスインフラサブネット（この例では172.16.55.0/24）を**Local**（ローカル） IPサブネットに、支店ロケーションのサブネット（この例では10.1.1.0/24）を**Remote**（リモート）サブネットにしているプロキシIDの例を次に示します。



次の図は、作成したプロキシIDを**Proxy ID**（プロキシ**ID**）フィールドに指定することで、そのプロキシIDをトンネル監視に適用した例です。



©2025 Palo Alto Networks, Inc.

トンネル監視が機能するには、*CPE* 上でトンネルモニタリング *IP* アドレスへのスタティックルートを構成する必要があります。支店のロケーションから*Prisma Access*へのトンネル監視に使用する宛先*IP*アドレスを探すには、***Panorama*** > ***Cloud Services***（クラウドサービス） > ***Status***（ステータス） > ***Network Details***（ネットワーク詳細）を選択して、***Service Infrastructure (***サービス インフラストラクチャ***)***ラジオボタンをクリックして、***Tunnel Monitor IP Address***（トンネル監視***IP***アドレス）を参照します。

STEP 12 | このロケーションにセカンダリWANリンクがある場合は、**Enable Secondary WAN**（セカンダリ**WAN**を有効にする）を選択します。

各リモートネットワークのセカンダリ*WAN*に対して、一意の*IPSec*トンネルを作成してください。*Prisma Access*では、複数のリモートネットワーク内のセカンダリ*WAN*に対する、同じ*IPSec*トンネルの再利用はサポートされていません。

セカンダリ WAN の設定は、次の展開ではサポートされていません。

- セカンダリ WAN がプライマリ IPsec トンネルを使用してアクティブ/アクティブモードに設定されている場合。
- 顧客宅内機器 (CPE) が、プライマリおよびセカンダリIPsecトンネルを使用する等コストマルチパス (ECMP) 構成で設定されている場合。

スタティックルートを使用する場合、トンネルのフェイルオーバー時間は検出時から15秒未満になりますが、ご利用のWANプロバイダによって異なります。

BGPルーティングを設定し、トンネル監視を有効にしている場合、セキュリティパラメータインデックス（SPI）が失敗していると判断するまでの、デフォルトのホールドタイムがもっとも短いのが、Tunnel Monitorです。これは、連続した15秒間のトンネル障害を検出すると、ピアへのすべてのルートを削除します。このように、Tunnel MonitorがBGPルートの動作を判断します。トンネルモニタリングを設定しない場合、ホールドタイマーはルートを削除する前にトンネルがダウンしている時間を決定します。 Prisma Accessは、RFC 4271で定義されているデフォルトのBGP HoldTime値90秒を使用します。これは、Prisma Accessが非アクティブなSPIのルートを削除するまでの最大待機時間です。ピアBGPデバイスに短いホールドタイムが設定されている場合、BGPホールドタイマーはより小さい方の値を使用します。

セカンダリトンネルが正常にインストールされた場合、プライマリトンネルが復旧するまでの間、セカンダリルートが優先されます。プライマリとセカンダリの両方が機能している場合は、プライマリルートが優先されます。

セカンダリ（バックアップ）接続に別の*BGP*ピアを使用する場合、*Prisma Access*は *CPE* によってアドバタイズされたマルチエグジットディスクリミネーター（*MED*）属性を尊重しません。この注意事項は、リモートネットワーク接続またはサービス接続のいずれかで複数の *BGP* ピアを使用する場合に適用されます。

©2025 Palo Alto Networks, Inc.

STEP 13 | ユーザーがアクセスする必要がある、リモートネットワークサイトのサブネットワークまたは個別のIPアドレスへのルーティングを有効にします。

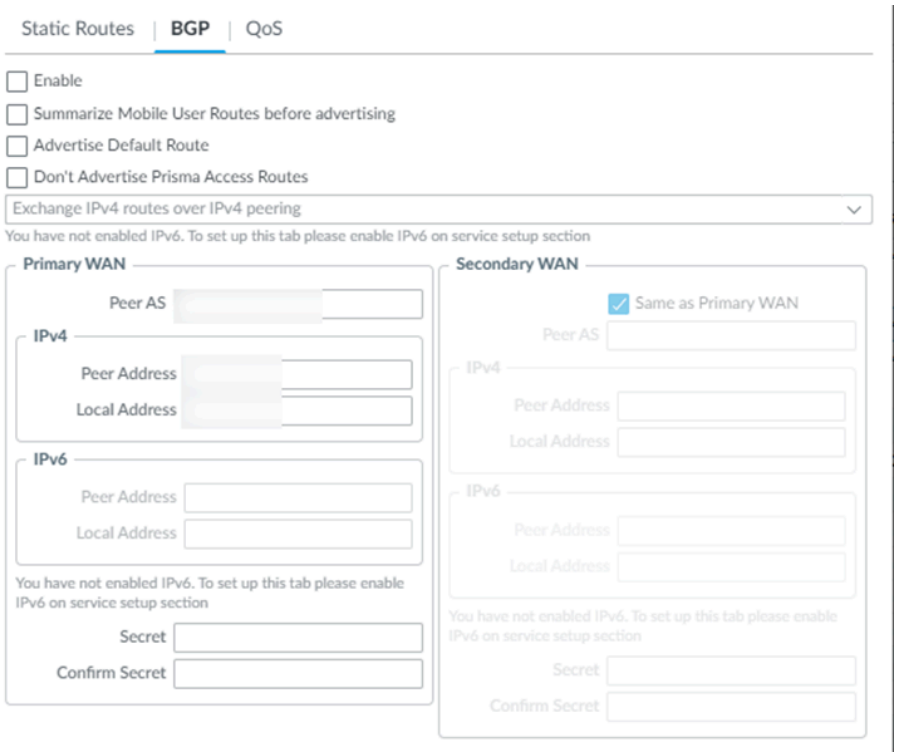
Prisma Accessはこの情報を使って、適切なサイトにリクエストをルーティングします。各サイトのネットワークは相互にオーバーラップすることはできません。また、サービスインフラ用またはユーザー用のPrisma AccessIPプール用に指定した各IPアドレスプールをオーバーラップさせることもできません。**Static Routes**（スタティックルート）、**BGP**、または両方の組み合わせを設定することができます。

- **Static Routes**（スタティックルート）を設定するには：
  1. **Static Routes**（スタティックルート）タブで**Add**（追加）をクリックして、リモートユーザーがアクセスする必要があるサブネットワークアドレス（例：172.168.10.0/24）、またはDNSサーバーなどのリソースの個別のIPアドレス（例：10.32.5.1/32）を入力します。
  2. この手順を繰り返して、Prisma Accessはこのロケーションにアクセスする必要があるすべてのサブネットまたはIPアドレスを指定します。



©2025 Palo Alto Networks, Inc.

- **BGP**を設定するには：
  1. **BGP** タブを選択します。
  2. (任意) **ECMP Load Balancing**（**ECMP**ロードバランシング）を選択します。ステップ8を参照してください。
  3. **ECMP Load Balancing**（**ECMP**ロードバランシング）で**None**（なし）を選択した場合は、BGPを入力します。



  4. リモートネットワークでBGPを有効にするには、**Enable**（有効）を選択します。

     BGPを有効にする場合、Prisma AccessインフラとeBGP接続の終端となる顧客構内設備（CPE）間に存在する可能性がある余分なホップに対応するために、Prisma Accessでは外部BGP（eBGP）のTTL値に8が設定されます。
  5. BGPから顧客構内設備（CPE）にアドバタイズされるモバイルユーザーIPサブネット数を要約して減らすには、**Summarize Mobile User Routes before advertising**（アドバタイズ前にモバイルユーザールートを要約する）を選択します。

     デフォルトでPrisma Accessは、モバイルユーザーのIPアドレスプールを、/24サブネットのブロックでアドバタイズします。それを要約すると、Prisma Accessによって指定したサブネットに基づいてプールがアドバタイズされます。たとえば、Prisma Accessは、パブリックユーザーのモバイルIPプールを、アドバタイズ前に10.8.1.0/24、10.8.2.0/24、10.8.3.0/24などのサブネットに分割するのではなく、/20のサブネットを使用して10.8.0.0/20のプールをアドバタイズします。これらのアドバタイズを要約することで、CPEルーティングテーブルに保存されるルート数を削減できる可能性があります。たとえば、限定された数のルートを受け付けるクラ

©2025 Palo Alto Networks, Inc.

ウドVPNゲートウェイ（仮想プライベートゲートウェイ（VGW）またはトランジットゲートウェイ（TGW））で、IPプールの要約を使用することができます。

Prisma Accessは、集約されたモバイルユーザールートに対してコミュニティ文字列を`0xFFFE:0xFFF0`に設定します。

6. Prisma Accessに、eBGPを使ったリモートネットワーク用のデフォルトルートのアドバタイズを許可するには、**Advertise Default Route**（デフォルトルートのアドバタイズ）を選択します。

   Advertise Default Route（デフォルトルートのアドバタイズ）を選択した場合、ネットワークにBGPがアドバタイズしている他のデフォルトルートが存在していないことを確認してください。そうしないと、ネットワークにルーティング上の問題が発生する可能性があります。

   アドバタイズするためにこの項目を選択する前に、デフォルトのルートを公開する必要があります。また、ネットワークに、*BGP*がアドバタイズしている他のデフォルトルートが存在していないことを確認してください。そうしないと、ネットワークにルーティング上の問題が発生する可能性があります。

7. Prisma Accessファイアウォール上のBGPピアが、組織のネットワークにルートを転送することを防止するには、**[Prisma Accessルートをアドバタイズしない]**を選択します。

   デフォルトで、Prisma Accessは、ローカルルート、および他のサービス接続、リモートネットワーク、およびモバイルユーザーサブネットから受信するすべてのプレフィックスを含め、すべてのBGPルーティング情報をアドバタイズします。Prisma AccessによるBGPアドバタイズメントの送信を防止しながら、受信したBGP情報を使って、他のBGPネイバーからルートを学習するには、このチェックボックスを選択します。

   このオプションを選択するとBGPアドバタイズメントは送信されないため、Prisma Accessへのルートを確立するために、オンプレミス機器でスタティックルートを設定する必要があります。

8. **Peer AS**を入力します。これは、リモートネットワークのファイアウォール、仮想ルーター、またはBGPルーターが所属している自律型システム（AS）です。

9. この接続を**Peer Address**（ピアアドレス）として設定するリモートネットワーク上の、eBGPルーターのルーターID として割り当てるIPアドレスを入力します。

10. （任意） Prisma Accessが、BGPのローカルIPアドレスとして使用するアドレスを入力します。

    Local Addressの指定は、接続のもう一方の側にあるデバイス（Amazon Web Service（AWS） Virtual Private Gatewayなど）が、BGPピアリングを正常に行うために、特定のローカルIPアドレスを必要としている場合などに役立ちます。指定するIPアドレス

©2025 Palo Alto Networks, Inc.

は、インフラサブネットまたはリモートネットワーク内のサブネットのIPアドレスと、競合またはオーバーラップしていないことを確認してください。

*CPE*上で*BGP*ローカル アドレスへのスタティック ルートを設定する必要があります。

11. （任意） BGPピア通信の認証のために、パスフレーズを入力して、その内容を確認します。
12. （任意）**Secondary WAN**（セカンダリ**WAN**）を設定しており、セカンダリ（バックアップ）BGPピアの**Peer Address**（ピアアドレス）または**Local Address**（ローカルアドレス）を変更する必要がある場合、**Same as Primary WAN**（プライマリ**WAN**と同じ）の選択を解除して一意のピアを入力します。また、必要に応じてセカンダリWANのローカルIPアドレスを入力します。

   リモート ネットワーク デプロイメントで IPv6 ネットワーク を使用する場合は、**IPv4**アドレスだけでなく **IPv6**アドレスも構成できます。また、IPv6アドレッシングを使用する前に、Prisma AccessインフラでIPv6ネットワークをグローバルに有効にする必要があります。

   一部のデプロイ環境では（例:AWS VPNゲートウェイを持つピアにBGPを使用している）、プライマリWANとセカンダリWANのBGPピアが異なっていることがあります。そのような場合、セカンダリWANに対して、別のBGPピアを設定することができます。

   セカンダリ*WAN*を持つ*BGP*デプロイ環境の場合、*Prisma Access*はプライマリトンネルとセカンダリトンネルの両方の状態を***UP***に設定しますが、ネットワークトラフィックに対しては標準の*BGP*アクティブ-バックアップ動作に従います。*Prisma Access*はプライマリ トンネルをアクティブに設定し、そのトンネルを介してのみトラフィックを送受信します。プライマリ トンネルに障害が発生した場合、*Prisma Access*は*BGP*ルールを使用して障害を検出し、セカンダリ トンネルをアクティブに設定し、セカンダリ トンネルのみを使用してトラフィックを送受信します。

STEP 14 | (任意) 場所に対して**QoS**を有効にし、**QoS**プロファイルを指定します。

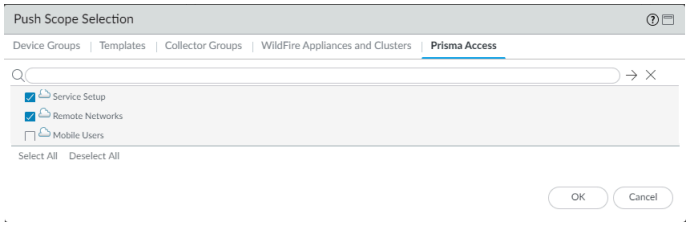
QoSオプションおよび全体的な設定は、[設定]でコンピュート ロケーションごとに指定しますが、QoSの有効化、無効化、およびQoSプロファイルの変更は、ここでロケーションごとに行うことができます。

STEP 15 | Panoramaに設定の変更内容をコミットし、設定をPrisma Accessにプッシュします。

1. **Commit**（コミット） > **Commit to Panorama**（**Panorama** へのコミット）をクリックします。
2. **Commit**（コミット） > **Commit and Push**（コミットしてプッシュ）をクリックします。**Edit Selections**（選択項目の編集） > **Prisma Access**の順に選択して、ネットワーク

©2025 Palo Alto Networks, Inc.

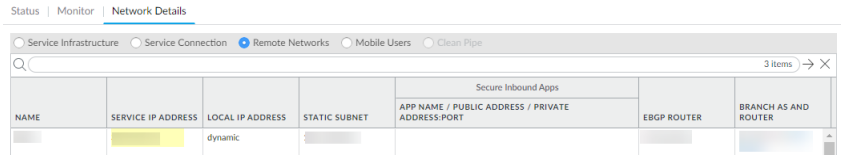
用のPrisma AccessおよびPrisma Access for service setupの両方を選択し、サービスに設定をプッシュします。



3. **OK**、**Push**（プッシュ）の順にクリックします。

STEP 16 | リモートネットワークロケーションにあるIPSec対応デバイスを設定して、ネットワーク用のPrisma AccessとのIPSec接続をセットアップします。

1. **Panorama** > **Cloud Services** > ステータス > ネットワーク詳細を選択し、 リモート ネットワーク ラジオ ボタンをクリックし、 サービス **IP** アドレス フィールドを表示して、このリモート ネットワーク接続の サービス **IP** アドレス を見つけます。 ネットワーク用Prisma Accessインフラストラクチャは、リモート ネットワーク接続用にこのまたはIPアドレスを割り当てているため、Prisma Accessリモート ネットワーク ロケーションとネットワーク用Prisma Accessの間でIPSecトンネルをセットアップするには、これをピアIPアドレスとして設定する必要があります。



2. **Panorama** > **Cloud Services**（クラウドサービス） > **Status**（ステータス） > **Network Details**（ネットワーク詳細） > **Remote Networks**（リモートネットワーク）ページで、リモートネットワークロケーションにあるデバイスの**Local IP address**（ローカル**IP**アドレス）を確認します。リモートネットワークロケーションでNATを実行している場合、**Local IP address**（ローカル**IP**アドレス）にはNAT処理後のデバイスのIPアドレスが表示されます。

STEP 17 | リモートネットワークロケーションのトラフィックを保護するには、セキュリティポリシールールを作成する必要があります。

1. **Policies (**ポリシー**)**を選択します。
2. ポリシールールを追加する**Device Group** （デバイス グループ）を選択します。Remote_Network_Device_Group、またはリモートネットワークロケーションを保護するポリシーを定義するために選択した親デバイスグループを選択することができます。
3. セキュリティポリシールールを作成します。任意の（Any）ゾーンから任意のゾーンへのトラフィックを許可するセキュリティポリシールールを定義していないことを確認してください。セキュリティポリシールールでは、テンプレート内に定義したゾーンを使用します。

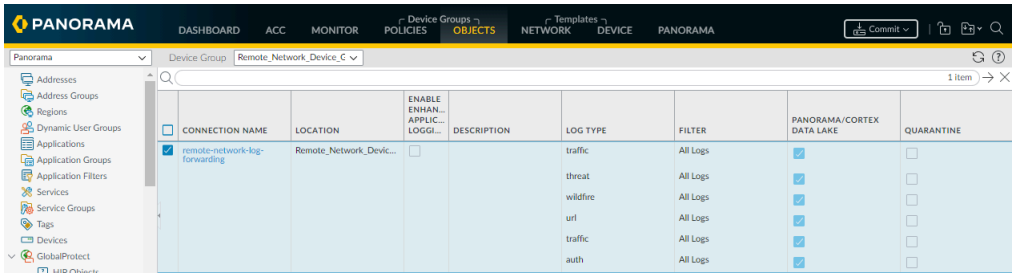
   ネットワーク上のユーザーが、Webサイトへのアクセスを拒否された場合、Palo Alto Networksでチケットを開く前に、Webサイトアクセス上の問題を報告してください。

©2025 Palo Alto Networks, Inc.

STEP 18 | Strata Logging Serviceへのロギングを有効にします。ログを転送する各ポリシー ルールにログ転送プロファイルを作成して、アタッチする必要があります。

1. **[Objects] > [**ログ転送**]** の順に選択します。
2. ポリシールールを追加した**Device Group**（デバイスグループ）を選択します（例：Remote_Network_Device_Group）。
3. ログ転送プロファイルを**Add**（追加）します。ログ転送プロファイル一致リストで、転送する各**Log Type**（ログタイプ）を**Add**（追加）します。
4. 転送方法として**Panorama/Strata Logging Service (**ロギングサービス**)**を選択し、Prisma AccessがログをStrata Logging Serviceに転送できるようにします。Panoramaからログを監視し、レポートを作成することができます。 Strata Logging Serviceはシームレスな統合を提供し、ログを本社のPanoramaにバックホ ールすることなく保存し、Panoramaは必要に応じてStrata Logging Serviceにクエリを実行することができます。

   Traffic（トラフィック）、Threat Prevention（脅威防御）、WildFire Submission（WildFire送信）、URL Filtering（URLフィルタリング）、Data Filtering（データフィルタリング）、およびStrata Logging ServiceへAuthentication（認証）ログを転送する例を次に示します。



5. **Policies**（ポリシー） **> Security**（セキュリティ）を選択して、ポリシールールを編集します。**Actions**（アクション）で、作成した Log Forwarding（ログ転送）プロファイルを選択します。

STEP 19 | Panorama にすべての変更をコミットし、その設定変更をPrisma Accessにプッシュします。

1. **Commit**（コミット） **> Commit and Push**（コミットしてプッシュ）をクリックします。
2. **[**選択内容を編集**]**をクリックし、**[Prisma Access]**タブで**[Push Scope (**スコープをプッシュ**)]**に**[**ネットワーク用**Prisma Access]**が選択されていることを確認し、**[OK]**をクリックする。
3. 変更を **Commit and Push**（コミットしてプッシュ）します。

STEP 20 | リモート ネットワークのステータスを確認します。

詳細は リモートネットワークがPrisma Accessに接続されているかどうかを確認する を参照してください。

 ©2025 Palo Alto Networks, Inc.

新しいモデルへの移行を計画する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

新規のPrisma Accessリモート ネットワーク デプロイメントの帯域幅は、コンピュート・ロケーションごとの集約レベルで割り当てられるが、これは帯域幅の集約モデルとも呼ばれます。コンピュート ロケーション レベルで帯域幅を割り当てると、Prisma Accessが負荷や需要に基づいて動的に各ロケーションの帯域幅を割り当てるため、ライセンスされたリモート ネットワークの帯域幅をより柔軟に割り当てることができます。

Prisma Accessのロケーションごとに帯域幅を割り当てる既存のデプロイメントを使用している場合は、集約帯域幅モデルに移行できます。リモートネットワークのQoSデプロイメントを移行することもできます。移行すると、すべてのリモートネットワークは集約帯域幅モデルを使用します。

集約帯域幅モデルへの移行を計画するには、次のチェックリストを使用します。

- ❑ 注) 移行後も変更されない以下のリモートネットワークコンポーネント:
  - データプレーンには変更はありません。トラフィックは、既存の構成を変更することなく、Prisma Accessのデータプレーンを流れ続けます。
  - 移行は既存のトンネルに影響を与えません。

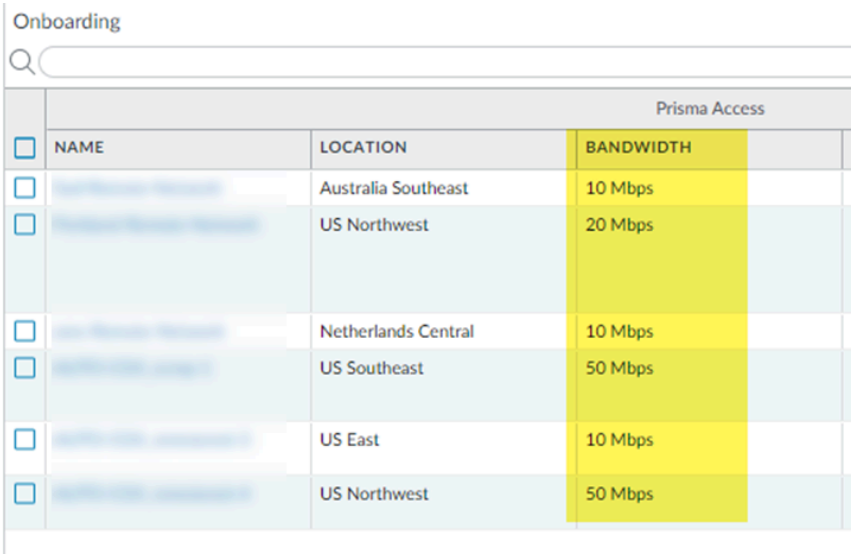
    IPSecトンネル パラメータを再構成する必要はありません。IKEゲートウェイ、IKEおよびIPSec暗号プロファイル、IPSecトンネル構成は変更されません。
  - デプロイメントをアグリゲート帯域幅モデルに移行しても、リモートネットワークサービスIPアドレス (リモート ネットワーク接続のためにPrisma AccessIPSecトンネル側で使用されるまたはパブリックIPアドレス）は変更されず、IPSec トンネルの再設定は必要ありません。
- ❑ Prisma AccessはIPSec終端ノードを割り当て、集約帯域幅モデルへの移行中にリモートネットワークに帯域幅を割り当てます。移行する前に、このモデルがどのように機能するかを理解する必要があります。

> 移行後、既存のリモート・ネットワークを別の *IPSec* 終端ノードに再割り当てしたい場合、*Prisma Access*は、変更をコミットしてプッシュした後、***Service IP Address (***サービス***IP***アドレス***)***を割り当てます。この場合、リモート ネットワーク トンネルの新しい*IP*アドレスを指すように*CPE*を再構成する必要があります。

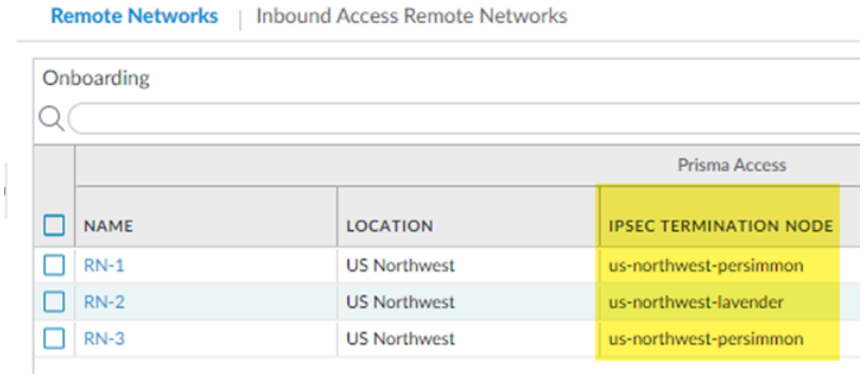
©2025 Palo Alto Networks, Inc.

- サポートされていない構成の場合、帯域幅割り当てタブは表示されず、移行するためのバナーも表示されません。次の構成は、集約帯域幅モデルへの移行ではサポートされていません。
  - 帯域幅が **1000 Mbps**のリモート ネットワーク。
  - PrismaのSD-WAN CloudBladeとの統合で使用されているPrisma Accessのバージョンが3.0より前のもの。
  - 2.1 Innovationより前のリモート ネットワーク サイトのアプリケーションへの安全な着信アクセスを提供するリモート ネットワーク構成。

  リモートネットワークでQoSを使用する場合は、移行する前にQoS移行ガイドラインに従ってください。
- デプロイメントで使用しているモデルが不明な場合は、**[Panorama]** > **[Cloud Services (**クラウドサービス**)]** > **[Configuration (**構成**)]** > **[Remote Networks (**リモート ネットワーク**)]**を選択します。
  - リモートネットワーク］領域に［帯域幅］フィールドが表示されている場合は、 Prisma Accessロケーション別に帯域幅を割り当てているため、集約帯域幅モデルに移行できます。

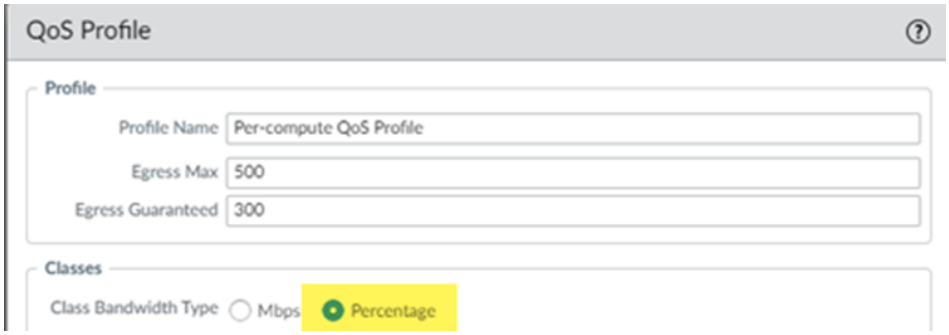


  - **IPSec**終端ノードが表示される場合は、すでに集約帯域幅モデルに移行しています。



 ©2025 Palo Alto Networks, Inc.

- 集約帯域幅モデルに移行した後、この変更は永続的なものであり、 Prisma Accessロケーションごとに帯域幅を割り当てるデプロイメントに戻すことはできません。
- 集約帯域幅モデルに移行するには、最低50 Mbpsの利用可能な帯域幅が必要です。
- 移行後にQoSを実装したい場合は、集約帯域幅デプロイメントのためのQoS設定の違いについて学んでください。
  - QoS プロファイルではクラス帯域幅タイプとして**Mbps**ではなくパーセンテージを使用するようにしてください。 コンピューティング場所によって帯域幅を割り当てるデプロイメントの場合、Prisma AccessはQoSプロファイルで**Mbps**の帯域幅タイプをサポートしません。



  - 保証された帯域幅比率を指定する方法と、サイトごとに帯域幅をカスタマイズする方法について理解します。

    保証された帯域幅比率を使用すると、コンピューティング ロケーションに割り当てられた合計帯域幅のパーセンテージを割り当てることができます。 Prisma Accessは保証された帯域幅をコンピューティング場所のIPSec終端ノードの数で均等に分割します。

    サイトごとに帯域幅をカスタマイズすることで、単一のIPSec終端ノードにサイトの割り当て比率を適用し、リモート ネットワーク設定でサイトごとにQoSプロファイルを指定できます。または、リモート ネットワークを選択し、**[QoS]**タブでQoSプロファイルを指定することにより、リモート ネットワーク構成中にQoSプロファイルを指定することもできます。
- リモート ネットワークの場所への安全なインバウンドアクセスを提供するようにリモート ネットワークを構成している場合は、セカンダリ WAN リンク (セカンダリ**WAN**を有効にする)、BGP、QoS、ソース NAT オプションの有効化など、既存のインバウンドアクセス機能がすべてサポートされます。また、Prisma Accessが割り当てるパブリックIPアドレスによって消費される帯域 幅にも変化はありません。 (5つのIPアドレスはリモート ネットワーク ライセンス割り当てから150 Mbpsを取得し、10個の IPアドレスは300 Mbpsを取得します)。

  移行後に受信アクセスを構成する必要がある場合は、 集約帯域幅モデルに固有の受信アクセス手順を使用します。

©2025 Palo Alto Networks, Inc.

- Palo Alto Networksでは、移行する前に、既存の帯域幅設定とライセンスされた帯域幅の合計をメモしておくことをお勧めします。

  それでも *Prisma Access*は移行中に帯域幅が移行されます。ベストプラクティスとして現在の設定をメモし、移行後にコンピューティング ロケーションの帯域幅を調整する必要があります。

  - **[Panorama] > [Cloud Services (**クラウド サービス**)] > [Configuration (**構成**)] > [Remote Networks (**リモート ネットワーク**)]** 選択して既存の帯域幅設定を確認し、各リモート ネットワーク接続で使用可能な既存の 帯域幅 をメモします。
  - **[Panorama] > [Licenses (**ライセンス**)]** に移動し、リモート ネットワークの合計ライセンス帯域幅 (Mbps) を確認します。この情報は、ライセンスの種類に応じて、**Prisma Access Net Capacity** または **GlobalProtect Cloud Service for Mobile Users**に含まれます。

移行後、デプロイメントにおける次の違いをメモします。

- 集約帯域幅リモートネットワークオンボーディング手順を使用して、すべての新しいリモートネットワークをオンボードします。
- 帯域幅使用統計を表示する場合、IPSec終端ノード レベルごとに統計を表示します。

移行された集約帯域幅デプロイメントの帯域幅割り当て

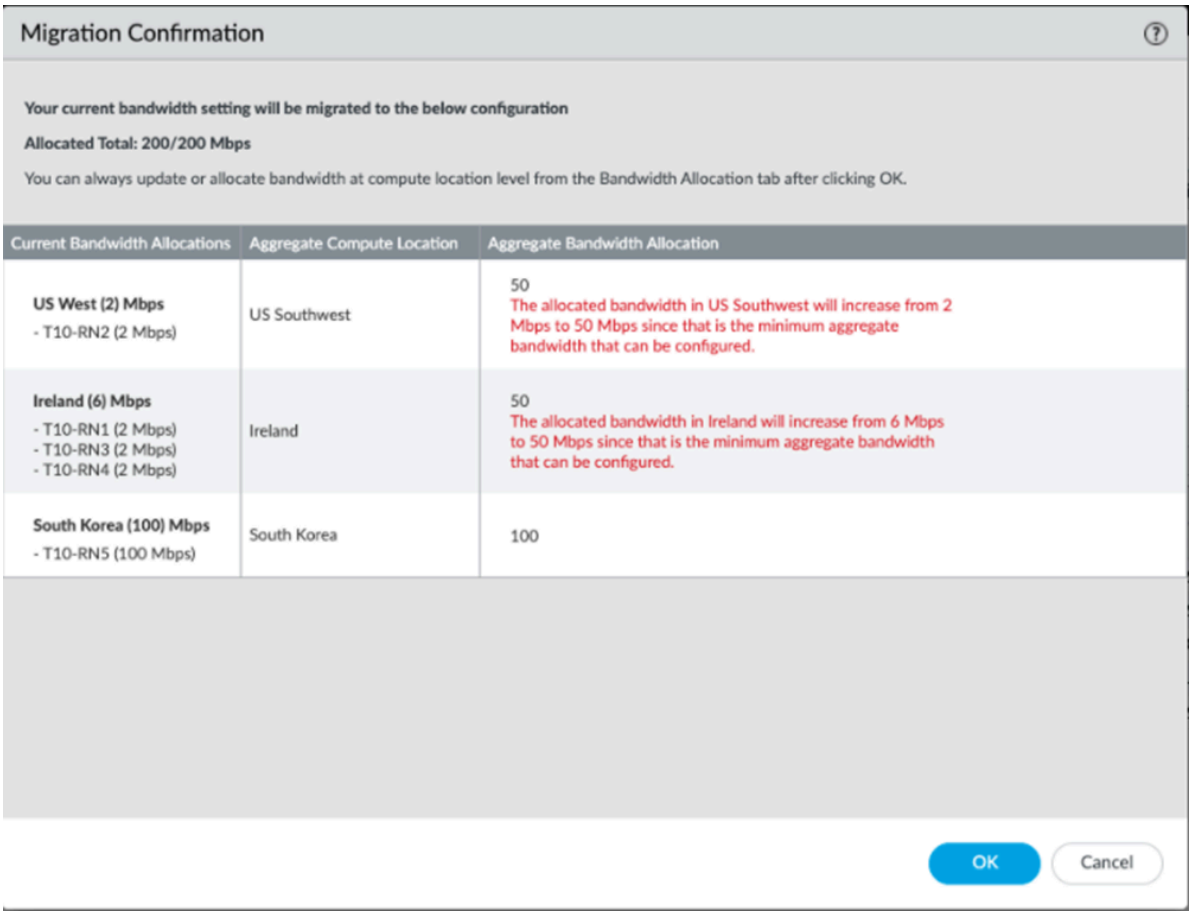
Prisma Accessロケーションごとに帯域幅を割り当てるデプロイメントを使用している場合、Prisma Access は、集約帯域幅モデルに移行すると、以下の変更を行います：

- Prisma Accessは特定のコンピューティング ロケーション内のすべてのロケーションの帯域幅を合計し、その合計帯域幅をそのコンピューティング ロケーションに割り当てます。

  たとえば、メキシコ西部、米国南西部、米国西部に3つのロケーション (ロケーション **1**、 ロケーション **2**、 ロケーション **3**) があり、既存の各ロケーションの帯域幅が50 Mbpsであるとします。各拠点は米国南西部のコンピューティング拠点にあるため、 Prisma Accessは3つの場所の帯域幅を合計し、米国南西部の場所に150Mbpsの帯域幅を割り当てます。

©2025 Palo Alto Networks, Inc.

- コンピューティングロケーション内のすべてのロケーションの合計帯域幅が50Mbps未満の場合、 Prisma Accessはそのコンピューティング場所の帯域幅が50 Mbpsに増加します。 Prisma Accessは、移行プロセス中に帯域幅の増加が必要となる場所を提供します。



- Prisma Accessは集約帯域幅デプロイメントでIPSec終端ノードを使用します。移行中、Prisma Accessは割り当てられた帯域幅1,000 Mbpsごとに、コンピューティング場所ごとに1つのIPSec終端ノードを提供します。たとえば、コンピューティング拠点に1500Mbpsの帯域幅を割り当てると、 Prisma Accessはそのロケーションに2つのIPSec終端ノードを提供します。

  リモート ネットワークのオンボーディング中に、IPSec終端ノードをリモート ネットワークに割り当てます。集約帯域幅移行では、 Prisma Accessは移行中にIPSec終端ノードをリモート ネットワークに関連付けます。次のリストは、移行のためのIPSec終端ノードの関連付けの例を示しています。

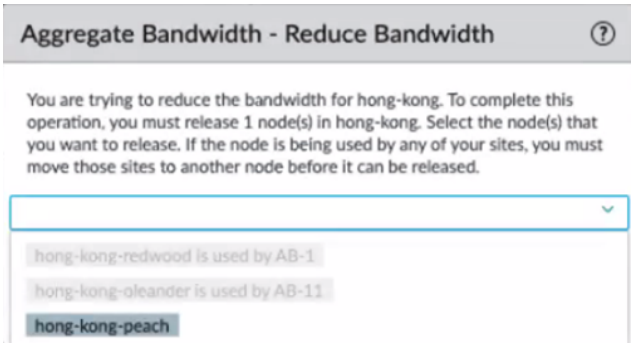
  - 同じコンピューティングロケーションに4つのリモートネットワークがあり、それぞれのロケーションの帯域幅が50Mbpsの場合、 Prisma Accessはそのコンピューティング ロケーションに200 Mbpsの帯域幅を割り当て、そのコンピューティング ロケーションに単一のIPSec終端ノードを提供し、そのIPSec終端ノードを4つのリモート ネットワークすべてに関連付けます。
  - 同じコンピューティング場所にそれぞれ100Mbpsのリモートネットワークが3つある場合、 Prisma Accessはそのコンピューティング ロケーションに300 Mbpsの帯域幅を割

©2025 Palo Alto Networks, Inc.

り当て、そのコンピューティング ロケーションに単一のIPSec終端ノードを提供し、そのIPSec終端ノードを3つのリモート ネットワークすべてに関連付けます。

- 同じコンピューティング場所に7つのリモートネットワークがあり、そのうち2つのリモートネットワークが500Mbps、5つのリモートネットワークがそれぞれ100Mbpsの場合、Prisma Accessはそのコンピューティング場所に1500 Mbpsの帯域幅を割り当てます。そのコンピューティングロケーションに割り当てられた帯域幅の合計は1,000Mbpsを超えているため、 Prisma Accessは2つの IPSec 終端ノードを割り当て、次の関連付けを行います。
  - 2つの500 Mbpsリモート ネットワークには、1つのIPSec終端ノード (1,000 Mbps リモート ネットワークごとに1つのノード) が割り当てられます。
  - 5つの100 Mbpsリモート ネットワークに1つのIPSec終端ノードが割り当てられます。

  移行後、IPSec終端ノードの関連付けを変更して、場所の帯域幅を増やすことができます。たとえば、2つのIPSec終端ノードがあるコンピューティング場所の場合、1つのIPSec終端ノードを1つの場所に再割り当てし、もう1つのIPSec終端ノードを残りの場所に再割り当てすることができます。これにより、IPSec終端ノードを共有していない場所に、より多くの帯域幅が効果的に提供されます。
- 帯域幅を十分に削減すると、IPSec終端ノードを解放する必要がある場合があります。たとえば、コンピューティング ロケーションの帯域幅を1500 Mbpsから800 Mbpsに削減する場合は、既存のIPSec終端ノードの1つを削除する必要があります。これらのノードのいずれかが既存の場所で使用されている場合は、IPSec 終端ノードを削除する前に、IPSec 終端ノードを再割り当てする必要があります。



QoS移行ガイドライン

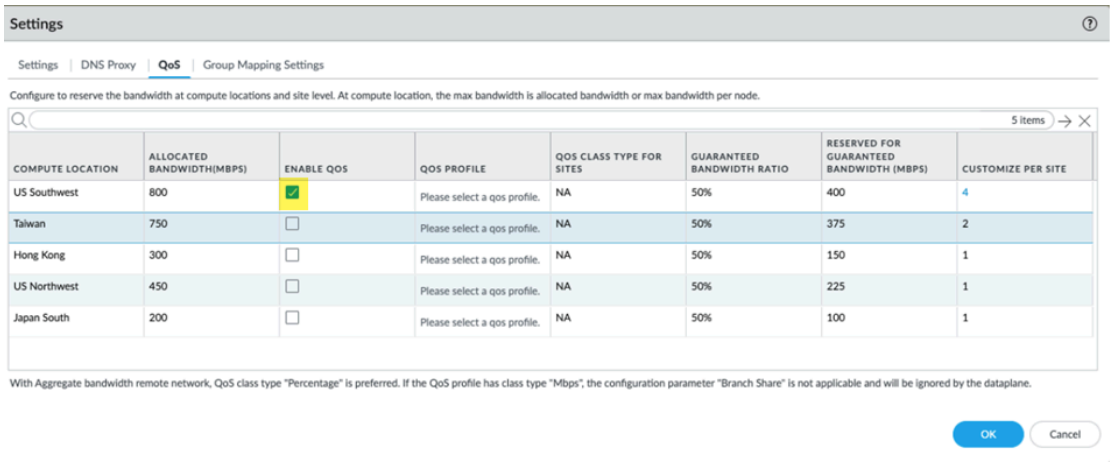
現在のPrisma Accessリモート ネットワーク デプロイメントでQoSを使用し、場所ごとに帯域幅を割り当てている場合、既存の QoS ポリシーとプロファイルを保持したまま、集約帯域幅のデプロイメントに移行できます。

集約帯域幅モデルを使用すると、コンピューティング場所ごとに集約レベルで帯域幅を割り当て、 Prisma Accessは場所ごとの負荷または需要に基づいて帯域幅を動的に割り当てます。

移行後、**QoS** タブにリモート ネットワーク設定 (**Panorama** > **Cloud Services** > **Configuration** (構成) > リモート ネットワーク > **Settings** (設定)) のQoS構成が表示されます。QoSが有効になっている場所にマップされるコンピューティング場所では、**[QoS**を有効にする] が選択され、QoSが有効になっていない場所にマップされるコンピューティング場所では、**[QoS**を有効にする] の選択が解除されます。

©2025 Palo Alto Networks, Inc.

次のスクリーンショットは、移行後のQoSタブのサンプルを示しています。米国西部のリモートネットワークではQoSが有効になっていますが、他の場所ではQoSが有効になっていません。米国西部の場所は米国南西部のコンピューティング場所にマップされるため、**QoS**タブには米国南西部のコンピューティング場所に対してQoSが有効になっていることが表示されます。

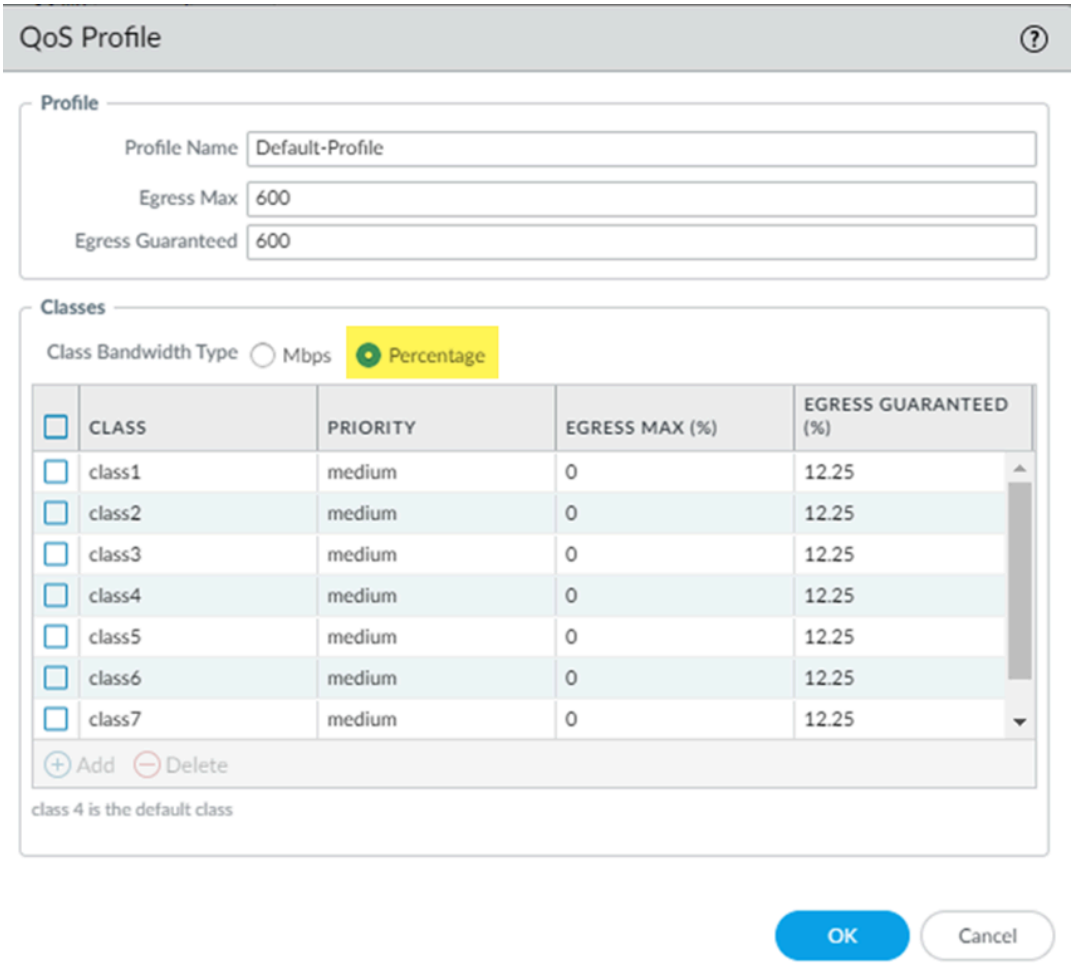


Palo Alto Networks は、集約帯域幅の展開におけるQoSに関して次の推奨事項と要件を示しています。

- 帯域幅は単一のコンピューティング ロケーション内のすべてのロケーションで共有されるため、 クラス帯域幅タイプを**Mbps**からパーセンテージに変更する必要があります。**Mbps**の帯

©2025 Palo Alto Networks, Inc.

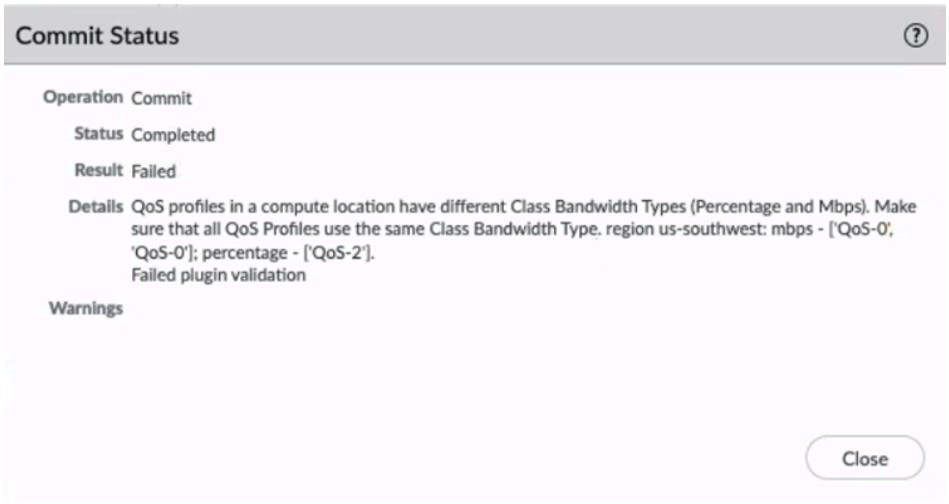
域幅タイプがサポートされるのは、場所ごとに帯域幅を割り当てる既存の展開があり、その後集約帯域幅の展開に移行する場合のみです。



- プロファイル内の Mbps に基づいて QoS 帯域幅の割り当てを調整することはできません。パーセンテージ帯域幅タイプを使用するプロファイルの場合は、保証帯域幅比率を調整し、サイトごとにQoSプロファイルをカスタマイズすることで、場所ごとにQoS帯域幅を変更できます。

©2025 Palo Alto Networks, Inc.

- コンピューティング ロケーションで帯域幅の種類を混在させることはできません。混在させると、コミット中にエラー メッセージが表示されます。

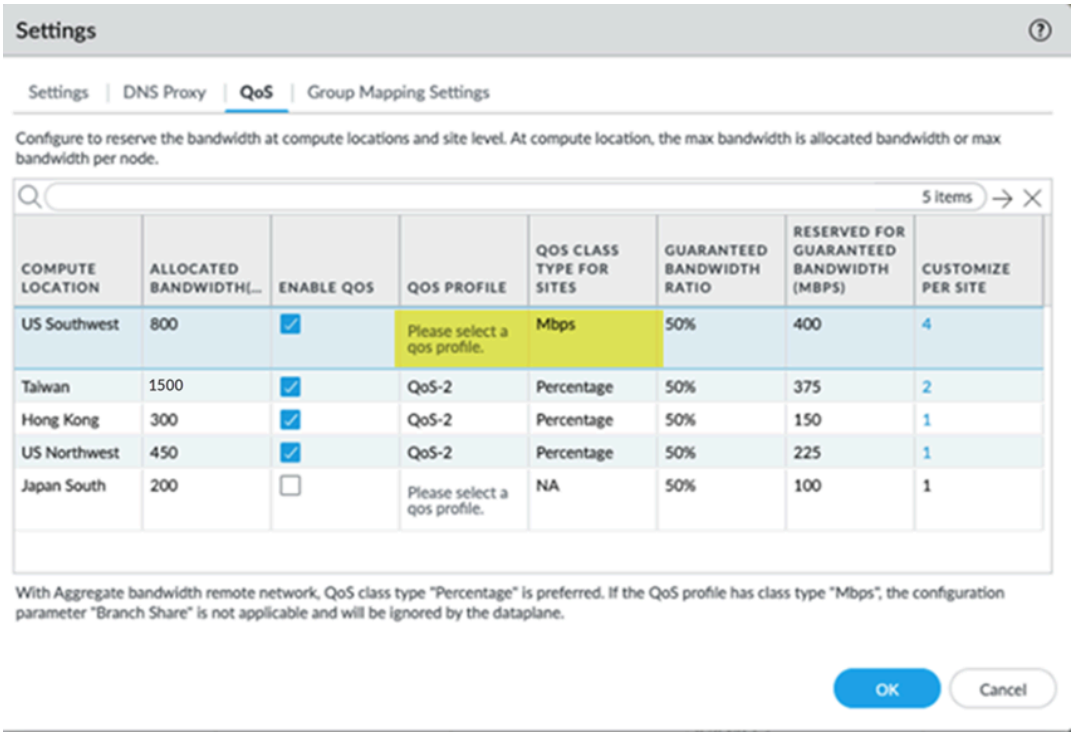


- 新しい場所を追加し、それらの場所が新しいコンピューティング場所に属している場合、新しいコンピューティング場所では、クラス帯域幅タイプがパーセンテージであるプロファイルのみを作成できます。
- クラス帯域幅タイプ が **Mbps**のQoSプロファイルを保持する場合、保証帯域幅比率に加えた変更やサイトごとのQoSプロファイルのカスタマイズは無視されます。
- 移行後、 クラス帯域幅タイプが**Mbps**のQoSプロファイルを使用するすべての場所では、**QoS**タブの対応するコンピューティング場所に対してサイトの**QoS**クラス タイプが**Mbps**と表示されます。クラス帯域幅タイプがパーセンテージのQoSプロファイルでは 、サイトの**QoS**クラス タイプがパーセンテージとして表示されます。

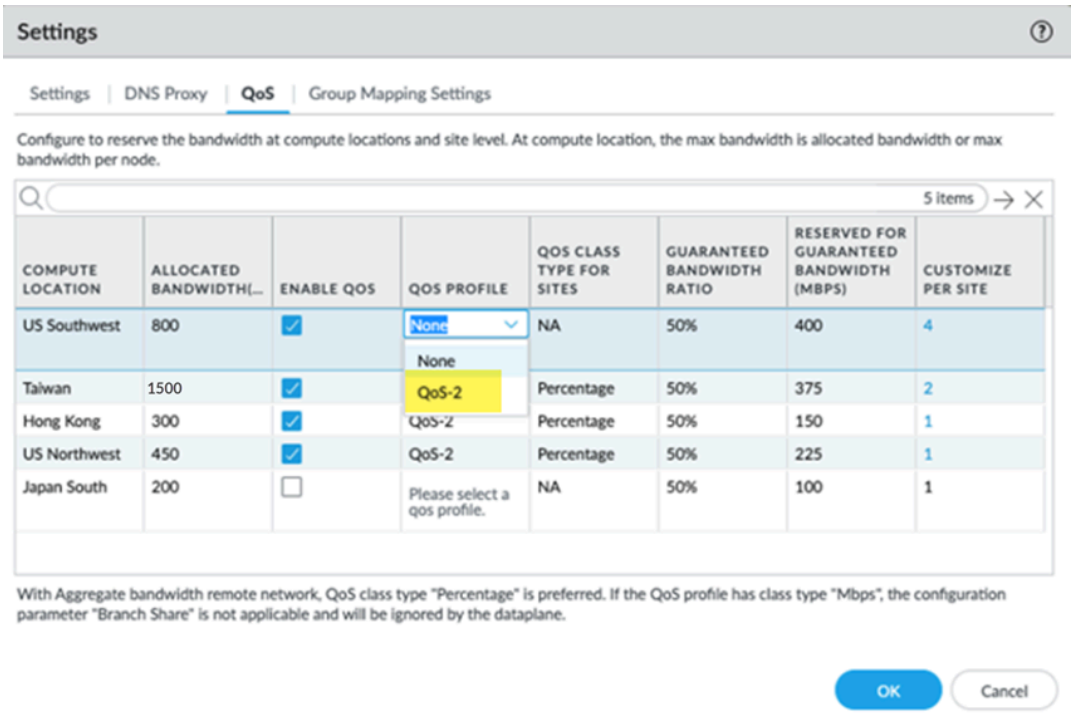
  また、 クラス帯域幅タイプが**Mbps**である QoSプロファイルを選択することはできません。次のスクリーンショットは、クラス帯域幅タイプが**Mbps**のQoSプロファイルを使用してい

©2025 Palo Alto Networks, Inc.

る米国南西部のコンピューティング ロケーションを示しています。この選択肢は、**QoS**プロファイル領域のドロップダウンでは選択できません。



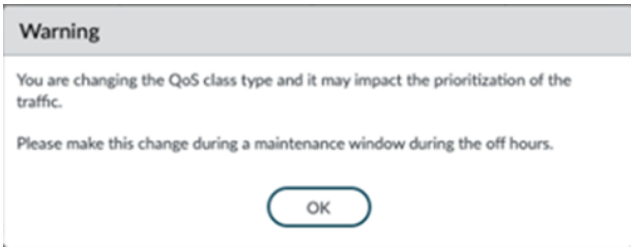
ただし、クラス帯域幅タイプとしてパーセンテージ を使用するQoSプロファイル (この例ではQoS-2) を選択できます。



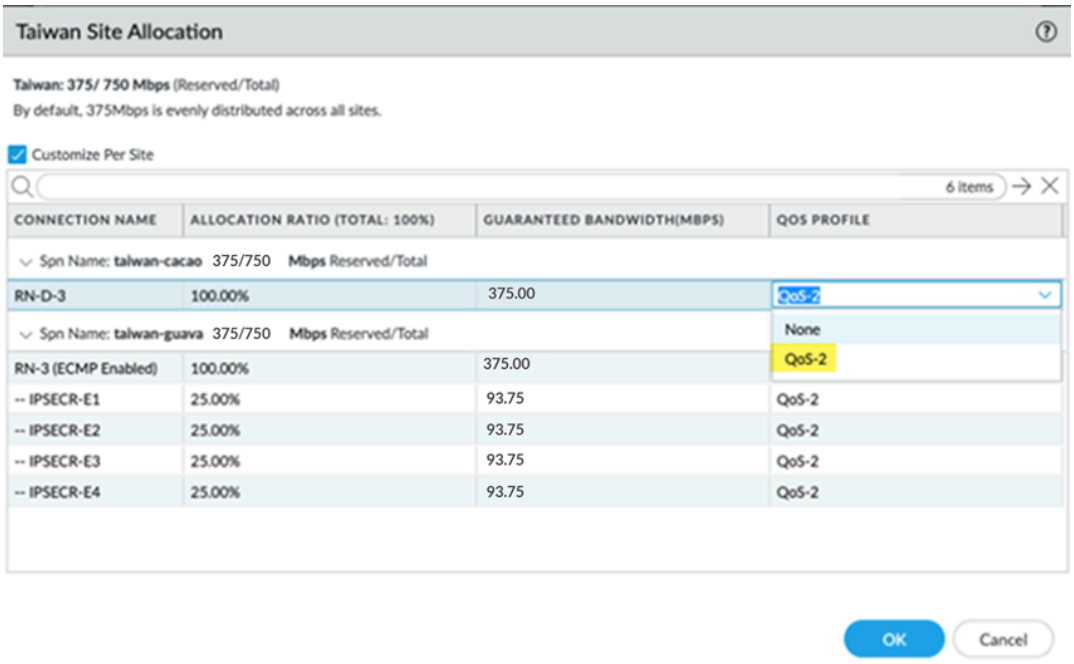
- コンピューティング ロケーションのQoSプロファイルをクラス帯域幅タイプ**Mbps** からパーセンテージに変更する場合は、メンテナンス ウィンドウまたはオフピーク時間中に変更を行

©2025 Palo Alto Networks, Inc.

う必要があります。QoSプロファイルを変更すると、トラフィックの優先順位が変更される場合があります。



- サイトごとに QoS プロファイルをカスタマイズする場合は、 クラス帯域幅タイプがパーセンテージのQoSプロファイルのみを選択できます。



帯域幅管理設定を移行する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

帯域幅管理設定を移行する方法を学ぶ。

ロケーションごとに帯域幅を割り当てるPrisma Accessリモートネットワークのデプロイメントを使用している場合、Prisma Accessでは、コンピュートロケーションごとに帯域幅を割り当てるデプロイメント（集約帯域幅モデル）に移行することで、デプロイメントをより柔軟でスケーラブルなものにすることができます。移行計画チェックリストを確認した後、次の手順に従って

©2025 Palo Alto Networks, Inc.

集約帯域幅モデルに移行します。リモートネットワークのQoSデプロイメントを移行することもできます。移行すると、すべてのリモートネットワークは集約帯域幅モデルを使用します。

移行する前に、帯域幅設定について以下の点を考慮してください:

- 移行後も変更されない以下のリモートネットワークコンポーネント:
  - Prisma Accessデータプレーン。
  - 既存のトンネルへの影響はありません。
  - IPSecトンネルパラメータの再構成はありません。
  - IKEゲートウェイ、IKEおよびIPSec暗号プロファイル、IPSecトンネル構成は変更されません。
  - リモートネットワークのサービス**IP**アドレスは、各リモートネットワークごとに変更されません。
- Prisma AccessはIPSec終端ノードを割り当て、集約帯域幅モデルへの移行中にリモートネットワークに帯域幅を割り当てます。
- サポートされていない構成の場合、帯域幅割り当てタブは表示されず、移行するためのバナーも表示されません。
- リモートネットワークにQoSがある場合は、移行する前にQoS移行ガイドラインに従ってください。
- 集約帯域幅モデルに移行した後、この変更は永続的なものであり、 Prisma Accessロケーションごとに帯域幅を割り当てるデプロイメントに戻すことはできません。
- 集約帯域幅モデルに移行するには、最低50 Mbpsの利用可能な帯域幅が必要です。
- 移行後にQoSを実装したい場合は、集約帯域幅デプロイメントのためのQoS設定の違いについて学んでください。
- 移行が完了したら、集約帯域幅リモートネットワークオンボーディング手順を使用して、すべての新しいリモートネットワークをオンボードします。
- 移行後、帯域幅使用統計を表示すると、IPSec終端ノードごとに表示されます。
- CLIを使用して移行を行わないでください。移行にはUIのみを使用してください。
- Strata Cloud Manager
- Panorama

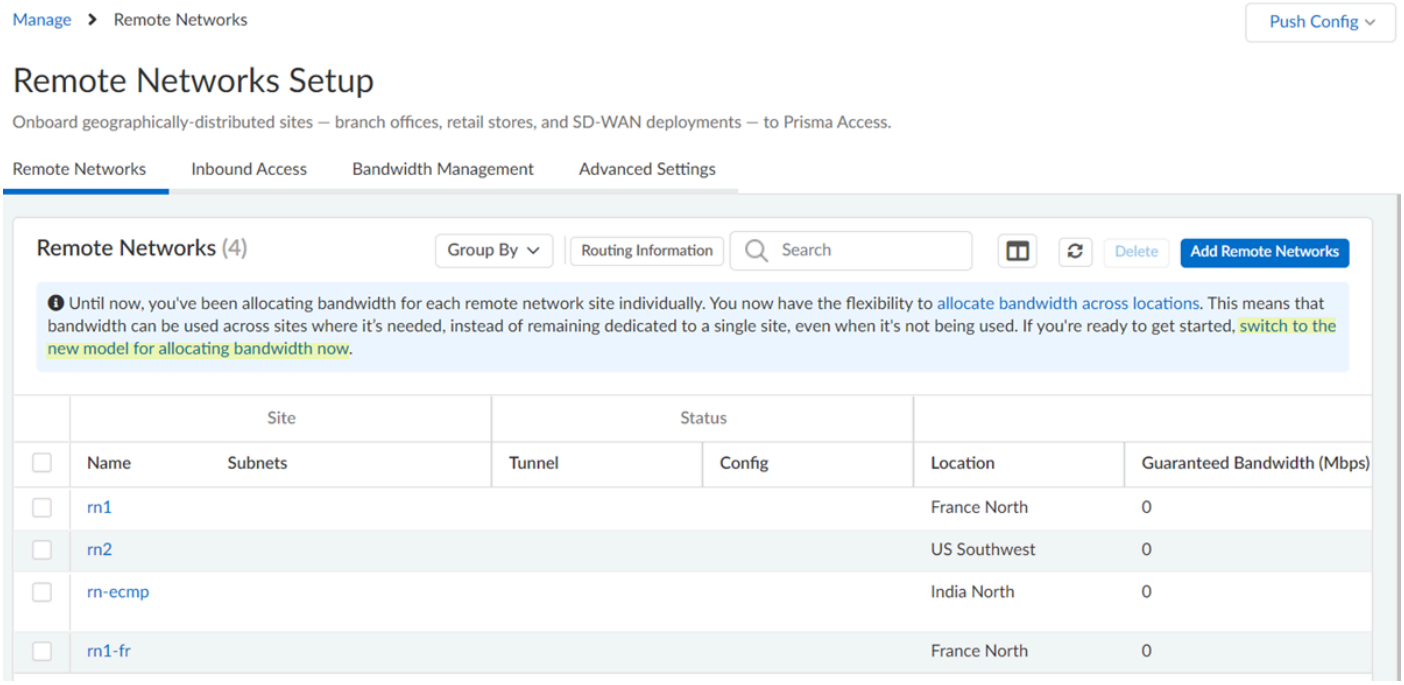
帯域幅管理設定を移行する（Strata Cloud Manager）

ロケーションごとに帯域幅を割り当てるPrisma Accessリモートネットワークのデプロイメントを使用している場合、Prisma Accessでは、コンピュートロケーションごとに帯域幅を割り当てるデプロイメント（集約帯域幅モデル）に移行することで、デプロイメントをより柔軟でスケーラブルなものにすることができます。移行計画チェックリストを確認した後、次の手順に従って集約帯域幅モデルに移行します。

STEP 1 | **[Workflows (ワークフロー)] > [Prisma Accessセットアップ] > [Remote Networks (リモートネットワーク)]**を選択します。

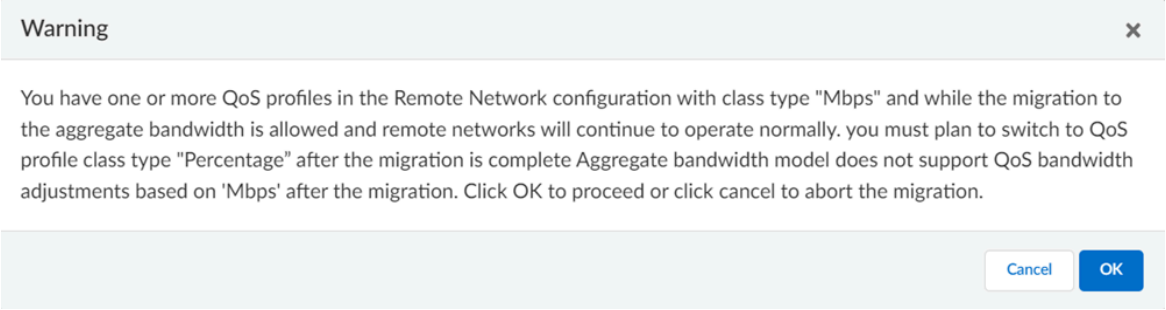
©2025 Palo Alto Networks, Inc.

STEP 2 | 今すぐ帯域幅を割り当てるための新しいモデルに切り替えてください。

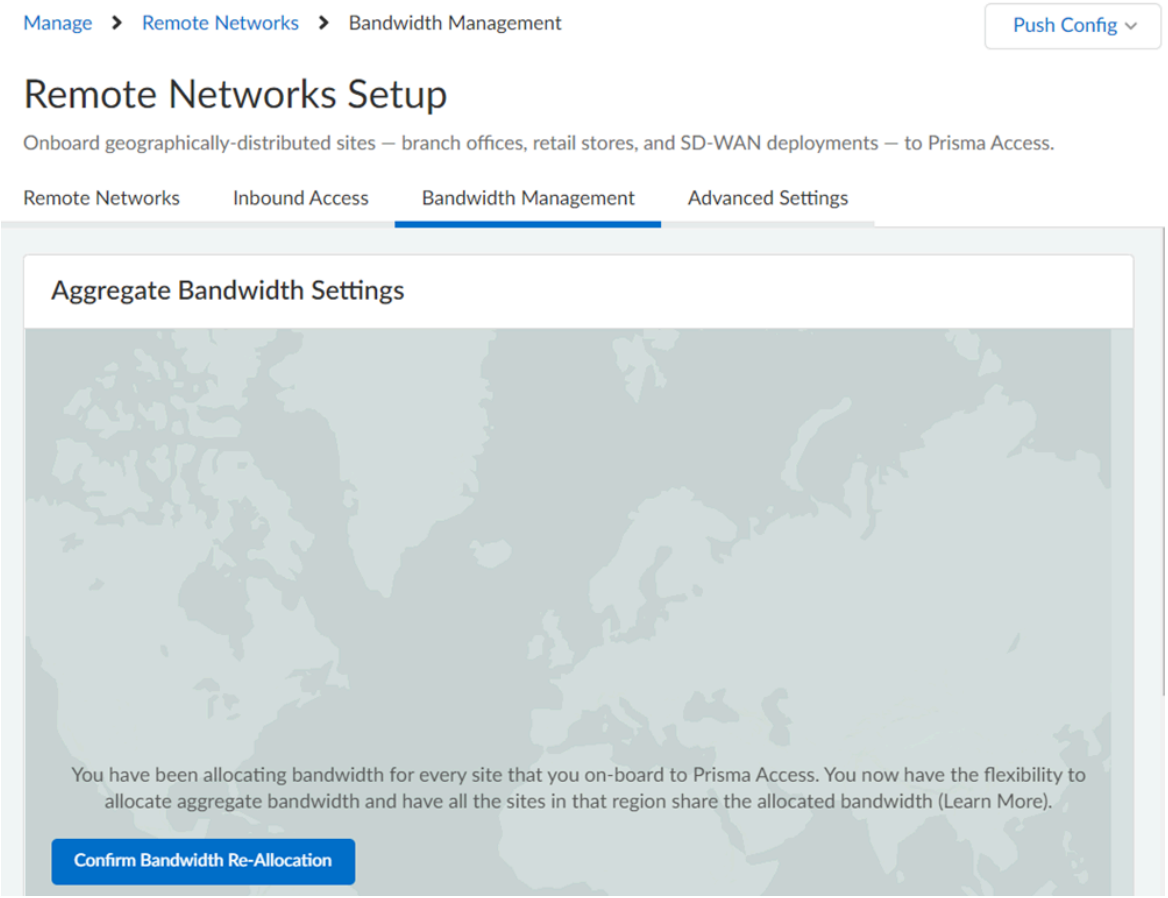


©2025 Palo Alto Networks, Inc.

- クラス帯域幅タイプが***Mbps***の*QoS*プロファイルがある場合、*Prisma Access*は、これらのプロファイルをクラス帯域幅タイプがパーセンテージに変更する必要があることを通知します。



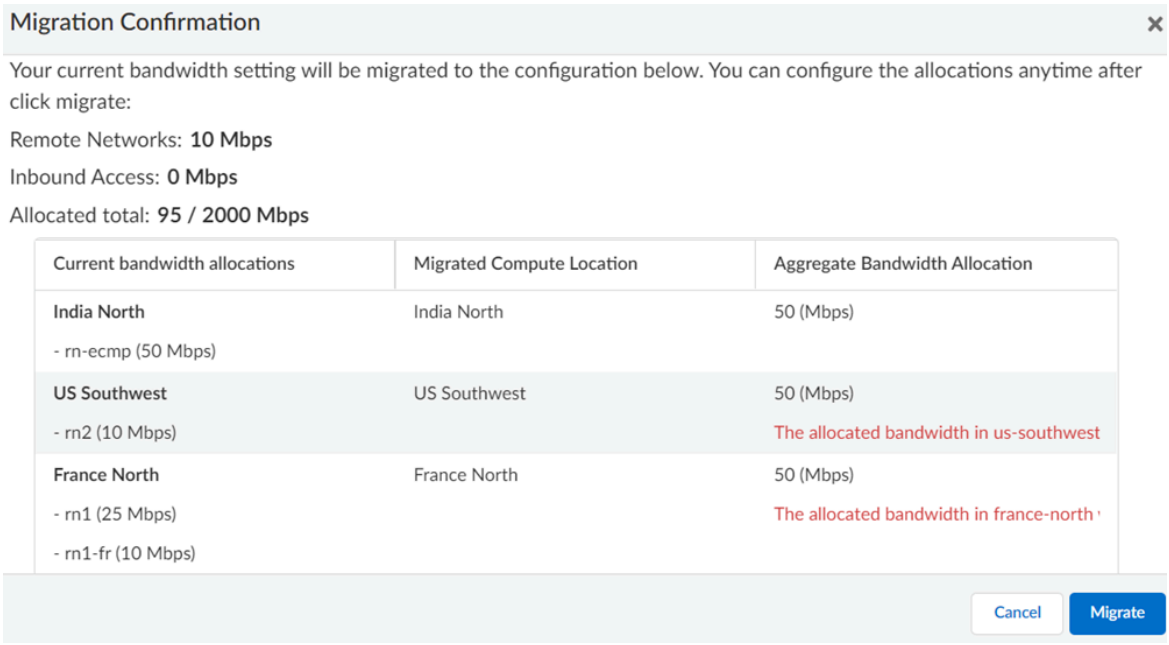
- または、***[Bandwidth Management (***帯域幅管理***)]*** タブで、***[Confirm Bandwidth Re-Allocation (***帯域幅の再割り当ての確認***)]***を選択します。



©2025 Palo Alto Networks, Inc.

STEP 3 | 情報を確認し、表示されるポップアップ ウィンドウで **[Migrate (移行)]** を選択します。

コンピューティングロケーション内のすべてのロケーションの合計帯域幅が*50Mbps*未満の場合、 *Prisma Access*はそのコンピューティング場所の帯域幅が *50 Mbps* に増加します。 *Prisma Access*は、移行プロセス中に帯域幅の増加が必要となる場所を提供します。



集約帯域幅モデルへの移行は永続的であり、元に戻すことはできません。移行する前に、 移行前チェックリストを確認してください。変更を有効にするには、変更を コミットしてプッシュする 必要があります。

Prisma Accessは割り当てられたリモート ネットワーク帯域幅を集約帯域幅モデルに移行します。

STEP 4 | 変更を **Commit and Push**（コミットしてプッシュ）します。

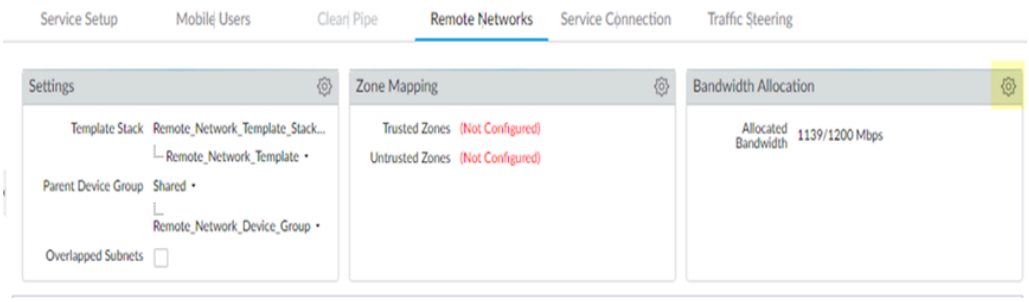
帯域幅管理設定を移行する（Panorama）

ロケーションごとに帯域幅を割り当てるPrisma Accessリモートネットワークのデプロイメントを使用している場合、Prisma Accessでは、コンピュートロケーションごとに帯域幅を割り当てるデプロイメント（集約帯域幅モデル）に移行することで、デプロイメントをより柔軟でスケーラブルなものにすることができます。移行計画チェックリストを確認した後、次の手順に従って集約帯域幅モデルに移行します。

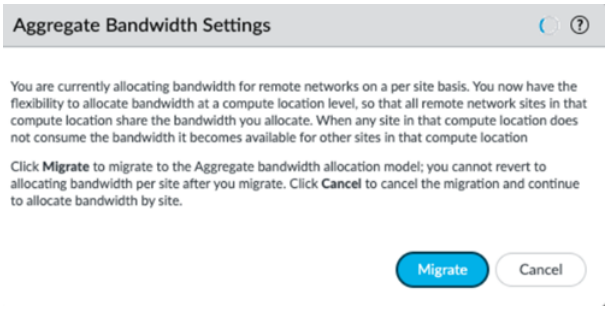
STEP 1 | **[Panorama] > [Cloud Services**（クラウドサービス）**] > [Configuration**（設定）**] > [Remote Networks**（リモートネットワーク）**]**を選択します。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 帯域幅割り当てエリアの歯車アイコンをクリックして、設定を編集します。

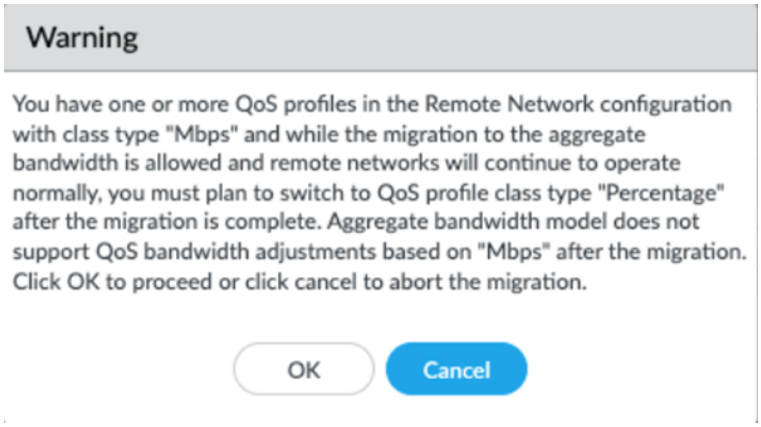


STEP 3 | 表示されるポップアップ ウィンドウで **[移行]** を選択します。



集約帯域幅モデルへの移行は永続的であり、元に戻すことはできません。移行する前に、 移行前チェックリストを確認してください。変更を有効にするには、変更を コミットしてプッシュする 必要があります。

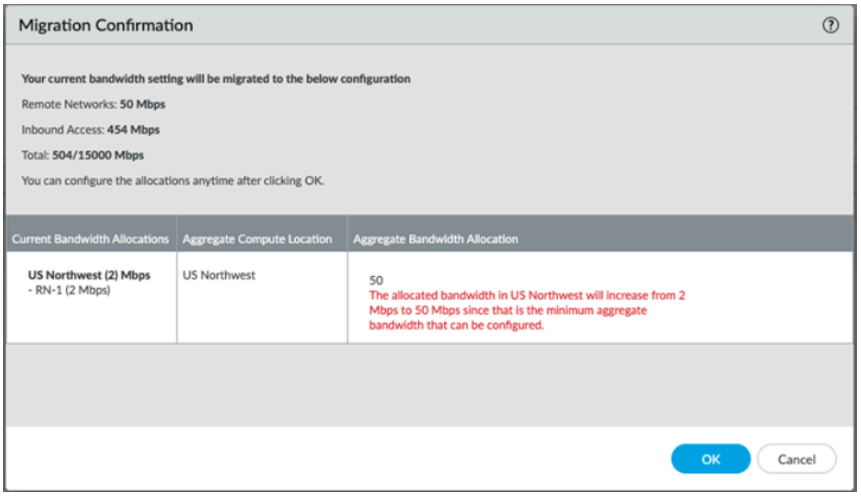
クラス帯域幅タイプが***Mbps***の*QoS*プロファイルがある場合、*Prisma Access*は、これらのプロファイルをクラス帯域幅タ イプのパーセンテージに変更する必要があることを通知します。



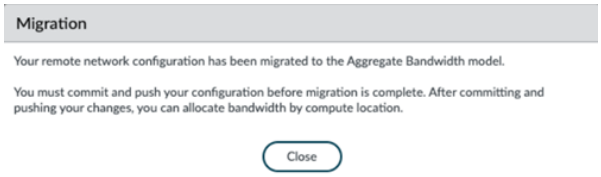
 ©2025 Palo Alto Networks, Inc.

STEP 4 | 移行確認 ウィンドウで情報を確認し、**[OK]**をクリックします。

コンピューティングロケーション内のすべてのロケーションの合計帯域幅が*50Mbps*未満の場合、 *Prisma Access*はそのコンピューティング場所の帯域幅が *50 Mbps* に増加します。 *Prisma Access*は、移行プロセス中に帯域幅の増加が必要となる場所を提供します。



Prisma Accessは割り当てられたリモート ネットワーク帯域幅を集約帯域幅モデルに移行し、確認ウィンドウを表示します。ウィンドウを閉じるには、**[Close (閉じる)]** をクリックします。



STEP 5 | 変更を **Commit and Push**（コミットしてプッシュ）します。

©2025 Palo Alto Networks, Inc.

リモートネットワークのオンボーディング

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

リモートネットワークの計画が完了したら、構成プロセスを開始できます。これには、リモート ネットワークのオンボーディング、リモート・ネットワーク・サイトのPrisma Accessへの接続、リモート ネットワークのルーティングとQoSの有効化などが含まれます。Prisma Access for netowrksを使って保護する各リモートネットワークに対して、必要なポリシー設定をPrisma Accessにプッシュし、各リモートネットワークをオンボーディングする必要があります。そうすることで、IPSecトンネル経由でリモートサイトからPrisma Accessへのトラフィック送信を開始できるようになります。次の手順のいずれかを使用して、帯域幅の割り当てタイプに応じてリモートネットワークをオンボードします:

リモートネットワークのオンボーディング方法について説明します。

- Strata Cloud Manager
- Panorama

リモートネットワークのオンボーディング (Strata Cloud Manager)

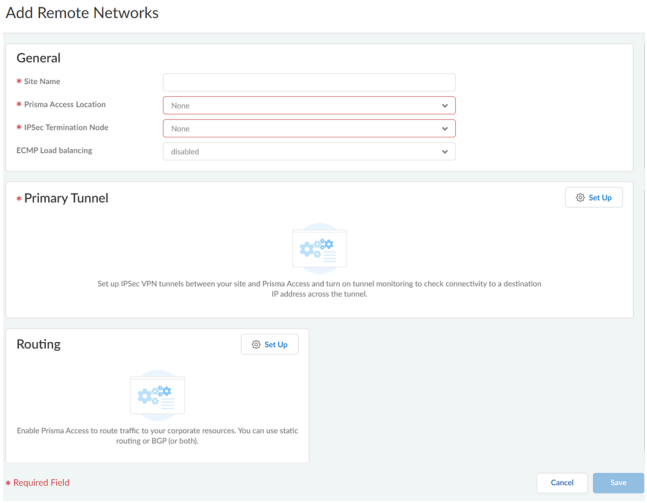
Prisma Accessに新しいリモート ネットワーク サイトを追加する方法は次のとおりです。まず、場所を指定し、接続に割り当てる帯域幅の量を定義します。

STEP 1 | Prisma Access (Managed by Strata Cloud Manager)を起動します。

STEP 2 | リモート ネットワークを展開する場所に帯域幅が割り当てられていることを確認します。リモート ネットワークの計画チェックリストを参照してください。

©2025 Palo Alto Networks, Inc.

STEP 3 | **[Workflows (ワークフロー)] > [Prisma AccessのSetup (セットアップ)] > [Remote Networks (リモート ネットワーク)] > [Add Remote Networks (リモートネットワークの追加)]**へ移動します。



STEP 4 | リモート ネットワークにわかりやすいサイト名を付けます。

STEP 5 | サイトが所在する**Region (地域)**と、最も近いPrisma Access**Location(ロケーション)**を選択します。

STEP 6 | (ダイナミック ルーティングに BGP を使用する予定の場合のみ) リモート ネットワーク サイトが最大 4 つのIPSecトンネルを使用できるように、**ECMP Load Balancing (ECMP ロード バランシング)** を有効にします。

ECMPロード バランシングにはBGPが必要です。QoSとスタティック ルートはサポートされていません。

ECMPを有効にすると、リモート ネットワーク トラフィックは、構成したトンネルを介して負荷分散されます。

STEP 7 | 詳細設定を構成します。

- (任意) **Static Entries (スタティックエントリ)**を使用して、FQDN を特定のIPアドレスに解決します。

  この機能は、組織内にゲスト インターネット サービスがあり、ゲストが検索エンジンを安全に使用して、会社のポリシーに違反する可能性のある不適切または不快なコンテンツ

 ©2025 Palo Alto Networks, Inc.

を検索しないようにしたい場合に役立ちます。これを行うには、スタティックエントリルールの一意の 名前 、**FQDN**、およびFQDN 要求を送信するIPアドレスを入力します。



- Prisma AccessにDNSリクエストをプロキシさせたい場合は、**UDP**クエリ再試行（クエリを再試行する間隔（秒）、および再試行の試行回数（秒））の値を設定する。

STEP 8 | リモート ネットワーク サイトをPrisma Accessに接続するためのIPSec VPNトンネルを作成するリモート ネットワーク サイトをPrisma Accessに接続する。

STEP 9 | スタティック ルーティングを設定します。

1. 本社またはデータ センターとの間でトラフィックをルーティングするためのスタティック ルートの場合は、ブランチで保護するIPサブネットまたはIPアドレスを追加します 。

   HQまたはデータセンター ネットワーク上のIPサブネットに変更を加えた場合は、スタティック ルートを手動で更新する必要があります。

STEP 10 | ダイナミック ルーティングを構成します。

1. HQまたはデータセンターのサブネットをアドバタイズするためのダイナミック ルーティングの場合は、 ダイナミック ルーティング用に**BGP**を有効にします。
2. (任意)**MRAI**タイマー 値を選択します。

   BGPルーティングでは、ネットワーク内のBGPルーティング収束を調整するために使用できる 最小ルート広告間隔 *(MRAI)*と呼ばれるタイマーが提供されます。MRAIは宛先ごとに更新のレートを制限するように機能し、BGPルータは同じプレフィックスのアドバタイズメントを送信する前に、少なくとも設定されたMRAI時間待機します。数値が小さいほど収束時間は速くなりますが、ネットワーク内に作成される広告は多くなります。数値が大きいほど、送信できる広告の数は減りますが、ルーティングの収束も遅くなる可能性があります。ルーティング収束の高速化と広告の削減の間の最適なバランスを実現するために、ネットワークに配置する数を決定します。

   MRAIの範囲を1 ～ 600秒に設定します。デフォルト値は30秒です。
3. 顧客構内装置（CPE）へのBGPを介したモバイル ユーザIPサブネットのアドバタイズ数を減らすには、**[Summarize Mobile User Routes before advertising**（アドバタイズ前にモバイルユーザールートを要約する）]を選択して、アドバタイズする前にサブネットを要約するようにPrisma Accessを指定します。

   デフォルトでPrisma Accessは、モバイルユーザーのIPアドレスプールを、/24サブネットのブロックでアドバタイズします。それを要約すると、Prisma Accessによって指定したサブネットに基づいてプールがアドバタイズされます。たとえば、Prisma Accessは、パブリックユーザーのモバイルIPプールを、アドバタイズ前に10.8.1.0/24、10.8.2.0/24、10.8.3.0/24などのサブネットに分割するのではな

 ©2025 Palo Alto Networks, Inc.

く、/20のサブネットを使用して10.8.0.0/20のプールをアドバタイズします。これらのアドバタイズを要約することで、CPEルーティングテーブルに保存されるルート数を削減できる可能性があります。たとえば、限定された数のルートを受け付けるクラウドVPNゲートウェイ（仮想プライベートゲートウェイ（VGW）またはトランジットゲートウェイ（TGW））で、IPプールの要約を使用することができます。

4. （任意） Prisma AccesseBGPを使用してリモート ネットワークのデフォルト ルート アドバタイズメントを開始するには、**[Advertise the Default Route (**デフォルト ルートのアドバタイズ**)]**を選択します。ネットワークに、BGPがアドバタイズしている他のデフォルトルートが存在していないことを確認してください。そうしないと、ネットワークにルーティング上の問題が発生する可能性があります。
5. (任意) セカンダリWANを設定していて、セカンダリ (バックアップ) BGPピアのピア アドレスを変更する必要がある場合は、**[Use different BGP Peer for Secondary Tunnel (**セカンダリ トンネルに別の**BGP**ピアを使用する**)]** を選択し、一意のピアを入力し、必要に応じてセカンダリWANのローカルIPアドレスを入力します。
6. （任意） Prisma AccessがHQまたはデータセンターにルートを転送しないようにするには、**[Do Not Export Routes (**ルートをエクスポートしない**)]**を選択します。

   デフォルトで、Prisma Accessは、ローカルルート、および他のサービス接続、リモートネットワーク、およびモバイルユーザーサブネットから受信するすべてのプレフィックスを含め、すべてのBGPルーティング情報をアドバタイズします。Prisma AccessによるBGPアドバタイズメントの送信を防止しながら、受信したBGP情報を使って、他のBGPネイバーからルートを学習するには、このチェック ボックスを選択します。

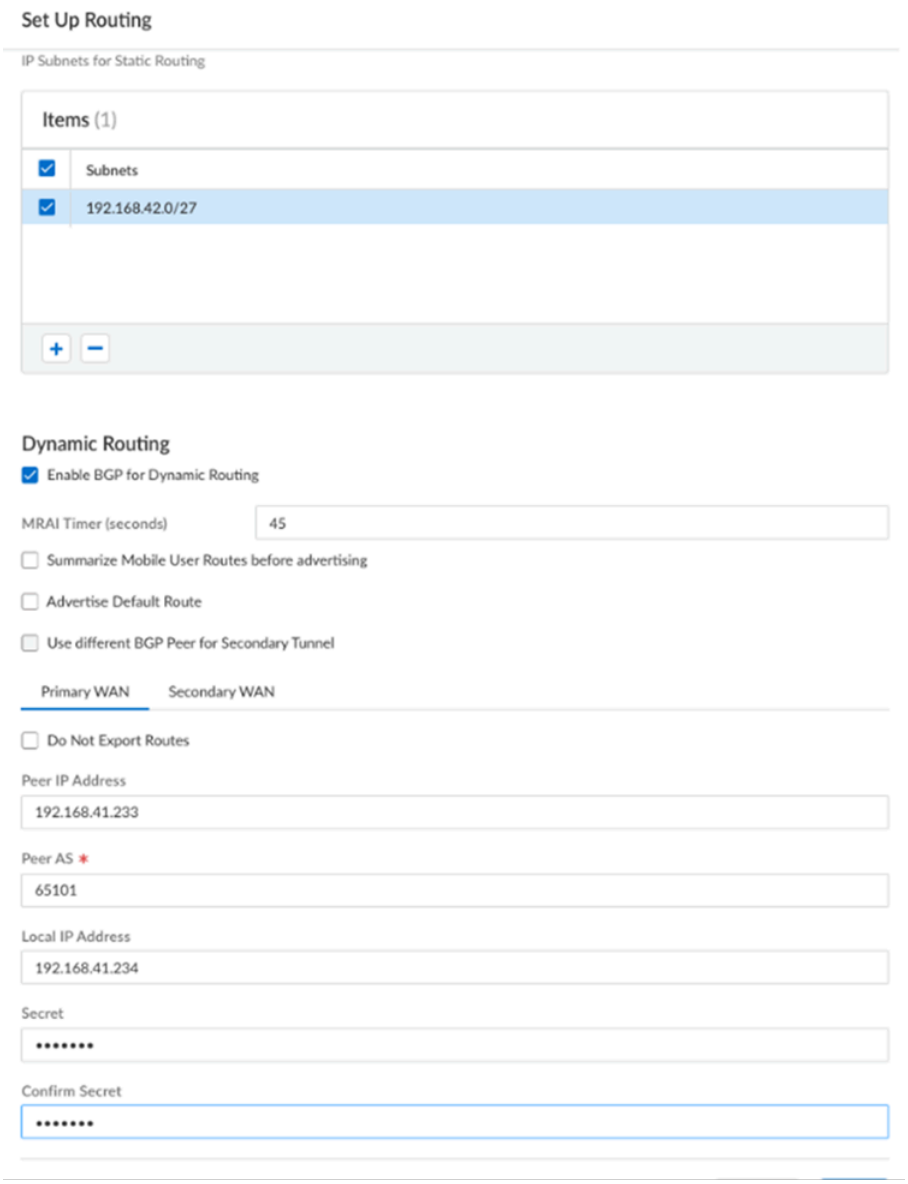
   > *Prisma Access*は*BGP*アドバタイズを送信しないため、このオプションを選択した場合は、*Prisma Access*に戻るルートを確立するために、オンプレミス機器にスタティック ルートを設定する必要があります。
7. HQまたはデータセンター ネットワーク上のeBGPルーターのルーターIDとして割り当てられた ピア**IP**アドレス を入力します。
8. ネットワークの自律システム (AS) である **Peer AS**を入力します。

   RFC 6996準拠のBGPプライベートAS番号を使用します。
9. が**BGP**のローカル**IP**アドレスとして使用するローカルIPアドレスPrisma Accessを入力します。

   ローカル アドレスは、BGPピアリングを成功させるためにHQまたはデータセンターデバイスで必要な場合にのみ必要です。指定するIPアドレスは、インフラサブネットまたはリモートネットワーク内のサブネットのIPアドレスと、競合またはオーバーラップしていないことを確認してください。
10. BGP ピア通信を認証するためのシークレットパスワードを入力します。

 ©2025 Palo Alto Networks, Inc.

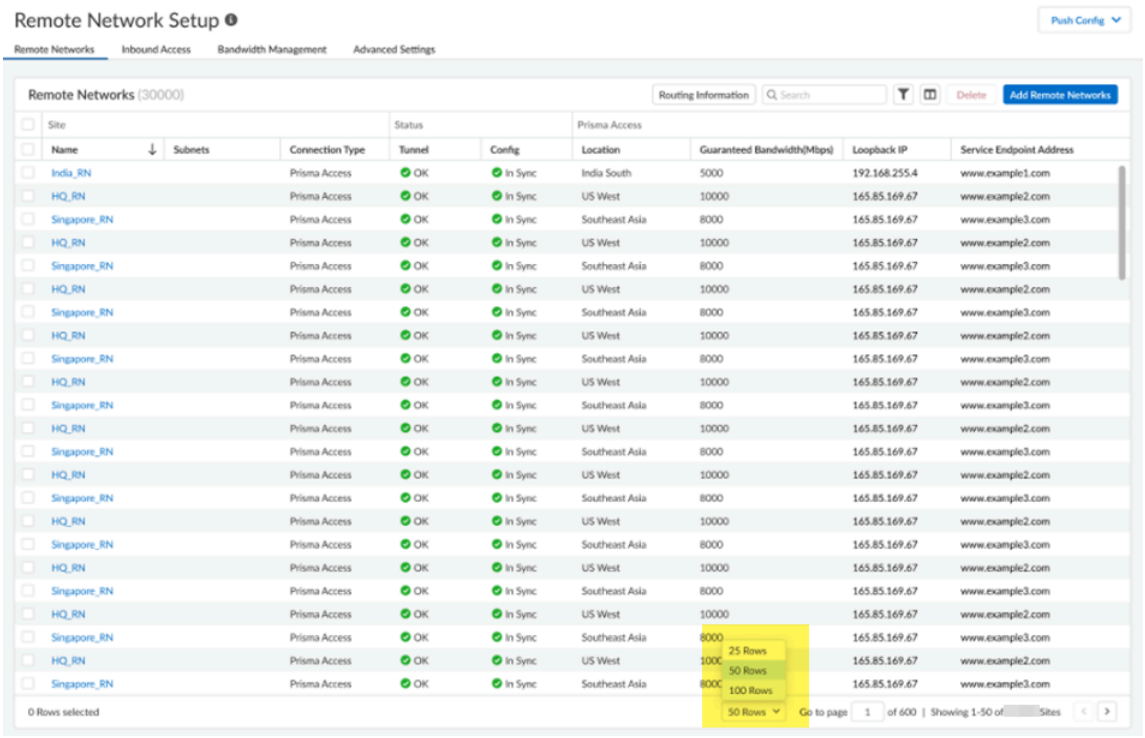
11. [シークレットの確認]を選択します。



*Prisma Access 5.2*以降、*Prisma Access*のデプロイメントでは、テナントごとに最大*25,000*のリモートネットワークと*50,000*の*IKE*ゲートウェイを搭載できます。この機能強化に対応するために、*Strata Cloud Manager Web*インターフェースに以下の変更が加えられました。

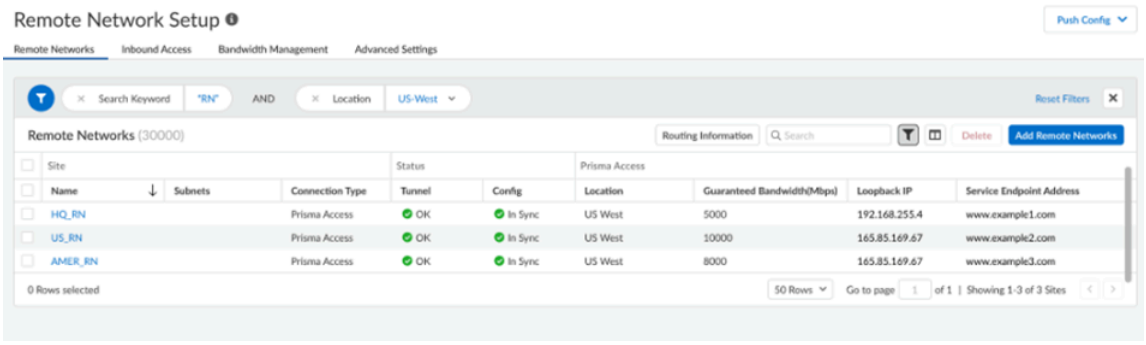
- ページ付けが有効になっており、特定のページに表示する行数を選択できます。

©2025 Palo Alto Networks, Inc.

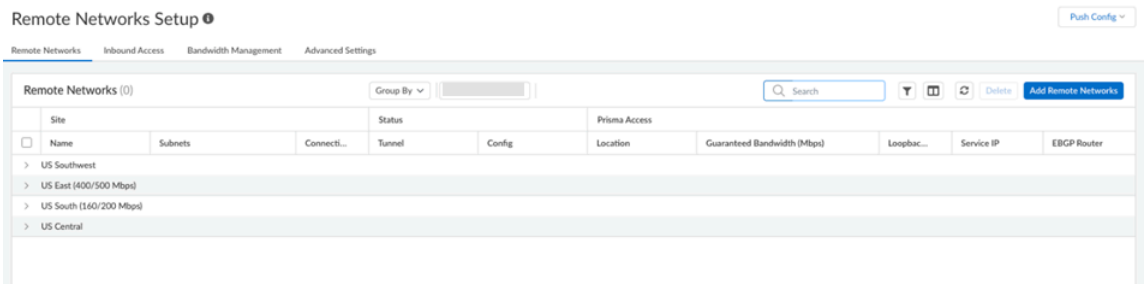


- リモート ネットワークではフィルタリングが有効になっています。

  フィルタリングを適用すると、結果の出力を名前で並べ替えることができます。



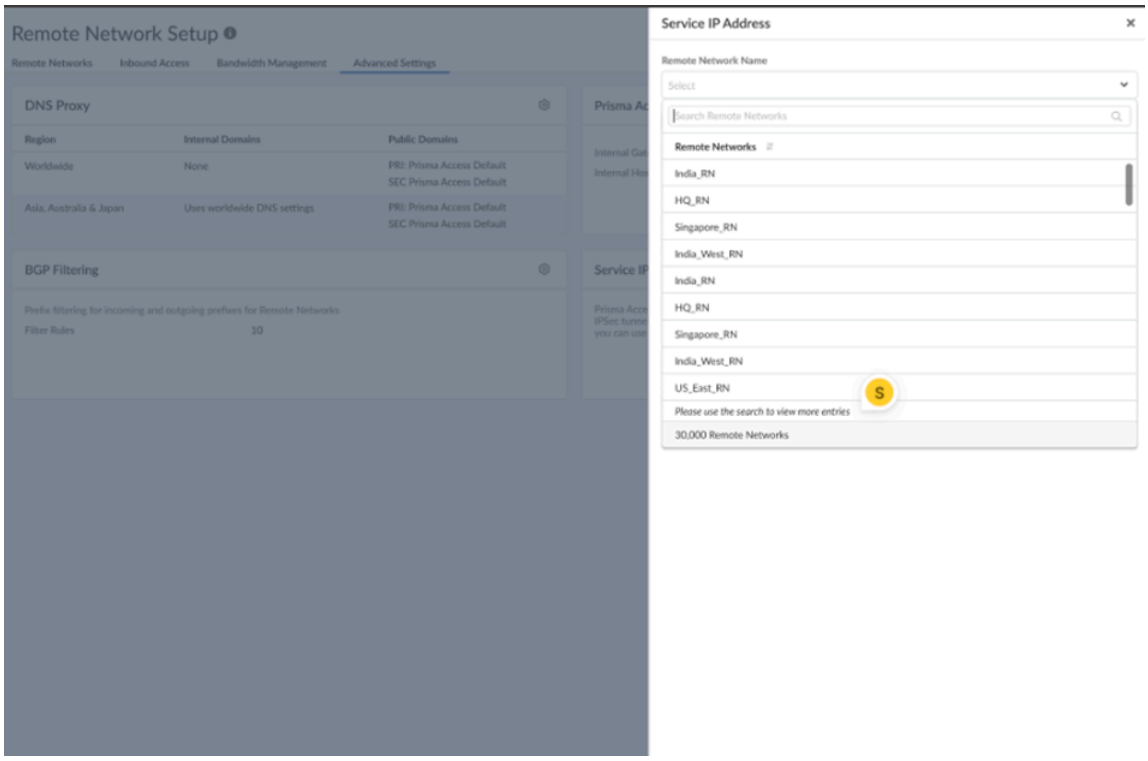
- **[Group By (**グループ化**)]**フィールドが新しく追加されます。**[Compute Location (**コンピューティング場所**)]**によるグループ化を選択した場合、すべてのグループが表示されますが、折りたたまれ、選択したページ サイズがグループに適用されます。コンピューティング場所を選択して拡張すると、選択したページ サイズに基づいて行が表示されます。



©2025 Palo Alto Networks, Inc.

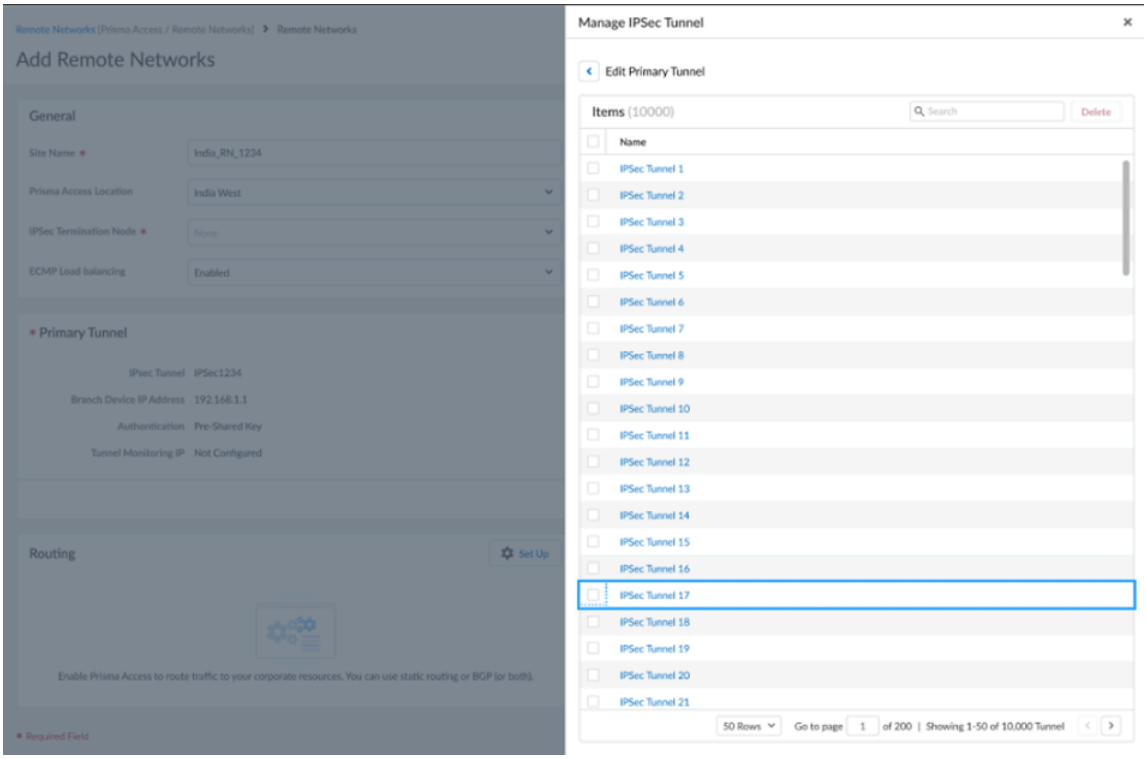
- リモート ネットワークがドロップダウンに表示される場合、Webインターフェースには最初の500項目が表示されます。テキスト ボックスに入力すると、リスト内で目的のリモート ネットワークを見つけることができます。

  さらに、リモート ネットワークの合計数も表示されます。

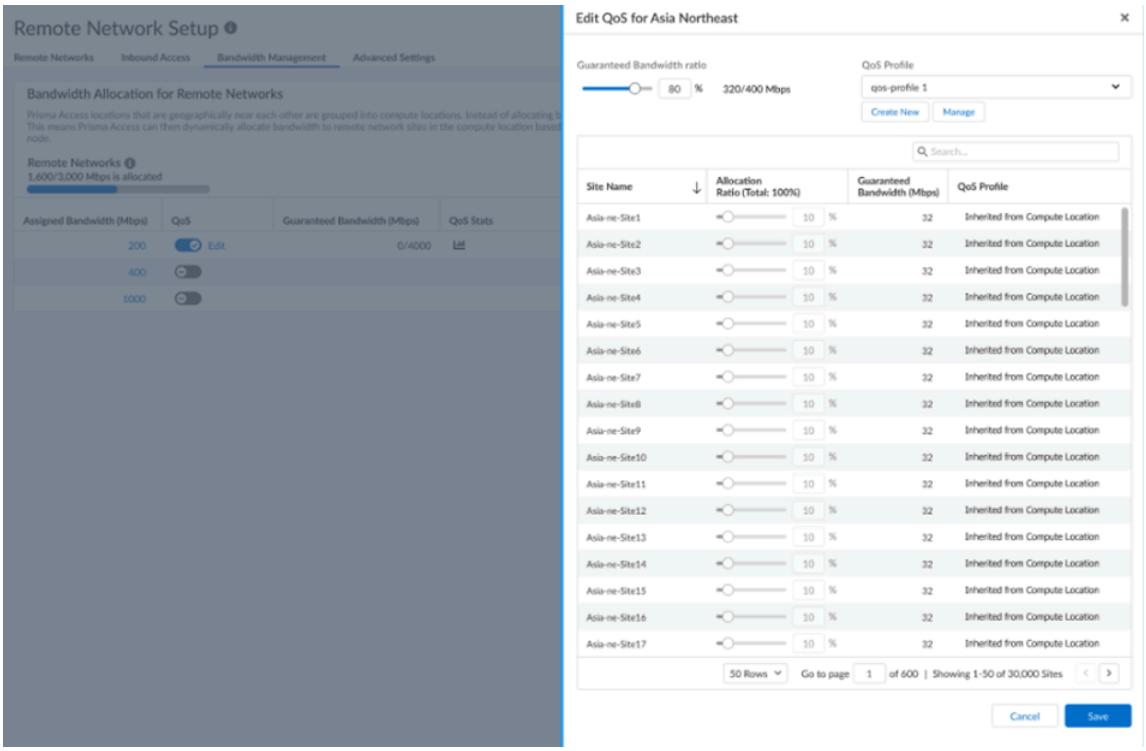


 ©2025 Palo Alto Networks, Inc.

- 以下の追加ページにはページ付けが適用されています。
  - IPSecトンネル

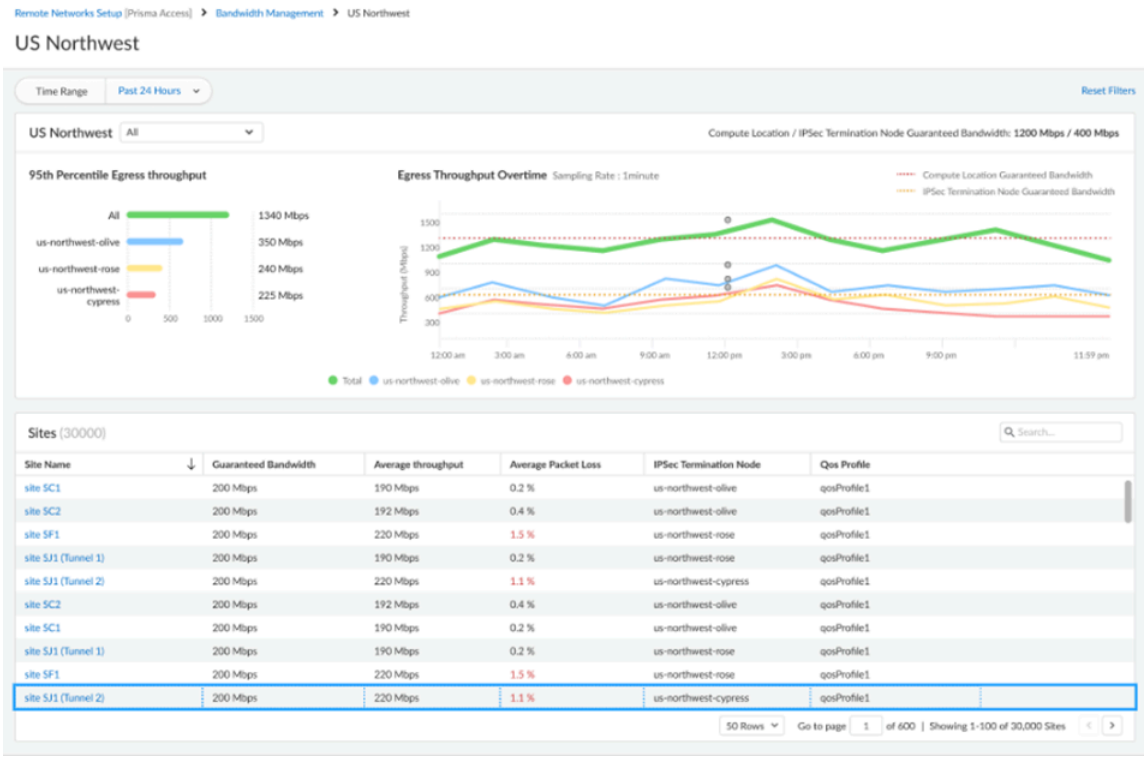


  - QoS:

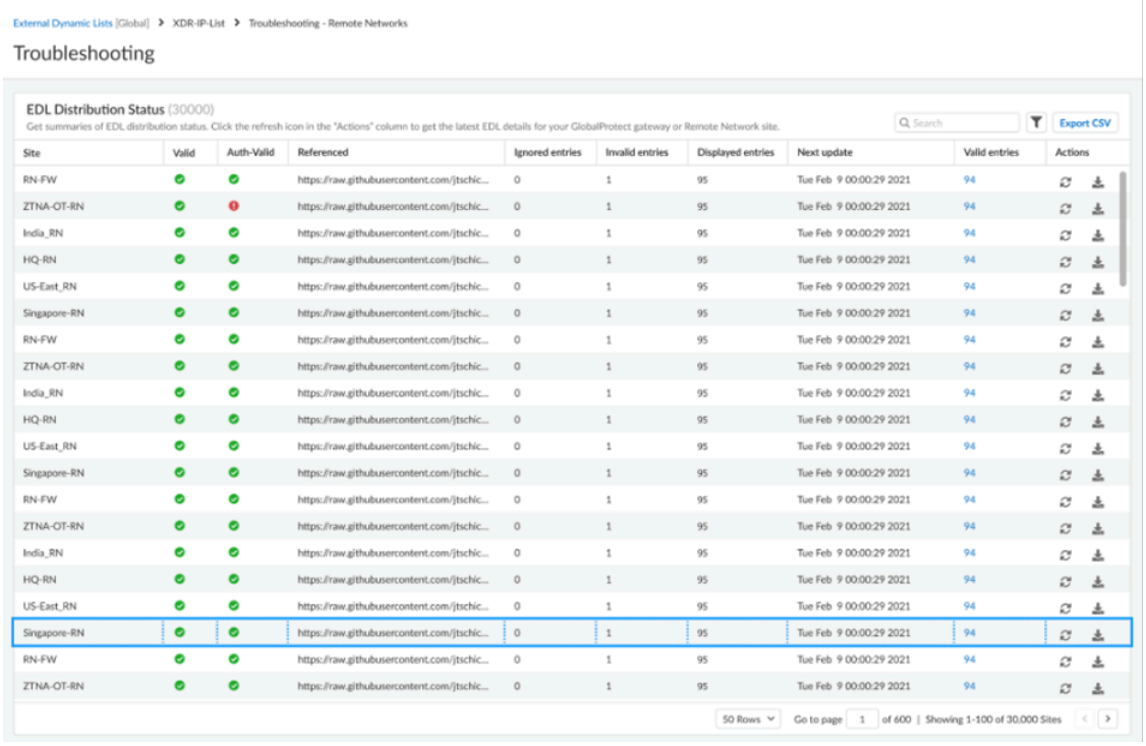


  - QoS統計情報:

 ©2025 Palo Alto Networks, Inc.



- トラブルシューティング - 外部動的リストの下にあるリモート ネットワーク:



リモートネットワークのオンボーディング (Panorama)

コンピュート ロケーションごとに帯域幅を割り当てるPrisma Accessリモートネットワーク デプロイメントを構成す るには、以下の手順を実行します。

 ©2025 Palo Alto Networks, Inc.

多数のリモートネットワーク（最大*1,000*）をオンボードする必要がある場合は、次の手順でリモートネットワークをオンボードし、リモートネットワーク構成をCSVファイルにエクスポートし、オンボードする他のリモートネットワークを*CSV*ファイルに追加し、*CSV*ファイルをインポートして*Prisma Access*に構成を保存します。

STEP 1 | **Panorama** > **Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Remote Networks**（リモートネットワーク）の順に選択して、**Settings**（設定）エリアの歯車型アイコンをクリックして設定を編集します。

1. Templates（テンプレート）セクションで、ネットワーク用のPrisma Accessにプッシュする設定を含んでいるテンプレートを**Add**（追加）します。たとえば、ゾーン設定、またはIPSecトンネル、IKEゲートウェイ、または暗号プロファイル設定を含んでいる既存のテンプレートがある場合、それを事前定義されたRemote_Network_Template_Stackに追加して、オンボーディングプロセスを簡素化することができます。

   スタックに複数のテンプレートを**Add**（追加）して、次に**Move Up**（上に移動）および**Move Down**（下に移動）を使って、それらを適切な順序に変更することができます。Panoramaはスタックの上から下へと評価していくため、スタック内で上にあるテンプレートの設定が、同じ設定が行われている下位のテンプレートよりも優先されます。そのため、この作業が重要になってきます。デフォルトのテンプレートをスタックの最上位から移動することはできません。

   プラグインからスタックに既存のテンプレートを追加できますが、プラグインから新しいテンプレートを作成することはできません。代わりに、このワークフローを使って新しいテンプレートを追加してください。

2. リモートネットワーク用のPrisma Accessの**Parent Device Group**（親デバイスグループ）を選択します。既存のデバイスグループを選択するか、または**Shared**（共有）を使用できます。

   セキュリティポリシー、セキュリティプロファイル、および他のポリシーオブジェクト（アプリケーショングループとオブジェクト、アドレスグループなど）、HIPオブジェクトとプロファイル、および認証ポリシーを含め、ネットワーク用のPrisma Accessがここで指定するデバイスグループ階層を使って、リモートネットワークユーザーに一貫したポリシーを適用するために必要な、すべての設定をプッシュします。

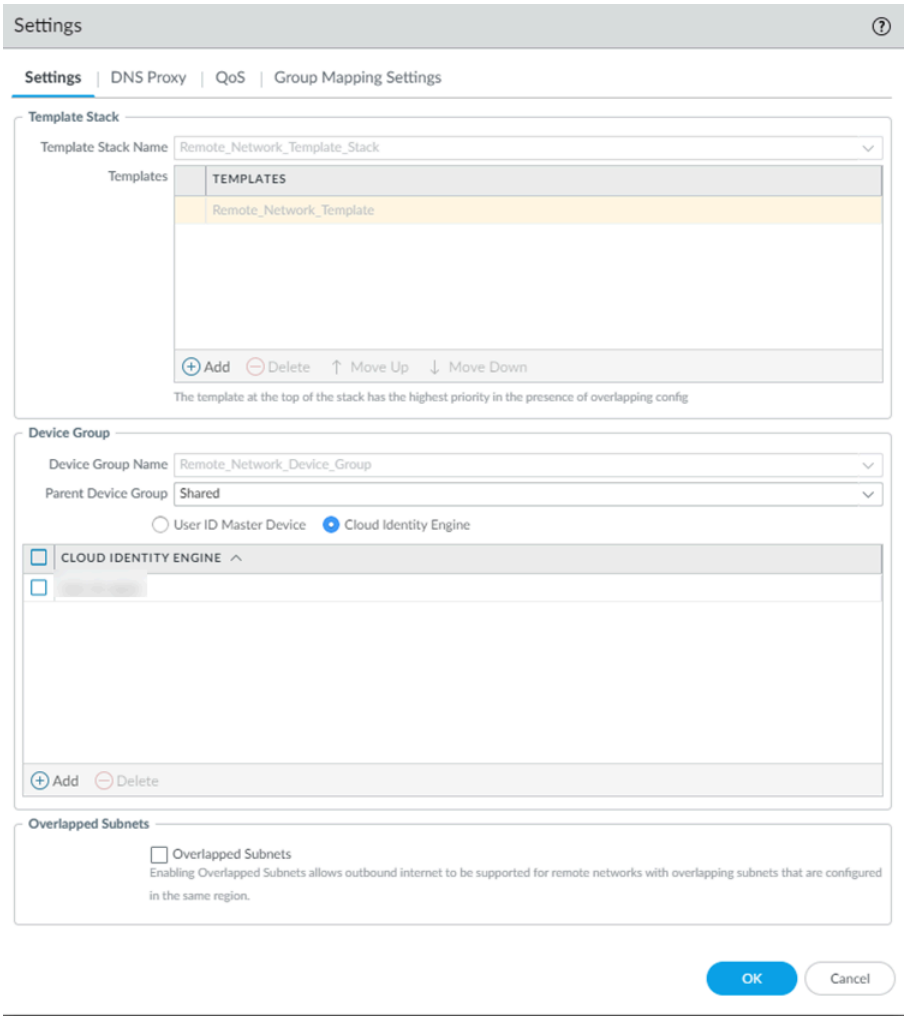
   まだ、リモートネットワークにプッシュする、すべてのポリシーを定義する必要はありません。代わりに、リモートサイトをオンボーディングするための設定を行います。次に元に戻って、リモートネットワークに一貫したポリシーをプッシュするために、完全な設定を行った、テンプレートとデバイスグループを追加します。

3. (任意) 次世代ファイアウォールをマスター デバイスとして構成した場合、またはCloud Identity Engineプロファイルを追加して、セキュリティ ポリシーでユーザーとグループの情報を選択できるようにした場合は、**User-ID** マスター デバイス または **Cloud Identity Engine**を選択し、作成したマスター デバイスまたはCloud Identity Engineプロファイルのいずれかを選択します。

©2025 Palo Alto Networks, Inc.

4. オーバーラップしたサブネットを持つリモートネットワークを設定する場合は、**Overlapped Subnets**（オーバーラップしたサブネット）チェックボックスを選択して、それらのロケーションのアウトバウンドインターネットアクセスを有効にします。

   オーバーラップしたサブネットを持つリモートネットワークロケーションを設定するといくつかの制限事項が発生しますが、状況によっては我慢できることもあります（たとえば、小売店舗ロケーションにゲスト用ネットワークを追加する場合）。



STEP 2 | （任意）リモートネットワークの**DNS Proxy**（**DNS**プロキシ）設定を行います。

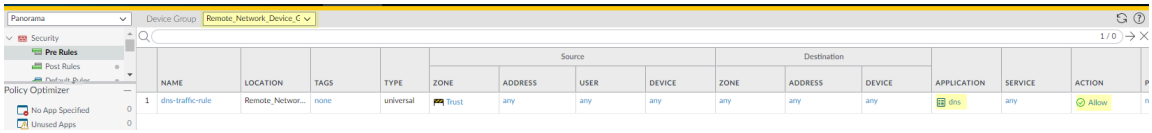
Prisma Accessでは、組織内部のドメインと外部のドメインの両方のドメインを解決する、DNSサーバーを指定することができます。指定しなかった場合、Prisma Accessはリモートネットワーク用のDNSリクエストのプロキシを行いません。

1. **Remote_Network_Device_Group**デバイスグループで、**Policies**（ポリシー） > **Security**（セキュリティ）を選択して、**Add**（追加）を選択し、DNSトラフィッ

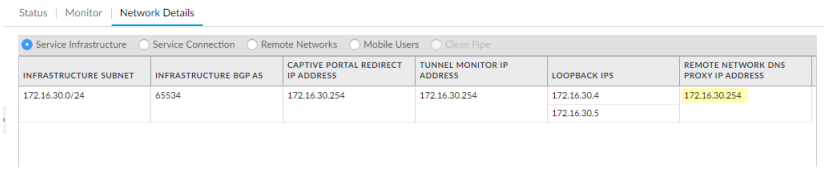
 ©2025 Palo Alto Networks, Inc.

クを許可するために **DNS**の**Application**（アプリケーション）および**Allow**（許可）の**Action**（アクション）を持つセキュリティポリシールールを追加します。

DNSトラフィックを許可するセキュリティポリシールールがない場合、DNS解決は行われません。



2. リモートネットワークからのDNSリクエストのプロキシを行うようにPrisma Accessを設定した場合、Prisma Accessの**Remote Network DNS Proxy IP Address**（リモートネットワーク**DNS**プロキシ**IP**アドレス）をプライマリDNSサーバーとして、ご自分のDNSサーバーをセカンダリDNSサーバーとして使用するように、そのネットワーク上のすべてのエンドポイントのDNS設定を更新してください。このDNSプロキシIPは、**Panorama** > **Cloud Services**（クラウドサービス） > **Status**（ステータス） > **Network Details**（ネットワーク詳細） > **Service Infrastructure**（サービスインフラ）から入手できます。



3. **Add**（追加）を選択して、1つまたは複数の**DNS**プロキシ設定を追加して、次の値を入力します。

   - ウィンドウの上部にあるドロップダウンから 地域 を選択します。

     DNS 設定をグローバルに適用するには **[Worldwide (全世界地域)]** を選択し、特定のシアターを選択するか、ロケーショングループ (劇場よりも小さい場所のグループ) ごとに設定を選択します。複数の設定を追加すると、最初に場所グループの設定が使用され、次に劇場の設定、最後に全世界の設定が使用されます。 Prisma Accessはリストの上から下に向かってルールを評価します。

   - 内部ドメインのDNS 設定を構成するルールを1つ以上追加します。

     - ルールの一意のルール名を入力します。
     - 内部DNSサーバーに、指定したドメインのみを解決させる場合は、**Domain List**（ドメインリスト）に解決するドメインを入力します。ドメインの前にアスタリスクを指定します (例:*.acme.com)。最大1,024個のドメインエントリを指定することができます。
     - 内部ドメインにアクセスできるカスタム**DNS**サーバーがある場合は、プライマリ**DNS**サーバーとセカンダリ**DNS**サーバーのIPアドレスを指定するか、**[Use Cloud Default (クラウドデフォルトを使用)]**を選択してデフォルトのPrisma AccessDNSサーバーを使用します。

 ©2025 Palo Alto Networks, Inc.

- パブリックドメインのDNS 設定を指定します。
  - クラウドのデフォルトを使用する- デフォルトを使用するPrisma AccessDNS サーバー。
  - **Same as Internal Domains (**内部ドメインと同じ**)**-内部ドメインの解決に使用するのと同じサーバーを使用する。このオプションを選択すると、パブリックドメインの解決に使用されるDNSサーバーは、[内部ドメイン]セクションの最初のルールに設定されたサーバーと同じになります。
  - **Custom DNS server (**カスタム**DNS**サーバー**)**- パブリック (外部) ドメインにアクセスできるDNSサーバーがある場合は、そのフィールドにプライマリDNSサーバーアドレスを入力します。

  (任意) **DNS**サフィックスを追加して、解決できない非修飾ホスト名が入力されたときにクライアントがローカルで使用する必要があるサフィックスを指定できます (例:acme.local)。ドメイン サフィックスの前にワイルドカード (*) 文字を入力しないでください (例: acme.com)。複数のサフィックスを追加できます。
- Prisma AccessにDNSリクエストをプロキシさせたい場合は、UDPクエリに使用する構成値（クエリ を再試行する間隔（秒）と再試行回数）を設定します。

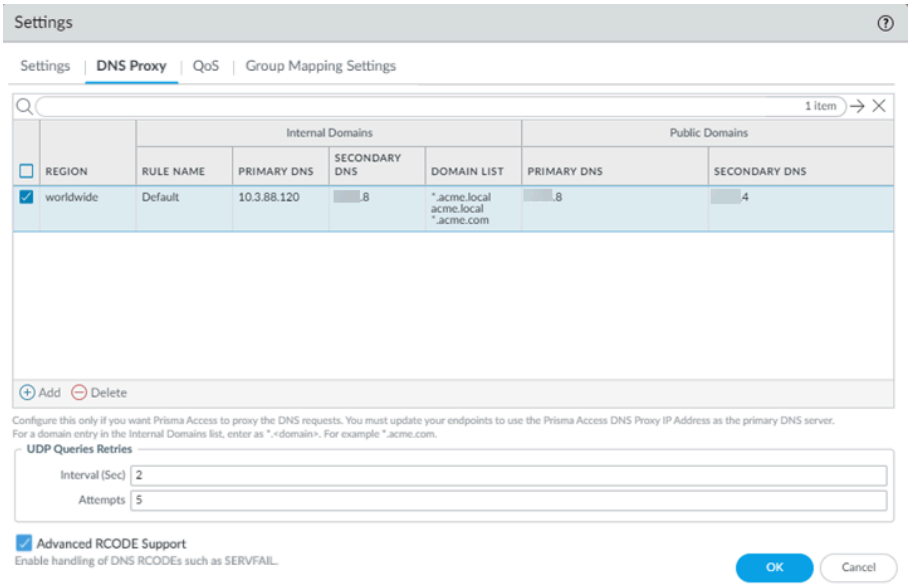
  Prisma Accessに GlobalProtect ユーザーのDNS要求をプロキシさせたい場合は、プライマリDNSサーバとしてリモートネットワーク**DNS**プロキシ**IP**アドレスを使用するようにエンドポイントを更新する必要があります (**[Panorama] > [Cloud Services] >** [ステータス] **>** [ネットワーク詳細] **>** [サービス インフラストラクチャ])。

4. (任意) 高度なRCODEサポートを選択すると、RCODE 2 (SERVFAIL) およびRCODE 5 (REFUSED) のDNS戻りコードを受信した場合にプライマリDNSサーバーがセカンダリDNSサーバーにフェイルオーバーできるようになります。

   SERVFAILのDNS応答コードはプライマリDNSサーバとの通信エラーを指し、REFUSEDのDNS応答コードはプライマリDNSサーバが要求された情報の提供を

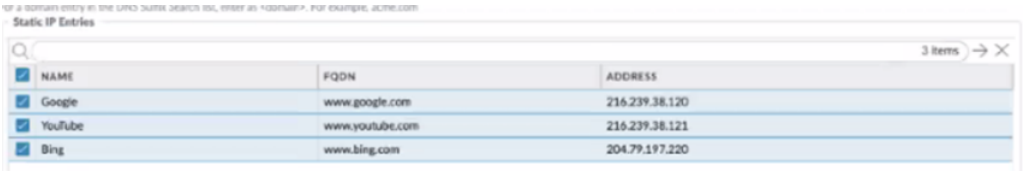
 ©2025 Palo Alto Networks, Inc.

拒否したことを意味します。どちらの場合も、サービスはセカンダリDNSサーバーにフェイルオーバーします。



5. (任意) スタティックIPエントリを使用して、FQDNを特定のIPアドレスに解決します。

   この機能は、組織内にゲスト インターネット サービスがあり、ゲストが検索エンジンを安全に使用して、会社のポリシーに違反する可能性のある不適切または不快なコンテンツを検索しないようにしたい場合に役立ちます。これを行うには、スタティックエントリ ルールの一意の 名前 、**FQDN**、およびFQDN 要求を送信するIPアドレスを入力します。



STEP 3 | (任意) リモート ネットワーク デプロイメントの**QoS**を有効にし、**QoS**プロファイル、 保証帯域幅比率、 保証帯域幅用に予約されている帯域幅の量 **(Mbps)** を指定し、必要に応じて、場所ごとにサイト オプションをカスタマイズします (サイトごとにカスタマイズ)。

QoSはコンピューティング ロケーション レベルで有効にしますが、後の手順でリモート ネットワークを追加するときに、サイトごとにQoSを有効または無効にするように指定したり、サイトごとにQoSプロファイルを指定したりできます。QoSを構成する前に、保証された帯域幅の指定やサイトごとの帯域幅のカスタマイズなど、 コンピューティング場所ごとに帯域幅を割り当てるリモート ネットワークでQoS がどのように機能するかを理解する必要があります。

 ©2025 Palo Alto Networks, Inc.

STEP 4 | （任意） Prisma Accessがユーザーおよびグループ情報を取得するために、Cloud Identity Engine (クラウドIDエンジン) の Directory Sync コンポーネントを使用するように **Group Mapping Settings (**グループ マッピング設定)を構成します。

Prisma Accessでグループ マッピング設定を使用してグループ・マッピングを有効にする前に、Active Directory (アクティブディレクトリ - AD) からユーザおよびグループ情報を取得するように Cloud Identity Engineを構成する必要があります。

STEP 5 | スタック内のいずれかのテンプレートに新しいゾーンを作成（**Network**（ネットワーク） **> Zones**（ゾーン） **> Add**（追加））するか、または追加した既存のテンプレートで参照されるゾーンをスタックにマップ（TrustedまたはUntrustedとして）します。Panoramaで、ポリシールールはデバイスグループ内に、ゾーンはテンプレート内に定義されています。そのため、ポリシールールに含まれているゾーンを参照するテンプレートを、テンプレートスタックに追加していることを確認する必要があります。

Palo Alto Networks®次世代型ファイアウォール上で、セキュリティポリシーはファイアウォールの物理/仮想インターフェイスにマップされているゾーン間で適用されています。ネットワーク用のPrisma Accessは2つのゾーンしかないため（TrustとUntrust）、インターネット宛てのトラフィックを持つゾーン（認可されたSaaSアプリケーションを含む）はすべてUntrustとして、内部ゾーンはすべてTrustとしてマップする必要があります。

1. （任意） ゾーンマッピング設定を編集します。

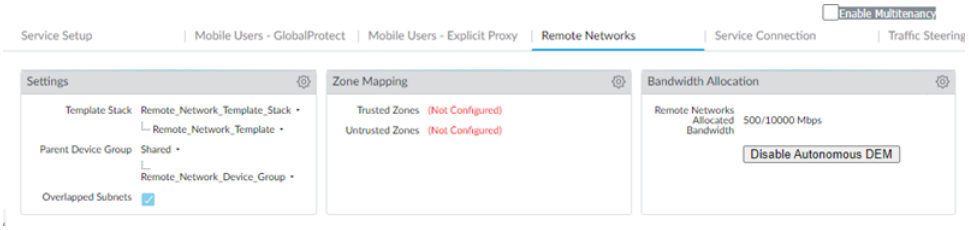
   デフォルトで、Prisma Access for netowrksテンプレートスタックのすべてのゾーンは、Untrustedゾーンに分類されています。ゾーンをまだ定義していない場合、またはRemote_Network_Template_Stack内のテンプレートにゾーン設定がない場合、ポリシーをPrisma Access for networksにプッシュする際に、ここに戻ってゾーンを追加することができます。
2. Trustedと指定する各ゾーンを選択して、**Add**（追加）をクリックし、それを**Trusted Zones**（信頼するゾーン）のリストに追加します。
3. **OK** をクリックしてマッピングを保存します。

 ©2025 Palo Alto Networks, Inc.

STEP 6 | 帯域幅割り当て領域の歯車アイコンをクリックして、オンボードする場所に帯域幅を割り当てます。

コンピュート ロケーションごとに集約レベルで帯域幅を割り当てます。詳細は Prisma Accessリモートネットワーク を参照してください。

アドオン ライセンスとして 自律型DEM を削除した場合、またはライセンスからリモート ネットワーク用の自律型*DEM*を削除した場合は、*[*自律型***DEM***を無効にする*]*を選択します。リモート ネットワークの自律型*DEM*を削除し、自律型*DEM*を無効にしないと、コミット時にエラーが発生します。



現在、場所ごとにリモート ネットワークをオンボードしている既存のリモート ネットワーク デプロイメントがある場合は、 集約帯域幅モデルに移行するかどうかを尋ねるポップアップ ウィンドウが表示されます。移行を続行するには [移行] をクリックし、移行をキャンセルするには [キャンセル] をクリックします。

集約帯域幅モデルへの移行は永続的であり、元に戻すことはできません。移行する前に、 移行前チェックリストを確認してください。変更を有効にするには、変更を コミットしてプッシュする 必要があります。

デプロイメントをアグリゲート帯域幅モデルに移行しても、サービス**IP**アドレス (リモート ネットワーク接続のためにPrisma AccessIPSecトンネル側で使用されるまたはパブリック**IP**アドレス）は変更されず、IPSec トンネルの再設定は必要ありません。

STEP 7 | オンボーディングしたい**Prisma Access**ロケーションに関連する、各コンピュートロケーションに必要な帯域幅割り当てを入力します。

入力した帯域幅の量を確認するには、帯域幅の量の横にあるチェックマークを選択します。量をキャンセルするには、**x**を選択します。

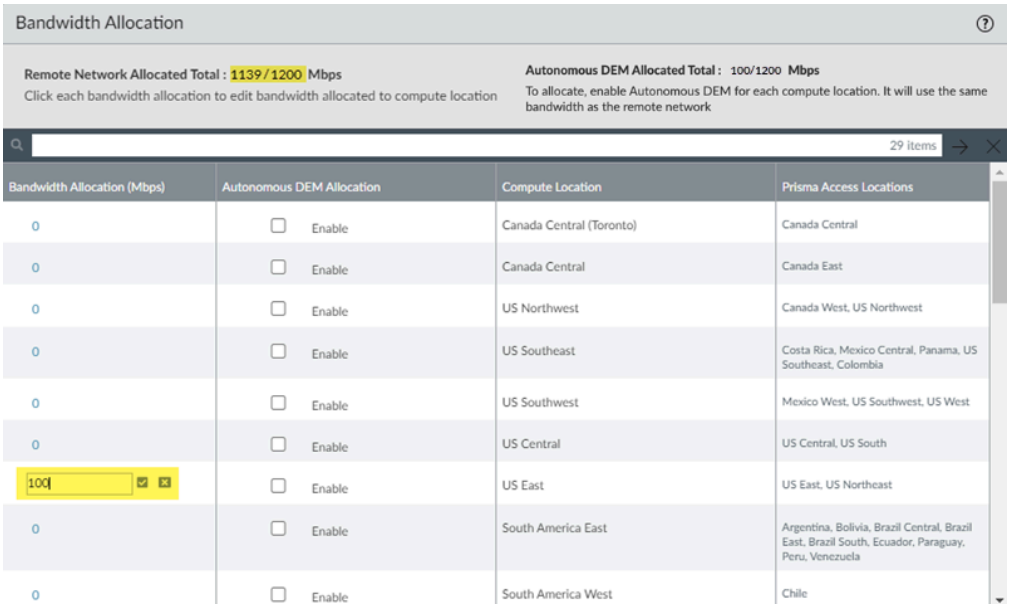
最小帯域幅50 Mbpsと、最大残りのライセンス帯域幅の最大帯域幅を指定します。

STEP 8 | (任意：リモート ネットワーク ライセンスの自律型DEMを使用したデプロイメントのみ) 帯域幅を割り当てたコンピューティングロケーションに対して 自律型**DEM**割り当てを有効にします 。

コンピューティング ロケーションに対して 自律型DEM を有効にすると、自律型DEM ライセンスによって使用される帯域幅の量は、コンピューティング ロケーションに対して指定した帯域幅と同じになります。自律型**DEM** 割り当て合計には、自律型DEMによって使用されている帯域幅と残りの帯域幅が表示されます。詳細については、自律型DEM ガイドを参照してください。

 ©2025 Palo Alto Networks, Inc.

STEP 9 | ページ上部の [割り当てられた合計]フィールドに帯域幅が反映されるまで待ってから、**[OK]**をクリックします。



STEP 10 | (任意)リモート ネットワークの場所への安全なインバウンドアクセスを提供するようにリモート ネットワークを構成する場合は、**[インバウンドアクセス リモート ネットワーク]** タブをクリックし、ワークフローに従って リモート ネットワークの安全なインバウンドアクセスを構成します。

STEP 11 | リモート ネットワークを追加し、名前を指定します。

入力後にリモートネットワークロケーション名を変更することはできません。オンボーディングを開始する前に、リモートネットワークの名前の設定体系を忘れずに確認してください。

STEP 12 | （任意：BGPデプロイ環境のみ）リモートネットワークがそのトラフィックに対して4つまでのIPSecトンネルを使用できるように、設定を作成します（**ECMP**ロードバランシング）。

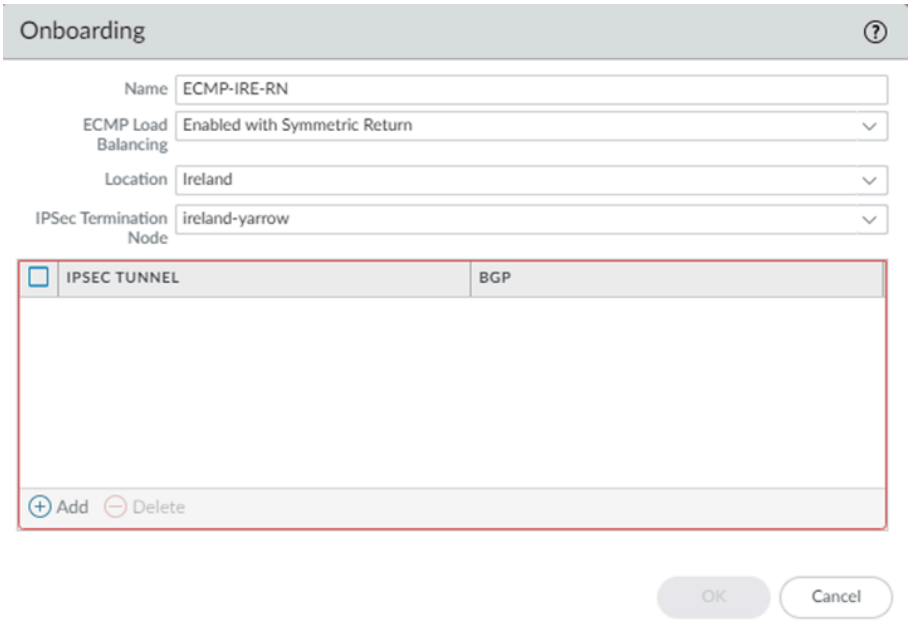
スタティック ルートはサポートされていません (BGPが必要です)。また、QoSが設定されている場合は、ECMPリンクの 割り当て比率を変更することはできません。デプロイ環境でリモートネットワーク接続用にIPSecトンネルを1つ使用している、またはスタティックルートを使用している場合は、**ECMP**ロードバランシングで**None**（なし）を選択して、15ステップに進んでください。

1. ECMPロードバランシングを有効または無効にする選択肢のいずれかを選択します。
   - **None**（なし）–ECMPロードバランシングを使用しません（このリモートネットワーク接続に対して、単一のリモートネットワークトンネルを使用します）。スタティックルートを使用する場合、このオプションしか選択できません。ECMPロードバランシングには、BGPが必要です。
   - **Enabled with Symmetric Return**（対称リターンとともに有効にする）–このリモートネットワーク接続に最大4つのIPSecトンネルを指定し、Prisma Accessがトラ

 ©2025 Palo Alto Networks, Inc.

フィックの送信に使用したのと同じリンクをリターントラフィックに使用するように強制します。

プライマリトンネルのいずれかがダウンした場合にのみ、1つまたは複数のトンネルをバックアップトンネルとして使用する場合に、このオプションを選択します。リンクに障害が発生した場合、Prisma Accessは他のいずれかのトンネルを使ってトラフィックを対称的に送受信します。



2. **Add**（追加）を選択して、リモートネットワーク接続用のIPSecトンネルを追加して、次の値を指定します。。

   - **Enable**（有効）–IPSecトンネルのBGPを有効にします。

     この選択項目は設定不可能です。ECMPを設定するには、BGPを有効にする必要があります。

   - **Summarize Mobile User Routes before advertising**（アドバタイジングを行う前に、モバイルユーザーのルートを要約）–BGPを介した、顧客構内設備（CPE）への、モバイルユーザーIPサブネットのアドバタイジング数を、それを要約することで減らします。

     デフォルトでPrisma Accessは、モバイルユーザーのIPアドレスプールを、/24サブネットのブロックでアドバタイズします。それを要約すると、Prisma Accessによって指定したサブネットに基づいてプールがアドバタイズされます。たとえば、Prisma Accessは、パブリックユーザーのモバイルIPプールを、アドバタイズ前に10.8.1.0/24、10.8.2.0/24、10.8.3.0/24などのサブネットに分割するのではなく、/20のサブネットを使用して10.8.0.0/20のプールをアドバタイズします。これらのアドバタイズを要約することで、CPEルーティングテーブルに保存されるルート数を削減できる可能性があります。たとえば、限定された数のルートを受け付け

©2025 Palo Alto Networks, Inc.

るクラウドVPNゲートウェイ（仮想プライベートゲートウェイ（VGW）またはトランジットゲートウェイ（TGW））で、IPプールの要約を使用することができます。

*ECMP*を使用するロケーションに対してルート要約を有効にする場合、そのロケーションへのすべてのリンクのルート要約を有効にする必要があります。そうしないと、コミット時にエラーが発生します。

Prisma Accessは、集約されたモバイルユーザールートに対してコミュニティ文字列を`0xFFFE:0xFFF0`に設定します。

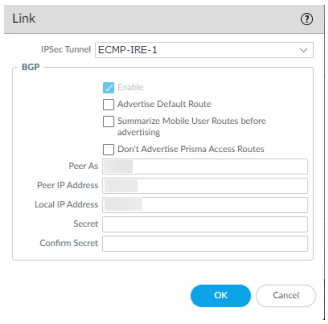
- デフォルトルートをアドバタイズする—Prisma AccessはeBGPを使用してリモートネットワークのデフォルト ルート広告を開始します。

  ネットワークに、*BGP*がアドバタイズしている他のデフォルトルートが存在していないことを確認してください。そうしないと、ネットワークにルーティング上の問題が発生する可能性があります。

- **Prisma Access**ルートをアドバタイズしない—Prisma AccessBGPピアが、組織のネットワークにルートを転送することを防止します。

  デフォルトで、Prisma Accessは、ローカルルート、および他のサービス接続、リモートネットワーク、およびモバイルユーザーサブネットから受信するすべてのプレフィックスを含め、すべてのBGPルーティング情報をアドバタイズします。Prisma AccessによるBGPアドバタイズメントの送信を防止しながら、受信したBGP情報を使って、他のBGPネイバーからルートを学習するには、このチェックボックスを選択します。

  このオプションを選択するとBGPアドバタイズメントは送信されないため、Prisma Accessへのルートを確立するために、オンプレミス機器でスタティックルートを設定する必要があります。



- (任意) **MRAI**タイマー値を選択します。

  BGPルーティングでは、ネットワーク内のBGPルーティング収束を調整するために使用できる 最小ルート広告間隔 *(MRAI)*と呼ばれるタイマーが提供されます。MRAIは宛先ごとに更新のレートを制限するように機能し、BGPルータは同じプレフィックスのアドバタイズメントを送信する前に、少なくとも設定されたMRAI時間待機します。数値が小さいほど収束時間は速くなりますが、ネットワーク内に作成される広告は多くなります。数値が大きいほど、送信できる広告の数は減りますが、ルーティングの収束も遅くなる可能性があります。ルーティング収束の高速化

 ©2025 Palo Alto Networks, Inc.

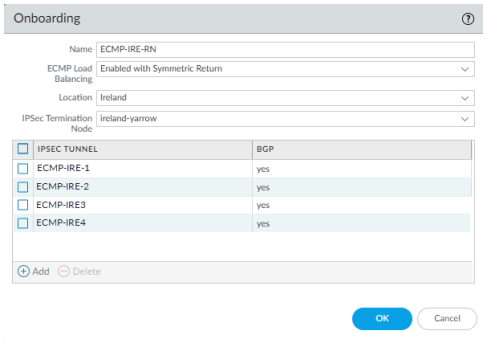
と広告の削減の間の最適なバランスを実現するために、ネットワークに配置する数を決定します。

MRAI の範囲を1 ～ 600秒に設定します。デフォルト値は30秒です。

- **Peer AS**—リモートネットワークのファイアウォール、仮想ルーター、またはBGPルーターが所属している自律型システム（AS）を指定します。
- **Peer IP Address**（ピアIPアドレス）—この接続を設定しているリモートネットワーク上の、eBGPルーターのルーターID として割り当てるIPアドレスを入力します。
- **Local IP Address(ローカルIPアドレス)**（任意） Prisma Accessが、BGPのローカルIPアドレスとして使用するアドレスを入力します。トンネルのPrisma Access側で使用するIPアドレスを指定します。

  Local Addressの指定は、接続のもう一方の側にあるデバイス（Amazon Web Service（AWS） Virtual Private Gatewayなど）が、BGPピアリングを正常に行うために、特定のローカルIPアドレスを必要としている場合などに役立ちます。指定するIPアドレスは、インフラサブネットまたはリモートネットワーク内のサブネットのIPアドレスと、競合またはオーバーラップしていないことを確認してください。
- **Secret**（シークレット）および**Confirm Secret**（シークレットの再入力）（任意）—BGPピア通信の認証のために、パスフレーズを入力して、その内容を確認します。

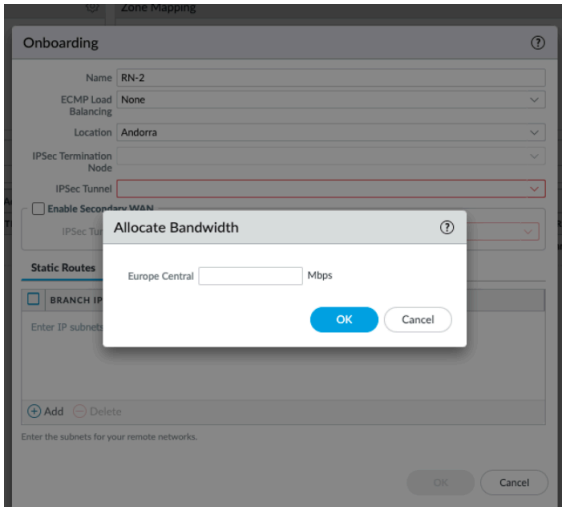
3. 前のステップを繰り返して、リモートネットワーク接続で使用するトンネルを、最大4つまで追加します。



 ©2025 Palo Alto Networks, Inc.

STEP 13 | リモートネットワークロケーションを保護するために必要なインフラをPrisma Accessが展開する、**Location**（ロケーション）を選択します。この地域は、リモートネットワークロケーションと地理的に近い場所でなければなりません。

ロケーションがマップされている コンピューティングロケーション にまだ帯域幅を割り当てていない場合は、 Prisma Accessはそのコンピューティング場所の帯域幅を入力するように求めます。



2 つのアスタリスクで示される場所は、 ローカル ゾーンです。このような立地は、コンピュート、ストレージ、データベース、インフラストラクチャー サービスを人口や産業の中心地の近くに配置することになりますが、いくつかの制限もあります。ローカル ゾーンを追加するには、Palo Alto Networksの担当者にお問い合わせください。

STEP 14 | このリモート ネットワークに使用する **IPSec** 終端ノードを選択します。

Prisma Accessはこのノードを使用して、リモート ネットワークの場所とコンピューティングのロケーションを関連付けます。

STEP 15 | （スタティックルーティングまたは単一トンネルのデプロイのみ）企業のロケーションにあるファイアウォール、ルーター、またはSD-WANデバイスにアクセスするための、新しい**IPSec Tunnel**（**IPSec**トンネル）設定を選択または追加します。

- Remote_Network_Template内の事前定義済みの IPSec テンプレートのいずれかを選択します。または、IPsec トンネル構成を含むテンプレートを Remote_Network_Template_Stack に追加した (または定義済みの Remote_Network_Template を変更した) 場合は、ドロップダウンからその **IPsec** トンネルを選択します。各リモートネットワーク接続用に作成しているトンネルは、Prisma Accessを各支店のロケーションにあるIPSec対応デバイスに接続するものであることに注意してください。

  IPSecトンネルを設定する場合は、以下のガイドラインを使用してください。

  - IKEゲートウェイ設定のピアアドレスは、各トンネルに対して一意でなければなりません。ただし、Crypto（暗号）プロファイルなど、他の一般的な一部の設定エレメントの再使用は可能です。
  - テンプレートから選択するIPSecトンネルは、Auto Key（自動鍵）交換とIPv4のみを使用する必要があります。

©2025 Palo Alto Networks, Inc.

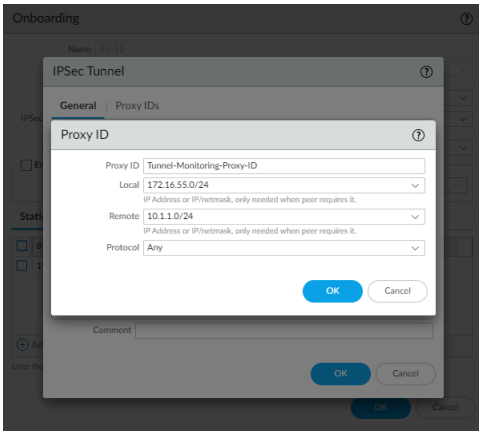
  - IPSec トンネル、IKE ゲートウェイ、および暗号プロファイル名は 31 文字を超えることはできません。
  - ダイナミックIKEピアがある同じロケーションへの、複数のリモートネットワークをオンボーディングする場合、すべてのリモートネットワーク設定で同じIKE暗号プロファイルを使用する必要があります。
- 新しいIPSecトンネル設定を作成するには、**New IPSec Tunnel**（新規**IPSec**トンネル）をクリックして、**Name**（名前）を入力してIKEゲートウェイ、IPSec暗号プロファイル、およびTunnel Monitoringの環境設定を行います。
  - 支店のロケーションにあるIPSec対応デバイスがポリシーベースのVPNを使用している場合、**Proxy IDs**（プロキシ**ID**）タブで、Prisma Accessがローカルデバイスとのの IPSecトンネルを正常に確立できるように、ローカルIPSecデバイスに設定されているプロキシIDと一致するプロキシIDを**Add**（追加）します。
- リプレイ攻撃を検出して無力化するために、**Enable Replay Protection**（リプレイプロテクションを有効にする）は選択された状態のままにしてください。
- 元のTOS情報を保持するため、カプセル化されたパケットの内部IPヘッダーから外部IPヘッダーにTOS（Type of Service）フィールドをコピーするには、**Copy TOS Header**（**TOS**ヘッダーのコピー）を選択します。

©2025 Palo Alto Networks, Inc.

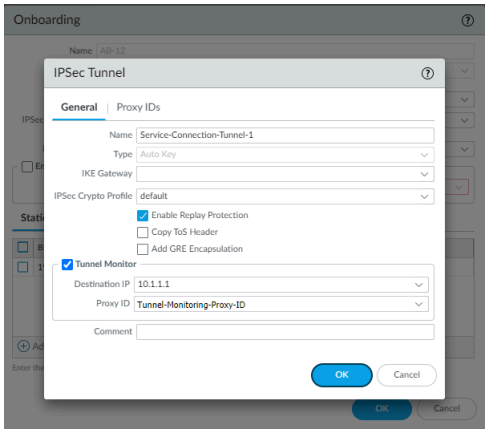
- サービス接続のトンネル監視を有効にするには、**Tunnel Monitor**（トンネル監視）を選択します。
  - **Destination IP**（宛先**IP**）アドレスを入力します。

    Prisma AccessがIPSecトンネル監視のために、ICMP pingリクエストを送信できる、支店のロケーションのIPアドレスを指定します。このアドレスは、Prisma Accessインフラのサブネット全体から、ICMPで到達可能であることを確認してください。
  - 複数のプロキシIDを使用するピアデバイスでトンネル監視をしようする場合、**Proxy ID**（プロキシ**ID**）を指定するか、またはインフラサブネットから支店のロケーションへのアクセスを可能にする、**New Proxy ID**（新しいプロキシ**ID**）を追加します。

    サービスインフラサブネット（この例では172.16.55.0/24）を**Local**（ローカル） IPサブネットに、支店ロケーションのサブネット（この例では10.1.1.0/24）を**Remote**（リモート）サブネットにしているプロキシIDの例を次に示します。



次の図は、作成したプロキシIDを**Proxy ID**（プロキシ**ID**）フィールドに指定することで、そのプロキシIDをトンネル監視に適用した例です。



©2025 Palo Alto Networks, Inc.

トンネル監視が機能するには、*CPE* 上でトンネルモニタリング *IP* アドレスへのスタティックルートを構成する必要があります。支店のロケーションから*Prisma Access*へのトンネル監視に使用する宛先*IP*アドレスを探すには、***Panorama*** > ***Cloud Services***（クラウドサービス） > ***Status***（ステータス） > ***Network Details***（ネットワーク詳細）を選択して、***Service Infrastructure***(サービス インフラストラクチャ)ラジオボタンをクリックして、***Tunnel Monitor IP Address***（トンネル監視*IP*アドレス）を参照します。

STEP 16 | このロケーションにセカンダリWANリンクがある場合は、**Enable Secondary WAN**（セカンダリ**WAN**を有効にする）を選択します。

各リモートネットワークのセカンダリ*WAN*に対して、一意の*IPSec*トンネルを作成してください。*Prisma Access*では、複数のリモートネットワーク内のセカンダリ*WAN*に対する、同じ*IPSec*トンネルの再利用はサポートされていません。

セカンダリ WAN の設定は、次の展開ではサポートされていません。

- セカンダリ WAN がプライマリ IPsec トンネルを使用してアクティブ/アクティブモードに設定されている場合。
- 顧客宅内機器 (CPE) が、プライマリおよびセカンダリIPsecトンネルを使用する等コストマルチパス (ECMP) 構成で設定されている場合。

スタティックルートを使用する場合、トンネルのフェイルオーバー時間は検出時から15秒未満になりますが、ご利用のWANプロバイダによって異なります。

BGPルーティングを設定し、トンネル監視を有効にしている場合、セキュリティパラメータインデックス（SPI）が失敗していると判断するまでの、デフォルトのホールドタイムがもっとも短いのが、Tunnel Monitorです。これは、連続した15秒間のトンネル障害を検出すると、ピアへのすべてのルートを削除します。このように、Tunnel MonitorがBGPルートの動作を判断します。トンネルモニタリングを設定しない場合、ホールドタイマーはルートを削除する前にトンネルがダウンしている時間を決定します。 Prisma Accessは、RFC 4271で定義されているデフォルトのBGP HoldTime値90秒を使用します。これは、Prisma Accessが非アクティブなSPIのルートを削除するまでの最大待機時間です。ピアBGPデバイスに短いホールドタイムが設定されている場合、BGPホールドタイマーはより小さい方の値を使用します。

セカンダリトンネルが正常にインストールされた場合、プライマリトンネルが復旧するまでの間、セカンダリルートが優先されます。プライマリとセカンダリの両方が機能している場合は、プライマリルートが優先されます。

セカンダリ（バックアップ）接続に別の*BGP*ピアを使用する場合、*Prisma Access*は *CPE* によってアドバタイズされたマルチエグジットディスクリミネーター（*MED*）属性を尊重しません。この注意事項は、リモートネットワーク接続またはサービス接続のいずれかで複数の *BGP* ピアを使用する場合に適用されます。

 ©2025 Palo Alto Networks, Inc.

STEP 17 | ユーザーがアクセスする必要がある、リモートネットワークサイトのサブネットワークまたは個別のIPアドレスへのルーティングを有効にします。

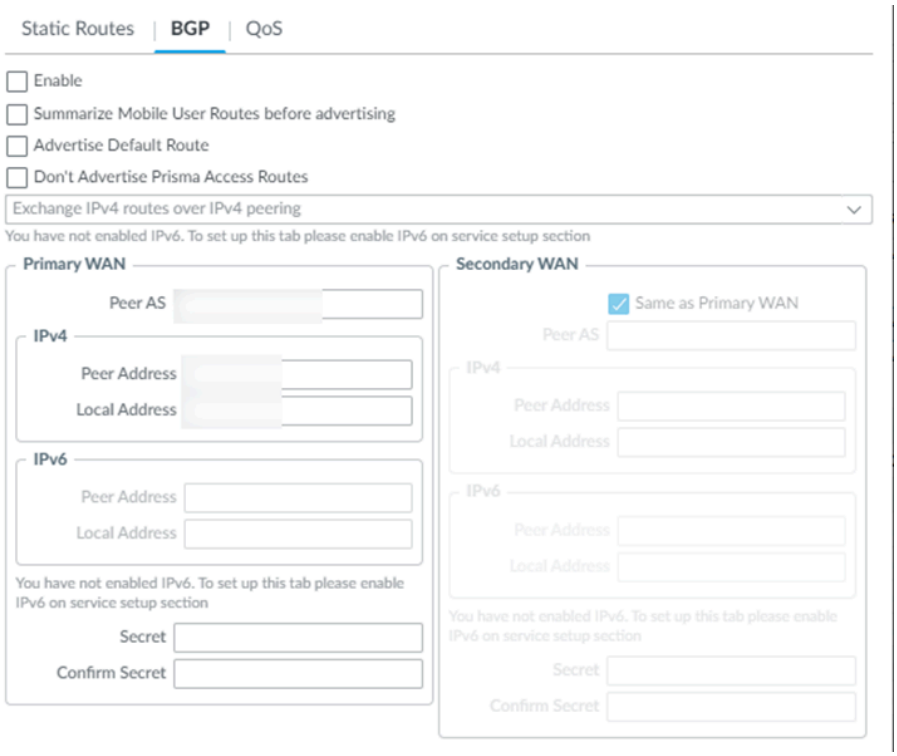
Prisma Accessはこの情報を使って、適切なサイトにリクエストをルーティングします。各サイトのネットワークは相互にオーバーラップすることはできません。また、サービスインフラ用またはユーザー用のPrisma AccessIPプール用に指定した各IPアドレスプールをオーバーラップさせることもできません。**Static Routes**（スタティックルート）、**BGP**、または両方の組み合わせを設定することができます。

- **Static Routes**（スタティックルート）を設定するには：
  1. **Static Routes**（スタティックルート）タブで**Add**（追加）をクリックして、リモートユーザーがアクセスする必要があるサブネットワークアドレス（例：172.168.10.0/24）、またはDNSサーバーなどのリソースの個別のIPアドレス（例：10.32.5.1/32）を入力します。
  2. この手順を繰り返して、Prisma Accessはこのロケーションにアクセスする必要があるすべてのサブネットまたはIPアドレスを指定します。



©2025 Palo Alto Networks, Inc.

- **BGP**を設定するには：
  1. **BGP** タブを選択します。
  2. (任意) **ECMP Load Balancing**（**ECMP**ロードバランシング）を選択します。ステップ12を参照してください。
  3. **ECMP Load Balancing**（**ECMP**ロードバランシング）で**None**（なし）を選択した場合は、BGPを入力します。



  4. リモートネットワークでBGPを有効にするには、**Enable**（有効）を選択します。

     BGPを有効にする場合、Prisma AccessインフラとeBGP接続の終端となる顧客構内設備（CPE）間に存在する可能性がある余分なホップに対応するために、Prisma Accessでは外部BGP（eBGP）のTTL値に8が設定されます。
  5. BGPから顧客構内設備（CPE）にアドバタイズされるモバイルユーザーIPサブネット数を要約して減らすには、**Summarize Mobile User Routes before advertising**（アドバタイズ前にモバイルユーザールートを要約する）を選択します。

     デフォルトでPrisma Accessは、モバイルユーザーのIPアドレスプールを、/24サブネットのブロックでアドバタイズします。それを要約すると、Prisma Accessによって指定したサブネットに基づいてプールがアドバタイズされます。たとえば、Prisma Accessは、パブリックユーザーのモバイルIPプールを、アドバタイズ前に10.8.1.0/24、10.8.2.0/24、10.8.3.0/24などのサブネットに分割するのではなく、/20のサブネットを使用して10.8.0.0/20のプールをアドバタイズします。これらのアドバタイズを要約することで、CPEルーティングテーブルに保存されるルート数を削減できる可能性があります。たとえば、限定された数のルートを受け付けるクラ

©2025 Palo Alto Networks, Inc.

ウドVPNゲートウェイ（仮想プライベートゲートウェイ（VGW）またはトランジットゲートウェイ（TGW））で、IPプールの要約を使用することができます。

Prisma Accessは、集約されたモバイルユーザールートに対してコミュニティ文字列を`0xFFFE:0xFFF0`に設定します。

6. Prisma Accessに、eBGPを使ったリモートネットワーク用のデフォルトルートのアドバタイズを許可するには、**Advertise Default Route**（デフォルトルートのアドバタイズ）を選択します。

   Advertise Default Route（デフォルトルートのアドバタイズ）を選択した場合、ネットワークにBGPがアドバタイズしている他のデフォルトルートが存在していないことを確認してください。そうしないと、ネットワークにルーティング上の問題が発生する可能性があります。

   アドバタイズするためにこの項目を選択する前に、デフォルトのルートを公開する必要があります。また、ネットワークに、*BGP*がアドバタイズしている他のデフォルトルートが存在していないことを確認してください。そうしないと、ネットワークにルーティング上の問題が発生する可能性があります。

7. Prisma Accessファイアウォール上のBGPピアが、組織のネットワークにルートを転送することを防止するには、**[Prisma Accessルートをアドバタイズしない]**を選択します。

   デフォルトで、Prisma Accessは、ローカルルート、および他のサービス接続、リモートネットワーク、およびモバイルユーザーサブネットから受信するすべてのプレフィックスを含め、すべてのBGPルーティング情報をアドバタイズします。Prisma AccessによるBGPアドバタイズメントの送信を防止しながら、受信したBGP情報を使って、他のBGPネイバーからルートを学習するには、このチェックボックスを選択します。

   このオプションを選択するとBGPアドバタイズメントは送信されないため、Prisma Accessへのルートを確立するために、オンプレミス機器でスタティックルートを設定する必要があります。

8. **Peer AS**を入力します。これは、リモートネットワークのファイアウォール、仮想ルーター、またはBGPルーターが所属している自律型システム（AS）です。

9. この接続を**Peer Address**（ピアアドレス）として設定するリモートネットワーク上の、eBGPルーターのルーターID として割り当てるIPアドレスを入力します。

10. （任意） Prisma Accessが、BGPのローカルIPアドレスとして使用するアドレスを入力します。

    Local Addressの指定は、接続のもう一方の側にあるデバイス（Amazon Web Service（AWS） Virtual Private Gatewayなど）が、BGPピアリングを正常に行うために、特定のローカルIPアドレスを必要としている場合などに役立ちます。指定するIPアドレス

©2025 Palo Alto Networks, Inc.

は、インフラサブネットまたはリモートネットワーク内のサブネットのIPアドレスと、競合またはオーバーラップしていないことを確認してください。

*CPE*上で*BGP*ローカル アドレスへのスタティック ルートを設定する必要があります。

11. （任意） BGPピア通信の認証のために、パスフレーズを入力して、その内容を確認します。
12. （任意）**Secondary WAN**（セカンダリ**WAN**）を設定しており、セカンダリ（バックアップ）BGPピアの**Peer Address**（ピアアドレス）または**Local Address**（ローカルアドレス）を変更する必要がある場合、**Same as Primary WAN**（プライマリ**WAN**と同じ）の選択を解除して一意のピアを入力します。また、必要に応じてセカンダリWANのローカルIPアドレスを入力します。

   リモート ネットワーク デプロイメントで IPv6 ネットワーク を使用する場合は、**IPv4**アドレスだけでなく **IPv6**アドレスも構成できます。また、IPv6アドレッシングを使用する前に、Prisma AccessインフラでIPv6ネットワークをグローバルに有効にする必要があります。

   一部のデプロイ環境では（例:AWS VPNゲートウェイを持つピアにBGPを使用している）、プライマリWANとセカンダリWANのBGPピアが異なっていることがあります。そのような場合、セカンダリWANに対して、別のBGPピアを設定することができます。

   セカンダリ*WAN*を持つ*BGP*デプロイ環境の場合、*Prisma Access*はプライマリトンネルとセカンダリトンネルの両方の状態を***UP***に設定しますが、ネットワークトラフィックに対しては標準の*BGP*アクティブ-バックアップ動作に従います。*Prisma Access*はプライマリ トンネルをアクティブに設定し、そのトンネルを介してのみトラフィックを送受信します。プライマリ トンネルに障害が発生した場合、*Prisma Access*は*BGP*ルールを使用して障害を検出し、セカンダリ トンネルをアクティブに設定し、セカンダリ トンネルのみを使用してトラフィックを送受信します。

STEP 18 | (任意) 場所に対して**QoS**を有効にし、**QoS**プロファイルを指定します。

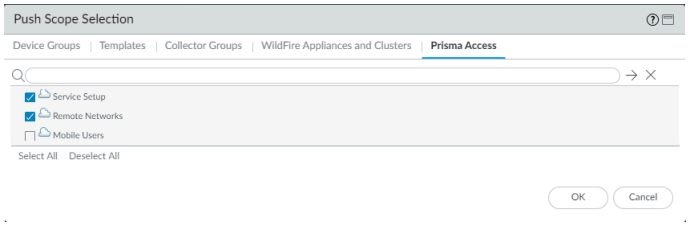
QoSオプションおよび全体的な設定は、[設定]でコンピュート ロケーションごとに指定しますが、QoSの有効化、無効化、およびQoSプロファイルの変更は、ここでロケーションごとに行うことができます。

STEP 19 | Panoramaに設定の変更内容をコミットし、設定をPrisma Accessにプッシュします。

1. **Commit**（コミット） > **Commit to Panorama**（**Panorama** へのコミット）をクリックします。
2. **Commit**（コミット） > **Commit and Push**（コミットしてプッシュ）をクリックします。**Edit Selections**（選択項目の編集） > **Prisma Access**の順に選択して、ネットワーク

 ©2025 Palo Alto Networks, Inc.

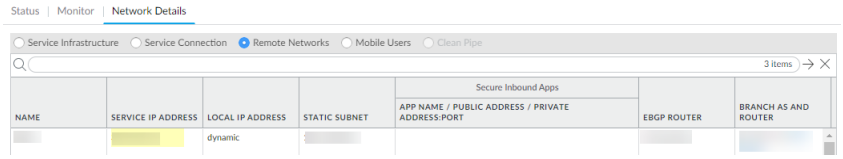
用のPrisma AccessおよびPrisma Access for service setupの両方を選択し、サービスに設定をプッシュします。



3. **OK**、**Push**（プッシュ）の順にクリックします。

STEP 20 | リモートネットワークロケーションにあるIPSec対応デバイスを設定して、ネットワーク用のPrisma AccessとのIPSec接続をセットアップします。

1. **Panorama** > **Cloud Services** > ステータス > ネットワーク詳細を選択し、 リモート ネットワーク ラジオ ボタンをクリックし、 サービス **IP** アドレス フィールドを表示して、このリモート ネットワーク接続の サービス **IP** アドレス を見つけます。 ネットワーク用Prisma Accessインフラストラクチャは、リモート ネットワーク接続用にこのまたはIPアドレスを割り当てているため、Prisma Accessリモート ネットワーク ロケーションとネットワーク用Prisma Accessの間でIPSecトンネルをセットアップするには、これをピアIPアドレスとして設定する必要があります。



2. **Panorama** > **Cloud Services**（クラウドサービス） > **Status**（ステータス） > **Network Details**（ネットワーク詳細） > **Remote Networks**（リモートネットワーク）ページで、リモートネットワークロケーションにあるデバイスの**Local IP address**（ローカル**IP**アドレス）を確認します。リモートネットワークロケーションでNATを実行している場合、**Local IP address**（ローカル**IP**アドレス）にはNAT処理後のデバイスのIPアドレスが表示されます。

STEP 21 | リモートネットワークロケーションのトラフィックを保護するには、セキュリティポリシールールを作成する必要があります。

1. **Policies (**ポリシー**)**を選択します。
2. ポリシールールを追加する**Device Group** （デバイス グループ）を選択します。Remote_Network_Device_Group、またはリモートネットワークロケーションを保護するポリシーを定義するために選択した親デバイスグループを選択することができます。
3. セキュリティポリシールールを作成します。任意の（Any）ゾーンから任意のゾーンへのトラフィックを許可するセキュリティポリシールールを定義していないことを確認してください。セキュリティポリシールールでは、テンプレート内に定義したゾーンを使用します。

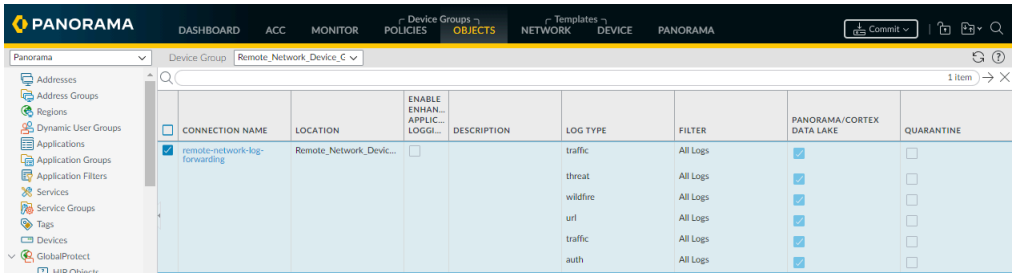
   ネットワーク上のユーザーが、Webサイトへのアクセスを拒否された場合、Palo Alto Networksでチケットを開く前に、Webサイトアクセス上の問題を報告してください。

©2025 Palo Alto Networks, Inc.

STEP 22 | Strata Logging Serviceへのロギングを有効にします。ログを転送する各ポリシー ルールにログ転送プロファイルを作成して、アタッチする必要があります。

1. **[Objects] > [**ログ転送**]** の順に選択します。
2. ポリシールールを追加した**Device Group**（デバイスグループ）を選択します（例：Remote_Network_Device_Group）。
3. ログ転送プロファイルを**Add**（追加）します。ログ転送プロファイル一致リストで、転送する各**Log Type**（ログタイプ）を**Add**（追加）します。
4. 転送方法として**Panorama/Strata Logging Service (**ロギングサービス**)**を選択し、Prisma AccessがログをStrata Logging Serviceに転送できるようにします。Panoramaからログを監視し、レポートを作成することができます。 Strata Logging Serviceはシームレスな統合を提供し、ログを本社のPanoramaにバックホ ールすることなく保存し、Panoramaは必要に応じてStrata Logging Serviceにクエリを実行することができます。

   Traffic（トラフィック）、Threat Prevention（脅威防御）、WildFire Submission（WildFire送信）、URL Filtering（URLフィルタリング）、Data Filtering（データフィルタリング）、およびStrata Logging ServiceへAuthentication（認証）ログを転送する例を次に示します。



5. **Policies**（ポリシー） **> Security**（セキュリティ）を選択して、ポリシールールを編集します。**Actions**（アクション）で、作成した Log Forwarding（ログ転送）プロファイルを選択します。

STEP 23 | Panorama にすべての変更をコミットし、その設定変更をPrisma Accessにプッシュします。

1. **Commit**（コミット） **> Commit and Push**（コミットしてプッシュ）をクリックします。
2. **[**選択内容を編集**]**をクリックし、**[Prisma Access]**タブで**[Push Scope (**スコープをプッシュ**)]**に**[**ネットワーク用**Prisma Access]**が選択されていることを確認し、**[OK]**をクリックする。
3. 変更を **Commit and Push**（コミットしてプッシュ）します。

STEP 24 | リモート ネットワークのステータスを確認します。

詳細については、「リモート ネットワーク接続ステータスの確認」を 参照してください。

©2025 Palo Alto Networks, Inc.

リモート ネットワーク サイトをPrisma Accessに接続する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Accessのライセンス

IPSec VPNトンネルを設定して、リモートネットワークとPrisma Accessを接続します。支店のIPSec デバイスからPrisma AccessにIPSecトンネルを作成する必要があります。

最初に作成するトンネルは、リモート ネットワーク サイトのプライマリ トンネルになります。その後、このワークフローを繰り返して、オプションでセカンダリ トンネルを設定できます。両方のトンネルがアップすると、プライマリ トンネルがセカンダリ トンネルよりも優先されます。リモート ネットワーク サイトのプライマリ トンネルがダウンした場合、プライマリ トンネルが復旧するまで、リモート ネットワークはセカンダリ トンネルにフォールバックします。

リモート ネットワーク サイトでトンネルを確立するために使用するIPSecデバイスに基づき、Prisma Accessはビルトインの推奨IKEおよびIPSecセキュリティ設定を提供します。推奨設定を使用してすぐに使用を開始することも、環境に合わせて必要に応じてカスタマイズすることもできます。

- プライマリおよびセカンダリ IPSec VPN トンネルの追加
- その他のIKEオプション
- その他のIPSecオプション

プライマリおよびセカンダリ IPSec VPN トンネルの追加

STEP 1 | Prisma Accessを起動します。

STEP 2 | **[Workflows (ワークフロー)] > [Prisma AccessのSetup (セットアップ)] > [Remote Networks (リモート ネットワーク)] > [Add Remote Networks (リモートネットワークの追加)]**へ移動し、プライマリ トンネルをセットアップします。すでにプライマリトンネルを設定している場合は、ここで続けてセカンダリトンネルを追加することもできます。

1. トンネルにわかりやすい名前を付けます。
2. Prisma Accessとのトンネルを確立するために使用する、リモート ネットワーク サイトにあるIPSecデバイスの**[Branch Device Type (ブランチ デバイス タイプ)]**を選択します。

©2025 Palo Alto Networks, Inc.

3. ［**Branch Device IP Address**］ で、トンネルエンドポイントを識別するスタティック **IP** アドレスまたはダイナミック IP アドレスのいずれかを選択します。

   ブランチデバイスの**IP**アドレスをダイナミックに設定する場合は、リモートネットワークサイトのIKE ID（**IKE**ローカル**ID**）または Prisma Access (**IKE** ピア識別) により、IPSec ピアが認証できるようになります。

   リモートネットワークが完全に展開されるまでは、Prisma Access IKE ID（**IKE** ピア **ID**）に使用する値がないため、通常は、Prisma Access IKE IDではなく、リモートネットワークサイト（**IKE** ローカル **ID**）のIKE IDを設定します。

STEP 3 | トンネルモニタリングをオンにする。

Prisma Accessがトンネルが稼働しているかどうかを判断するために使用する、リモートネットワーク上のトンネル監視宛先**IP**アドレスを入力し、ブランチIPSecデバイスがポリシーベースVPNを使用している場合は、関連するプロキシ**ID**を入力します。

入力したトンネル監視 IP アドレスは自動的にブランチ サブネットワークのリストに追加されます。

STEP 4 | トンネル設定を保存します。

続行するには

- IKE および IPSec の高度な暗号設定をセットアップおよびカスタマイズします。その他のIKEオプションとその他のIPSecオプションを参照してください。
- 「リモートネットワークのルーティングを有効にする」を行います。

その他のIKEオプション

Prisma Accessは、選択したIPSecデバイス タイプに基づいて、リモート ネットワーク サイト デバイスとPrisma Access間のIKE フェーズ1鍵交換プロセスに推奨される暗号セット と鍵寿命を提供します。推奨設定を使用することも、環境に応じて設定をカスタマイズすることもできます。

IKEネゴシエーションに使用するブランチデバイスとPrisma Accessの **IKE** プロトコル バージョンを選択します。

[IKEv1 Only Mode]を選択すると、Prisma AccessはネゴシエーションにIKEv1プロトコルのみを使用できます。**[IKEv1 Only Mode]**を選択すると、Prisma AccessはネゴシエーションにIKEv1プロトコルのみを使用できます。**IKEv2**優先モードを選択した場合、Prisma Accessはブランチ IPSecデバイスもIKEv2をサポートしている場合にのみ、IKEv2プロトコルを使用します。ブランチIPSecデバイスがIKEv2をサポートしていない場合、Prisma AccessはIKEv1プロトコルの使用に戻ります。

 ©2025 Palo Alto Networks, Inc.

IKEv1 暗号プロファイル を追加して、IKE フェーズ 1 のキー交換プロセスに使用される暗号化および認証アルゴリズムを定義する IKE 暗号設定をカスタマイズします。

Prisma Accessは、このトンネルの確立に使用されているブランチ デバイス タイプに基づいて、デフォルトの IKE 暗号プロファイルを自動的に使用します。

- 暗号化- IKE SA ネゴシエーションで使用される暗号化アルゴリズムを指定します。

  Prisma Accessは、次の暗号化アルゴリズムをサポートしています。3des (168 ビット)、aes-128-cbc (128 ビット)、aes-192-cbc (192 ビット)、aes-256-cbc (256 ビット)、および des (56 ビット)。null (暗号化なし) を選択することもできます。
- 認証- IKE SA ネゴシエーションで使用される認証アルゴリズムを指定します。

  Prisma Accessは、sha1 (160 ビット)、sha256 (256 ビット)、sha384 (384 ビット)、sha512 (512 ビット)、および md5 (128 ビット) の認証アルゴリズムをサポートします。null (認証なし) を選択することもできます。
- **DH** グループ—IKE SA ネゴシエーションで IKE の対称キーを生成するために使用される Diffie-Hellman (DH) グループを指定します。Diffie-Hellman アルゴリズムは、一方の秘密鍵ともう一方の公開鍵を使用して共有のシークレットを作成します。これは、両方の VPN トンネル ピアによって共有される暗号化鍵です。

  Prisma Accessは次のDHグループをサポートします。グループ 1 (768 ビット)、グループ 2 (1024 ビット-デフォルト）、グループ 5 (1536 ビット)、グループ 14 (2048 ビット)、グループ 19 (256 ビット楕円曲線グループ)、グループ 20 (384 ビット楕円曲線グループ)です。セキュリティを最強にするには、最も大きい番号のグループを選択します。
- ライフタイム- IKE フェーズ 1 キーが有効である単位と時間を指定します (デフォルト 8 時間)。IKEv1 の場合、security association (SA) は、鍵の有効期限が切れる前にアクティブに鍵更新されません。IKEv1 フェーズ 1 の鍵更新は、SA の有効期限が切れた場合にのみトリガーされます。IKEv2 の場合、キーの有効期限が切れる前に SA の鍵更新する必要があります。SA の有効期限が切れたときに鍵更新すされない場合、SA は新しいフェーズ 1 鍵を開始する必要があります。
- **IKEv2 Authentication Multiple**—認証カウントを決定するために、Key Lifetime (キーの有効期間) で乗算される値を指定します（範囲は 0 ～ 50、デフォルトは 0）。認証カウントは、セキュリティ処理ノードが IKEv2 IKE SA 鍵更新を実行できる回数であり、この回数だけ実行した後は、IKEv2 再認証をやり直す必要があります。デフォルト値の 0 は、再認証機能が無効になります。

IKE パッシブ モード を有効にして、Prisma Accessが IKE 接続にのみ応答し、IKE 接続を開始しないようにします。

IKE NAT トラバーサルは デフォルトでオンになっています。

これは、IKE および UDP プロトコルに UDP カプセル化が使用され、IPSec VPNトンネルのエンドポイント間にあるネットワークアドレス変換（NAT）デバイスを通過できることを意味します。

©2025 Palo Alto Networks, Inc.

その他のIPSecオプション

Prisma Accessは、選択したIPSecデバイス タイプに基づいて、セキュリティ・アソシエーション（SA）のIKE フェーズ2において、ブランチデバイスと Prisma Access 間のIPSecトンネル内のデータを保護するために推奨されるIPSecプロトコルと鍵の有効期間設定のセットを提供します。推奨設定を使用することも、環境に応じて設定をカスタマイズすることもできます。

IPSec 暗号プロファイル をカスタマイズして、Auto Key IKE が IKE フェーズ 2 中に IKE SA のキーを自動的に生成するときに、トンネル内でデータを保護する方法を定義します。

Prisma Accessは 、ブランチ デバイス タイプ ベンダーに基づいてデフォルトのIPSec暗号プロファイルを自動的に構成します。デフォルトのプロファイルを使用することも、カスタムプロファイルを作成することもできます。

- **IPSec** プロトコル- VPN トンネルを通過するデータを保護します。Encapsulating Security Payload (**ESP**) プロトコルは、データの暗号化、ソースの認証、およびデータ整合性の検証を行います。Authentication Header (**AH**) プロトコルは、ソースの認証とデータ整合性の検証を行います。

  IPSec プロトコルとして **ESP** を使用する場合は、IPSec SA ネゴシエーションで使用される暗号化 アルゴリズムも指定します。

  Prisma Accessは、次の暗号化アルゴリズムをサポートしています: aes-256-gcm (256 ビット)、aes-256-cbc (256 ビット)、aes-192-cbc (192 ビット)、aes-128-gcm (128 ビット)、aes- 128-cbc (128 ビット)、3des (168 ビット)、およびdes (56 ビット)。null (暗号化なし) を選択することもできます。

認証- IPSec SA ネゴシエーションで使用される認証アルゴリズムを指定します。

Prisma Accessは、sha1 (160 ビット)、sha256 (256 ビット)、sha384 (384 ビット)、sha512 (512 ビット)、および md5 (128 ビット) の認証アルゴリズムをサポートします。IPSecプロトコル が ESPの場合は、[none (なし)] (認証なし) を選択することもできます。

DH グループ-IPSec security association (Security Associations - SA) ネゴシエーションで IKE の Diffie-Hellman (DH) グループを指定します。

Prisma Accessは次のDHグループをサポートします。グループ 1 (768 ビット)、グループ 2 (1024 ビット-デフォルト）、グループ 5 (1536 ビット)、グループ 14 (2048 ビット)、グループ 19 (256 ビット楕円曲線グループ)、グループ 20 (384 ビット楕円曲線グループ)です。セキュリティを最強にするには、最も大きい番号のグループを選択します。Prisma Accessが IKE フェーズ 1 中に作成するキーを更新したくない場合は、**no-pfs**(完全転送秘密なし) を選択します。このオプションを選択すると、Prisma AccessはIPSec SAネゴシエーションに現在のキーを再利用します。

ライフタイム- ネゴシエートされたキーが有効である単位と時間を指定します (デフォルトは 1 時間)。

ライフサイズ- キーが暗号化に使用できるデータの単位と量を指定します。

 ©2025 Palo Alto Networks, Inc.

リモートネットワークのルーティングを有効にする

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Accessのライセンス

Prisma Accessがトラフィックをリモート ネットワークにルーティングするためには、Prisma Accessを使用してセキュリ ティを確保したいサブネットワークのルーティング情報を提供する必要があります。これには複数の方法があります。リモート・ネットワーク・サイトで各サブネットワークへのスタティック ルートを定義するか、サービス接続ロケーションとPrisma Accessの間でBGPを設定するか、または両方の方法を組み合わせて使用します。

スタティックルートを設定し、BGPも有効にした場合、スタティックルートが優先されます。リモートネットワークロケーションのサブネットワーク数がさほど多くない場合、スタティックルートの使用が便利なことが多いですが、重複するサブネットを持つ多数のリモートネットワークが存在する大規模なデプロイ環境では、BGPを使用するとスケーリングが容易になります。

- スタティック ルート- リモート サイトからPrisma Accessへのスタティック ルートを有効にするには、Prisma Accessに確保させたいリモート サイトのサブネット ワークまたは個々のIPアドレスを特定する（インバウンド トラフィックとアウトバウンド トラフィッ クの両方）。各サイトのサブネッ トワークは、互いに重なってはいけません。また、ユーザー向けPrisma Accessに指定したIPプール、またはインフラストラクチャ サブネットと重なってはいけません。
- **BGP**– BGPを有効にしてリモート ネットワークとの間でトラフィックを動的にルーティングする場合は、ブランチのeBGPルーターのBGP情報を提供する必要があります。
  - ブランチ ルータの自律システム **(AS)** 番号- リモート ネットワークのeBGPルータが属するAS。これは ピア**AS**と呼ばれます。
  - ルータ **ID**- リモート ネットワーク上のeBGPルータのルーターIDとして割り当てられたIPアドレス。これはピア アドレスと呼ばれます。

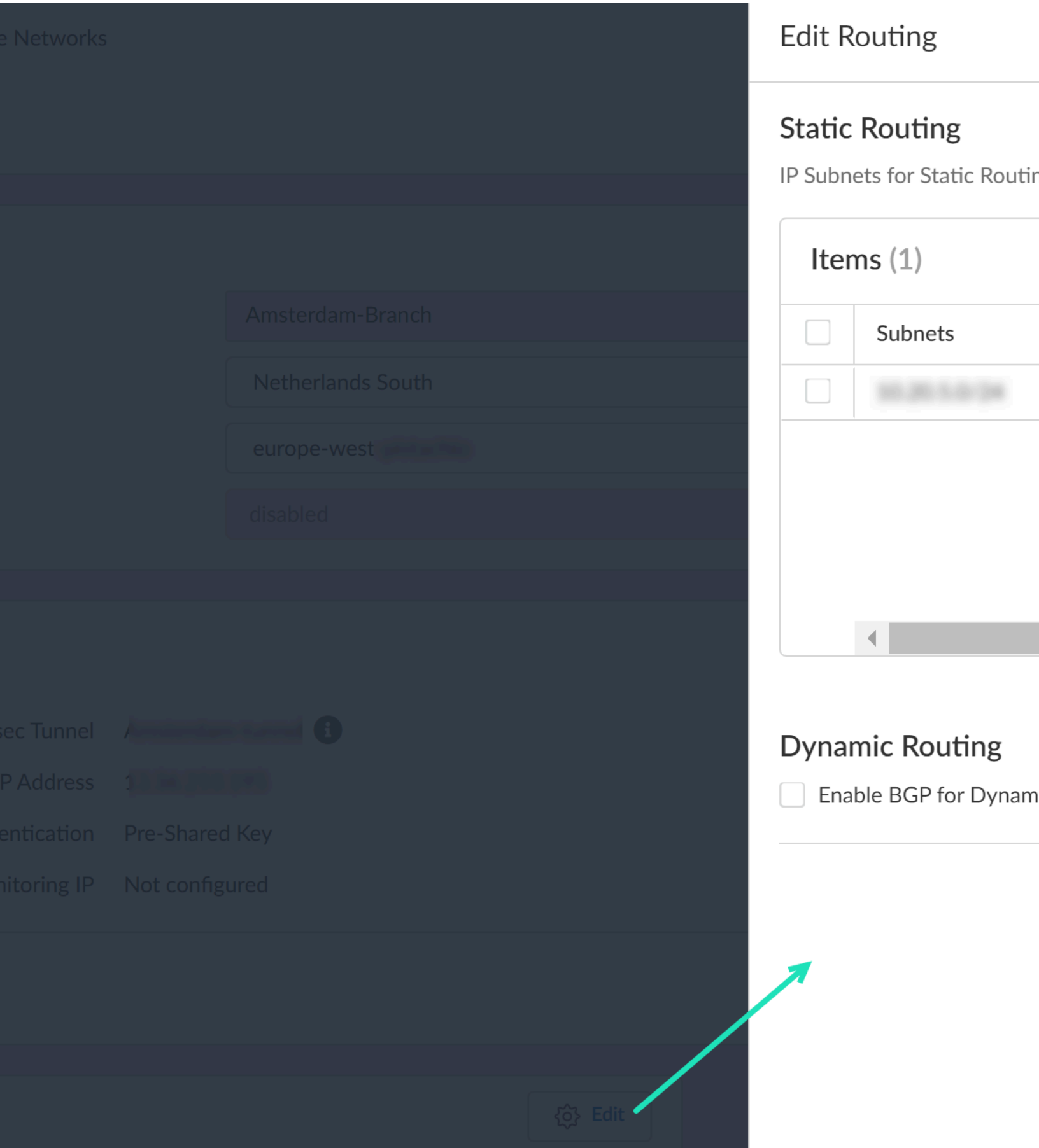
  スタティック ルートと BGP ルーティングの両方を設定した場合、スタティック ルートが優先されます。

リモート ネットワーク サイトのルーティング設定を構成する方法は次のとおりです。

©2025 Palo Alto Networks, Inc.

ルーティング設定を追加または調整するには、 **[Workflows (ワークフロー)]** > **[Prisma Accessセットアップ]** > **[Remote Networks (リモートネットワーク)]**に移動し、リモート ネットワーク サイトを追加または編集します。

©2025 Palo Alto Networks, Inc.



©2025 Palo Alto Networks, Inc.

スタティック ルートを設定します。

ブランチとの間のトラフィックをルーティングするためにスタティック ルートを使用している場合は、ブランチで保護するIPサブネットまたはIPアドレスを追加します 。ブランチのIPサブネットに変更を加えた場合は、スタティック ルートを手動で更新する必要があることに注意してください。

ダイナミック ルーティングを設定します。

ダイナミック ルーティングを使用してブランチ サブネットをアドバタイズするには、 ダイナミック ルーティングに対して**BGP**を有効にし 、次の設定を構成します。

- ルートをエクスポートしない- Prisma Accessがリモートネットワークにルートを転送しないようにします。

  デフォルトで、Prisma Accessは、ローカルルート、および他のサービス接続、リモートネットワーク、およびモバイルユーザーサブネットから受信するすべてのプレフィックスを含め、すべてのBGPルーティング情報をアドバタイズします。Prisma AccessによるBGPアドバタイズメントの送信を防止しながら、受信したBGP情報を使って、他のBGPネイバーからルートを学習するには、このチェック ボックスを選択します。

  > *Prisma AccessはBGPアドバタイズを送信しないため、このオプションを選択した場合は、Prisma Accessに戻るルートを確立するために、オンプレミス機器にスタティック ルートを設定する必要があります。*

- ピア**IP**アドレス- リモート ネットワーク上のeBGPルーターのルーターIDとして割り当てられたピアIPアドレスを入力します。
- ピア**AS**- ネットワークの自律システム (AS) であるピアASを入力します。

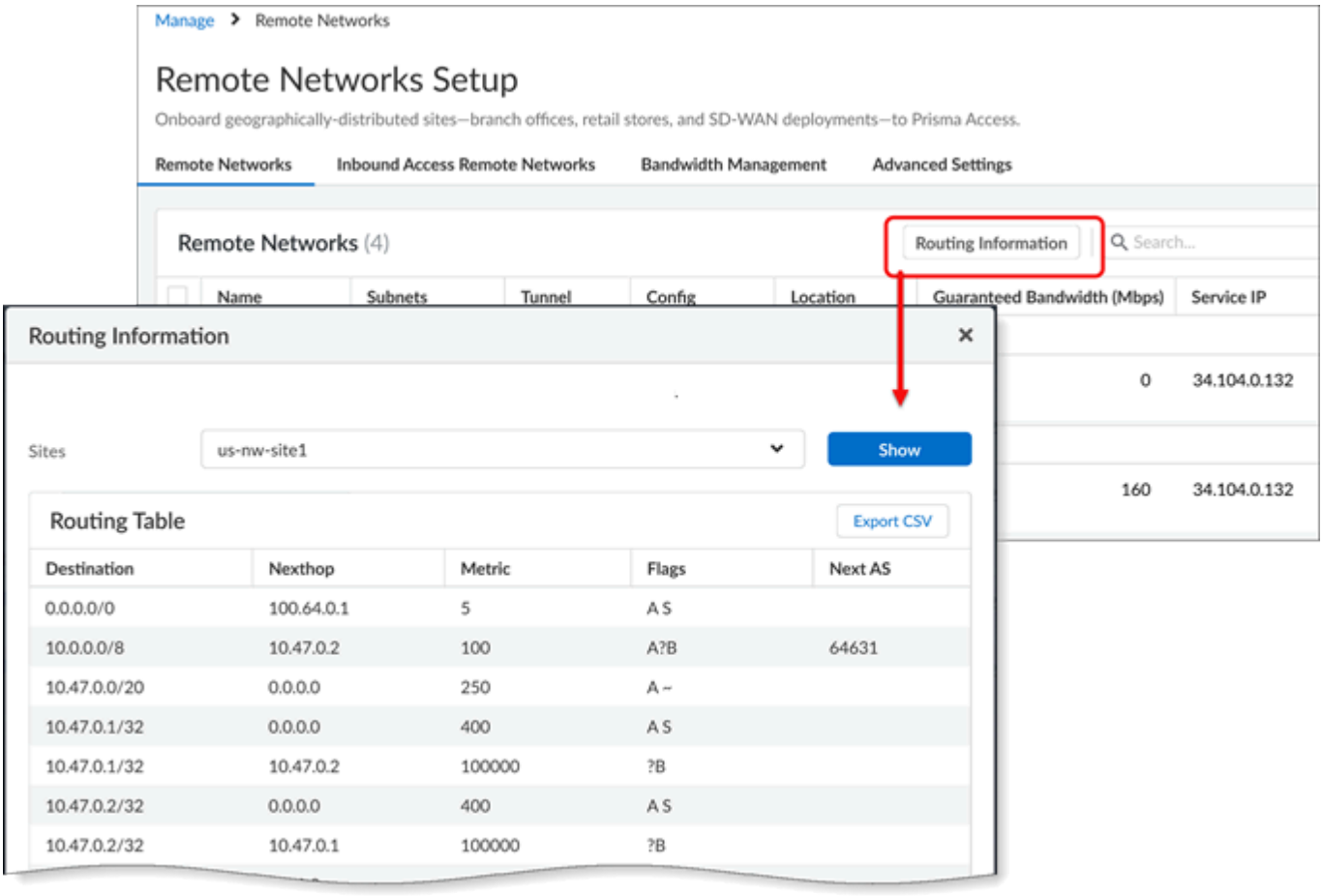
  RFC 6996 準拠のBGPプライベートAS番号を使用する必要があります。
- ローカル**IP**アドレス- Prisma AccessがBGPのローカルIPアドレスとして使用するIPアドレスを入力します。

  ローカル アドレスは、BGPピアリングを成功させるためにリモート サイト デバイスで必要な場合にのみ必要です。指定するIPアドレスは、インフラサブネットまたはリモートネットワーク内のサブネットのIPアドレスと、競合またはオーバーラップしていないことを確認してください。
- シークレット- BGP ピア通信を認証するためのシークレット パスワードを入力し、 シークレットを確認します。

サイト接続のトラブルシューティング

トラブルシューティングの目的で、リモート ネットワーク サイトまたはサービス接続サイトのルーティング テーブルを表示できるようになりました。リモート ネットワークまたはサービス接続ダッシュボードで ルーティング情報 ボタンを見つけます。

©2025 Palo Alto Networks, Inc.



©2025 Palo Alto Networks, Inc.

複数のリモートネットワークを搭載

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

リモート ネットワークのオンボードと構成のプロセスを効率化するために、少なくとも1つのリモート ネットワークをオンボードし、それらの設定をコンマ区切り値 (CSV) テキスト ファイルにエクスポートするオプションがあります。CSVファイルには、エクスポート用に選択したネットワークの、IPSecトンネルおよびIKEゲートウェイ設定に関する値が含まれており、それらの設定をオンボーディングする新たな各ネットワークに合わせて編集することができます。してCSVファイルに100件の新しいリモートネットワークを含めるように変更して、そのCSVファイルをインポートすると、新しいリモートネットワークロケーションのオンボーディング処理を高速化することができます。

CSVファイルに、BGP共有シークレット、IKE事前共有鍵、プロキシID、IKE暗号プロファイル、IPSec暗号プロファイルなどの、鍵やパスワードは含まれていません。そのため、IPSecトンネルおよびIKEゲートウェイ設定に必要な鍵やパスワードは、CSVファイルのインポート開始時に選択したネットワークから継承されます。

一括インポートを使用する場合、これらのロケーションを保護するために、Prisma Accessがインフラをデプロイするまで待機する必要があります。

STEP 1 | **Panorama** > **Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Remote Networks**（リモートネットワーク）の順に選択します（Onboarding（オンボーディング）セクション）。

STEP 2 | ロケーションを選択して、前にオンボーディングしたリモートネットワークの設定を**Export**（エクスポート）します。

まだ場所を追加していない場合は、場所を追加してから、その構成をダウンロードする必要があります。リモートネットワークを選択して、**Export**（エクスポート）をクリックする必要があります。設定が含まれているCSVファイルが、コンピュータにダウンロードされます。

STEP 3 | (コンピューティング場所によってのみ帯域幅を割り当てるデプロイメント) オンボードする場所に帯域幅が割り当てられていることを確認します。

オンボードする各ロケーションには、帯域幅が割り当てられる対応するコンピューティングロケーションがあります。

1. **[Panorama]** > **[Cloud Services (**クラウド サービス**)]** > **[Configuration (**構成**)]** > **Remote Networks (**リモート ネットワーク**)** を選択し、帯域幅割り当て 領域の歯車をクリックします。
2. 表示されるテーブルの帯域幅割り当てフィールドを確認します。

   このエリアの表は、コンピュートロケーションとPrisma Accessロケーションのマッピングを示したものです。オンボードする場所に関連付けられているコンピューティング

 ©2025 Palo Alto Networks, Inc.

場所に帯域幅を割り当てる必要があります。たとえば、日本中部のロケーションをオンボードするには、アジア北東部のコンピューティング ロケーションに帯域幅が割り当てられていることを確認します。

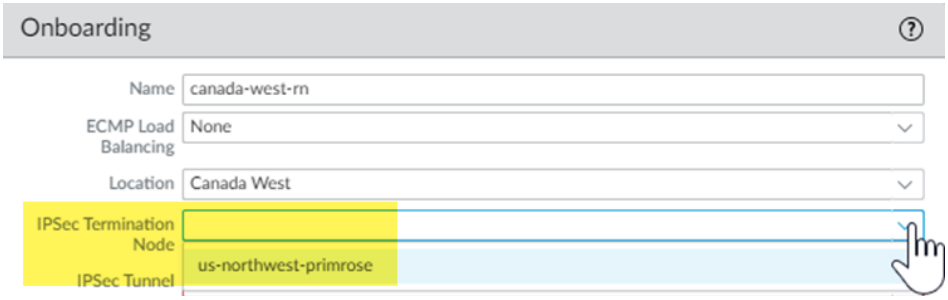
3. オンボードする場所に関連付けられているコンピューティング場所にまだ帯域幅を割り当てていない場合は、ここで追加します。

STEP 4 | (コンピューティング場所によってのみ帯域幅を割り当てるデプロイメント) オンボードする場所に関連付けられている**IPSec**終端ノードを見つけます。

オンボーディング中にリモート ネットワークに*IPSec* 終端ノードを割り当て、この値をCSVファイルの**spn-name**列に入力します。各IPSec終端ノードは最大1,000 Mbpsの帯域幅を提供できます。

IPSec終端ノードを見つけるには、次のいずれかのアクションを実行します。

- **Panorama** > **Cloud Services** > **Configuration** (構成) > リモート ネットワークリモート ネットワークの追加を選択し、オンボードする場所を選択して 、オンボーディング領域で選択した IPSec 終端ノードをメモします。



- Prisma Accessを管理するPanoramaでコマンドラインインターフェース（CLI）セッションを開き、 `show plugins cloud_services remote-networks agg-bandwidth region` *compute-location-name*と入力します。ここで、*compute-location-name* は、オンボードする場所に関連付けられているコンピューティングの場所です。IPSec 終端ノードが `spn-name-list` フィールドに表示されます。

STEP 5 | CSVファイルを編集して、リモートネットワーク用の設定を追加します。

このファイルのフィールドと取り得る値についてはリモート ネットワーク テーブルのフィールドを参照してください。

エクスポートしたファイルに記載されているネットワーク名は変更する必要があります。ファイルに重複する名前が存在していると、インポートは失敗します。

STEP 6 | CSVファイルを**Import**（インポート）します。

ファイルからの設定が画面に表示されます。ファイルをインポートすることを選択したリモートネットワークは、モデル設定としての役割を果たします。ファイルに記載されているリモートネットワークは、一意である必要がない鍵と未設定の値をモデルから継承します。

©2025 Palo Alto Networks, Inc.

STEP 7 | 変更をコミット、プッシュ配信します。

1. 変更内容を、**Commit**（コミット） > **Commit and Push**（コミットしてプッシュ）します。
2. **OK**、**Push**（プッシュ）の順にクリックします。

リモート ネットワーク テーブルのフィールド

リモートネットワークテーブル内のフィールドの説明を、次の表に示します。**Required**（必須）行が**Y**のフィールドは必須フィールドで、**N**のフィールドは任意です。

項目	詳説	必須？（はい/いいえ）
名前	リモートネットワーク名。	Y
bandwidth	(場所によってのみ帯域幅を割り当てる展開) リモート ネットワークに割り当てられた帯域幅。使用できる値： • 2 Mbps • 5 Mbps • 10 Mbps • 20 Mbps • 25 Mbps • 50 Mbps • 100 Mbps • 150 Mbps • 300 Mbps • 500 Mbps • 1000 Mbps *1000 Mbps*帯域幅オプションはプレビュー モードです。プレビュー中のスループットはベストエフォート方式で提供され、実際のパフォーマンスはトラフィックの組み合わせによって異なります。	Y
リージョン	リモート ネットワークの場所です。	Y

©2025 Palo Alto Networks, Inc.

項目	詳説	必須？（はい/いいえ）
	このドキュメントに記載されている通りにロケーションを入力してください（例：米国西部、または日本南部）。	
subnets	リモートネットワークのLAN側の、静的にルーティングされたサブネット。複数のサブネットはカンマで区切ります。	N
bgp_peer_as	リモートネットワークピアデバイスのBGP AS番号（ASN）。	N
bgp_peer_address	リモートネットワークピアデバイスのBGPピアアドレス。	N
tunnel_name	IPSecトンネル設定名。一意の値が必要です。	Y
gateway_name	IKEゲートウェイ設定名。一意の値が必要です。	Y
peer_ip_address	Prisma AccessピアデバイスのIPアドレスを入力します。	N
local_id_type	Prisma Accessがピアデバイスに提示する、IKE IDのタイプ。このファイルをインポートするリモートネットワークで証明書を使用する場合、指定されたすべてのインポートタイプは、Configured Certificate（設定された証明書）の値を参照します。	N
local_id_value	Prisma Accessがピアデバイスに提示する、IKE IDの値。このファイルをインポートするリモートネットワークで証明書を使用する場合、指定されたすべてのインポートタイプは、Configured Certificate（設定された証明書）の値を参照します。	N
peer_id_type	ピアがPrisma Accessに提示する、IKE IDの値。このファイルをインポートするリモートネットワークで証明書を使用する場合、指定されたすべてのインポートタイプは、Peer Certificate（ピア証明書）の値を参照します。	N
peer_id_value	Prisma Accessがピアデバイスに提示する、IKE IDの値。このファイルをインポートするリモートネットワークで証明書を使用する場合、指	N

©2025 Palo Alto Networks, Inc.

項目	詳説	必須？（はい/いいえ）
	定されたすべてのインポートタイプは、Peer Certificate（ピア証明書）の値を参照します。	
monitor_ip	クラウドが、IPSecトンネルが動作しており、ピアネットワークに到達可能であるかどうかを判断するために使用する、トンネル監視IPアドレス。 トンネルモニターのプロキシID値はエクスポートできません。	N
proxy_ids	ピア用に設定されたプロキシID。ルートベースのVPNの場合、このフィールドは空欄にしてください。プロキシIDを次のCSV構成形式で指定します: [{"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	セカンダリIPSecトンネルを有効にするかどうかを指定します。使用できる値はyesとnoです。	N
sec_tunnel_name	セカンダリIPSecトンネル設定名。セカンダリトンネルを指定する場合、一意の値が必要です。	N
sec_gateway_name	セカンダリIKEゲートウェイ設定名。セカンダリトンネルを指定する場合、一意の値が必要です。	N
sec_peer_ip_address	セカンダリIPSecトンネル用Prisma Accessピアデバイスの IPアドレス。	N
sec_local_id_type	Prisma Accessがセカンダリ IPSecトンネル用ピアデバイスに提示する、IKE IDのタイプ。このファイルをインポートするリモートネットワークで証明書を使用する場合、指定されたすべてのインポートタイプは、Configured Certificate（設定された証明書）の値を参照します。	N

©2025 Palo Alto Networks, Inc.

項目	詳説	必須？（はい/いいえ）
sec_local_id_value	Prisma AccessがセカンダリIPSecトンネル用ピアデバイスに提示する、IKE IDの値。このファイルをインポートするリモートネットワークで証明書を使用する場合、指定されたすべてのインポートタイプは、Configured Certificate（設定された証明書）の値を参照します。	N
sec_peer_id_type	ピアがセカンダリIPSecトンネル用Prisma Accessに提示する、IKE IDの値。このファイルをインポートするリモートネットワークで証明書を使用する場合、指定されたすべてのインポートタイプは、Peer Certificate（ピア証明書）の値を参照します。	N
sec_peer_id_value	Prisma AccessがセカンダリIPSecトンネル用ピアデバイスに提示する、IKE IDの値。このファイルをインポートするリモートネットワークで証明書を使用する場合、指定されたすべてのインポートタイプは、Peer Certificate（ピア証明書）の値を参照します。	N
sec_monitor_ip	クラウドが、IPSecトンネルが動作しており、ピアネットワークに到達可能であるかどうかを判断するために使用する、セカンダリIPSecトンネル用トンネル監視IPアドレス。 トンネルモニターのプロキシ*ID*値はエクスポートできません。	N
sec_proxy_ids	セカンダリIPSecトンネル用に設定されたプロキシID。ルートベースのVPNの場合、このフィールドは空欄にしてください。プロキシIDを次のCSV構成形式で指定します: [{"name":"*proxyidname*", "local":"*1.2.3.4/32*", "remote":"*4.3.2.1/32*", "protocol":{"udp": {"local-port":*123*, "remote-port":*234*}}}, {"name":"*proxyidname2*", "local":"*2.3.4.5/32*", "remote":"*3.4.5.6/32*", "protocol":{"tcp": {"local-port":*234*,"remote-port":*345*}}}]	N

©2025 Palo Alto Networks, Inc.

項目	詳説	必須？（はい/いいえ）
ecmp_link_1_tunnel_name	(ECMPデプロイメントのみ) ECMPトンネル1のIPSec トンネル構成の名前。一意の値が必要です。	
ecmp_link_1_gateway_name	(ECMPデプロイメントのみ) ECMP トンネル1のIKEゲートウェイ構成の名前。一意の値が必要です。	
ecmp_link_1_peer_ip_address	（ECMPデプロイメントのみ） ECMPトンネル1のPrisma Accessピア デバイスのIPアドレス。	
ecmp_link_1_local_id_type	（ECMPデプロイメントのみ）Prisma AccessがECMPトンネル1の相手デバイスに提示するIKE IDのタイプ。このファイルをインポートするリモートネットワークで証明書を使用する場合、指定されたすべてのインポートタイプは、Configured Certificate（設定された証明書）の値を参照します。	
ecmp_link_1_local_id_value	（ECMPデプロイメントのみ）Prisma AccessがECMPトンネル1の相手デバイスに提示するIKE IDの値。このファイルをインポートするリモートネットワークで証明書を使用する場合、指定されたすべてのインポートタイプは、Configured Certificate（設定された証明書）の値を参照します。	
ecmp_link_1_peer_id_type	（ECMPデプロイメントのみ）ECMPトンネル1に対して、ピアからPrisma Accessに提示されるIKE IDの値。このファイルをインポートするリモートネットワークで証明書を使用する場合、指定されたすべてのインポートタイプは、Peer Certificate（ピア証明書）の値を参照します。	
ecmp_link_1_peer_id_value	（ECMPデプロイメントのみ）Prisma AccessがECMPトンネル1の相手デバイスに提示するIKE IDの値。このファイルをインポートするリモートネットワークで証明書を使用する場合、指定されたすべてのインポートタイプは、Peer Certificate（ピア証明書）の値を参照します。	

©2025 Palo Alto Networks, Inc.

項目	詳説	必須？（はい/いいえ）
ecmp_link_1_monitor_ip	(ECMPデプロイメントのみ) クラウドがIPSecトンネルが稼働しており、ピア ネットワークがECMPトンネル1に到達可能であることを判断するために使用するトンネル監視IPアドレス。 トンネルモニターのプロキシ*ID*値はエクスポートできません。	
ecmp_link_1_proxy_ids	(ECMPデプロイメントのみ) ECMPトンネル1のピアに設定されているプロキシID。ルートベースのVPNの場合、このフィールドは空欄にしてください。プロキシIDを次のCSV構成形式で指定します: [{"name":"*proxyidname*", "local":"*1.2.3.4/32*", "remote":"*4.3.2.1/32*", "protocol":{"udp": {"local-port":*123*, "remote-port":*234*}}}, {"name":"*proxyidname2*", "local":"*2.3.4.5/32*", "remote":"*3.4.5.6/32*", "protocol":{"tcp": {"local-port":*234*,"remote-port":*345*}}}]	
ecmp_link_1_bgp_peer_as	(ECMPデプロイメントのみ) ECMPトンネル1のリモート ネットワーク ピア デバイスのBGP自律型システム番号 (ASN)。	
ecmp_link_1_bgp_peer_address	(ECMPデプロイメントのみ) ECMPトンネル1のリモート ネットワーク ピア デバイスのBGPピア アドレス。	
ecmp_link_2_tunnel_name	(ECMPデプロイメントのみ) ECMPトンネル2のIPSec トンネル構成の名前。一意の値が必要です。	
ecmp_link_2_gateway_name	(ECMPデプロイメントのみ) ECMP トンネル2のIKEゲートウェイ構成の名前。一意の値が必要です。	
ecmp_link_2_peer_ip_address	（ECMPデプロイメントのみ） ECMPトンネル2のPrisma Accessピア デバイスのIPアドレス。	
ecmp_link_2_local_id_type	（ECMPデプロイメントのみ）Prisma AccessがECMPトンネル2の相手デバイスに提示するIKE IDのタイプ。このファイルをインポー	

©2025 Palo Alto Networks, Inc.

項目	詳説	必須？（はい/いいえ）
	トするリモートネットワークで証明書を使用する場合、指定されたすべてのインポートタイプは、Configured Certificate（設定された証明書）の値を参照します。	
ecmp_link_2_local_id_value	（ECMPデプロイメントのみ）Prisma AccessがECMPトンネル2の相手デバイスに提示するIKE IDの値。このファイルをインポートするリモートネットワークで証明書を使用する場合、指定されたすべてのインポートタイプは、Configured Certificate（設定された証明書）の値を参照します。	
ecmp_link_2_peer_id_type	（ECMPデプロイメントのみ）ECMPトンネル2に対して、ピアからPrisma Accessに提示されるIKE IDの値。このファイルをインポートするリモートネットワークで証明書を使用する場合、指定されたすべてのインポートタイプは、Peer Certificate（ピア証明書）の値を参照します。	
ecmp_link_2_peer_id_value	（ECMPデプロイメントのみ）Prisma AccessがECMPトンネル2の相手デバイスに提示するIKE IDの値。このファイルをインポートするリモートネットワークで証明書を使用する場合、指定されたすべてのインポートタイプは、Peer Certificate（ピア証明書）の値を参照します。	
ecmp_link_2_monitor_ip	(ECMPデプロイメントのみ) クラウドがIPSecトンネルが稼働しており、ピア ネットワークがECMPトンネル2に到達可能であることを判断するために使用するトンネル監視IPアドレス。 トンネルモニターのプロキシ*ID*値はエクスポートできません。	
ecmp_link_2_proxy_ids	(ECMPデプロイメントのみ) ECMPトンネル2のピアに設定されているプロキシID。ルートベースのVPNの場合、このフィールドは空欄にしてください。プロキシIDを次のCSV構成形式で指定します:	

©2025 Palo Alto Networks, Inc.

項目	詳説	必須？（はい/いいえ）
	[{"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	(ECMPデプロイメントのみ) ECMPトンネル2のリモート ネットワーク ピア デバイスのBGP自律型システム番号 (ASN)。	
ecmp_link_2_bgp_peer_address	(ECMPデプロイメントのみ) ECMPトンネル2のリモート ネットワーク ピア デバイスのBGPピア アドレス。	
ecmp_link_3_tunnel_name	(ECMPデプロイメントのみ) ECMPトンネル3のIPSec トンネル構成の名前。一意の値が必要です。	
ecmp_link_3_gateway_name	(ECMPデプロイメントのみ) ECMP トンネル3のIKEゲートウェイ構成の名前。一意の値が必要です。	
ecmp_link_3_peer_ip_address	（ECMPデプロイメントのみ） ECMPトンネル3のPrisma Accessピア デバイスのIPアドレス。	
ecmp_link_3_local_id_type	（ECMPデプロイメントのみ）Prisma AccessがECMPトンネル3の相手デバイスに提示するIKE IDのタイプ。このファイルをインポートするリモートネットワークで証明書を使用する場合、指定されたすべてのインポートタイプは、Configured Certificate（設定された証明書）の値を参照します。	
ecmp_link_3_local_id_value	（ECMPデプロイメントのみ）Prisma AccessがECMPトンネル3の相手デバイスに提示するIKE IDの値。このファイルをインポートするリモートネットワークで証明書を使用する場合、指定されたすべてのインポートタイプは、Configured Certificate（設定された証明書）の値を参照します。	

©2025 Palo Alto Networks, Inc.

項目	詳説	必須？（はい/いいえ）
ecmp_link_3_peer_id_type	（ECMPデプロイメントのみ）ECMPトンネル3に対して、ピアからPrisma Accessに提示されるIKE IDの値。このファイルをインポートするリモートネットワークで証明書を使用する場合、指定されたすべてのインポートタイプは、Peer Certificate（ピア証明書）の値を参照します。	
ecmp_link_3_peer_id_value	（ECMPデプロイメントのみ）Prisma AccessがECMPトンネル3の相手デバイスに提示するIKE IDの値。このファイルをインポートするリモートネットワークで証明書を使用する場合、指定されたすべてのインポートタイプは、Peer Certificate（ピア証明書）の値を参照します。	
ecmp_link_3_monitor_ip	(ECMPデプロイメントのみ) クラウドがIPSecトンネルが稼働しており、ピア ネットワークがECMPトンネル3に到達可能であることを判断するために使用するトンネル監視IPアドレス。 トンネルモニターのプロキシ*ID*値はエクスポートできません。	
ecmp_link_3_proxy_ids	(ECMPデプロイメントのみ) ECMPトンネル3のピアに設定されているプロキシID。ルートベースのVPNの場合、このフィールドは空欄にしてください。プロキシIDを次のCSV構成形式で指定します: [{"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	(ECMPデプロイメントのみ) ECMPトンネル3のリモート ネットワーク ピア デバイスのBGP自律型システム番号 (ASN)。	

©2025 Palo Alto Networks, Inc.

項目	詳説	必須？（はい/いいえ）
ecmp_link_3_bgp_peer_address	(ECMPデプロイメントのみ) ECMPトンネル3のリモート ネットワーク ピア デバイスのBGPピア アドレス。	
ecmp_link_4_tunnel_name	(ECMPデプロイメントのみ) ECMPトンネル4のIPSecトンネル構成の名前。一意の値が必要です。	
ecmp_link_4_gateway_name	(ECMPデプロイメントのみ) ECMP トンネル4のIKEゲートウェイ構成の名前。一意の値が必要です。	
ecmp_link_4_peer_ip_address	（ECMPデプロイメントのみ） ECMPトンネル4のPrisma Accessピア デバイスのIPアドレス。	
ecmp_link_4_local_id_type	（ECMPデプロイメントのみ）Prisma AccessがECMPトンネル4の相手デバイスに提示するIKE IDのタイプ。このファイルをインポートするリモートネットワークで証明書を使用する場合、指定されたすべてのインポートタイプは、Configured Certificate（設定された証明書）の値を参照します。	
ecmp_link_4_local_id_value	（ECMPデプロイメントのみ）Prisma AccessがECMPトンネル4の相手デバイスに提示するIKE IDの値。このファイルをインポートするリモートネットワークで証明書を使用する場合、指定されたすべてのインポートタイプは、Configured Certificate（設定された証明書）の値を参照します。	
ecmp_link_4_peer_id_type	（ECMPデプロイメントのみ）ECMPトンネル4に対して、ピアからPrisma Accessに提示されるIKE IDの値。このファイルをインポートするリモートネットワークで証明書を使用する場合、指定されたすべてのインポートタイプは、Peer Certificate（ピア証明書）の値を参照します。	
ecmp_link_4_peer_id_value	（ECMPデプロイメントのみ）Prisma AccessがECMPトンネル4の相手デバイスに提示するIKE IDの値。このファイルをインポートするリモートネットワークで証明書を使用す	

©2025 Palo Alto Networks, Inc.

項目	詳説	必須？（はい/いいえ）
	る場合、指定されたすべてのインポートタイプは、Peer Certificate（ピア証明書）の値を参照します。	
ecmp_link_4_monitor_ip	(ECMPデプロイメントのみ) クラウドがIPSecトンネルが稼働しており、ピア ネットワークがECMPトンネル4に到達可能であることを判断するために使用するトンネル監視IPアドレス。 トンネルモニターのプロキシ*ID*値はエクスポートできません。	
ecmp_link_4_proxy_ids	(ECMPデプロイメントのみ) ECMPトンネル4のピアに設定されているプロキシID。ルートベースのVPNの場合、このフィールドは空欄にしてください。プロキシIDを次のCSV構成形式で指定します: [{"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	(ECMPデプロイメントのみ) ECMPトンネル4のリモート ネットワーク ピア デバイスのBGP自律型システム番号 (ASN)。	
ecmp_link_4_bgp_peer_address	(ECMPデプロイメントのみ) ECMPトンネル4のリモート ネットワーク ピア デバイスのBGPピア アドレス。	
spn-name	(コンピューティング場所によってのみ帯域幅を割り当てるデプロイメント) IPSec 終端ノードの名前。このフィールドは、コンピューティング場所ごとに帯域幅を割り当てるデプロイメントに必須です。	

©2025 Palo Alto Networks, Inc.

リモートネットワークがPrisma Accessに接続されているかどうかを確認する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

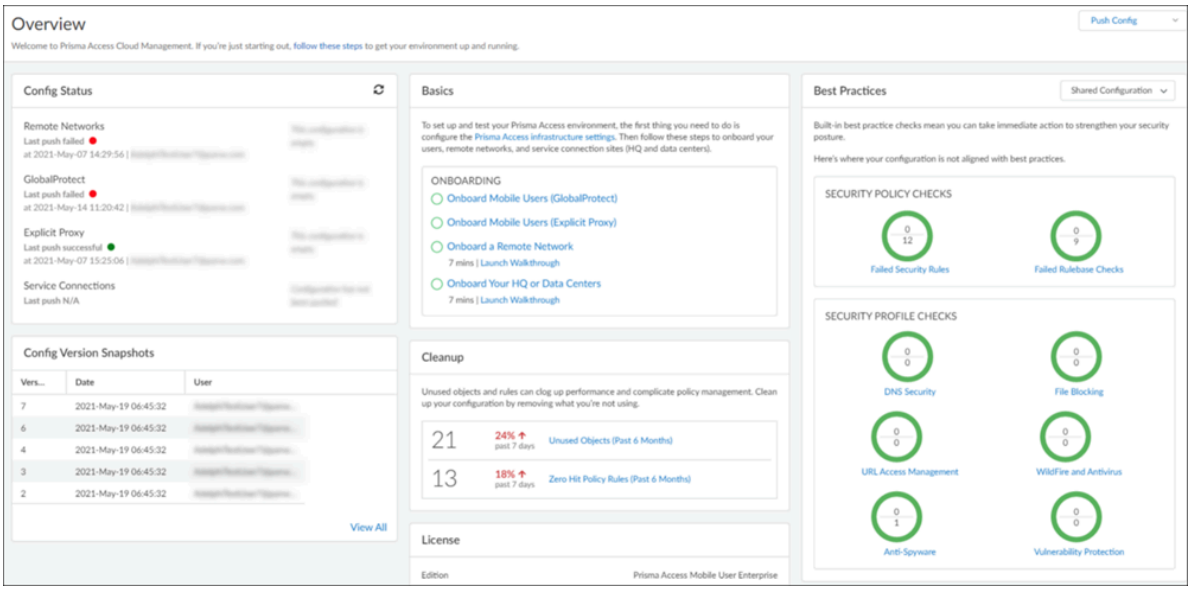
リモートネットワークでIPSec VPNデバイスを構成したら、トンネルのステータスを確認します。リモートネットワークの状態を確認するときは、次の点に注意してください。

- リモートネットワークへのIPsecトンネルの状態を確認します。
- リモートネットワークを検証する際の最後のステップは、ログを確認し、トラフィックがPrisma Accessを通過していることを確認することです。エラーまたは警告がある場合は、Prisma Accessでリモートネットワークデバイスのシステム ログインとローカルログを確認してください。設定に進む前に、エラーや警告をすべて解決してください。
- 必要に応じてリモートネットワークを追加し続けます。
- Strata Cloud Manager
- Panorama

リモートネットワークが接続されているかどうかを確認する Prisma Access （Strata Cloud Manager）

[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access]を選択し、**[Configuration Scope (設定スコープ)]** を **Prisma Access**に設定し、 **Prisma Access[Sync Status (同期ステータス)] > [Remote Networks (リモートネットワーク)]**を選びます。

©2025 Palo Alto Networks, Inc.



リモートネットワークが接続されているかどうかを確認する Prisma Access （Panorama）

STEP 1 | **Panorama** > **Cloud Services**（クラウドサービス） > **Status**（ステータス） > **Status**（ステータス）を選択して、リモートネットワーク接続が正常に展開されていることを確認します。

Deployment Status（デプロイステータス）では、オンボーディングおよびデプロイジョブのステータスを参照することができます。また、完了したジョブのステータスに関する詳細情報も参照することができます。

STEP 2 | 選択した地域内のリモートネットワークの、ロケーションを表しているマップを表示するには、**Panorama** > **Cloud Services**（クラウドサービス） > **Status**（ステータス） > **Monitor**（監視）の順に選択して、**Remote Networks**（リモートネットワーク）タブをクリックします。

STEP 3 | 地域を選択すると、その地域の詳細情報が表示されます。

©2025 Palo Alto Networks, Inc.

STEP 4 | マップの下にあるタブをクリックすると、その他のリモートネットワーク統計情報が表示されます。

Status（ステータス）タブ：

- **Location**（ロケーション）–リモートネットワークがデプロイされたロケーション。
- **Remote Peer**（リモートピア）–リモートネットワークが、IPSecトンネル接続を行っているピア。
- **IPSec**終端ノード- リモート ネットワークに関連付けられたIPSec終端ノード。このフィールドは、コンピューティング場所ごとに帯域幅を割り当てる場合にのみ表示されます。
- **ECMP**–リモートネットワーク接続で**ECMP Load Balancing**（**ECMP**ロードバランシング）が有効になっているかどうか。
- **Config Status**（設定ステータス）–サービスへの設定の最後のプッシュのステータス。ローカルで変更を行ったけれども、まだクラウドに設定をプッシュしていない場合、ステータスには**Out of sync**（非同期）が表示されます。ステータスインジケータ上にカーソルを移動すると、詳細情報が表示されます。設定をPrisma Accessにコミットしてプッシュすると、Config Statusが**In sync**になります。
- **BGP Status**（**BGP**ステータス）–リモートネットワークロケーションにあるファイアウォールまたはルーターと、Prisma Access間の、BGP状態に関する情報を表示します。一時的にステータスが各種BGP状態（**idle**、**active**、**open send**、**open pend**、**open confirm**）に切り替わることがありますが、一般的にBGPステータスには次のような項目が表示されます。
  - **Connect**（接続）–リモートネットワークロケーションのルーターが、Prisma AccessとのBGPピアリレーションシップの確立を試みています。
  - **Established**（確立済み）–BGPピアリレーションシップが確立されています。

    このフィールドには、BGP接続がエラー状態にあるかどうかも表示されます。
  - **Warning**（警告）–8分間以上に渡ってBGPステータスの更新がありません。ファイアウォールが機能停止している可能性があります。

©2025 Palo Alto Networks, Inc.

- **Error**（エラー）–BGPステータスが不明です。

- **Tunnel Status**（トンネルのステータス）–Prisma Accessとリモートネットワーク間の接続の運用ステータス。

Statistics（統計）タブ：

- **Location**（ロケーション）–リモートネットワークがデプロイされたロケーション。
- **Remote Peer**（リモートピア）–このリモートネットワークが、IPSecトンネルをセットアップしている、企業のロケーション。
- **Ingress Bandwidth (Mbps)**（入口帯域幅）–リモートネットワークのロケーションからPrisma Accessへの帯域幅。

  Ingress Bandwidth（入口帯域幅）、*Ingress Peak Bandwidth*（入口ピーク帯域幅）、*Egress Bandwidth*（出口帯域幅）、および*Egress Peak Bandwidth*（出口ピーク帯域幅）フィールドには、リモートネットワークの帯域幅消費が割り当てられている帯域幅の*80%*を超えた場合、数字が赤色で表示されます。
- **Ingress Peak Bandwidth (Mbps)**（入口ピーク帯域幅）–リモートネットワークのロケーションからクラウドサービスへのピーク負荷。
- **Engress Bandwidth (Mbps)**（出口帯域幅）–リモートネットワークのロケーションからPrisma Accessへの帯域幅。
- **Egress Peak Bandwidth (Mbps)**（出口ピーク帯域幅）–Prisma Accessからリモートネットワークのロケーションへのピーク負荷。

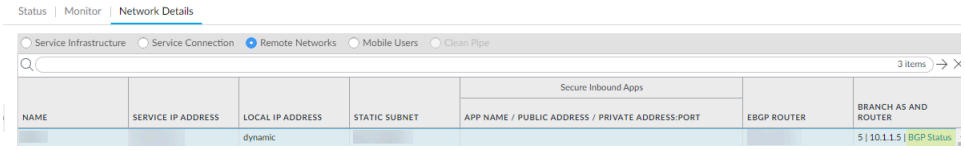
地域内の場所に関する統計情報を確認するには、[帯域幅の使用状況]を選択します。

詳細な帯域幅の使用状況を確認するには、場所のチェックマークを選択します。コンピューティングの場所ごとに帯域幅を割り当てるデプロイメントの場合、IPSec終端ノードを選択して、そのノードの統計情報を表示します。 Prisma Accessは、95パーセンタイル標準を使用して統計情報を収集します。この標準では、ピーク使用率での帯域幅を追跡し、使用率のピークと大きなバーストの上位5パーセントを無視します。

リモート接続BGPステータスの検証

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

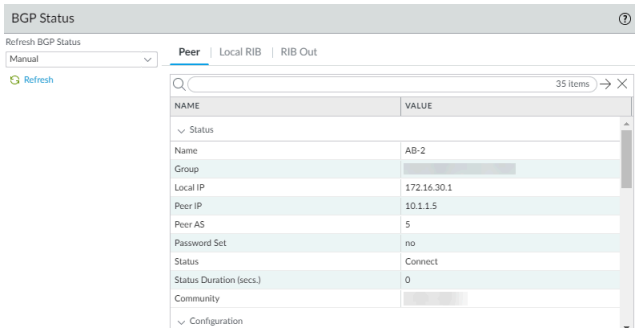
BGPを設定した場合、**[Panorama]** > **[Cloud Services**（クラウドサービス）**]** > **[Status**（ステータス）**]** > **[Network Details**（ネットワーク詳細）**]** > **[Remote Networks**（リモートネットワーク）**]** > **[BGP Status**（**BGP**ステータス）**]**の順に選択して、そのステータスを確認することができます。



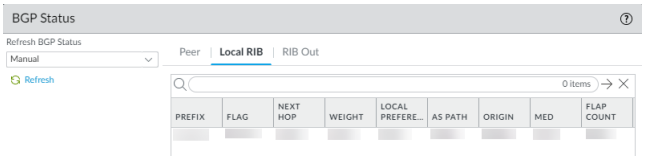
 ©2025 Palo Alto Networks, Inc.

BGP Status（BGPステータス）ダイアログが表示されます。このタブには、次の情報が表示されます。

- **Peer**（ピア）–ステータス、ルート数合計、設定、およびランタイム統計とカウンタを含む、BGPピアのルーティング情報。ルート数合計は**bgpAfiIpv4-unicast Counters**エリアの、**Incoming Total**（着信合計）および**Outgoing Total**（発信合計）フィールドに表示されます。



- **Local RIB**–各ピアから受信したルーティング情報で、ルーティング情報ベース（RIB）に保管されます。



- **RIB Out**–BGP更新メッセージを利用して、Prisma Accessがピアにアドバタイズするルーティング情報。このテーブルの例、およびBGPがモバイルユーザー向けに作成したIPアドレスプールをどのように活用するのかについては、「サービス接続およびリモートネットワーク接続用にBGPがモバイルユーザーIPアドレスプールをアドバタイズする仕組み」を参照してください。

©2025 Palo Alto Networks, Inc.

WAN リンクで接続されたリモート ネットワークとサービス接続を設定する

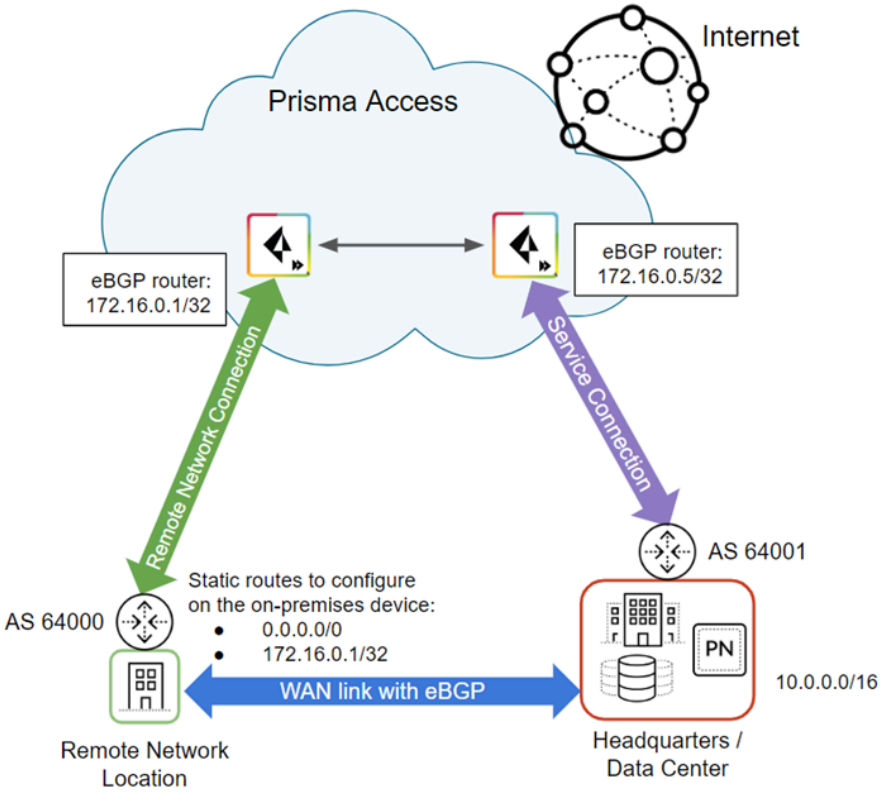
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

リモート ネットワークのロケーションと、サービス接続を備えたHQまたはデータ センターがWANリンクを介して直接接続されているデプロイメントの場合、最適なルーティング (eBGPを使用) を確保するには、次の操作を行う必要があります。

- eBGPルーターアドレスに、スタティック ルートを追加します。すべてのトラフィックをPrisma Accessに送信するデフォルトのルートに加えて、IPSec対応デバイスまたはリモートネットワークのルーターに、ローカルにスタティック ルートを追加する必要があります。
- IPSec対応デバイスまたは本社のルーターから、直接接続されているもう一方のロケーションのeBGPピアにアドバタイズされるルートをフィルタリングします。ベストプラクティスとして、WANリンクで許可するルートのみをアドバタイズするように本社のBGPルーターに設定し、本社のeBGPルーターがPrisma Accessから学習したルートを、Prisma Accessが保護するもう一方のリモートネットワークロケーションにアドバタイズしないようにすることをお勧めします。この例で、本社のeBGPルーターは、支店の従業員が本社サーバー（サブネット）に接続するために必要なルートのみをアドバタイズします。

本社ロケーションのサーバーに2つのパスを持つ、小売業の例を次の図に示します。片方のパスは、本社にあるサーバーにアクセスする従業員に、直接接続を提供するWANリンクです。もう一方のパスは、このロケーションのその他のユーザーが生成したトラフィックを保護します。たとえば、Wi-Fi経由または支店オフィスのkioskを使って小売業者のWebサイトにアクセスし、在庫を確認する顧客が生成したトラフィックがそれに該当します。このトラフィックは、リモートネットワークおよび本社へのトンネル経由で送信されます。

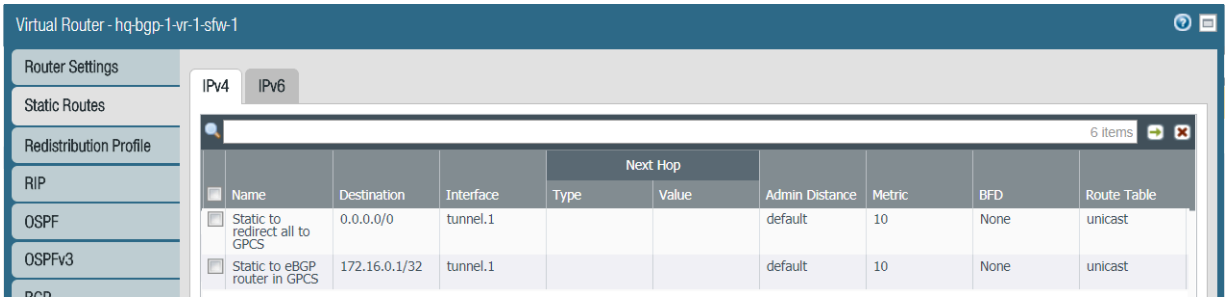
©2025 Palo Alto Networks, Inc.



この設定を行うには、リモートネットワーク接続を作成して、サービス接続を作成し、リモートネットワークと本社ロケーションをオンボーディングします。最適なルーティングを実現するための、各ロケーションでのルーター設定のセットアップ方法を以下に示します。

STEP 1 | ルーターまたはリモートネットワークロケーションにあるオンプレミスIPSec対応デバイスに、スタティック ルートを追加します。

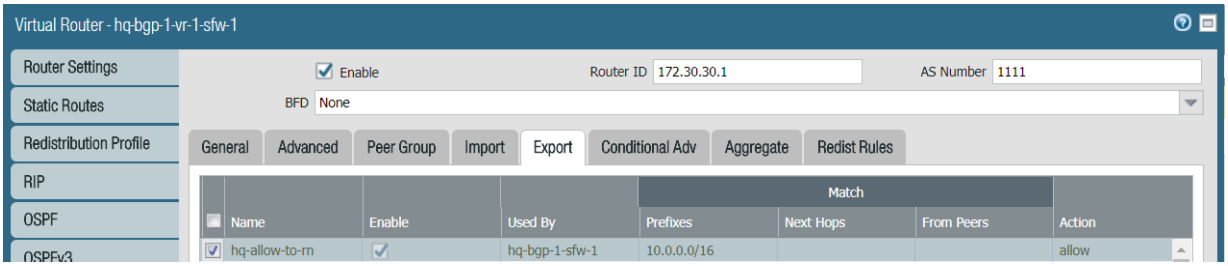
WANリンクの末端にPalo Alto Networksファイアウォールがある場合、**Network**（ネットワーク） > **Virtual Routers**（仮想ルーター） > **Static Routes**（スタティックルート）の順に選択して、スタティックルートを**Add**（追加）します。



 ©2025 Palo Alto Networks, Inc.

STEP 2 | WANリンクで直接接続されている、もう一方のロケーションにアドバタイズするルートを設定します。

この例では、本社ロケーションでこの設定を行う必要があります。WANリンクの終端にPalo Alto Networksファイアウォールがある場合、ルートの再配信をセットアップして、**Network**（ネットワーク） > **Virtual Routers**（仮想ルーター） > **BGP**で、エクスポートするBGPルートを設定します。



 ©2025 Palo Alto Networks, Inc.

リモートネットワークのQoS

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス ❑ Minimum Required Prisma Access Version:3.0 Preferred

新しいPrisma Accessデプロイメントでは、コンピュートロケーション別にリモートネットワークの帯域幅がオンボードされます。リモート ネットワークでQoSを使用するには、QoSを有効または無効にし、コンピューティング場所レベルで保証される帯域幅を指定します。ただし、サイトごとに帯域幅をカスタマイズすることで、場所ごとにQoSと保証帯域幅を調整できます。

Prisma Accessは*IPSec* 終端ノードを使用してコンピューティング ロケーションの帯域幅を分割します。各IPSec終端ノードは最大1,000 Mbpsの帯域幅を提供できます。コンピューティング拠点に1,000Mbps以上の帯域幅を割り当てると、 Prisma Accessは追加のIPSec終端ノードを提供します。

- Strata Cloud Manager
- Panorama

リモートネットワークのQoS（Strata Cloud Manager）

QoSを使用して、リモート ネットワーク内の重要なトラフィックを優先し、コンピューティング ロケーションのリモート ネットワーク サイトの最大帯域幅と保証帯域幅を設定します。

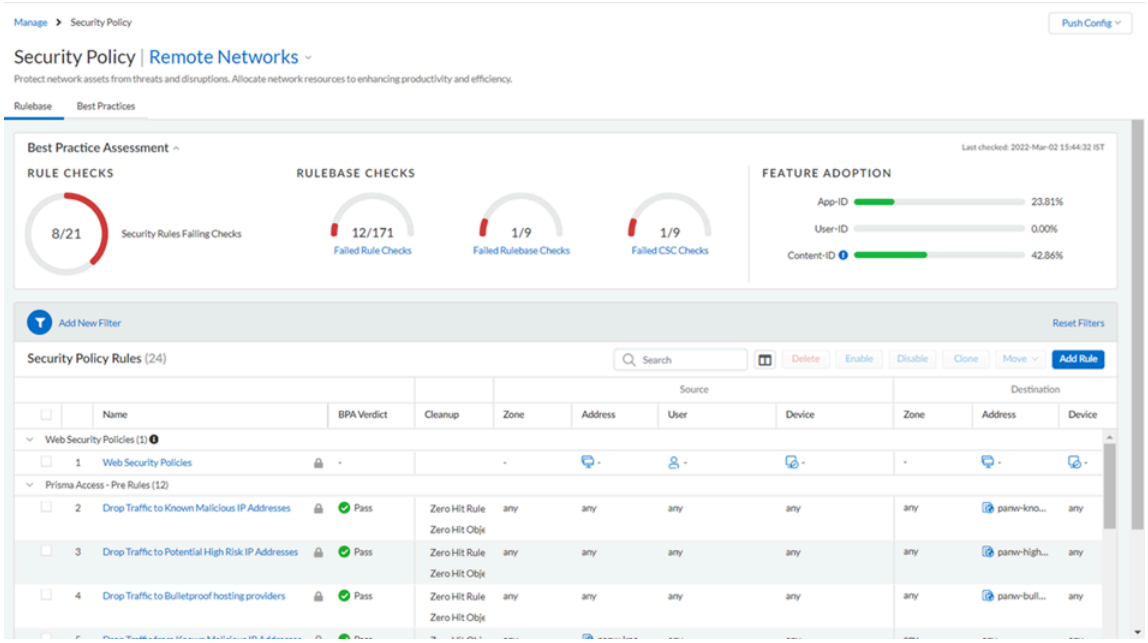
©2025 Palo Alto Networks, Inc.

STEP 1 | QoS処理を受けるトラフィックをマークします。

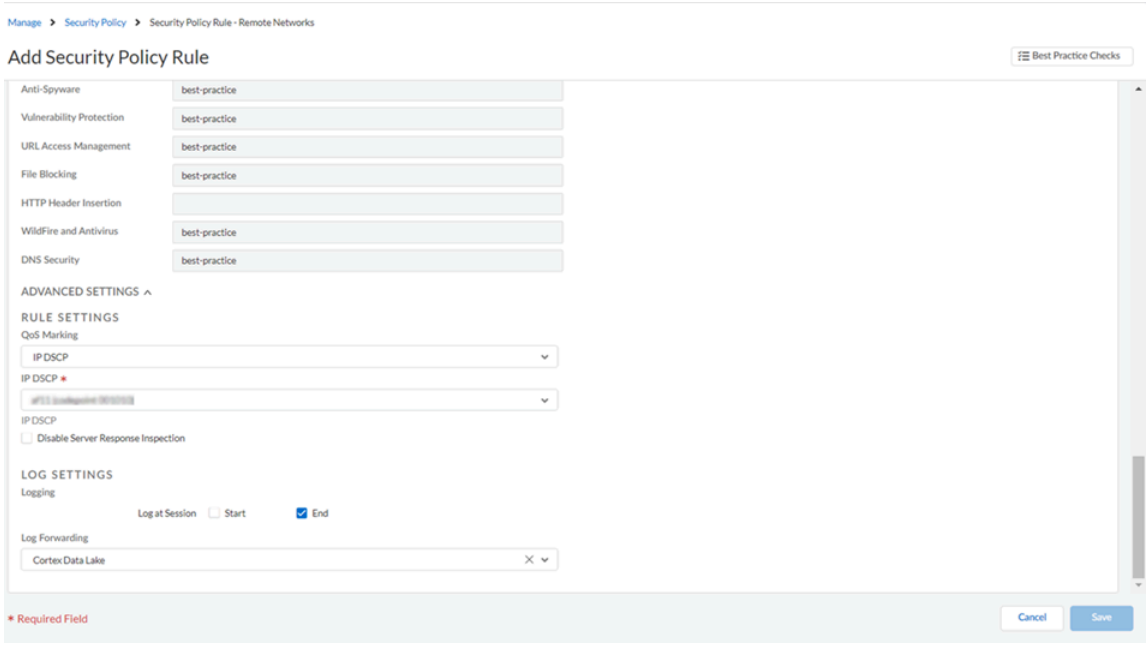
1. **[Manage (管理)] > [Configuration (設定)] > [NGFW]Prisma Access > [Security Services (セキュリティ サービス)] > [Security Policy (セキュリティ ポリシー)]**を選択します。

   リモート ネットワーク用のポリシーを作成していることを確認します。

2. ルールを追加します。



3. 詳細設定 でDSCP値を割り当てて着信トラフィックをマークし、ポリシーを保存します。

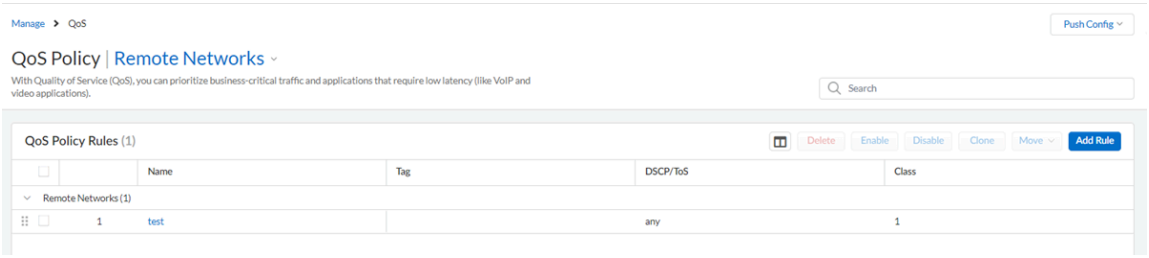


 ©2025 Palo Alto Networks, Inc.

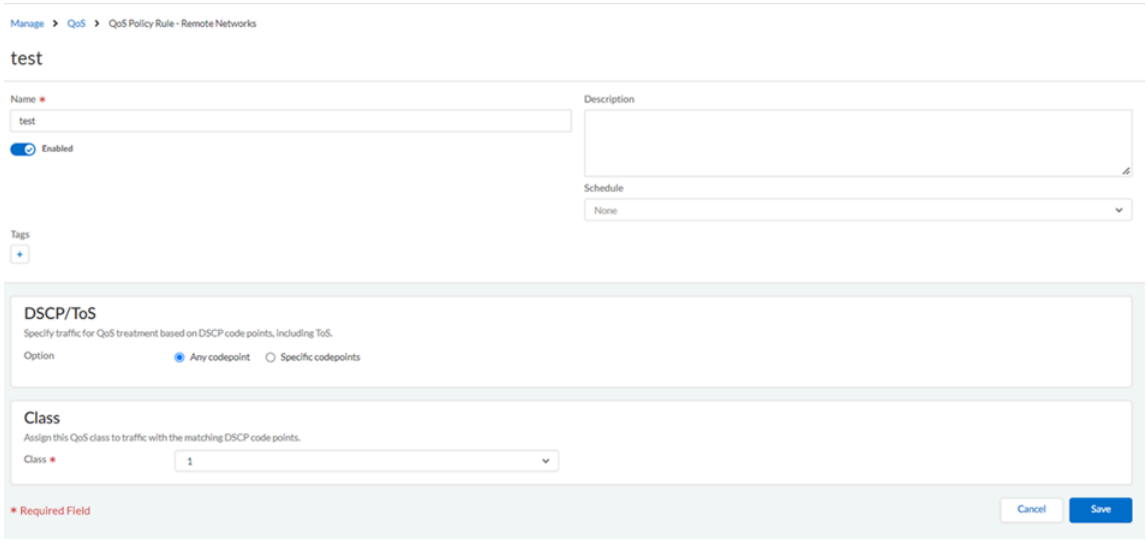
STEP 2 | 1つまたは複数のQoSポリシールールを追加します。

DSCPマーキングを利用可能な8つのクラスのいずれかにバインドするには、QoSポリシーを使用します。次の手順で、QoSクラスが受ける処理を定義します。QoSクラスにより、QoSポリシー ルールにマッチしたトラフィックの優先度と帯域幅が決まります。

1. **[Monitor (監視)]** > **[Network Services (ネットワーク サービス)]** > **[QoS]**を選択して開始します。
2. ルールを追加します。



3. 値を入力してポリシーを保存します。



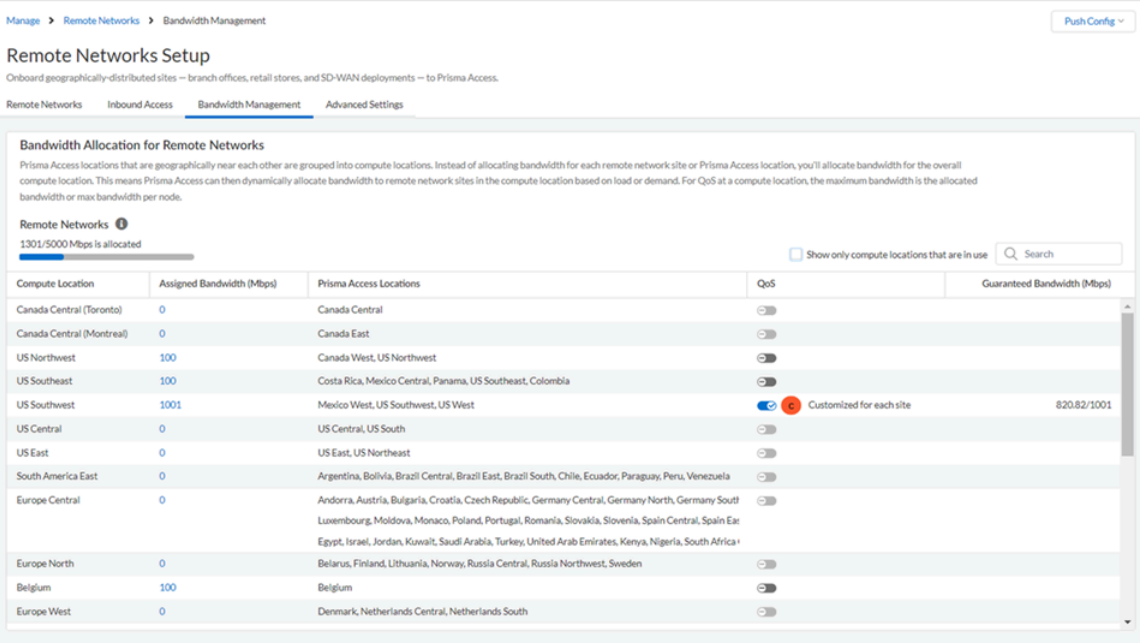
 ©2025 Palo Alto Networks, Inc.

STEP 3 | リモート ネットワークの場所で QoS を有効にします。

1. **[Manag (管理)] > [Service Setup (サービスセットアップ)] > [Remote Networks (リモートネットワーク)] > [Bandwidth Management (帯域幅管理)]**を選択します。
2. QoSをデプロイしたいPrisma Accessロケーションを決定し、各Prisma Accessロケーションに対応するコンピューティング ロケ ーションを見つけてください。

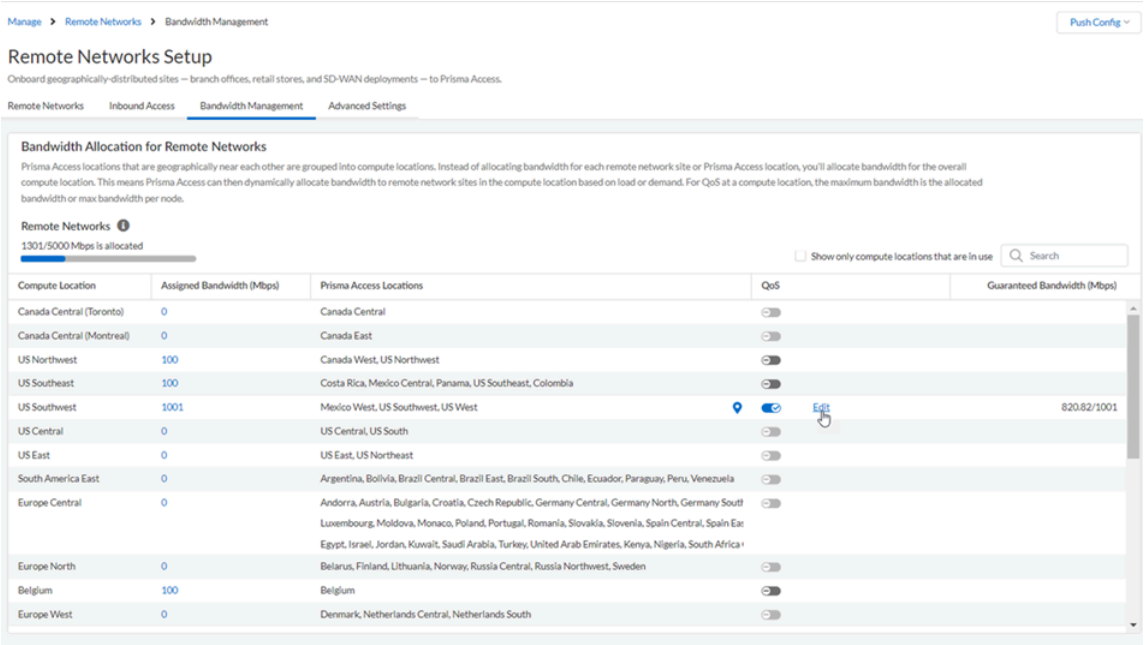
   それぞれのPrisma Accessロケーションにはコンピューティング ロケ ーションから帯域幅が割り当てられるため、QoS を割り当てる場所のコンピューティング場所の名前を知っておく必要があります。
3. **QoS**列のコンピューティング ロケーションレベルでQoSを有効にします。

   入力した設定は、このコンピューティング ロケーションに対応するすべての場所に適用されます。



 ©2025 Palo Alto Networks, Inc.

STEP 4 | コンピューティング ロケ ーションのQoS設定を編集します 。



1. 保証帯域幅比率を選択します。これは、コンピューティング ロケーションに割り当てられた帯域幅全体に基づく比率です。

   たとえば、米国南西部のコンピューティング ロケーションに1001 Mbpsの帯域幅を割り当て、 保証帯域幅比率 を82%と入力した場合、そのコンピューティング ロケーションの保証帯域幅は820.82 Mbpsになります。

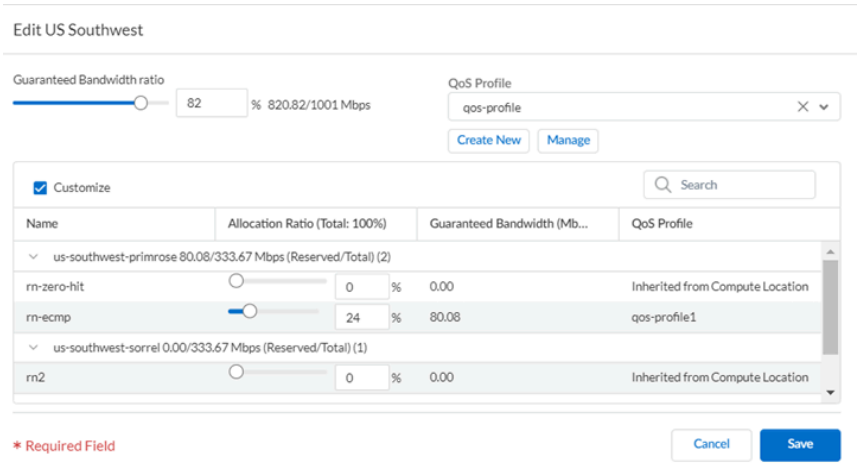
   デフォルトでは、各リモート ネットワークには接続数に等しいパーセンテージが割り当てられます。たとえば、コンピューティング ロケーションに4つの接続があり、合計保証帯域幅が820.82 Mbpsの場合、各ロケーションはその帯域幅の25%である205.2 Mbpsを受け取ります。

   AIOps搭載ADEMライセンスが有効になっている場合、ライセンスはすべてのコンピューティング ロケ ーションで自動的に有効になります。
2. QoSプロファイルを新規作成する か、既存の QoS プロファイルを 管理します 。

   出口ポイントでトラフィックを形成するには、QoSプロファイルを使用します。
3. (任意) コンピューティング ロケーションのリモート ネットワーク サイトの QoS 設定をカスタマイズします。コンピューティング ロケーションごとに複数のリモート ネットワークがあり、各リモート ネットワークの帯域幅比率またはQoSプロファイルを変更

©2025 Palo Alto Networks, Inc.

する場合は、[カスタマイズ] を選択し、帯域幅割り当て比率、QoSプロファイル、またはその両方を変更します。



[カスタマイズ] を選択し、同じ*IPSec*終端ノードに追加のリモート ネットワークをオンボードすると、新しくオンボードされたサイトの割り当て比率は*0*になり、既存のサイトと新しくオンボードされたサイト間の割り当て比率を手動で再調整する必要があります。

STEP 5 | 変更を保存します。

STEP 6 | 設定をプッシュします 。

リモートネットワークのQoS（Panorama）

Prisma AccessでQoSを設定するには、次の作業を実施します。

©2025 Palo Alto Networks, Inc.

STEP 1 | QoSの着信トラフィックをマーキングするために、リモートネットワークおよびモバイルユーザー向けのセキュリティポリシールールを、1つまたは複数追加します。

これらのポリシーを使ってトラフィックフローを照合し、それに選択したDSCP値を割り当てます。

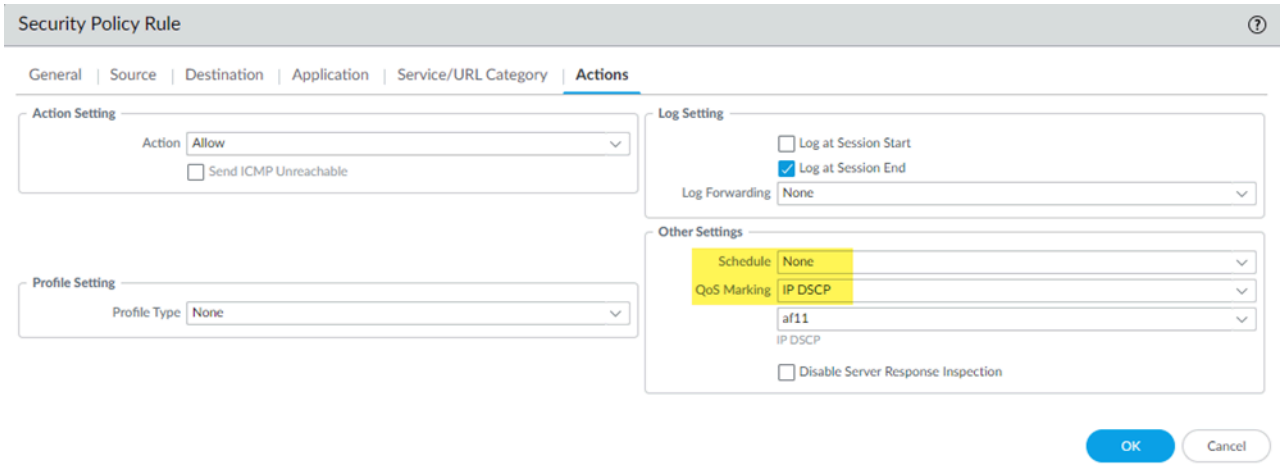
1. **[Policies**（ポリシー）**] > [Security**（セキュリティ）**] > [Pre Rules**（プレルール）**]**を順に選択します。

   代わりに、**Policies**（ポリシー） **> Security**（セキュリティ） **> Post Rules**（ポストルール）を選択して、プレルール後に評価されるルール順序の最後に、ルールを追加します。

   正しい***Device Group***（デバイスグループ）を選択していることを確認してください。リモートネットワークのセキュリティルールを作成するには、リモートネットワークのデバイスグループを選択（例：***Remote_Network_Device_Group***）します。モバイルユーザーの場合は、モバイルユーザー用デバイスグループを選択（例：***Mobile_User_Device_Group***）します。
2. セキュリティポリシー ルールを**Add**（追加）します。
3. ルールの **Name [名前]** を入力します。
4. パケットの送信元または宛先フィールド用の一致条件を定義します。

   詳細は、「セキュリティポリシールールの作成」を参照してください。
5. **Actions**（アクション）をクリックして、次に**QoS Marking**（**QoS**マーキング）で**IP DSCP**または**IP Precedence**を選択します。
6. QoS値をバイナリ形式で入力するか、またはドロップダウンリストから値を選択します。

   次のスクリーンショットは、**IP DSCP**値**af11**がマーキングされているトラフィックと一致する、セキュリティポリシールールを表しています。



©2025 Palo Alto Networks, Inc.

STEP 2 | 1つまたは複数のQoSポリシールールを追加します。

DSCPマーキングを利用可能な8つのクラスのいずれかにバインドするには、QoSポリシーを使用します。後ほど、1つまたは複数のQoSプロファイルを作成する際に、これらのクラスを使用します。

1. **[Policies**（ポリシー）**] > [QoS] > [Pre Rules**（プレ ルール）**]**を選択します。

   代わりに Post Rules (ポスト ルール)(**Policies**（ポリシー） **> QoS > Post Rules**（ポスト ルール）)を選択して、プレ ルール後に評価されるルール順序の最後に、ルールを追加します。

   サービス接続は*QoS*ポストルールをサポートしていません。サービス接続にはプレルールのみを使用してください。

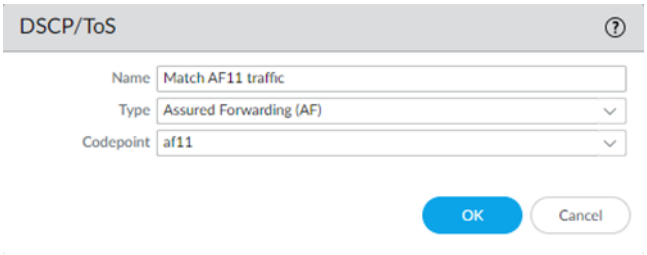
   サービス接続に対する正しい**Device Group**（デバイスグループ）（例：**Service_Conn_Device_Group**）、またはリモートネットワーク接続に対する正しいデバイスグループ（例：**Remote_Network_Device_Group**）を選択していることを確認してください。Shared（共有）デバイスグループ内のルールに、**General**（全般）、**DSCP/ToS**,および**Other**（その他）設定値以外の値が定義され

©2025 Palo Alto Networks, Inc.

ている場合、Prisma Accessはリモートネットワークおよびサービス接続にルールを適用されません。

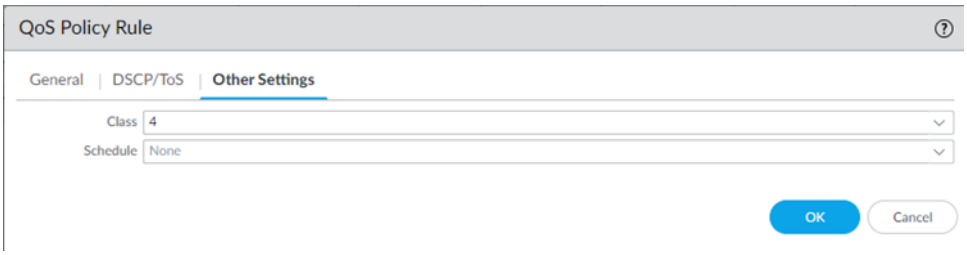
2. QoSポリシー ルールを**Add**（追加）します。
3. **General**（全般）をクリックし、ポリシールールの名前を入力します。
4. **DSCP/ToS**タブをクリックしてから、**Codepoints**（コードポイント）をクリックし、1つまたは複数のコードポイントを**Add**（追加）します。

   クリーンパイプのデプロイメントでは、ソース、宛先、またはアプリケーションなどのポリシーに追加のQoS設定を指定できます。
5. DSCP/ToSルールの**Name**（名前）を指定して、次に**Type**（タイプ）と**Codepoint**（コードポイント）を選択します。



   代わりに、デフォルト値の**Any**（任意）をそのまま使用して、トラフィックに定義されているDifferentiated Services Code Point（DSCP）値またはIP優先度/Type of Service（ToS）にかかわらず、ポリシーをトラフィックと照合します。
6. **Other Settings**（その他の設定）タブをクリックして、次にルールに割り当てるQoS **Class**（クラス）を選択します。

   QoSプロファイルにクラス特性を定義します。
7. **OK** をクリックします。



STEP 3 | サービス接続およびリモートネットワーク接続のQoSトラフィックを、発信時にシェーピングするには、1つまたは複数のQoSプロファイルを作成します。

QoSクラスを定義してそれらに帯域幅を割り当てることで、プロファイルを使って発信ポイントでトラフィックをシェーピングできます。Prisma Access向けにQoSを有効にする場合、既存のQoSプロファイルを選択するか、または新しいQoSプロファイルを作成する必要があります。

1. 作成するプロファイルに対して正しいテンプレート（**Remote_Network_Template**または**Service_Conn_Template**）を選択して、次に**Network**（ネットワーク） > **Network Profiles**（ネットワークポリシー） > **QoS Profile**（QoSプロファイル）の順に選択します。次に

 ©2025 Palo Alto Networks, Inc.

2. プロファイルを**Add**（追加）します。
3. プロファイル **Name**（名前）を入力します。
4. そのQoSプロファイルルール用の合計帯域幅の制限を設定します。
   - サービス接続またはリモートネットワーク接続から送信されるトラフィックの最大スループット（Mbps）を、**Egress Max**（発信最大帯域幅）に入力します。
     - サービス接続の場合、最高で1 Gpbs（1,000 Mbps）までの値を指定します。

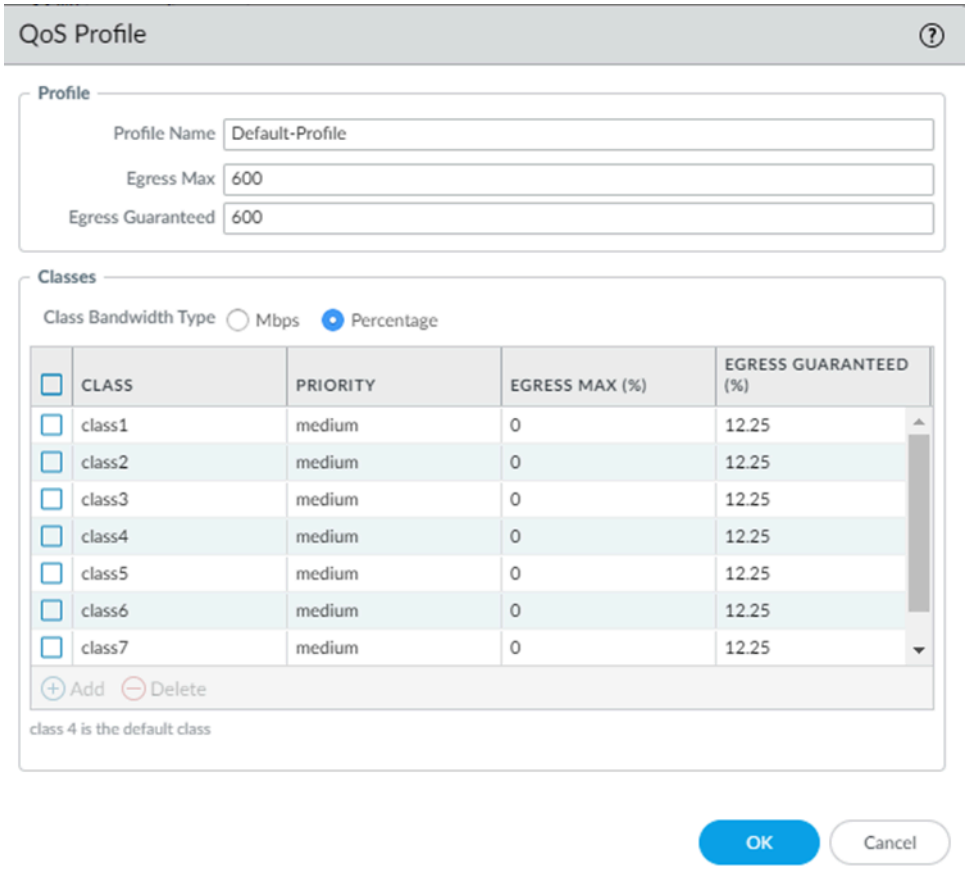
       *1 Gbps*を超える数字を入力しないでください。*Prisma Access*は、サービス接続ごとの*IPSec*トンネルのサービス接続帯域幅を計算し、複数のトンネル全体で累積的には計算しません。
   - リモートネットワーク接続の場合、0の値を入力してください。
   - **Egress Guaranteed**（発信最低保証帯域幅）値に、このプロファイルで保証されている帯域幅（Mbps）を入力します。
     - サービス接続には、**Egress Guaranteed**（発信最低保証帯域幅）に、このプロファイルで保証されている帯域幅（Mbps）を入力します。

       Egress Guaranteed [最低保証帯域 出力側]の値を超えるトラフィックは、ベストエフォートで、保証されません。保証されているが未使用の帯域幅は、すべてのトラフィックが利用できる状態のままになります。
     - リモートネットワーク接続の場合、0の値を入力してください。
5. Classes（クラス）セクションで、1つまたは複数のクラスを**Add**（追加）し、8つの個別のQoSクラスにマーキングする方法を指定します。
   - リモートネットワークによって計算場所で帯域幅を割り当てるために使用されるQoSプロファイルについて、クラス帯域幅タイプをパーセンテージに変更し、この領域に入力する**Egress Max (**出力側**MAX)**および**Egress Guaranteed (**最低保証帯域 出力側**)**値のパーセンテージを入力します。
   - サービス接続や場所によって帯域幅を割り当てるリモートネットワークによって使用されるQoSプロファイルについては、**Mbps**のタイプを指定してください。
   - クラスの **Priority (**優先順位**)** を選択します（(**real-time**（リアルタイム）、**high**（高）、**medium**（中）、または**low**（低）)）。
   - 作成した各QoSクラスに割り当てられたトラフィックの、**Egress Max**（発信最大帯域幅）を入力します。
     - 計算場所によって帯域幅を割り当てるリモートネットワークの場合は、**0**を入力してください。
     - 帯域幅ベースのQoSプロファイル（サービス接続や場所によって帯域幅を割り当てるリモートネットワークで使用される）については、Mbps単位で値を入力してください。QoSクラスのEgress Max（発信最大保証帯域幅）は、QoSプロファイルに定義されたEgress Max以下でなければなりません。

©2025 Palo Alto Networks, Inc.

- 各QoSクラスに対して、**Egress Guaranteed**（発信保証帯域幅）パーセンテージまたは帯域幅をMbpsで入力します。リモートネットワークのQoSプロファイルについて、パーセンテージを入力してください。

  あるクラスに対し割り当てられた保証帯域は、そのクラスのために確保されているわけではなく、未使用の帯域はすべてのクラスで使用可能な状態になっています。トラフィックのクラスが発信保証帯域幅を超えた場合Prisma Accessはそのトラフィックをベストエフォート方式で通過させます。
- プロファイルのクラス帯域幅タイプを入力してください。



6. **OK** をクリックします。

STEP 4 | （サービス接続のみ）サービス接続でQoSを有効にし、QoSプロファイルを接続に適用します。

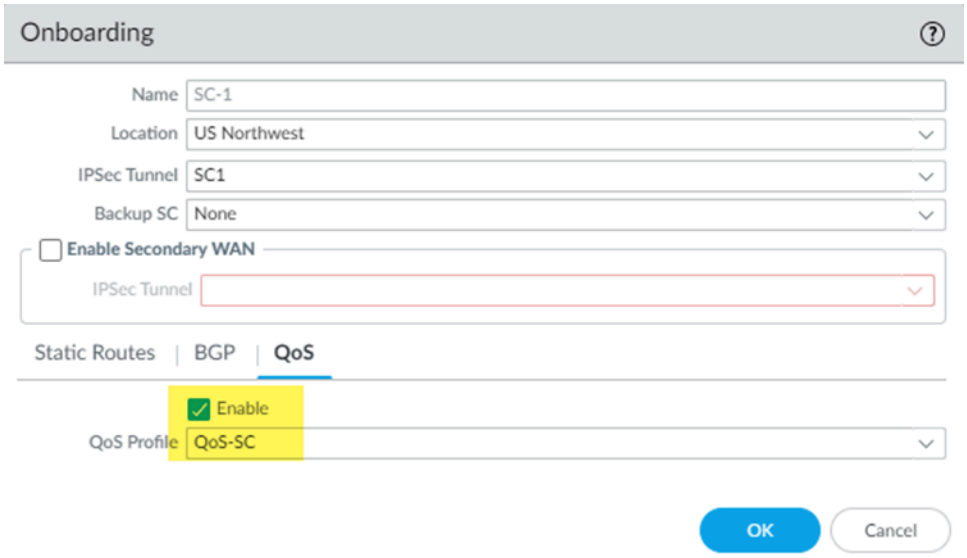
1. QoSを有効にするには、**[Panorama]** > **[Cloud Services]** > **[Configuration (設定)]** > **[Service Setup (サービスセットアップ)]**を選択し、接続名を選択し、**QoS**タブをクリックしてから、QoSを有効にします。

   リモートネットワークの帯域幅を、計算場所ではなくPrisma Accessリモートネットワークで割り当てる場合は、サービス接続と同じ方法でQoSを構成する。**[Panorama]** > **[Cloud Services**（クラウドサービス）**]** > **[Configuration**（設定）**]** > **[Remote Networks**（リモートネットワーク）**]**の順に選択して、リモートネットワーク接続の**Name**（名前）のハイパーテキストを選択し、**QoS**タブをクリックし

©2025 Palo Alto Networks, Inc.

て、QoSを**Enable**（有効）にします。計算場所によって帯域幅を割り当てる場合（デフォルトの方法）、ステップ5に進み、リモートネットワークのQoSを設定します。

2. QoSプロファイルを選択し、**OK**をクリックします。



STEP 5 | （計算場所によって帯域幅を割り当てるリモート ネットワーク デプロイメント）リモートネットワークの場所でQoSを有効にします。

1. QoSをデプロイしたいPrisma Accessロケーションを決定し、各ロケーションに対応するコンピューティング ロケ ーションを見つけてください。

   それぞれのロケーションにはコンピューティング ロケ ーションから帯域幅が割り当てられるため、QoS を割り当てる場所のコンピューティング場所の名前を知っておく必要があります。計算場所間のマッピングのリストについては、Prisma Accessロケーションを参照するか、**[Panorama] > [Cloud Services] > [Configuration (設定)] > Remote Networks (リモートネットワーク) > [Aggregate Bandwidth (帯域幅の集約)]**を選択し、ギアアイコンをクリックしてください。マッピングは、コンピューティングロケーションおよび**Prisma Access Location**の列に表示されます。

2. **Panorama > Cloud Services (クラウドサービス) > Configuration (設定) > Remote Networks (リモートネットワーク) > Settings (設定)**を選択し、設定を編集するためにギアをクリックし、**QoS**を選択します。

3. コンピューティング ロケーション レベルで**QoS**を有効にします。

   入力した設定は、このコンピューティング ロケーションに対応するすべての場所に適用されます。

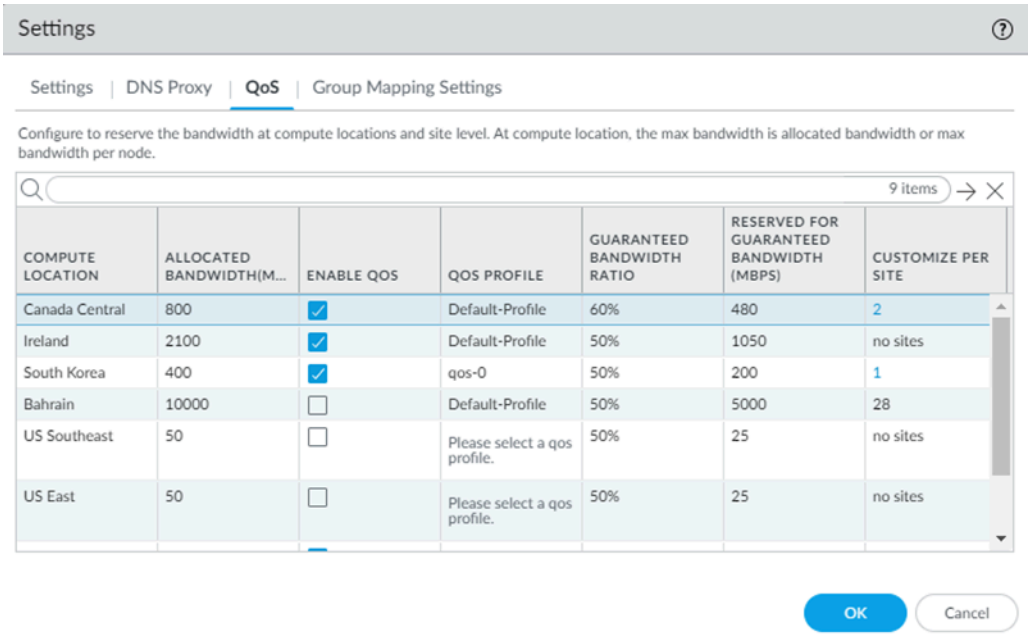
©2025 Palo Alto Networks, Inc.

4. **QoS**プロファイル、保証された帯域幅比、および保証された帯域幅（**Mbps**）を入力します。
   - このコンピュート場所で使用する**QoS**プロファイルを入力してください。

     リモートネットワークごとに異なるQoSプロファイルを使用したい場合は、後のステップで説明されているように、**[Customize Per Site (**サイトごとにカスタマイズ**)]**を使用してください。
   - 保証帯域幅比率を入力します。これは、コンピューティング ロケーションに割り当てられた帯域幅全体に基づく比率です。

     たとえば、Canada Centralのコンピュートロケーションに800 Mbpsの帯域幅を割り当てた場合、**Guaranteed Bandwidth Ratio (**保証帯域幅比**)**に**60%**を入力すると、そのコンピュートロケーションの保証帯域幅は480 Mbpsになります。
   - 選択したQoSプロファイルおよびコンピュートロケーションで、**Reserved for Guaranteed Bandwidth**（保証帯域幅として予約されている帯域幅）（**Mbps**）を入力します。

   次のスクリーンショットは、カナダ中部、アイルランド、韓国のコンピュートロケーションでQoSが有効になっていることを示しています。



5. (任意) コンピュートロケーションごとに複数のリモートネットワーク接続があり、各ロケー ションの帯域幅比率またはQoSプロファイルを変更する場合は、リモートネットワークロケーショ ンをオンボードし、**[Customize Per Site (**サイトごとにカスタマイ

©2025 Palo Alto Networks, Inc.

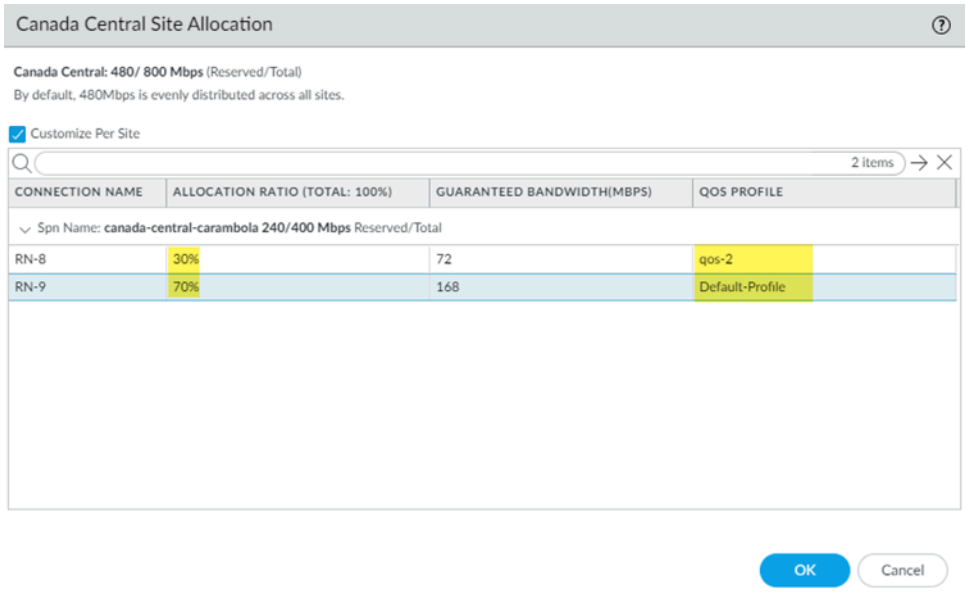
ズ)]を選択して、帯域幅割り当て比率、QoSプロファイル、 またはその両方を変更します。

- 保証帯域幅をカスタマイズするには、**[Customize Per Site(サイトごとにカスタマイズ)]**領域の数値をクリックし、**[Customize Per Site(サイトごとにカスタマイズ)]**を選択して、**[Allocation Ratio (配分比率)]**を変更します。

  デフォルトでは、各リモート接続には接続数に等しいパーセンテージが割り当てられます。たとえば、コンピューティング ロケーションに4つの接続があり、合計保証帯域幅が100 Mbpsの場合、各ロケーションはその帯域幅の25%である25 Mbpsを受け取ります。

  > ***[Customize Per Site (サイトごとにカスタマイズ)]*** を選択し、同じ*IPSec*終端ノードに追加のリモート ネットワークをオンボードすると、新しくオンボードされたサイトの割り当て比率は***0***になり、既存のサイトと新しくオンボードされたサイト間の割り当て比率を手動で再調整する必要があります。
  >
  > サイトごとにカスタマイズしない場合、リモートネットワークを追加すると帯域幅の割合が自動的に再調整されます。例えば、サイトごとにカスタマイズを選択しなかった場合、*4*つのリモートネットワークがオンボードされていると、それぞれのリモートネットワークの配分比率は*25%*です。もし*5*番目のリモートネットワークを追加すると、*5*つのサイトすべてが再バランスされ、保証された帯域幅*20%*を受け取ります。

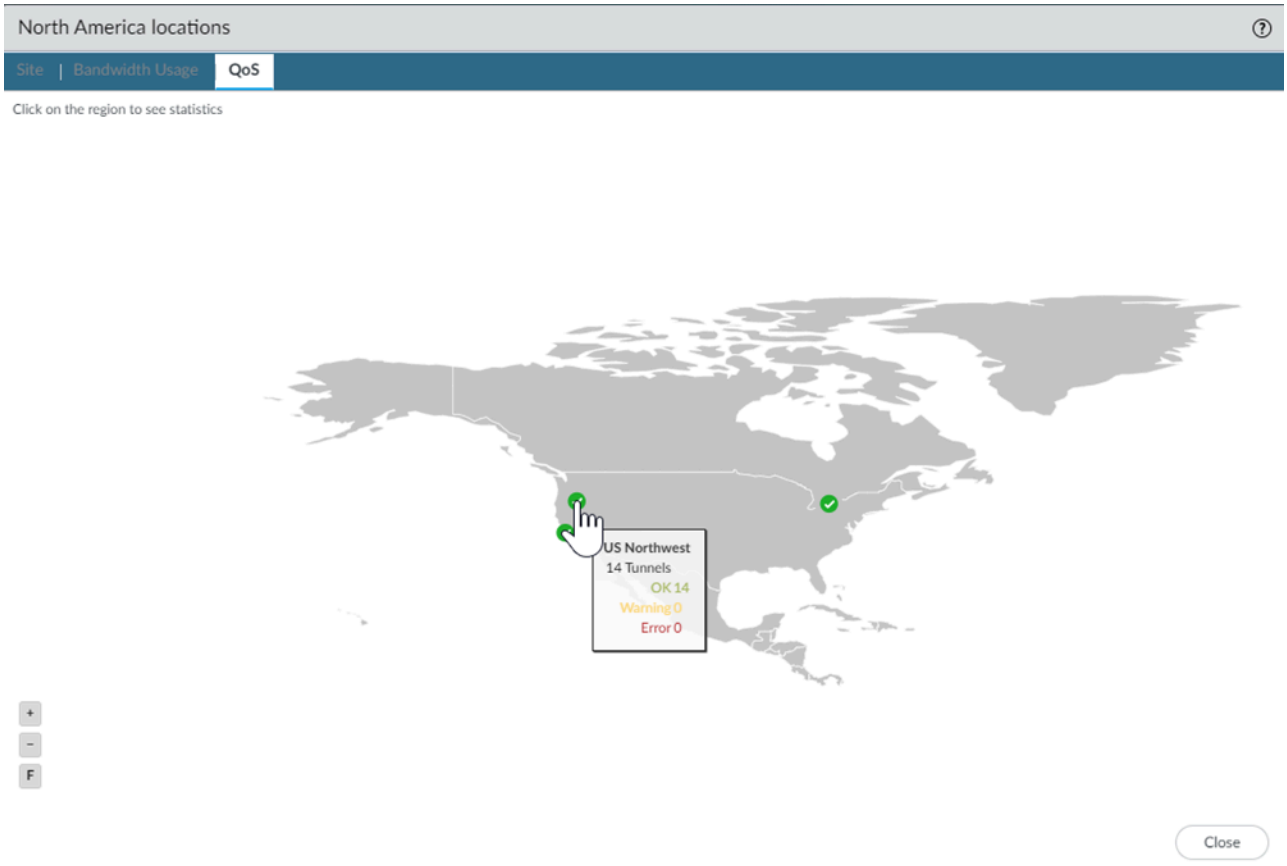
- リモートネットワークレベルでQoSプロファイルを指定したい場合は、リモートネットワークのために異なる**QoS**プロファイルを選択してください。



©2025 Palo Alto Networks, Inc.

STEP 6 | QoSステータスを確認します。

- リモートネットワークの場合、**[Panorama]** > **[Cloud Services (クラウドサービス)]** > **[ステータス]** > **[Monitor (監視)]** > **[Remote Networks (リモートネットワーク)]**を選択し、**QoS**を選択し、次に場所を選択します。

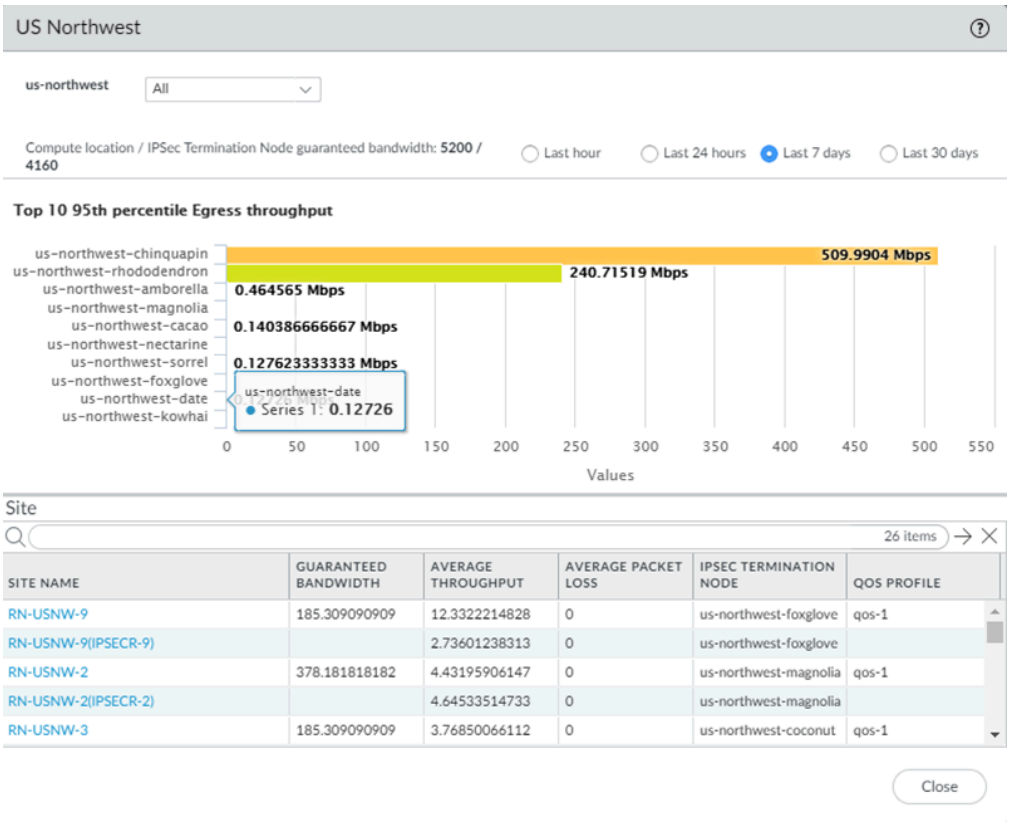


最も高いスループットを持つ10のIPSec終端ノードのリモート・ネットワーク統計表示。 Prisma Accessは統計情報の収集に95パーセンタイル標準を使用し、利用率のピー

 ©2025 Palo Alto Networks, Inc.

ク時の帯域幅を追跡し、利用率のピークや大きなバーストの上位5パーセントを無視します。

時間範囲（過去**1**時間、過去**24**時間、過去**7**日間、過去**30**日間）を選択すると、その期間の統計が表示されます。

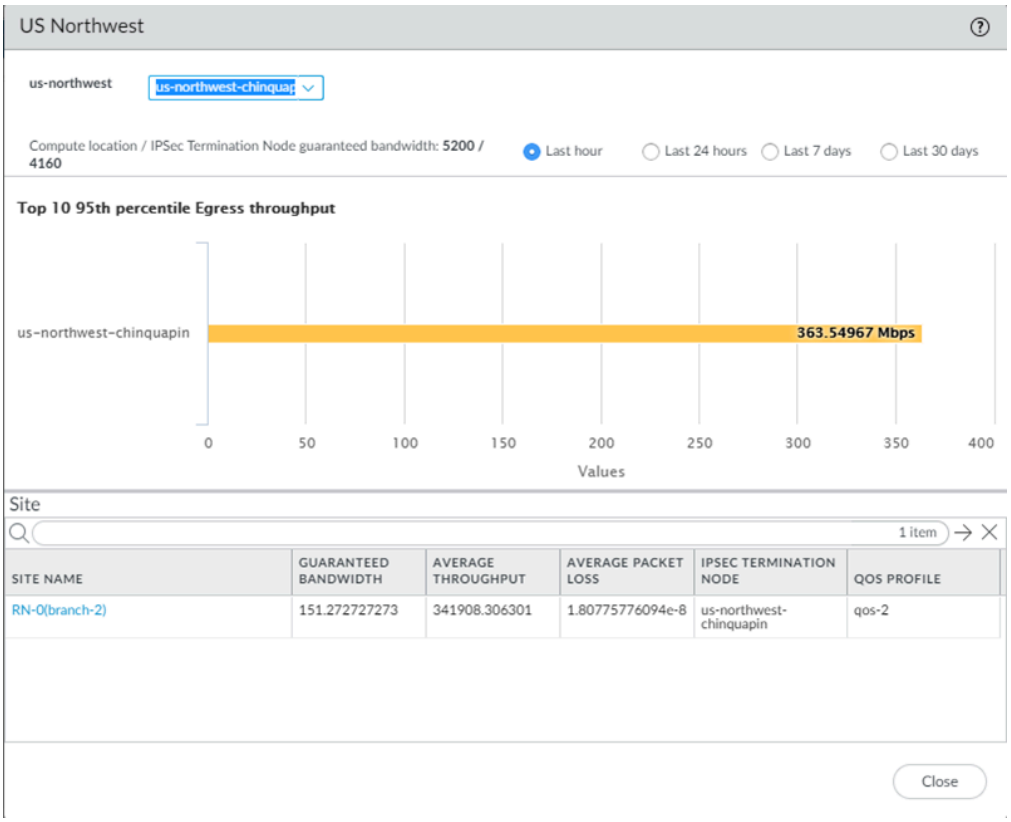


最も高いイグジット帯域幅を使用しているリモートネットワークは、保証帯域幅、平均スループット、平均パケットロス、およびリモートネットワークで使用されてい

 ©2025 Palo Alto Networks, Inc.

るIPSec終端ノードとQoSプロファイルのリモートネットワークの場所の統計情報とともに、サイト領域に表示されます。ロケーションを検索することもできます。

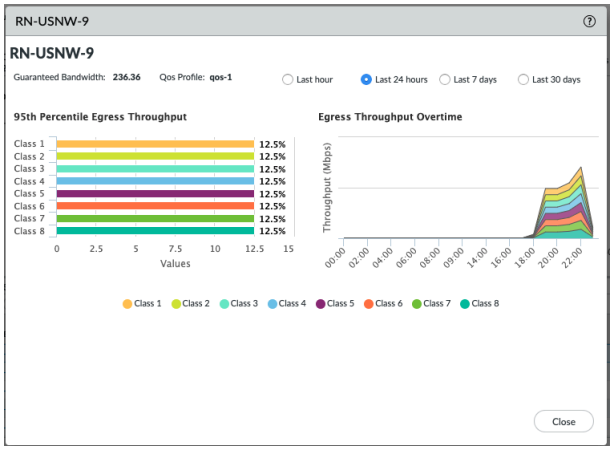
特定のIPSec終端ノードに関連付けられたリモートネットワークを表示するには、ページの上部にあるドロップダウンを「すべて」から特定のIPSec終端ノードに変更して、そのIPSec終端ノードおよびそのサイトのリモートネットワークの統計を表示します。



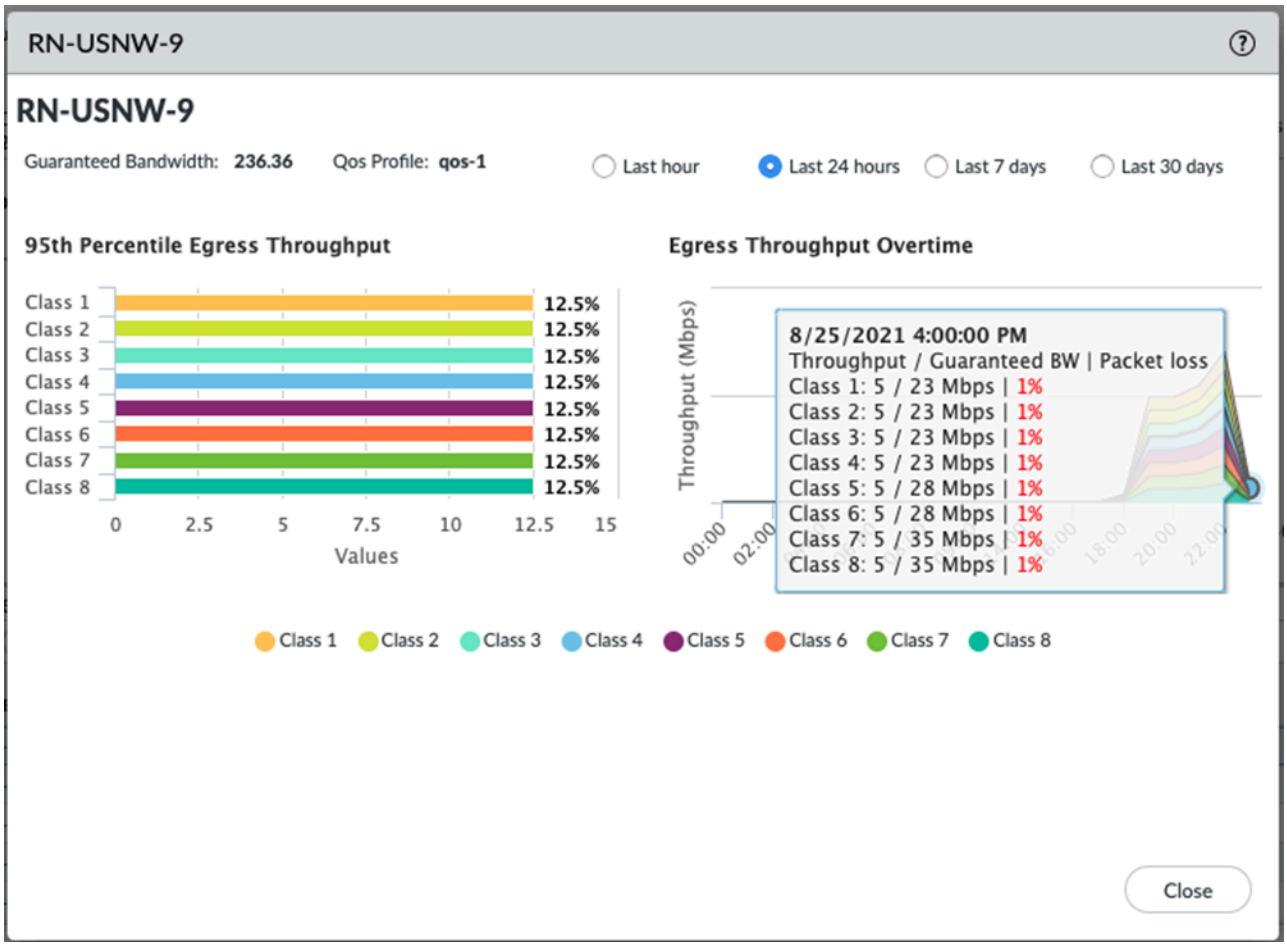
特定のトラフィックをQoSクラスでソートしてサイトを表示するには、サイト名をクリックしてください。リモートネットワークサイトの保証された帯域幅、出口スルー

©2025 Palo Alto Networks, Inc.

プット、および時間にわたるスループット表示。この情報を過去1時間、過去24時間、過去7日間、または過去30日間でソートすることもできます。



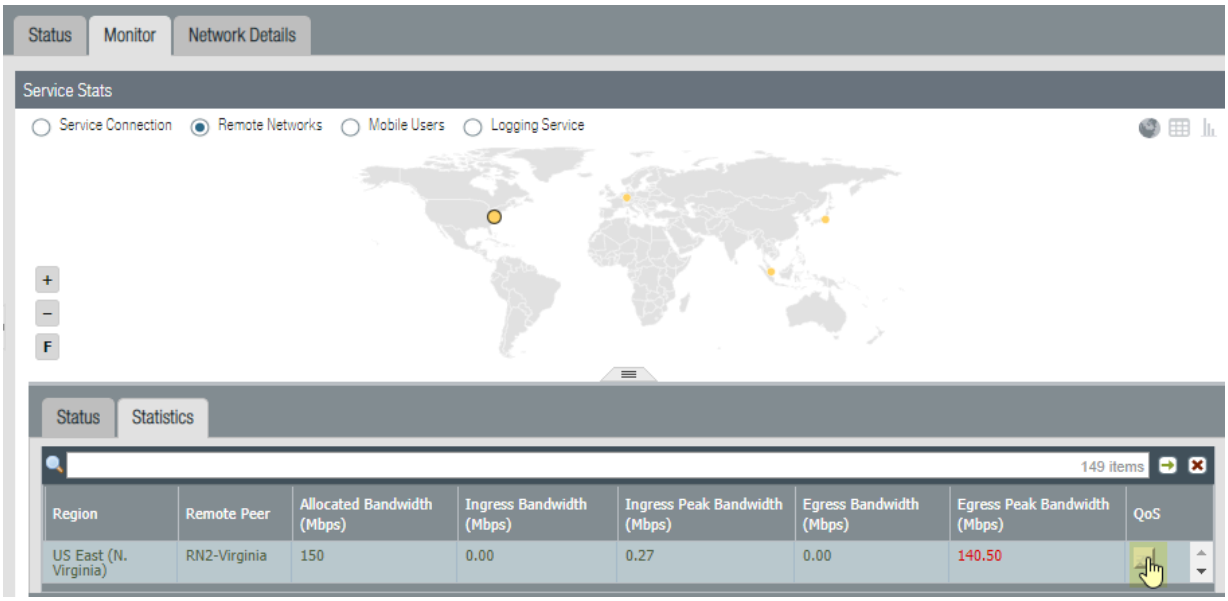
右側のグラフにカーソルを合わせると、特定の期間の詳細情報が得られます。



- サービス接続のために、**[Panorama]** > [クラウドサービス] > [ステータス] > [監視] > [サービス接続]を選択し、地域を選択してから、統計を監視します。

QoS統計情報を記載したページを表示するには、**QoS**をクリックします。

©2025 Palo Alto Networks, Inc.

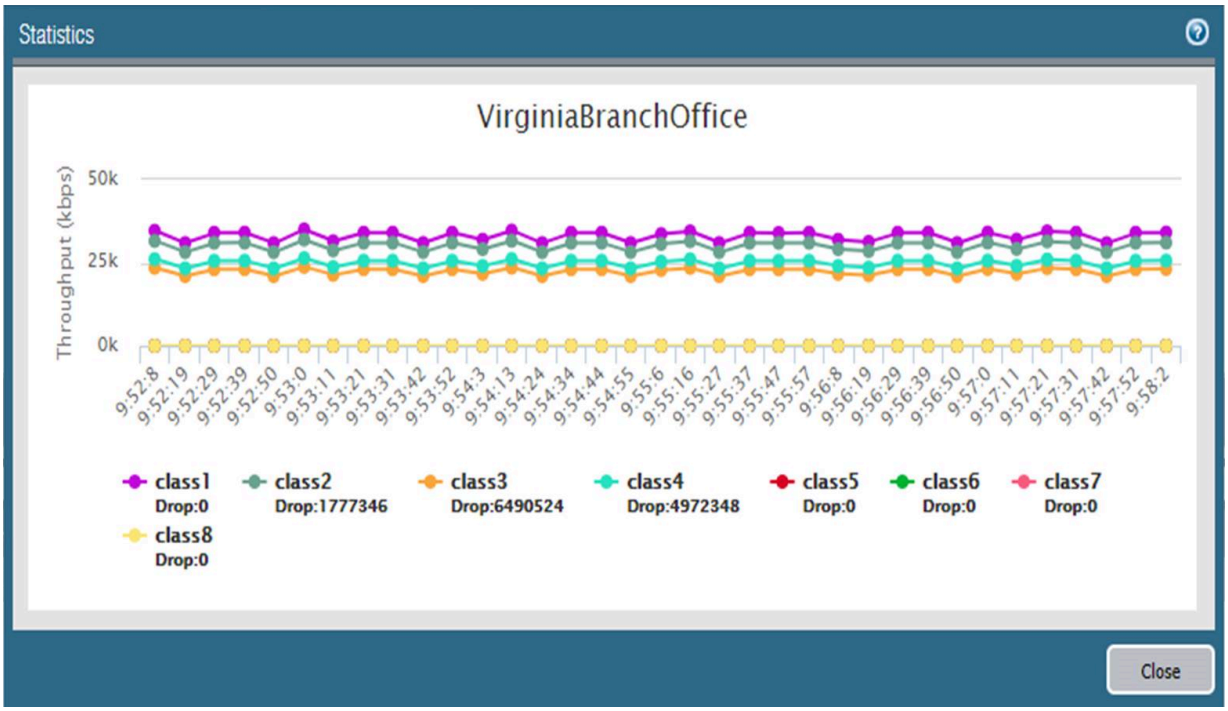


このページには、クラスあたりの破棄パケット数を含めた、リアルタイムの、および履歴的な、QoS統計情報を示すグラフが表示されます。このグラフは、QoSが有効になっている

©2025 Palo Alto Networks, Inc.

サービス接続またはリモートネットワーク接続のみを対象にしており、接続の過去5分間のネットワークアクティビティを表示します。グラフは10秒ごとに更新されます。

クラス1、2、3、4に対して渡されたトラフィックを、次の図に示します。図の下にあるデータは、クラス2、3、4のQoS設定に基づいて破棄されたパケット数を表しています。



保証帯域幅を変更する

保証帯域幅を変更する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

1つのIPSec終端ノードに関連付けられたリモート ネットワークの場所が複数ある場合は、各サイトの保証帯域幅を変更できます。次の例では、カナダ東部の拠点がカナダ中部の拠点よりも多くの帯域幅を受信するようにします。そのためには、次の手順を実行します。

STEP 1 | **[Panorama] > [Cloud Services**（クラウドサービス）**] > [Configuration**（設定）**] > [Remote Networks**（リモートネットワーク）**] > [Settings (**設定)**]**を選択します。

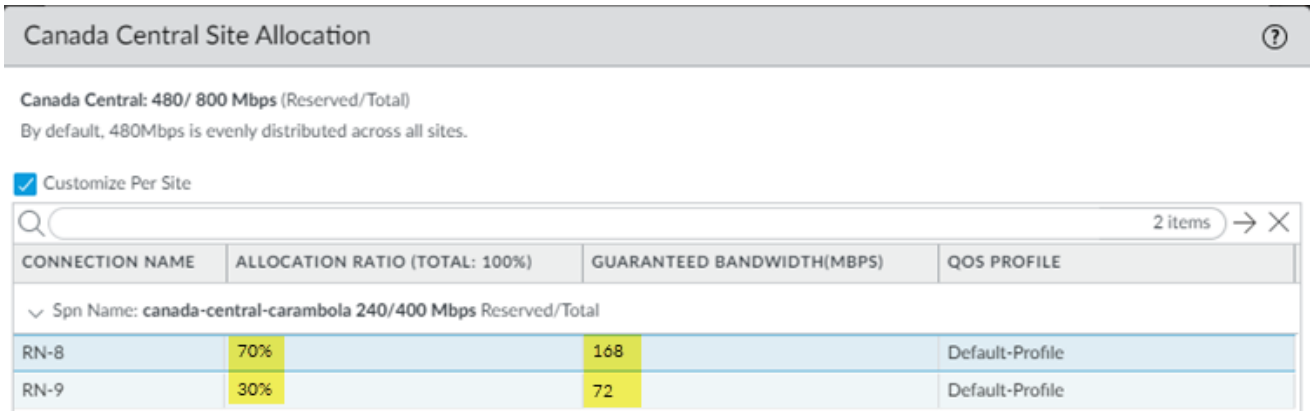
STEP 2 | 歯車をクリックして設定を編集し、**QoS** を選択します。

STEP 3 | **QoS** を有効にし、**QoS**プロファイル (この例ではデフォルト-プロファイル) と 保証帯域幅比をCanada Centralコンピューティング ロケーションに割り当てます。

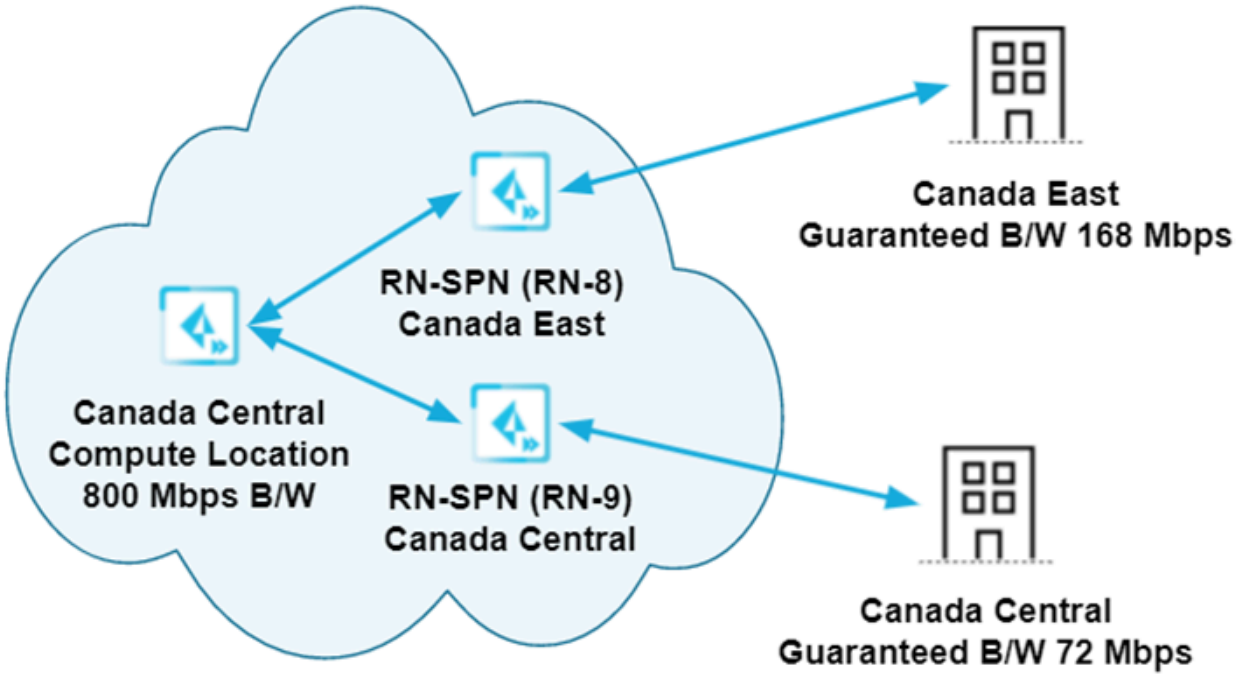
©2025 Palo Alto Networks, Inc.

STEP 4 | [サイトごとにカスタマイズ]を選択し、[サイトごとにカスタマイズ]を有効にして、RN-8 リモート ネットワーク (カナダ東部ロケーション) に RN-9 リモート ネットワーク (カナダ中部ロケーション) よりも高い帯域 幅割り当て比率 を適用します。

次の例では、RN-8 の割り当て比率が70%、RN-9の割り当て比率が30%であることを示しています。保証帯域幅 **(Mbps)** もそれに応じて変化し、新しい保証帯域幅の量が表示されます。



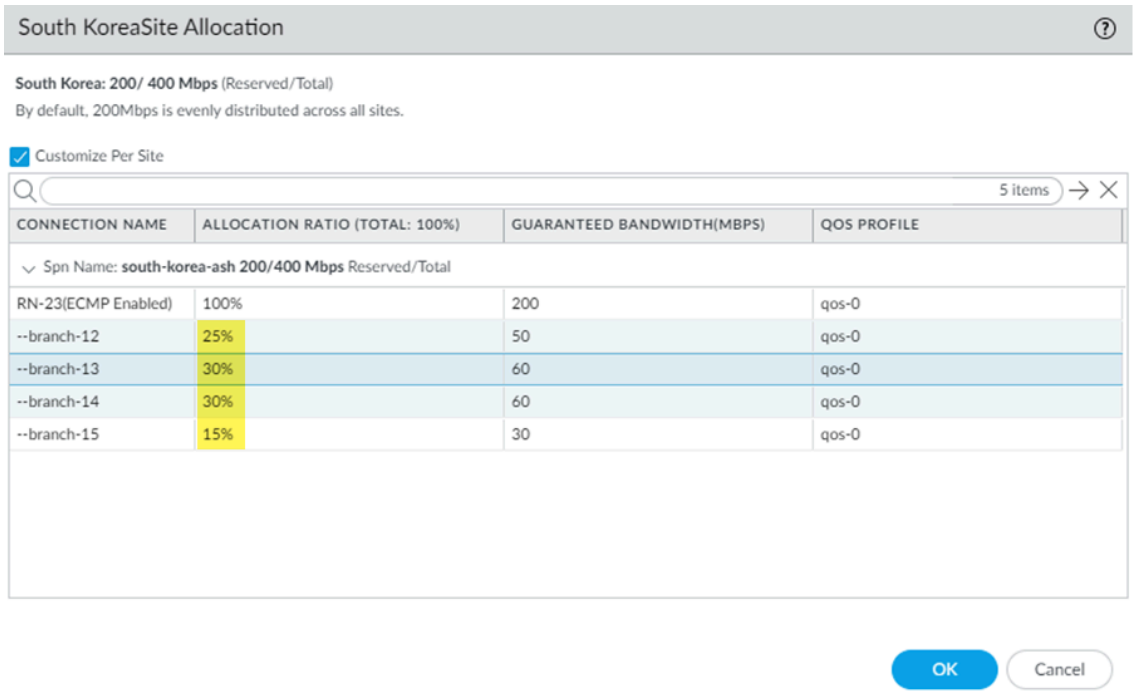
完了すると、構成により2つのサイトに対して次の帯域幅割り当てが保証されます。



リモート ネットワークの場所ごとに異なるQoSプロファイルを割り当てることもできます。異なるプロファイルを割り当てるには、サイトごとにカスタマイズ機能を有効にし、リモート ネットワークの場所ごとに異なるQoSプロファイルを選択します。

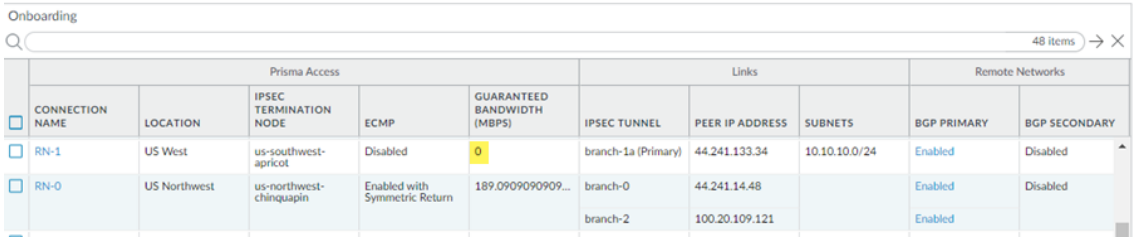
単一のリモート ネットワークに対して複数のIPSecトンネルを使用するためにECMPが有効になっているリモート ネットワークがある場合は、そのリモート ネットワークの場所に対して使用するIPSecトンネルの割り当て比率を 変更できます。

©2025 Palo Alto Networks, Inc.



STEP 5 | 変更を保存してコミットします。

保証された帯域幅の値は **[Panorama]** > **[Cloud Services]** > [ステータス] > [モニター] > [リモート ネットワーク] 領域の **[Guaranteed Mbps (**保証された**Mbps)]** 領域に表示されます。帯域幅を指定しなかった場合は0 として表示されます。



 ©2025 Palo Alto Networks, Inc.

リモート ネットワーク–ハイ パフォーマンス

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス これは限定提供リリースです。この機能を有効にするには、*Palo Alto Networks* のアカウント担当者にお問い合わせください。

ビジネスの規模が拡大し、オフィスの拠点が地理的に分散するにつれて、Prisma Accessリモート ネットワークは、ブランチサイトへの迅速なデプロイを可能にし、ユーザーにクラス最高のセキュリティを提供します。高い帯域幅を持つブランチ サイトを搭載するために、Prisma Accessはリモート ネットワーク-ハイ パフォーマンスを提供します。

リモートネットワーク（高パフォーマンス）をオンボードするには、ブランチサイトの場所を指定し、 Prisma Accessはサイトに最も近い場所を選択します。冗長性と回復力を確保するために、オプションでサイトにセカンダリ (バックアップ) の場所を設定できます。高性能リモートネットワークでは、3 Gbpsの帯域幅ごとに1つのサービスIPアドレスが使用されるため、リモート ロケーションごとに複数のIPSecデバイスを構成および管理する際の複雑さが解消されます。

セカンダリー・ロケーションは、*Prisma Access (Managed by Panorama)*のデプロイメントではサポートされていません。

リモートネットワーク - 高パフォーマンスの計画を立てたら、この設定プロセスには、高性能リモートネットワークのPrisma Accessへのオンボー ド、QoSとルーティングの有効化などが含まれます。

リモート ネットワーク - 高性能機能とガイドライン

高性能リモート ネットワークは、次のコア機能を提供します。

- コンピューティング領域内のノードあたり最大3 Gbpsの総合帯域幅
- リモートサイトからのリモートネットワークトンネルあたり最大2 Gbpsの帯域幅
- Prisma SD-WANと拡張 (サードパーティ) CPEデプロイメントにより、サービスIPアドレスごとに最大500のリモート ブランチに対応

ブランチ サイトに高パフォーマンスのリモート ネットワークを構成する場合は、次のガイドラインと、サイトとリモート ネットワークの違いに注意してください。

- **Prisma Access** ロケーション- リモート ネットワーク-ハイ パフォーマンスは、Prisma Accessロケーションのサブセットをサポートします。

©2025 Palo Alto Networks, Inc.

- **Quality of Service (** クオリティ オブ サービス **- QoS)**- ブランチサイトの場合、 Prisma Accessはサイトごとのレベルで**QoS**をサポートし、選択した**QoS**プロファイルはサイト全体に適用されます。
- 認定情報レート **(CIR)**- サイトごとに使用される帯域幅の量を確保してコミットするには、**CIR**を指定します。コンピューティング ロケーションで帯域幅を共有するリモート ネットワークが複数ある場合、そのコンピューティング ロケーションで他のサイトとの競合が発生すると、リモート ネットワーク - 高パフォーマンスは少なくとも CIR で指定された帯域幅を受け取ります。
- **IPSec**終端ノード- リモート ネットワークとは異なり、Prisma Access (Managed by Strata Cloud Manager)デプロイメントのオンボーディング時に IPSec 終端ノードを選択する必要はありません。 Prisma Accessは自動的にリモートネットワーク接続の負荷分散を行い、サイトへの帯域幅割り当てを最大化します。

  Panoramaからオンボードされたリモート ネットワークの**IPSec**終端ノードを選択する必要があります。
- トンネルとコンピューティングのロケーションの冗長性とサイトあたりの最大トンネル数- 高性能リモート ネットワークでは、場所と IPSec の冗長性の両方を構成できます。
  - 場所の冗長性 (1 つの コンピューティング ロケーションにプライマリロケーションを指定し、別のコンピューティング場所に セカンダリ 場所を指定します)。

    セカンダリ ロケーションの構成はオプションであり、セカンダリ ロケーションはプライマリ ロケーションとは異なる コンピューティング ロケーション に配置する必要があります。
  - IPSec トンネルの冗長性 (トンネルを アクティブ/アクティブ または アクティブ/パッシブとして指定)。

  この表には、トンネルごとの場所の最小数と最大数が示されています。

ロケーションのデプロイメントタイプ	トンネル デプロイメントタイプ	トンネルの最小数 トンネル	の最大数
プライマリのみ	アクティブ/パッシブ	1	2
プライマリのみ	アクティブ/アクティブ	2	4
プライマリとセカンダリ	アクティブ/パッシブ	2	4
プライマリとセカンダリ	アクティブ/アクティブ	4	8

- デプロイメントタイプに基づくサービス**IP**アドレスの割り当て- 受信するサービスIPアドレスの数は、高性能リモート ネットワークを1つの場所にセットアップしたか、プライマリデプ

 ©2025 Palo Alto Networks, Inc.

ロイメントとセカンダリデプロイメントの2つの異なる場所にセットアップしたかによって異なります。

- 高性能リモート ネットワークをセカンダリ ロケーションのない単一のロケーションに設定した場合、Prisma Accessは単一のサービスIPアドレスを提供します。
- プライマリ構成とセカンダリ構成でコンピューティング ロケーションの冗長性を設定すると、Prisma Accessは2つのサービスIPアドレス (プライマリ構成とセカンダリ構成にそれぞれ1つずつ) を提供します。

アクティブ/パッシブ構成でIPSecトンネルを設定する場合、 Prisma Accessは両方のトンネルに単一のサービスIPアドレスを提供します（標準のPrisma Accessリモート ネットワーク構成)。

- 帯域幅に基づくサービス**IP**アドレスの割り当て—Prisma Accessはコンピューティング ロケーションの帯域幅3Gbpsごとに1つのIPアドレスまたはFQDNが提供されます。
- コンピューティング ロケーションごとの帯域幅- 標準のリモート ネットワークに帯域幅を割り当てるのと同じように、コンピューティング ロケーションごとに帯域幅を割り当てます 。構成を開始する前、または高パフォーマンスのリモート ネットワークの作成中に、帯域幅を計画して割り当てることができます。
- **IPv6**サポート- リモート ネットワーク - 高パフォーマンスデプロイメントではIPv6 はサポートされません。

次の手順のいずれかを使用して、帯域幅の割り当てタイプに応じてリモートネットワークをオンボードします:

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

Strata Cloud Manager

Strata Cloud Managerでリモートネットワーク（高パフォーマンス）を追加する方法は次のとおりです。

STEP 1 | Strata Cloud Managerから**[Workflows (**ワークフロー**)]** > **[Prisma Access**セットアップ**]** > **[Branch Sites (**ブランチ サイト**)]**に移動します。

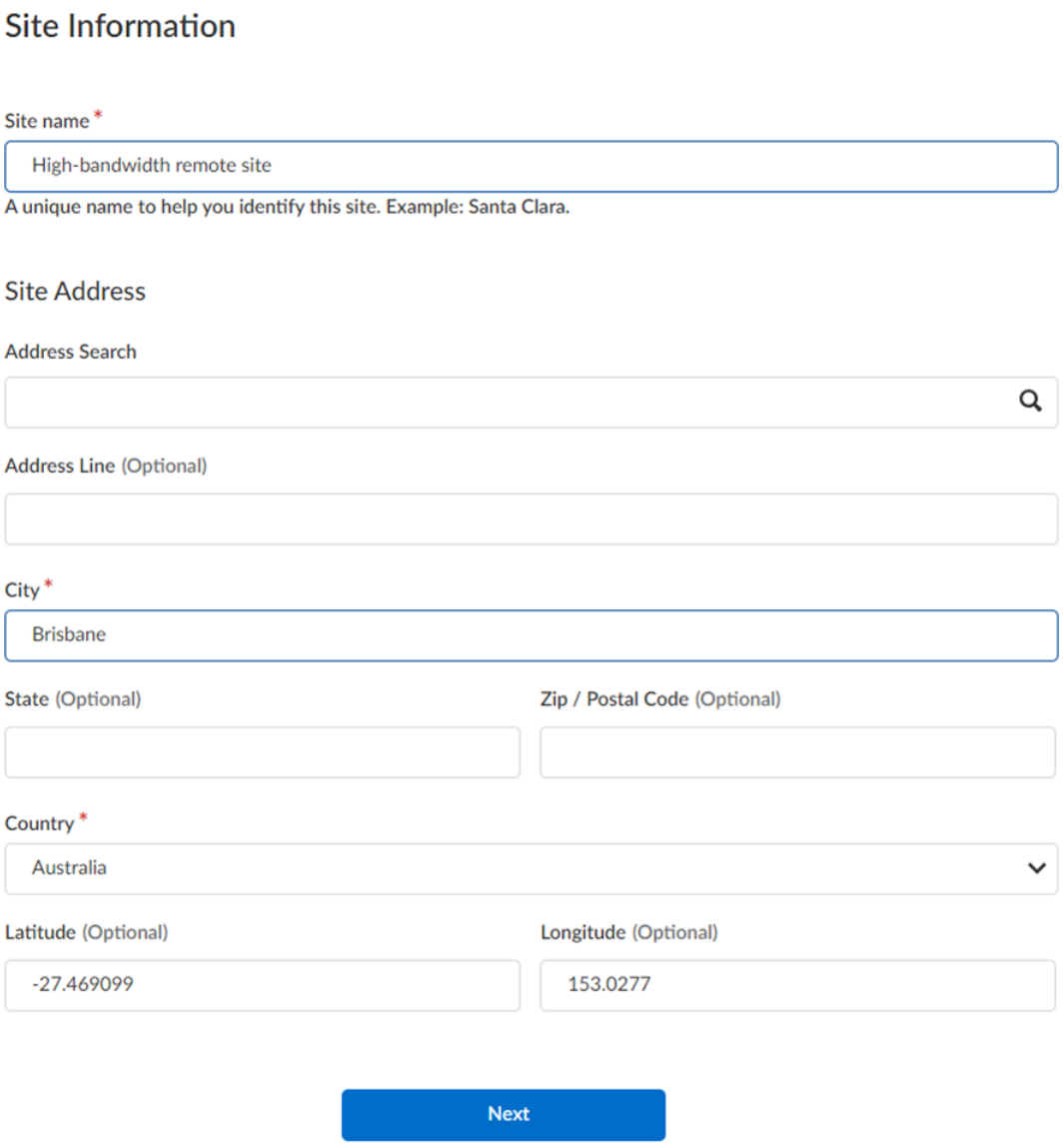
この選択は、ブランチ サイト用に作成したトンネルが CPE (Palo Alto Networks次世代ファイアウォールまたはサードパーティのCPE) によって終了されることを示します。

STEP 2 | サイトを追加し 、リモート ネットワークに分かりやすいサイト名を付けます。

©2025 Palo Alto Networks, Inc.

STEP 3 | サイトの都市と国を選択します。

より正確な検索を行うには、住所を追加してください。



STEP 4 | **Next**（次へ）をクリックします。

STEP 5 | **QoS CIR (Committed Information Rate)** をMbps単位で入力します。

コンピューティング ロケーションで帯域幅を共有する複数のリモート ネットワークがあり、そのコンピューティング ロケーション内の他のサイトと帯域幅の競合がある場合、リモートネットワーク - 高パフォーマンスは少なくとも CIR で指定された帯域幅を受け取ります。

プライマリ サイトとセカンダリ サイトを構成する場合は、異なるコンピューティング リージョンを指定し、セカンダリ リージョンにはCIRの20%が割り当てられます。たとえば、サ

©2025 Palo Alto Networks, Inc.

イトに100MbpsのCIRを設定すると、 Prisma Accessはプライマリ サイトに 100 Mbps CIRを提供し、セカンダリ サイトに20 Mbps CIRを提供します。

CIRが500Mbpsで、コンピューティングロケーションの残りの帯域幅がすべて他のサイトで使用されている場合、 Prisma Accessは500 Mbps を超える帯域幅はすべてドロップします。ただし、他のサイトが帯域幅を使用していない場合、高性能リモート ネットワークの帯域幅は、コンピューティング ロケーションに割り当てられた帯域幅まで 500 Mbps を超えることができます。

最小CIR 1 Mbps、最大CIR 2000 Mbpsを入力します。コンピューティング リージョンに指定した帯域幅を超えないようにしてください。

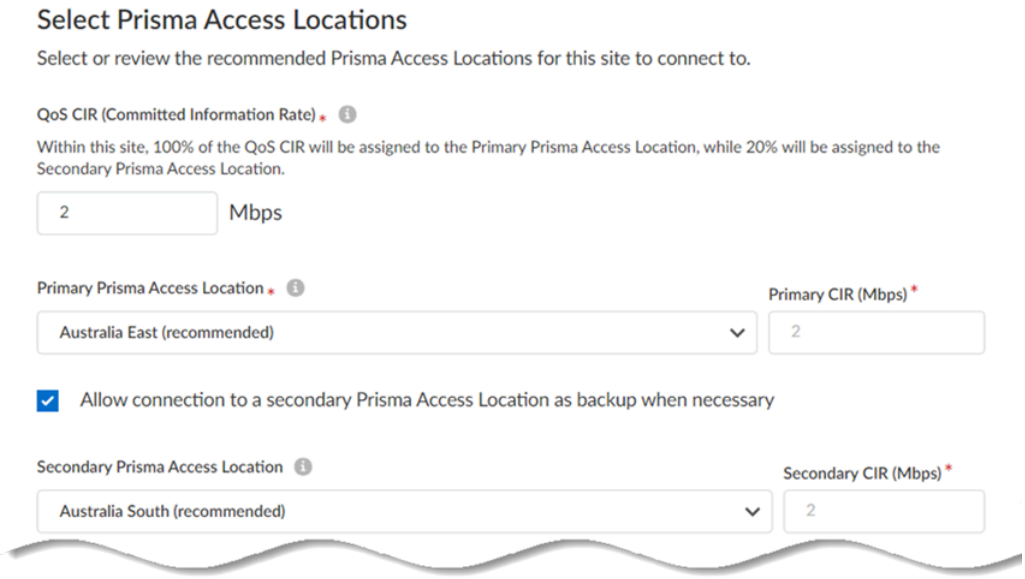
STEP 6 | **Primary Prisma Access Location (**プライマリ**Prisma Access**のロケーション**)**を選択します。リストに複数の場所が推奨されている場合は、デプロイメントに最適な場所を選択します。

STEP 7 | (任意) セカンダリ (バックアップ) サイトを作成するには、**[Allow connection to a secondary Prisma Access Location as backup when necessary (**必要に応じてバックアップとしてセカ

 ©2025 Palo Alto Networks, Inc.

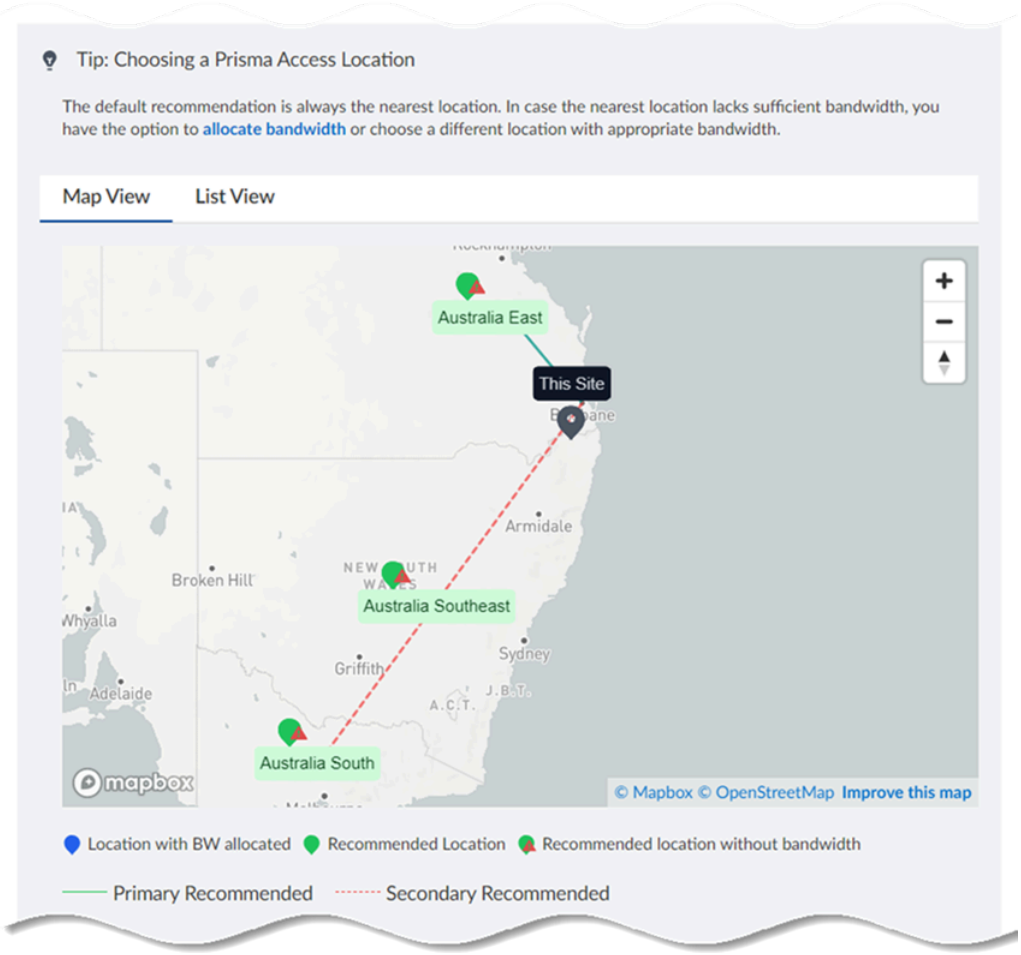
ンダリ **Prisma Access** ロケーションへの接続を許可する**)]** を選択し、 **[Secondary Prisma Access Location (**セカンダリ **Prisma Access** ロケーション**)]**を選択します。

この選択肢を選択した場合、 Prisma Accessはプライマリ ロケーションとは異なるコンピューティング ロケーションにある最適なセカンダリ ロケーションを事前に入力します。複数の場所が 推奨されている場合は、デプロイメントに最適な場所を選択します。



Prisma Accessは、選択を支援するために、推奨場所を示す地図を提供します。

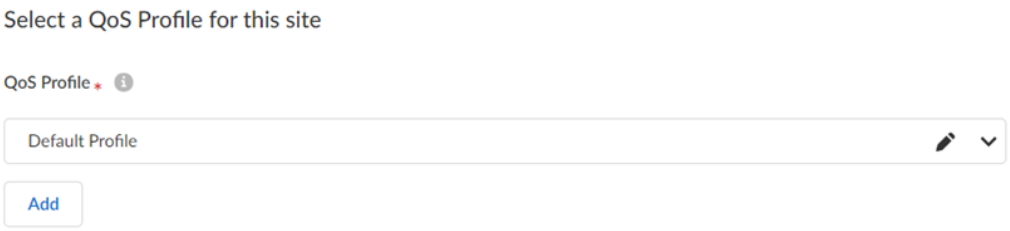
 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

STEP 8 | このサイトに使用する**QoS**プロファイルを選択します。

リモート ネットワーク - 高パフォーマンスでは、単一のQoSプロファイルが使用されます。

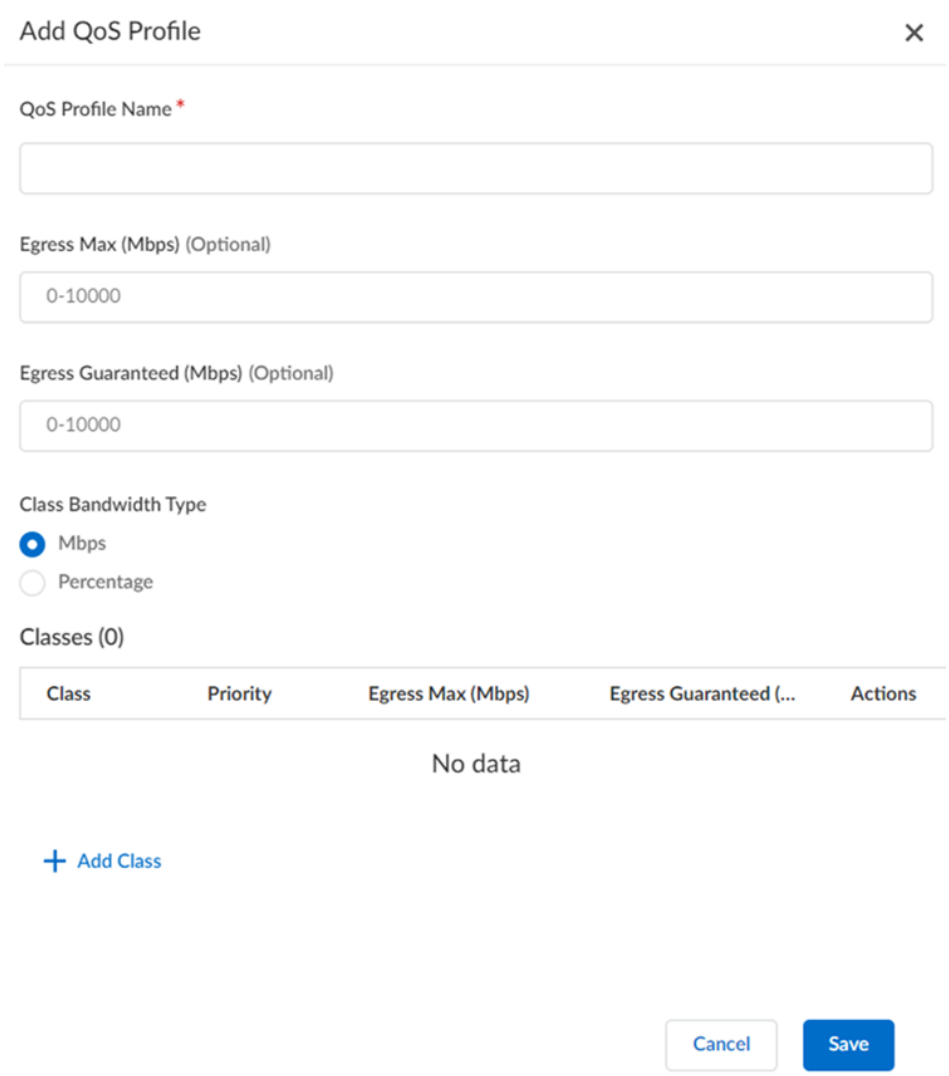


QoSプロファイルをまだ作成していない場合は、次の値を指定してQoSプロファイルを追加します 。

- 一意の **QoS**プロファイル名を入力します。
- (任意)サービス接続またはリモートネットワーク接続から送信されるトラフィックの最大スループット（Mbps）を、**Egress Max**（発信最大帯域幅） **(Mbps)**に入力します。
- (任意) このプロファイルの保証帯域幅を Mbps 単位で表す **Egress Guaranteed (**最低保証帯域 出力側**) (Mbps)** 値を入力します。
- クラス帯域幅タイプとしてパーセンテージまたは**Mbps**を入力します。

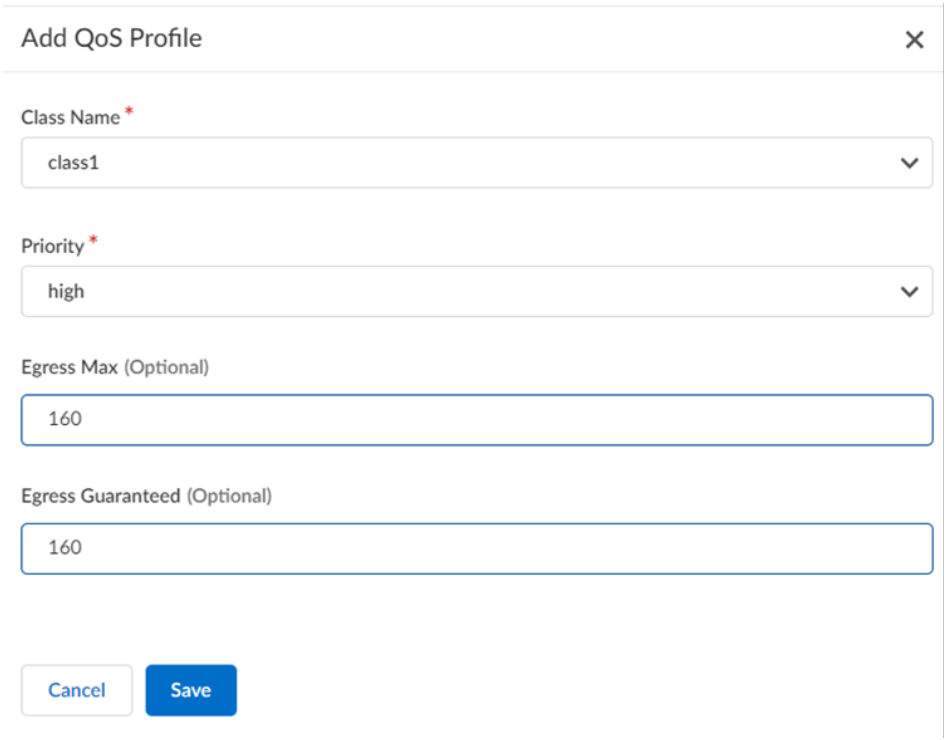
  リモート ネットワークの QoS - 高パフォーマンスでは、保証された帯域幅比率は使用されません。

©2025 Palo Alto Networks, Inc.



- Classes（クラス）セクションで、クラスを**Add**（追加）し、8つの個別のQoSクラスにマーキングする方法を指定します。
  - クラス名を入力します。
  - クラスの **Priority (**優先順位**)** を選択します(**[real-time**（リアルタイム）**]**、**[high**（高）**]**、**[medium**（中）**]**、または**[low**（低）**]**）。
  - サービス接続またはリモートネットワーク接続から送信されるトラフィックの最大スループット（Mbps）を、**Egress Max**（発信最大帯域幅）に入力します。
  - このプロファイルの保証帯域幅を Mbps 単位で表す**Egress Guaranteed (**最低保証帯域出力側**)** 値を入力します。
- 変更を保存します。

©2025 Palo Alto Networks, Inc.

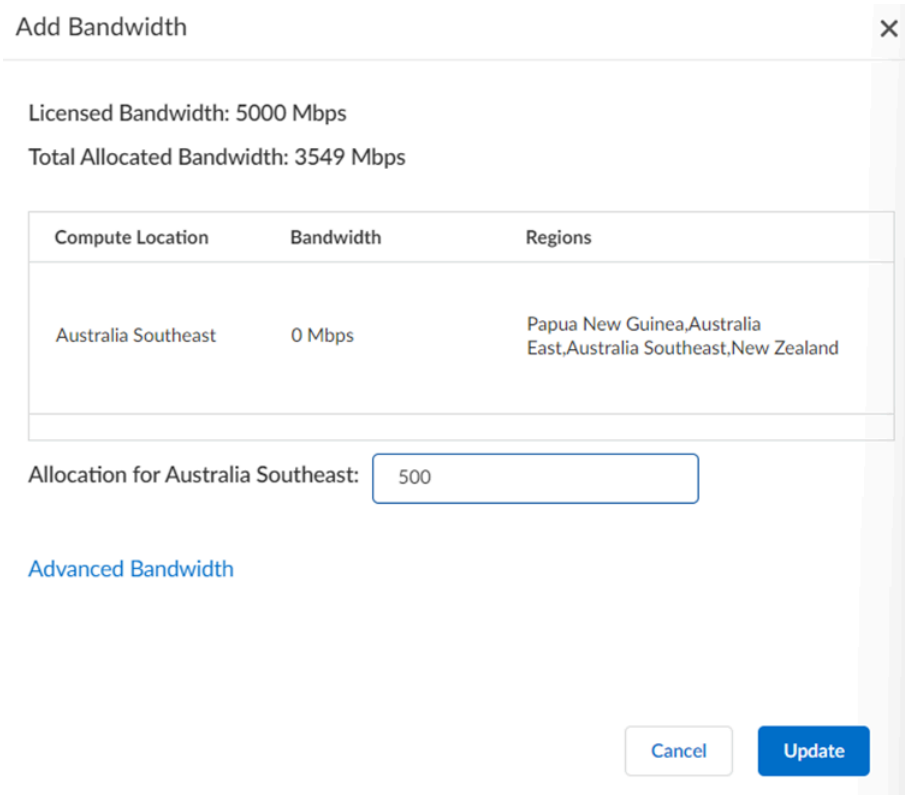


STEP 9 | まだ帯域幅を割り当てていない場合、Prisma Accessは、選択したロケーションに関連するコンピュートロケー ションの帯域幅を割り当てるように促します。コンピューティング ロケーションごとに50 Mbpsの最小帯域幅を指定します。



 ©2025 Palo Alto Networks, Inc.

STEP 10 | 選択した場所にまだ帯域幅を割り当てていない場合は割り当ててから、変更を更新します。



STEP 11 | **Next**（次へ）をクリックします。

STEP 12 | トンネルと回線の設定を定義します。

1. トンネル モードを選択します: アクティブ/アクティブ または アクティブ/パッシブ。

   トンネル モードでは、高性能リモート ネットワークに使用するISP回線の数を指定します。

   - アクティブ/アクティブを選択した場合、 Prisma Accessは4つのISP回線を使用して、2つまたは4つのアクティブ トンネルを作成します。
   - アクティブ/パッシブを選択した場合、 Prisma Accessは2つのISP回線を使用して2つのアクティブ トンネルを作成します。アクティブ トンネルがダウンすると、パッシブ トンネルがアクティブになります。
2. 使用するインターネット回線の数を選択します。

   Prisma Accessは、ここで指定した回線数、および配備がアクティブ/アクティブかアクティブ/パッシブかに基づいて、次の表に示すようにトンネルを割り当てます。

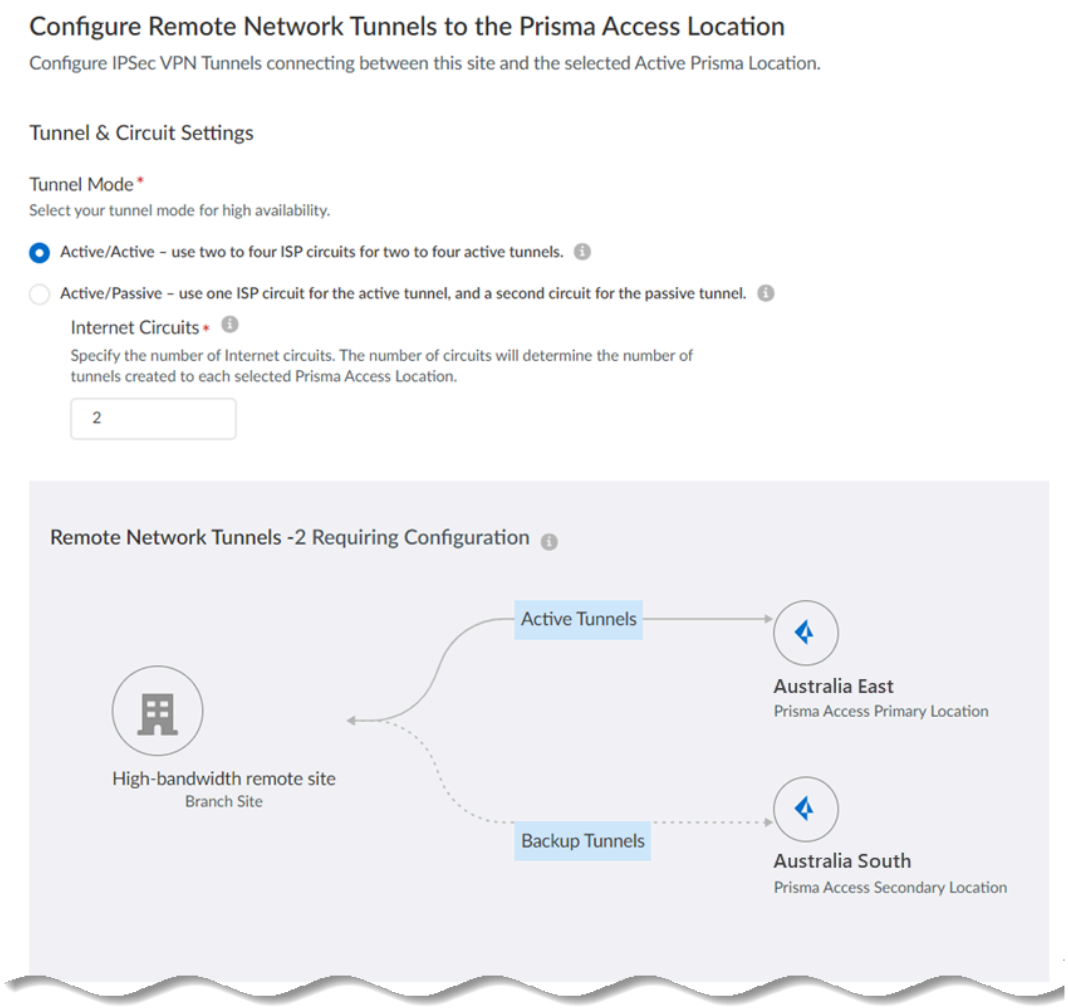
回路数	デプロイメント タイプ	トンネルの数
1	アクティブ/パッシブ	1 (アクティブ トンネル用に1つ)。

©2025 Palo Alto Networks, Inc.

回路数	デプロイメントタイプ	トンネルの数
2	アクティブ/アクティブ	2 (アクティブなトンネルごとに 1つ)。 プライマリロケーションとセカンダリロケーションを選択した場合、 Prisma Accessはプライマリ ロケーション用に1つのアクティブ トンネルを作成し、セカンダリ ロケーション用に1つのアクティブ トンネルを作成します。
2	アクティブ/パッシブ	2 (アクティブなトンネルごとに 1つ)。 プライマリロケーションとセカンダリロケーションを選択した場合、 Prisma Accessはプライマリ ロケーション用にアクティブ トンネルとパッシブ トンネルを1つずつ作成し、セカンダリ ロケーション用にアクティブ トンネルとパッシブ トンネルを1つずつ作成します。アクティブなトンネルがダウンした場合、 Prisma Accessはアクティブになるパッシブ トンネルには同じサービスIPアドレスまたはFQDNを使用します。
4	アクティブ/アクティブ	4 (アクティブなトンネルごとに 1つ)。 プライマリロケーションとセカンダリロケーションを選択した場合、 Prisma Accessはプライマリ ロケーション用に2つのアクティブ トンネルを作成し、セ

©2025 Palo Alto Networks, Inc.

回路数	デプロイメントタイプ	トンネルの数
		カンダリ ロケーション用に2つのアクティブ トンネルを作成します。

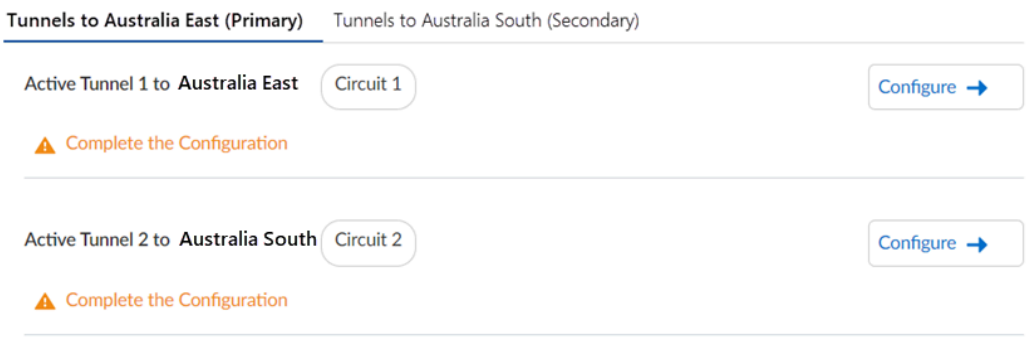


 ©2025 Palo Alto Networks, Inc.

3. (任意) IPSecトンネル設定を構成します 。

   Prisma AccessはデフォルトのIPSecトンネル設定を提供します。これらの設定により、リモート ネットワーク トンネルのIPSecおよびIKE暗号設定が決まります。変更する場合は、 プライマリ トンネル を選択し、設定を編集します 。

   セカンダリロケーションを指定すると、 Prisma Accessはプライマリ トンネルからセカンダリ トンネルに値が自動的に入力されます。セカンダリ トンネルを編集するには、そのトンネルを選択して設定を編集します 。



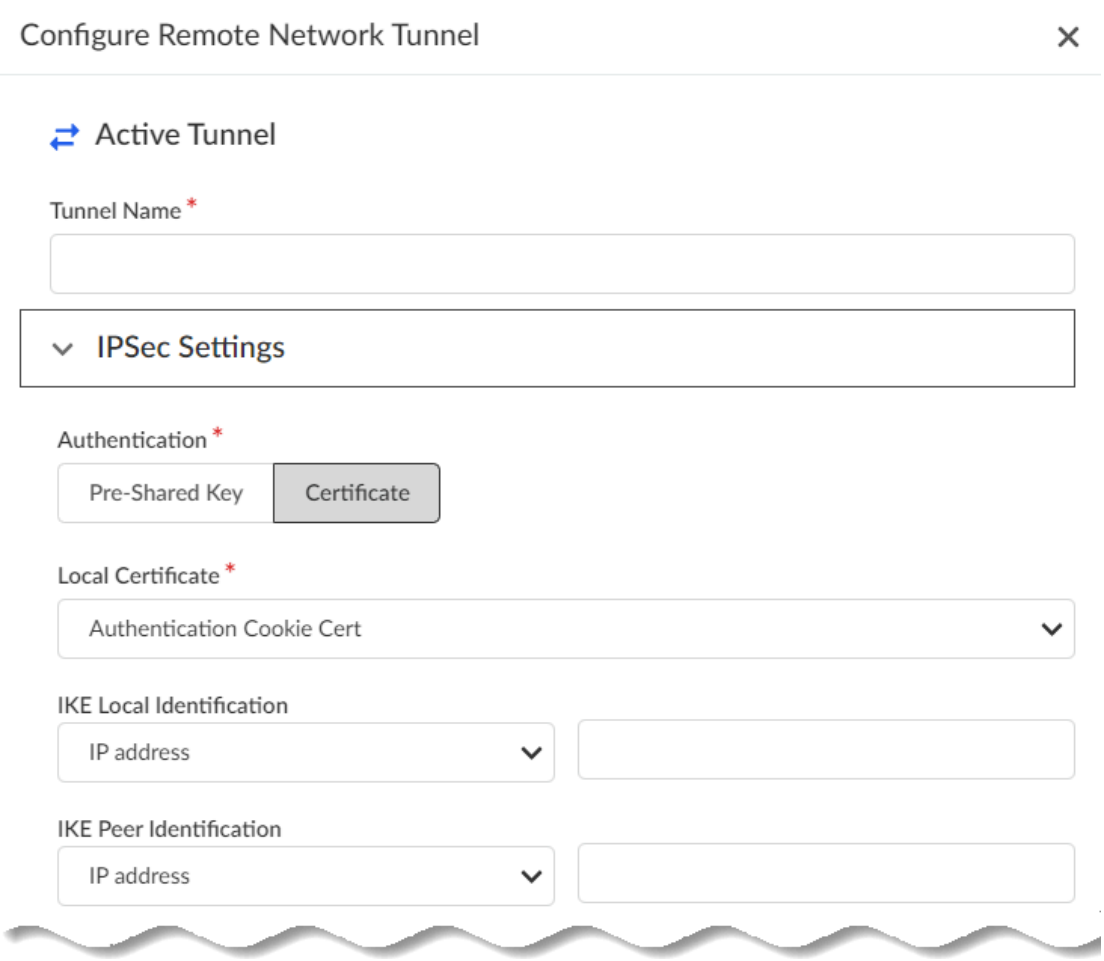
   これらの設定をメモしてください。サイトでIPSecトンネルを終了するCPEの設定と一致する必要があります。

   - アクティブ トンネルに一意の トンネル名を付けます。
   - **IPSec**設定を指定します。
     - 認証 タイプ（ 事前共有鍵 または 証明書）を指定します。

       事前共有鍵を指定する場合は、 事前共有鍵を入力して確認します。

       証明書を指定する場合は、使用する ローカル証明書 を入力します。この証明書はStrata Cloud Manager内に既に存在している必要があります 。
     - **IKE** ローカル **ID(IP** アドレス、 識別名 **(**件名**)**、 ユーザー **FQDN (**電子メール アドレス**)**、または **FQDN (**ホスト名**)** のいずれか) を指定します。
     - **IKE** ピア **ID(IP** アドレス、 識別名 **(**件名**)**、 ユーザー **FQDN (**電子メール アドレス**)**、または **FQDN (**ホスト名**))** を指定します。

©2025 Palo Alto Networks, Inc.

- 

- Peer ID Check（ピア ID チェック）で以下のいずれかのタイプを指定します。
  - **Exact**（完全）– ローカル設定とピア IKE ID ペイロードが完全に一致するピア ID のみを許可します。
  - **Wildcard**（ワイルドカード）– （*）より前のすべての文字に一致するピア ID を許可します。ワイルドカードの後の文字は一致する必要はありません。
- （任意）ピア ID が証明書のピア ID に一致しなくても IKE セキュリティ アソシエーション (SA) を正常に確立できるようにするには、**Permit peer identification and**

©2025 Palo Alto Networks, Inc.

certificate payload identification mismatch（ピア **ID** と証明書ペイロード **ID** の不一致を許可する）をクリックします。

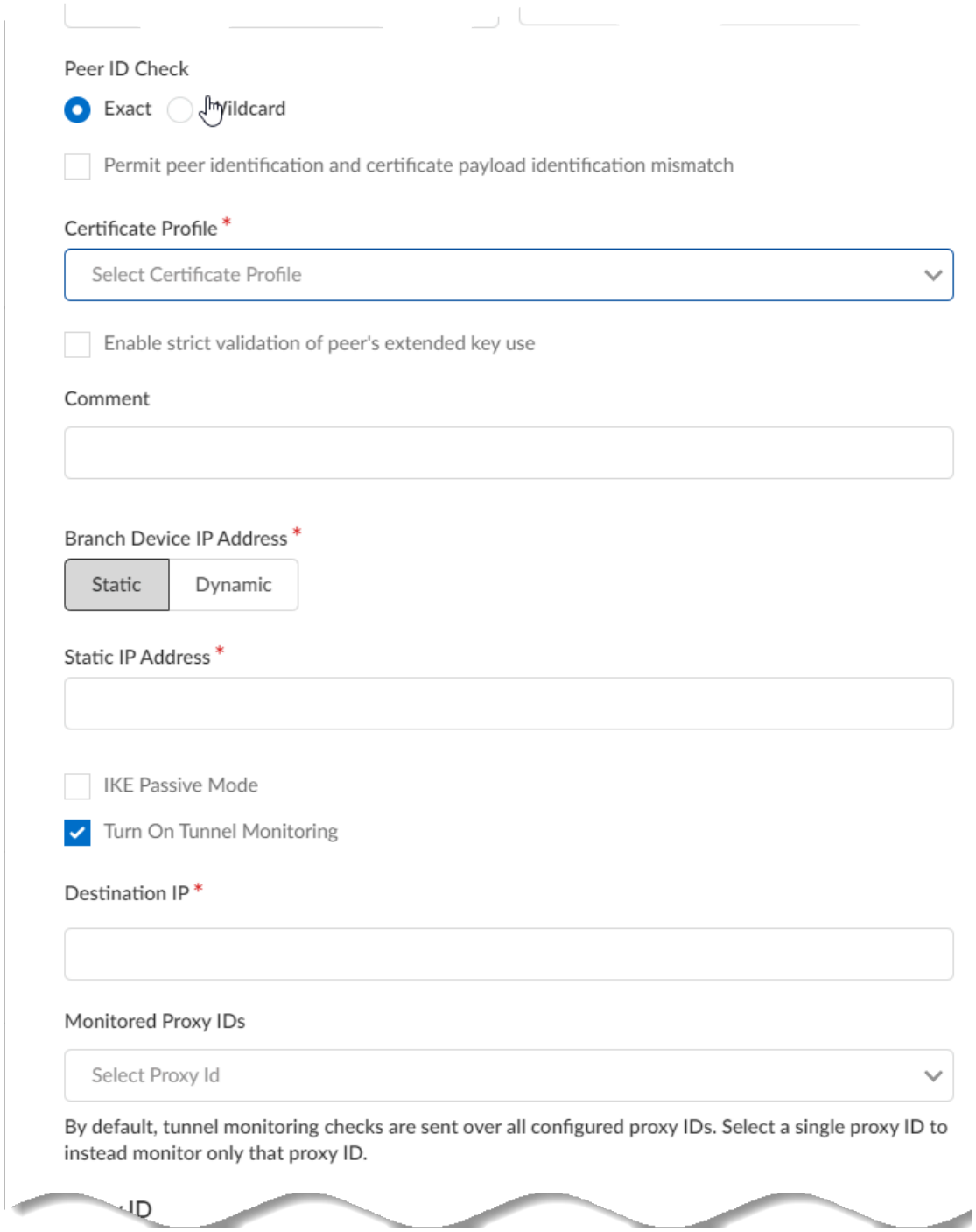
- **Certificate Profile (**証明書プロファイル**)** を選択します。証明書プロファイルには、ピア ゲートウェイの認証方法に関する情報が含まれています。
- （任意）鍵の使用方法を厳密に制御する場合は、**Enable strict validation of peer's extended key use**（ピアの拡張鍵使用の厳密な検証を有効にする）をクリックします。
- ブランチ デバイスの **IP** アドレス (静的 または 動的) を選択します。
  - 「静的」を選択した場合は、IPSecトンネルに使用する静的**IP**アドレスを入力します。
  - IPアドレスを自動的に取得するには、**Dynamic (**動的**)** を指定します。
- （任意、推奨）**IKE**パッシブモードを有効にすると、 Prisma AccessはIKE 接続に応答しますが、接続を開始しません。

  必須ではありませんが、**IKE**パッシブ モード は推奨される設定です。
- (任意) トンネル監視をオンにします。

  リモートネットワーク上のトンネル監視 宛先**IP** アドレスを入力します。 Prisma Accessはトンネルが稼働しているかどうかを確認し、ブランチ IPSec デバイスがポ

©2025 Palo Alto Networks, Inc.

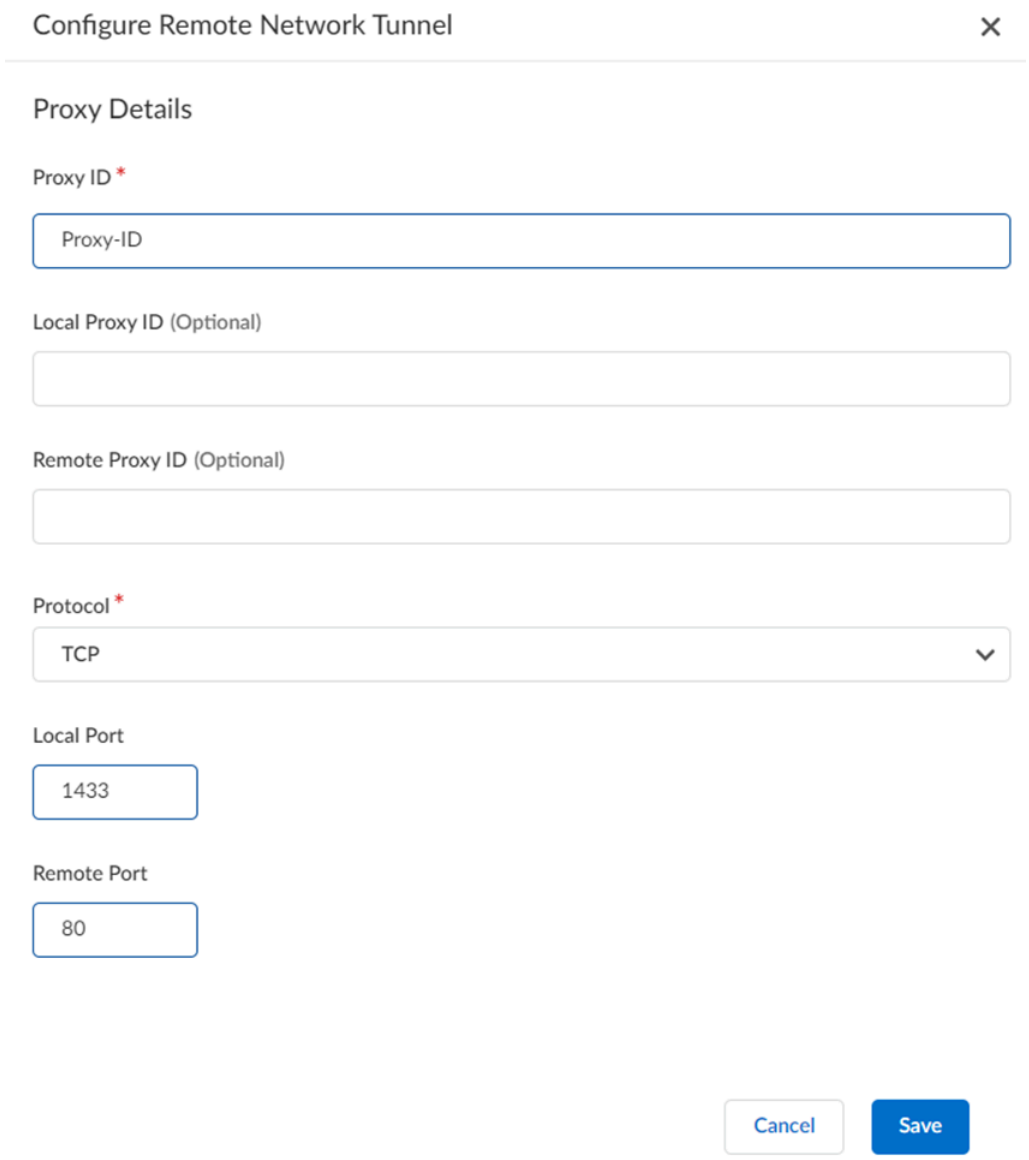
リシーベースのVPNを使用している場合は、関連付けられている プロキシ**ID**を監視対象プロキシ**ID**として入力します。

- 

- (任意) プロキシ ID が必要な場合:
  - プロキシ **ID** を追加し 、 プロキシ**ID**を入力します。
  - 必要に応じて、 ローカル プロキシ **ID** と リモート プロキシ **ID**を入力します。
  - プロキシIDに使用する プロトコル を入力します。数値、**TCP**、または **UDP**を入力します。

 ©2025 Palo Alto Networks, Inc.

- TCP または UDP の ローカル ポート と リモート ポート を指定するか
- 変更内容を保存します 。



- **IKE** 詳細オプションを指定します。
  - **IKE** プロトコル バージョンを選択します。
  - **IKEv1**暗号プロファイルを選択します。

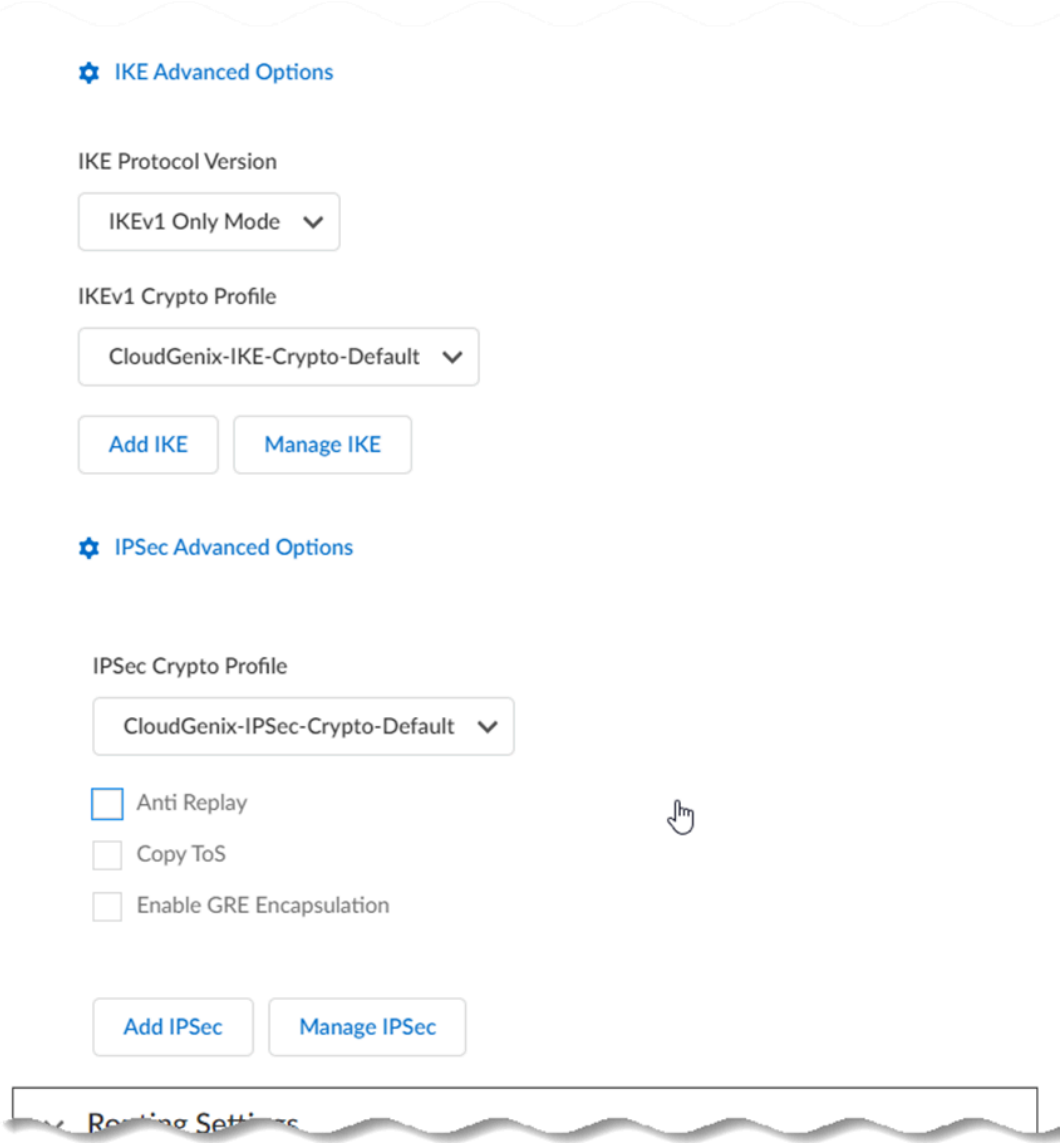
    暗号プロファイルを追加するには、**IKE**を追加します。既存の IKE プロファイルを管理するには、**[IKE** を管理**]**をクリックし 、編集するプロファイルを選択します。
  - **IKEv2**暗号プロファイルを選択します。

    暗号プロファイルを追加するには、**IKE** を追加します。既存の IKE プロファイルを管理するには、**[IKE** を管理**]**をクリックし 、編集するプロファイルを選択します。

©2025 Palo Alto Networks, Inc.

- **IPSec** 詳細オプションを指定します。
  - **IPSec**暗号プロファイルを選択します。

    暗号プロファイルを追加するには、**IPSec**を追加します。既存の IPSec プロファイルを管理するには、**[IPSec** を管理]をクリックし 、編集するプロファイルを選択します。
  -



- ルーティング設定を選択します。
  - ルーティング タイプ (静的 または 動的) を選択します。

    静的を選択した場合は、サイトで保護する IP サブネットまたは IPアドレスを追加します 。

    動的を選択した場合:
    - ネットワークの自律システム (AS) である **Peer AS**を入力します。

 ©2025 Palo Alto Networks, Inc.

RFC 6996準拠のBGPプライベートAS番号を使用します。

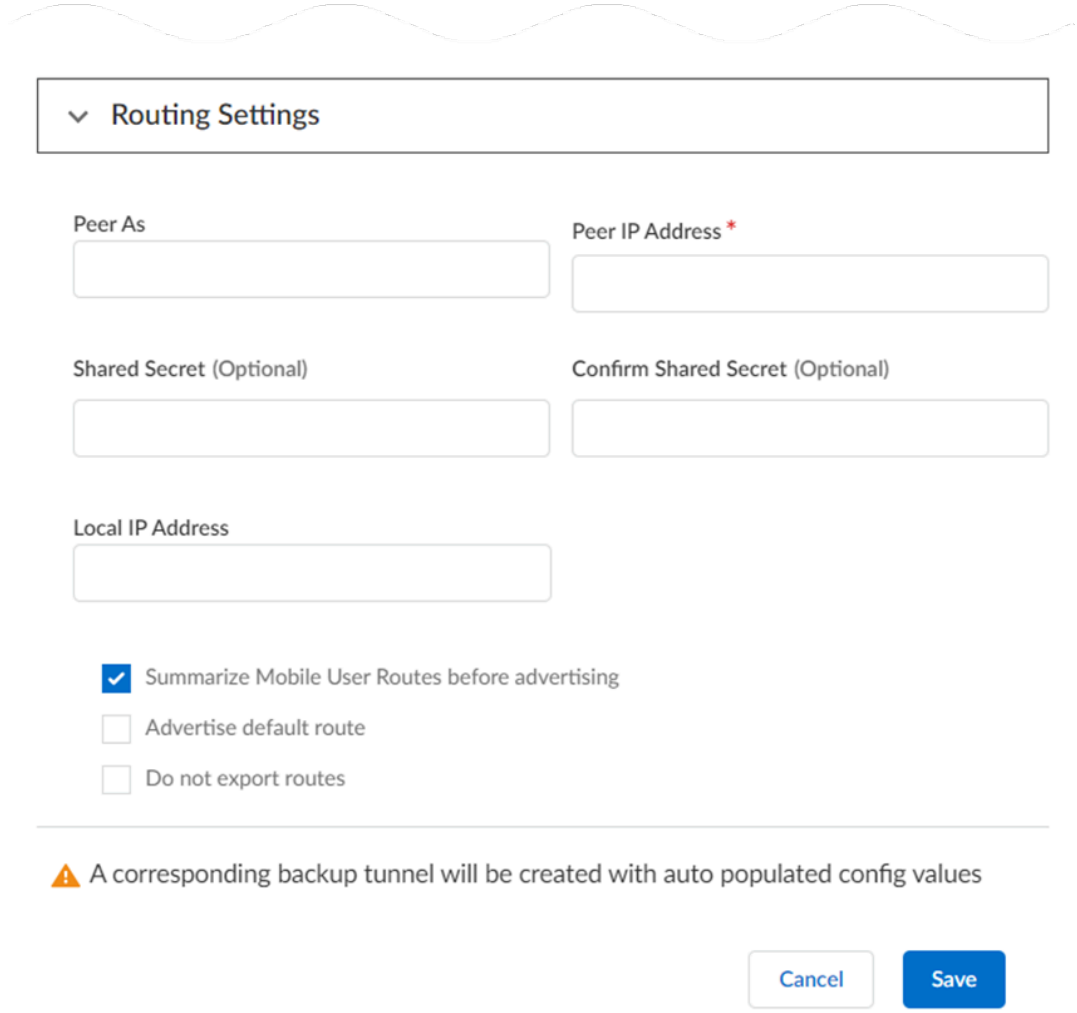
- HQまたはデータセンター ネットワーク上のeBGPルーターのルーターIDとして割り当てられたピア**IP**アドレスを入力します。
- (任意) BGP ピア通信を認証するための共有シークレットパスワードを入力します。
- Prisma AccessがBGPのローカル**IP**アドレスとして使用するローカルIPアドレスを入力します。
- （任意） Prisma Accessがサブネットを要約してからアドバタイズすることで、顧客構内装置（CPE）へ の BGP によるモバイル・ユーザ IP サブネットのアドバタイズ数を減らすには、「アドバタイズ前にモバイル ユーザー ルートを要約する」を選択します。
- （任意） Prisma Accessが eBGP を使用してリモート・ネットワークのデフォルト・ルート広告を発信 するようにするには、**[Advertise Default Route (**デフォルトルートをアドバタイズする**)]**を選択します。ネットワークに、BGPがアドバタイズしている他のデフォルトルートが存在していないことを確認して

©2025 Palo Alto Networks, Inc.

ください。そうしないと、ネットワークにルーティング上の問題が発生する可能性があります。

- （任意） Prisma AccessがHQまたはデータセンターにルートを転送しないようにするには、**[Do Not Export Routes (**ルートをエクスポートしない**)]**を選択します。

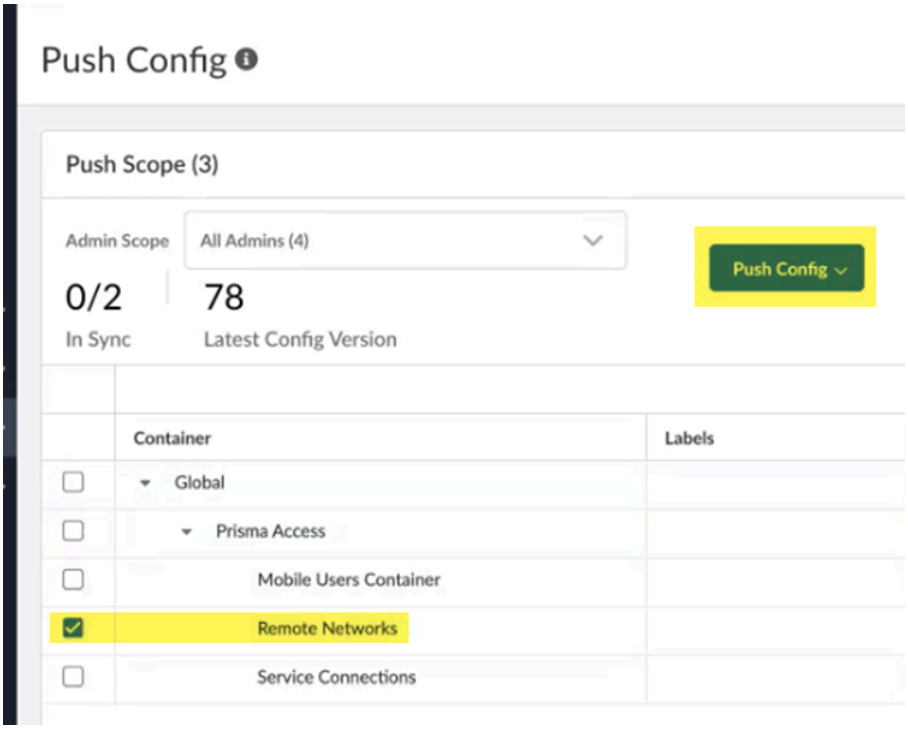
4. IPSecトンネルの変更を保存します 。



STEP 13 | 保存して終了します。

 ©2025 Palo Alto Networks, Inc.

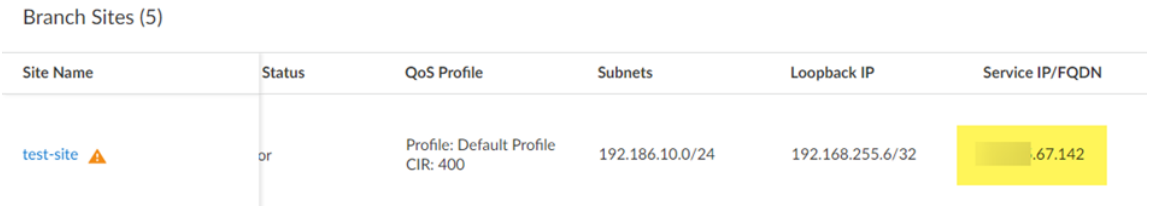
STEP 14 | **[Push Configuration (プッシュ構成)]** をクリックして構成の変更を保存します。 **[Push Scope (プッシュ スコープ)]**で **[Remote Networks (リモート ネットワーク)]** が選択されていることを確認してください。



STEP 15 | CPEで指定したサービス**IP**アドレスを見つけます。

リモート ネットワークを設定するときは、サービスIPアドレスをCPEのピアIPアドレスとして使用して、IPSecトンネルを終了します。

1. **[Workflows (ワークフロー)]** > **[Prisma SASE Setup (Prisma SASEセットアップ)]** > **[Branch Site Management (ブランチ サイト管理)]** > **[Extended CPE Site (拡張CPEサイト)]**に移動します。
2. サービス **IP/FQDN** アドレスを見つけます。



Panorama

リモートネットワークの設定手順 - ハイ・パフォーマンスは、オンボーディング中に**IPSec** 終端ノードを選択するなど、Prisma Access (Managed by Panorama)の標準的なリモート ネットワークのオンボーディングと同じである。

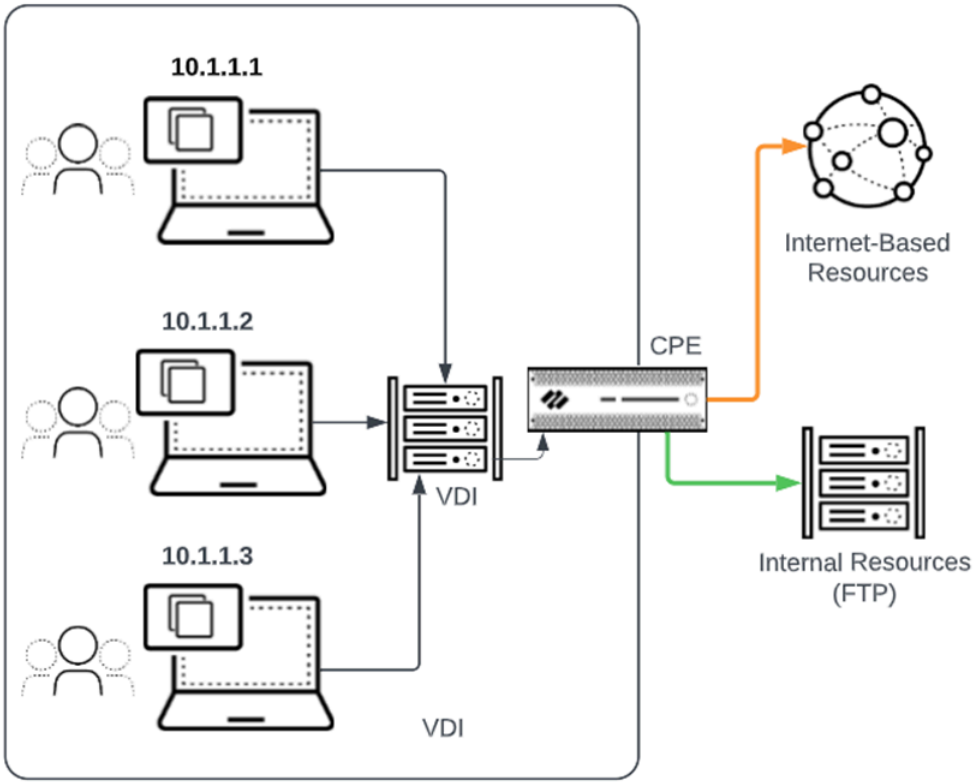
©2025 Palo Alto Networks, Inc.

ターミナルサーバーを使用した共有デスクトップVDIとPrisma Accessの統合

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Accessのライセンス

仮想デスクトップ インフラストラクチャ (VDI) は、仮想マシンを使用して仮想デスクトップをプロビジョニングおよび管理するテクノロジーです。VDI は、管理対象サーバーを使用してデスクトップ環境を展開し、要求に応じてエンドユーザーにデプロイします。エンドユーザーは、プロビジョニングされた VDI デスクトップから、インターネット ベースのパブリック アプリやリソース、FTP接続から利用できるプライベート アプリやリソースなど、必要なリソースにアクセスします。

VDI ポロジは、共有デスクトップまたは専用デスクトップのいずれかを使用して実装できます。デスクトップが共有されている場合、複数のユーザーが単一のIPアドレスの背後に配置され、ポートを使用してユーザーを区別します。



VDIデプロイメントで共有デスクトップ実装を使用する場合、 Prisma Accessは組織のVDIユーザーと内部および外部のリソースを保護しながら、エンド ユーザーが単一のログインを使用してインターネットおよびFTPリソースに安全にアクセスできるようにするソリューションを提供

©2025 Palo Alto Networks, Inc.

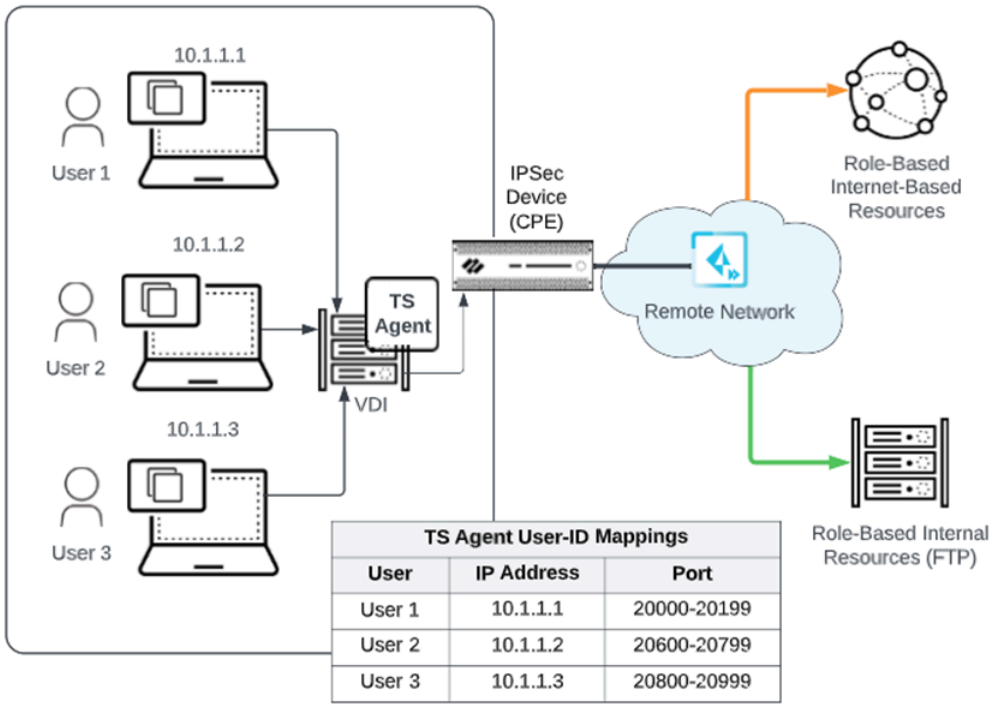
します。このソリューションでは、VDIサーバーにインストールするPalo Alto Networks TSエージェントを使用します。

TSエージェントは、ユーザーがIPアドレスを共有する場合にユーザー名とIPアドレスのマッピングを識別することに関連する問題を解決するためにインストールされるユーザーIDソフトウェアです。TSエージェントがインストールされると、ログオンしているすべてのユーザーが監視され、個々のユーザーには特定のポートのセットが割り当てられます。Prisma AccessがVDIからこのVDIネットワーク トラフィックを受信すると、ユーザーの送信元ポートに基づいてユーザを識別します。このデプロイメントにより、管理者がVDIエンド ユーザーのインターネットおよび内部サイトへのアクセスを制御するためのセキュリティ ポリシー ルールを作成できるクラウドベースのソリューションが提供されます。

ネットワークにデフォルト ルートがある場合は、1つ以上のリモート ネットワークをオンボードし、TSエージェントを実装して、組織内のユーザーとリソースを簡単に保護できます。

このデプロイメントでは、次のようになります。

- Windowsベースのターミナル サーバー上の特定のユーザーを識別するには、TSエージェントでポート範囲を指定します。TSエージェントは、割り当てられたポート範囲をPrisma Accessに通知し、Prisma Accessはユーザとユーザーグループに基づいてポリシーを適用できるようにします。
- リモート ネットワークは、FTPおよびインターネット ベースのリソースのセキュリティとアクセス制御を強化します。



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

*TS*エージェントから収集されたユーザー マッピング情報を再配信することはできません。

©2025 Palo Alto Networks, Inc.

クラウド マネージドPrisma AccessでTSエージェントとPrisma Accessリモートネットワークを使用してVDIを 統合するには、以下の手順を実行します。

STEP 1 | VDIサーバーにPalo Alto Networks TSエージェントをインストールして構成します 。

すべてのユーザーを正しくマッピングするには、ユーザーがログインするすべてのターミナル サーバー上に TS エージェントをインストールする必要があります。

1. VDI Windowsサーバーで、Palo Alto Networksターミナル サーバー (TS) エージェントをインストールして構成します。
2. TSエージェントがエンド ユーザーに割り当てるポートの範囲を定義します。

   互換性マトリックスから*TS*エージェントでサポートされているスケール数を確認します。
3. (任意) 複数のVDIサーバーがある場合は、各サーバーにTSエージェントを構成します。

STEP 2 | リモートネットワークを搭載し、クラウドマネージドPrisma AccessのVDIブランチサイトに接続します（未接続の場合）。

STEP 3 | リモート ネットワークがVDIと通信できるように、ブランチのIPSecデバイス (CPE) のオプションを構成します。

- Prisma Accessで構成したパラメータに一致するIPSecトンネルのIPSecおよびIKE暗号パラメータを構成します。
- リモートネットワークの IPSec トンネルのPrisma Access側として、サービスIPアドレス (**Manage** (管理) > **Remote Networks** (リモートネットワーク) > **Service IP** (サービスIP)) を使用します。
- リモート ネットワーク トンネルへのVDIトラフィックを許可するようにIPSecデバイス上のルートを構成します。
- トンネル経由でTSエージェントへのリモート ネットワーク トラフィックを許可するようにIPSecデバイス上のルートを構成します。
- 必要に応じて、トラフィックがトンネルを通過できるようにIPSecデバイスでセキュリティ ポリシーを構成します。

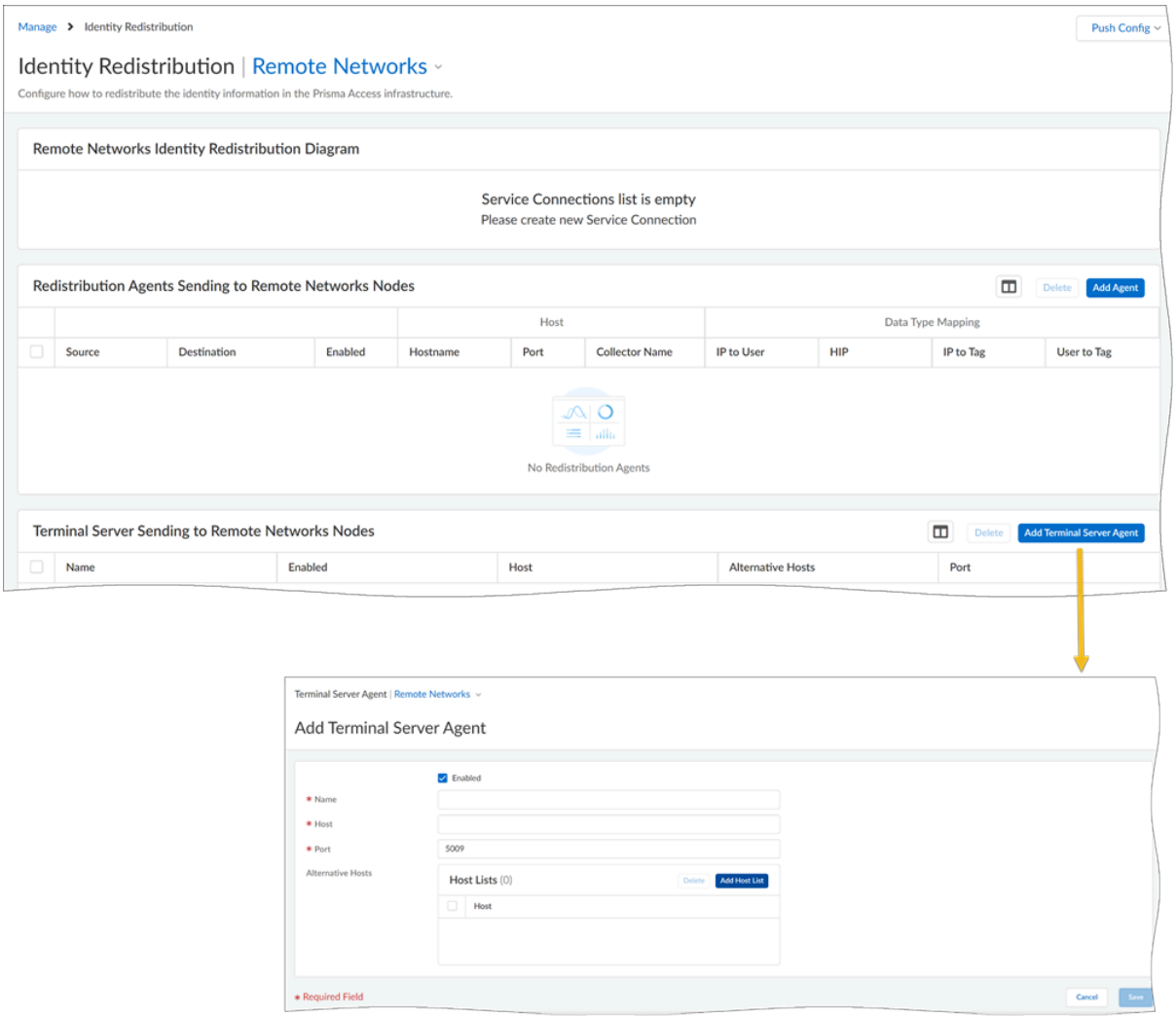
©2025 Palo Alto Networks, Inc.

STEP 4 | リモート ネットワークでのユーザー マッピングを許可するようにTSエージェントを構成します。

Manage (管理) > Configuration (設定) > NGFWとPrisma Access > Identity Services (IDサービス) > Identity Redistribution (ID配信)へと移動し、**Configuration Scope (設定スコープ)**をリモートネットワークに設定し、ターミナルサーバーエージェントを追加します。

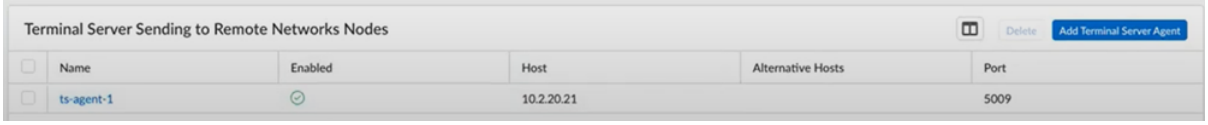
- エージェントが **Enabled (有効)** になっていることを確認します。
- TSエージェントの名前を入力します。
- TSエージェントがインストールされているWindowsホストのIPアドレスを入力します。
- エージェントがユーザーマッピング要求をリッスンするポート番号を入力します。

  ポートはデフォルトで5009に設定されています。
- 変更を保存します。



次の例では、ホスト アドレスが 10.2.20.21、ポートが 5009 に設定されたエージェントがあります。

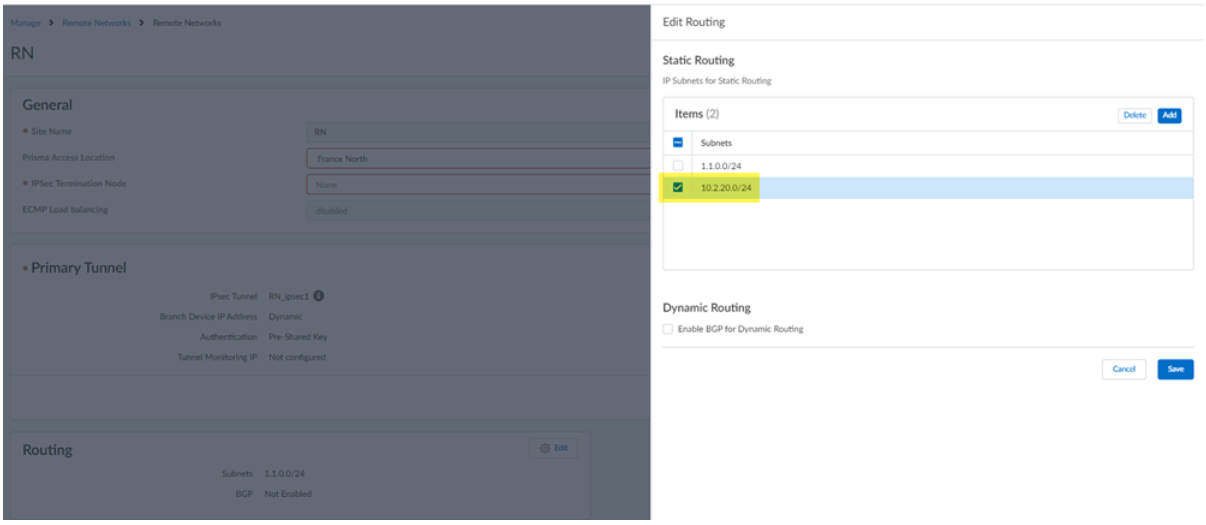
©2025 Palo Alto Networks, Inc.



STEP 5 | VDIとPrisma Accessリモートネットワーク間のルーティングを許可します。

1. **[Manage (管理)] > [Service Setup (サービスセットアップ)] > [Remote Networks (リモートネットワーク)] > *[remote-network-name]* > [Routing (ルーティング)]**に移動し、VDIサブネットへのルートを追加します 。

   このサブネットを追加すると、TSエージェントはリモート ネットワークと通信できるようになります。次のスクリーンショットの例では、VDIサブネットは 10.2.20.0/24 です。



2. [管理] > [構成] > [セキュリティ サービス] > [セキュリティ ポリシー]に移動し、スコープを [リモート ネットワーク]に設定して、VDIサブネットとリモート ネットワーク間のトラフィックを許可するセキュリティ ポリシー ルール ([ルールの追加]) を追加します。

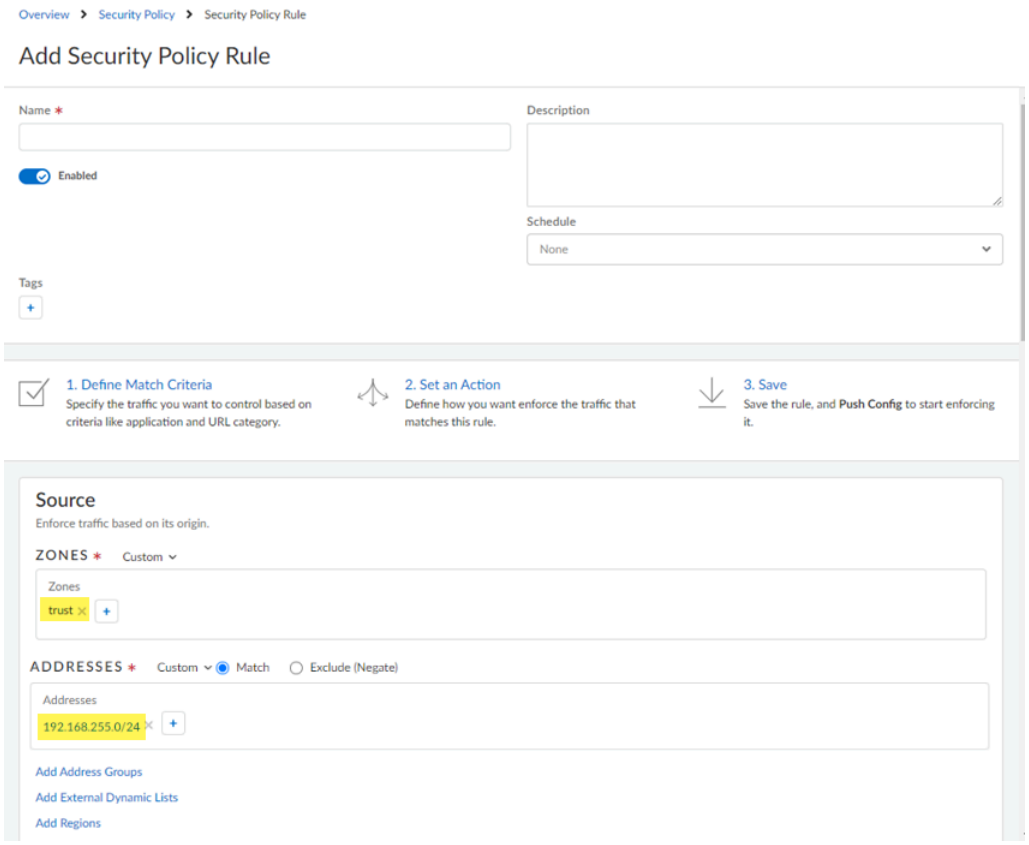
   VDI からPrisma Accessに接続するリモート ネットワークのユーザーには、Prisma Accessインフラストラクチ ャ サブネットのIPアドレスが割り当てられるため、インフラストラクチャ・サブネットとVDIサブネット間のルーティングを許可する必要があります。

   - ルールが 有効になっていることを確認してください。
   - 送信元- 次のパラメータを設定します。
     - ゾーン- **Trust(信頼できる)**に設定します。
     - アドレス- インフラストラクチャサブネット用のアドレスオブジェクトを作成し(**Manage (管理) > Shared (共有) > Infrastructure Settings (インフラストラクチャ**

 ©2025 Palo Alto Networks, Inc.

設定) > **Infrastructure Subnet** (インフラストラクチャ サブネット))、ここにアドレスオブジェクトを追加します。

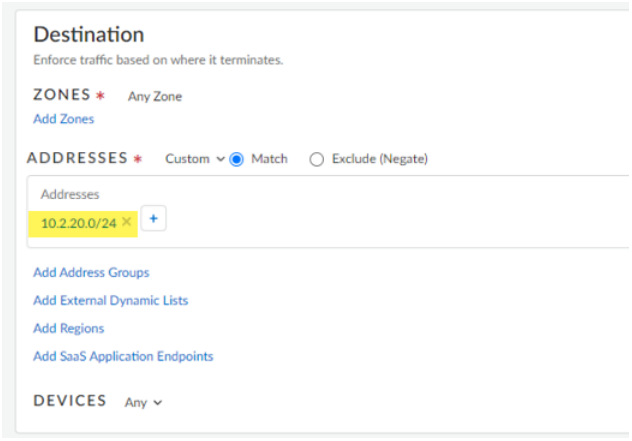
実際のインフラストラクチャ サブネットを入力するよりも、アドレス オブジェクトを使用する方が優先されます。サブネットが変更された場合、アドレス オブジェクトを変更でき、その変更はアドレス オブジェクトが使用されているすべての構成に適用されるためです。



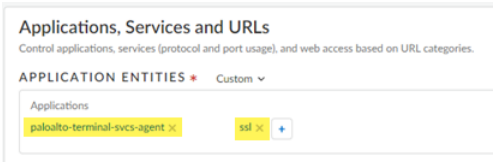
- 宛先- TSエージェントを実行しているVDIホストをアドレスに追加します。

  複数のVDIホストでTSエージェントを構成している場合は、すべてをここに追加します。

©2025 Palo Alto Networks, Inc.



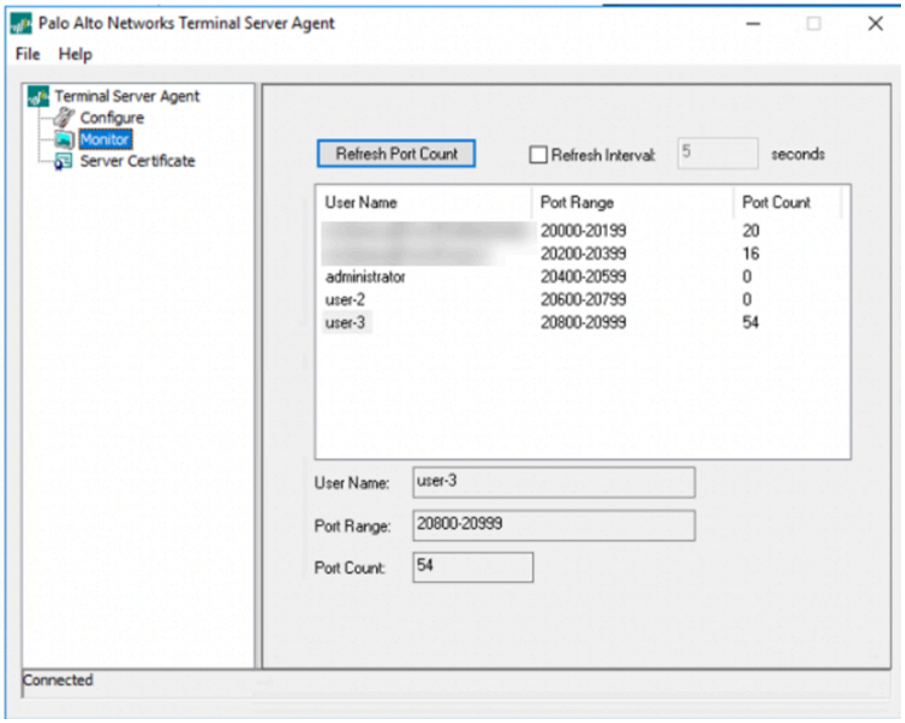
- アプリケーション、サービス、および **URL - paloalto-terminal-svcs-agent**とをアプリケーション エンティティに追加します。



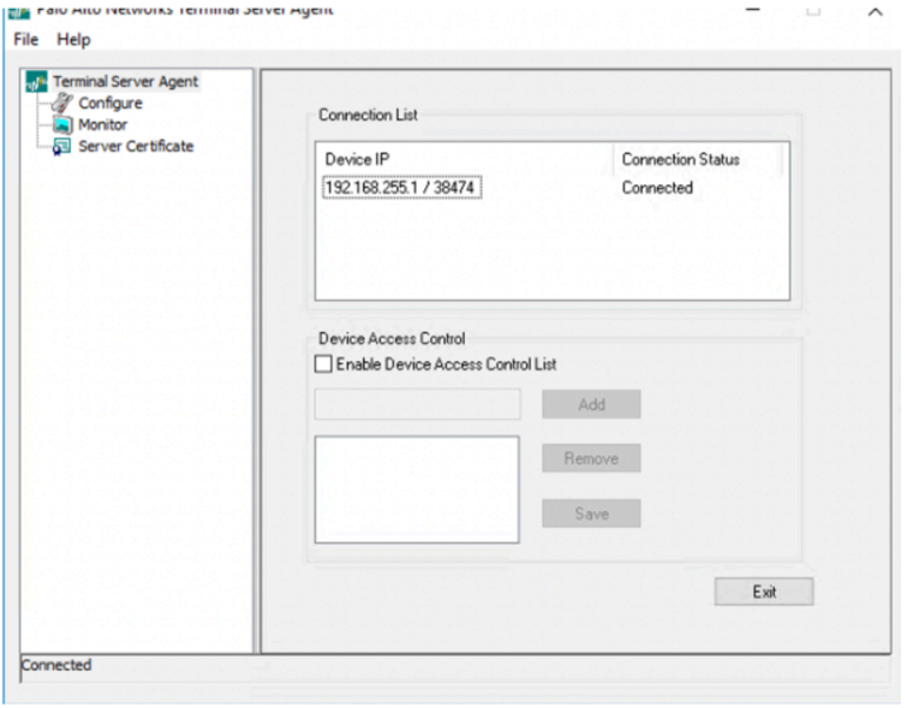
 ©2025 Palo Alto Networks, Inc.

STEP 6 | 実装が正しく動作していることを確認します。

1. TSエージェントで、エージェントのステータス を監視し 、TSエージェントが正しいユーザー名とポートのマッピングを反映していることを確認します。

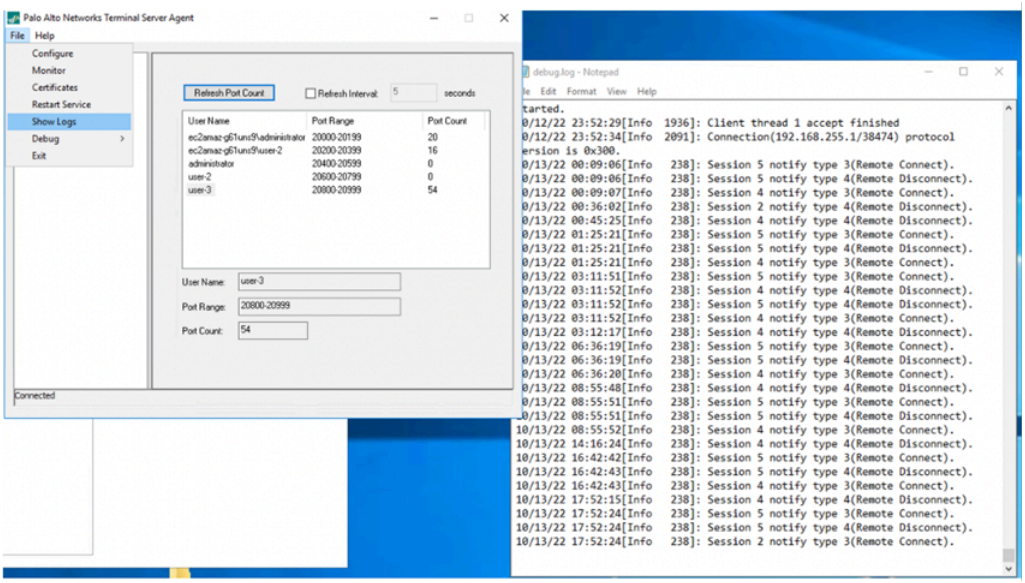


2. リモート ネットワークのIPアドレスがTSエージェントに接続されていることを確認します。

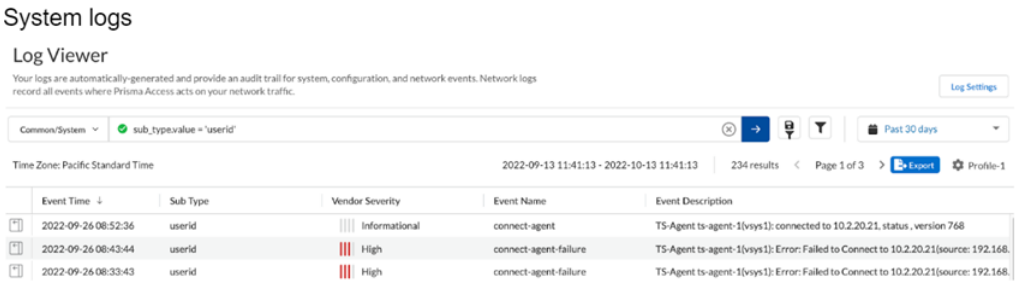


3. [ファイル] > [ログの表示]に移動して、TSエージェントのログ メッセージを表示します。

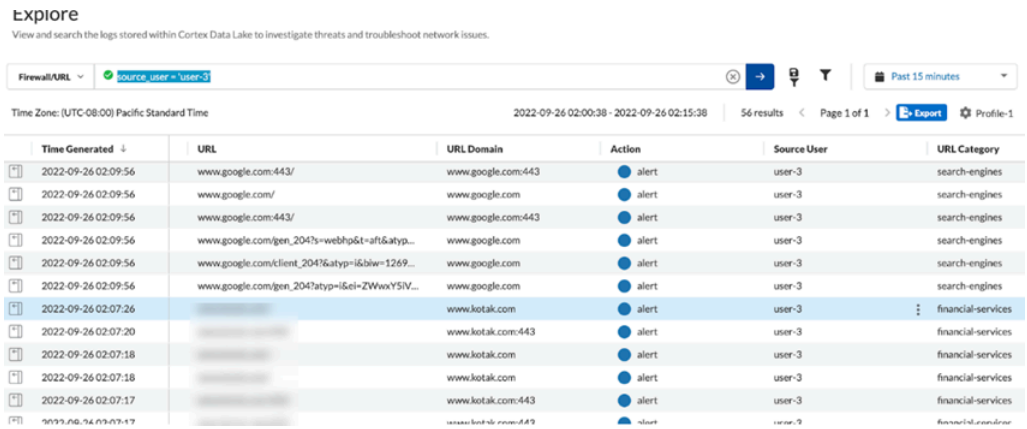
©2025 Palo Alto Networks, Inc.



4. Prisma Access (Managed by Strata Cloud Manager)で、**[Activity (アクティビティ)]** > **[Log Viewer (ログ ビューアー)]** > **[Common/System (共通/システム)]** に移動し、リモート ネットワークがTSエージェントに接続できることを確認します。



5. **[Activity (アクティビティ)]** > **[Log Viewer (ログ ビューアー)]** > **[Firewall/URL (ファイアウォール/URL)]** に移動し、リモート ネットワークがIDベースのポリシーを適用できることを確認します。



 ©2025 Palo Alto Networks, Inc.

Prisma Access監視と可視性

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス ❑ Autonomous DEMアクセスするにはADEM Observabilityライセンスが必要です 。

Prisma Accessはセキュリティ アクティビティを把握し、デプロイメントを監視するために、次の機能を提供します。これらの機能は、ログ、リモート ネットワーク、サービス接続、モバイル ユーザー、ライセンスを取得したエンティティ全体のアラート通知、およびインタラクティブ ダッシュボードを通じてネットワークとユーザーのトラフィックを可視化し、ネットワークで動作しているアプリケーション、脅威、ユーザー、セキュリティ サブスクリプションに関するデータを包括的に表示します。また、Strata Cloud ManagerではPrisma Accessを監視することもできます。

- Prisma Accessログ

  ログは自動生成され、システム、設定、およびネットワークイベントに監査証跡を提供します。ネットワーク・ログは、Prisma Accessがネットワーク・トラフィックに作用したすべてのイベ ントを記録します。たとえば、Prisma Accessがセキュ リティ ルールに基づいてトラフィックをブロックしたとき、認証ルールに基づいてユーザーにアクセスを許可したとき、またはQoSルールに基づいてトラフィックをシェーピングしたときに、エントリが記録されます。Prisma Accessのログは Strata Cloud ManagerとPanoramaの管理インターフェースで見ることができます。

- Prisma Access アクティビティダッシュボードとレポート

  アクティビティは、ログ データから、ポリシーの更新を通知し、エンタープライズのセキュリティとユーザーの生産性のギャップを埋めるために使用できる重要な調査結果まで、ネットワークで何が起こっているかを包括的に表示します。

- Strata Cloud ManagerでPrisma Accessを監視する
- Strata Cloud Managerの監視 (Monitor) と Workflows (ワークフロー) のセクションを使用して、ネットワークトラフィック全体と管理している製品とサブスクリプションを包括的に可視化します。
- Prisma Accessと自律型DEM

  Autonomous DEMはセキュアアクセスサービスエッジ内のすべてのユーザートラフィックに対して、ネイティブでエンドツーエンドの可視性と洞察を提供します（Strata Cloud Manager）。 Autonomous DEM 機能はGlobalProtectアプリケーションとPrisma Access にネイティブに統合されており、したがって、追加のアプライアンスやエージェントを導入する必要はありません。デジタル エクスペリエンスの問題の原因を迅速に特定し、修復を簡素化できます。

- Strata Cloud Managerコマンドセンター

  コマンド センターは、ネットワーク上のIoTデバイス、ユーザー、ホスト、トラフィックのインタラクティブな視覚的な概要を提供します。コマンド センターは、クラウド配信のセキュリティとADEMサブスクリプションのデータを活用して、ネットワーク上のデータの脅威、ユーザー エクスペリエンス、セキュリティに関する重要な情報を表示します。

  この図表形式の表現によりデータとの対話が可能になり、ネットワークで発生したイベントの関係性も可視化できるため、異常な状況を発見し、ネットワーク セキュリティ ルールの強化方法を見つけることができます。

©2025 Palo Alto Networks, Inc.

Prisma Accessログ

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

ログが自動的に生成されます。これはタイムスタンプされたファイルで、システムイベントまたはPrisma Accessが監視するネットワークトラフィックイベントの監査証跡を提残します。ログエントリには artifacts が含まれます。これはログされたイベントのプロパティ、アクティビティ、挙動です。つまり攻撃者のアプリケーションタイプや IP アドレスなどです。各ログタイプは個別のイベントタイプの情報を記録します。たとえば、Prisma Accessはスパイウェア、脆弱性、またはウイルスのシグネチャに一致するトラフィックを記録する脅威ログを生成する場合があります。Prisma Access (Managed by Strata Cloud Manager)は、ネットワークログ(トラフィック、脅威、URL、ファイル、HIPマッチなど)、エンドポイントログ、共通ログ(システムと構成)を提供します。ログエントリごとに詳細を表示できます。また、脅威ログについては、脅威の詳細を確認し、脅威のオーバーライドが実施されているかどうかを確認できます。

- Strata Cloud Manager
- Panorama

Prisma Access ログ (Strata Cloud Manager)

Strata Cloud Managerを使用している場合、 **[Incidents & Alerts (インシデントとアラート)] > [Log Viewer (ログ ビューアー)]**に移動します。

Prisma Access (Managed by Strata Cloud Manager)は、ネットワーク ログ (トラフィック、脅威、URL、ファイル、HIPマッチ) と共通ログ (システムと構成) を提供します。

各ログ エントリの詳細を表示できます。また、脅威ログについては、脅威の詳細を確認し、脅威のオーバーライドが実施されているかどうかを確認できます。もっと詳しく知る。

Prisma Access ログ (Panorama)

Prisma Access (Managed by Panorama)インターフェースでPrisma Accessログを見ることもできます。Prisma Accessインフラストラクチャは、すべてのログをStrata Logging Serviceに転送する。 Prisma Accessは、クラウド サービス プラグインを使用して DD からログ結果を取得し、リモート ネットワークとモバイル ユーザーのトラフィック・ログの集計ビューを提供します。Prisma Access、PanoramaまたはStrata Cloud Managerに使用している管理インターフェースに関係なく、Prisma Access (Managed by Strata Cloud Manager)の[アクティビティ > ログ] > [ログビューア]でログを見ることができます。

Prisma Accessクラウド サービス インフラからのログに加えて、.NET Frameworkを管理するPanoramaアプライアンスから直接ログを表示することもできます。ログを表示するには、**Monitor (監視) > Logs (ログ)**へ移動します。もっと詳しく知る。

©2025 Palo Alto Networks, Inc.

外部ログおよびその他のデータ

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

Activity (アクティビティ) > **Logs** (ログ)に保存されているPrisma Accessログについて、すでにご覧になったり操作したりすることに慣れているかもしれません。しかし、TBライセンスあたりのCortex XDR Proデータレイクを使用している場合、Prisma Accessが様々な外部サードパーティ送信元からのログやその他のデータの取り込みもサポートしていることをご存知ですか？セットアップが完了したら、Strata Logging Serviceハブ 上のアプリを使用してログを表示し、ログ転送を設定します。サポートされているベンダーは次のとおりです。

• Windowsイベントコレクタのアクティブ化	• Corelight Zeek	• PAN IoT Security
• Amazon S3	• ElasticSearch Filebeat	• PingFederate
• Apache Kafka	• Forcepoint DLP	• PingOne for Enterprise
• AWS	• Fortinet Fortigate	• Prisma Cloud
• AWS CloudTrailとAmazon Cloudwatch	• Google Cloud Platform	• Prisma Cloud Compute
• Azure Event Hub	• Google Kubernetes Engine	• Proofpoint Targeted Attack Protection (プルーフポイント標的型攻撃対策)
• Azure Network Watcher	• Google ワークスペース	• ServiceNow CMDB
• BeyondTrust Privilege Management Cloud	• Microsoft Azure	• Elasticsearch Filebeatを使用したWindows DHCP
• Check Point FW1/VPN1	• Microsoft Office 365	• Workday
• Cisco ASA	• Okta	• Zscaler Cloud Firewall

サードパーティ ソースから取り込まれたログを唯一のデータ ソースとして使用することも、Palo Alto NetworksPrisma Accessログおよび追加のデータ ソースと組み合わせて使用することもできます。

Palo Alto Networks を使用すると、ネットワーク、エンドポイント、クラウドなど、すべてのデータ ソースからデータを収集、統合、正規化することで、運用上の負担を軽減し、SOC運用を大幅に簡素化できます。エンタープライズ全体のアプリケーションの使用状況、トラフィックパターン、脅威、インシデントに関する統合ビューと実用的な知見を取得します。

©2025 Palo Alto Networks, Inc.

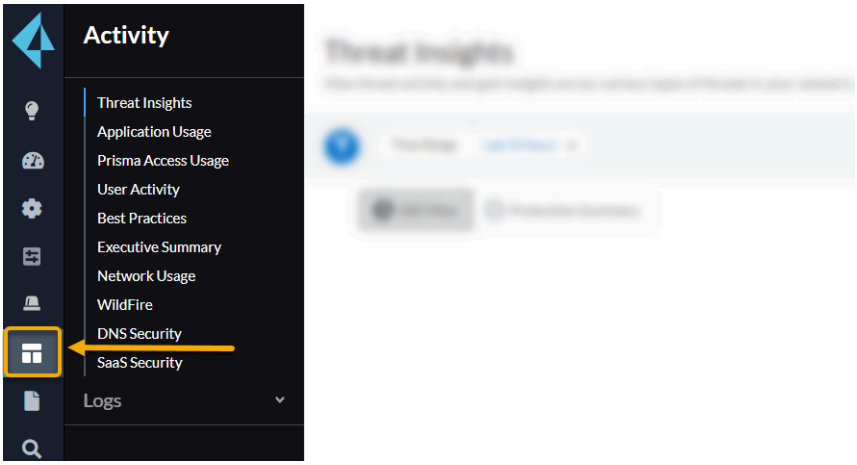
Prisma Access アクティビティダッシュボードとレポート

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Panorama Managed Prisma Access	❑ Prisma Accessのライセンス ❑ アクティビティダッシュボードとレポートのライセンスとその他の要件を確認する

アクティビティでは、 ポリシーの更新を通知し、企業のセキュリティとユーザーの生産性のギャップを埋めるために使用できる重要な調査結果が特定されます。アクティビティにより、次のことが実現します:

- ネットワークで動作しているアプリケーション、脅威、ユーザー、セキュリティ サブスクリプションに関するデータを探索できるインタラクティブなダッシュボード。
- オフラインで共有したり、定期的な更新をスケジュールしたりできるレポート。
- Log Viewer (ログビューア)では、システム、設定、およびネットワークイベントの監査証跡を実施できます。ダッシュボードからログ ビューアーに移動して、より多くのコンテキストを取得し、データをドリルダウンすることができます。
- セキュリティ アーティファクトの検索を使用すると、ファイル ハッシュ、URL、ドメイン、IPアドレス (IPv4またはIPv6) などのアーティファクトを検索して、そのアーティファクトのみのデータと対話できます。検索結果には、アーティファクトの履歴、アーティファクトに関する脅威インテリジェンス、アーティファクトに関するサードパーティの分析結果が含まれます。

Prisma Access (Managed by Strata Cloud Manager)およびPanorama Managed Prisma Accessユーザーは Prisma Access (Managed by Strata Cloud Manager)アプリからアクティビティを使用できます。まず、左のナビゲーション ペインからPrisma Access (Managed by Strata Cloud Manager)を起動し[アクティビティ]タブをクリックします。



 ©2025 Palo Alto Networks, Inc.

インサイトは、Prisma SASE FedRAMP High「In Process」認定の一部としてサポートされています。アクティビティは、Prisma SASE FedRAMP High「In Process」認定の一部としてサポートされています。

- アクティビティを始める

©2025 Palo Alto Networks, Inc.

Strata Cloud ManagerでのPrisma Accessの表示と監視

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス ❑ これはPrisma Access Insightsの機能です。

Palo Alto NetworksStrata Cloud Manager Command Centerは、AIを活用したネットワーク セキュリティ プラットフォームです。Strata Cloud ManagerとStrata Cloud Manager Command Centerを使用すると、単一の合理化されたユーザー インターフェースから、Palo Alto Networksネットワーク セキュリティ インフラストラクチャを簡単に管理できます。

Command CenterのActivity Insights、Command Centerの[Monitor (監視)]と[Workflows (ワークフロー)]セクションを使用して、ネットワーク トラフィック全体、管理している製品やサブスクリプションの包括的な可視性を得ることができます。

- アプリケーションの表示と監視- 使用しているアプリケーションに関する情報については、**[Activity Insights (アクティビティ インサイト)] > [Applications (アプリケーション)]** にアクセスしてください。
- アプリケーション アクセラレーションの表示と監視- アプリケーション アクセラレーションは、アプリケーションのパフォーマンス低下の原因に対処し、リアルタイムでその影響を軽減して、Prisma Access GlobalProtectおよびリモート ネットワーク ユーザーのユーザー エクスペリエンスを向上させます。高速化されたすべてのアプリケーションの詳細を表示するには、 **Activity Insights (アクティビティ インサイト) > アプリケーション** に移動します。
- モバイル ユーザーの表示-すべてのユーザーでは、 次世代ファイアウォール (NGFW) やPrisma AccessなどのPalo Alto Networksのセキュリティ ソリューションに接続しているすべてのユーザーの概要が提供されます。ブランチ サイト、サービス接続、リモート ロケーションのいずれであっても、ユーザーのNGFWまたはPrisma Accessへの接続ステータスを簡単に確認できます。**Activity Insights (アクティビティ インサイト) > Insights (インサイト) > Users (ユーザー)** に移動して、Prisma Access **Agent Users (エージェント ユーザー)** 、 **Agentless Proxy Users (エージェントレス プロキシ ユーザー)** 、 **Office Users (オフィス ユーザー)**、**Other Users (その他のユーザー)**に関する情報を表示します。
- ブランチ サイトの表示と監視-**[Monitor (監視)] > [Branch Sites (ブランチサイト)] > [Prisma Access]** に移動して、リモート ネットワークの健全性と接続性、およびさまざまな Prisma Access の場所にデプロイされているすべてのリモート ネットワークの使用状況を表示します。リアルタイムの接続ステータスと帯域幅消費の詳細、およびその他のデプロイメントの詳細が表示されます。モバイル ユーザー、支社、小売店はリモート ネットワークに接続します。リモート ネットワークとモバイル ユーザーに設定されているトンネルの正常性も表示できます。

©2025 Palo Alto Networks, Inc.

- データ センターの表示と監視-**[Monitor (監視)] > [Data Centers (データセンター)] > [Service Connections (サービス接続)]**に移動して、集約されたサービス接続データと個々のサービス接続に関する情報を表示します。

  [Monitor (監視)] > [Data Centers (データセンター)] > [ZTNA Connectors (ZTNAコネクタ)] に移動して、ZTNAコネクタ グループと個々の ZTNA コネクタの健全性とステータスを表示します。
- ZTNA コネクタ アクセス オブジェクトを可視化するには**[Monitor (監視)] > [Data Centers (データセンター)] > [ZTNA Access Objects (ZTNAアクセスオブジェクト)]** に移動します。
- ネットワーク サービスの表示と監視-**[Monitor (監視)] > [Network Services (ネットワークサービス)] > [GlobalProtect Authentication (GlobalProtect認証)]**に移動して、アプリケーションへのアクセスに関するユーザー エクスペリエンスに影響する一般的なネットワーク サービスのパフォーマンスを表示します。ネットワークサービスには、GlobalProtect認証の成功数と失敗数のレポートが含まれ、モバイルユーザーがPrisma Accessに接続できるかどうかの指標となります。指定した時間範囲内にサーバーに転送された DNS プロキシ要求と応答を表示するには**[Monitor (監視)] > [Network Services (ネットワークサービス)] > [DNS]**に移動します。
- サブスクリプションの使用状況の表示と監視-**[Monitor (監視)] > [Subscription Usage (サブスクリプションの使用状況)]**と、これまでに消費したライセンスの数など、**Prisma Access Base**サブスクリプションの詳細が表示されます。
- **Prisma Access** の場所の表示と監視-**[Monitor (監視)] > [Prisma Access Locations]**に移動して、リモート ネットワークとモバイル ユーザーのすべてのPrisma Accessのロケーションの健全性の概要を確認します。Prismaアクセス ロケーションのステータスとStrata Logging Service接続を表示する時間範囲を選択したり、すべてのPrismaアクセス ロケーションを一覧表示する表を表示したり、個々のPrisma Accessロケーションを名前で選択してその詳細を表示したりできます。
- **Prisma Access** のアップグレードの表示-**[Workflows (ワークフロー)] > [Software Upgrades (ソフトウェア アップグレード)] > [Prisma Access]**を選択して、Prisma Access のアップグレード プロセスに関する情報を表示します。
- サードパーティのデバイス **ID** の表示と監視-**[Monitor (監視)] > [Devices (デバイス)] > [IOT]** に移動して、過去30分以内に接続されたIoTデバイスの数、選択した時間範囲内に接続されたすべてのIoTデバイス、接続されたすべてのIoTデバイスの詳細など、IoTデバイスに関する分析情報を取得します。
- リモート ブラウザ分離の表示と監視-**{Monitor (監視)} > {Users (ユーザー)}**を選択すると、アクティブなRBIユーザーの数、傾向、接続ステータス、RBIロケーション ステータス、トラフィック測定、ライセンス消費などのメトリックを表示して、RBIデプロイメントを可視化できます。

Strata Cloud ManagerでPrisma Access Monitoringを開始する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス ❑ これはPrisma Access Insights機能です。

©2025 Palo Alto Networks, Inc.

Prisma Accessでは、Strata Cloud Managerコマンドセンターで Prisma Access環境を継続的に監視することができます。複数のダッシュボードにより、さまざまなデプロイメント、アラート、および Prisma Accessインフラストラクチャを集中的に表示できます。イベントやステータスに注意が必要な場合、 Prisma Accessによってアラート通知が送信されるので、修正可能な問題をすぐに特定できます。また、Prisma Accessチームが取り組んでいる修正も見ることができます。Autonomous DEMライセンスがあれば、時間範囲を選択または設定することで見たいデータをフィルタリングし、[Monitor (監視)]ページでベースライン情報を見ることができます。

Time Range Selection Filter (時間範囲選択フィルター)

Time Range (時間範囲) 選択フィルターは、時間範囲で情報をフィルターするダッシュボードの上部に表示されます。

時間はローカライズされているため、お住まいの地域の現地時間に基づいてフィルタリングできます。データは1分ごとに取得されますが、ほとんどのヒストグラムに表示されるデータポイントは、選択した 時間範囲 によって異なります。

便利なように、Prisma Accessでは、いくつかの定義済みの範囲から時間範囲を選択するか、独自の日付と時刻の範囲を設定することができます：

- 最後の**15**分

  3分ごとに1つのデータポイント、合計5つのデータポイント。
- 過去**1**時間

  3分ごとに1つのデータポイント、合計20のデータポイント。
- 過去**3**時間

  3分ごとに1つのデータポイント、合計60のデータポイント。
- 過去**24**時間

  5分ごとに1つのデータポイント、合計288のデータポイント。
- 過去**7**日

  30分ごとに1つのデータポイント、合計336のデータポイント。
- 過去**30**日

  3時間ごとに1つのデータポイント、合計180のデータポイント。

©2025 Palo Alto Networks, Inc.

- カスタム

  フィルターで使用可能な事前設定された時間範囲の選択に加えて、カスタムの時間間隔 (たとえば、日付と時刻の例は 6月1日の午後5時に開始し、6月2日の午後4時に終了します) を設定できます。

  開始時刻を設定するには、まずカレンダーで日付を選択し、次に **[Start (開始)]**の下の時刻を選択します。開始時間を適用し、カレンダーで終了日を選択し、**[End (終了)]**で時間を選択して終了時間を設定します。

  カスタム時間範囲を設定すると、それが保存され、リアルタイム データではなく時間範囲フィルターを使用してデータを表示する Insights 内のすべてのウィジェットに適用されます。

  カスタム時間間隔については、事前に入力された 時間範囲 の選択肢から選択できます。

  - 最後の**15**分

    3分ごとに1つのデータポイント、合計5つのデータポイント。
  - 過去**1**時間

    3分ごとに1つのデータポイント、合計20のデータポイント。
  - 過去**3**時間

    3分ごとに1つのデータポイント、合計60のデータポイント。
  - 過去**24**時間

    5分ごとに1つのデータポイント、合計288のデータポイント。
  - 過去**48**時間

    30分ごとに1つのデータポイント、合計96のデータポイント。
  - 過去**7**日

    30分ごとに1つのデータポイント、合計336のデータポイント。
  - 過去**30**日

    3時間ごとに1つのデータポイント、合計240のデータポイント。

ウィジェットのベースライン

購入した場合はAI-Powered ADEMライセンスがある場合、次のモニター ページのトレンド ウィジェット全体にベースライン データ バンドが表示されます。ユーザー、ブランチ サイト、データセンター、およびネットワーク サービス。ウィジェットは、トレンド ライン全体にわたって背景にベースラインを表示します。これにより、データがベースラインの上限または下限を超えたかどうかを一目で確認できます。

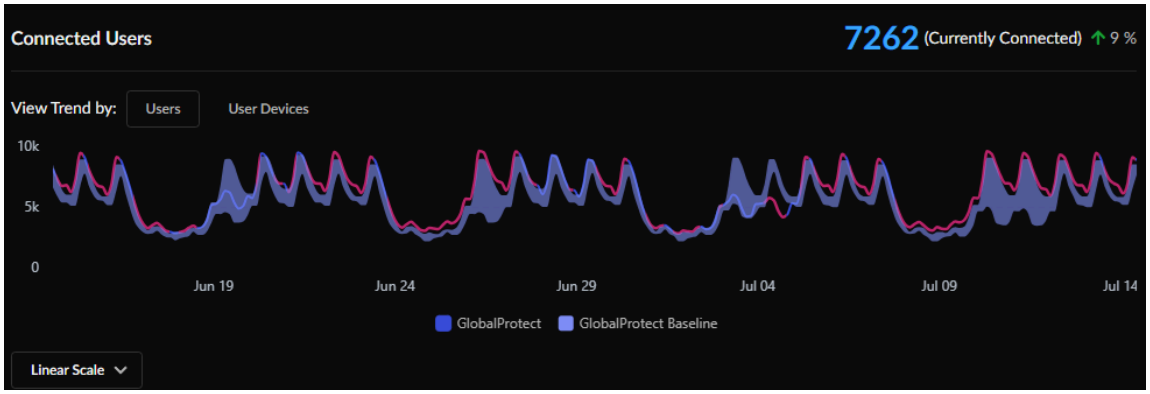
ベースラインデータは、1時間単位で計算され、特定のトンネル、サイト、Prisma Accessのロケーション、またはGlobalProtectのユーザー数について、それらの1時間単位のビンの過去28日間のデータを考慮します。たとえば、火曜日の午後1時から午後2時までのベースラインは、過去4週間の火曜日の午後1時から午後2時までの時間枠から計算されます。下限は収集された履歴データの10パーセンタイルであり、上限は90パーセンタイルです。これにより、帯域幅、ユーザー数、認証数、DNSプロキシの要求と応答の傾向を確認できます。ベースライン データは過

 ©2025 Palo Alto Networks, Inc.

去28日間の履歴データから取得されるため、ベースラインを正しく計算するには、新しくオンボードされたテナントが28日間稼働し、データが豊富である必要があります。データが28日未満の場合、矛盾が生じる可能性があります。

ウィジェットのトレンド ラインの値がベースラインの上限または下限から逸脱すると、その期間のトレンド ラインがWebインターフェースに赤で表示されます。

次の例は、[Users (ユーザー)]ページの**[Connected User (接続ユーザー)]**ウィジェットのGlobalProtectベースラインを示します。



アプリケーションの表示と監視

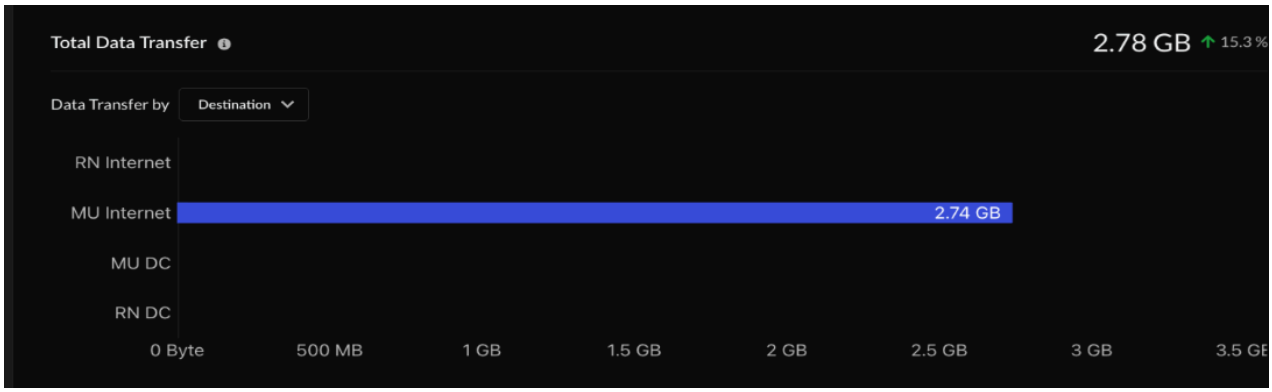
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス ❑ これはPrisma Access Insights機能です。

Strata Cloud Managerコマンドセンターを使用して、ネットワーク内の Prisma Accessアプリケーション、アプリケーションを使用するユーザー、およびそれらの潜在的なセキュリティへの影響を監視します。**Insights (知見) > Applications (アプリケーション)**にアクセスすると、アプリケーションの脅威、ユーザー、データ転送、リスクスコア、ユーザーエクスペリエンスに関する情報とともに、Prisma Accessアプリケーションを可視化できます。

データ転送総数

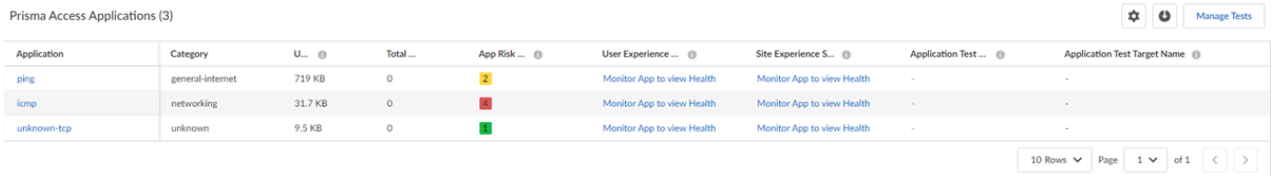
合計データ転送量には、選択した時間範囲におけるPrisma Accessファイアウォール間の合計データ転送量が表示されます。他のフィルターオプションには、「フィルターを追加」ドロップダウンを使用してください。この例では、アプリケーションカテゴリ別のデータ転送が表示され、上位のアプリケーションとそれらのアプリケーションの合計データ転送量が表示されます。宛先別の合計転送データを表示することもできます。

©2025 Palo Alto Networks, Inc.



Prisma Accessアプリケーション

このウィジェットを使用して、どのアプリケーションが監視され、そのアプリケーションで合成テストが実行されているかを確認できます。テーブルには、各アプリケーションの正常性を示すエクスペリエンス スコアも表示されます。［**Manage Tests (テストの管理)**］ボタンをクリックすると、［Application Tests (アプリケーションテスト)］テーブルにすべてのPrisma Accessアプリケーションに設定されているすべての合成テストが表示されます。



列	詳説
アプリケーション	監視対象のアプリケーションのアプリケーションID。
カテゴリ	アプリケーション タイプ
使用率	特定のアプリケーションに対して検出されたPrisma Accessインフラストラクチャ内のトラフィックの合計です。
脅威の総数	アプリケーションが受けた脅威の総数。
アプリケーション リスクスコア	この特定のアプリケーションの脅威データ。1 が最もリスクが低く、5 が最も高いリスクです。
ユーザー体験	Autonomous DEMが収集したアプリケーションエクスペリエンススコア。このアプリケーションで監視されているすべてのユーザーを対象に集計されます。

©2025 Palo Alto Networks, Inc.

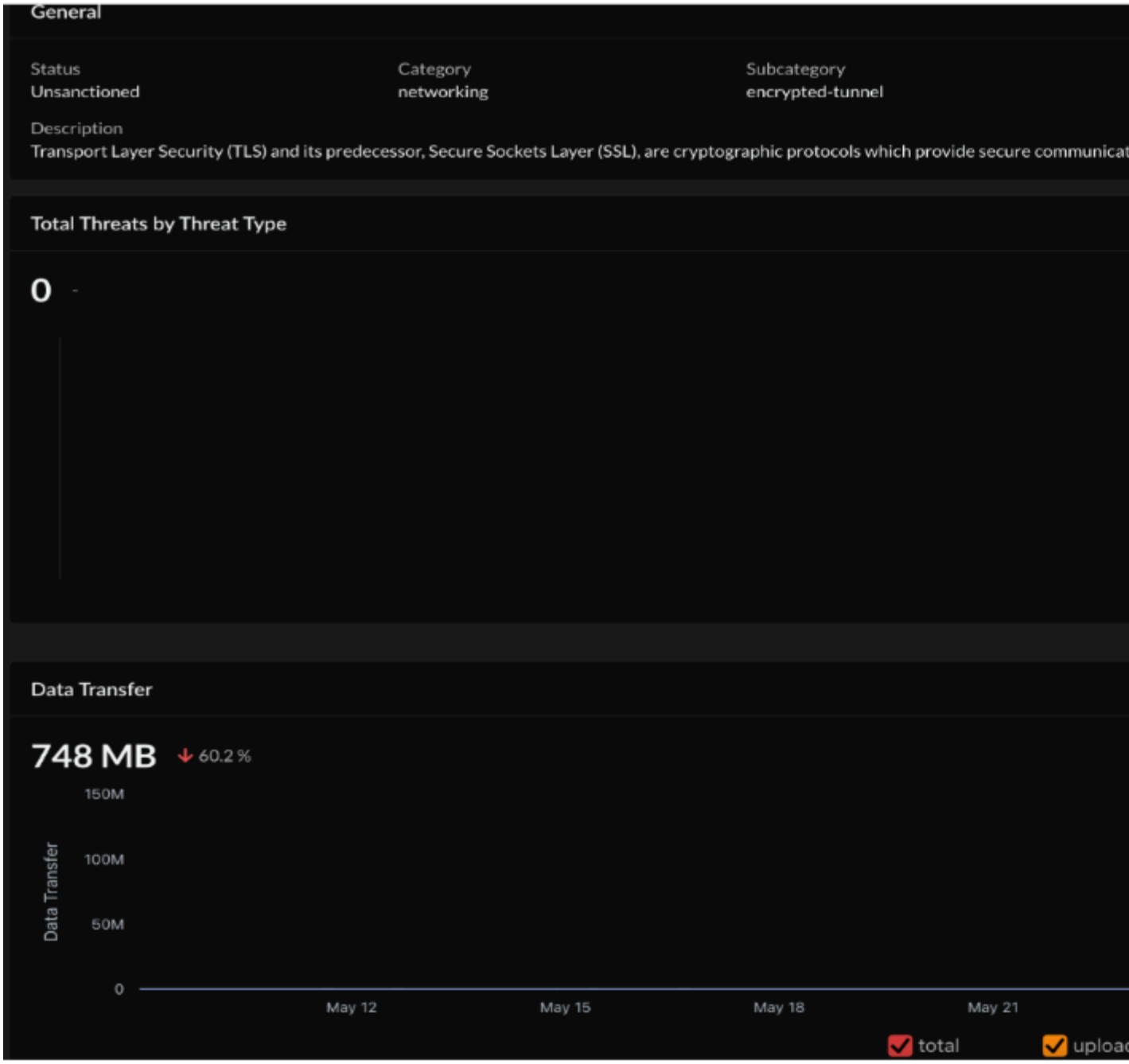
列	詳説
サイトエクスペリエンススコア	この特定のブランチサイトのアプリケーションエクスペリエンススコア。
アプリケーションテスト名	このアプリケーション用にユーザーが設定したテストの名前。
アプリケーション テスト ターゲット名	さまざまなエンドポイントからの模擬テストの対象となる FQDN の IP アドレス。

アプリケーションの詳細情報

アプリケーションを選択すると、ステータス、カテゴリ、サブカテゴリ、ポート、テクノロジー、リスクスコアなどの一般的な詳細が表示されます。

- 脅威タイプ別の脅威の合計 – アプリケーションに対する現在の脅威。
- 合計ユーザー数 – 指定された時間範囲内にこのアプリケーションにアクセスしたユーザーの総数。
- データ転送 – このアプリケーション用にアップロードまたはダウンロードされたデータが表示されます。

©2025 Palo Alto Networks, Inc.



アプリの高速化の表示と監視

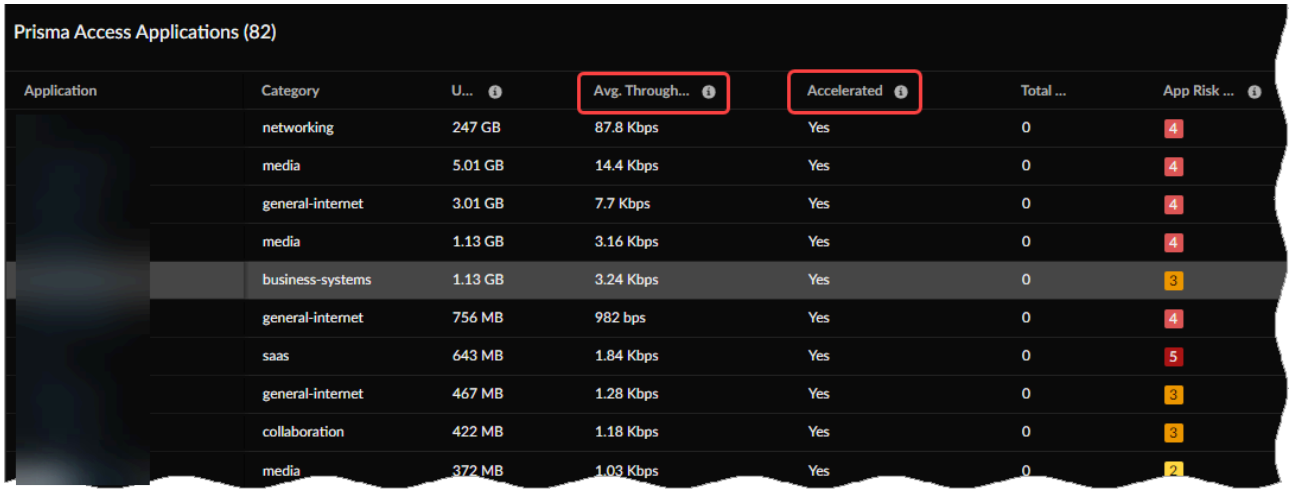
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessのライセンス

©2025 Palo Alto Networks, Inc.

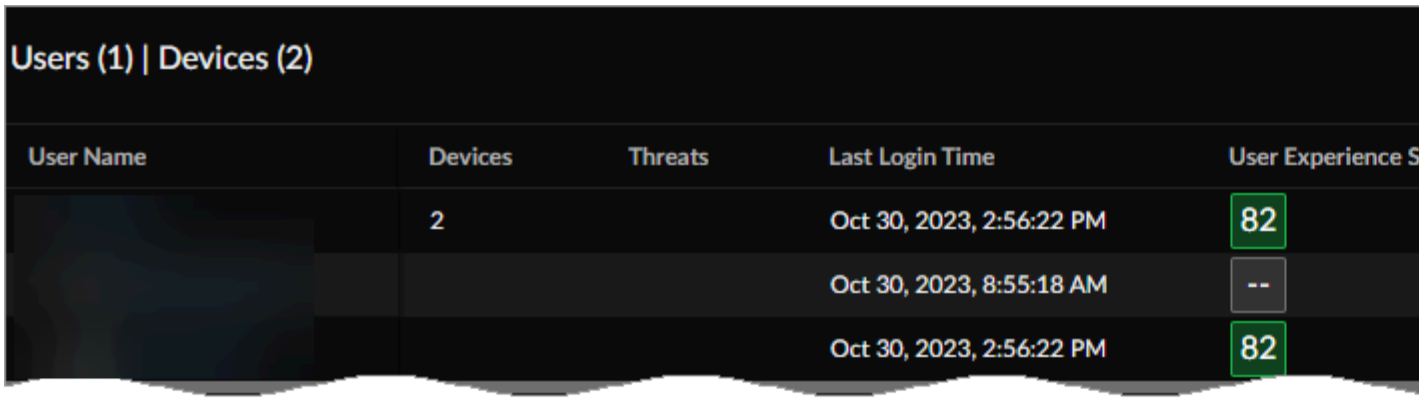
App Acceleration (アプリアクセラレーション)は、アプリケーションパフォーマンスの低下の原因に対処し、リアルタイムで対処して緩和することで、Prisma AccessGlobalProtectとリモートネットワークユーザーのユーザーエクスペリエンスを向上させます。

ユーザーがアプリケーションにアクセスすると、ワイヤレス接続の低下、ネットワークの輻輳、その他の要因によってスループットが低下し、アプリケーションのパフォーマンスが低下することがあります。これらのネットワークの問題は、従業員のエクスペリエンスに悪影響を及ぼし、生産性を低下させる可能性があります。アプリアクセラレーションは、デバイスの機能、ネットワークの機能、アプリケーションのコンテキストを安全に把握してスループットを最大化し、変化するネットワーク状況に合わせてリアルタイムで調整します。

Strata Cloud Managerコマンドセンターで、**[Insights (知見)] > [Applications (アプリケーション)]** に移動して、環境内で高速化されたアプリケーションの詳細を表示します。Prisma Accessアプリケーション テーブルには平均が含まれます。(平均) 全体列は、ユーザーのトラフィックが高速化された場合にのみ表示され、高速列には、アプリケーション トラフィックの一部またはすべてが高速化されたことが示されます。



環境内のアプリアクセラレーション ユーザーに関する情報を表示するには、**[Insights (知見)] > [Users (ユーザー)]** に移動します。環境でアプリアクセラレーションが有効になっているユーザーには、ユーザー | デバイス テーブルがあり、そこに[Traffic Accelerated (a高速化されたトラフィック)]列が表示されます。この列は、ユーザーのアプリケーション トラフィックの一部またはすべてが高速化されたことを示します。



 ©2025 Palo Alto Networks, Inc.

AI 搭載の自律型DEM (ADEM) は App Acceleration (アプリアクセラレーション)と統合され、高速化されたアプリケーションの数や全体的なパフォーマンスの向上などの指標を提供します。**SASE Health (SASE健全性) > Experience (エクスペリエンス)** にアクセスして、**[Accelerated Applications (高速化されたアプリケーション)]** タブと **[Monitored Applications (監視対象アプリケーション)]** タブで ADEM パフォーマンス メトリック を表示します。

モバイル ユーザーを表示する

どこで使用できますか?	何が必要ですか?
• Prisma® Access(Strata Cloud Managerによる管理)	• Prisma Accessのライセンス • AI搭載ADEMライセンス

Activity Insights (アクティビティインサイト)を確認する:Palo Alto NetworksのPrisma Accessセキュリティ ソリューションに接続されているすべてのユーザとホストの概要を示すユーザー。ユーザーまたはホストのPrisma Accessへの接続ステータスは、ブランチサイト、サービス接続、またはリモートロケーションのいずれであっても簡単に判断できます。表示：

- 現在Palo Alto Networksのセキュリティソリューションに接続しているユニークユーザーとPrisma Accessに接続しているユーザーの合計数。
- 特定の時間範囲内に接続されたユーザーの数を、Prisma Accessを介して接続したユーザー別に分類したもの。
- Prisma Accessを介して接続しているエージェントベースのユーザー。
- Prisma Accessに接続しているエージェントベースまたはブラウザベースの明示型プロキシユーザー。
- Prisma Access Browsersを介して接続したユーザー。
- Prisma Accessにアクセスしている管理対象外デバイスユーザーのリスト。
- ブランチ ロケーションからPrisma Accessに接続しているユーザーのリスト。
- 特定のサービス接続を使用してデータセンターを接続しているユーザーのリスト。

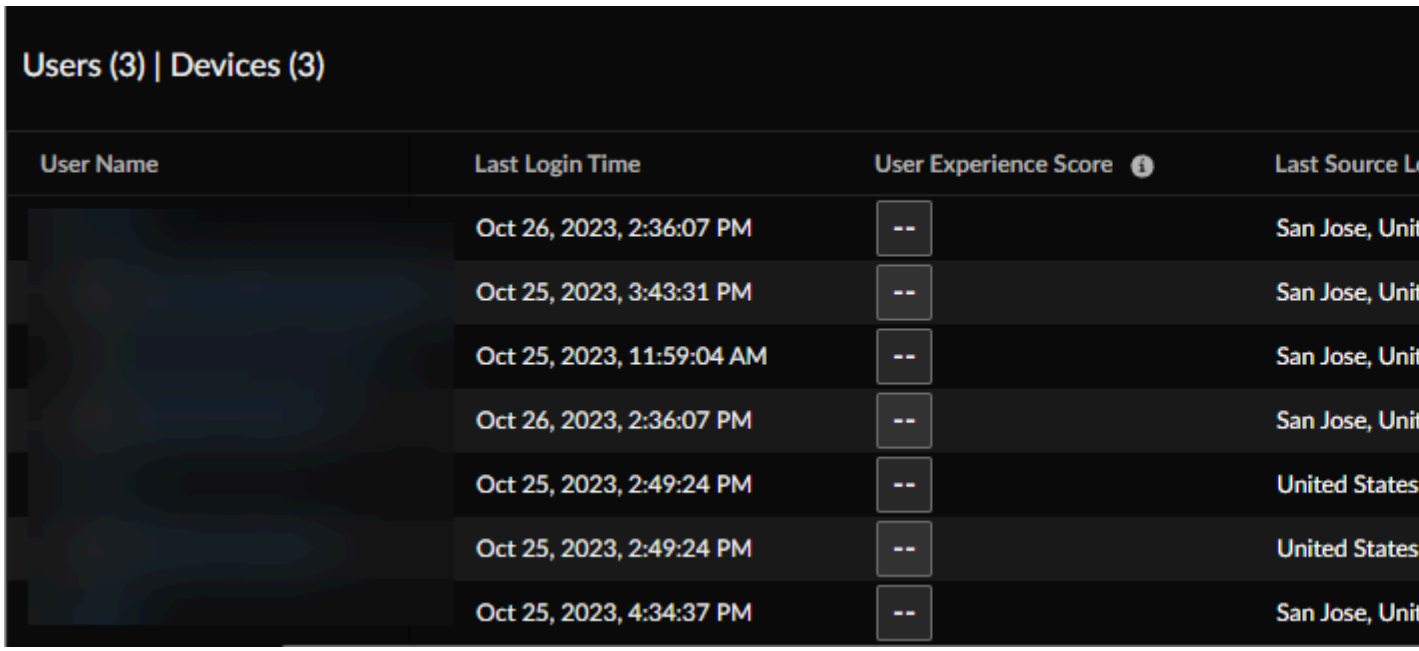
モバイル ユーザー向けのIPv6の表示と監視

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 5.0 イノベーション ❑ Prisma Accessライセンス

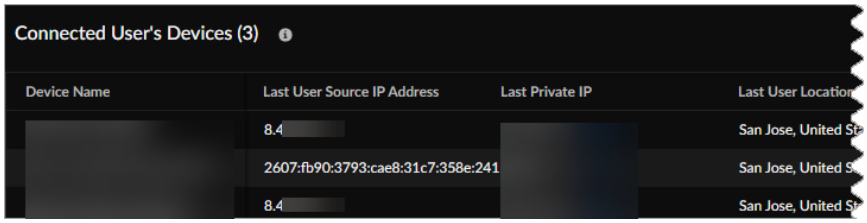
モバイルユーザー - GlobalProtectデプロイメントで IPv6ネットワークを 使用する場合は、Prisma Accessを設定することで、モバイル ユーザー ネットワークで IPv6 アドレスを使用できます。また、IPv6アドレスを使用する前に、Prisma AccessインフラストラクチャでIPv6ネットワークをグローバルに有効にする必要があります。

©2025 Palo Alto Networks, Inc.

GlobalProtect デプロイメントに IPv6 を使用すると、ユーザー |[デバイス] テーブルの [送信元IPアドレス] 列に IPv4 アドレスまたは IPv6 アドレスが表示されます。

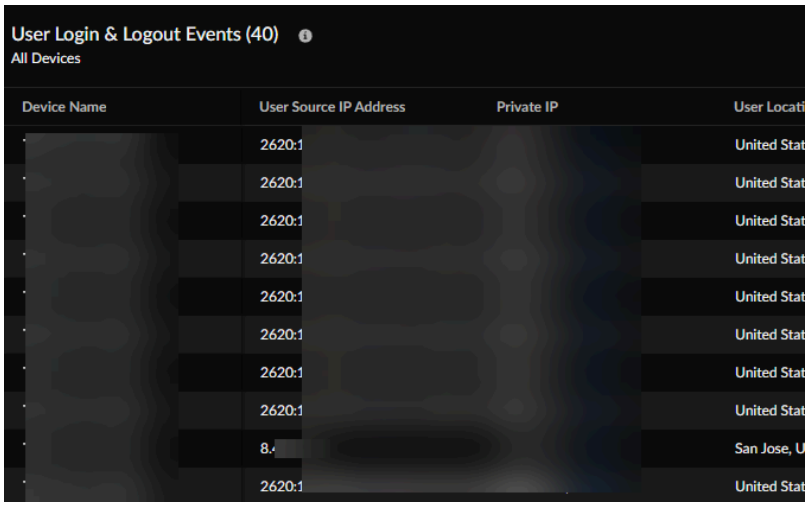


接続しているユーザーを選択すると、そのユーザーのデバイスの傾向に関する情報が表示されます。[Connected User's Devices (接続ユーザーのデバイス)] テーブルには、ユーザーのデバイスに関するデータが表示され、これには [最後のユーザーの送信元IPアドレス] や [最後のプライベート IP] など、1 つのデバイス エントリの IPv4 アドレスと IPv6 アドレスを含めることができます。



IPv6 アドレス情報は、[User Login & Logout Events ([ユーザーログイン＆ログアウトイベント)] テーブルで確認できます。[ユーザー送信元IPアドレス] 列と [プライベートIPアドレス] 列には、IPv4 アドレスまたは IPv6 アドレスが表示されます。

©2025 Palo Alto Networks, Inc.



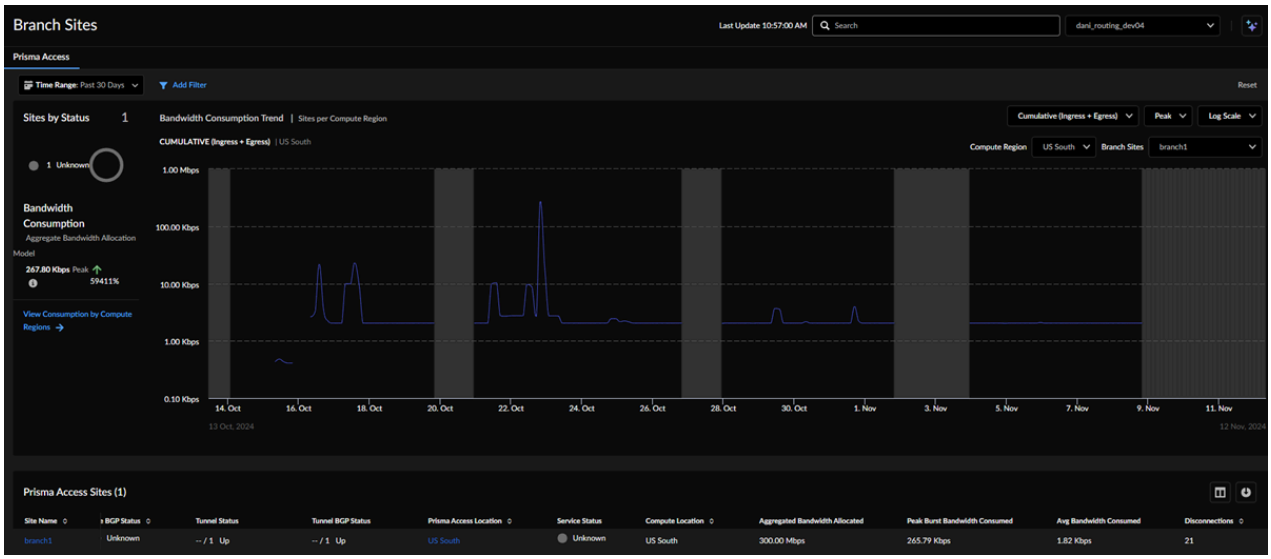
ブランチサイトの表示と監視

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス ❑ adem-aiops-value

[Monitor (監視)] > **[Branch Sites (支店サイト)]** > **Prisma Access** 選択すると、 リモートネットワークの健全性と接続性、およびさまざまなPrisma Access場所に配置されたすべてのリモートネットワークの使用状況が表示されます。リアルタイムの接続ステータスと帯域幅消費の詳細、およびその他のデプロイメントの詳細が表示されます。リモート ネットワークに設定されているトンネルの正常性も表示できます。

リモート ネットワークを計画し、リモート ネットワーク帯域幅を割り当て、リモート ネットワークをオンボードする方法については 、「Prisma Access リモート ネットワーク」 を参照してください。ブランチ サイトを表示するには、**[Monitor (監視)]** > **[Branch Sites (支店サイト)]** > **[Prisma Access]**に移動します。

©2025 Palo Alto Networks, Inc.



ステータス別のサイト

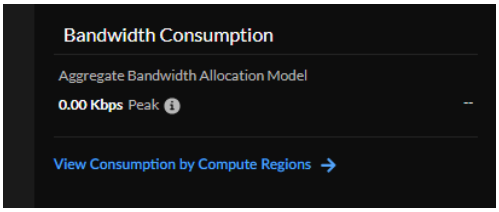
リモート ネットワーク サイトをステータス別に表示します。選択した時間範囲内で、 稼働中、停止中、非アクティブ、または利用不可の状態にあるサイトの数と、 警告 が出ているサイトの数を確認できます。



帯域幅使用量

帯域幅消費量は、集約帯域幅割り当てモデルにおけるテナントのすべてのコンピューティング リージョン全体で、コンピューティング リージョンで消費される最高のピーク帯域幅を示します。サイトごとの帯域幅割り当てモデルでは、すべてのサイトの中でサイトによって消費される最高のピーク帯域幅が表示されます。ピーク値は、選択した時間フィルターの期間にわたって計算されます。

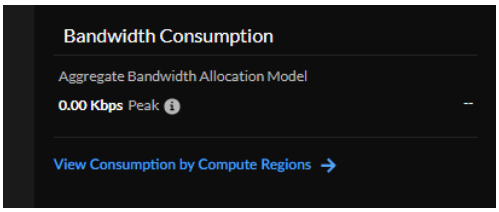
すべてのコンピューティング リージョンと構成済みの IPSec 終端ノードの消費値と傾向グラフを表示するには、[コンピューティング リージョン別の消費量を表示] を選択します。



コンピューティング リージョン別の使用量の表示

[Monitor (監視)] > [Branch Sites (支店サイト)] > Prisma Accessに移動します 。集約帯域幅割り当てモデルを使用する場合は、 帯域幅消費 ウィジェットで [コンピューティング リージョン別の消費量を表示] を選択して、リージョンの帯域幅消費量と傾向を確認します。

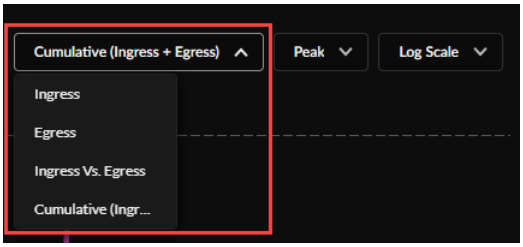
 ©2025 Palo Alto Networks, Inc.



[コンピューティング リージョン] ページには、選択した [時間範囲] 内の帯域幅消費データが表示されます。コンピューティング リージョンの 平均帯域幅、 中央帯域幅、 ピーク帯域幅を示すテーブルを表示できます。

コンピューティング リージョン別の帯域幅消費傾向 グラフには、コンピューティング リージョンに関するデータが表示されます。データをフィルタリングして、表示する情報を絞り込みます。

- 累積（入力+出力）、 入力、 出力、または 入力**vs**出力をドロップダウンから選択します。



- 選択した期間の ピーク、 中央値、または 平均の帯域幅消費傾向を表示します。デフォルト設定は ピーク 帯域幅消費です。



- ログスケール または 線形スケール。
- 計算領域- 表示する領域を 1 つ以上選択します。

IPSec 終端ノード使用率 グラフでは、特定のコンピューティング リージョンで構成された IPSec 終端ノードの帯域幅消費量を表示できます。表示する情報を絞り込むには、データをフィルタリングします。

- データを表示するコンピューティング リージョンを選択します。
- 表示するコンピューティング リージョンの特定のサイトを選択します。
- 選択した IPSec 終端ノードで終了するサイトの帯域幅消費傾向を表示するには、**[Node Aggregate (**ノード集計**)]** または **[Breakdown by Sites (**サイト別の内訳**)]** を選択します。
- ピーク、 平均、または 中央値を表示します。

 ©2025 Palo Alto Networks, Inc.

- ログスケール または 線形スケールを表示します。



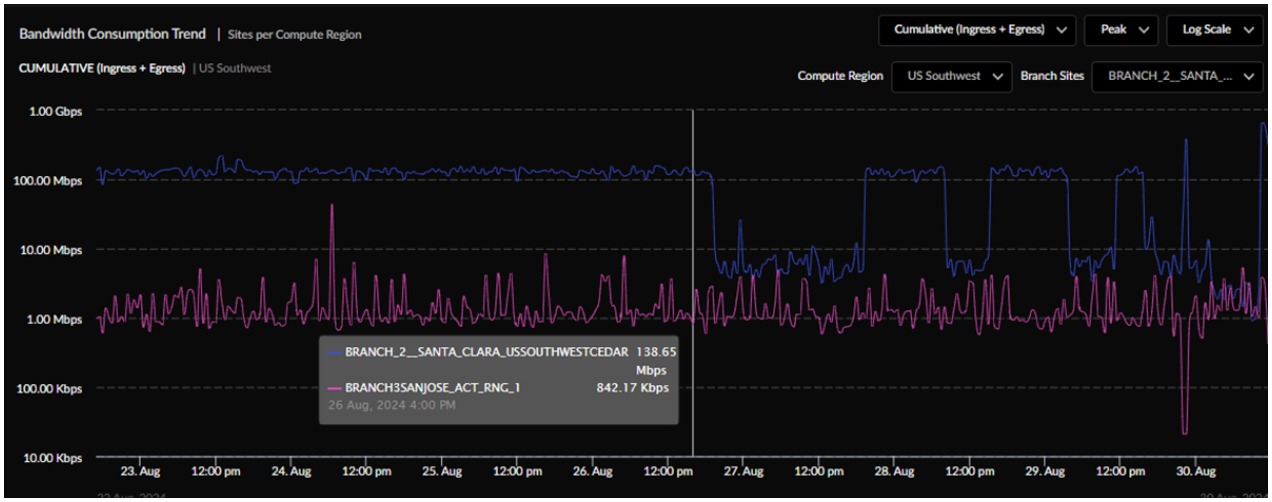
帯域消費量の推移

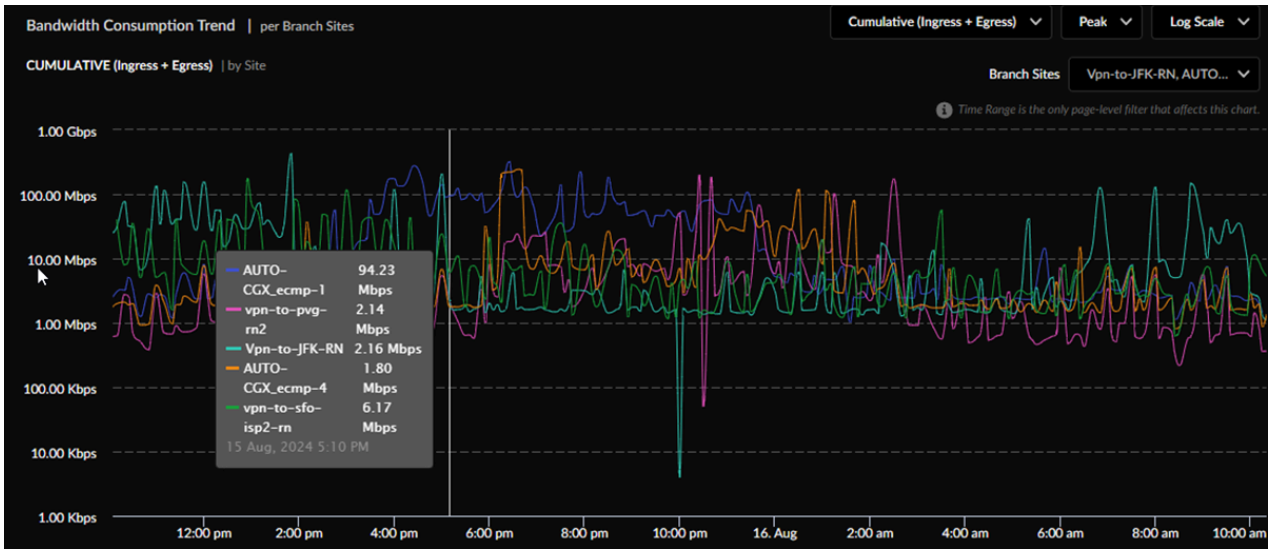
メインの ブランチ サイト ページでは、集約帯域幅割り当てモデルを使用している場合はすべてのコンピューティング リージョンのコンピューティング リージョンごとの帯域幅消費傾向サイト を表示でき、 サイトごとの帯域幅割り当てモデルを使用している場合は ブランチ サイトごとの帯域幅消費傾向を 表示できます。集約帯域幅割り当てモデルの場合、コンピューティング リージョンを選択し、そのコンピューティング リージョン内で帯域幅消費傾向に関心のあるサイトを選択できます。データをフィルタリングして表示する情報を絞り込み、グラフの上にマウスを置くとその時点でのサイトの帯域幅消費量を表示できます。

- デフォルトのビューには 累積 **(**入力 **+** 出力**)** 帯域幅消費量が表示されます。その他のオプションは 入力、出力、または 出力 **vs**出口。
- 選択した期間のピーク、中央値、または 平均の帯域幅消費傾向を表示します。デフォルト設定は ピーク 帯域幅消費です。
- ログスケールまたは線形スケール。

©2025 Palo Alto Networks, Inc.

- コンピューティング リージョン- テナントが集約帯域幅割り当てモデルを使用する場合、リージョン内で終了するサイトの内訳を含むコンピューティング リージョンを表示します。各コンピューティング リージョンについて、そのコンピューティング リージョンで終了するサイトを選択して、帯域幅の消費傾向を表示します。
- ブランチ サイト- 選択した期間のトレンド ラインをグラフに表示するには、最低 1 サイト、最大 10 サイトを選択します。





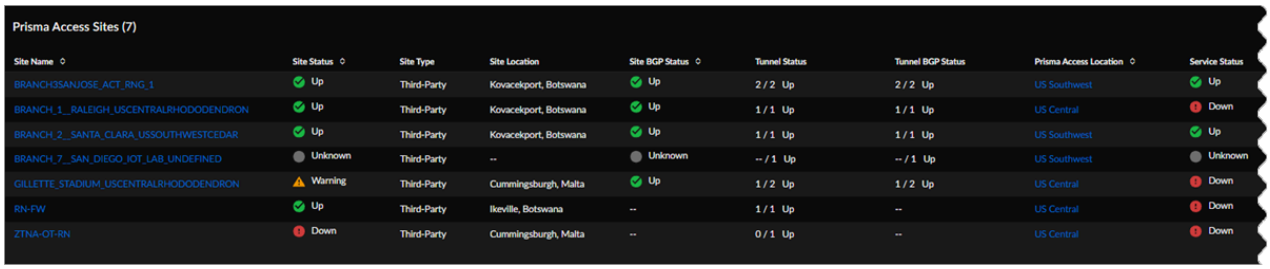
Prisma Access サイト

Prisma Access サイト テーブルにはリモートPrisma Access サイトと情報が表示されます 。

- サイト名- Prisma Access サイトの一意の名前。
- サイトのステータス–稼働中、 停止中、 警告、または 不明。
- サイトの種類- サードパーティ。
- サイトの場所- Prisma Access サイトの場所。
- サイト **BGP** ステータス- サイトの BGP ステータスが 稼働中、停止中、または 不明のいずれかを示します。

©2025 Palo Alto Networks, Inc.

- トンネル ステータス- サイトのトンネルの数と、そのうち稼働中のトンネルの数。
- トンネル **BGP** ステータス- 各トンネルの BGP ステータス。
- **Prisma Access** の場所- この Prisma Access サイトの場所。場所を選択すると、Prisma Access の場所の 詳細が表示されます。
- サービス ステータス- このフィールドは、サイトが接続されているインスタンスまたはファイアウォールのステータスを示します。ステータスは 稼働中、停止中、または 不明になります。
- コンピューティング ロケーション- すべての Prisma Access ロケーションは、最適化されたパフォーマンスとレイテンシに基づいて、セキュリティ処理コンピューティング ロケーションまたはリージョンにマッピングされます。地理的に近い少なくとも 2 つ (多くの場合はそれ以上) の Prisma Access ロケーションが、1 つのコンピューティング ロケーションにグループ化されます。
- 割り当てられた集約帯域幅- 選択した時間範囲内にサイトに割り当てられた集約帯域幅。この列は、集約帯域幅モデルを使用した場合にのみ表示されます。
- 消費されたピークバースト帯域幅- 選択した時間範囲内でこのサイトの入力値と出力値を組み合わせて得られた累積ピーク値。
- 消費された平均帯域幅- 選択した時間範囲内でこのサイトの入力値と出力値を組み合わせて得られた累積平均値。
- 切断- 選択した期間中にこのサイトで切断が何回発生したか。
- 切断期間- 選択した時間範囲内でサイトが切断されていた合計時間（秒単位）。



ハイパフォーマンスなブランチ サイトの可視化

高パフォーマンス ブランチ (RN-HP) は従来のブランチとは異なる属性を持ち、両方がテナント内に共存します。Prisma Access の高パフォーマンス ブランチ サイトには、次のような利点があります。

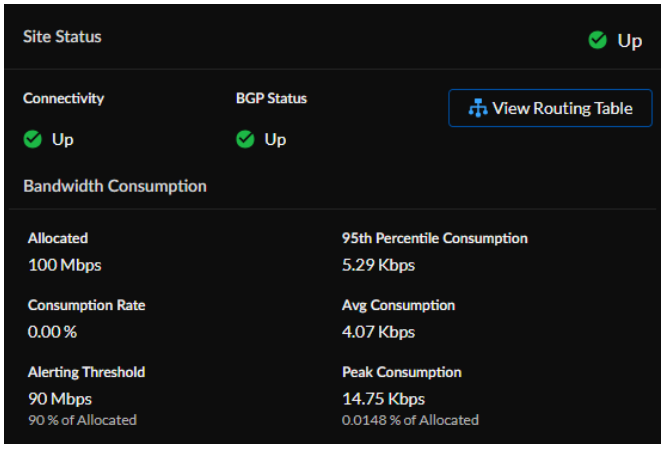
- このアーキテクチャは、ネットワーク処理機能とセキュリティ処理機能を分離することで容量効率に対処します。大容量パケット処理能力を備えた ION デバイスは、最大 5 Gbps の容量を持つ複数のブランチ接続を終端し、セキュリティ処理を SPN に分散します。
- 単一の IP または FQDN を使用して、リージョン内の複数のブランチを単一のネットワーク処理ノード (NPN) に終了できます。
- IPSec 終端ノードへのブランチ サイトの終端を監視および管理する必要がなくなりました。適切な SPN がブランチ トラフィックの検査を実行し、NPN が負荷分散を実行します。
- 冗長性のために異なるリージョンを指定できるようにすることで、真の高可用性を実現できます。

 ©2025 Palo Alto Networks, Inc.

環境内の高パフォーマンス ブランチとレガシー ブランチの両方を表示できます。Strata Cloud Manager で、**[Monitor (監視)]** > **[Branch Sites (ブランチサイト)]** > **[Prisma Access]**に移動し、**[Prisma Accessサイト]** テーブルからブランチ サイトを選択します。

Prisma Access サイトの詳細

任意の Prisma Access サイト名 を選択してその サイト ステータスを表示します。ここでは接続性 と **BGP** ステータス (稼働中、 停止中、 非アクティブ、または 利用不可) を確認できます。選択した時間間隔の帯域幅の ピーク消費量 を表示します。



帯域幅消費傾向 グラフで 累積 **(**入力 **+** 出力**)** 情報を表示できます。

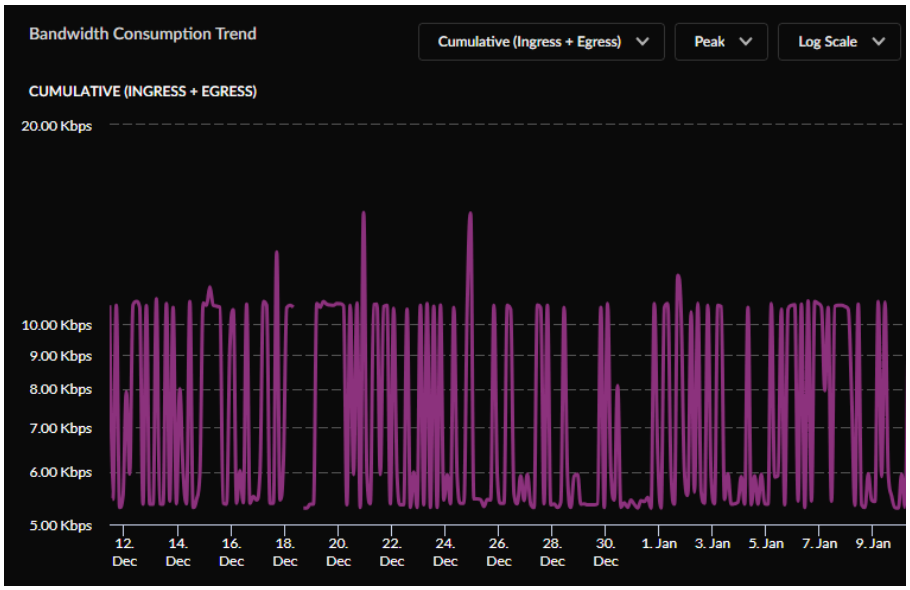
- ドロップダウンを使用して、 入力、 出力、 入力 **vs**出力、または 累積（入力 **+** 出力）です。



- ブランチ サイトの帯域幅消費傾向チャートのメトリックは ピーク (既定)、 平均、または 中央値別で表示されます。



©2025 Palo Alto Networks, Inc.



ルートテーブルの可視性

到達可能性の課題に対処できるように、各リモート ネットワーク サイトのルート テーブルを可視化します。宛先 IP アドレスのルート テーブル検索を実行して、目的の宛先に到達するために使用できるルートがあるかどうかを判断できます。この情報を使用して、障害の他の潜在的な原因を調査できます。この知識があれば、到達可能性に影響を与える可能性のある問題の解決に集中することができます。

[ルーティング テーブルの表示] を選択すると、このブランチの ルーティング テーブルが表示されます。このテーブルには、Prisma Access からブランチで利用可能な宛先の IP ルートが含まれています。

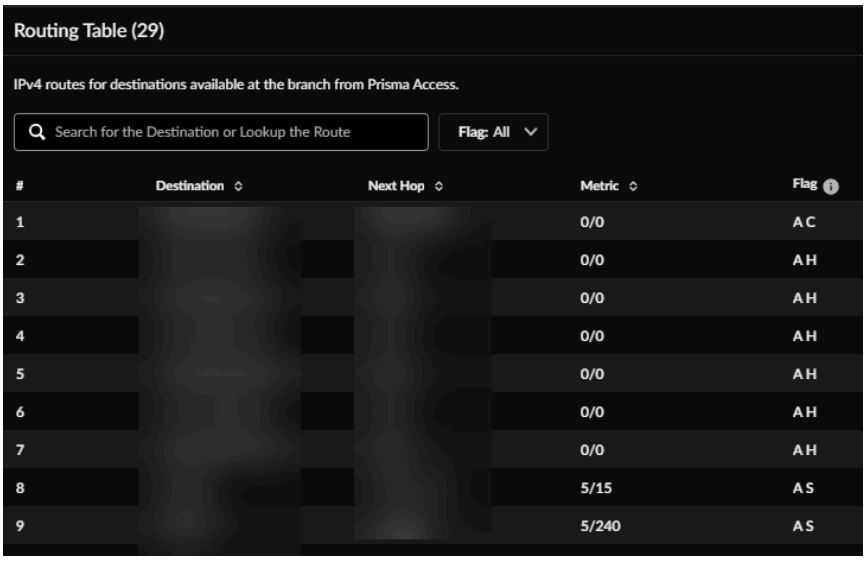
- 検索バーを使用して目的地を選択したり、ルートを検索したりします。
- ドロップダウンを使用して、 フラグでフィルタリングします。

ルーティング テーブルには

- **#**–ルート番号 が表示されます。
- 宛先- 到達可能なネットワークの IP アドレスとサブネット。
- ネクスト ホップ- 宛先ネットワークへの次のホップにあるゲートウェイの IP アドレス。ネクスト ホップが 0.0.0.0 の場合は、デフォルト ルートを表します。
- メトリック- ルーティング プロトコルによって決定されたルートのメトリック。
- フラグ- このルートに関する情報は次のとおりです。
- • **AB**–アクティブで、BGP から学習されました。
  - **AC**–アクティブで接続されています。宛先 - ネットワーク。
  - **AH**–アクティブで接続されています。宛先 - ホストのみ。
  - **AR**–RIP からアクティブに学習。
  - **O1** – OSPF 外部タイプ -1
  - **O2** – OSPF 外部タイプ -2

©2025 Palo Alto Networks, Inc.

- **Oi** – OSPF エリア内
- **Oo**–OSPF エリア間。
- **S**–非アクティブかつ静的。
- **A S** – 動的かつ静的。



トンネル

このサイトのトンネルとトンネル データを表示します。

- トンネル名- トンネルの一意の名前。
- **Prisma Access**ロケーション- このリモート ネットワークの Prisma Accessロケーション。
- トンネルのステータス–稼働中、停止中、**Init (**イニシャル**)**、または 使用不可。
- トンネル **BGP** ステータス–稼働中、停止中、または 不明。
- トンネル監視- トンネル監視を有効にしている場合、この列にはトンネル監視が 稼働中 か 停止中かが表示されます。有効にしていない場合、この列には **[Not Configured (**未構成**)]**と表示されます。
- 平均スループット- 選択した時間範囲のトンネルの平均帯域幅。入力、 出力、 入力 **vs**出力、または選択した 累積（入力 **+** 出力） 値を考慮します。
- ピークスループット- 選択した時間範囲のトンネルのピーク帯域幅。入力、 出力、 入力 **vs**出力、または 累積（入力 **+** 出力）を考慮します。
- 送信元 **IP** アドレス- 送信元 IP アドレス。
- 宛先エンドポイント アドレス- トンネルが稼働しているかどうかを判断するための Prisma Access の IP または FQDN アドレス。
- 切断- 選択した時間範囲内での切断回数。
- 切断期間- 選択した時間範囲内でトンネルが切断されている時間（秒単位）。

トンネル名 を選択すると、 トンネルのステータス、 帯域幅消費傾向、その他のトンネルの詳細が表示されます。

©2025 Palo Alto Networks, Inc.

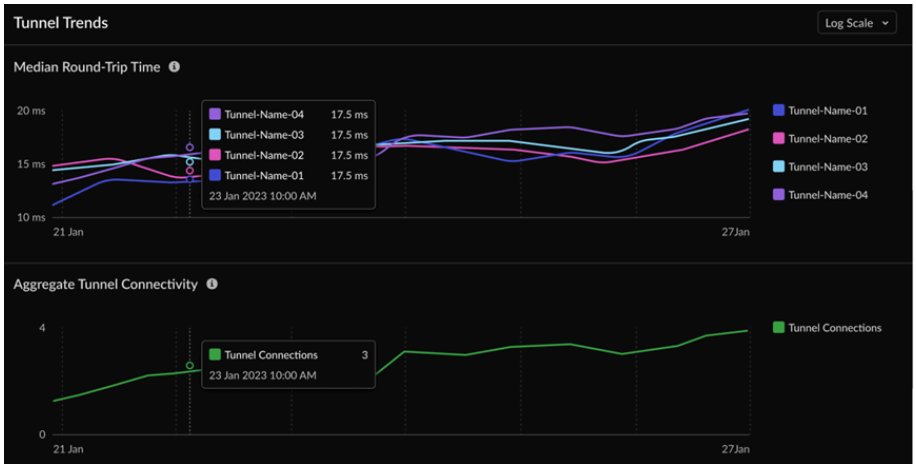


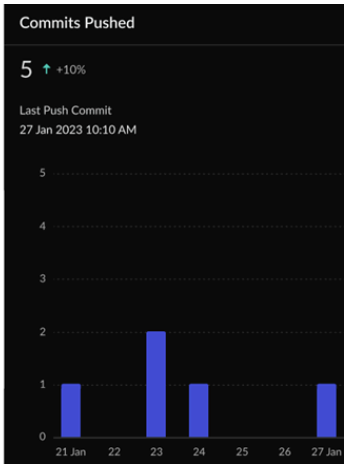
トンネルトレンド

トンネル監視 を有効にすると、複数のトンネルを選択し、それらの平均 ラウンドトリップ時間を表示できます。トンネルのセットを指定しない場合は、デフォルトでは、観測された RTT が最も高い 10 個のトンネルの RTT の中央値が計算されます。

集約されたトンネル接続には、 選択した時間範囲に接続されたトンネルの合計数が表示されます。いずれかのグラフにマウスを合わせると、特定の時間における接続数が表示されます。

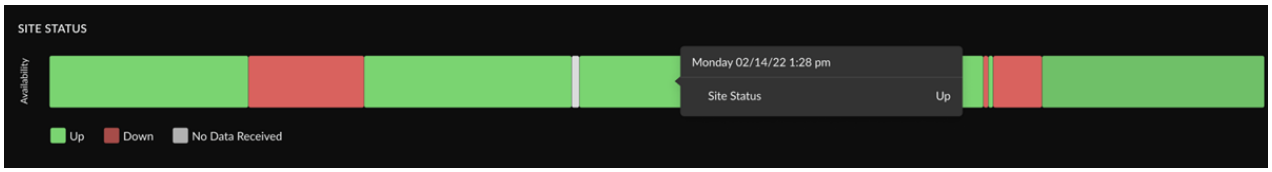
[Commits Pushed (プッシュされたコミット)] には、選択した 時間範囲 内にプッシュされたコミットの数と、 最後のプッシュコミット が発生した日時が表示されます。





サイトの状態

サイト ステータス には、選択した期間のサイトの可用性が表示されます。緑は 、この期間中にサイトが稼働していたことを意味し、 赤はサイトが停止していたことを意味し、 灰色は 、表示されている期間中にデータが利用できなかったことを意味します。



データセンターの表示と監視

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

 ©2025 Palo Alto Networks, Inc.

サービスコネクション

サービス接続 (企業アクセス ノード (CAN) とも呼ばれる) を使用すると、モバイル ユーザーとリモート ネットワークのユーザーはプライベート アプリやリソースにアクセスでき、モバイル ユーザーとリモート ネットワークは相互に通信できるようになります。Palo Alto Networksでは、Prisma Accessデプロイメント時に必ずサービス接続を作成することを推奨しています。すべてのサービス接続により、本社またはデータセンターのリソースにアクセスでき、リモート ネットワークとモバイル ユーザーが相互に通信できるようになります。

受信するサービス接続の数は、Prisma Access ライセンスによって異なります。サービス接続とその構成方法の詳細については、[Prisma Access サービス接続] を参照してください。

Strata Cloud Manager で、**[Monitor(監視)] > [Data Centers (データセンター)] > [Service Connections (サービス接続)]** を選択して、サービス接続を可視化します。

ZTNA コネクタ

Zero Trust Network Access (ZTNA) コネクタを使用すると、Prisma Accessを組織のプライベート アプリに接続できます。ZTNA コネクタは、自動化されたセキュア トンネルを使用して、モバイル ユーザーとブランチ ロケーションのユーザーにプライベート アプリへのアクセスを提供します。ZTNA コネクタはトンネルを自動的に設定します。プライベート アプリが配置されているデータ センターや本社、パブリック クラウドの場所、パートナー ネットワークへの IPSec トンネルやルーティングを手動で設定する必要はありません。

Strata Cloud Manager で、**[Monitor(監視)] > [Data Centers (データセンター)] > [ZTNA Connectors (ZTNAコネクタ)]** を選択して、ZTNAコネクタを可視化します。

サービス接続の表示と監視

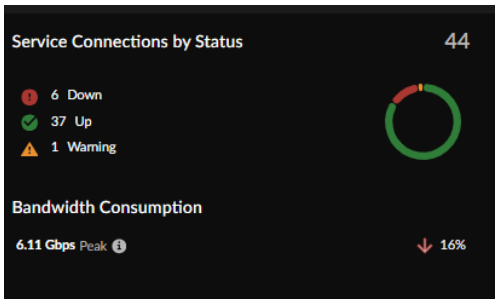
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

集約されたサービス接続データと個々のサービス接続に関する情報を表示します。サービスコネクションにより、モバイルユーザーとリモートネットワークの両方が可能になります。サービスコネクションは、企業リソースへのアクセスを提供するだけでなく、モバイルユーザーが支店ロケーションに到達できるようにします。Strata Cloud Manager でサービス接続を表示して、サービス接続のステータス、帯域幅の消費傾向、トンネルのデータと傾向、および全体的なサービス接続の健全性に関する情報を確認できます。**[Monitor (監視)] > [Data Centers (データセンター)] > [Service Connections (サービス接続)]**を選択して開始します。

ステータス別のサービス接続

すべてのサービス接続の正常性状態を表示できます。色分けされたグラフには、稼働中、停止中、または注意が必要なサービス接続の数の分布が表示されます。過去 30 日間にサービス接続で消費された帯域幅の概要を表示できます。

©2025 Palo Alto Networks, Inc.

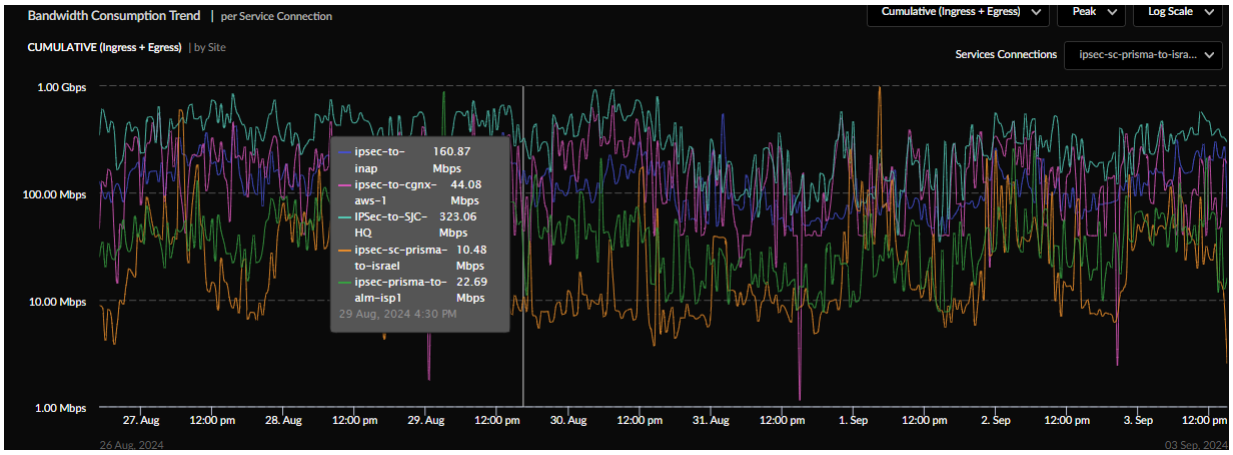


帯域幅消費量 は、サイトごとの帯域幅割り当てモデルにおいて、すべてのサイトにわたってサイトによって消費される最高のピーク帯域幅を示します。ピーク値は、選択した時間フィルターの期間にわたって計算されます。

帯域消費量の推移

サービス接続ごとの帯域幅消費傾向を表示します。この傾向には、各サービス接続による帯域幅の消費量と、平均およびピークの使用率が表示されます。

- デフォルトのビューには 累積 (入力 + 出力) 帯域幅消費量が表示されます。その他のオプションは 入力、出力、または 出力 vs出力。
- 選択した期間の ピーク、 中央値、または 平均の帯域幅消費傾向を表示します。デフォルト設定は ピーク 帯域幅消費です。
- ログスケール または 線形スケール。
- 1 ～ 10 個の サービス接続 を選択すると、選択した時間範囲内のグラフにトレンド ラインが表示されます。グラフの上にマウスを置くと、選択した各サービス接続に関する情報が表示されます。



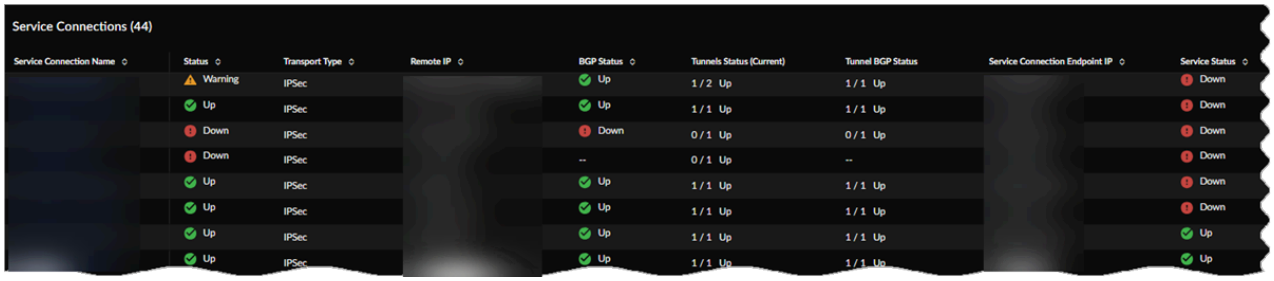
サービス接続テーブル

サービス接続 テーブルには、ステータス、リモートIPアドレス、BGPステータス、現在のトンネル ステータスなどのサービス接続に関するデータが表示されます。サービス接続の詳細については、サービス接続名 を選択してください。

- サービス接続名- サービス接続の一意の名前。
- ステータス–稼働中、停止中、警告、または不明。
- 転送タイプ- IPSec。

 ©2025 Palo Alto Networks, Inc.

- リモート **IP**- リモートIPアドレス。
- **BGP**ステータス- サイトのBGPステータスが 稼働中、停止中、または 不明のいずれかを示します。
- トンネルのステータス **(**現在**)**- サイトのトンネルの数と、そのうち稼働中のトンネルの数。
- トンネル **BGP** ステータス- 各トンネルのBGPステータス。
- サービス接続エンドポイント **IP**- サービス接続のエンドポイント IP アドレス。
- サービス ステータス- このフィールドは、サイトが接続されているインスタンスまたはファイアウォールのステータスを示します。ステータスは 稼働中、停止中、または 不明になります。
- **Prisma Access**の場所- サービス接続のPrisma Accessのロケーションです。
- 平均帯域幅消費量- 平均帯域幅消費量（Kbps）。
- ピーク帯域幅消費量- ピーク帯域幅消費量（Kbps）。

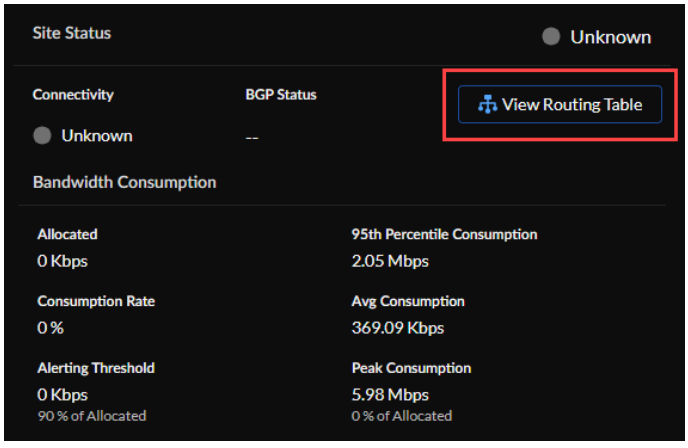


サービスコネクションの詳細を表示

任意の サービス接続名 を選択して、その詳細を表示します。過去 30 日間の サービス接続ステータスと 消費帯域幅を 表示します。帯域幅消費傾向 グラフには、選択した期間における各サービス接続による帯域幅消費が表示されます。

サイトの状態

任意の サービス接続名 を選択してその サイト ステータスを表示します。ここで、接続性と**BGP** ステータス ([稼働中]、[停止中]、[非アクティブ]、または[利用不可]) を確認できます。選択した時間間隔の帯域幅の ピーク消費量 を表示します。



ルートテーブルの可視性

 ©2025 Palo Alto Networks, Inc.

到達可能性の課題に対処できるように、各サービス接続のルート テーブルを可視化します。宛先 IP アドレスのルート テーブル検索を実行して、目的の宛先に到達するために使用できるルートがあるかどうかを判断できます。この情報を使用すると、Prisma Accessインフラストラクチャからガイダンスを受け取り、その他の潜在的な障害の原因を調査できます。この知識があれば、到達可能性に影響する問題の解決に集中することができます。

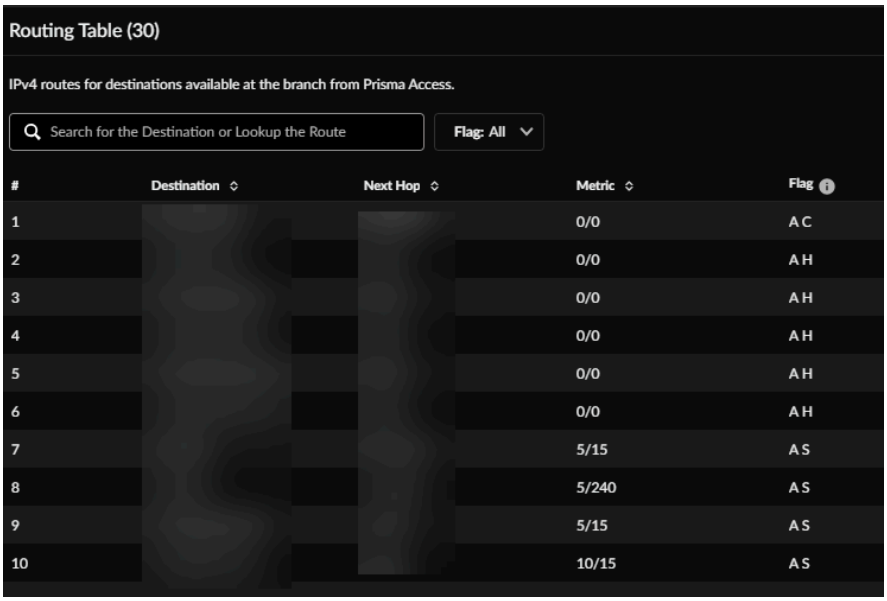
[ルーティング テーブルの表示] を選択すると、このブランチの ルーティング テーブルが表示されます。このテーブルには、Prisma Access からブランチで利用可能な宛先の IP ルートが含まれています。

- 検索バーを使用して目的地を選択したり、ルートを検索したりします。
- ドロップダウンを使用して、 フラグでフィルタリングします。

ルーティング テーブルには次の内容が表示されます。

- **#**– ルート番号
- 宛先– 到達可能なネットワークの IP アドレスとサブネット。
- ネクスト ホップ- 宛先ネットワークへの次のホップにあるゲートウェイの IP アドレス。ネクスト ホップが 0.0.0.0 の場合は、デフォルト ルートを表します。
- メトリック- ルーティング プロトコルによって決定されたルートのメトリック。
- フラグ- このルートに関する情報は次のとおりです。
- - **AB**–アクティブで、BGP から学習されました。
  - **AC**–アクティブで接続されています。宛先 - ネットワーク。
  - **AH**–アクティブで接続されています。宛先 - ホストのみ。
  - **AR**–RIP からアクティブに学習。
  - **O1** – OSPF 外部タイプ -1
  - **O2** – OSPF 外部タイプ -2
  - **Oi** – OSPF エリア内
  - **Oo**–OSPF エリア間。
  - **S**–非アクティブで静的。
  - **AS**–アクティブかつ静的。

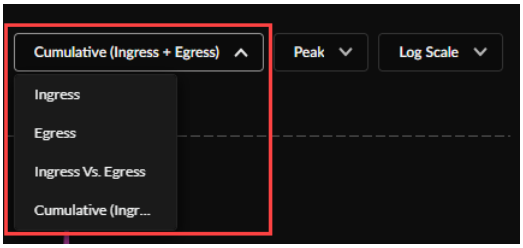
 ©2025 Palo Alto Networks, Inc.



帯域消費量の推移

帯域幅消費傾向には、 デフォルトで 累積 **(**入力 **+** 出力**)** 情報が表示されます。

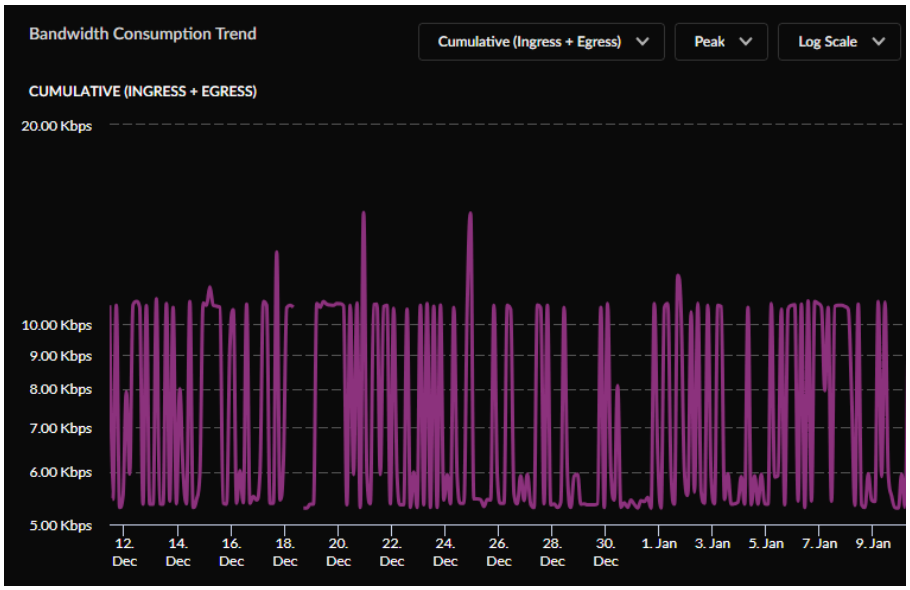
- ドロップダウンを使用して、 入力、 出力、 入力 **vs**出力、または 累積（入力 **+** 出力）です。



- ブランチ サイトの帯域幅消費傾向チャートのメトリックは ピーク (既定)、 平均、または 中央値別で表示されます。

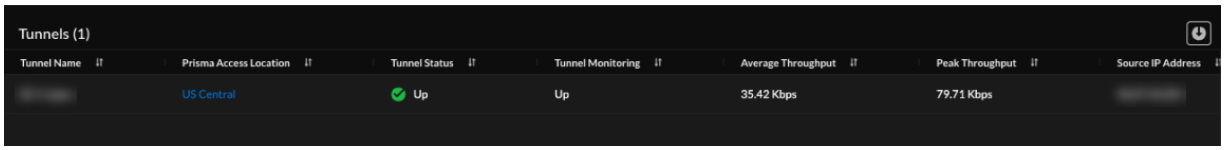


 ©2025 Palo Alto Networks, Inc.



トンネル

このサービス接続に トンネルが いくつあるかを確認し、各トンネルの詳細を表示します。トンネル データをダウンロードするには、[ダウンロード] アイコンを選択します。

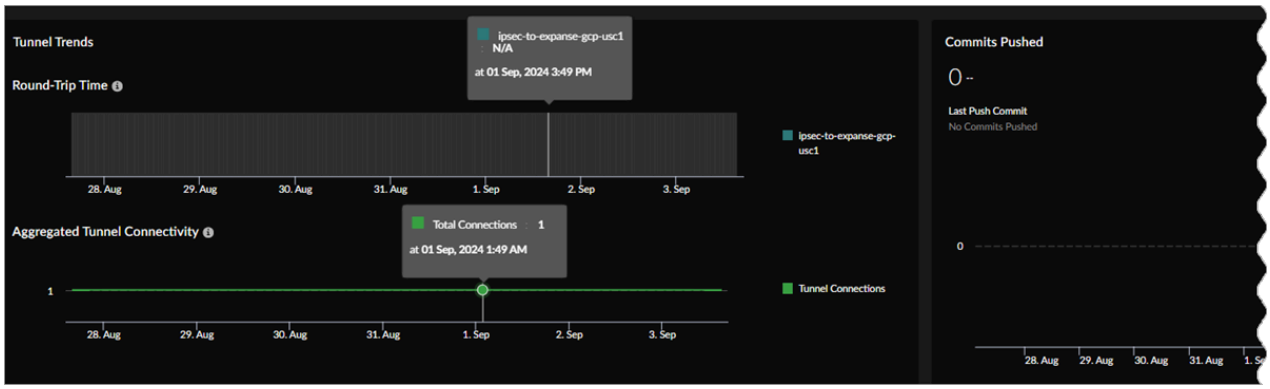


トンネルトレンド

複数のトンネルを選択して、その平均 ラウンドトリップ時間を表示できます。トンネルのセットを指定しない場合は、観測された RTT が最も高い 10 個のトンネルの RTT の中央値が計算されます。

集約されたトンネル接続には、 選択した時間範囲に接続されたトンネルの合計数が表示されます。いずれかのグラフにマウスを合わせると、特定の時間における接続数が表示されます。

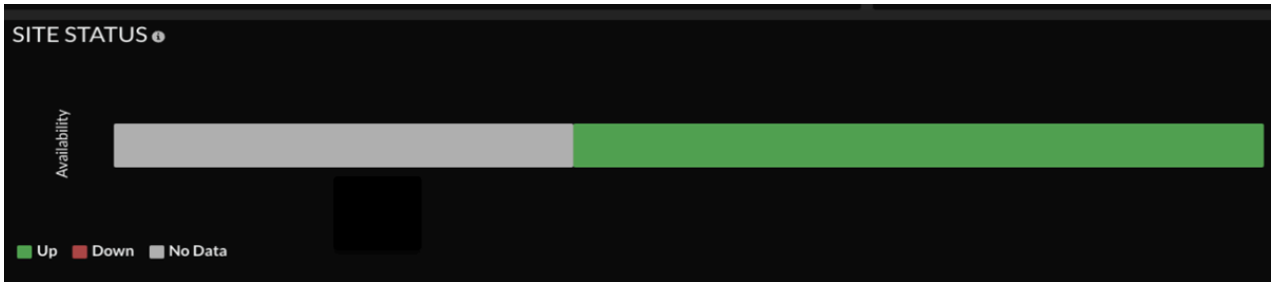
[Commits Pushed (プッシュされたコミット)] には、選択した 時間範囲 内にプッシュされたコミットの数と、 最後のプッシュコミット が発生した日時が表示されます。



 ©2025 Palo Alto Networks, Inc.

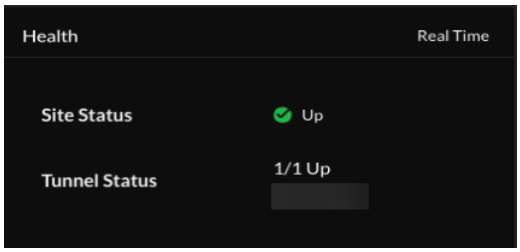
サイトの状態

サイト ステータス には、選択した期間のサイトの可用性が表示されます。緑は、この期間中にサイトが稼働していたことを意味し、赤はサイトが停止していたことを意味し、灰色は、表示されている期間中にデータが利用できなかったことを意味します。



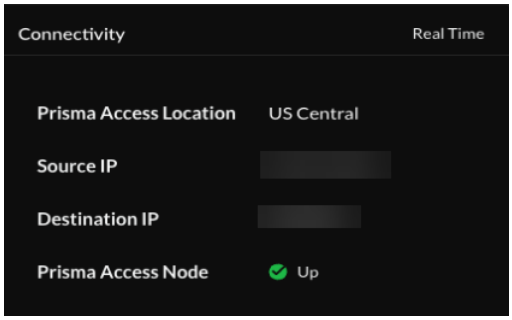
ヘルス

Health (健全性) には サイトのステータスが表示され、サイト内の各トンネルの名前とステータスが表示されます。



接続

接続性は、サイトが接続されているPrisma Accessロケーション、その送信元と宛先のIP、およびPrisma Accessノードのステータスを表示します。



使用量

使用量には、 帯域幅消費量の詳細が表示されます。



Colo-Connectの表示と監視

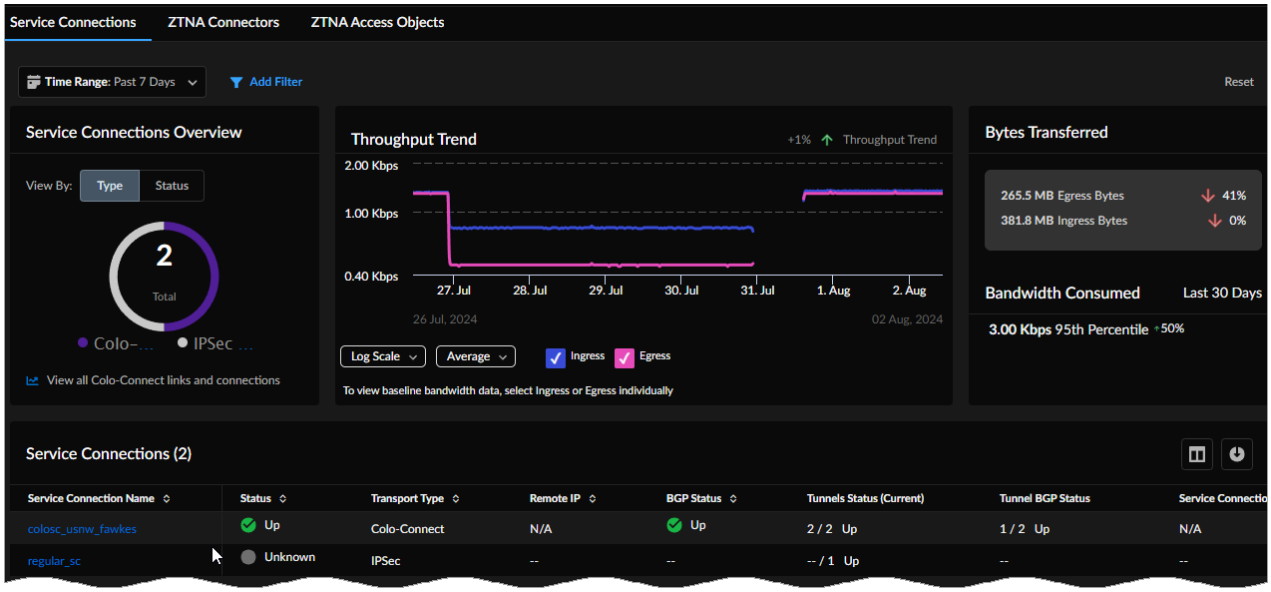
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	Prisma Accessライセンス

©2025 Palo Alto Networks, Inc.

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	

Prisma AccessColo-Connectは、クラウド ネイティブのGCPインターコネクト技術を活用して、プライベート アプリケーションへの高帯域幅サービス接続を提供します。Colo-Connectは既存のIPSecトンネルベースのサービス接続と共存するため、高帯域幅のスループットを必要としない小規模なデータセンターへのプライベートアプリケーションアクセスを提供する必要がある場合は、それらのデータセンターへのサービス接続も使用できます。Colo-Connectリンクの数とステータス、スループットの傾向、個々のトンネル、接続、リンクの詳細などのメトリックを表示して、Colo-Connec のデプロイメントを可視化します。Colo-Connectサービス接続に関するデータを表示することで、デプロイメントの健全性と接続性の全体像を把握できます。

クラウド相互接続を介したハイブリッド クラウドおよびオンプレミス データ センターへのプライベート接続を表示および監視するには、**[Monitor (監視)]** > **[Data Centers (データセンター)]** > **[Service Connections (サービス接続)]**にアクセスしてください。



サービス接続の概要

サービス接続の概要には、トランスポートタイプ別のサービス接続の数が表示されます。

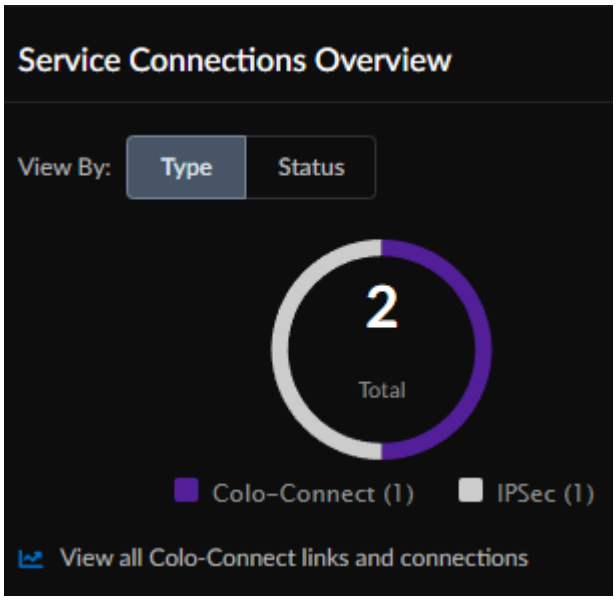
接続されたトランスポートの集計を タイプ 別または可用性 ステータス別に表示できます。

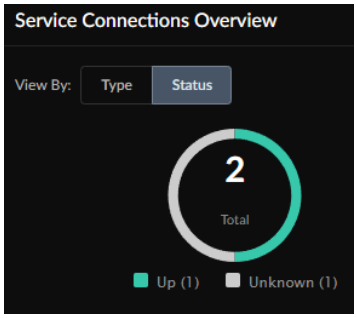
- **IPSec**
- **Colo-Connect**

トンネルトランスポートの種類をステータス別に表示できます。**Up (稼働中)**、**Down (停止中)**、**Degraded (劣化)**、または **Unknown (不明)**。

Colo-Connect の詳細ページを表示するには、[すべての **Colo-Connect** リンクと接続を表示] を選択します。

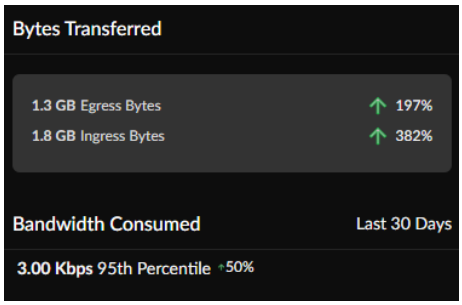
©2025 Palo Alto Networks, Inc.





サービス接続の概要転送バイト数と消費帯域幅

転送されたバイト数には、 消費された入力バイト数と出力バイト数の合計と、以前に選択した時間範囲からの消費量の差が表示されます。消費された帯域幅には、 過去 30 日間に消費された帯域幅の 95 パーセンタイルが表示されます。



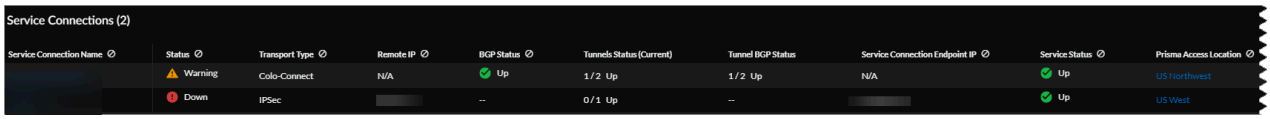
サービスコネクション

サービス接続 テーブルには、指定されたサービス接続ごとに次の詳細が表示されます。

- サービス接続名- Colo-Connect または IPSec サービス接続の名前。サービス接続名 を選択して、その詳細ページに移動します。
- ステータス- 稼働中、ダウン、劣化、不明。
- トランスポート タイプ- Colo-Connect または IPSec。
- リモート IP– 宛先 IP。

©2025 Palo Alto Networks, Inc.

- **BGP** ステータス- 一部の BGP トンネルが稼働中で、一部がダウンしている場合は、稼働中、ダウン中、または警告。
- トンネル ステータス **(**現在**)**– 現在のトンネル ステータス。
- トンネル **BGP** ステータス- BGP ステータス (アップ、ダウン、警告) によるトンネルの数。
- サービス接続エンドポイント**IP**– Prisma Accessノード IP アドレス。
- サービス ステータス- サービス ステータスは、アクティブなサービス接続またはデータ センター クラスター (複数のクラスター) のステータス (稼働中、停止中、警告) によって決まります。
- **Prisma** アクセス ロケーション–**Prisma** アクセス ロケーションを選択します。
- 平均帯域幅消費量- 選択した時間範囲内でのサイトの平均帯域幅消費量。
- ピーク帯域幅消費量- 選択した時間範囲内でのサイトのピーク帯域幅消費量。



サービスコネクションの詳細を表示

メイン ページの [サービス接続] テーブルから、トランスポート タイプ が Colo-Connect であるサービス接続を選択し、その詳細ページに移動します。



サービス接続ステータス、コネクト、同時セッション

- サービス接続の アクセス ロケーション と **GRE** トンネル のステータス (アップ、ダウン、または警告) を確認します。
- **Colo-Connect** リンクと接続の合計数を表示します。
- 同時セッションには 、現在のセッション数と過去 30 日間の合計セッション数が表示されます。

スループットの傾向

スループット トレンドには、選択した時間範囲内でこのサービス接続によって消費された入力および出力スループット トラフィックが表示されます。

 ©2025 Palo Alto Networks, Inc.

転送バイト数と消費帯域幅

転送バイト数 には、このサービス接続で消費された入力バイト数と出力バイト数の合計と、以前に選択した時間範囲からの消費量の差が表示されます。消費された帯域幅 には、過去 30 日間にサービス接続が消費した帯域幅の 95 パーセンタイルが表示されます。

GRE トンネル

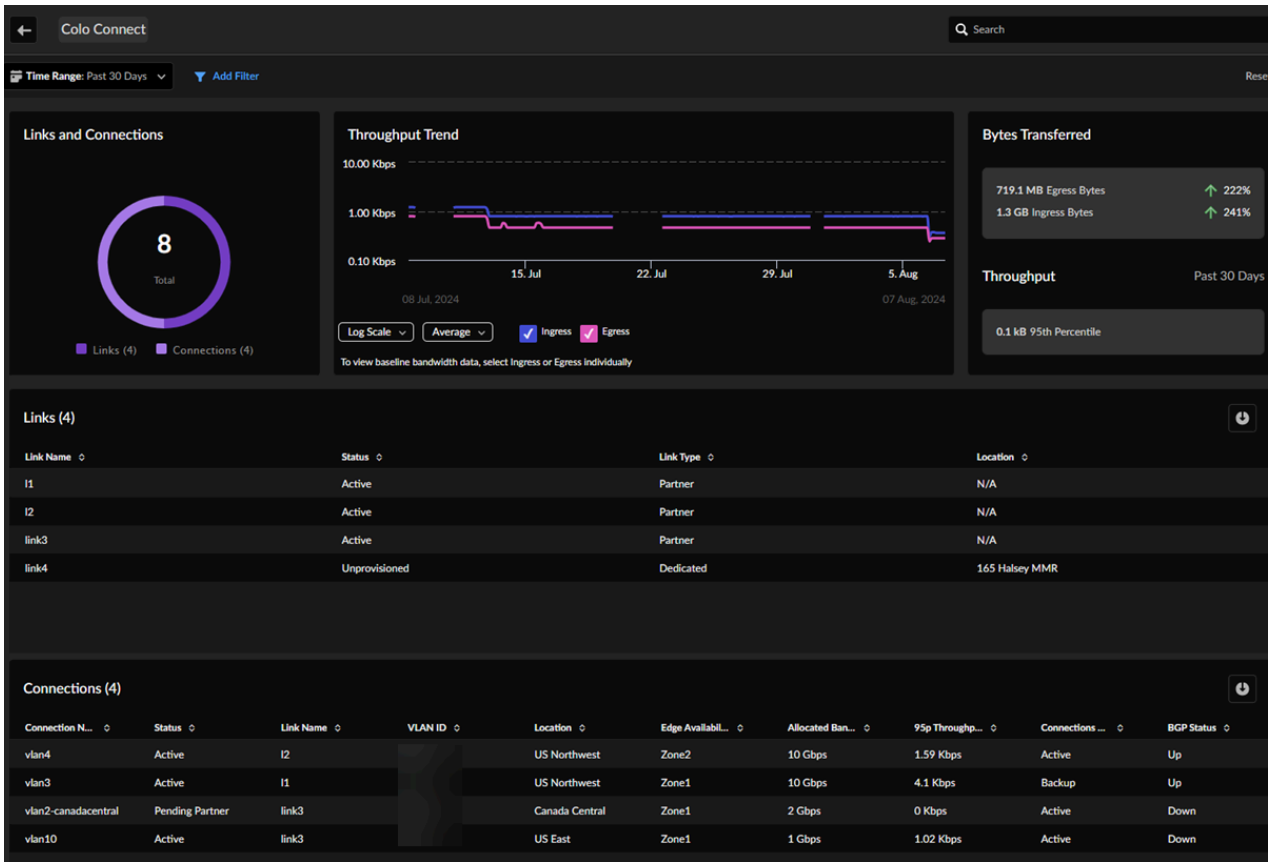
このサービス接続のトンネルの詳細を表示します。

- トンネル名- 一意のトンネル名。
- トンネルのステータス- アップ、ダウン、不明。
- 接続名- 接続の一意の名前。
- トンネル状態- 接続ステータス (アクティブまたはバックアップ)。
- リモート **IP**– 宛先 IP アドレス。
- ソース **IP**- ローカル デバイスの IP アドレス。
- **95%** スループット- 過去 30 日間に消費された帯域幅の 95 パーセンタイル。
- ピーク スループット- 選択した時間範囲内のピーク スループット。
- **BGP** ステータス- 稼働中、停止中、劣化、不明。
- **BGP** ローカル **IP**–BGP ローカル IP。
- 切断– このトンネルで切断された回数。
- 切断期間- 切断が続いた時間。
- 入力バイト数- 選択した時間範囲内で消費された入力バイト数。
- 出力バイト- 選択した時間範囲内で消費された出力バイト数。
- 入力パケット数- 入力パケット数。
- 出力パケット数- 出力パケット数。

*Colo-Connect*の詳細

メインの [サービス接続] ページで、[サービス接続の概要] ウィジェットから [すべての **Colo-Connect** リンクと接続を表示] を選択して、**Colo-Connect** の詳細ページを開きます。このページのウィジェットには、現在の詳細が表示されます (現在の詳細とは、過去 20 分間の詳細情報を指します)。

©2025 Palo Alto Networks, Inc.



リンクと接続

円グラフには、現在の Colo-Connect リンクと接続の合計数が表示されます。

リンク

表には、現在の Colo-Connect リンクの詳細が表示されます。

- リンク名- 一意の Colo-Connect リンク名。
- ステータス- アクティブまたはメンテナンス。
- リンク タイプ- パートナーまたは専用。
- ロケーション- Prisma Accessのロケーション。

接続

現在の Colo-Connect リンクの詳細を表示します。接続の上にマウスを置くと、表示されるステータスに関する情報が表示されます。

- 接続名- 一意の Colo-Connect 接続名。
- ステータス- アクティブ、保留中パートナー、廃止。
- リンク名- 接続のリンク名。
- **VLAN ID**—接続の VLAN ID。
- ロケーション- Prisma Accessのロケーション。
- エッジ可用性ゾーン- Zone1 または Zone2。

©2025 Palo Alto Networks, Inc.

- 割り当てられた帯域幅- 1 Gbps、2 Gbps、5 Gbps、10 Gbps、または 20 Gbps。
- **95%** スループット- 消費された帯域幅の 95 パーセンタイル。
- 接続状態- アクティブまたはバックアップ。
- **BGP** ステータス- アップまたはダウン。

ZTNAコネクタの表示と監視

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス ❑ これはPrisma Access Insightsの機能です。

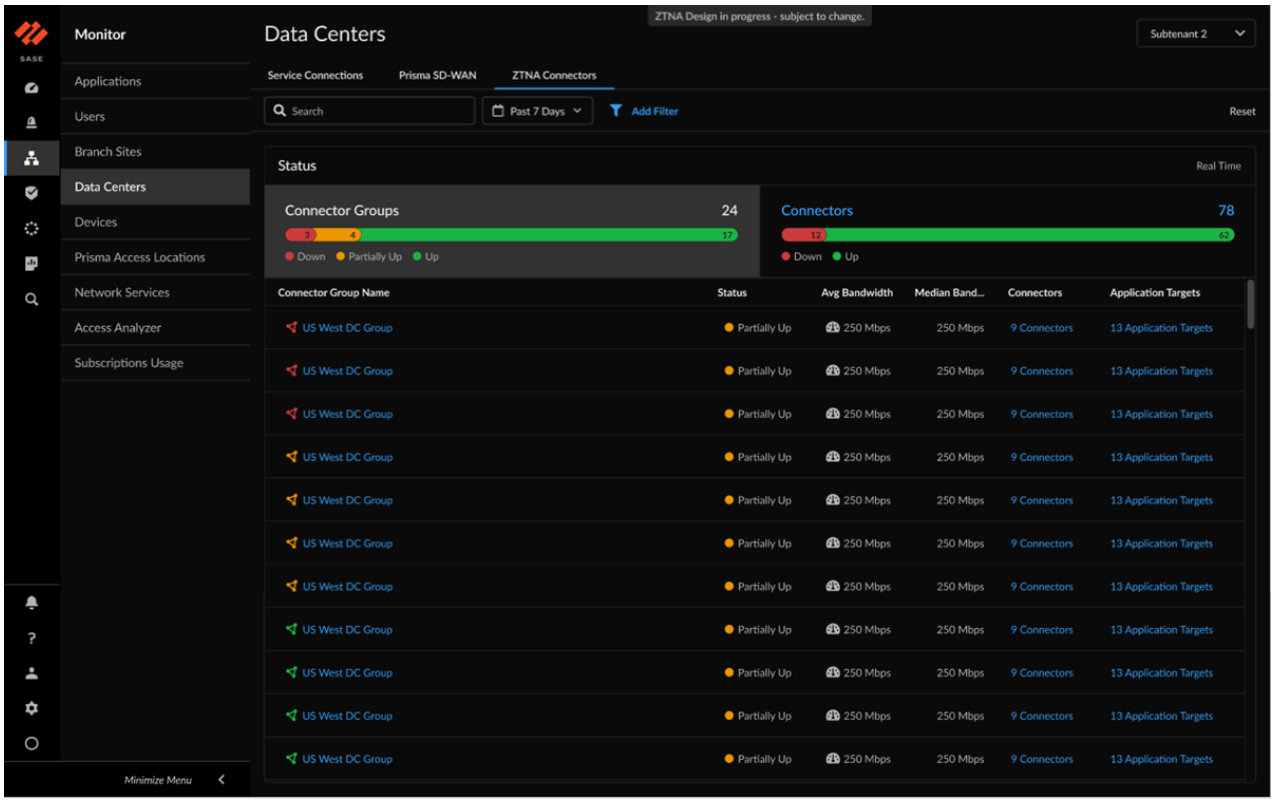
ゼロ トラスト ネットワーク アクセス (ZTNA) コネクタは、すべてのアプリケーションのプライベート アプリケーション アクセスを簡素化します。環境内のZTNAコネクタVMは、プライベート アプリケーションとPrisma Accessとの間に自動的にトンネルを形成します。設定されているすべてのZTNAコネクタの概要を表示します。これには、コネクタに関連付けられているアプリケーションターゲット、その平均帯域幅と中央値、およびステータス（アップ、部分アップ、またはダウン）が含まれます。モニター > データセンター > **ZTNA**コネクタ をStrata Cloud Managerで選択し、ZTNAコネクタとコネクタ グループのパフォーマンスを確認します。

ZTNA コネクタ グループのステータス

各グループ内のコネクタによって、コネクタ グループの ステータスが決まります。

- コネクタ グループ 内のすべての コネクタ が稼働している場合、 ステータス は 稼働中 (緑) になります。
- すべての コネクタ がダウンしている場合、ステータスは 停止中（赤）になります。
- 一部のコネクタが稼働中で、一部が停止している場合、 ステータスは部分的に稼働中 (オレンジ) になります。
- 無効なコネクタは灰色で表示されます。

©2025 Palo Alto Networks, Inc.



ZTNAコネクタのステータス

コネクタに関連付けられたアプリケーション ターゲットやステータスなど、構成されたすべてのコネクタの概要を表示します。

任意のコネクタ名を選択すると、各コネクタに関連付けられているコネクタ グループとアプリケーション ターゲットの詳細が表示されます。

ZTNAコネクタ アクセス オブジェクトの表示と監視

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

FQDN、IPサブネット、ワイルドカードによって追加されたアプリの数、各アクセス オブジェクトの接続ステータス、各アクセス オブジェクトに関連付けられている コネクタ グループ と コネクタ などのデータを表示することで、ZTNAコネクタ アクセス オブジェクトを通じて追加されたプライベート アプリを可視化します。この情報を表示することで、デプロイメントの健全性と接続性の全体像を把握できます。

データセンター 内のプライベート アプリは、コネクタ仮想マシン (VM) を介してPrisma Accessに接続します。これらのアクセス オブジェクト (FQDN、FQDNワイルドカード、またはIPサブネット) に基づいてアプリを追加できます。

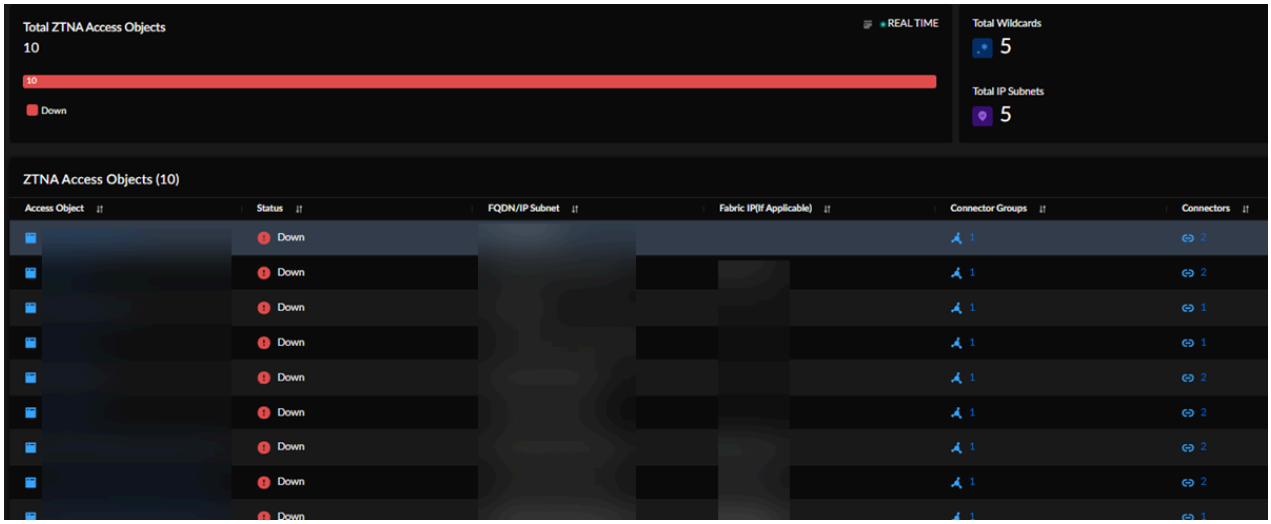
 ©2025 Palo Alto Networks, Inc.

- **FQDN**– Prisma Access は、ZTNA コネクタにオンボードするアプリケーションのFQDNを、アプリケーションIPアドレス ブロック内のIPアドレスに解決します。
- ワイルドカード- ワイルドカードベースのアプリの場合は、FQDN ベースのコネクタ グループを作成し、アプリ ターゲットに使用するワイルドカード (*.example.com など) を指定します。ユーザーがワイルドカードと一致するサイトにアクセスすると、モバイルユーザーとリモートネットワークユーザーがそれらのアプリに ZTNA Connector からアクセスできるように自動的にオンボーディングされます。
- **IP** サブネット- IP サブネット ベースのコネクタ グループを作成し、アプリ ターゲットに使用する IP サブネットを入力します。

Strata Cloud Managerで、**[Monitor (監視)] > [Data Centers (データセンター)] > [ZTNA Access Objects (ZTNAアクセスオブジェクト)]**に移動して、ZTNAコネクタ アクセス オブジェクトを可視化します。

すべてのアクセスオブジェクト

合計**ZTNA**アクセス オブジェクト を表示して、すべてのZTNAコネクタ アクセス オブジェクト (FQDN、ワイルドカード、IP サブネット) に関する情報をリアルタイムで表示します。**[ZTNA**アクセス オブジェクトの合計]と**[ZTNA**アクセス オブジェクト]テーブルの数字は一致している必要があります。これは、FQDN アプリ、サブネット アプリ、検出されたワイルドカード アプリの数を表します。



- 環境内の **ZTNA** アクセス オブジェクト の合計をステータス別にグラフで表示します。これは、アクセス オブジェクトの自動化されたセキュア トンネルが稼働中、部分的に稼働中、ダウン中、または無効であることを意味します。ステータスが停止中の場合、このアクセス オブジェクトに関連付けられているコネクタはアプリケーションに到達できません。
  - 稼働中–すべてのトンネルが稼働しています。
  - 部分的に稼働中- 一部のトンネルは稼働中で、その他はダウンまたは無効になっています。
  - 停止中- すべてのトンネルがダウンしています。

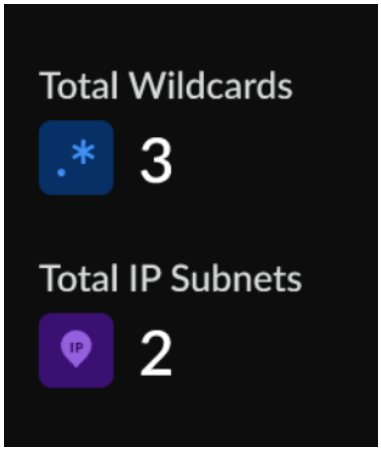
 ©2025 Palo Alto Networks, Inc.

- 無効- すべてのトンネルが無効になります。

[ZTNA アクセス オブジェクトの合計**]**ウィジェットでステータスの色の四角形を選択すると、**ZTNA** アクセス オブジェクト テーブルでアクセス オブジェクトをステータス別に並べ替えることができます。

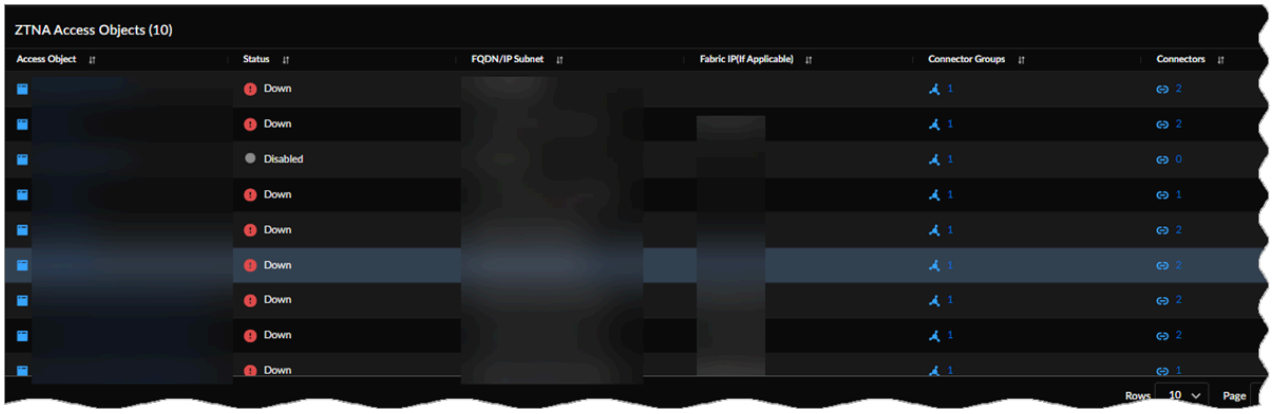


- ワイルドカードの合計と **IP** サブネットの合計には、 オンボードしたIPサブネットとワイルドカード ルールの数の概要が表示されます。これは、作成したワイルドカード ルールの数であり、これらのルールを作成した結果として検出されたアプリの数とは異なります。



 ©2025 Palo Alto Networks, Inc.

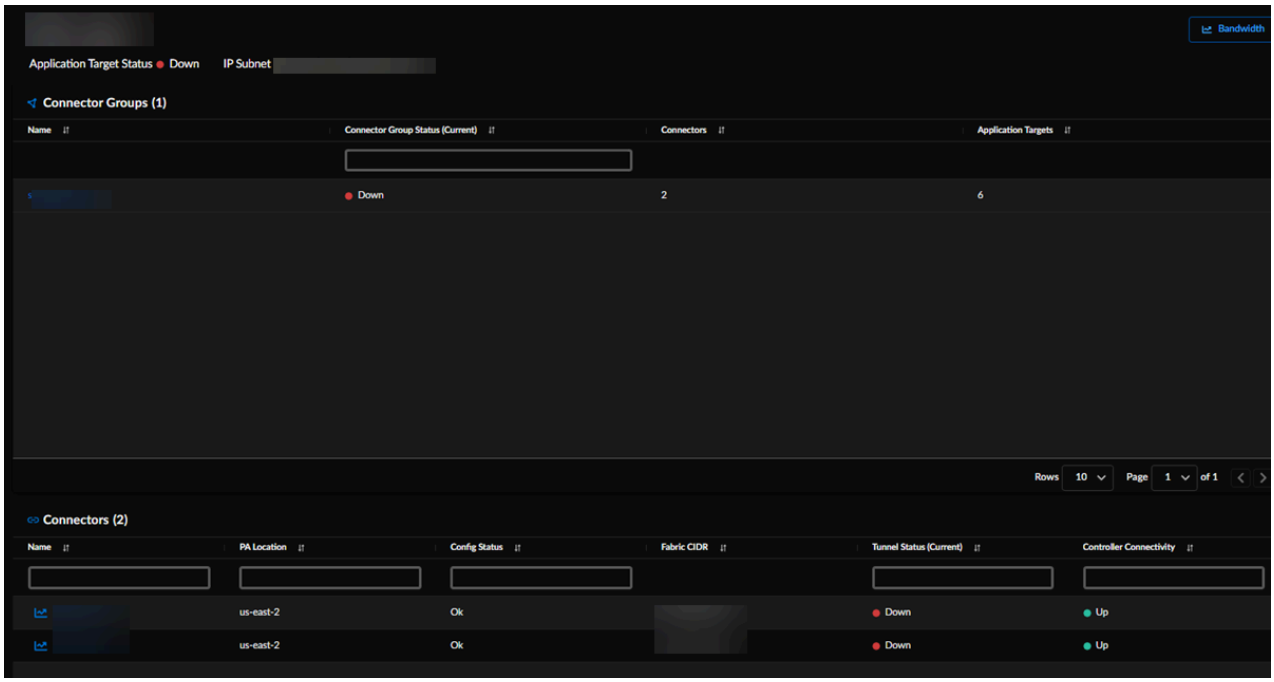
- **ZTNA** アクセス オブジェクトは、すべてのアクセス オブジェクトに関する情報を提供します。
  - アクセス オブジェクト - 特定のアクセス オブジェクトを選択して、その詳細を表示します。
  - ステータス - アクセス オブジェクトの自動セキュア トンネルは、稼働中、部分的に稼働中、ダウン中、または無効です。
  - **FQDN/IP** サブネット - このアクセス オブジェクトを追加するために使用されるFQDNまたはIPサブネット。
  - ファブリック **IP (**該当する場合**)** - このアクセス オブジェクトに関連付けられているファブリックIP。
  - コネクタ グループ - コネクタ グループは、コネクタとアプリケーションの論理的なグループです。アクセス オブジェクトに関連付けられているコネクタ グループを表示します。
  - コネクタ – コネクタは、Prisma Accessに接続するデータセンターで実行されているVMを表します。アクセス オブジェクトに関連付けられているコネクタを表示します。



任意のアクセス オブジェクトを選択して、その詳細を表示します。

- コネクタ グループ - このアクセス オブジェクトに関連付けられているコネクタ グループの数を確認します。コネクタ グループを選択して、そのサービス接続に関する情報を表示します。
- コネクタ グループのステータス **(**現在**)** - 稼働中、部分的に稼働中、ダウン、または無効。
- コネクタ - このコネクタ グループ内のコネクタの数。
- アプリケーション ターゲット - このコネクタ グループ内のアプリケーション ターゲットの数。
- 帯域幅 - このアクセス オブジェクトの帯域幅情報を表示するには、[帯域幅] ボタンを選択します。

©2025 Palo Alto Networks, Inc.



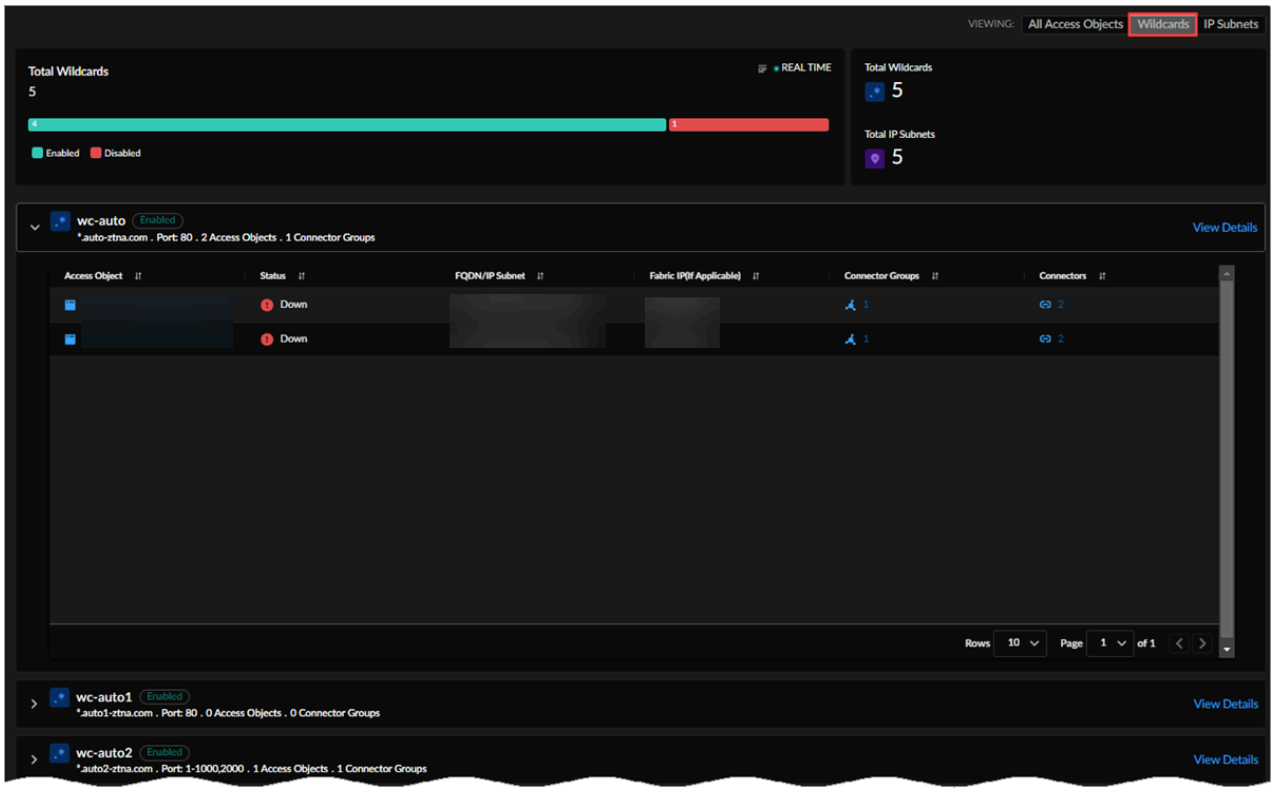
アクセス オブジェクトのコネクタのいずれかを選択して、その詳細を表示します。

- **PA (Prisma Access)** ロケーション- 各コネクタに関連付けられたPrisma Accessロケーション。
- 構成ステータス - コネクタの構成ステータスはOKまたはエラーです。ステータスがエラーの場合、ZTNAコネクタのオンボーディングは完了していません。
- ファブリック**CIDR** - このコネクタに関連付けられているファブリックCIDR。
- トンネル ステータス **(**現在**)** - このコネクタの自動セキュリティ トンネル ステータス。
- コントローラの接続性 - アップ、部分的に稼働中、停止中、または無効。

ワイルドカード

ワイルドカード アクセス オブジェクトを表示するには、ワイルドカードを選択します。ステータス別の ワイルドカードの合計数、ワイルドカードの合計数、**IP**サブネットの合計数を表示します。

©2025 Palo Alto Networks, Inc.



ワイルドカードの横にある矢印を選択するか、[詳細の表示] を選択して、このワイルドカードを構成するアクセス オブジェクトに関する情報を表示します。

- アクセス オブジェクト - 特定のアクセス オブジェクトを選択して、その詳細を表示します。
- ステータス - アクセス オブジェクトの自動セキュア トンネルは、稼働中、部分的に稼働中、ダウン中、または無効です。
- **FQDN/IP** サブネット - このアクセス オブジェクトを追加するために使用されるFQDNまたはIPサブネット。
- ファブリック **IP (**該当する場合**)** - このアクセス オブジェクトに関連付けられているファブリックIP。
- コネクタ グループ - コネクタ グループは、コネクタとアプリケーションの論理的なグループです。アクセス オブジェクトに関連付けられているコネクタ グループを表示します。
- コネクタ – コネクタは、Prisma Accessに接続するデータセンターで実行されているVMを表します。アクセス オブジェクトに関連付けられているコネクタを表示します。



任意のアクセス オブジェクトを選択して、その詳細を表示します。

- コネクタ グループ - このアクセス オブジェクトに関連付けられているコネクタ グループの数を確認します。コネクタ グループを選択して、そのサービス接続に関する情報を表示します。

 ©2025 Palo Alto Networks, Inc.

- コネクタ グループのステータス (現在) - 稼働中、部分的に稼働中、ダウン、または無効。
- コネクタ - このコネクタ グループ内のコネクタの数。
- アプリケーション ターゲット - このコネクタ グループ内のアプリケーション ターゲットの数。
- 帯域幅 - このアクセス オブジェクトの帯域幅情報を表示するには、[帯域幅] ボタンを選択します。

ワイルドカード内のアクセス オブジェクトに関連付けられている一意のコネクタ グループまたはコネクタを表示するには、コネクタ グループ または コネクタを 選択します。

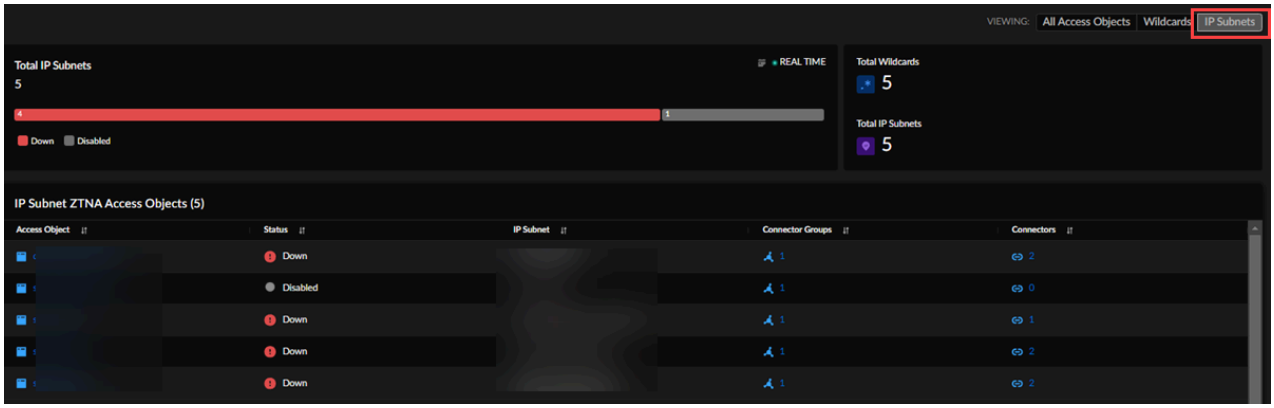
IP サブネット

IPサブネットを 選択すると、IPサブネット アクセス オブジェクトの合計が表示されます。1つのIPサブネット アクセス オブジェクトは、複数の異なるアプリのグループで構成されます。

環境内の**IP**サブネットの合計をステータス (稼働中、部分的に稼働中、停止中、無効) 別に表示します。

IPサブネット**ZTNA**アクセス オブジェクトは、すべてのアクセス オブジェクトに関する情報を提供します。

- - アクセス オブジェクト - 特定のアクセス オブジェクトを選択して、その詳細を表示します。
  - ステータス - 稼働中、部分的に稼働中、ダウン中、または無効。
  - **IP**サブネット- このアクセス オブジェクトを追加するために使用される**IP**サブネット。
  - コネクタ グループ - コネクタ グループは、コネクタとアプリケーションの論理的なグループです。アクセス オブジェクトに関連付けられているコネクタ グループを表示します。
  - コネクタ - コネクタは、データセンターで実行され、Prisma Accessに接続しているVMを表します。アクセス オブジェクトに関連付けられているコネクタを表示します。



任意のアクセス オブジェクトを選択して、その詳細を表示します。

- コネクタ グループ - このアクセス オブジェクトに関連付けられているコネクタ グループの数を確認します。コネクタ グループを選択して、そのサービス接続に関する情報を表示します。
- コネクタ グループのステータス (現在) - 稼働中、部分的に稼働中、ダウン、または無効。

 ©2025 Palo Alto Networks, Inc.

- コネクタ - このコネクタ グループ内のコネクタの数。
- アプリケーション ターゲット - このコネクタ グループ内のアプリケーション ターゲットの数。
- 帯域幅 - このアクセス オブジェクトの帯域幅情報を表示するには、[帯域幅] ボタンを選択します。

IPサブネット内のアクセス オブジェクトに関連付けられている一意のコネクタ グループまたはコネクタを表示するには、コネクタ グループまたはコネクタを選択します。

ネットワーク サービスの表示と監視

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス ❑ これはPrisma Access Insightsの機能です。

アプリケーションへのアクセスに関するユーザー エクスペリエンスに影響する一般的なネットワーク サービスのパフォーマンスを表示します。ネットワークサービスには、モバイルユーザーが Prisma Access に接続できることを示す GlobalProtect 認証の成功数と失敗数のレポートや、指定した時間範囲内にサーバに転送された DNS プロキシ要求と応答の表示が含まれる。

グローバルプロテクト認証チェック

Strata Cloud Managerの**[Monitor (監視)]** > **[Network Services (ネットワークサービス)]** > **[GlobalProtect認証]**にアクセスし、環境に影響するGlobalProtect認証の成功と失敗を確認する。

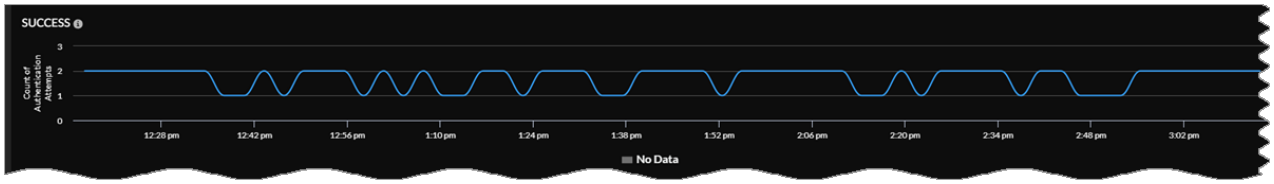
- 時間範囲 フィルターを設定して、その時間範囲のネットワーク サービス データを確認します。
- **Prisma Access**ロケーションを指定すると、選択した時間範囲内の認証成功、合計失敗、およびタイムアウト失敗が表示されます。

このデータは、特定の時点で GlobalProtectポータルへの認証を試みているモバイル ユーザーの数を表します。GlobalProtectポータルは、検証のためにモバイル ユーザーの資格情報をオンプレミスのActive Directory (アクティブディレクトリ - AD)サーバーに送信し、認証が成功または失敗します。認証失敗が多数発生した場合は、特定の場所の問題やオンプレミスの認証サーバーがダウンしていることを示すネットワーク イベントと失敗を関連付けることができます。これらのグラフのデータは、ネットワークの問題を解決するネットワーク管理者にトラブルシューティングの洞察を提供します。GlobalProtectポータルおよびゲートウェイでモバイル ユーザーの認証成功または失敗の傾向の数を表示し、このデータを使用して時間の経過に伴う認証成功またはフェイルオーバーのパターンを把握し、Prisma Accessデプロイメントで正常または異常となる可能性のある数の範囲を確立できます。たとえば、異常なカウントは、GlobalProtectポータルの可用性の問題や認証サーバーの低速化により、既存のユーザーが Prisma Access に接続できないことを示している可能性があります。または、異常なカウントは、多数のユーザーが一度に顧客のネットワークにオンボードされたことを示している可能性があります。

©2025 Palo Alto Networks, Inc.

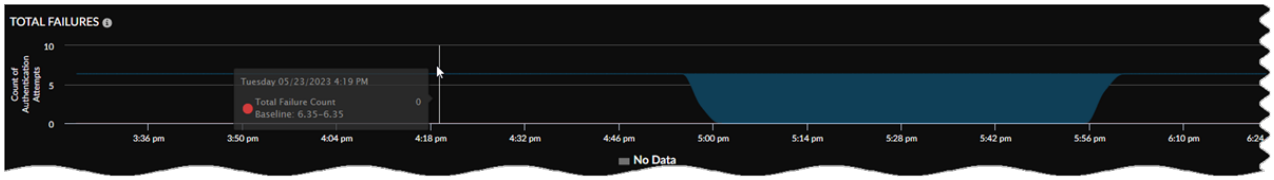
GlobalProtect認証成功

さまざまなロケーションでのGlobalProtectの認証成功数の詳細を表示します。グラフの任意のポイントにカーソルを合わせると、特定の時間に表示されたさまざまなPrisma Accessロケーション サイトで認証に成功したユーザー数の詳細が表示されます。



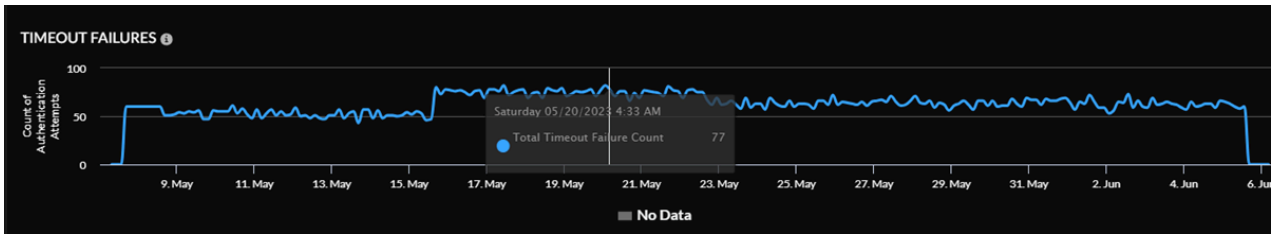
GlobalProtect 認証失敗総数

さまざまなロケーションの GlobalProtect の認証失敗数に関する詳細を表示します。グラフの任意のポイントにカーソルを合わせると、米国東部やカナダ東部など、表示されているPrisma Accessロケーション サイトごとに、特定の時刻に認証に失敗したユーザー数の詳細が表示されます。



GlobalProtect認証タイムアウト失敗

さまざまなロケーションの GlobalProtect の認証失敗数に関する詳細を表示します。グラフの任意のポイントにカーソルを合わせると、米国東部やカナダ東部など、表示されているPrisma Accessロケーション サイトごとに、特定の時刻に認証に失敗したユーザー数の詳細が表示されます。



DNS

Strata Cloud Manager の**[Monitor (監視)]** > **[Network Services (ネットワークサービス)]** > **[GlobalProtect認証]**にアクセスし、定した時間範囲内にサーバーに転送されたDNSプロキシ要求と応答を表示します。

使用できるフィルターは次のとおりです。

- 期間
- **DNS**プロキシ名

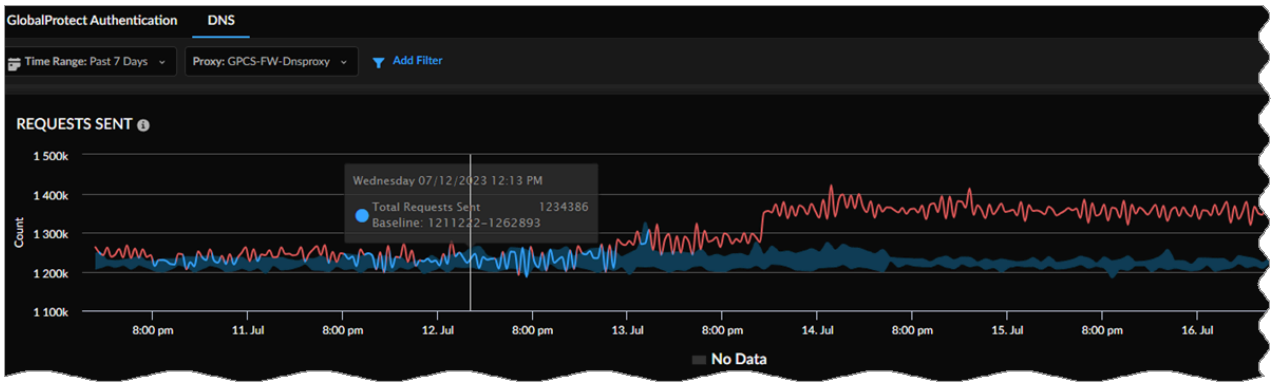
DNSプロキシフィルタの値は過去30日間に関連し、ロード時に自動的に選択されます（つまり、明示的なプロキシデータがない場合は、明示的なプロキシフィルタは存在しません）。グラ

 ©2025 Palo Alto Networks, Inc.

フの上にマウスを置くと、特定の時間に DNS プロキシ サーバーに送信された要求 と 受信した要求のすべての詳細が表示されます。

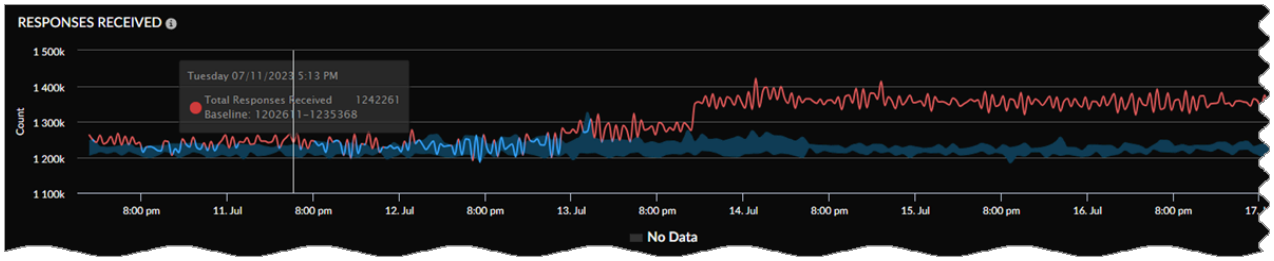
要求が送信されました

指定した時間範囲にサーバーに転送されたネットワーク要求とクエリを表示します。グラフ内の任意のポイントにカーソルを合わせると、その時点で DNS プロキシ サーバーに送信された要求に関する情報が表示されます。フィルタリングするプロキシ名を選択した場合は、そのプロキシのデータが表示されます。



受け取った応答

指定した期間内にテナント全体で受信した応答の合計を表示します。グラフ内の任意のポイントにカーソルを合わせると、その時点で受信した応答に関する情報が表示されます。フィルタリングするプロキシ名を選択した場合は、そのプロキシのデータが表示されます。



ネットワーク サービスの表示と監視:グローバルプロテクト認証チェック

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス ❑ これはPrisma Access Insights機能です。

ネットワークサービスには、GlobalProtect認証の成功数と失敗数のレポートが含まれ、モバイルユーザーがPrisma Accessに接続できるかどうかの指標となります。開始するには、**[Monitor (監視)] > [Network Services (ネットワークサービス)] > [GlobalProtect Authentication (GlobalProtect認証)]** をStrata Cloud Managerで選択します。

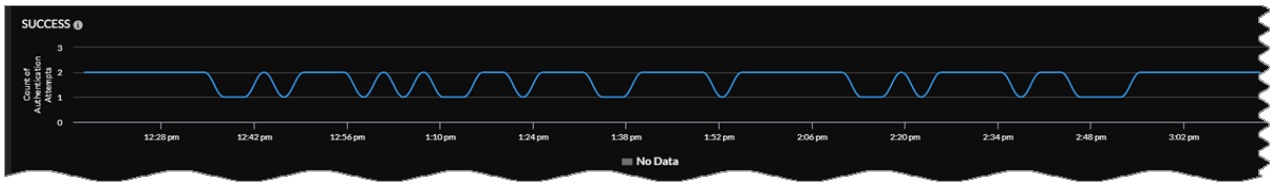
- 時間範囲 フィルターを設定して、その時間範囲のネットワーク サービス データを確認します。

©2025 Palo Alto Networks, Inc.

- **Prisma Access**ロケーションを指定すると、選択した時間範囲内の認証成功、合計失敗、およびタイムアウト失敗が表示されます。

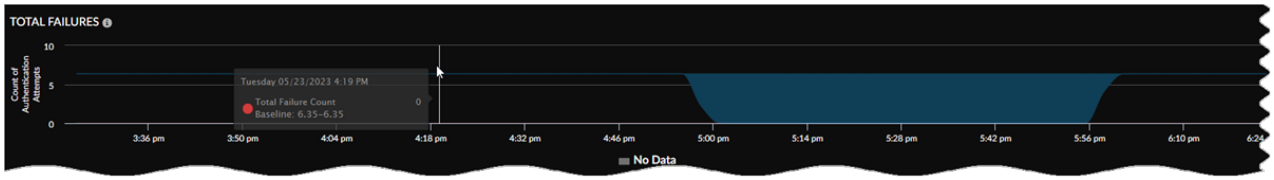
GlobalProtect認証成功

さまざまなロケーションでのGlobalProtectの認証成功数の詳細を表示します。グラフの任意のポイントにカーソルを合わせると、特定の時間に表示されたさまざまなPrisma Accessロケーション サイトで認証に成功したユーザー数の詳細が表示されます。



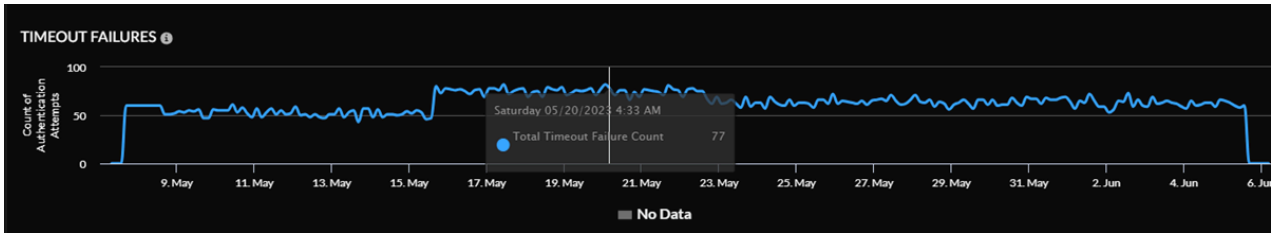
GlobalProtect 認証失敗総数

さまざまなロケーションの GlobalProtect の認証失敗数に関する詳細を表示します。グラフの任意のポイントにカーソルを合わせると、米国東部やカナダ東部など、表示されているPrisma Accessロケーション サイトごとに、特定の時刻に認証に失敗したユーザー数の詳細が表示されます。



GlobalProtect認証タイムアウト失敗

さまざまなロケーションの GlobalProtect の認証失敗数に関する詳細を表示します。グラフの任意のポイントにカーソルを合わせると、米国東部やカナダ東部など、表示されているPrisma Accessロケーション サイトごとに、特定の時刻に認証に失敗したユーザー数の詳細が表示されます。



ネットワーク サービスの表示と監視:DNS

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス ❑ これはPrisma Access Insightsの機能です。

©2025 Palo Alto Networks, Inc.

Network Services（ネットワーク サービス）**DNS**は、指定した時間範囲内にサーバーに転送された DNS プロキシ要求と応答を表示します。

使用できるフィルター:

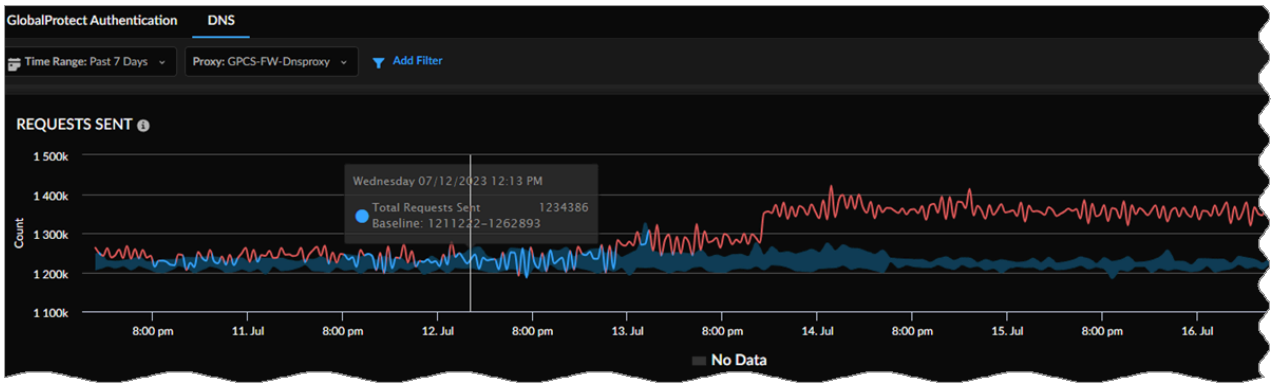
- 期間
- **DNS**プロキシ名

DNSプロキシフィルタの値は過去30日間に関連し、ロード時に自動的に選択されます（つまり、明示的なプロキシデータがない場合は、明示的なプロキシフィルタは存在しません）。

グラフの上にマウスを置くと、特定の時間に DNS プロキシ サーバーに送信された要求 と 受信した要求のすべての詳細が表示されます。

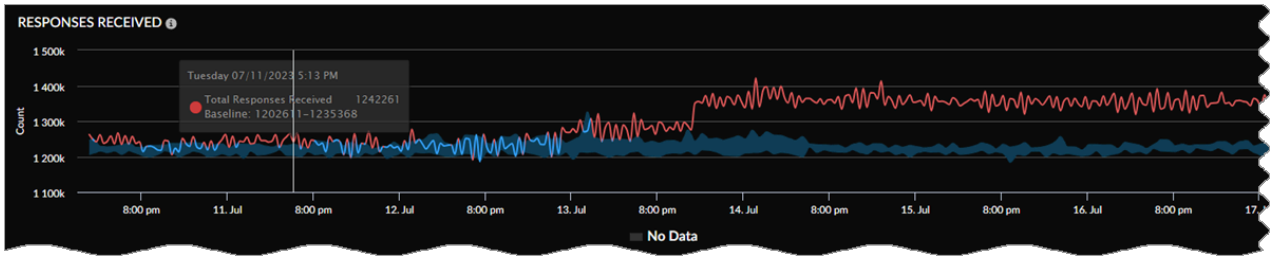
要求が送信されました

指定した時間範囲にサーバーに転送されたネットワーク要求とクエリを表示します。グラフ内の任意のポイントにカーソルを合わせると、その時点で DNS プロキシ サーバーに送信された要求に関する情報が表示されます。フィルタリングするプロキシ名を選択した場合は、そのプロキシのデータが表示されます。



受け取った応答

指定した期間内にテナント全体で受信した応答の合計を表示します。グラフ内の任意のポイントにカーソルを合わせると、その時点で受信した応答に関する情報が表示されます。フィルタリングするプロキシ名を選択した場合は、そのプロキシのデータが表示されます。

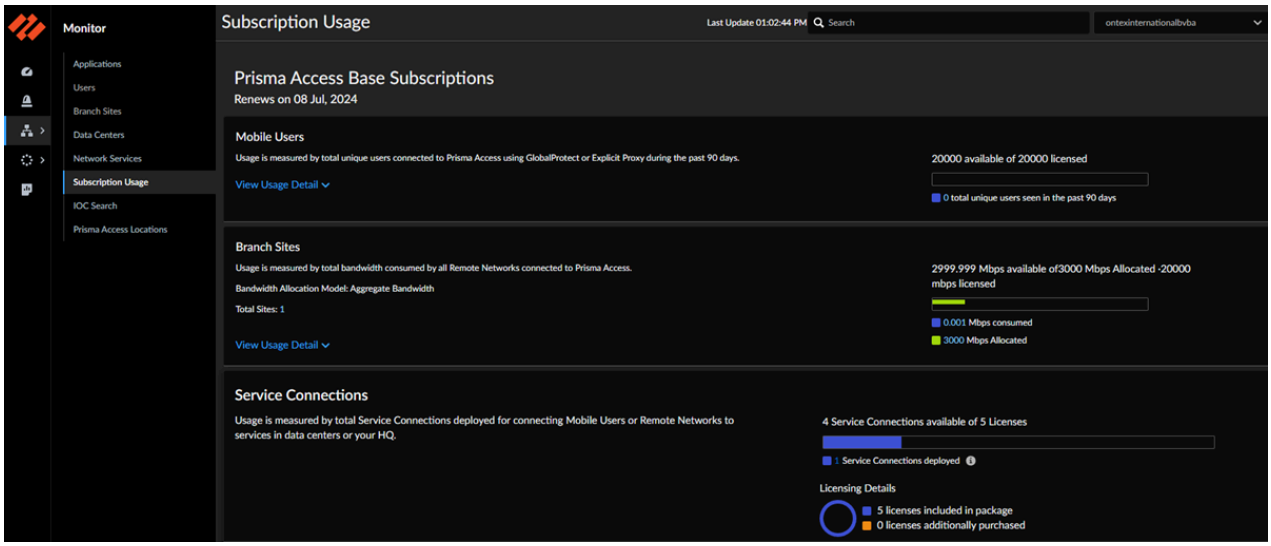


 ©2025 Palo Alto Networks, Inc.

サブスクリプションの使用状況を表示

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

[Monitor (監視)] > **[Subscription Usage (サブスクリプションの使用状況)]**を選択すると、これまでに消費したライセンス数など、**[Prisma Access Base Subscriptions (基本サブスクリプション)]**に関する詳細が表示されます。

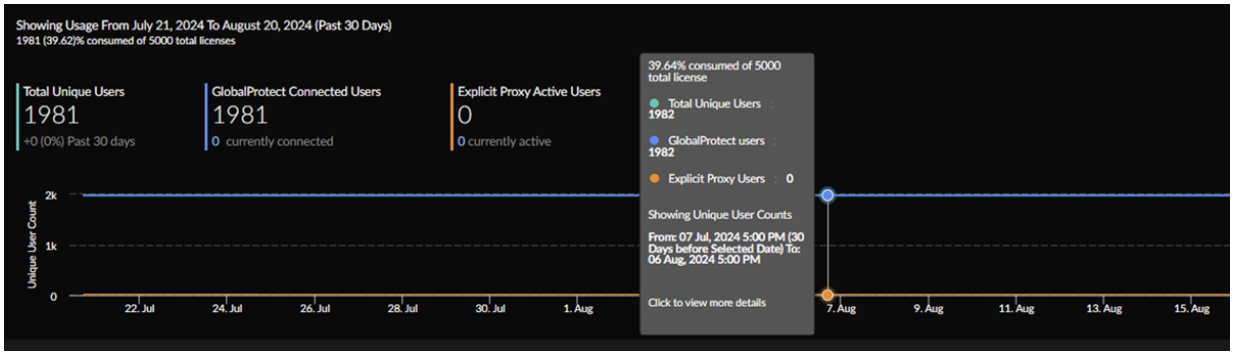


- モバイルユーザー–これまでに利用したユニークなモバイルユーザーライセンス数を表示します。ライセンスは過去30日間のPrisma Accessログインデータに基づいているため、ウィジェットには過去30日間にPrisma Accessに接続したユニークモバイルユーザーが消費したライセンスの合計数が表示されます。過去30日間に1回以上Prisma Accessにログインしたユーザーが、1つのモバイルユーザーライセンスの消費に貢献します。

  過去 30 日間のライセンス使用状況の詳細を表示するには、[使用状況の詳細を表示]を選択します。過去 30 日間のユニークユーザーの総数、GlobalProtect に接続しているユーザーの総

©2025 Palo Alto Networks, Inc.

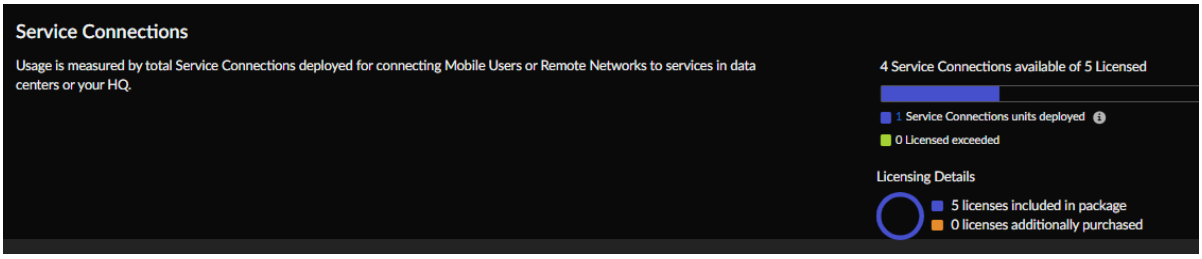
数、およびExplicit Proxyアクティブユーザーの総数を表示できます。グラフにカーソルを合わせると、その時点で使用されていたライセンスが表示されます。



- ブランチサイト-Prisma Accessに接続されているすべてのリモートネットワークによる合計帯域幅使用量が表示されます。Mbps単位で、割り当てた帯域幅と消費した帯域幅を表示します。Prisma Accessに接続されているすべてのリモート・ネットワークで消費された帯域幅の合計で使用量が表示されます。

  [使用状況の詳細を表示]を選択すると、帯域幅割り当てモデルに基づいて、コンピューティング リージョンまたはブランチサイトごとのライセンス帯域幅使用量が表示されます。いずれの場合も、ライセンス計算の対象となる 30 日間の 1 日のピーク帯域幅消費値が示されます。コンピュートリージョンまたはブランチサイトを選択して、グラフビューをフィルタリングできます。グラフには、コンピュートリージョンごとまたはサイトごとに 3 本の線がプロットされており、毎日のピーク消費値、コンピュートリージョンまたはサイトに割り当てられた帯域幅、および毎日のピークから取得された 95 パーセンタイル値を示しています。

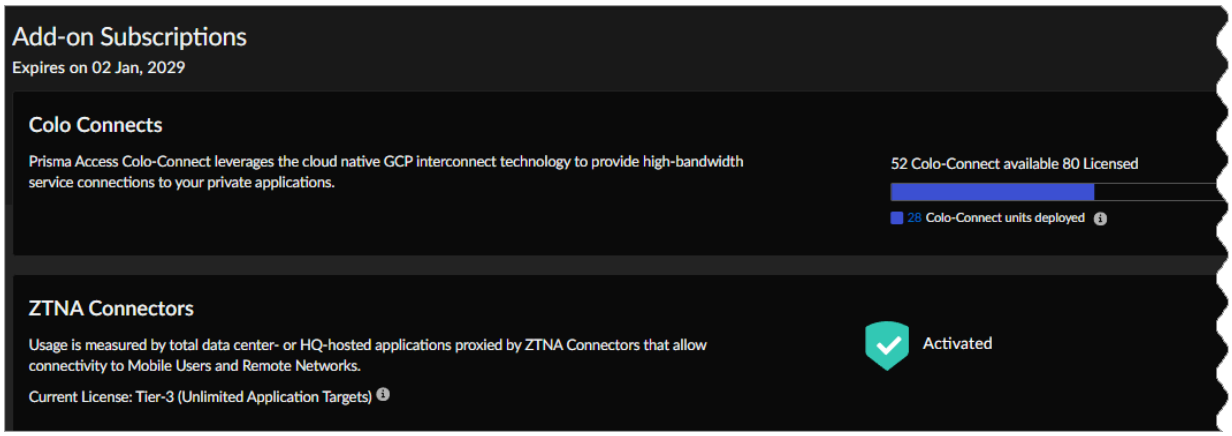
- サービス接続 – これまでに消費したサービス接続ライセンスの数を確認できます。



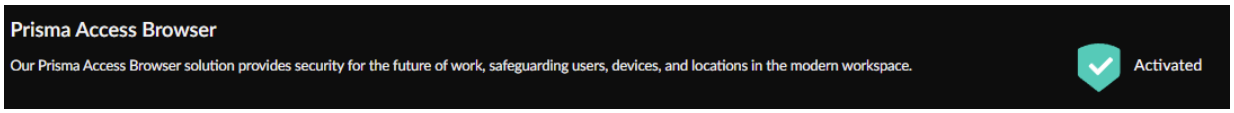
購入した追加ライセンスを確認するには、このページのアドオン サブスクリプションセクションを参照してください。購入したライセンスの総数と、これまでに利用していないライセンス数を確認できます。以下の画像は、購入できる追加ライセンスの一部を示しています。

©2025 Palo Alto Networks, Inc.

- **Colo-Connects** —Prisma Access Colo-Connectは、クラウドネイティブのGCPテクノロジーを活用して、プライベートアプリケーションに高帯域幅のサービス接続を提供します。



- **Prisma Access Browser** —Prisma Access Secure Enterprise Browser (Prisma Access Browser)は、保護機能を非管理対象デバイスにまで拡張するネイティブ統合エンタープライズブラウザを通じて、管理対象デバイスと非管理対象デバイスの両方を保護する唯一のソリューションです。Prisma Access Browserは、ブラウザにセキュリティを設定することにより、ビジネスアプリとデータを保護します。Prisma Access Browserサブスクリプションは、アドオン サブスクリプションまたは **Prisma Access**基本サブスクリプションに表示されます。
  - **Prisma Access**基本サブスクリプション – テナントには Prisma Access Browser スタンドアロンライセンスがあります。
  - アドオン サブスクリプション – すべてのモバイルユーザー向けにPrisma Access Browserライセンスを購入すると、Prisma Access Browser サブスクリプションが有効になります。



Prisma Accessのロケーションを表示および監視する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス ❑ これはPrisma Access Insightsの機能です。

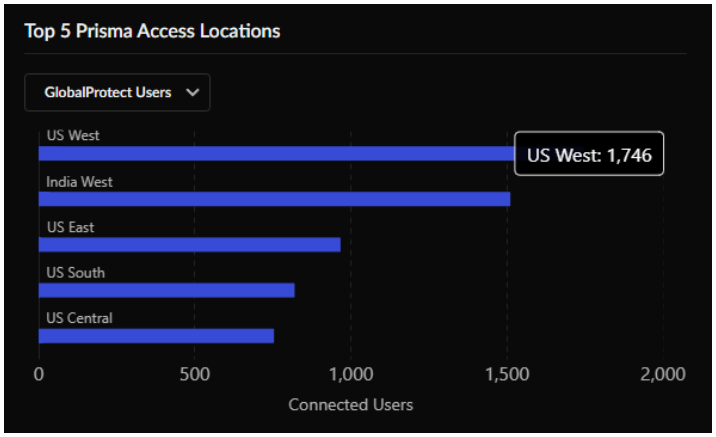
[Monitor (監視)] > **[Prisma Access Locations (ロケーション)]**を選択すると、リモートネットワークとモバイルユーザーのために、すべてのロケーションの健全性の概要が表示されます。

トップ5Prisma Accessロケーション

棒グラフには、選択した時間帯に消費された帯域幅の合計に基づいて、リモートネットワーク、サービス接続、GlobalProtectモバイルユーザー、またはExplicit Proxyモバイルユーザー（ドロップダウンから選択）の上位5位Prisma Accessロケーションに関するデータが表示されます。

©2025 Palo Alto Networks, Inc.

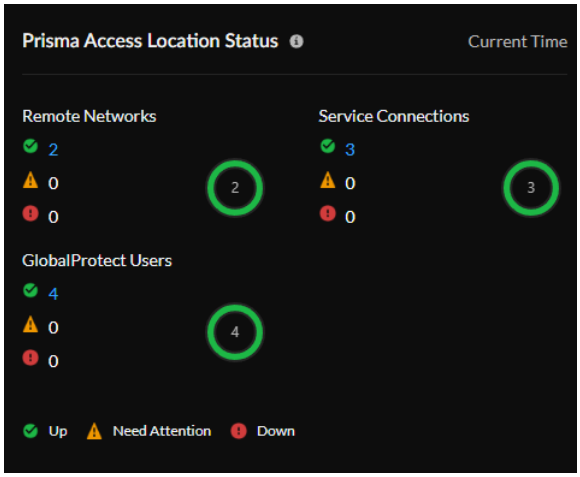
いずれかのバーにマウスを合わせると、その特定の場所に何人のユーザーがいるかが表示されます。



Prisma Accessロケーションのステータス

ライセンスに応じて、このウィジェットは、Prisma Accessにログインしているリモートネットワークサ イト、サービス接続サイト、一意の GlobalProtect ユーザー、および一意の Explicit Proxy ユーザーの数を表示します。ウィジェットの色コードは、次のステータスにあるリモートネットワーク、サービス接続、GlobalProtect ユーザー、および明示的なプロキシ ユーザーの数に基づいています。

- 接続済み （緑）–すべてのPrisma Access ロケーションはつながっています。
- 切断 （赤）–すべてのPrisma Accessロケーションが切断されています。
- 部分的に接続 （オレンジ）–1つ以上のPrisma Accessロケーションが切断されています。



Strata Logging Service接続性

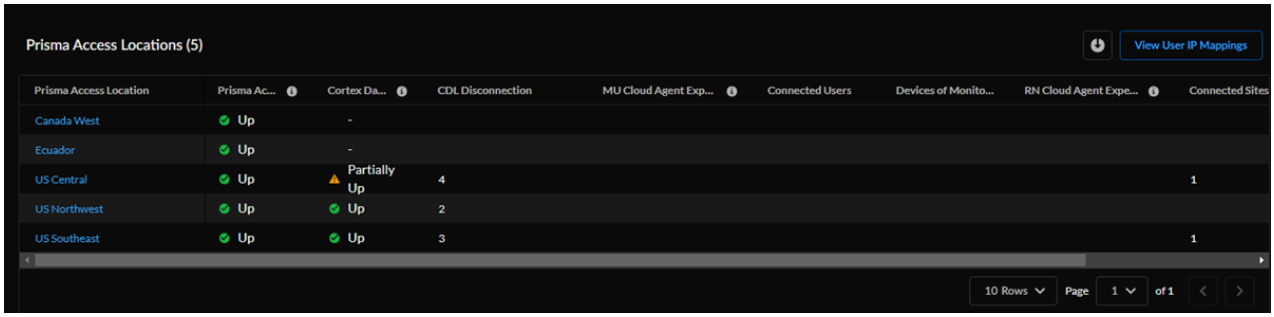
[Strata Logging ServiceConnectivity (Strata Logging Service接続性)]: このウィジェットを使用すると、Prisma Accessライセンスのアクティベーション時に選択したStrata Logging Service地域のすべてのPrisma Accessインスタンスから、Strata Logging Service接続の健全性を可視化できます。ファイアウォールがStrata Logging Serviceワークから切断され、ファイアウォールのログを取得していないかどうかを判断するのに役立ちます。各テナントは、任

©2025 Palo Alto Networks, Inc.

意の地域にある 1 つのStrata Logging Serviceにのみ接続できます。Prisma Accessは5分ごとにStrata Logging Serviceデータベースをポーリングし、ノード（モバイルユーザー、リモートネットワーク、サービス接続）とStrata Logging Serviceデータベース間の接続性をチェックします。

Prisma Accessロケーションのステータス

Prisma Access ロケーション ステータスをリアルタイムで表示します。特定の場所において、1人のユーザーが複数のホストからログインした場合、そのユー ザーは1人のユーザーとしてカウントされるが、2つの異なるPrisma Accessロケーションからログインしたユーザーが期間内に1つから切断し、片方のロケーションからログイン した場合、そのユーザーは2人のユーザーとしてカウントされます。ロケーションを選択すると、消費された帯域幅、ステータス、Strata Logging Service接続、ユーザーIDとグループ マッピングなどの詳細が表示されます。



サードパーティデバイスIDの表示と監視

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

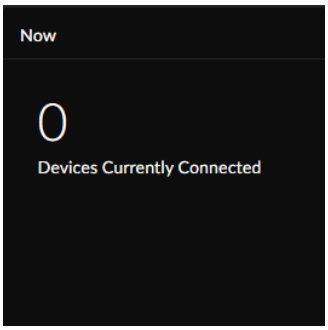
Prisma AccessでCloud Identity Engineを使用して、サードパーティのIoT検出ソー スからの情報を適用し、ネットワーク内のデバイスのセキュリティ ギャップを特定し、 解決する作業を簡素化できる。セットアップと構成の詳細については、「Prisma Accessでのサードパーティデバイスの設定」を参照してください。

[Monitor (監視)] > [Devices (デバイス)] > [IOT] に移動して、 過去30分以内に接続されたIoTデバイスの数、選択した時間帯に接続されたすべてのIoTデバイス、接続されたすべてのIoTデバイスの詳細など、IoTデバイスに関する洞察を得ることができます。

現在の接続済みデバイス

過去 30 分間に接続されたデバイスの数 (ある場合) を表示します。**Now (現在)**は常に現在接続中のデバイスを過去30分間に限って表示します。

©2025 Palo Alto Networks, Inc.

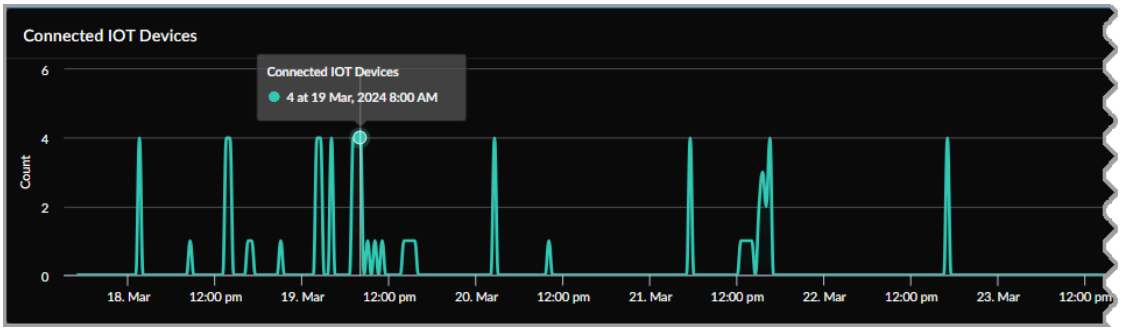


接続済みIoTデバイス

接続されている **IoT** デバイスには、時間範囲でフィルタリングされた接続デバイスの数が表示されます。**[**フィルターの追加**]**ドロップダウンから他のフィルターオプションを選択して、表示されるデータをカスタマイズします。

- カテゴリ – このデバイスが属するカテゴリ。
- **Mac**アドレス – デバイスのMACアドレス。
- プロファイル – デバイスプロファイル。
- ベンダー – デバイスのベンダー。
- 送信元**IP** – デバイスのIPアドレス。
- **Prisma Access**ロケーション – デバイスのPrisma Accessロケーション。
- ブランチサイト – デバイスが存在するブランチサイト。

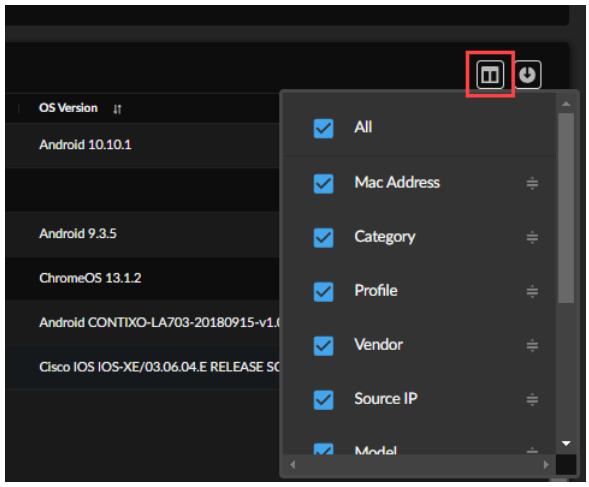
グラフ内のポイントにカーソルを合わせると、特定の時間におけるユーザー数が表示されます。一定期間のユーザー動向を把握することで、利用状況のモニタリングや異常なパターンの調査に役立ちます。



IoT デバイス

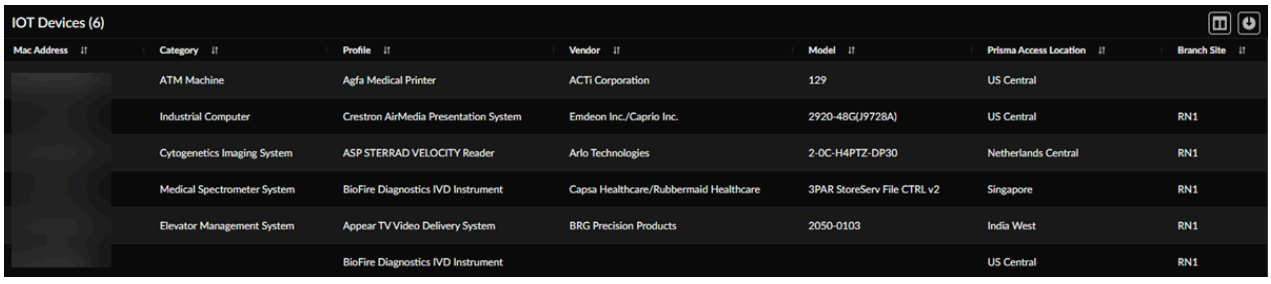
選択した時間範囲で接続された IoT デバイスの数を表示します。列ドロップダウンを使用して、テーブルに表示される列を選択または選択解除します。

©2025 Palo Alto Networks, Inc.



- **Mac**アドレス – デバイスのMACアドレス。
- カテゴリ – このデバイスが属するカテゴリ。
- プロファイル – デバイスプロファイル。
- ベンダー – デバイスベンダー。
- 送信元 **IP** – デバイスの IP アドレス。
- モデル – デバイスモデル。
- **OS** バージョン – OS バージョン。
- **OS** ファミリ – デバイスが属する OS ファミリ。
- **Prisma Access**ロケーション – 使用されているPrisma Accessロケーション。
- ブランチサイト – デバイスが存在するブランチサイト。

次の IoT デバイスの表は、カスタマイズされた列選択を示しています。テーブルのすべての列を表示するには、ドロップダウンですべてのオプションを選択します。



リモートブラウザ分離の表示と監視

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 5.0 イノベーション

 ©2025 Palo Alto Networks, Inc.

Strata Cloud ManagerのMonitor (監視)セクションとWorkflows (ワークフロー)セクションを使用することで、Strata Cloud Managerを使用して、ネットワークトラフィックを包括的に可視化し、リモートブラウザ隔離（RBI）を行うことができます。アクティブな RBI ユーザーの数、傾向、接続ステータス、RBI ロケーション ステータス、トラフィック測定、ライセンス消費などのメトリックを表示して、RBIデプロイメントの可視性を高めます。ユーザーに関するデータを表示することで、デプロイメントの正常性と接続性の全体像を把握できます。

RBI は、ユーザーのインターネット閲覧アクティビティを、RBI プロバイダーがホストする隔離された環境にリダイレクトします。ウェブサイトはユーザー向けにレンダリングされ、ユーザーは自分のデバイスやネットワークから未知のサイトや危険なサイトに直接アクセスすることなく、必要なリソースを表示できます。 このタイプのブラウザ リダイレクトでは、Prisma AccessはRBI プロバイダーと簡単に統合できます。

 ©2025 Palo Alto Networks, Inc.

Prisma Accessと自律型DEM

どこで使用できますか?	何が必要ですか?
• Strata Cloud Manager Managed Prisma Access • Panorama Managed Prisma Access	❑ Prisma Accessのライセンス ❑ Autonomous DEMライセンス

Prisma Accessの自律型DEMを使い始めると、SASE環境内のすべてのユーザー、アプリケーション、リモート サイトのデジタル エクスペリエンスを継続的に監視できます。それぞれのライセンスを持っている限り、Prisma Accessに接続するGlobalProtectモバイル ユーザーに対して自律型DEMを有効にすることができます。

- チートシート:ADEM付きPrisma Access
- 自律型DEMを使い始める
- 自律型DEMによるユーザートラフィックとアプリケーションの監視

©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

Prisma Access ユーザーベースのポリシー

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • Cloud Identity Engine	• Prisma Accessライセンス

Prisma Accessでは、モバイルユーザーとリモートネットワークロケーションのユーザーに対して、ユーザーベースのポリシーを一貫して適用するために、IPアドレス - ユーザー名間マッピングのマッピングを設定する必要があります。また、グループメンバーシップに基づくポリシーを適用する場合、ユーザー名からユーザーグループへのマッピングを設定する必要があります。

ポリシーを作成および構成する際に、ドロップダウンリストからグループを選択するには、ユーザー名からユーザーグループへのマッピングから取得したユーザーグループのリストを取得するようにPanoramaを構成することもできます。

以下のセクションでは、User-IDを構成および実装するための概要と手順を提供し、Cloud Identity Engineを使用してPrisma AccessでのIPアドレスからユーザー名、ユーザー名からユーザーグループへのマッピングを取得します。

Prisma Accessのユーザー ベース ポリシーを設定します

- Strata Cloud Manager
- Panorama

©2025 Palo Alto Networks, Inc.

Prisma Access ユーザーベースのポリシー

Prisma AccessとCloud Identity Engineを統合した後、Prisma AccessがCloud Identity Engineに接続され、Cloud Identity EngineがPrisma Accessとディレクトリ情報を共有していることを確認する必要があります。

Prisma Accessで自分のディレクトリがPrisma Accessに表示されていることを確認します。

[Manage (管理)] > **[Configuration (設定)]** > **[NGFWとPrisma Access]** > **[Identity Services (IDサービス)]** > **[Cloud Identity Engine (クラウドIDエンジン)]** に移動します。

ポリシールールにユーザーおよびグループを追加できることを確認します。

[Manage (管理)] > **[Configuration (設定)]** > **[NGFW]Prisma Access** > **[Security Services (セキュリティ サービス)]** > **[Decryption (復号化)]**を選択します。

セキュリティまたは復号ポリシー規則で、[ユーザー]ドロップダウンにActive Directory (アクティブディレクトリ - AD)ユーザーおよびグループエントリが表示されることを確認します。これで、これらのユーザーとグループをセキュリティおよび復号ポリシールールに追加できます。

Cloud Identity Engine (クラウドIDエンジン)が正常に接続されていることを確認したら、ユーザーアクティビティレポートを 実行して、ユーザーベースの行動をより詳細に把握することができます。

©2025 Palo Alto Networks, Inc.

Prisma Access ユーザーベースのポリシー (Panorama)

ここでは、Prisma AccessのユーザーIDの設定方法を説明しています。

STEP 1 | モバイルユーザーおよびリモートネットワークロケーションにいるユーザーの、IPアドレス - ユーザー名間マッピングを設定します。

- Mobile Users-GlobalProtectデプロイメントの場合、Prisma AccessのGlobalProtectエージェントは自動的にユーザーIDマッピングを実行します。
- リモートネットワークのユーザーの場合は、リモートネットワークデプロイメント用のユーザーIDを設定して、IPアドレスをユーザーIDにマップします。

STEP 2 | モバイルユーザーおよびリモートネットワークロケーションにいるユーザーの、ユーザーグループマッピングにユーザー名を設定します。

モバイルユーザー（GlobalProtect 、Explicit Proxy、およびリモートネットワークデプロイメント）の場合、Cloud Identity Engineのディレクトリ同期コンポーネントを構成して、Active Directory（AD）からユーザーとグループの情報を取得するようにします。次に、モバイルユーザー（GlobalProtect またはリモートネットワーク）でグループマッピング設定を設定します。

また、LDAPサーバプロファイルを使用して、モバイルユーザーやリモートネットワークのユーザーに対して、ユーザー名からユーザーグループへのマッピングを有効にすることもできます。

すべてのグループ情報を取得するのではなく、取得するグループを指定できるように、*LDAP* サーバープロファイル内のGroup Include List（含めるグループのリスト）を使用することをお勧めします。

STEP 3 | 次のいずれかのアクションを実行して、Panoramaがセキュリティポリシーでユーザー名とユーザーグループのマッピングを使用できるようにします。

- Cloud Identity Engine (クラウド ID エンジン)のDirectory Sync コンポーネントを設定して、Active Directory (アクティブディレクトリ - AD)からユーザーおよびグループ情報を取得します。次に、Mobile Users-GlobalProtect 、Mobile Users-Explicit Proxy、またはリモートネットワークデプロイメントでグループマッピング設定を構成します。
- グループの完全な識別名 (DN) を指定して、グループベースのポリシーを設定します。

STEP 4 | PanoramaへのHIP情報の再配信

©2025 Palo Alto Networks, Inc.

Cloud Identity EngineとPrisma Accessを統合する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

- Strata Cloud Manager
- Panorama

Cloud Identity EngineとPrisma Accessを統合する (Strata Cloud Manager)

Cloud Identity Engine (ディレクトリ同期) は、Prisma AccessにActive Directory (アクティブディレクトリ - AD)情報への読み取り専用アクセスを許可します。これにより、ユーザーやグループのセキュリティポリシーや復号化ポリシーを簡単に設定および管理できるようになります。

Cloud Identity Engineは、オンプレミスのアクティブディレクトリとAzureアクティブディレクトリの両方で動作します。

Prisma AccessでCloud Identity Engineをセットアップするには、まずハブに行ってCloud Identity Engineをアクティベートし、Prisma Accessに追加します。次にPrisma Accessに行き、Prisma Accessがディレクトリデータにアクセスできることを確認します。

©2025 Palo Alto Networks, Inc.



STEP 1 | Cloud Identity Engineのアクティベート

Cloud Identity Engineは、ハブ上のサポートされている任意のアプリとアクティブディレクトリ情報を共有できます。無料で、利用開始に認証コードは必要ありません。Cloud Identity Engineセットアップには、ハブでのCloud Identity Engineアプリの有効化、Active Directoryマッピングを収集するためのCloud Identity Engineエージェントの構成、Cloud Identityとエージェント間の相互認証の構成が含まれます。

Cloud Identity Engineインスタンスは、Prisma AccessとStrata Logging Serviceをデプロイしたのと同じリージョンにデプロイしてください。

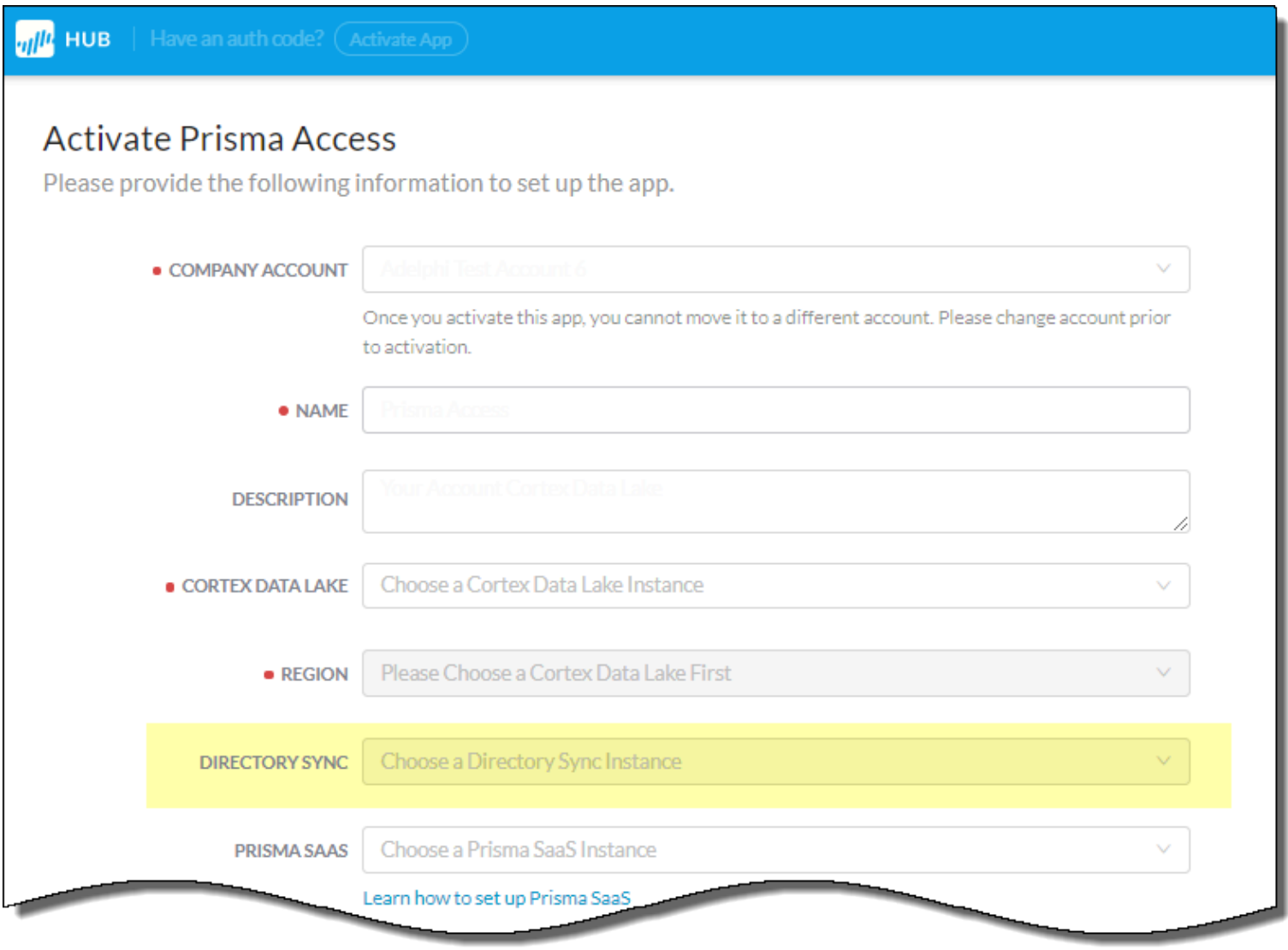
STEP 2 | Prisma Access用のCloud Identity Engineを有効にします。

Prisma AccessをCloud Identity Engineに関連付けるのは、Prisma Accessを最初にアクティベートするときでも、アクティ ベート後でもいつでも可能です。

- **Prisma Access**をアクティベート中 **:**Cloud Managed Prisma Accessを最初にアクティブ化するときに、Prisma Accessで使用するCloud Identity Engineインスタンスを選択できま

©2025 Palo Alto Networks, Inc.

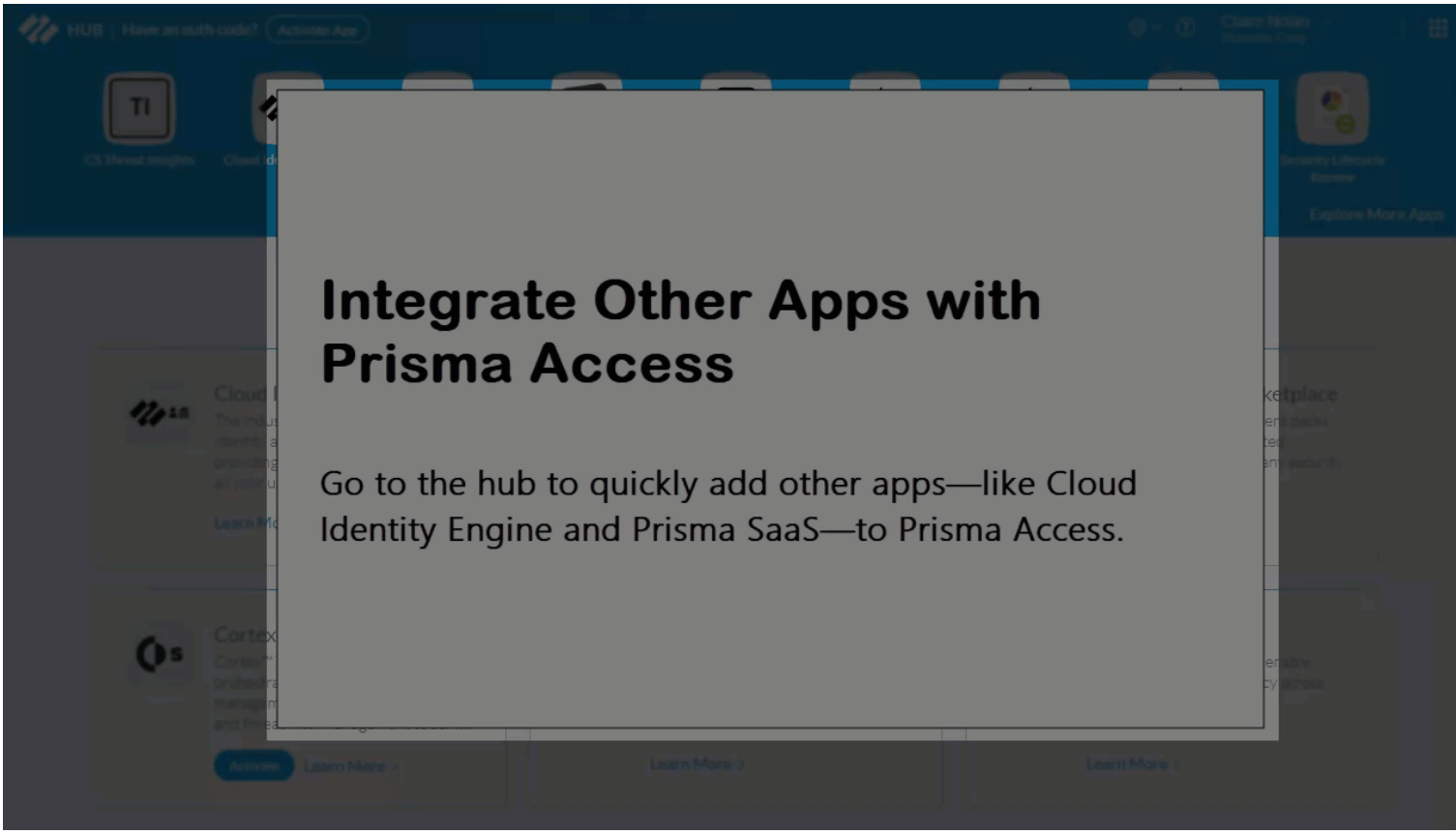
す。Prisma Accessと同じリージョンにデプロイされているインスタンスを必ず選択してください。



- **Prisma Access**のアクティベート後 **:**既存のPrisma Accessインスタンスに対してCloud Identity Engineを有効にするには、ハブにログインします。ハブ設定のドロップダウン（上部メニューバーの歯車を参照）から、［アプリを管理］を選択します。更新し

©2025 Palo Alto Networks, Inc.

たいPrisma Accessインスタンスを見つけ、Prisma Accessで使用したいCloud Identity Engineインスタンスを選択します。



STEP 3 | Prisma AccessがCloud Identity Engineに接続されていることを確認します。

Cloud Identity EngineとPrisma Accessを統合する (Panorama)

Prisma Accessは、ユーザー/グループベースのポリシーを適用するために、組織のクラウドディレクトリもしくはActive Directory (アクティブディレクトリ - AD)からユーザー/グループ情報を取得します。必要に応じてPrisma Accessは、Azure Active Directory などの一部のクラウド ディレクトリ ベンダーからユーザーの行動ベースのリスク シグナルを取得して、自動化されたセキュリティ アクションを適用します。Cloud Identity Engineを使用することで、ユーザーとグループ情報の検索を簡素化できます。

ユーザーおよびグループ情報の検索を簡素化するだけでなく、Cloud Identity EngineをPrisma Accessと統合することで、クラウド ディレクトリまたはADの帯域幅と負荷を解放することができる。

以下の手順を実行することで、Cloud Identity Engineを使用して、モバイル ユーザー、リ モート ネットワーク、またはその両方のPrisma Accessのユーザーおよびグループ情報を取得できます。

Prisma AccessとのCloud Identity Engine統合には、以下の実装制限があります：

©2025 Palo Alto Networks, Inc.

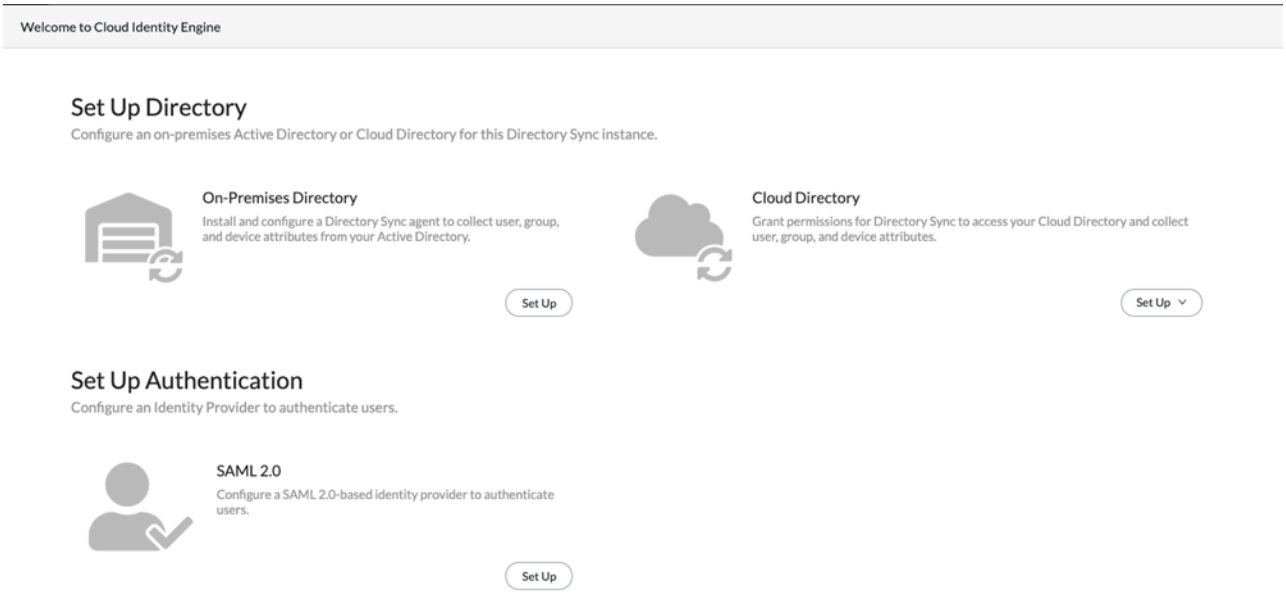
- Prisma Accessはグループ内での以下の特殊文字の使用をサポートしておらず、コミット操作が失敗するため、Cloud Identity Engineで使用するグループに以下の特殊文字がないことを確認します。
  - "（二重引用符）
  - '（アポストロフィ）
  - <（しょうなり不等号）
  - >（だいなり不等号）
  - &（アンパサンド ）
- Cloud Identity Engine をPrisma Accessと関連付ける場合、ユーザー名はドメインを含むNetBIOS形式を使用する必要があります。ユーザー名は、電子メール形式 (ユーザー名@ドメイン)、 **NetBIOS\sAMAccountName** 形式、またはユーザー プリンシパル名 (UPN) 形式 (ユーザー名@ドメイン.com)に指定できます。
- グループ名は、**distinguishedName**フォーマットを使用する必要があります（例:**CN=Users,CN=Builtin,DC=Example,DC=com**）。
- Directory Syncでは、Group Include List（グループ包含リスト）（**Device**（デバイス） > **User Identification**（ユーザーID） > **Group Mapping Settings**（グループマッピング設定） > **Group Include List**（グループ包含リスト））で指定した設定が適用されません。すべてのデバイス グループおよびテンプレートで使用されているグループを含め、ユーザー/グループ情報は、全体的な設定から取得されます。

STEP 1 | Prisma Access用のCloud Identity Engineインスタンスを作成し、インスタンス名をメモします。

Cloud Identity Engine をアクティベートする際に、インスタンスが作成されます。このインスタンス名は、後の手順でクラウドIDエンジンとPrisma Accessを関連付けるときに使用します。Prisma Access用に個別のインスタンスを作成する必要がある場合は、必要に応じてそれを作成してインスタンス名を書き留めておきます。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | ディレクトリデータを取得するようにCloud Identity Engineを設定します。



STEP 3 | (オンプレミスの Active Directory のみを使用したデプロイメント) オンプレミスのActive Directoryを使用する場合は、 Cloud Identity Agent のインストールと設定 を行ってオンプレミスのADと通信し、Cloud Identity Engineサービスとエージェント間の相互認証を構成します。

STEP 4 | Prisma Accessでクラウドエンジンを有効にします。

1. Prisma Accessを管理するPanoramaで、ユーザー名からユーザーグループへのマッピング設定タブを選択します。
   - モバイル ユーザー - GlobalProtectデプロイメントの場合は、 **[Panorama]** > **[クラウドサービス]** > **[Configuration (構成)]** > **[モバイルユーザー—GlobalProtect]**をクリックし、歯車アイコンを選択して設定を編集し、**[グループ マッピング設定]**を選択します。
   - [Mobile Users—Explicit Proxy (モバイル ユーザー - 明示型プロキシ)]デプロイメントの場合は、 **[Panorama]** > **[クラウドサービス]** > **[Configuration (構成)]** > **[Mobile Users—Explicit Proxy (モバイル ユーザ - 明示型プロキシ)]**をクリックし、歯車アイコンを選択して設定を編集し、**[Group Mapping Settings (グループ マッピング設定)]**を選択します。
   - リモートネットワーク デプロイメントの場合は、 **[Panorama]** > **[クラウドサービス]** > **[Configuration (構成)]** > **[リモートネットワーク]**をクリックし、歯車アイコンを選択して設定を編集し、 **[Group Mapping Settings (グループ マッピング設定)]**を選択します。
2. **Enable Directory Sync Integration**（**Directory Sync**統合を有効にする）を選択して、Prisma Accessを使ったCloud Identity Engineを有効にします。

©2025 Palo Alto Networks, Inc.

3. 以下の情報を入力します。
   - プライマリユーザー名を入力します。このフィールドは必須です。

     プライマリユーザー名 属性は、ログとレポートで使用される形式を制御します。プライマリ ユーザー名属性が **userPrincipalName (**ユーザープリンシパル名**) (UPN)** の場合、すべてのログエントリとレポートエントリにその形式でソースユーザーが表示されます。多くのデプロイメントでは、UPN、**sAMAccountName**、メールのいずれかの形式を使用します。組織で別の属性を使用している場合は、ここで指定して、組織全体でログ記録とレポート作成の一貫性を確保できます。

     Azure AD 又はOktaディレクトリを設定する場合、 Cloud Identity Engine の ID プロバイダ(IdP)として、 プライマリユーザー名 として ユーザープリンシパル名を指定します。Prisma Access は、Azure AD とOkta Directoryで使用されるuserPrincipalName (UPN) 属性をサポートします。
   - （任意）**E-Mail**（メール）属性（**mail**など）を入力します。
   - （任意）ユーザーの代替名属性を使用する場合、それらを入力します。3つの代替ユーザー名（**Alternate User Name 1**、**Alternate User Name 2**、および**Alternate User Name 3**）を入力することができます。
4. 完了したら**OK**をクリックします。

STEP 5 | **Commit**（コミット） > **Commit and Push**（コミットおよびプッシュ）の順に選択して、変更内容をコミットおよびプッシュします。

 ©2025 Palo Alto Networks, Inc.

Prisma AccessのユーザーIDグループ マッピングの取得

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama) • Cloud Identity Engine	• Prisma Accessライセンス

Prisma AccessでユーザーIDのマッピングを設定したら、モバイルユーザーおよびリモートネットワークのユーザーに対する、現在のユーザー名対ユーザーグループ情報を取得できるようになる必要があります。Cloud Identity Engine でグループ マッピング を構成すると、ユーザー名とユーザー グループのマッピングが実行されますが、それらのユーザー グループはセキュリティ ポリシー ルールで選択できません。次世代ファイアウォールをマスター デバイスとして構成する か、Cloud Identity Engineを構成する ことで、グループを設定して、セキュリティ ポリシー ルールのドロップダウン リストで選択できるようにすることができます。

- Cloud Identity Engine
- マスターデバイス
- 長い形式のDistinguished Name (識別名- DN)エントリ

Cloud Identity Engine

Cloud Identity Engineを使用してユーザーとグループの情報を取得するだけでなく、Cloud Identity Engine を使用してセキュリティ ポリシー ルールにユーザー グループ名を入力することもできます。この統合により、オンプレミスまたはVM-Seriesの次世代ファイアウォールをこの目的のために マスター デバイス として構成する必要がなくなります。ただし、マスター デバイスは引き続きサポートされます。

Cloud Identity Engineを使用して、Panorama 管理の マルチテナント デプロイメントでグループ名を入力することもできますが、これはマスター デバイスを使用する場合には不可能です。

Cloud Identity Engineがセキュリティ ポリシー ルールにグループ名を入力できるようにするには、次の手順を実行します。

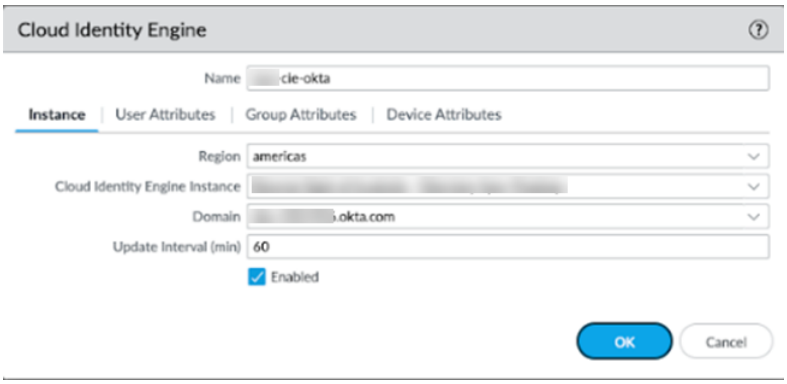
STEP 1 | Cloud Identity Engineで、Cloud Identity Engineをアクティベートし 、 オンプレミス または クラウドベースのディレクトリを追加します (まだ追加していない場合)。

©2025 Palo Alto Networks, Inc.

STEP 2 | Cloud Identity Engineをマッピング ソースとして構成します。

1. Prisma Accessを管理するPanoramaから、**[Panorama]** > **[User Identification (ユーザーID)]** > **[Cloud Identity Engine (クラウドIDエンジン)]** 選択し、プロファイルを追加します 。
2. インスタンスの場合は、次のパラメータを指定します。
   - リージョン- テナントのリージョン エンドポイントを選択します。

     選択するリージョンは、*Cloud Identity Engine* テナントをアクティブ化したときに選択したリージョンと一致する必要があります。
   - **Cloud Identity Engine** インスタンス- プロファイルに関連付けるCloud Identity Engineインスタンスを選択します。
   - ドメイン- 使用するディレクトリが含まれているドメインを選択します。
   - 更新間隔 (分)- Cloud Identity Engineアプリから Panoramaへの更新の間隔 (更新間隔とも呼ばれます) をPanoramaが待機する分数を入力します。デフォルトは 60 分で、範囲は 5 ~ 1440 です。
3. プロファイルが 有効 であることを確認します。

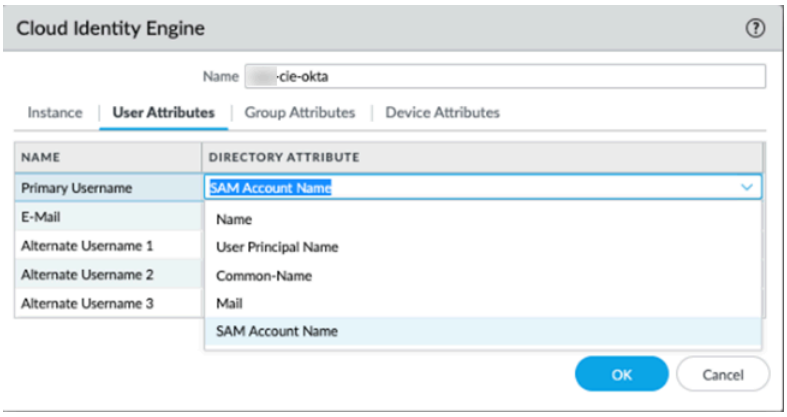


4. ユーザー属性の場合は、プライマリユーザー名の形式を選択します。オプションで、電子メールと代替ユーザー名の形式を選択できます。ユーザーが複数のユーザー名形式

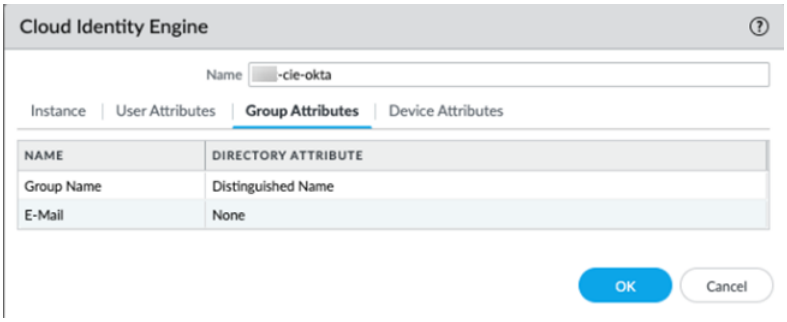
 ©2025 Palo Alto Networks, Inc.

を使用してログインする場合、最大 3 つの代替ユーザー名フォーマットを構成できます。

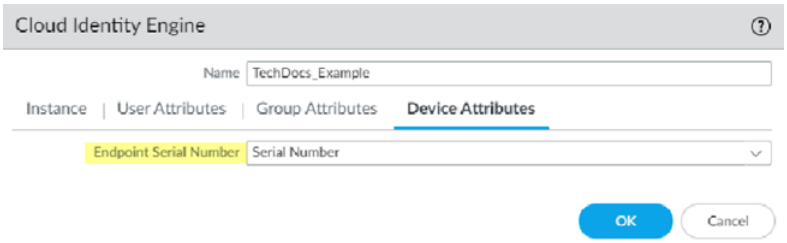
セキュリティ ポリシー ルールでユーザーを表示すると、ユーザー名はここで選択したプライマリ ユーザー名の形式で表示されます。



5. グループ属性の場合は、グループ名 の形式を選択します。



6. デバイス属性は**[None (なし)]**のままにします。

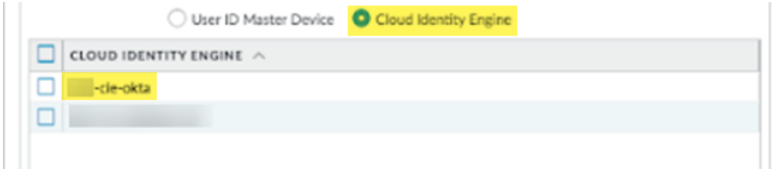


7. 「**OK**」 をクリックし、変更をコミットしてプッシュします 。

©2025 Palo Alto Networks, Inc.

STEP 3 | Prisma Access構成にプロファイルを添付します。

1. 追加するデプロイメントの設定に移動します。
   - モバイル ユーザー - GlobalProtectデプロイメントの場合は、**[Panorama]** > **[Cloud Services (クラウドサービス)]** > **[Configuration (構成)]** > [モバイル ユーザー - **GlobalProtect]** を選択し、歯車をクリックして [設定]を編集します。
   - モバイル ユーザー - Explicit Proxyデプロイメントの場合は、**[Panorama]** > **[Cloud Services (クラウドサービス)]** > **[Configuration (構成)]** > [モバイル ユーザー - **Explicit Proxy]** を選択し、歯車をクリックして [設定]を編集します。
   - モバイル ユーザー - Remote Networksデプロイメントの場合は、**[Panorama]** > **[Cloud Services (クラウドサービス)]** > **[Configuration (構成)]** > [モバイル ユーザー - **Remote Networks]** を選択し、歯車をクリックして [設定]を編集します。
2. **Cloud Identity Engine**を選択します。
3. 作成した Cloud Identity Engineプロファイルを選択します。



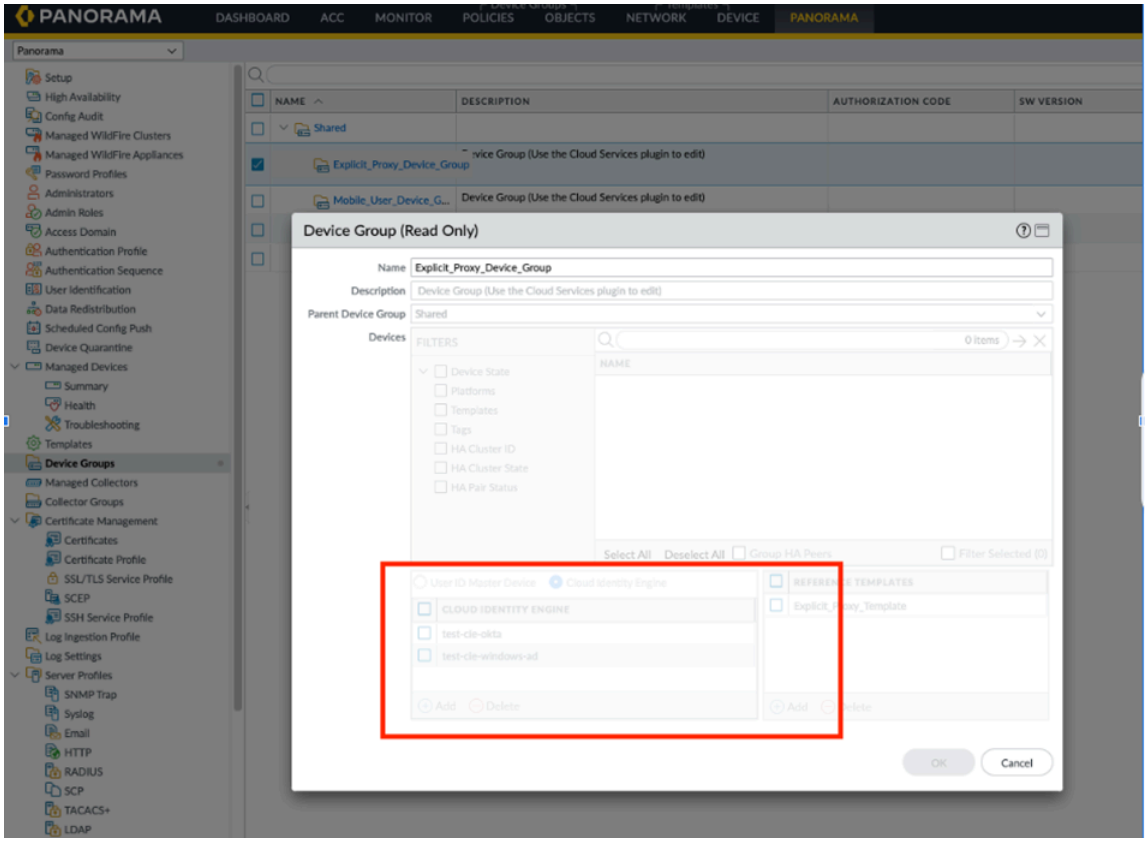
STEP 4 | **Commit**（コミット） > **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

©2025 Palo Alto Networks, Inc.

STEP 5 | Prisma Accessにクラウド ID エンジンからのマッピング情報があることを確認します。

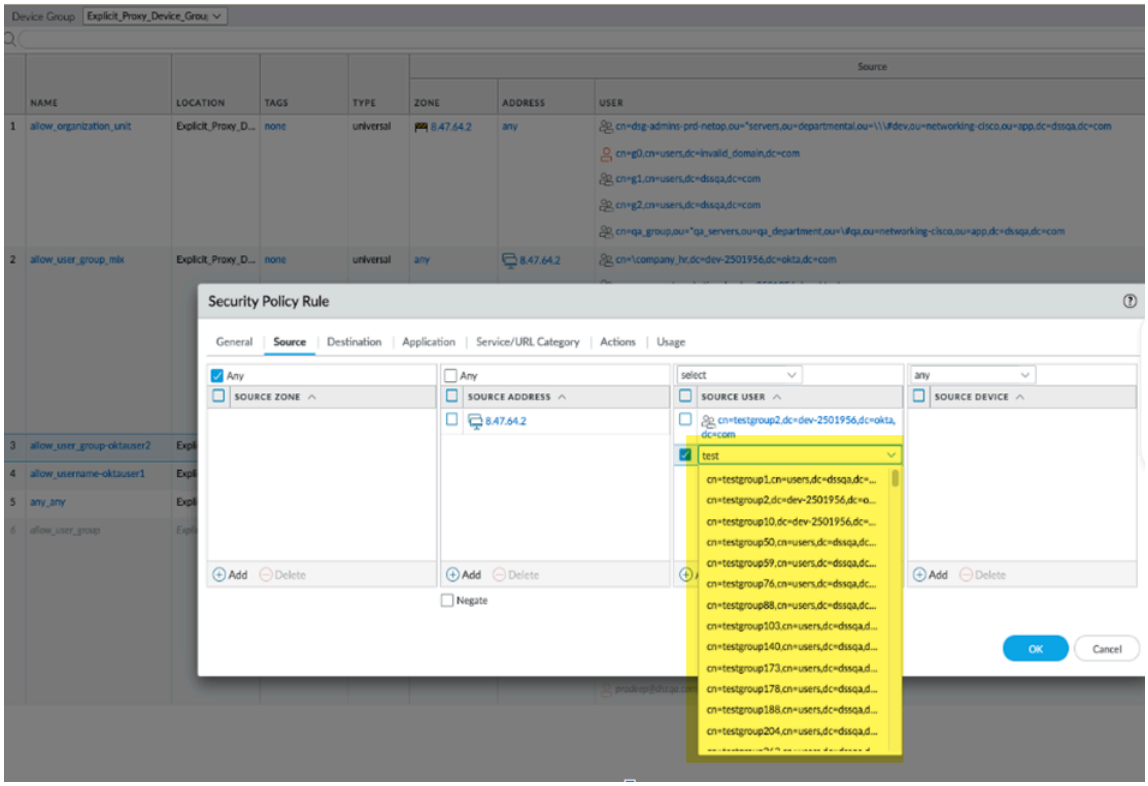
1. **Panorama** > **Device Groups (デバイスグループ)** > ***<template-name>***を選択します。*<template-name>*は構成するデプロイメントのテンプレートであり、Cloud Identity Engineプロファイルがデバイスグループにアタッチされていることを確認します。

   次の例は、デバイス グループがExplicit_Proxy_Device_Groupに正常に接続されていることを示しています。



2. **[Objects (オブジェクト)]** > **[Security (セキュリティ)]** > **[Pre Rules (事前ルール)]**を選択し、セキュリティ ポリシー ルールを追加して 、ユーザー領域にグループが入力されていることを確認します。

 ©2025 Palo Alto Networks, Inc.



マスターデバイス

Cloud Identity Engine でグループ マッピング を構成すると、ユーザー名とユーザー グループのマッピングが実行されますが、それらのユーザー名とユーザー グループはセキュリティ ポリシーに入力されません。ユーザーベースおよびグループベースのポリシーの作成または変更を簡素化するために、マスター デバイスを使用して、セキュリティ ポリシー ルールのドロップダウン リストにグループ名を追加できます。各デバイス グループのマスター デバイスとしてファイアウォールを指定する必要があります。マスター デバイスを追加すると、デバイス グループはマスター デバイスで定義されているすべてのポリシーを継承します。このため、そのデバイス グループにはスタンドアロンの専用デバイスを使用する必要があります。

セキュリティ ポリシーのドロップダウン リストでグループ名を選択できるようにするには、Palo Alto Networks では、デバイス グループごとに マスター デバイス を指定することをお勧めします。オンプレミスファイアウォールまたはVM-seriesファイアウォールを、マスターデバイスとして設定できます。

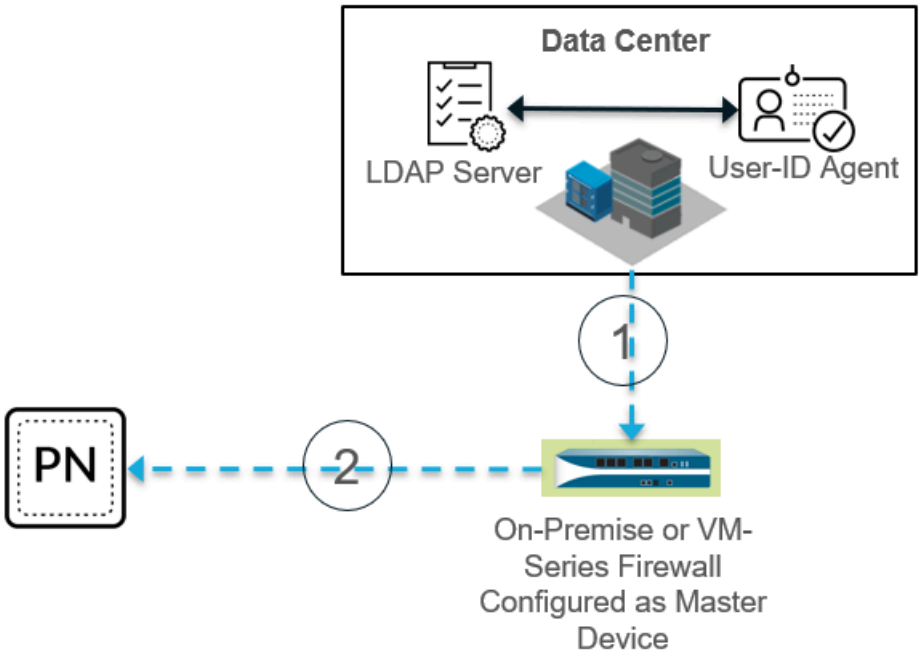
次の図は、管理者がオンプレミスデバイスを**Master Device**（マスターデバイス）として設定した、ユーザーIDデプロイ環境を表しています。図中のコールアウトは、プロセスを表しています。

1. 管理者がマスター デバイスとして構成した次世代オンプレミス ファイアウォールまたはVM-Seriesファイアウォールは、データ センター内のLDAPサーバーとUser-IDエージェントから最新のユーザー名とユーザー グループのマッピングを取得します。

©2025 Palo Alto Networks, Inc.

2. Panorama は、マスター デバイスからユーザー名とユーザー グループのマッピングを取得します。

   Panorama は、セキュリティ ポリシーのドロップダウン リストにグループ名を入力する目的でのみこのマッピングを使用するため、グループに基づくポリシーの作成が簡素化されます。



オンプレミスまたはVM-Seriesファイアウォールのマスターデバイスとしての設定

オンプレミスまたはVM-Seriesファイアウォールをマスターデバイスとして設定するには、次の手順を使用してください。

デバイス グループごとに *1* つのマスター デバイスのみを使用できます。異なるデバイス グループにマスター デバイスを構成する必要がある場合は、デバイス グループごとに個別のマスター デバイスを作成する必要があります。

STEP 1 | マスター デバイスとして使用したいデバイスが、Prisma Accessを管理しているPanoramaによって管理されていることを確認してください。

管理対象デバイスは **[Panorama]** > **[管理対象デバイス]**で確認できます。

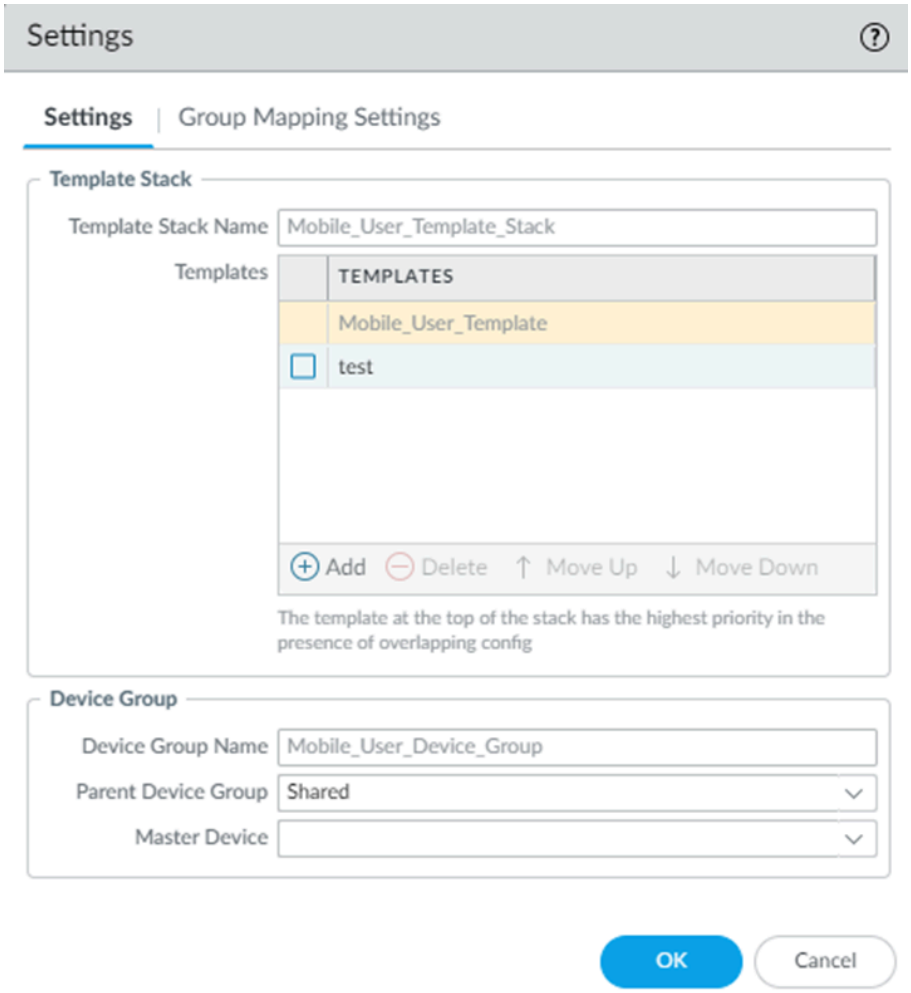
STEP 2 | Prisma Accessモバイル ユーザーまたはリモート ネットワーク デプロイメントにマスター・デバイスを追加します。

- モバイル ユーザー - GlobalProtectデプロイメントの場合は、**[Panorama]** > **[Cloud Services (クラウドサービス)]** > **[Configuration (構成)]** > [モバイル ユーザー -

©2025 Palo Alto Networks, Inc.

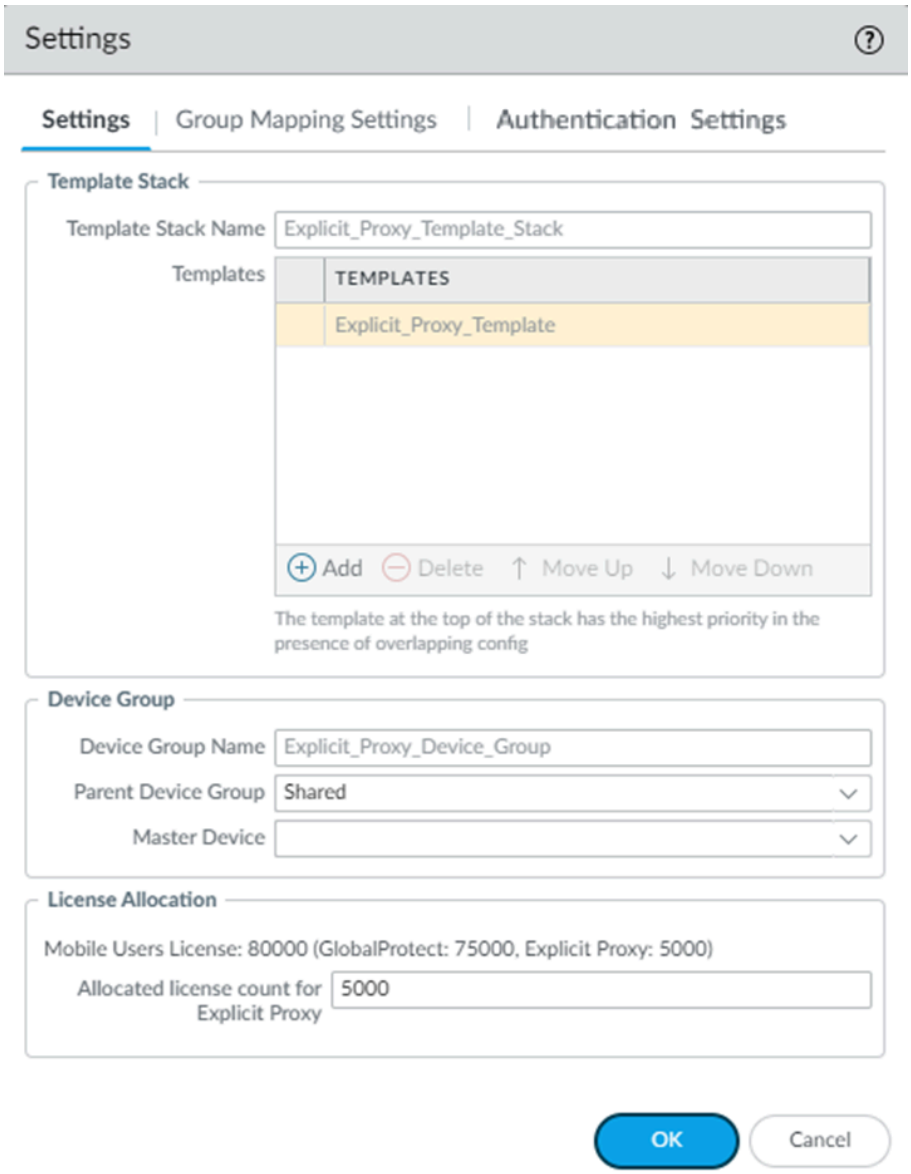
GlobalProtect]を選択し、**[Settings (設定)]**で歯車アイコンをクリックして、 マスター デバイスとして指定するオンプレミス ファイアウォールを選択します。

デフォルトの デバイス グループ名 (この場合は***Mobile_User_Device_Group***) と 親デバイス グループ (この場合は***Shared*** **(共有)**) を使用する場合、別のデバイス グループに関連付けられていないデバイスがドロップダウンの選択肢に表示されます。マスター デバイスを別のデバイス グループに関連付けている場合は、そのデバイス グループに関連付けられている 親デバイス グループを 選択して、ドロップダウンに表示します。



- モバイル ユーザー - 明示型プロキシの展開の場合は、**[Panorama]** > **[Cloud Services (クラウドサービス)]** > **[Configuration (構成)]** > [モバイル ユーザー - 明示型プロキシ]を選択し、[設定]で歯車アイコンをクリックして、作成した マスター デバイス を選択します。

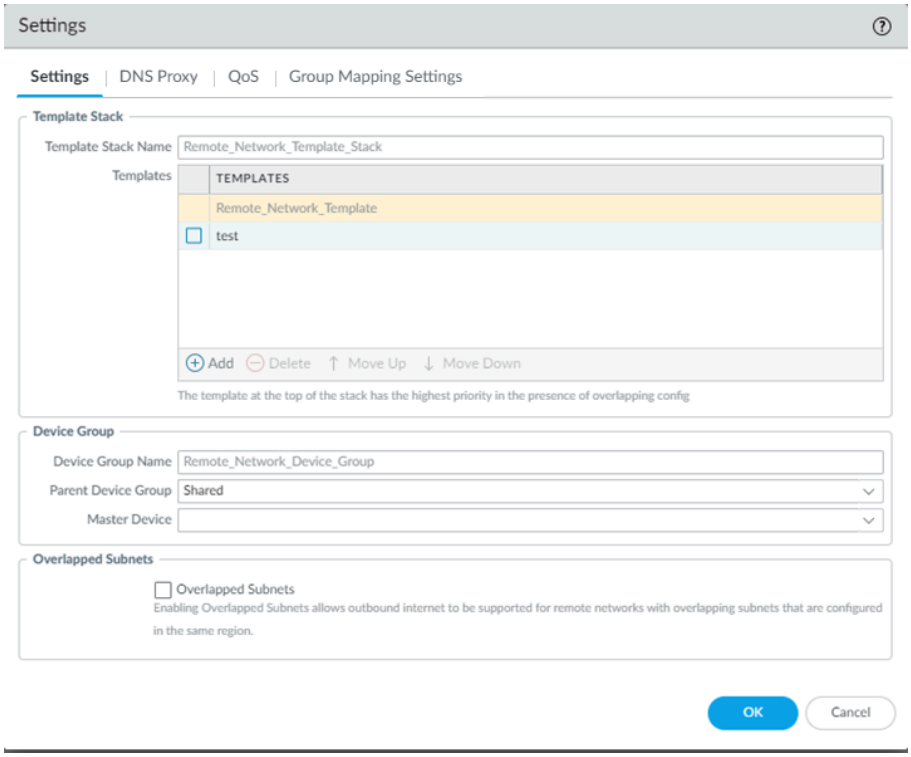
©2025 Palo Alto Networks, Inc.



- リモート ネットワークデプロイメントの場合、リモート ネットワーク接続を持つデバイス グループで、**[Panorama > [Cloud Services (クラウドサービス)] > [Configuration (構**

©2025 Palo Alto Networks, Inc.

成)] > **[Remote Networks (リモート ネットワーク)]**を選択し、[設定]で歯車アイコンをクリックして、作成した マスター デバイス を選択します。



*Prisma Access*はマスター デバイスに関連付けられているデバイス グループのみに対して、ユーザー名とユーザー グループのマッピングを自動的に入力します。この例では、自動入力は ***Remote_Network_Device_Group*** デバイス グループでのみ実行され、他のデバイス グループには入力されません。

STEP 3 | **OK** をクリックします。

長い形式のDistinguished Name (識別名- DN)エントリ

次世代ファイアウォールをマスター デバイスとして設定していない場合、またはセキュリティ ポリシー ルールにユーザーとグループを入力するように Cloud Identity Engineを設定していない場合は、代わりにPanoramaで長い形式のDistinguished Name (識別名- DN) エントリを使用できます。 Prisma Accessは、DNエントリを使用して、Panoramaで設定したユーザーIDベースのポリシーを評価します。

たとえば、IT部門で働いており、1階にいる**Bob Alice**というユーザーの場合、ポリシーが1階のすべてのITスタッフに適用される場合、一致するセキュリティ ポリシーには`cn=first_floor`、`ou=it_staff`、`dc=dev`、`dc=example`、`dc=com`が含まれます。ポリシーがBob Aliceにのみ適用される場合は、`cn=Bob Alice`、`ou=it_staff`、`dc=dev`、`dc=example`、`dc=com` が含まれます。

©2025 Palo Alto Networks, Inc.

アイデンティティ情報再配信

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

セキュリティ ポリシーを一貫して適用できるように、GlobalProtectがローカルで発見したアイデンティティデータをPrisma Access環境全体に共有します。また、リモートネットワークサイトやサービス接続サイト（本社やデータセンター）にあるオンプレミスデバイスとアイデンティティデータを共有することもできます。

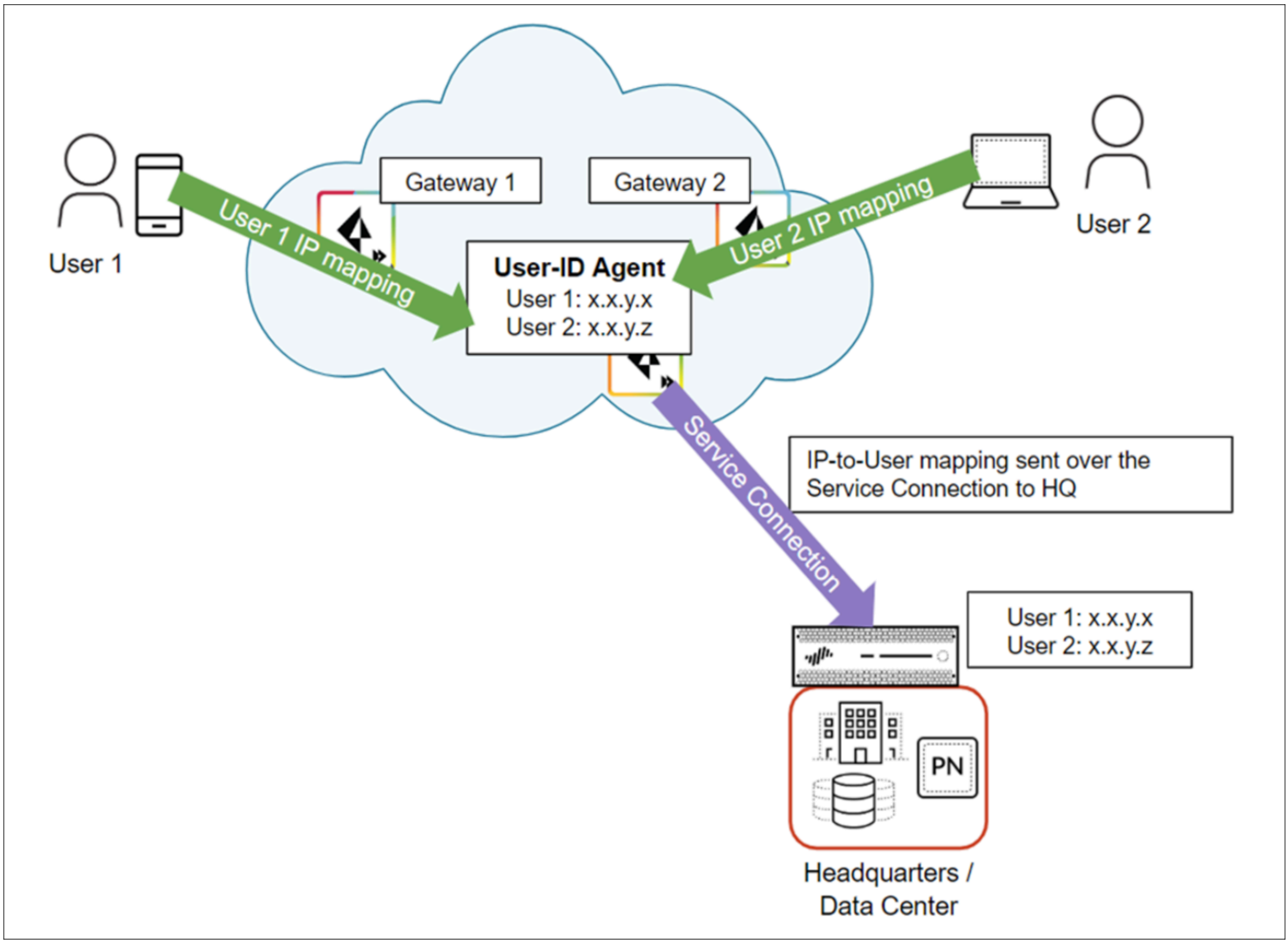
モバイルユーザーが、ユーザーベースのポリシーを持つデバイスによって保護されたリモートネットワークロケーションまたは本社/データセンターのリソースにアクセスするには、Prisma Accessのモバイルユーザーとリモートネットワークのユーザーの**ID**データを、そのオンプレミスデバイスに再配信する必要があります。

ユーザーがPrisma Accessに接続すると、Prisma Accessはユーザーの**ID**データを収集して保存します。

次の例では、Prisma Accessに既存のIPアドレスとユーザ名のマッピングがある2人のモバイルユーザーを示したものです。Prisma Accessはこのマッピングを、本社/データセンターを保護するオンプレミス・デバイスへのサービス接続によって再配信します。

Prisma Access (Managed by Strata Cloud Manager)は、サービス接続をID再配信エージェント（User-IDエージェントとも呼ばれる）として自動的に機能させます。

©2025 Palo Alto Networks, Inc.



- Strata Cloud Manager
- Panorama

アイデンティティ情報再配信 (Strata Cloud Manager)

セキュリティ ポリシーを一貫して適用できるように、Prisma AccessはGlobalProtectがローカルで発見したアイデンティティデータをPrisma Access環境全体に共有します。また、Prisma Accessはリモートネットワークサイトやサービス接続サイト（本社やデータセンター）にあるオンプレミスデバイスとアイデンティティデータを共有することもできます。

Prisma Access (Managed by Strata Cloud Manager)では、IDデータの再配信をデフォルトで一部有効にし、残りの部分については、再配信を有効にする設定を非常にシンプルにしました（共有するデータを選択するチェックボックスをオンにするだけです）。

アイデンティティ配信ダッシュボードから、アイデンティティデータの共有方法を確認し、データの再配信を管理できます（**[Manage (管理)]** > **[Configuration (設定)]** > **[NGFWとPrisma Access]** > **[Identity Services (IDサービス)]**

©2025 Palo Alto Networks, Inc.

再配信できるアイデンティティデータには、次のものがあります。

- HIPデータ
- IPアドレスとタグのマッピング
- IPアドレスとユーザのマッピング
- ユーザーとタグのマッピング
- 隔離されたデバイス

IDの再配信を始める:

- IDの再配信を設定する
- 侵害されたデバイスを特定して隔離する

IDの再配信を設定する

IDの再配信を設定する

サービス接続の設定を確認する

本社またはデータセンターにサービス接続をまだ設定していない場合は、まずサービス接続を設定します。Prisma AccessでIDデータを環境全体で共有するためには、サービス接続が必要です。Prisma Accessはサービス接続が自動的に再配信エージェントとして動作するようにします。新規作成したサービスコネクションサイトにUser-IDエージェントアドレスが割り当てられていることが確認できたら、このサイトを再配信エージェントとして使用できます。Prisma Accessではこの処理が自動的に行われ、数分かかります。

ユーザー*ID*再配信管理 -特に大規模な*Prisma Access*デプロイメントでは、ユーザー*ID*再分配のためにきめ細かい制御が必要になることがあります。ユーザー*ID*再ディストリビューション管理を使用すると、 ユーザー ***ID***列のチェックマークを削除して特定のサービス接続のデフォルトの*ID*再ディストリビューション動作を手動で無効にし、*ID*再ディストリビューションに使用する特定のサービス接続を選択できます。ほとんどの構成ではこれを行う必要はありません。この機能を有効にするには、*Palo Alto Networks*サポートにお問い合わせください。

[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access] > [Identity Services (IDサービス)] > [Identity Redistribution (ID再配信)]に移動し、 設定範囲 をサービス接続に設定して、サービス接続のユーザーIDエージェントの詳細を確認します。

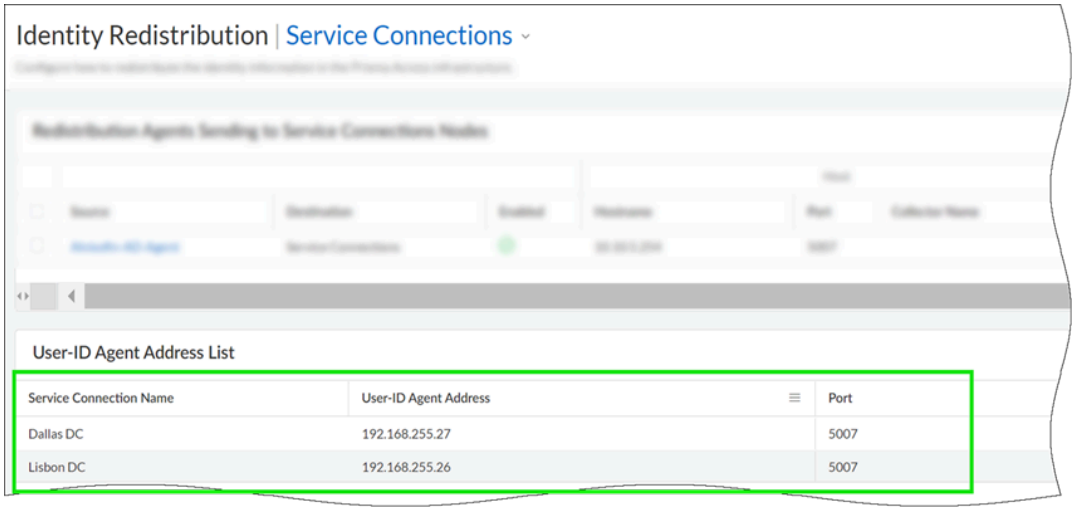
©2025 Palo Alto Networks, Inc.

Prisma Accessからオンプレミスデバイスへ**ID**データを送信します。

サービス接続の**User-ID**エージェント情報は、オンプレミスデバイスに**ID**データを配信するための**Prisma Access**の設定に必要なすべてです。

[Manage (管理)] > [Configuration (設定)] > [NGFWとPrisma Access] > [Identity Services (IDサービス)] > [Identity Redistribution (ID再配信)]に移動し、 設定範囲 をサービス接続に設定して、サービス接続のユーザーIDエージェントの詳細を取得します。

Panorama または Palo Alto Networks NGFW 上でPrisma Accessをデータ再配信エージェントとして構成するには、以 下の詳細を参照してください。

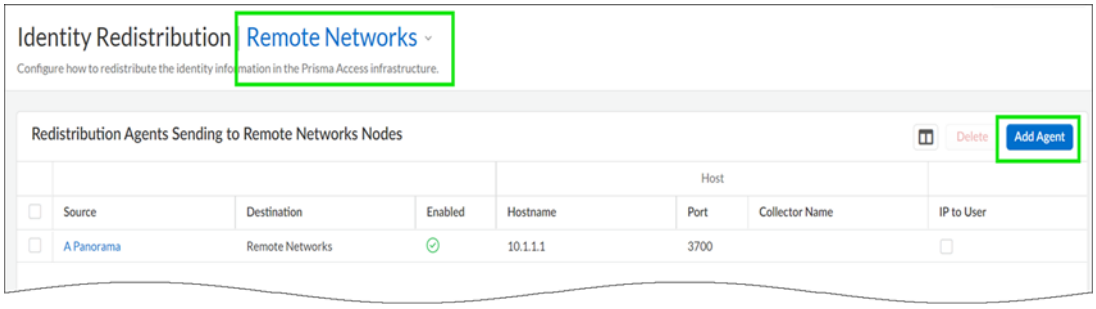


オンプレミスデバイスからPrisma Accessへ**ID**データを送信します。

オンプレミスのデバイスを再配信エージェントとしてPrisma Accessに追加します。追加したデバイスは、アイデンティティデータをPrisma Accessに配信できるようになります。

- リモートネットワークサイトのデバイスから

  Identity Redistribution (ID再配信)ダッシュボードを開き、設定範囲をリモートネットワークに設定し、エージェントを追加します。ホストの詳細を指定するだけでなく、デバイスがPrisma Accessと共有するデータのタイプを選択します。オプション設定には、名前とデバイスの事前共有キーが含まれます。

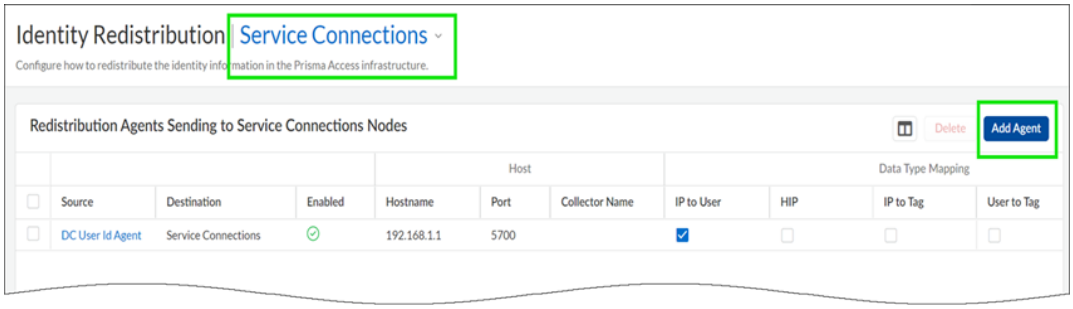


- サービス接続サイトのデバイスからの場合：

  Identity Redistribution (ID再配信)ダッシュボードを開き、設定範囲をサービス接続に設定し、エージェントを追加します。ホストの詳細を指定するだけでなく、デバイスがPrisma

 ©2025 Palo Alto Networks, Inc.

Accessと共有するデータのタイプを選択します。オプション設定には、名前とデバイスの事前共有キーが含まれます。

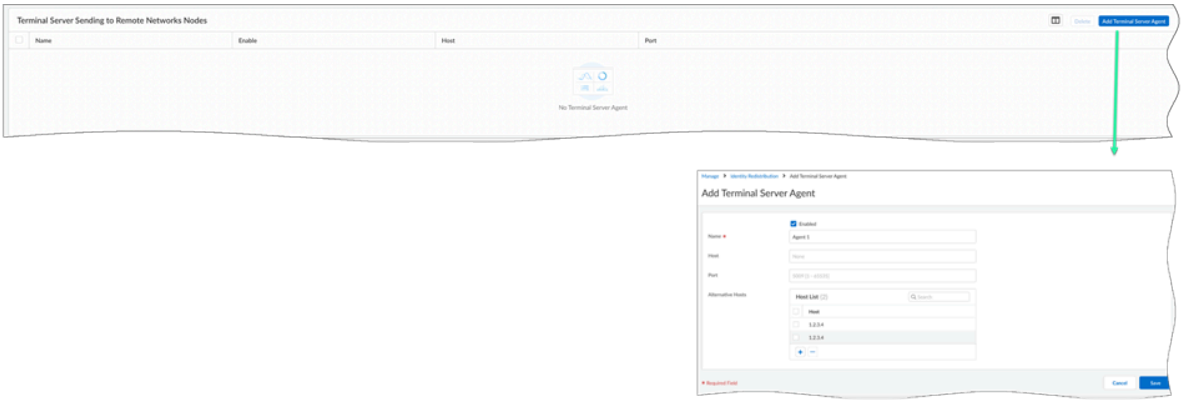


ターミナルサーバエージェントのユーザーマッピングの設定

Windowsベースのターミナル サーバー上の特定のユーザーを識別するため、ターミナルサーバー(TS)エージェントは各ユーザーにポート範囲を割り当てます。TSエージェントは、割り当てられたポート範囲をPrisma Accessに通知するため、Prisma Accessはユーザーとユーザーグループに基づいてポリシーを適用できます。

[ID再配信]ダッシュボードで、構成範囲をリモートネットワークに設定し、「ターミナルサーバーからリモートネットワークノードへの送信」の「ターミナルサーバーエージェント」を追加します。

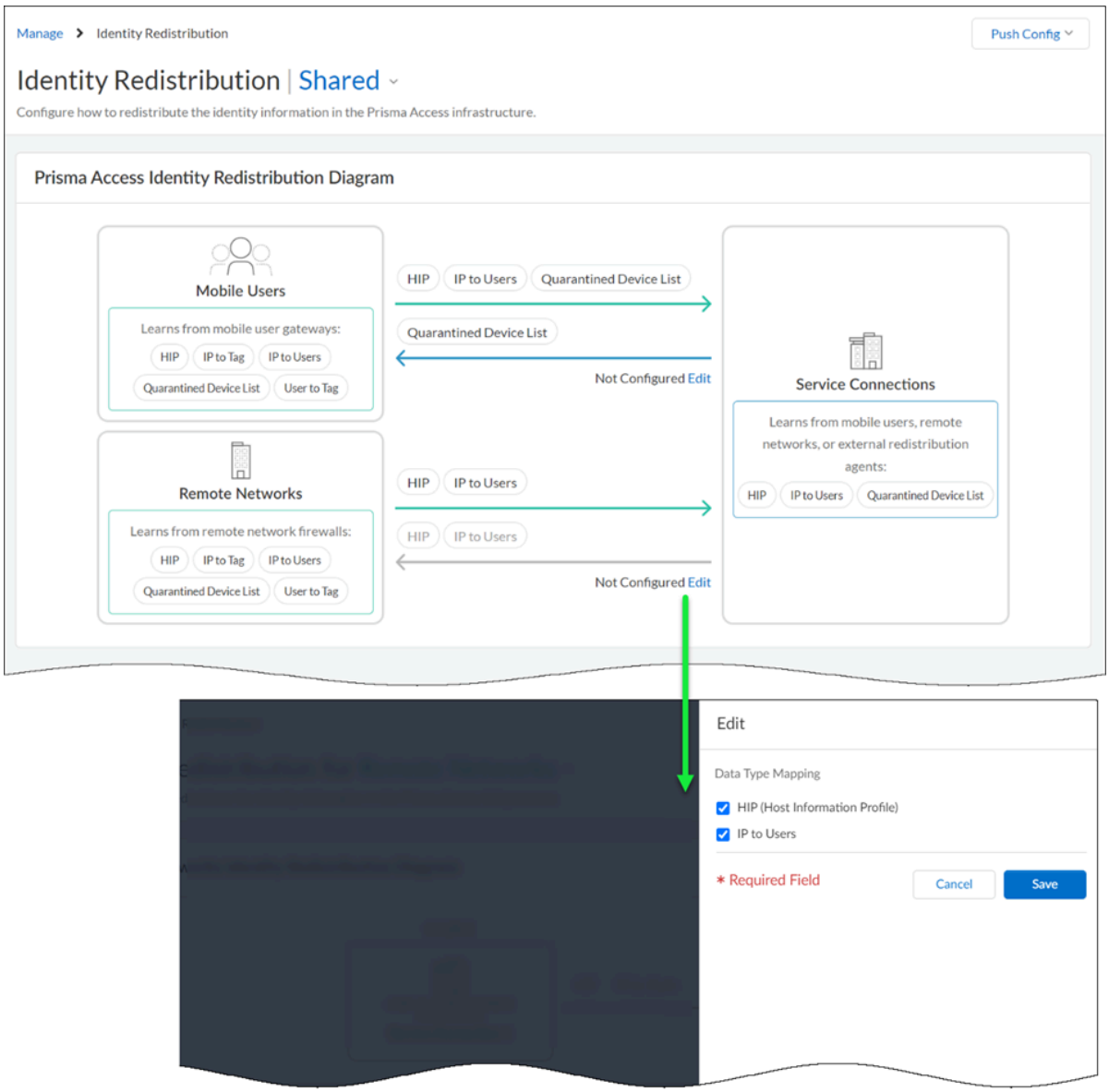
- デフォルトでは、設定は有効になっています。
- TSエージェントの名前を入力します。
- TSエージェントがインストールされているWindowsホストのIPアドレスを入力します。
- エージェントがユーザーマッピング要求をリッスンするポート番号を入力します。ポートはデフォルトで5009に設定されています。
- 変更を保存します。



 ©2025 Palo Alto Networks, Inc.

Prisma Access環境全体にIDデータを配信

[Identity Redistribution(ID再配信)]ダッシュボードで、図を編集して、各送信元から収集し、Prisma Access全体で共有するIDデータを指定します。



変更を有効にするには、Prisma Accessに設定をプッシュします。

アイデンティティ情報再配信 (Panorama)

User-IDを構成した後、IPアドレス - ユーザー名間マッピングをPrisma Accessから、ネットワーク リソースへのアクセスを保護するすべての次世代ファイアウォールに再配信することで、すべてのモバイル ユーザーとリモートネットワーク ロケーションのユーザーに対して、ユーザーベースのポリシーを一貫して適用することができる。次のいずれかの方法を使用して、IPアドレスとユーザー名のマッピングをモバイル ユーザーおよびオンプレミスの次世代ファイアウォールからリモート ネットワーク内のユーザーに再配信します。その逆も同様です。

©2025 Palo Alto Networks, Inc.

- Prisma AccessからオンプレミスファイアウォールへのUser-ID情報の再配信
- オンプレミスのファイアウォールからPrisma AccessへのユーザーID情報の再配信

Prisma AccessからオンプレミスファイアウォールへのUser-ID情報の再配信

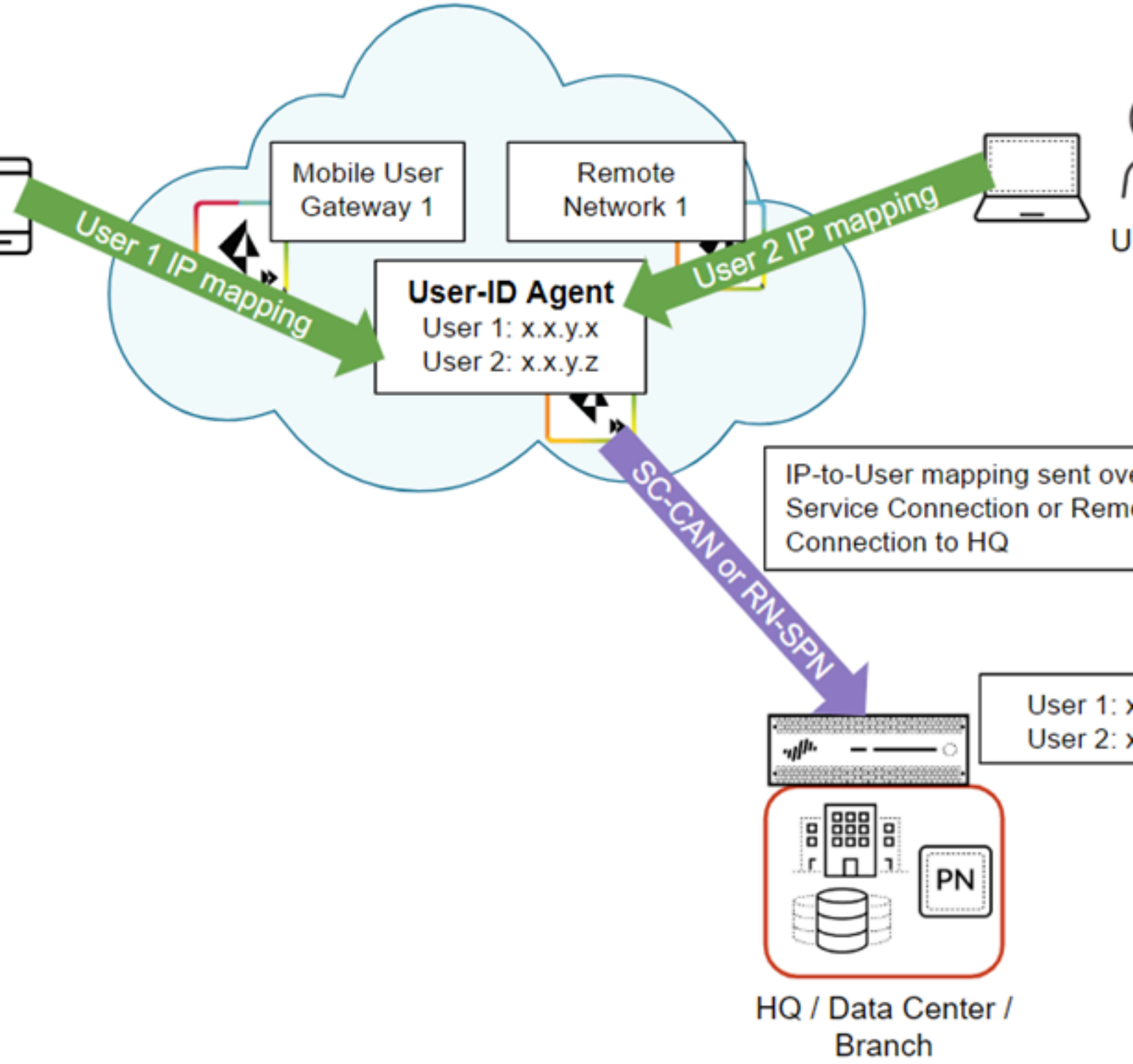
Prisma Accessからオンプレミスファイアウォールへの**User-ID**情報の再配信。

モバイル ユーザーがリモート ネットワーク ロケーションまたはHQ/データセンターのリソースにアクセスする必要があり、そのリソースがユーザー ベースのポリシーを持つオンプレミスの次世代ファイアウォールで保護されている場合、Prisma Accessモバイル ユーザーとリモート ネットワークのユーザーからオンプレミス ファイアウォールにIPアドレス - ユーザー名間マッピングを再配信する必要があります。ユーザーがPrisma Accessに接続すると、このユーザー対IPアドレスのマッピング情報が収集、保管されます。

次の図は、Prisma Accessに既存のIPアドレス - ユーザー名間マッピングを持つ2人のモバイル ユーザーを示 したものです。Prisma Accessはこのマッピングを、サービス接続（SC-CAN）またはリモート ネットワーク接続（RN-SPN）を使って、本社/データセンターを保護するオンプレミス ファイアウォールに再配信します。

*Prisma Access*は、サービス接続またはリモート ネットワーク接続を、レイヤ*3*ネットワークへのアンダーレイ パスとして機能する*IPSec*トンネルとして使用します。*IPSec*の信頼されたトンネルを経由する任意のルート パスを使用して、プライベートにアドレス指定された宛先に対して、このマッピングを再配信できます。

 ©2025 Palo Alto Networks, Inc.



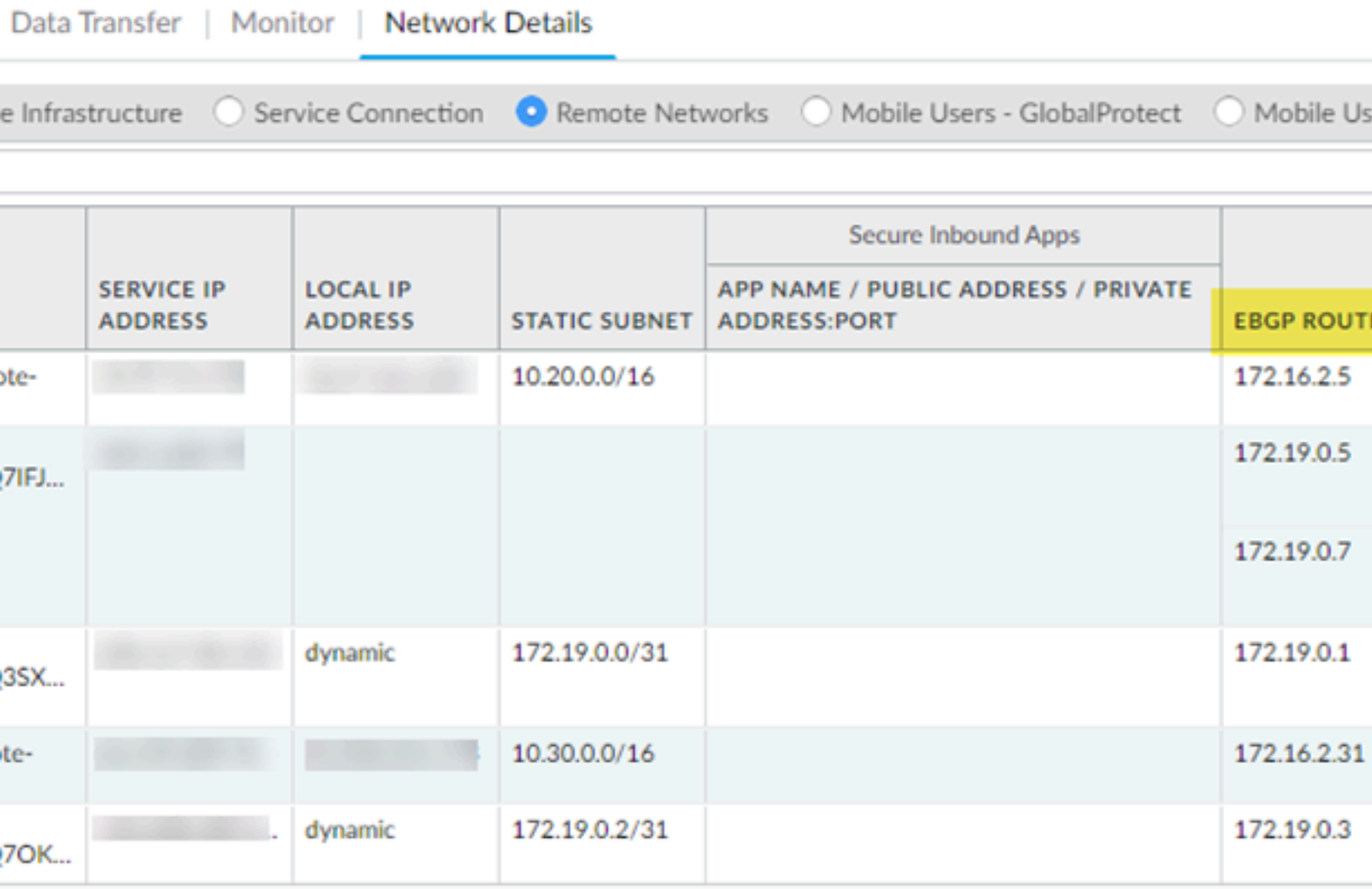
Prisma Accessからオンプレミスファイアウォールに User-IDマッピングを再配布するには、次の手順を実行してください。

©2025 Palo Alto Networks, Inc.

再配信パスにあるファイアウォールを含め、オンプレミス ファイアウォール *(SC-CAN* または *RN-SPN)* にユーザー*ID*を再配信する接続に*SSL*暗号化解除を適用しないようにしてください。あるいは、再配信トラフィックに復号化除外を適用することもできます。

STEP 1 | データ再配信エージェントを構成するときに使用する IP アドレスを忘れずにメモしてください。

- リモートネットワーク接続の場合は、 **EBGP**ルーター アドレスを見つけてください。 **(Panorama > Cloud Services (**クラウドサービス**) > Status (**ステータス**) > Network Details (**ネットワークの詳細**) > Remote Networks (**リモートネットワーク**) > EBGP Router (EBGP**ルーター**))**。



- サービス接続の場合は、 **User-ID** エージェントのアドレスを見つけます **([Panorama] > [Cloud Services (**クラウドサービス**)] > [Status (**ステータス**)] > [Network Details (**ネット

 ©2025 Palo Alto Networks, Inc.

ワークの詳細)] > [Service Connection (サービス接続)] > [User-ID Agent Address (User-ID エージェントのアドレス)])。

本社またはデータセンターのサービス接続をまだ設定していない場合は、サービス接続の構成から始め てください。Prisma Accessはサービス接続を使用して環境全体でIDデータを共有し、Prisma Accessは自動的にサービス接続を再分配エージェントとして機能させます。新規作成したサービスコネクションサイトにユーザー ID エージェント アドレスが割り当てられていることが確認できたら、このサイトを再配信エージェントとして使用できます。Prisma Accessではこの処理が自動的に行われ、数分かかります。

ユーザー*ID*の再ディストリビューション管理- 特に大規模な*Prisma Access*のデプロイメントでは、ユーザー*ID*の再ディストリビューションに対してきめ細かい制御が必要になる場合があります。ユーザー*ID*再ディストリビューション管理を使用すると、 ユーザー *ID*列のチェック マークを削除して特定のサービス接続のデフォルトの*ID*再ディストリビューション動作を手動で無効にし、*ID*再ディストリビューションに使用する特定のサービス接続を選択できます。ほとんどの構成ではこれを行う必要はありません。この機能を有効にするには、*Palo Alto Networks*サポートにお問い合わせください。

Data Transfer | Monitor | Network Details

ce Infrastructure | Service Connection | Remote Networks | Mobile Users - GlobalProtect | Mobile Use

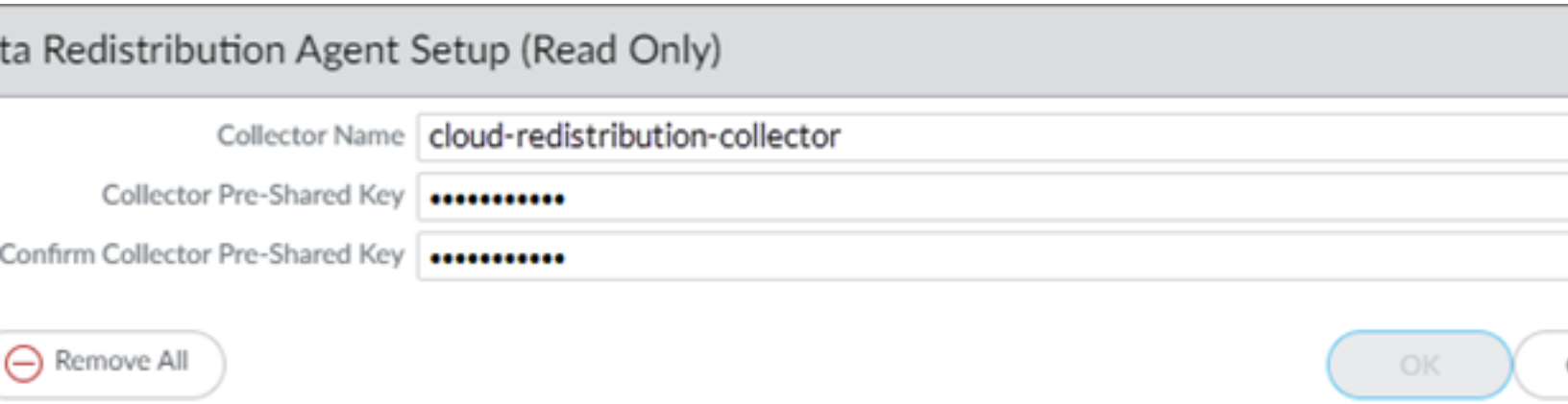
	SERVICE IP ADDRESS	USER-ID AGENT ADDRESS	LOCAL IP ADDRESS	STATIC SUBNET	EBGP ROUTER
	[redacted]	172.16.2.9	[redacted]	10.10.0.0/16	172.16.0.9
DC2	[redacted]	172.16.2.2	[redacted]	192.168.203.0/24 192.168.200.0/24 192.168.201.0/24	172.16.2.2
DC1	[redacted]	172.16.2.3	[redacted]	192.168.100.0/24 192.168.101.0/24 192.168.103.0/24	172.16.2.3

©2025 Palo Alto Networks, Inc.

STEP 2 | Prisma Accessを、ユーザーマッピング情報を再配信するUser-IDエージェントとして設定します。

1. Prisma Accessを管理するPanoramaで、**[Device (デバイス)]** > **[Data Redistribution (データ再配信)]** > **[Collector Settings (コレクター設定)]**を選択します。

   サービス接続でコレクターを構成するには、 **Service_Conn_Template**;リモートネットワーク接続でコレクターを設定するには、 **Remote_Network_Template**を選択します。
2. 設定を編集するには、歯車型アイコンをクリックします。
3. **Collector Name**（コレクタ名）と**Collector Pre-Shared Key**（IDコレクタ事前共有鍵）を指定して、Prisma AccessをUser-IDエージェントに設定します。
4. **OK** をクリックして変更内容を保存します。

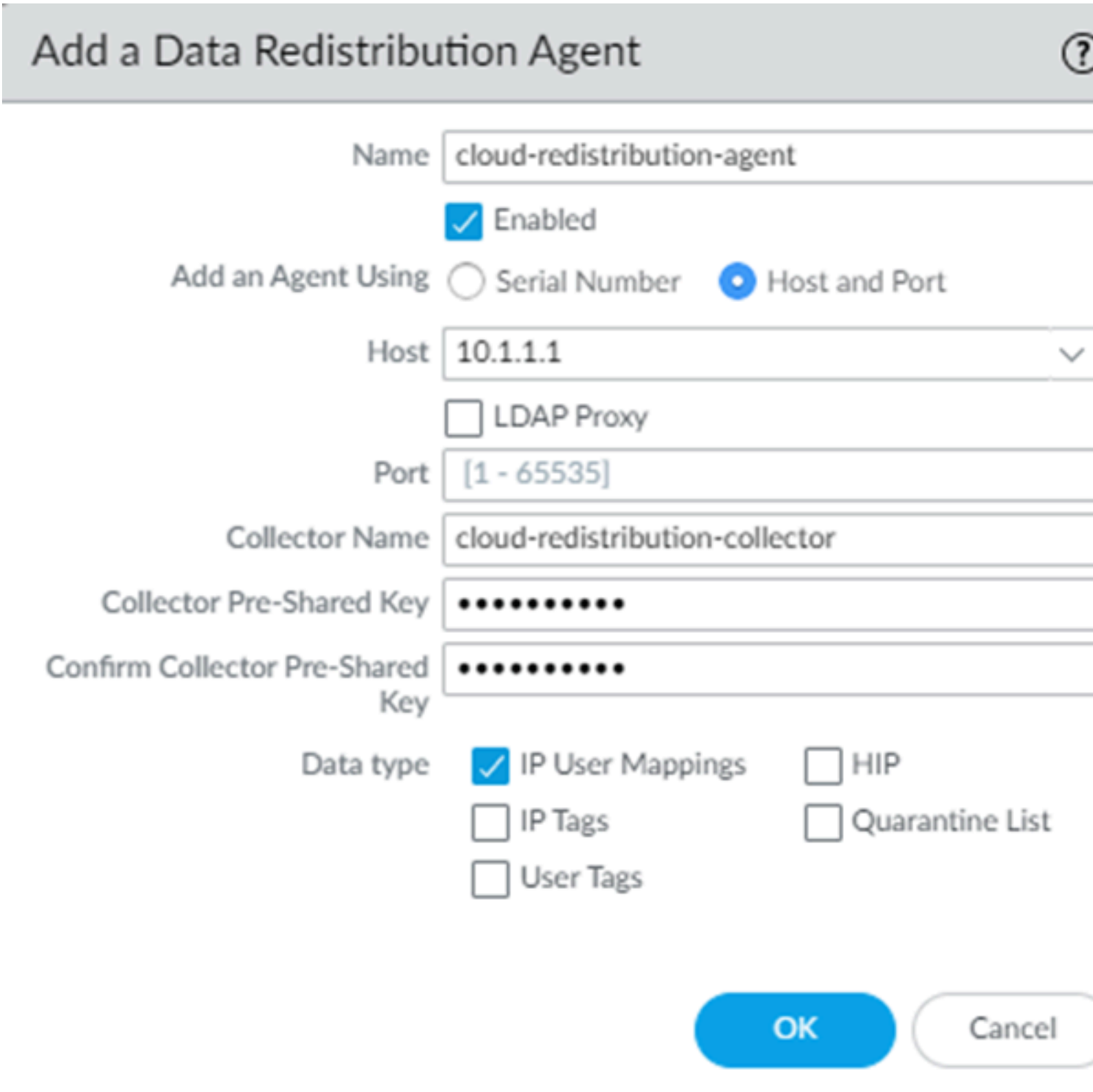


 ©2025 Palo Alto Networks, Inc.

STEP 3 | Prisma AccessからUser-IDマッピングを収集するように、オンプレミスファイアウォールを設定します。

1. オンプレミスのファイアウォールから、 **[Device (デバイス)]** > **[Data Redistribution (データの再配布)]** > **[Agents (エージェント)]**を選択します。
2. User-IDエージェントを**Add**（追加）して、それに**Name**（名前）を指定します。
3. **Host and Port**（ホストおよびポート）を選択します。
4. **Host (ホスト)**欄に、Prisma Accessから **User-ID Agent Address (User-IDエージェントアドレス)**（サービス接続の場合）または **EBGP Router Address (EBGPルータアドレス)**（リモート・ネットワーク接続の場合）を入力します。
5. 先の手順で作成したPrisma Accessコレクタの、**Collector Name**（コレクタ名）および**Collector Pre-Shared Key**（コレクタ事前共有鍵）を入力します。
6. **IP User Mappings**（**IP** ユーザー マッピング）を選択します。
7. **OK** をクリックします。
8. マッピングを再配信するサービス接続またはリモートネットワーク接続ごとに、これらの手順を繰り返します。

©2025 Palo Alto Networks, Inc.



オンプレミスのファイアウォールからPrisma AccessへのユーザーID情報の再配信

オンプレミス・ファイアウォールからPrisma AccessにユーザーID情報を再配信します。

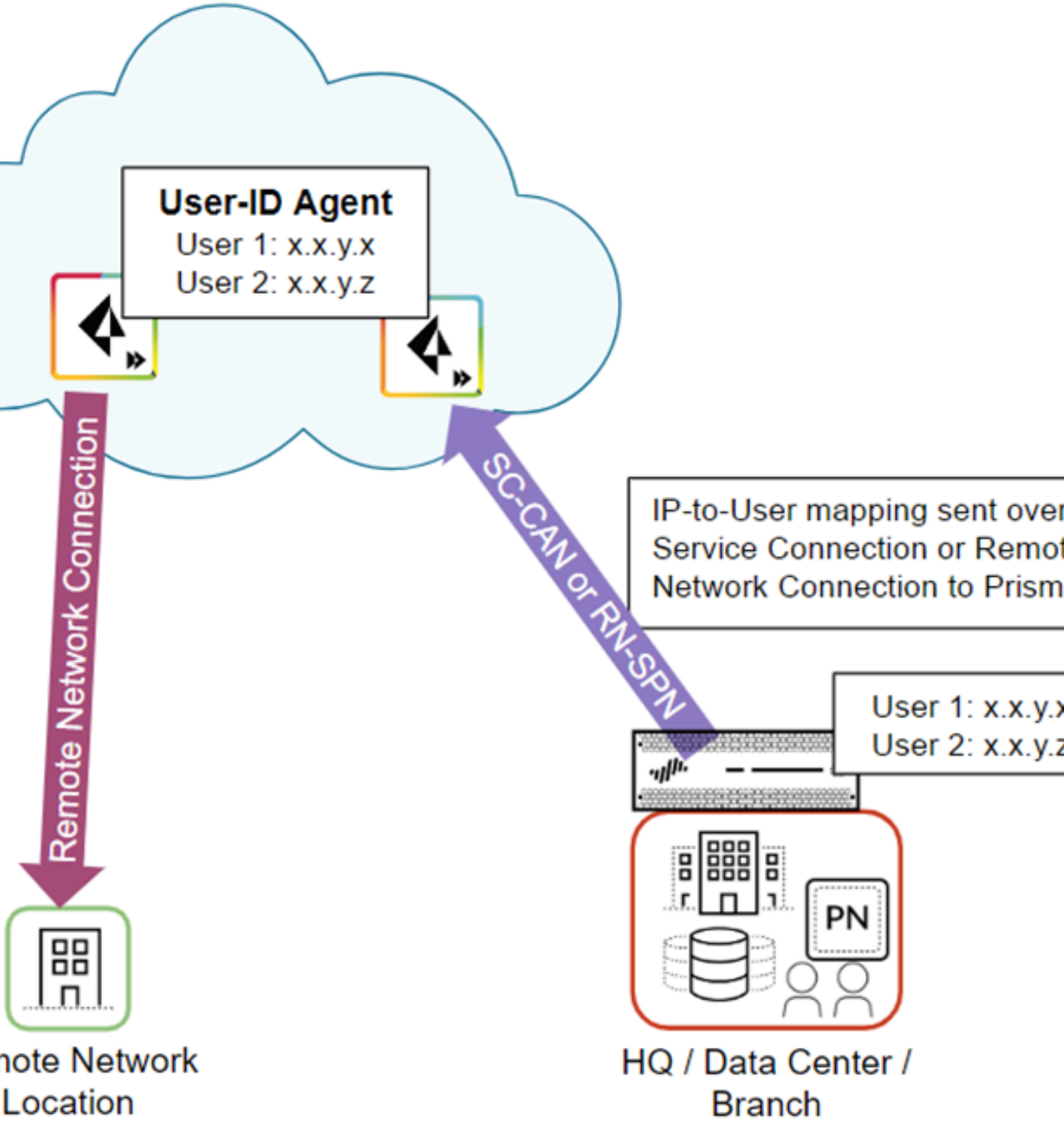
©2025 Palo Alto Networks, Inc.

ユーザーベースのポリシーで次世代オンプレミスファイアウォールに保護されている支店または本社にユーザーが存在しており、そのユーザーがPrisma Accessで保護されている他の支店のリソースにアクセスする必要がある場合、オンプレミスファイアウォールからPrisma AccessにIP address-to-user nameマッピングを再配信します。

次の図は、既存のIPアドレス - ユーザー名間マッピングを持つオンプレミスの次世代ファイアウォールを備えた本社/データセンターを示したものです。 Prisma Accessはサービス接続（SC-CAN）またはリモートネットワーク接続（RN-SPN）でファイアウォールに接続し、オンプレミスのファイアウォールはマッピングをPrisma Accessに再配信します。

以下の図は、Prisma Accessサービス接続またはリモート ネットワーク接続がマッピングの再配信に使用されて いる様子を示したものです。IPSecの信頼されたトンネルを経由する任意のルート パスを使用して、プライベートにアドレス指定された宛先に対して、このマッピングを再配信できます。

©2025 Palo Alto Networks, Inc.



©2025 Palo Alto Networks, Inc.

オンプレミス ファイアウォールからPrisma Accessにユーザー IDマッピングを再配信するには、以下の手順を実行します。

STEP 1 | Prisma AccessにUser-ID情報を再配信するように、オンプレミスファイアウォールを設定します。

1. オンプレミスのファイアウォールから、**[Device (デバイス)]** > **[Data Redistribution (データの再配布)]** > **[Collector Settings (コレクタ設定)]**を選択します。
2. 設定を編集するには、歯車型アイコンをクリックします。
3. **Collector Name**（コレクタ名）と**Collector Pre-Shared Key**（コレクタ事前共有鍵）を指定して、オンプレミスファイアウォールをUser-IDエージェントに設定します。
4. **OK** をクリックして変更内容を保存します。

STEP 2 | オンプレミス ファイアウォールからユーザー IDマッピングを収集するようにPrisma Accessを構成します。

1. Prisma Accessを管理するPanoramaから、**[Device (デバイス)]** > **[Data Redistribution (データ再配信)]** > **[Agents (エージェント)]** を選択します。

   ページ上部の**[テンプレート]**ドロップダウンで、**[Service_Conn_Template]**(サービス接続用)または**[Remote_Network_Template]**(リモートネットワーク接続用)が選択されていることを確認してください。
2. User-IDエージェントを**Add**（追加）して、それに**Name**（名前）を指定します。
3. **Host and Port**（ホストおよびポート）を選択します。
4. ファイアウォールが**Host**（ホスト）内のユーザーマッピングの送信に使用する、MGTインターフェイスのIPアドレスまたはサービスルートを入力します。

   MGT インターフェイスの場合は IP アドレスの代わりにホスト名を入力できます。
5. ステップ1で作成したオンプレミス ファイアウォール用コレクタの値を使って、**Collector Name**（コレクタ名）および**UCollector Pre-Shared Key**（コレクタ事前共有鍵）を入力します。
6. **IP User Mappings**（**IP** ユーザー マッピング）を選択します。
7. **OK** をクリックします。

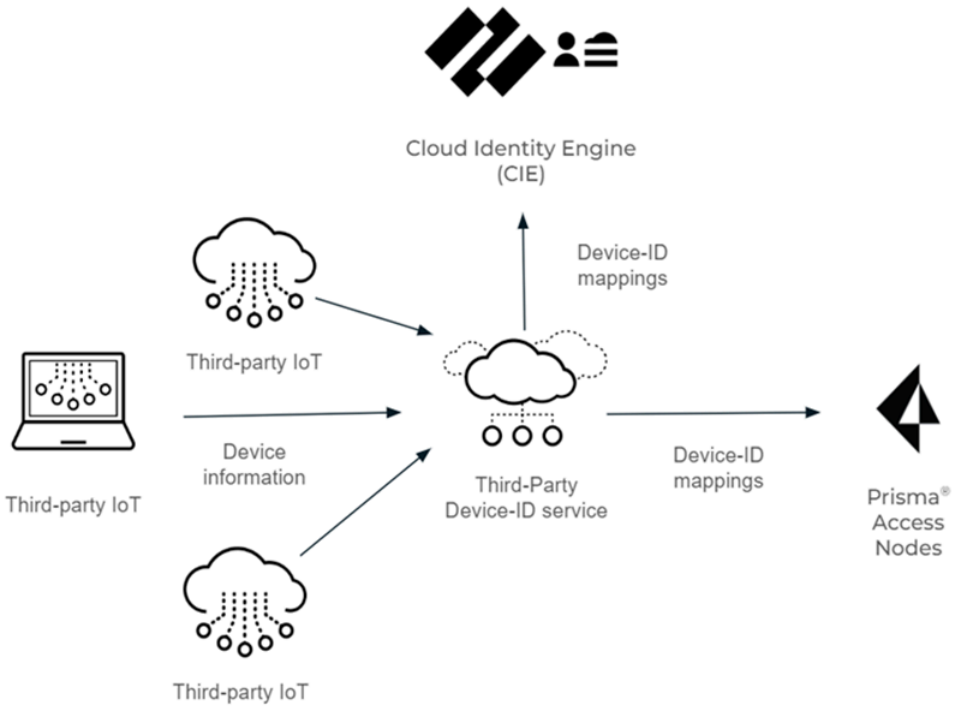
©2025 Palo Alto Networks, Inc.

Prisma Accessでサードパーティ デバイスIDを設定する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) この機能をPrisma Access環境で使用したい場合は、アカウントチームにお問い合わせください。	❑ Cloud Identity Engine機能を有効にしたPrisma Accessライセンス

Prisma Accessと共にCloud Identity Engineを使用して、サードパーティのIoT検出ソー スからの情報を適用し、ネットワーク内のデバイスのセキュリティ ギャップを特定し、 解決する作業を簡素化できる。API を使用してCloud Identity EngineでThird-Party Device-IDをセットアップした後、 Prisma Accessでデバイスオブジェクトとセキュリティ ポリシー ルールをセットアップして、Cloud Identity Engineを通じてサードパーティのIoT可視化ソリューションから情報を取得し、使用してデバイスの可視化と制御を行うことができます。

下図では、Third-Party Device-ID (サードパーティ デバイスID) サービスがサード パーティのIoTソリューションからデバイ ス情報を受信し、IPアドレスからデバイスへのマッピングとしてクラウドIDエンジンとPrisma Accessセキュリティ処理ノード（SPN）に送信します。



- Strata Cloud Manager

©2025 Palo Alto Networks, Inc.

- Panorama

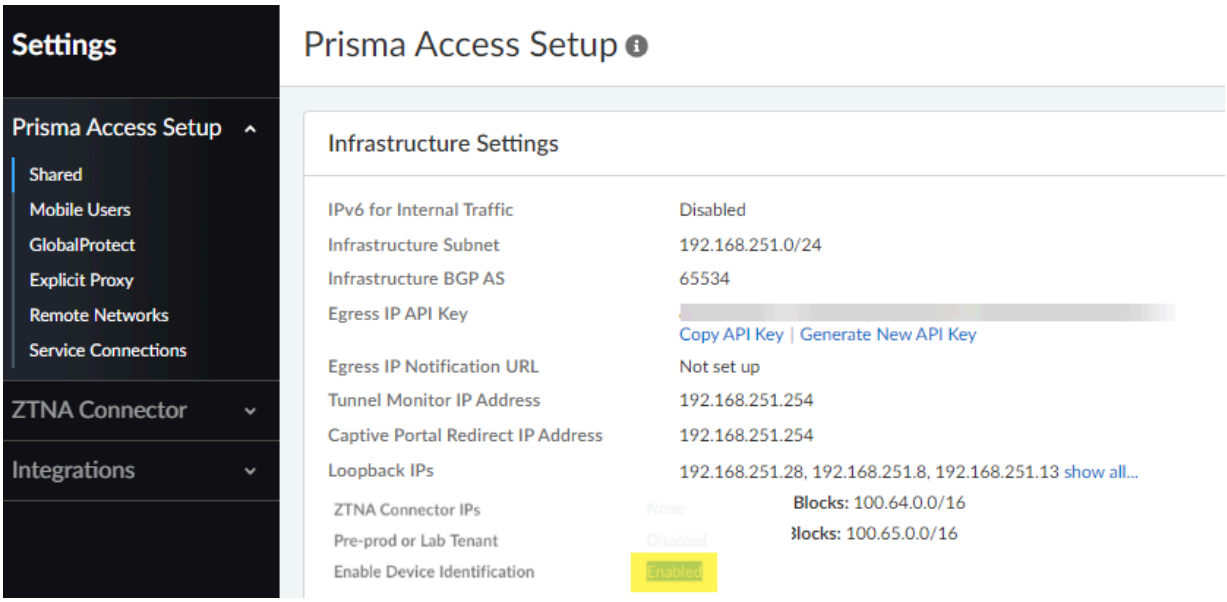
Prisma Accessでサードパーティ デバイスIDを設定する （Strata Cloud Manager）

サードパーティのデバイスIDを構成するには、次のタスクを完了します。

STEP 1 | クラウド ID エンジンでサードパーティ Device-ID をアクティブ化します。

この手順には、署名された証明書をアップロードし、それを API で使用してサードパーティのIoTベンダーと通信し、デバイスID情報をダウンロードすることが含まれます。

STEP 2 | **[Settings (設定)] > [Prisma AccessSetup (セットアップ)] > [Shared (共有)]**または**[Workflows (ワークフロー)] > [Prisma Access Setup (セットアップ)] > Prisma Access**を開き、**[Enable Device Identification (デバイス識別を有効にする)]**を**[Enabled (有効)]**に設定して、Prisma Accessでサードパーティ デバイスIDを有効にします。



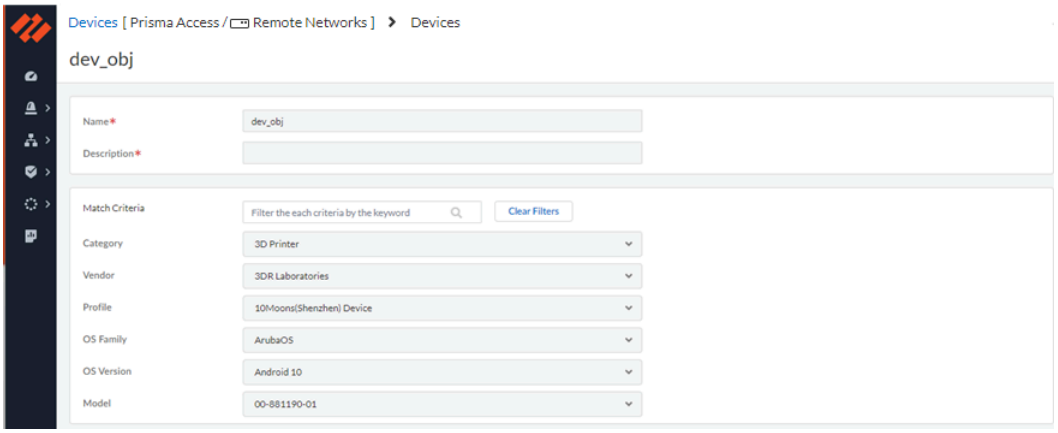
STEP 3 | デバイス オブジェクトを設定し、デバイス属性を入力します。**[Manage (管理)] > Configuration (設定) > (NGFW**と**Prisma Access)**、 [configuration scope (設定範囲)]を**[**リモー

 ©2025 Palo Alto Networks, Inc.

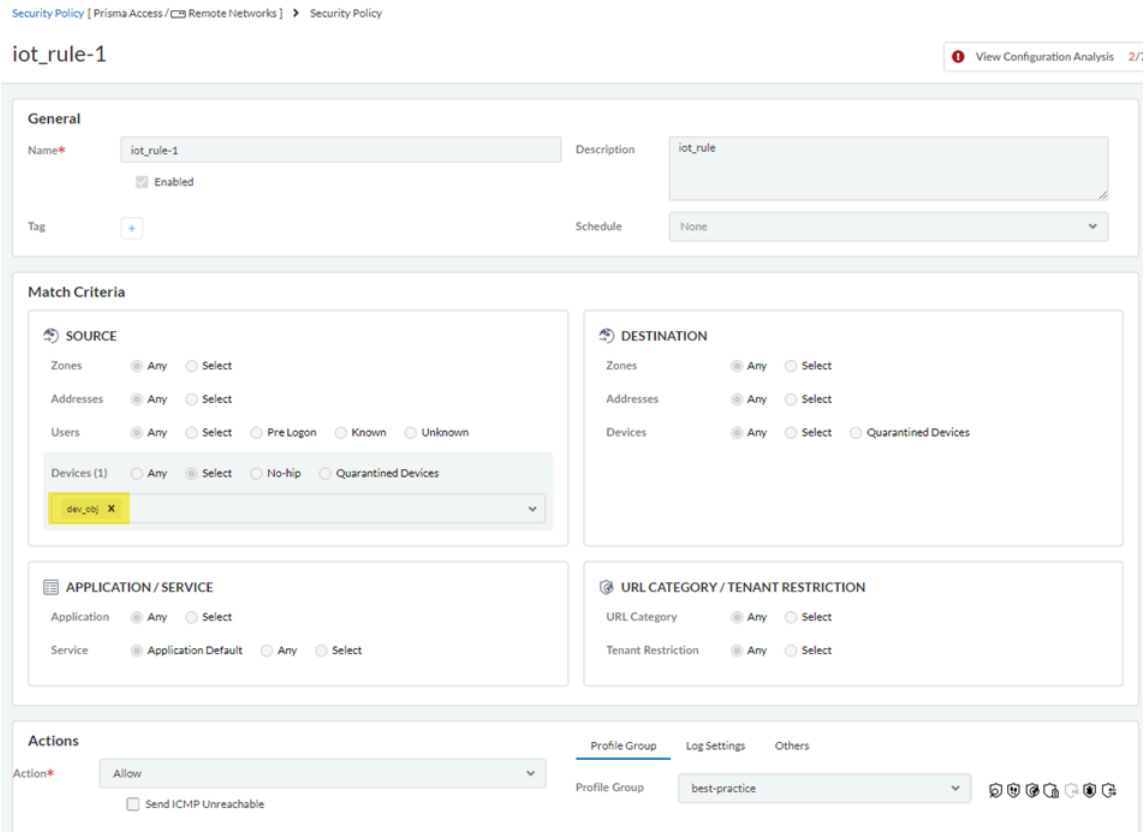
ト ネットワーク]に設定し、[オブジェクト] > [デバイス][デバイスの追加]の順に選択します。リモート ネットワーク デバイス グループに属していることを確認してください。

1. サードパーティ オブジェクトの属性に一致するデバイス オブジェクトを追加します。

   Cloud Identity Engine マッピング 領域にはサードパーティ デバイスの属性が表示され、そこから取得した任意の属性を使用できます。



STEP 4 | **[Manage (管理)] > [Configuration (設定)] > [NGFW and Prisma Access]**に移動し、[設定範囲]を[リモート ネットワーク]に設定し、[セキュリティ サービス] > [セキュリティ ポリシー]を選択します。セキュリティポリシーを追加し、デバイス 領域に作成したデバイスオブジェクトを追加します。

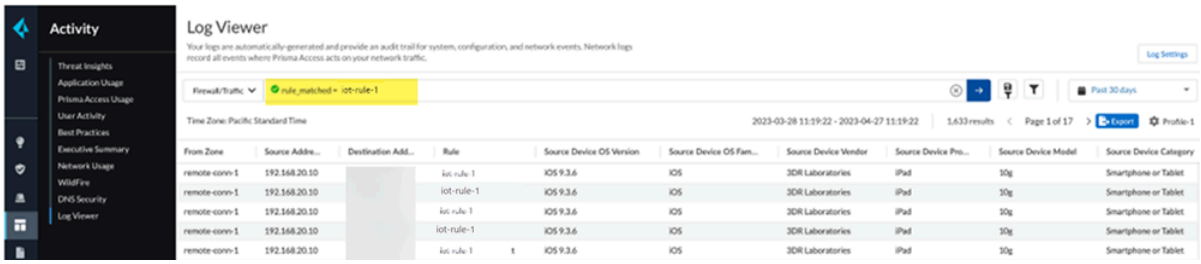


 ©2025 Palo Alto Networks, Inc.

STEP 5 | プッシュ スコープで**Remote Networks**（リモート ネットワーク）を選択していることを確認して、**[Push Config (設定をプッシュ)]**を実施して、Prisma Access設定に変更を保存します。

STEP 6 | **[Incidents & Alerts]** > **[Log Viewer]**で**[Firewall/Traffic]**を選択し、`[rule_matched = rulename]`（*[rulename]*はサードパーティ製IoTデバイス用に作成したセキュリティポリシールール）と入力して作成したルールの下でトラフィックを検索して、Prisma AccessがDevice-ID ログを受信していることを確認します。ここで*[rulename]*は、サードパーティ製IoTデバイス用に作成したセキュリティ ポリシー ルールです。

デバイスIDとIPアドレスのマッピングがログに表示されます。



Prisma Accessでサードパーティ デバイスIDを設定する（Panorama）

サードパーティのデバイスIDを構成するには、次のタスクを完了します。

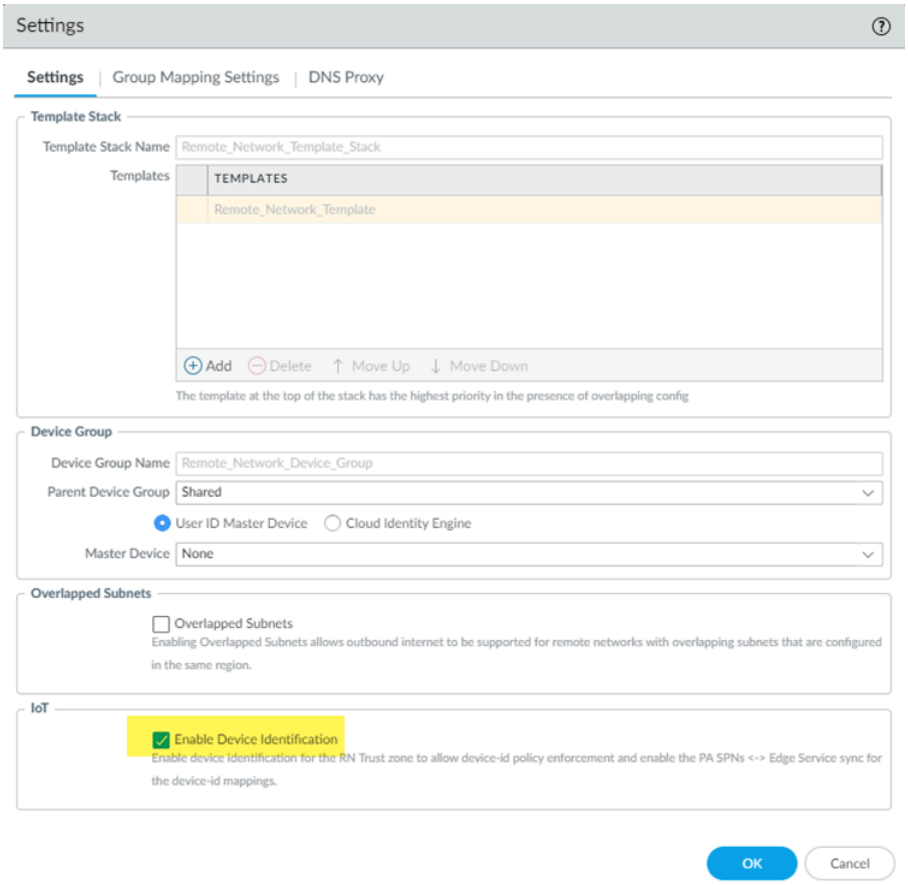
STEP 1 | クラウド ID エンジンでサードパーティ Device-ID をアクティベートします。

この手順には、署名された証明書をアップロードし、それを API で使用してサードパーティのIoTベンダーと通信し、デバイスID情報をダウンロードすることが含まれます。

STEP 2 | **[Panorama]** > **[Cloud Services (クラウドサービス)]** > **[Configuration (設定)]** > **[Remote Networks (リモートネットワーク)]** > **[Settings (設定)]**に進み、歯車をクリックして設定を

 ©2025 Palo Alto Networks, Inc.

編集し、**[Enable Device Identification**（デバイス識別を有効にする）**]**を選択して、Prisma Accessでサードパーティデバイス ID を有効にします。



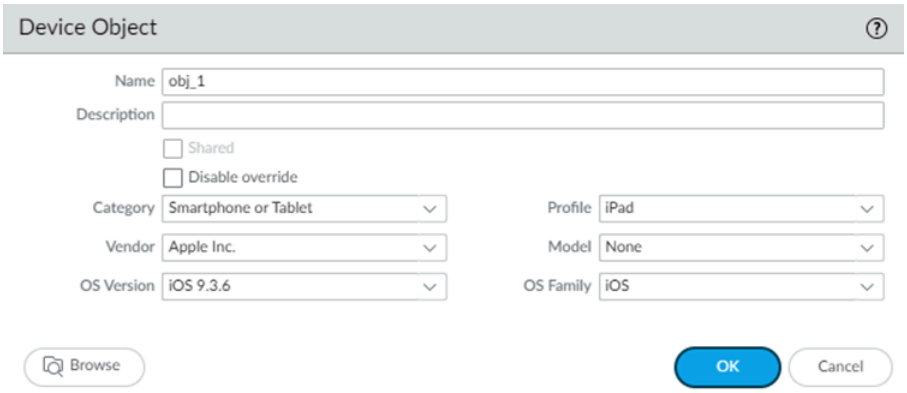
©2025 Palo Alto Networks, Inc.

STEP 3 | デバイス オブジェクトを設定し、デバイス属性を入力します。

1. [オブジェクト] > [デバイス] に移動し、すべてのデバイス ID 属性に一致するデバイス オブジェクトを追加します 。

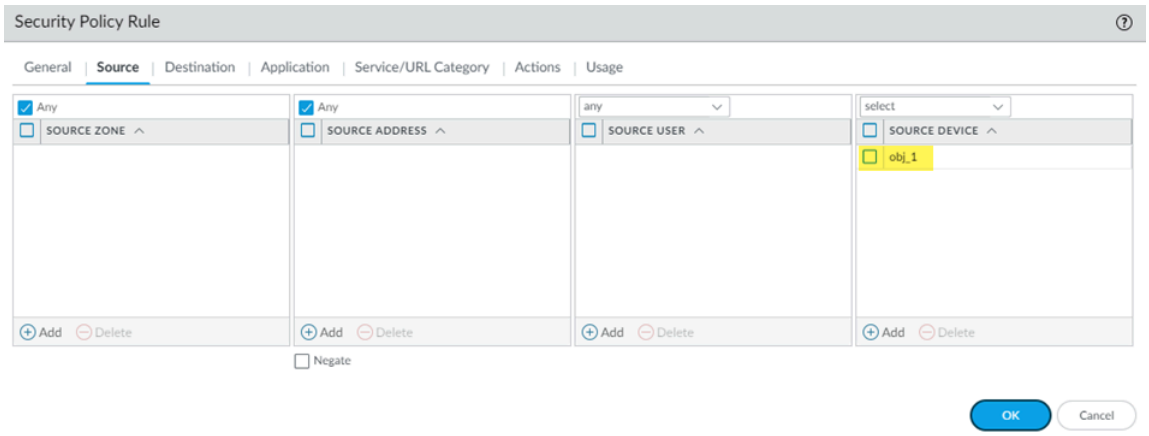
   Remote_Network_Device_Group または **Shared (**共有**)** デバイス グループに属していることを確認してください。
2. サードパーティ オブジェクトの属性に一致するデバイス オブジェクトを追加します。

   Cloud Identity Engine マッピング 領域にはサードパーティ デバイスの属性が表示され、そこから取得した任意の属性を使用できます。



STEP 4 | [ポリシー] > [セキュリティ] > [事前ルール] に移動して、セキュリティ ポリシーを追加し、[デバイス] 領域で作成したデバイス オブジェクトを 送信元デバイスとして追加します。

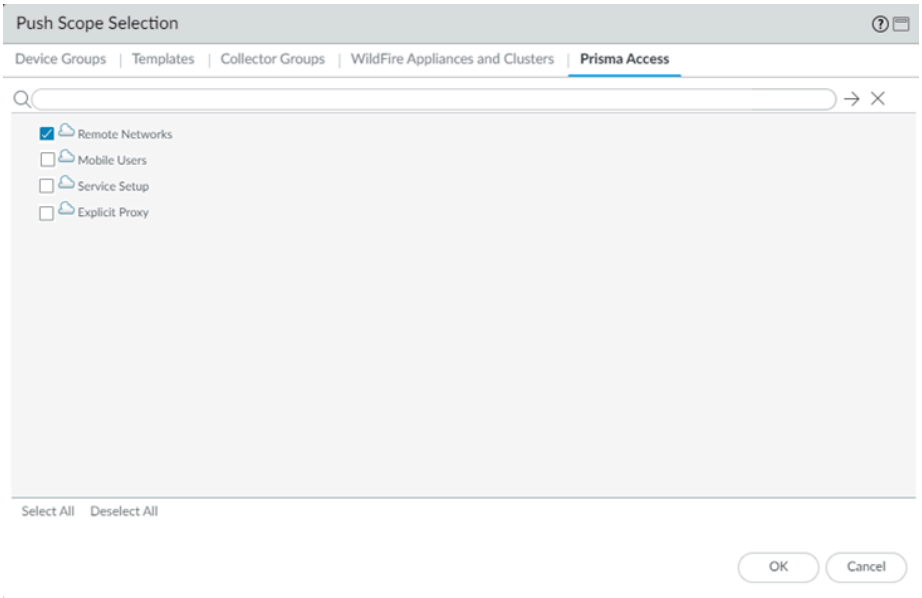
Remote_Network_Device_Group または **Shared (**共有**)** デバイス グループに属していることを確認してください。



 ©2025 Palo Alto Networks, Inc.

STEP 5 | 変更をコミットしてプッシュし、**[Push Scope (プッシュ スコープ)]**で **[Remote Networks (リモート ネットワーク)]** が選択されていることを確認します。

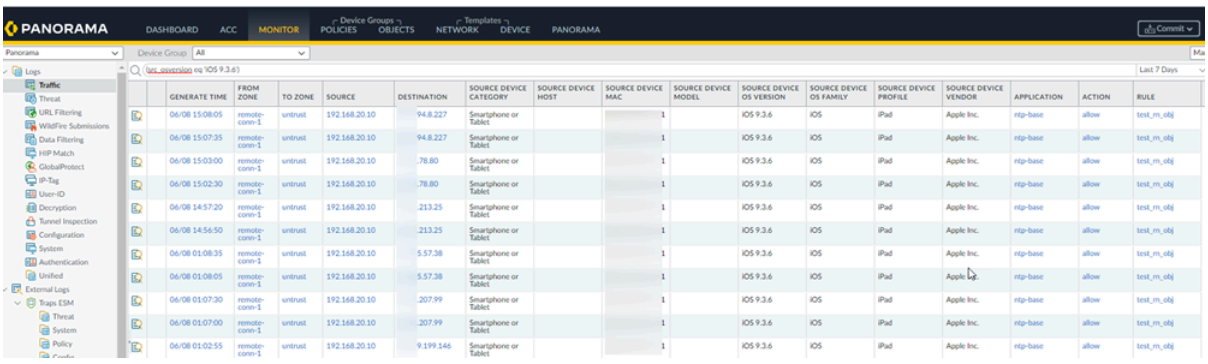
1. **Commit**（コミット） > **Commit and Push**（コミットしてプッシュ）をクリックします。
2. [選択内容を編集]をクリックし、**[Prisma Access]**タブで**[Push Scope (スコープをプッシュ)]**に[リモートネットワーク]が選択されていることを確認し、**[OK]**をクリックする。



3. **[Commit and Push (コミットしてプッシュ)]** をクリックします。

STEP 6 | Prisma Access が「Device-ID ログ」を受信していることを確認するには、**[Monitor (監視)]** > **[Logs (ログ)]**に進み、**[Traffic (トラフィック)]** logsに`rule_matched = rulename`（*[rulename]*はサードパーティ製 IoT デバイス用に作成したセキュリティ ポリシー ルール）と入力して、作成したルールの下でトラフィックを検索する。

デバイスIDとIPアドレスのマッピングがログに表示されます。



 ©2025 Palo Alto Networks, Inc.

サードパーティのデバイス ID API

Cloud Identity Engine ユーザーインターフェースを使用してサードパーティのデバイス ID サービスにオンボーディングすると、これらの API を使用して、ネットワークで検出され、サードパーティのデバイス IDサービスに保存された判定、つまり IP アドレスとデバイスのマッピングを管理できます。これらのマッピングは、どの属性が特定の IP アドレスを持つデバイスに属するかをPrisma Accessに伝え、特定の属性を持つデバイスをターゲットとするセキュリティ ポリシーを定義できるようにします。

これらの API は、Cloud Identity Engine テナントに保存されているデータに直接アクセスしません。むしろ、API はサードパーティのデバイス ID サービスの IP アドレスとデバイスのマッピングと相互作用し、これらのマッピングは Cloud Identity Engine と共有されます。

サードパーティデバイス ID API は、証明書、API キー、および API リクエストのベース URL を使用します。サードパーティのデバイス ID API リクエストを認証するには、Cloud Identity Engine ユーザーインターフェイスでのオンボーディング中に取得した署名付き証明書と API トークンを使用する必要があります。

証明書と API キーがあれば、サードパーティのデバイス ID サービスに対してリクエストを行うことができます。証明書とその公開鍵、API キー、およびベース URL を各リクエストで提供します。例:

```
curl --cert onida1.crt --key onida.key "https://device-identity-
broker-beta.service-edge.panservicetest.com/:443/api/v1/token/
{apiKey}/verdicts"
```


- 判決の更新
- すべての判定を削除する
- クエリ評決
- IPアドレスによるクエリ判定
- クエリ判定統計

判決の更新

IPアドレスとデバイスのマッピングを追加、変更、または削除します。

概要

URI	`/api/v1/token/{apiKey}/verdicts:update`
HTTP 方式	POST

詳説

サードパーティ デバイスIDは、ネットワーク内のサードパーティのIoT検出ソースからデータを取り込み、Prisma Accessがデバイス固有のセキュリティ ポリシー ルールを適用するために使用

 ©2025 Palo Alto Networks, Inc.

できるIPアドレスとデバイスのマッピングを作成します。このAPIを使用して、新しいマッピングを追加したり、既存のマッピングを変更したり、マッピングを削除したりします。

マッピングを追加または変更するには更新フィールドを使用し、マッピングを削除するには削除フィールドを使用します。

マッピングがすでに存在する場合、更新によりリクエスト本文で指定された属性で既存のデバイス属性が上書きされます。マッピングが存在しない場合は、更新によって新しいマッピングが作成されます。

このAPIは部分的な更新をサポートしていません。マッピングの特定の属性を更新する場合は、更新したくない属性の以前の値も再入力する必要があります。属性を空白のままにすると、既存の値が消去されます。

一度に最大10,000個のマッピングを更新または削除できます。要求はアトミックです。つまり、成功した応答はシステムがすべてを処理したことを意味し、失敗した応答はシステムが何も処理しなかったことを意味します。

項目

項目	詳説
更新	更新または作成するIPアドレスとデバイスのマッピングの属性を提供するJSONオブジェクト。ipと少なくとも1つの他の属性を入力する必要があります。
消去	削除するマッピングのIPアドレスを指定するJSONオブジェクト。

以下に例を示します。

```
{ "update": [ { "ip": "string", "serialNo": "string", "mac":
 "string", "category": "string", "vendor": "string", "model":
 "string", "os": "string", "osFamily": "string", "hostname":
 "string", "profile": "string", } ], "delete": [ { ip: "string" } ] }
```

成功応答

成功すると、HTTP応答コードは200になります。さらに、応答には、次のフィールドを持つJSONオブジェクトが含まれています。

項目	詳説
更新時間	リクエストが成功した時刻を表すUNIXタイムスタンプ。

以下に例を示します。

```
{ "updateTime": unix-timestamp }
```


©2025 Palo Alto Networks, Inc.

エラー応答

エラーが発生した場合、HTTP応答コードは次のいずれかになります。

応答コード	詳説
400	無効な要求です。要求が不完全または何らかの形で不正でした。再試行する前に要求を修正してください。
401	不正なトークン。APIトークンを再生成してみてください。それでも問題が解決しない場合は、サポートにお問い合わせください。
409	コンフリクト。別の更新ジョブまたは削除ジョブが実行中であるため、リクエストを処理できませんでした。他のジョブが終了した後に再試行してください。
429	要求が多すぎます。システムが特定の期間内に発行したリクエストが多すぎるため、リクエストを処理できませんでした。1秒あたりのリクエスト数を1回を超えないようにしてください。しばらく待ってからもう一度試してください。

さらに、応答ボディには次のフィールドが含まれます。

項目	詳説
コード	エラーコード。
メッセージ	エラーメッセージ。

オブジェクトの更新

IPアドレスとデバイスのマッピングを更新するために必要な情報を記します。この JSON オブジェクトには次のフィールドがあります。

項目	詳説
ip	デバイスのIPアドレス。
更新時間	マッピングが最後に更新された日時を表すUnixタイムスタンプ。
category	デバイス タイプ。例:プリンター
売り手	デバイス ベンダー。例:株式会社SHARP
model	デバイス モデル。例:MX-6070N

©2025 Palo Alto Networks, Inc.

os	デバイス オペレーティング システム。例:ThreadX 5
OSファミリー	デバイスのOSが属するファミリー。例:ThreadX RTOS
プロファイル	デバイス プロファイル例:シャーププリンター

すべての判定を削除する

サードパーティのデバイスIDサービスからすべてのIPアドレスとデバイスのマッピングを削除します。

概要

URI	/api/v1/token/{apiKey}/verdicts:all
HTTP 方式	削除

詳説

サードパーティのデバイスIDサービスに、サードパーティのデバイスIDサービス内のすべてのIPアドレスとデバイスのマッピングを削除するよう依頼します。正常な応答は、サービスがすべてのマッピングを削除したことを意味します。エラー応答はマッピングを削除できなかったことを意味します。

成功応答

成功すると、HTTP応答コードは200になります。応答ボディは空です。

エラー応答

エラーの場合、HTTP応答コードは次のいずれかになります。

応答コード	詳説
401	不正なトークン。APIトークンを再生成してみてください。それでも解決しない場合は、サポートに連絡してください。
409	コンフリクト。別の進行中の更新または削除ジョブがあるため、システムはリクエストを処理できませんでした。他のジョブが終了した後に再試行してください。
429	リクエストが多すぎます。システムが特定の時間内に大量のリクエストを発行したため、システムはリクエストを処理できませんでした。1秒間に複数のリクエストを処理しないようにしてください。しばらく待ってからもう一度試してください。

©2025 Palo Alto Networks, Inc.

さらに、応答ボディには次のフィールドが含まれます。

項目	詳説
コード	エラーコード。
メッセージ	エラーメッセージ。

クエリ評決

サードパーティのデバイスIDサービス内のIPアドレスとデバイスのマッピングを取得します。

概要

URI	/api/v1/token/{apiKey}/verdicts? bookmark={STRING}&pageLen={INTEGER}
HTTP 方式	開始

詳説

すべてのマッピングまたはサブセットのいずれかを返します。

すべてのマッピングを返すには、パラメータを指定せずに要求を一度送信します。レスポンスの`nextBookmark`の値をメモしておきます。URIに追加されたブックマークに対して、その値を使用して別の要求を送信します。呼び出し元は、すべてのマッピングを返したことを示す応答でカウントが空になるまでクエリを繰り返します。

マッピングのサブセットを返すには、pageLen を使用して取得するマッピングの数を指定します。最大数は10,000 です。

パラメータ

このAPIは、次のパラメータを受け入れます。

パラメータ	詳説
ブックマーク	（任意）すべてのマッピングを返す最初の要求の後に使用されます。
pageLen	（任意）取得するマッピングの数。範囲は1～ 10,000です。指定しない場合のデフォルト値は10,000です。

©2025 Palo Alto Networks, Inc.

成功応答

成功すると、HTTP応答コードは200になります。さらに、応答には、次のフィールドを持つJSONオブジェクトが含まれています。

項目	詳説
nextBookmark	すべてのマッピングが返されるまで繰り返しクエリを実行するためにブックマ使用する値。
count	応答で返されるマッピングの数を表す整数。
判定	要求で指定されたマッピングを含むオブジェクト。

以下に例を示します。

```
{ "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" } ] } }
```

エラー応答

エラーが発生した場合、HTTP応答コードは次のいずれかになります。

応答コード	詳説
400	無効な要求です。要求が不完全または何らかの形で不正でした。 再試行する前に要求を修正する必要があります。
401	不正なトークン。
429	要求が多すぎます。特定の期間に発行された要求が多すぎるため、要求を処理た。1秒あたり1回まで要求は許可されません。しばらく待ってから、もう一度い。

さらに、応答ボディには次のフィールドが含まれます。

項目	詳説
コード	エラーコード。
メッセージ	エラーメッセージ。

©2025 Palo Alto Networks, Inc.

判定オブジェクト

IPアドレスとデバイスのマッピングを正常にクエリしたときに返されるオブジェクトです。このオブジェクトには、次の情報が含まれています。

項目	詳説
ip	デバイスのIPアドレス。
更新時間	マッピングが最後に更新された日時を表すUnixタイムスタンプ。
category	デバイス タイプ。例:プリンター
ベンダー	デバイス ベンダー。例:株式会社SHARP
モデル	デバイス モデル。例:MX-6070N
os	デバイス オペレーティング システム。例:ThreadX 5
OSファミリー	デバイスのOSが属するファミリー。例:ThreadX RTOS
プロファイル	デバイス プロファイル例:シャーププリンター

IPアドレスによるクエリ判定

IPアドレスに基づいてIPアドレスとデバイスのマッピングを取得します。

概要

URI	/api/v1/token/{apiKey}/verdicts?ip={STRING}
HTTP 方式	開始

詳説

IPアドレスを使用して、対応するデバイス マッピングを返します。URIに、カンマで区切られた最大10個のIPアドレスのリストを追加することで、複数のマッピングを取得できます。

サービスがIPアドレスに関連付けられたマッピングを見つけられない場合、そのIPアドレスのマッピングは返されません。

成功応答

成功すると、HTTP応答コードは200になります。さらに、応答には、次のフィールドを持つJSONオブジェクトが含まれています。

項目	詳説

©2025 Palo Alto Networks, Inc.

count	応答で返されるマッピングの数を表す整数。
判定	要求で指定されたマッピングを含むオブジェクト。

以下に例を示します。

```
{ "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" } ] } }
```

エラー応答

エラーが発生した場合、HTTP応答コードは次のいずれかになります。

応答コード	詳説
400	無効な要求です。要求が不完全または何らかの形で不正でした。 再試行する前に要求を修正してください。
401	不正なトークン。
429	要求が多すぎます。システムが特定の時間内に大量の要求を発行したため、シ 理できませんでした。1秒間に複数の要求を処理しないようにしてください。し らもう一度試してください。

さらに、応答ボディには次のフィールドが含まれます。

項目	詳説
コード	エラーコード。
メッセージ	エラーメッセージ。

クエリ判定統計

Third-Party Device-ID(サード パーティ デバイスID)サービスに関する統計情報を取得します。

概要

URI	/api/v1/token/{apiKey}/verdicts:statistics
HTTP 方式	開始

©2025 Palo Alto Networks, Inc.

成功応答

成功すると、HTTP応答コードは200になります。さらに、応答には、次のフィールドを持つJSONオブジェクトが含まれています。

項目	詳説
判定	テナント内のIPアドレスとデバイスのマッピングに関する統計を含むオブジェルドが含まれます。 • totalCount - テナント内のIPアドレスとデバイスのマッピングの合計数。 • totalUpdate - 作成されてから更新されたIPアドレスとデバイスのマッピング • totalDelete - テナントが作成されてから削除されたIPアドレスとデバイスの
requestRcvd	テナントが各種類の要求を受信した回数を含むオブジェクト: • update - 受信した判決の更新要求の数。 • deleteAll - 受信したすべての判定を削除する要求の数。 • query - 受信したクエリ評決およびIPアドレスによるクエリ判定要求の数。 • Statistics - 受信したクエリ判定統計要求の数。

以下に例を示します。

```
{ "verdicts: { "totalCount":1, "totalUpdate":0, "totalDelete":0, },
 "requestRcvd": { "update":1, "deleteAll":0, "query":0,
 "statistics":1 } }
```

エラー応答

エラーが発生した場合、HTTP応答コードは次のいずれかになります。

応答コード	詳説
401	不正なトークン。
429	要求が多すぎます。特定の期間に発行された要求が多すぎるため、要求を処理た。1秒あたり1回まで要求は許可されません。しばらく待ってから、もう一度い。

さらに、応答ボディには次のフィールドが含まれます。

項目	詳説
コード	エラーコード。

©2025 Palo Alto Networks, Inc.

項目	詳説
メッセージ	エラーメッセージ。

©2025 Palo Alto Networks, Inc.

Prisma Accessマルチテナント

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)での複数のテナントを管理する方法については、Prisma SASEを参照してください。	❑ Prisma Accessのライセンス

このセクションでは、Prisma Accessで複数のテナントを管理するための情報のみを提供します（Panorama）。Prisma Access (Managed by Strata Cloud Manager)での複数のテナントを管理する方法については、Prisma SASEを参照してください。

複数のPrisma Accessインスタンスを管理できるように、Prisma Accessにはマルチテナント機能が用意されています。この機能を利用すれば、単一のPanoramaアプライアンス（または高可用性（HA）モードで2つのアプライアンス）上に最高200件のインスタンスを作成することができます。それぞれのテナントは独自な個別のテンプレートおよびテンプレートスタック、デバイスグループ、およびアクセスドメインを保有します。

マルチテナント機能は、既存の、または今後の非マルチテナントデプロイ環境に影響を与えないため、普段通りに利用することができます。マルチテナント機能は、組織がPrisma Accessの複数のインスタンスを管理する必要がある場合にのみ有効にすることをお勧めします。

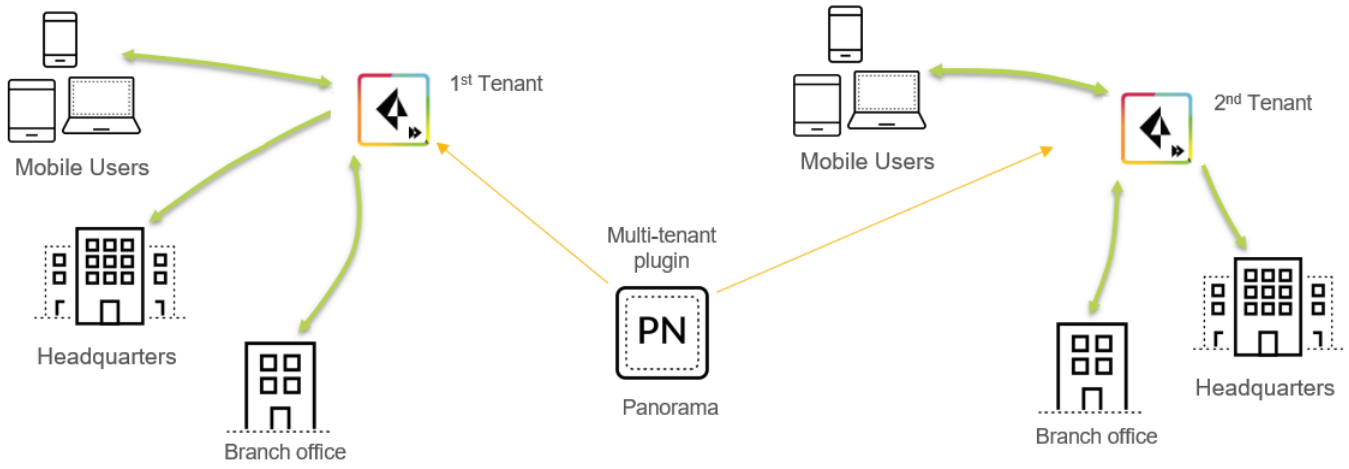
このセクションは、リモートネットワーク、モバイルユーザー、またはリモートネットワークとモバイルユーザーを組み合わせたデプロイ環境のテナントを設定するために実施する作業についてのみ説明しています。Clean Pipeサービスを設定するには、Clean Pipe向けPrisma Accessを参照してください。

マルチテナント設定の概要

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)での複数のテナントを管理する方法については、Prisma SASEを参照してください。	❑ Prisma Accessのライセンス

マルチテナント機能を有効にすると、単一のPanoramaアプライアンス上で複数のPrisma Accessインスタンスを利用することができます。各インスタンスは、*Tenant*（テナント）と呼ばれています。

各Prisma Accessテナントは専用のPrisma Accessインスタンスを持ち、テナント間で共有されることはありません。



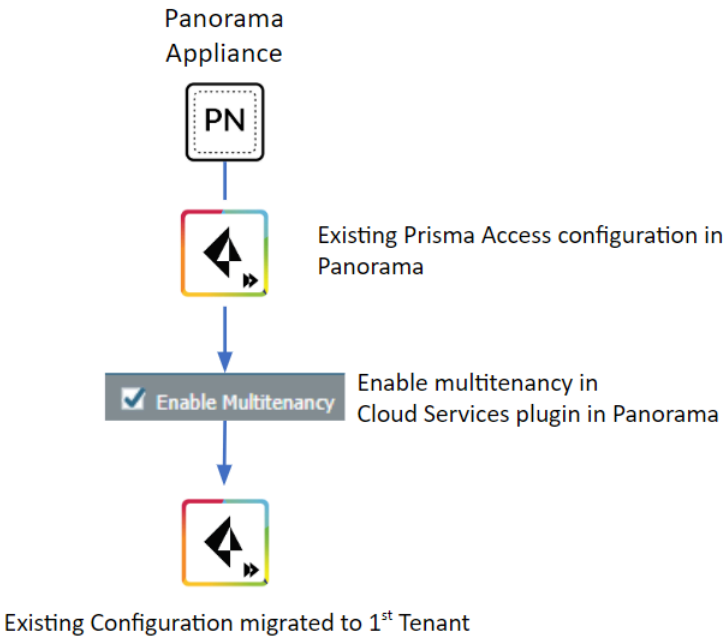
単一のPanoramaアプライアンスで複数のテナントを管理する機能を設定するには、次のワークフローを使用します。

©2025 Palo Alto Networks, Inc.

STEP 1 | マルチテナント機能を有効にします。既存のPrisma Accessインスタンスが存在している場合、マルチテナント機能を有効にすると、既存のPrisma Access設定が最初のテナントへと自動的に移行されます。

最初の（移行した）テナントに名前を付け、アクセス ドメインを指定します。Prisma Accessは、既存の設定に関連しているテンプレート、テンプレートスタック、およびデバイスグループを移行して、作成したアクセスドメインにそれらを関連付けます。

最初の設定を移行すると、Panoramaの管理ユーザーがsuperuserになり、すべてのPrisma Accessテナントを作成、管理できるようになります。



STEP 2 | 次に、Prisma Accessにテナントを追加します。

複数のテナントをデプロイするには、次のライセンスの最小要件を満たしていることを確認してください。

*Panorama*から取得した*Prisma Access*ライセンスのタイプを決定するには、***[Panorama]*** > ***[Licenses (***ライセンス***)]***を選択します。

- **Business**、**Business Premium**、**Zero Trust Network Access (ZTNA) Secure Internet Gateway (SIG)**、または **Enterprise** ライセンスをお持ちの場合は、次の最小要件をガイドラインとして使用してください。

  ネットワークは**Prisma Access**、ユーザーは**Prisma Access**：

  ローカル エディションをお持ちの場合は、テナントごとに最低 200 ユニットが必要であり、すべてのテナントがローカルになります。

  Worldwideエディションをお持ちの場合、**Worldwide**テナントを作成するには、最低1,000ユニットが必要です。テナントに200～999ユニットを割り当てる場合は、Prisma

 ©2025 Palo Alto Networks, Inc.

Accessが**Local (**ローカル**)**テナントを作成し、テナントに1,000ユニット以上を割り当てる場合は、Prisma Accessが**Worldwide (**世界領域**)**テナントを作成します。

単位は、リモートネットワーク用Prisma Accessでは帯域幅（Mbps）、ユーザー用Prisma Accessではモバイルユーザー数に相当します。

- ライセンスの種類が **GlobalProtect Cloud Service**で始まる場合は、次の最小値をガイドラインとして使用してください。

  Prisma Access for Networks– ライセンスでは、テナントごとに最低200 Mbpsが利用可能である必要があります。

  Prisma Accessユーザーの場合- ライセンスでは、テナントごとに最低200人のモバイルユーザーが利用可能である必要があります。

  両方のタイプのPrisma Access設定で、各タイプの追加ライセンスを追加することができます（最低ライセンスに加算される）。テナントあたりの必要な最低割り当て量を維持し、許可されている総合ライセンス容量を超過しない限り、オンボーディング後に各テナントの帯域幅またはモバイルユーザー割り当てを増減することができます。

リモートネットワークのみ、モバイルユーザーのみ、またはその両方に対してマルチテナント設定を行えます。マルチテナントを有効にした場合、それに応じて各テナントにライセンスを割り当てます。

リモートネットワークおよびモバイルユーザーのライセンスを保有している場合、モバイルユーザーまたはリモートネットワークのみの個別のテナントを設定することができます。たとえば、Prisma Accessのデプロイメントにモバイル ユーザーとリモート ネットワーク用の**Worldwide Edition (**全世界領域エディション**)** ライセンスがある場合、テナントに最低1,000 人のモバイル・ユーザを指定すれば、モ バイル・ユーザ専用のテナントを設定できます。

最初に作成するテナントごとに、 Prisma Accessは各テナントのテンプレート、テンプレートスタック、デバイス グループを自動的に作成し、作成したアクセス ドメインに関連付けます。 この環境を作成すると、Prisma Accessはテナントのデバイス グループとテンプレートに基づく管理ロールを使用してテナント レベルの管理者ユーザーを作成し、そのロールに基づいて管理ユーザーを作成できるようになります。このようにして、Panoramaアプライアン

 ©2025 Palo Alto Networks, Inc.

スが管理する他のテナントへのユーザーアクセスを禁止した、単一のテナントにアクセスする管理ユーザーを作成します。

Prisma Accessは次の命名規則に従って、テンプレートスタック、テンプレート、およびデバイスグループを作成します。

- 名前が**sc-stk-***tenant*のサービス接続テンプレートスタック、ここで*tenant*はテナント名を表しています。
- 名前が**sc-tpl-***tenant*のサービス接続テンプレート。
- 名前が**sc-dg-***tenant*のサービス接続デバイスグループ。
- 名前が**mu-stk-***tenant*のモバイルユーザーテンプレートスタック。
- 名前が**mu-tpl-***tenant*のモバイルユーザーテンプレート。
- 名前が**mu-dg-***tenant*のモバイルユーザーデバイスグループ。
- 名前が**rn-stk-***tenant*のリモートネットワークテンプレートスタック。
- 名前が**rn-tpl-***tenant*のリモートネットワークテンプレートスタック。
- 名前が**rn-dg-***tenant*のリモートネットワークデバイスグループ。
- 名前が**ep-stk-***tenant*のExplicit Proxyテンプレートスタック。
- 名前が**ep-tpl-***tenant*のExplicit Proxyテンプレート。
- 名前が**ep-dg-***tenant*のExplicit Proxyデバイスグループ。
- 名前が**cp-stk-***tenant*のClean Pipeテンプレートスタック。
- 名前が**cp-tpl-***tenant*のClean Pipeテンプレート。
- 名前が**cp-dg-***tenant*のClean Pipeデバイスグループ。

テンプレート スタック、テンプレート、デバイス グループは、ライセンスが付与されていないものも含め、すべてのPrisma Accessタイプに対して作成されます。たとえば、リモートネットワーク用ライセンスを購入した場合、Prisma Accessはリモートネットワーク、モバイルユーザー、およびClean Pipeに対して、テンプレートスタック、テンプレート、およびデバイスグループを自動的に作成します。

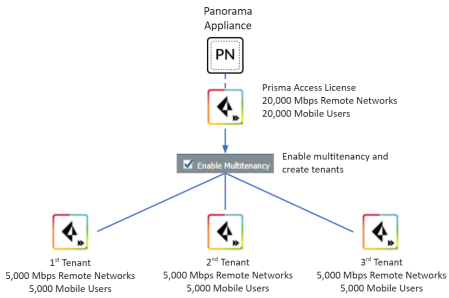
カスタムテンプレートを追加した場合、それらがPrisma Accessが作成したテンプレートに優先されることはありません。

PanoramaでCloud Servicesプラグインに関連付けられたライセンスに基づいて、各テナントにリモートネットワークおよびモバイルユーザーのライセンスリソースを割り当てます。

20,000 Mbpsのリモートネットワーク帯域幅プールおよび20,000人のモバイルユーザーを持つライセンスを使った、Prisma Accessデプロイメント例を次の図に示します。管理者は、既存の設定に対してリモートネットワーク帯域幅に5,000 Mbps、および5,000人のモバイルユーザーを割り当てました。管理者がマルチテナント機能を有効にすると、このライセンス割り当てが他のすべての設定と一緒に最初のテナントに移行されます。次に管理者は追加のテナントを作成し、それぞれリモートネットワーク用に5,000 Mbpsの帯域幅プール、モバイルユーザー用に5,000人分を割り当てています。Prisma Accessは、全体のライセンス割り

 ©2025 Palo Alto Networks, Inc.

当てからライセンスリソースを割り当てます。この設定作業完了後、ライセンスには5,000 Mbpsのリモートネットワーク帯域幅と5,000人のモバイルユーザーが残っています。



 ©2025 Palo Alto Networks, Inc.

マルチテナントデプロイの計画

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)での複数のテナントを管理する方法については、Prisma SASEを参照してください。	• Prisma Accessのライセンス

マルチテナント機能を有効にする前に、最初のテナントを移行してから、追加のテナントを作成します。次の作業を完了する前に、必要な情報とリソースがすべて用意されていることを確認してください。

- 既存のシングルテナントデプロイメント環境を、マルチテナントデプロイメント環境に移行する場合、次のPrisma Access機能はサポートされていないことに注意してください。サポートされていない機能のリストについては、Palo Alto Networks互換性マトリックスを参照してください。
- 既存のPrisma Access設定がない場合は、マルチテナントを有効にしてテナントを追加し、作成後にテナントを構成できます。詳細については まったく新しいマルチテナントのデプロイメントを作成するを参照してください。
- リモートネットワークおよびモバイルユーザーのライセンス割り当てを記録します。

  ライセンスを開いて（**Panorama** > **Licenses**（ライセンス））、Prisma Accessのリモートネットワークの**Total Mbps**（合計**Mbps**）（リモートネットワーク帯域幅プール）およびモバイルユーザーの**User Limit**（ユーザー限度）（ライセンスされたユーザー数合計）を探します。

  テナントの作成時には、この割り当てられているライセンスから、リモートネットワークおよびモバイルユーザー用のリソースを割り当てます。リモートネットワークまたはモバイルユーザー向けにライセンスされているMbpsを使い切ると、それ以上のテナントは作成できません。

  既存の設定の帯域幅とモバイルユーザー割り当ても、記録しておく必要があります。設定を最初のテナントに移行したら、これらの値をチェックして、最初のテナントの移行が正しく行われたことを確認してください。
- 各テナントを識別するために使用する、名前のリストを作成します。

  テナント名を作成する場合、*Tenant-1*、*Tenant-2*、*Tenant-3*...のような名付け方をしないでください。ログ出力で、システムログはテナント名をわずかな文字で記録しているため、似たような名前を持つテナントが存在すると、テナントとログに記載されている名前との対応を判別することが、困難になる可能性があります。テナントには、一意の短い名前を使用することをお勧めします（例：*Acme*または*Hooli*）。

©2025 Palo Alto Networks, Inc.

- 各テナントに割り当てる、作成する管理ユーザーのリストを作成します。また、同時にログインできる最大管理ユーザー数を記録します。

  管理ユーザーが、設定の変更やコミット操作などの標準的なマルチテナント操作を実施する場合、Panoramaに最大で12名の管理ユーザーが同時にログインできるようにすることをお勧めします。

  複数のテナントを管理できる管理ユーザーは、1回のコミット操作で最高200テナントを同時にプロビジョニングできます。
- 複数のテナントを有効にするために十分なライセンスリソースがあることを、忘れずに確認してください。

  各テナントの最低ライセンス割り当ては、リモートネットワークの場合200 Mbpsまたは200モバイルユーザーとなっています。リモートネットワークまたはモバイルユーザーのみのテナントを作成することもできます。また、同じPanoramaで異なる設定を持つテナントを利用できます。たとえば、各テナントが最低限のライセンス割り当てを満たしており、テナントを設定しているPanoramaで関連するライセンスがアクティブ化されている場合、リモートネットワークのみのテナント、モバイルユーザーのみのテナント、またはモバイルユーザーとリモートネットワークの両方を持つテナントを作成することができます。
- マルチテナントモードでテナントを設定する場合、サービス接続/リモートネットワーク接続用の各IPSecトンネルおよびIKEゲートウェイに対して一意の名前を作成し、またできる限り他のテナントと重複しない名前を使用するようにしてください。他のテナントが同じ名前のトンネルまたはゲートウェイを使用していると、機能に影響はありませんが、そのIPSecトンネルやIKEゲートウェイを削除しようとしても、削除することはできません。

  この警告は、QoSプロファイルを含むすべてのオブジェクトに適用されます (オブジェクトの1つが別のテナントによって参照されている場合、マルチテナント展開で重複する名前を持つオブジェクトを削除することはできません)。
- シングルテナントユーザーはシステムログを参照できません。スーパーユーザーのみが参照できます。ただし、テナント別にログをソートすることができます。
- モバイルユーザーが単一のPrisma Accessテナントの場合、ユーザーは1つのライセンス ユニットを消費します。ユーザーが単一のマルチテナントのデプロイメントで追加のテナントにログインする場合、ユーザーはログインしているテナントごとに1つのライセンス ユニットを消費します。たとえば、1人のユーザーが5つのテナントにログインしている場合、そのユーザーは合計で5つのモバイル ユーザー ライセンス ユニットを消費します。
- マルチテナント機能を使用しており、テナントレベルの管理ユーザーとしてログインした場合、Panorama Task Manager（Panorama Webインターフェースの下部にある**Tasks**（タスク）をクリック）には、superuser（Admin）が実行したタスクも含めて、すべてのテナントのすべてのタスクが表示されます。
- いくつかのPrisma Access機能はマルチテナントでの使用はサポートされていません。詳細については、Palo Alto Networks互換性マトリックスのマルチテナントでサポートされていない機能を参照してください。

©2025 Palo Alto Networks, Inc.

- Panoramaの設定をバックアップした後、以前に保存した設定に戻す場合、次の 順番で操作を行うと、Panoramaは保存した設定に戻すことができません：

  1. Panorama 構成をバックアップします。
  2. テナントを削除します。
  3. 設定を復元します。

  テナントを削除すると、テナントを削除する前に保存した以前のバックアップは使用できません。ただし、テナントを削除した後に作成したバックアップは使用できます。

©2025 Palo Alto Networks, Inc.

まったく新しいマルチテナントのデプロイメントを作成する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)での複数のテナントを管理する方法については、Prisma SASEを参照してください。	❑ Prisma Accessのライセンス

マルチテナントのデプロイメントを作成し、既存のPrisma Access設定がない場合は、マルチテナントを有効にしてテナン トを追加し、作成後にテナントを構成できます。

既存のシングルテナントのデプロイメントがあり、マルチテナントのデプロイメントに移行する場合は、ワークフローを使用して マルチテナントを有効にし、最初のテナントを移行します。

既存の設定がない最初のテナントを作成する場合は、次の相違点とガイドラインに従ってください。

- 移行する設定がないので、 Prisma Accessは各テナントのテンプレート、テンプレート スタック、デバイス グループを作成し、テナント作成時に作成したアクセス ドメインに関連付けます。Prisma Accessが使用している命名規則についてはマルチテナント設定の概要を参照してください。
- オプションとして、テナント レベルのアクセス ドメインを作成した後、管理者をアクセス ドメインに関連付けることで、単一のテナントの管理を許可する 管理ユーザーを作成 できます。
- 既存のテンプレートやデバイス グループ（たとえば、Panorama で管理されているオンプレミス デバイ スのテンプレートで、Prisma Accessでも使用する必要があるもの）がある場合は、アクセス ドメインを作成し て構成するときに、それらのデバイス グループとテンプレート ドメインを必ず アクセス ドメインに追加してください。デバイス グループとテンプレートをアクセス ドメインに追加しないと、Cloud Services プラグインでPrisma Accessコンポーネントを設定するときに、それらを表示したり選択したりすることができません。

©2025 Palo Alto Networks, Inc.

マルチテナントの有効化と最初のテナントの移行

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)での複数のテナントを管理する方法については、Prisma SASEを参照してください。	❑ Prisma Accessのライセンス

マルチテナント機能を有効にして、既存の設定を作成した最初のテナントに移行するには、次のワークフローを使用してください。既存の構成がない場合は、マルチテナントを有効にしてテナントを追加してから構成できます。

マルチテナント機能を有効にすると、Prisma Accessは設定内の次のコンポーネントを移行します。

- トンネル設定も含めた、すべてのサービス接続/リモートネットワークトンネルのオンボーディング情報。
- 既存のモバイルユーザーのオンボーディング情報。
- Strata Logging Service情報。
- 既存の自律型DEM（ADEM）の設定
- サービス接続、リモートネットワーク、およびモバイルユーザーの、テンプレート、テンプレートスタック、およびデバイスグループ。

ユーザー数 (モバイル ユーザー デプロイメントの場合)、帯域幅 (リモート ネットワーク デプロイメントの場合)、およびデプロイメントごとに割り当てるAutonomous DEM (ADEM)（ADEMライセンスを購入した場合）を指定する必要があります。

これらのデバイスグループは変化するため、次のワークフローのように、アクセスドメインを作成して、移行したデバイスグループ、テンプレート、およびテンプレートスタックを追加します。

既存の*Prisma Access*設定が存在しておらず、新しいマルチテナント デプロイメントを最初から作成している場合は、このワークフローを使用しないでください。テナントをPrisma Accessに追加するの手順に従って最初のテナントを作成してください。

STEP 1 | このデプロイメントに割り当てるライセンスユニットの数を決定します。

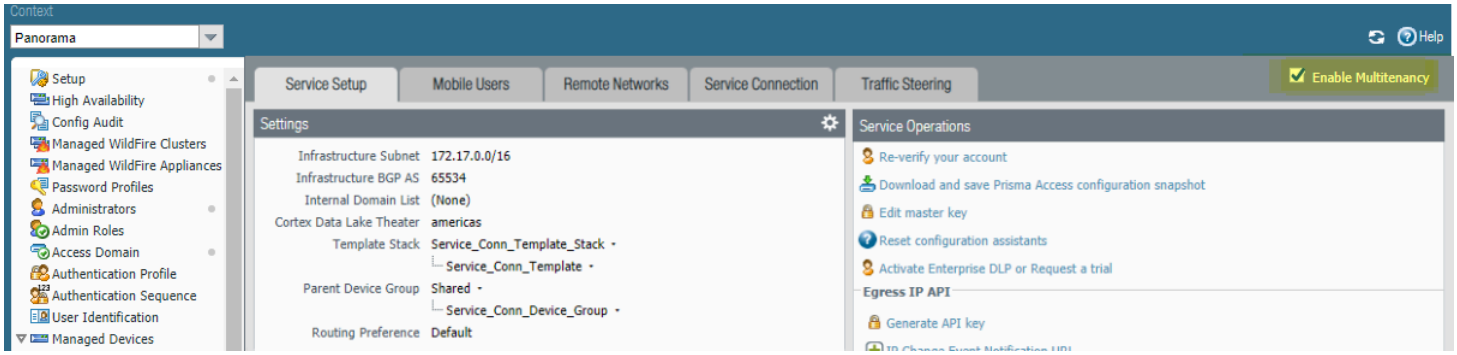
Prisma Accessが最初のテナントに設定を移行する間に、以下を指定する必要があります。

- テナントのリモートユーザーデプロイメントに割り当てる帯域幅 (該当する場合)。
- テナントのモバイルユーザー デプロイメントに割り当てるユーザー (該当する場合)。
- モバイル用途とリモートネットワーク (該当する場合) に割り当てるADEMユニットの数。

STEP 2 | **Panorama** > **Cloud Services**（クラウドサービス） > **Configuration**（設定）を選択します。

©2025 Palo Alto Networks, Inc.

STEP 3 | **Enable Multitenancy**（マルチテナント機能を有効にする）（ページの右上にあります）を選択します。



マルチテナントを有効にすると、Panoramaは既存のPrisma Access設定が最初のテナントに移動するこ とを通知する通知を表示します。

マルチテナントを有効にすると、デプロイメントは永続的にマルチテナントのデプロイメントに変更され、シングルテナントモードに戻すことはできません。

STEP 4 | 既存の設定を最初のテナントに移行するには、**OK**をクリックします。

テナントページが表示され、ウィンドウの中央に円グラフが表示されます。

- リモートネットワークライセンスまたはモバイルユーザーライセンスをお持ちの場合は、ライセンスされたリモートネットワーク帯域幅とモバイルユーザーの使用可能量が表示されます。
- (リモートネットワークとモバイルユーザーのデプロイメントのみ) 自律型DEMライセンスを購入した場合、ADEM で使用できるユニット数が表示されます。
- Clean Pipeをデプロイメントしている場合、テナントの帯域幅量が表示されます。

STEP 5 | テナントに対して使用するデプロイタイプを選択します。

- テナントに対してリモートネットワーク、モバイルユーザーデプロイ環境の場合、または両方のデプロイタイプを設定する場合は、**Remote Networks/Mobile Users**（リモートネットワーク/モバイルユーザー）を選択します。
- Clean Pipeデプロイの場合は、**Clean Pipe**を選択します。

  このセクションでは、リモートネットワーク、モバイルユーザー、またはリモートネットワークとモバイルユーザーデプロイタイプの両方に対するテナントの設定方法のみ説明しています。Clean Pipeサービスを設定するには、Clean Pipe向けPrisma Accessを参照してください。

©2025 Palo Alto Networks, Inc.

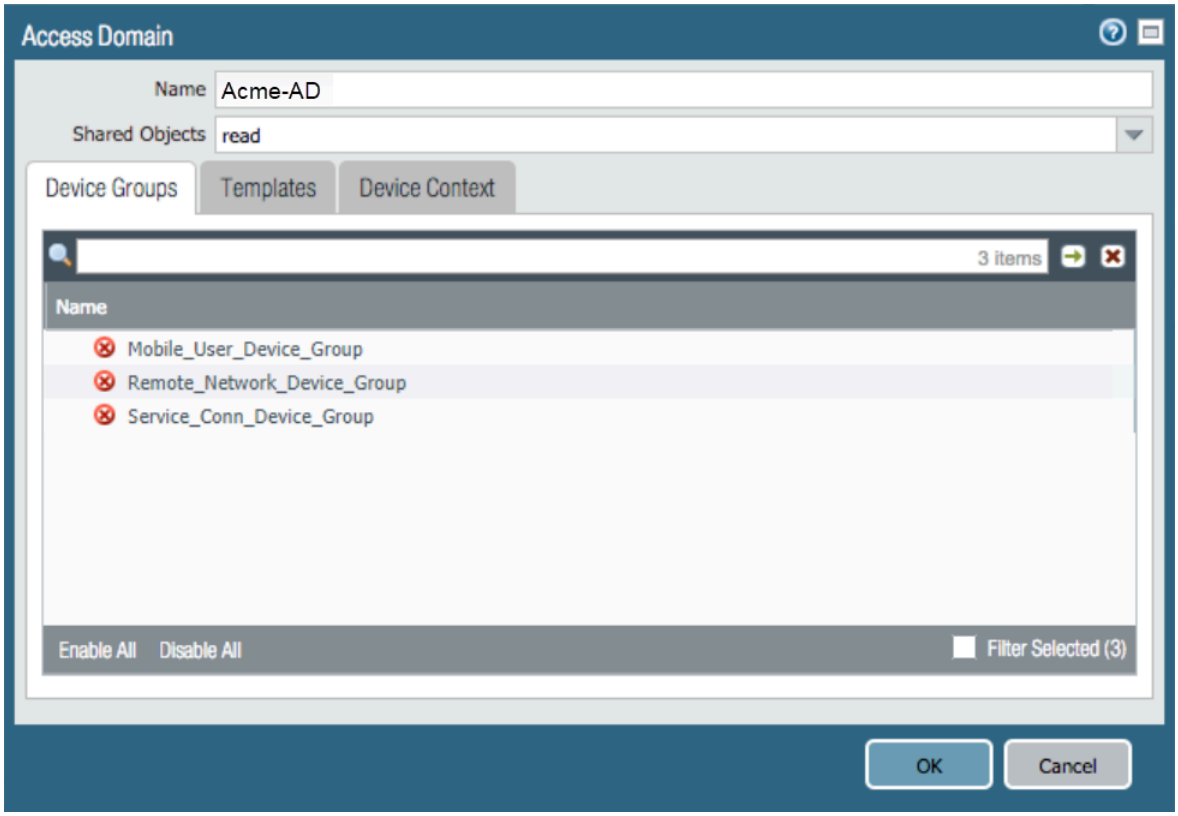
STEP 6 | 既存の設定を最初のテナントに移行します。

最初に移行されたサブテナントの名前は、移行するテナントから自動的に入力され、編集できません。

1. 下矢印をクリックして**New Access Domain**（新規アクセスドメイン）を選択して、新しい**Access Domain**（アクセスドメイン）を作成します。
2. アクセスドメインの**Name**（名前）を入力して、**OK**をクリックします。

   Prisma Accessは**Mobile_User_Device_Group**、**Remote_Network_Device_Group**、および **Service_Conn_Device_Group** デバイスグループを新しいアクセス ドメインに追加します。

   デフォルトのデバイスグループとテンプレートを、最初に移行したサブテナント以外のサブテナントに関連付けないでください。

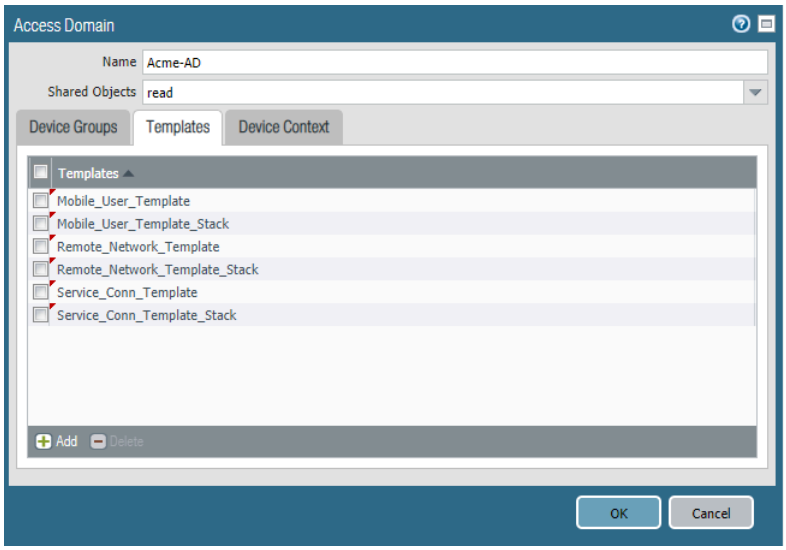


3. (任意) [テンプレート]をクリックして、Prisma Accessによって次のテンプレートとテンプレートスタックが追加されていることを確認します。
   - **Explicit_Proxy_Template**
   - **Explicit_Proxy_Template_Stack**
   - **Mobile_User_Template**
   - **Mobile_User_Template_Stack**
   - **Remote_Network_Template**
   - **Remote_Network_Template_Stack**
   - **Service_Conn_Template**

©2025 Palo Alto Networks, Inc.

- **Service_Conn_Template_Stack**

  これらは、標準的なPrisma Accessデプロイメントのデフォルトのテンプレートスタックとテンプレートです。他のテンプレートを追加した場合は、Prisma Accessがそれらを追加したことを確認してください。



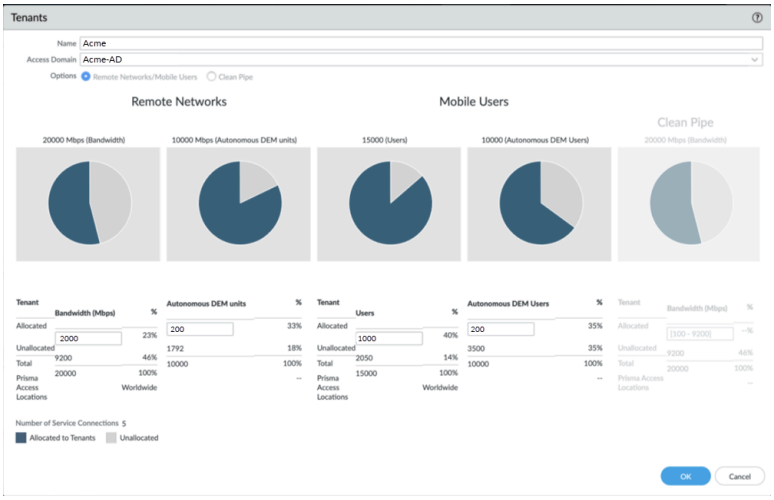
4. （任意） この設定に他のテンプレートを関連付けている場合は、それらのテンプレートを選択します。
5. **OK**をクリックして、**Access Domain**（アクセスドメイン）ページを閉じ、**Tenants**（テナント）ページに戻ります。

©2025 Palo Alto Networks, Inc.

STEP 7 | リモートネットワークの **[帯域幅 (Mbps)]**、モバイルユーザーの**[ユーザー]**、および各デプロイメントタイプに割り当てる自律型**DEM** ユーザーの数に値を入力します。

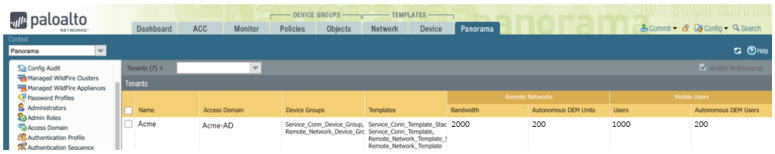
テナントにADEMユニットを割り当てる場合は、次のガイドラインに従ってください。

- モバイル ユーザーおよびリモート ネットワークに割り当てることができるADEMユニットの数は、基本ライセンスの数以下に限られます。
- 割り当てることができるユニットの最小数は200です。
- テナントにADEMユニットを割り当てた後、それらのユニットを編集または削除できます。
- デプロイメント タイプ (モバイル ユーザーまたはリモート ネットワーク) のADEMライセンスを購入していない場合、その選択肢はグレー表示されます。



STEP 8 | **OK** をクリックします。

Panorama > **Cloud Services**（クラウドサービス） > **Configuration**（設定）ページに、最初のテナントが正常に移行されたことを知らせるメッセージが表示され、**Tenants**エリアに**Tenants**ドロップダウンが追加されます。



 ©2025 Palo Alto Networks, Inc.

STEP 9 | すべてのテンプレートとデバイス グループがテナントに入力されていることを確認します。

1. ドロップダウンリストからテナントを選択します。
2. **[Panorama]** > **[Cloud Services**（クラウドサービス）**]** > **[Configuration**（設定）**]**へと移動します。
3. [サービスのセットアップ]を選択します。
4. 設定を編集するには、歯車をクリックします。
5. 正しいテンプレートスタック、テンプレート、およびデバイス グループ (それぞれ Service_Conn_Template_Stack、Service_Conn_Template、および Service_Conn_Device_Group) が設定に入力されていることを確認します。
6. 既存の設定がある他のタブ（例:モバイルユーザー**—GlobalProtect**、モバイルユーザー**—Explicit Proxy**、リモートネットワーク、またはサービス接続など）に移動し、ギアをクリックして設定を編集し、正しいテンプレートスタック、テンプレート、およびデバイス グループが設定に入力されていることを確認します。

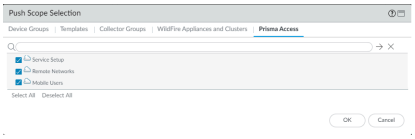
STEP 10 | 変更をローカルでPanoramaにコミットします **([**コミット**]** > **[Panorama**にコミット**]**。

STEP 11 | **[**コミット**]** > **[Panorama**にコミット**]** を選択すると、Prisma Accessを管理しているパノラマにローカルで変更内容が保存されます。

ローカルコミットを実行しない場合、変更をコミットしてプッシュしても、Prisma Accessコンポーネントはプッシュスコープに表示されません。

STEP 12 | 変更をコミットしてプッシュし、Prisma Accessでアクティブにします。

1. **Commit**（コミット） > **Commit and Push**（コミットしてプッシュ）の順に選択し、Push Scope（プッシュ スコープ）で **Edit Selections**（選択内容の編集）を行います。
2. **Prisma Access**を選択し、作成したテナントを選択して、**Service Setup**（サービスセットアップ）、**Remote Networks**（リモートネットワーク）、および**Mobile Users**（モバイルユーザー）を選択します。

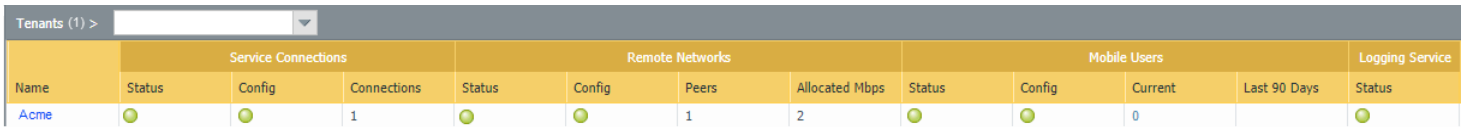


3. **OK** をクリックして、プッシュ スコープに対する変更を保存します。
4. 変更をコミットしてプッシュします。

©2025 Palo Alto Networks, Inc.

STEP 13 | **Panorama** > **Cloud Services**（クラウドサービス） > **Status**（ステータス）を選択します。

Status（ステータス）ページに、すべてのテナントのステータスが表示されます。作成したテナントは1つだけなので、表示されるのはそのテナントだけです。そのテナントをドロップダウンから選択すると、テナントの詳細なステータスが表示されます。



ドロップダウンからテナントを選択すると、テナントのStatus（ステータス）ページに移動します。

STEP 14 | Prisma Accessに、他のテナントを追加します。

©2025 Palo Alto Networks, Inc.

テナントをPrisma Accessに追加する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)での複数のテナントを管理する方法については、Prisma SASEを参照してください。	❑ Prisma Accessのライセンス

既存の情報を最初のテナントとして移行したら、追加のテナントを作成、設定することができます。最初のテナントの後に作成する各テナントに対して、Prisma Accessより独自のテンプレートスタックとドメイングループを持つ、個別のアクセス ドメインが作成されます。

Prisma Accessに他のテナントを追加するには、このワークフローを使用してください。

すべてが新しいマルチテナントデプロイメント環境を作成している場合は、このワークフローを使って最初のテナント、およびそれ以降のテナントを追加してください。詳細については まったく新しいマルチテナントのデプロイメントを作成するを参照してください。

STEP 1 | PanoramaにsuperuserとしてログインしPanoramaます。

STEP 2 | テナントを追加、設定します。

1. **[Panorama] > [Cloud Services**（クラウドサービス）**] > [Configuration**（設定）**]**の順に選択して、新しいテナントを追加します。

   Remote Networks/Mobile Users（リモートネットワーク/モバイルユーザー）を忘れずに選択してください。Clean Pipeデプロイ環境を作成、設定する場合は、Clean Pipe向けPrisma Accessを参照してください。
2. **Name**（名前）に分かりやすいテナント名を指定します。
3. 新しい**Access Domain**（アクセスドメイン）を**Add**（追加）して、それに分かりやすい**Name**（名前）を指定したら、**OK**をクリックして**Tenants**（テナント）ウィンドウに戻ります。

   OKをクリックすると、 Prisma Accessはテンプレート、テンプレート スタック、デバイス グループを自動的に作成し、作成したアクセス ドメインに関連付けます。

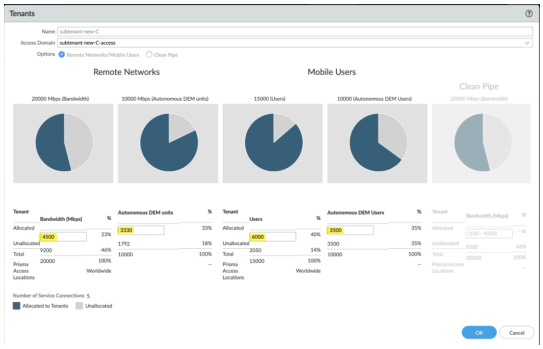
STEP 3 | **Remote Networks**（リモートネットワーク）に割り当てる**Bandwidth (Mbps)**（帯域幅）、および**Mobile Users**（モバイルユーザー）に割り当てる**Users**（ユーザー数）を指定します。

©2025 Palo Alto Networks, Inc.

STEP 4 | (Autonomous DEM のみを使用したデプロイメント)自律型DEM (ADEM)ライセンスを購入した場合は、ADEMに割り当てるユニット数を選択します。

テナントにADEMユニットを割り当てる場合は、次のガイドラインに従ってください。

- モバイル ユーザーおよびリモート ネットワークに割り当てることができるADEMユニットの数は、基本ライセンスの数以下に限られます。
- 割り当てることができるユニットの最小数は200です。
- テナントにADEMユニットを割り当てた後、それらのユニットを編集または削除できます。
- デプロイメント タイプ (モバイル ユーザーまたはリモート ネットワーク) のADEMライセンスを購入していない場合、その選択肢はグレー表示されます。

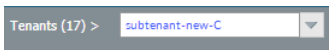


STEP 5 | **[OK]** を クリックして最初のテナントを作成します。

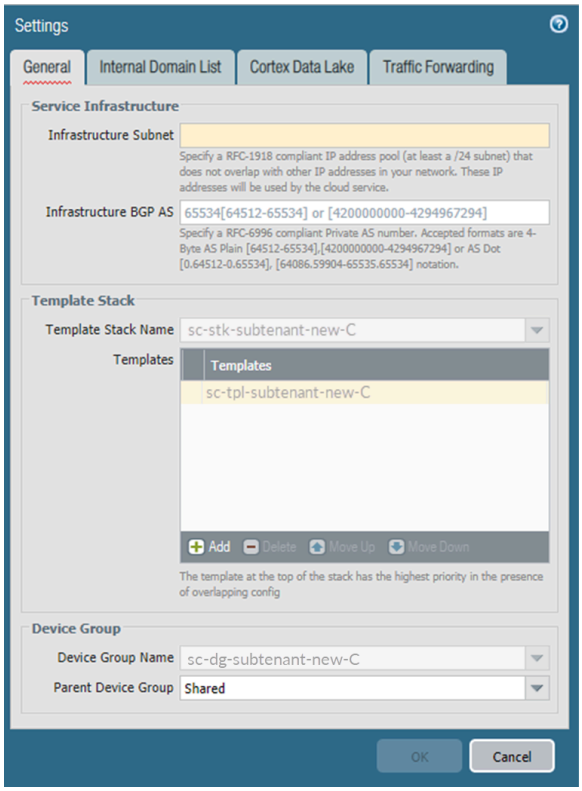
©2025 Palo Alto Networks, Inc.

STEP 6 | Prisma Accessが、テンプレート スタック、テンプレート、およびデバイス グループのサービス設定を、作成したばかりのテナントのサービス接続設定に適用していることを確認してください。

1. 作成したテナントを**Tenant**（テナント）ドロップダウンから選択します。



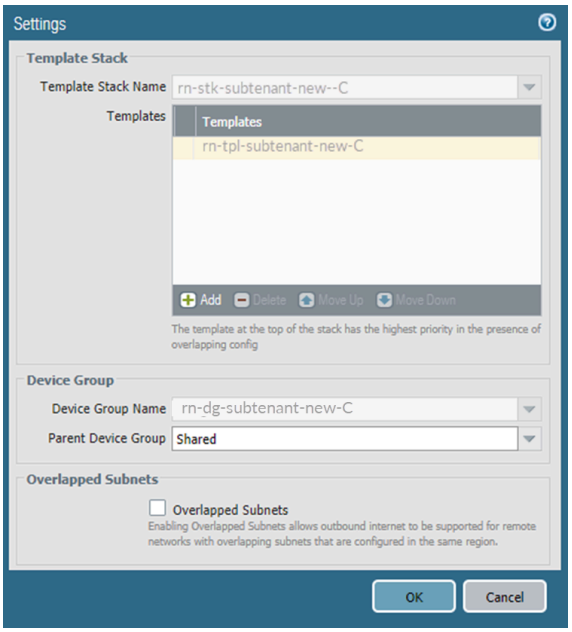
2. **[Panorama] > [Cloud Services**（クラウドサービス）**] > [Configuration**（設定）**] > [Service Setup**（サービスのセットアップ）**]**を選択します。
3. 設定を編集するには、**Settings**（設定）エリアの右側にある歯車型アイコンをクリックします。
4. Prisma Accessがテンプレートスタック（**sc-stk-***tenant*）、テンプレート（**sc-tpl-***tenant*）およびデバイス グループ（**sc-dg-***tenant*）を、サービス接続設定に関連付けていることを確認してください。
5. **Parent Device Group**（親デバイス グループ）が**Shared**（共有）に設定されていることを確認し、**OK**をクリックします。



 ©2025 Palo Alto Networks, Inc.

STEP 7 | Prisma Accessがテンプレート スタック、テンプレート、およびデバイス グループをリモート ネットワーク設定に適用したことを確認します。

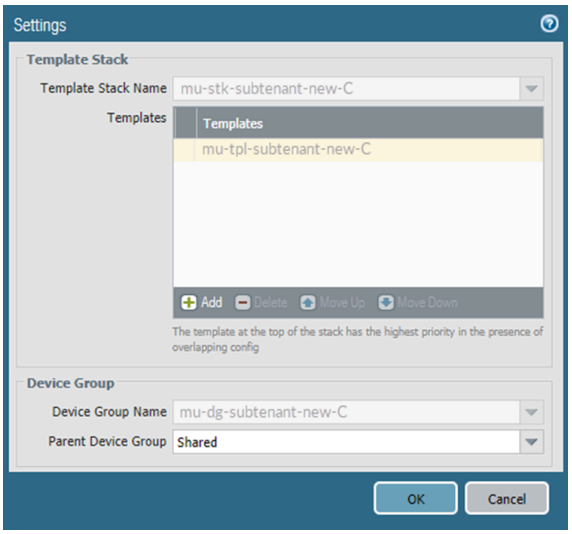
1. **[Panorama] > [Cloud Services**（クラウドサービス）**] > [Configuration**（設定）**] > [Remote Networks**（リモートネットワーク）**]**の順に選択し、**[Settings**（設定）**]**エリアの右側にある歯車型アイコンをクリックして、設定を編集します。
2. Prisma Accessがテンプレートスタック（**rn-stk-***tenant*）、テンプレート（**rn-tpl-***tenant*）およびデバイス グループ（**rn-dg-***tenant*）を、リモートネットワーク設定に関連付けていることを確認してください。
3. **Parent Device Group**（親デバイス グループ）が**Shared**（共有）に設定されていることを確認し、**OK**をクリックします。



©2025 Palo Alto Networks, Inc.

STEP 8 | Prisma Accessがテンプレート スタック、テンプレート、およびデバイス グループをモバイル ユーザ設定に適用したことを確認してください。

1. **Panorama** > **Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Mobile Users**（モバイルユーザー）の順に選択し、**Settings**（設定）エリアの右側にある歯車型アイコンをクリックして、設定を編集します。
2. Prisma Accessがテンプレートスタック（**mu-stk-*tenant***）、テンプレート（**mu-tpl-*tenant***）およびデバイス グループ（**mu-dg-*tenant***）を、サービス接続設定に関連付けていることを確認してください。
3. **Parent Device Group**（親デバイス グループ）が**Shared**（共有）に設定されていることを確認し、**OK**をクリックします。



STEP 9 | 変更をローカルでPanoramaにコミットします ([コミット] > [**Panorama**にコミット]。

STEP 10 | （モバイルユーザーデプロイメントのみ）–インフラストラクチャのサブネットを追加し、変更をコミットしてプッシュし、Prisma Accessでアクティブにします。

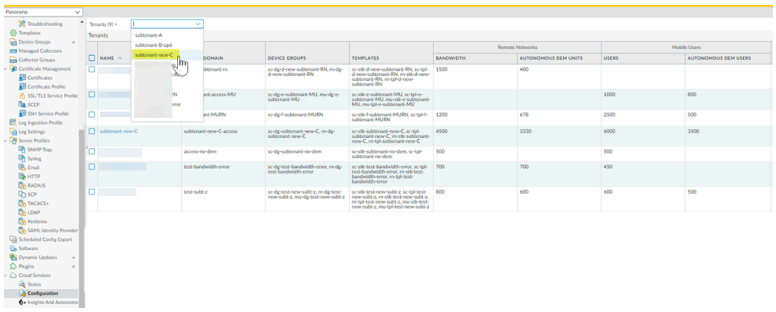
モバイル ユーザーの変更を有効にするには、これらの手順が必要です。

1. **[Panorama]** > [クラウド サービス] > [構成] > [サービス セットアップ]を選択し、歯車アイコンをクリックして設定を編集し、インフラストラクチャ サブネットを構成します。
2. [コミット] > [コミットしてプッシュ]を選択し、プッシュ スコープで [選択内容の編集]を選択して、モバイル ユーザーが選択されていることを確認します。
3. **OK** をクリックして、プッシュ スコープに対する変更を保存します。
4. 変更をコミットしてプッシュします。

 ©2025 Palo Alto Networks, Inc.

STEP 11 | **[Panorama]** > **[**クラウドサービス**]** > **[**構成**]** > ***[***テナント名***]*** を選択して、作成した新しいテナントを選択し、テナントの構成を続行します。

1. サービスインフラの設定。
2. プライベート アプリへのアクセスを許可するサービス接続を作成します。
3. リモート ネットワークのライセンスがある場合は、リモート ネットワークをオンボードして構成します 。
4. リモートユーザーのライセンスがある場合は、Prisma Access (Managed by Panorama)のGlobal Protectを設定します。



 ©2025 Palo Alto Networks, Inc.

テナントの削除

以下の手順を実行して、Prisma Access (Managed by Panorama)デプロイメントのテナントを削除します。

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)での複数のテナントを管理する方法については、Prisma SASEを参照してください。	❑ Prisma Access ライセンス

- マルチテナントのデプロイメントのすべてのテナントを削除することはできますが、テナントを追加または削 除する管理者レベルの*Prisma Access*設定を削除することはできません。
- テナントを削除すると、*Prisma Access*はライセンスが付与されているテンプレートとデバイス グループ セットを削除しますが、ライセンスが付与されていないセットは削除しません。たとえば、*Prisma Access for Users*ライセンスを保有している場合にテナントを削除すると、*Prisma Access*ではモバイルユーザー関連のテンプレート スタック、テンプレート、デバイスグループが削除されますが、ライセンスを保有していない*Prisma Access for Networks*に対して作成されているセットは削除されません。これらの未使用のテンプレートとデバイスグループセットは、テナントを削除した後に手動で削除できます。

STEP 1 | Prisma Accessを管理する Panorama から、**[Panorama]** > **[Cloud Services (**クラウドサービス**)]** > **[Configuration (**設定**)]**を選択します。

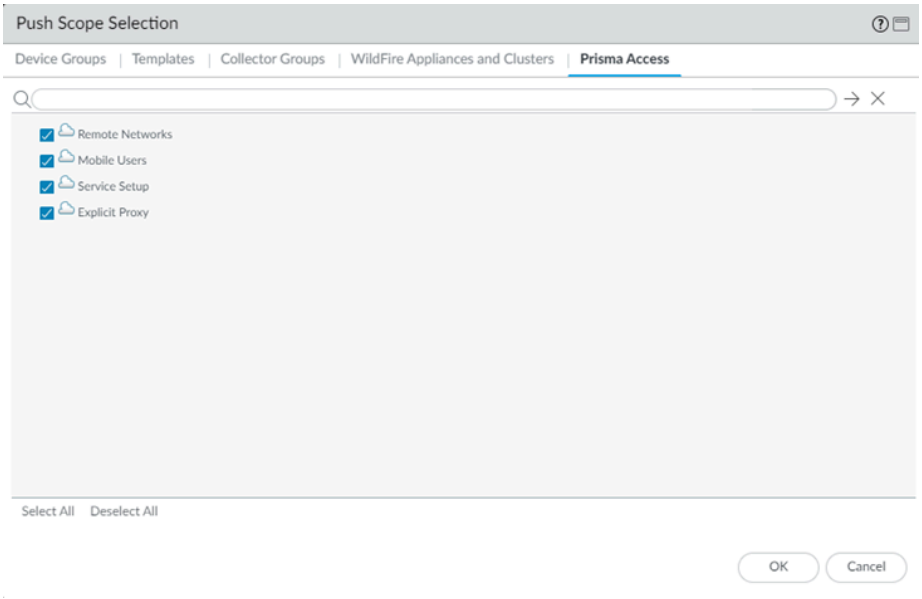
STEP 2 | テナントを選択し、それに関連付けられているすべての設定を削除します。

この手順は、サービス接続、モバイル ユーザー、リモート ネットワーク、クリーン パイプの設定など、すべての設定がテナントから削除されるようにするためのベストプラクティスとして実行します。

©2025 Palo Alto Networks, Inc.

STEP 3 | 変更をPrisma Accessにコミット、プッシュします。

1. **Commit** > **Push to Devices**を選択します。
2. 選択内容の編集をクリックし、削除したすべてのコンポーネント (デプロイメントに応じて、リモートネットワーク、モバイルユーザー、サービス セットアップ、明示的プロキシ、クリーンパイプなど) が選択されていることを確認します。



3. **Push**（プッシュ）をクリックします。

STEP 4 | 1つまたは複数のテナントを選択し、削除します。

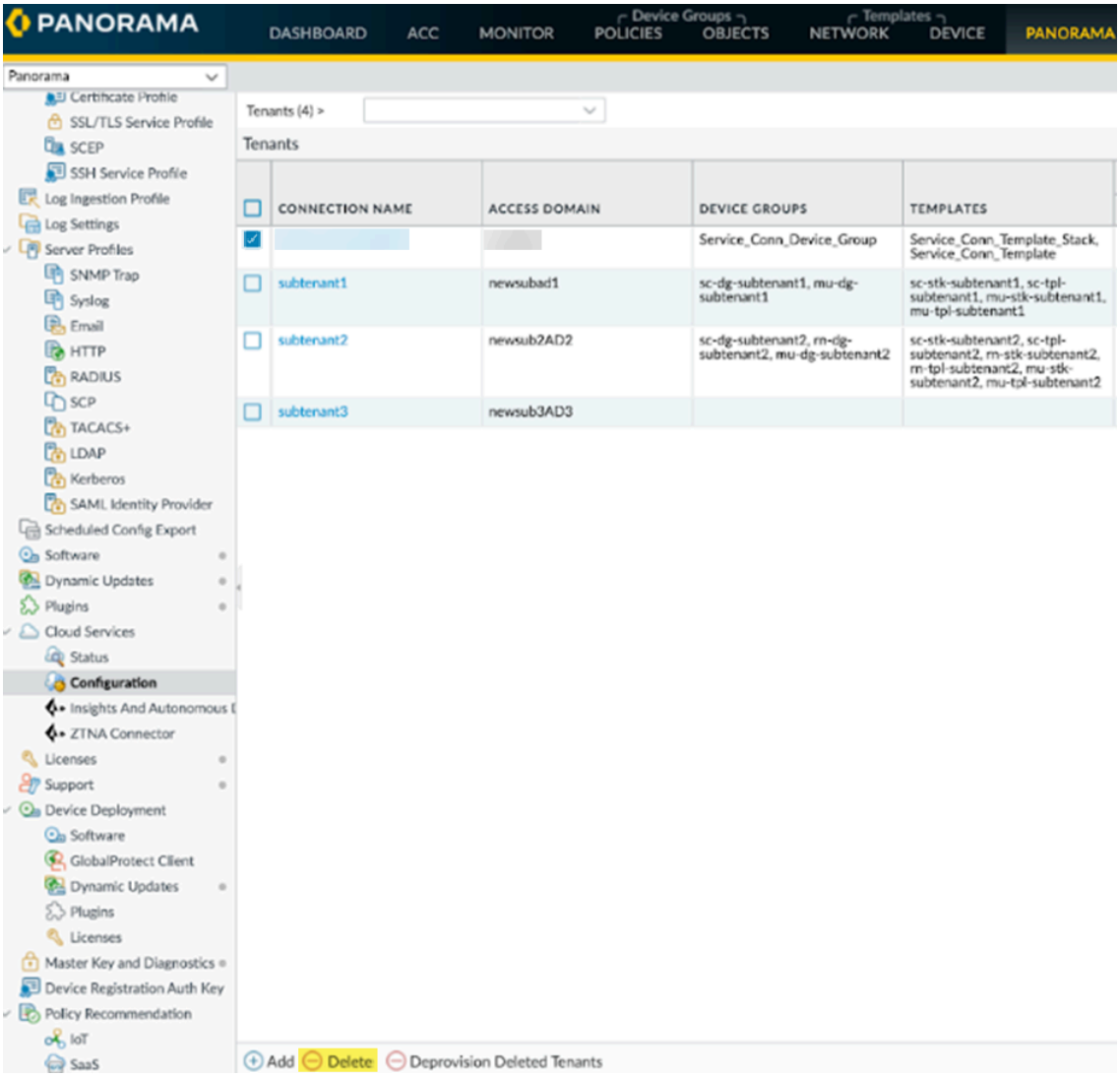
テナントを削除すると、Panoramaからテナントが削除されますが、Prisma Accessインフラストラクチャからは削除されません。テナントを削除してインフラストラクチャから削除する

©2025 Palo Alto Networks, Inc.

には、次の手順に示すように、テナントを削除し、ローカル コミットを実行してから、プロビジョニング解除します。

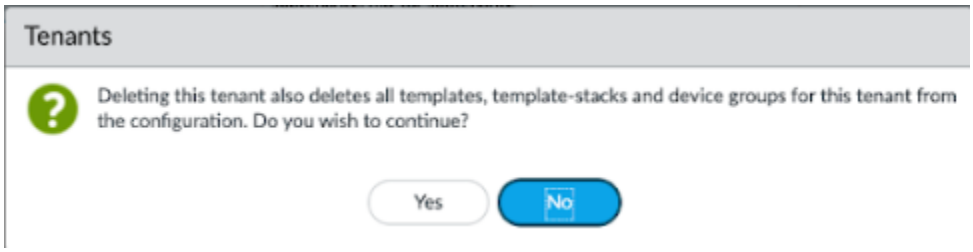
テナントを削除してもプロビジョニング解除を行わない場合でも、Palo Alto Networksのサポートに連絡してテナントを取得できます。

PanoramaをHA構成でセットアップしている場合は、HAペアの[Active Panorama]からのみ削除およびプロビジョニング解除操作を実行します。



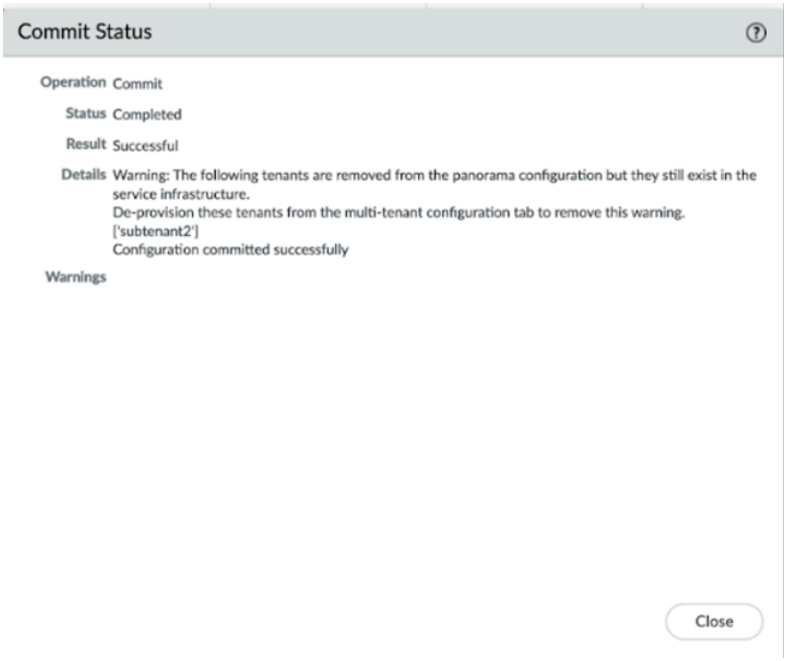
ポップアップ ウィンドウが表示され、テナントの削除プロセスを確認します。続行する場合は **Yes**をクリックし、削除をキャンセルする場合は**No**をクリックします。

©2025 Palo Alto Networks, Inc.



STEP 5 | Panorama にローカルで変更をコミットするには、 **[Commit (コミット)] > [Commit to Panorama (Panoramaにコミット)]**そして変更を[コミット]します。

ローカル コミット後、テナントは削除マークが付けられ、テナント リストから削除されるが、Prisma Accessインフラストラクチャからは削除されません。削除されたテナントを示すポップアップが表示されます。



 ©2025 Palo Alto Networks, Inc.

STEP 6 | (任意) Prisma Accessインフラストラクチャからテナントを完全に削除するには、**[Deprovision Deleted Tenants**（削除したテナントのデプロビジョン）**]**を実行します。

テナントのプロビジョニング解除:

- 設定とPrisma Accessインフラストラクチャから削除します。消去したものは取り戻すことができません。
- テナントに割り当てられたライセンスを再取得します。



確認メッセージが表示され、デプロビジョニングされるテナントの名前が表示されます。テナントのデプロビジョニングを続行する場合は［**OK**］をクリックし、操作をキャンセルする場合は［キャンセル］をクリックします。

テナントのプロビジョニングを解除すると、テナントとそれに割り当てられているすべてのリソースが完全に削除され、これらのテナントに割り当てられていたライセンスが回復します。テナントを取得できません。

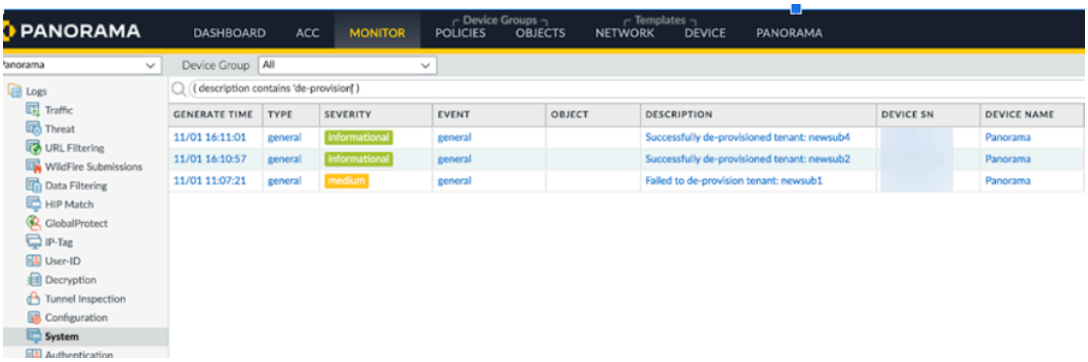


プロビジョニングを解除する必要のあるテナントがない場合は、次のメッセージが表示されます。



 ©2025 Palo Alto Networks, Inc.

STEP 7 | (任意) デプロビジョニング操作のステータスを確認するには、**[Monitor (モニター)]** > **[Logs (ログ)]** > **[System (システム)]** を開きます。プロビジョニング解除操作とテナントの名前がログに表示されます。



©2025 Palo Alto Networks, Inc.

テナントレベルの管理ユーザーの作成

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)での複数のテナントを管理する方法については、Prisma SASEを参照してください。	❑ Prisma Accessのライセンス

各テナントの管理ユーザーを作成する必要があります。テナントレベルの管理者は、各自のテナント設定を表示、変更できますが、他のテナントにアクセスすることはできません。特定のテナントの管理ユーザーを作成するには、次の作業を行います。テナントレベルの管理ユーザーの役割ベースのアクセス制御（RBAC）については、テナントレベルの管理ユーザーに対するロールベースアクセスの制御を参照してください。

単一テナントを管理しているユーザーは、***Monitor***（監視） > ***Logs***（ログ） > ***System***（システム）を選択できないため、システムログを参照することはできませんこの制限は、管理用ロール***Device Group and Template***（デバイスグループとテンプレート）を持つすべての管理者に適用されます。マルチテナントモードでシステムログを参照できるのは、*superuser* のみになります。

©2025 Palo Alto Networks, Inc.

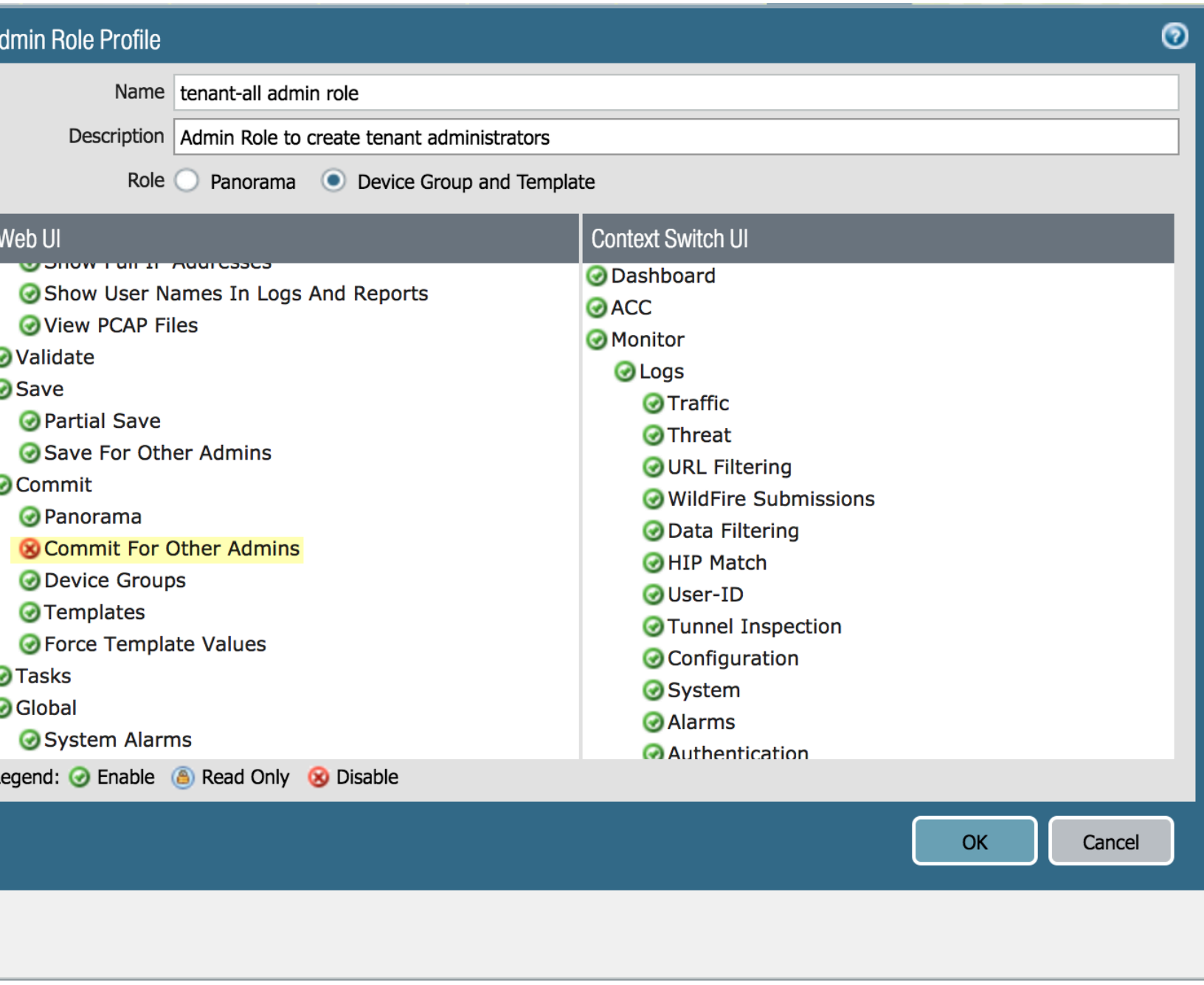
STEP 1 | タイプが**Device Group and Template**（デバイスグループとテンプレート）の、管理用ロールを作成します。

1. **Panorama > Admin Roles**（管理用ロール）の順に選択します。
2. **Role**（ロール）が**Device Group and Template**（デバイスグループとテンプレート）の、管理用ロールプロファイルを**Add**（追加）します。
3. **OK** をクリックします。

単一の管理用ロールプロファイルを作成して、それを複数のテナント間で共有できます。ただし、各テナントに対して個別の管理者を作成する必要があります。

組織ニーズに合わせて管理用ロールを編集できますが、***Commit for Other Admins***（他の管理者のためにコミット）の選択は解除することをお勧めします。この項目の選択を解除すると、テナントレベルのユーザーは各自が行った変更のみをコミットでき、まだコミットされていない他のテナントレベル管理ユーザーの変更を、意図せずにコミットしてしまうことを防止できます。

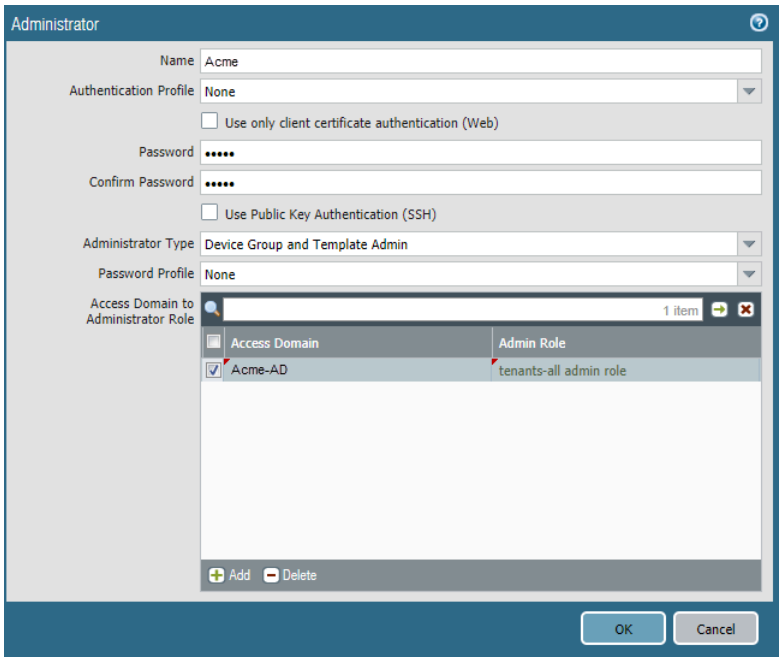
©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

STEP 2 | テナントの管理者を作成、設定します。

1. **Panorama** > **Administrators** [管理者]
2. 管理者を**Add**（追加）します。
3. 新しい管理者の**Password**（パスワード）を入力、再入力します。
4. **Administrator Type**（管理者タイプ）に**Device Group and Template Admin**（デバイスグループとテンプレート）を指定します。
5. テナントのデバイスグループと関連する**Access Domain**（アクセスドメイン）を指定します。
6. ステップ1で作成した、テナント用の**Admin Role**（管理用ロール）を指定します。



STEP 3 | **OK** をクリックします。

STEP 4 | 必要に応じてステップ2およびステップ3を繰り返し、テナントを管理するその他のユーザーを追加します。

STEP 5 | **Commit**（コミット） > **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

©2025 Palo Alto Networks, Inc.

テナントレベルの管理ユーザーに対するロールベースアクセスの制御

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)での複数のテナントを管理する方法については、Prisma SASEを参照してください。	❑ Prisma Accessのライセンス

マルチテナントデプロイ環境を管理する場合、ロールベースのアクセス制御（RBAC）を使ってテナントレベルの管理ユーザーを作成することができます。

Panoramaで、テナントレベル管理ユーザーのRBACレベルのアクセスを変更するには、テナントレベルの管理ユーザーを作成します。**Role**（ロール）が**Device Group and Template**（デバイスグループ）で、Panorama **Web UI**エリアへのアクセスを**Enable**（有効）にする、**Disable**（無効）にする、または**Read Only**（読み取り専用）にした、管理用ロールプロファイルを使用します。テナントレベルユーザーのすべてのPanoramaコンポーネントへのアクセスを管理するには、この方法を使用してください。ただし、Prisma Accessを管理しているCloud Servicesプラグインへのアクセスは例外です。

テナントレベルのユーザーによる、Panorama内のPrisma Accessコンポーネントの設定を制限したい場合は、管理用ロールを使用できません。Prisma Access固有の設定作業を禁止する場合は、Cloud Servicesプラグインへのユーザーによるアクセスを防止する必要があります。この場合、参照することもできなくなります。この方法を利用して、セキュリティポリシーを変更し、変更内容をPanoramaにプッシュする権限を持つセキュリティプロフェッショナル向けの管理ユーザーを作成できますが、Prisma Access設定を表示、変更することはできません。

ユーザーの*Cloud Services*プラグインへのアクセスを有効化/無効化できますが、ユーザーに読み取り専用アクセスを与えることはできません。ユーザーが*Cloud Services*プラグインを表示するアクセス権を保有していると、ユーザーはそのコンポーネント（*Prisma Access*も含む）の設定も変更できてしまいます。

テナントレベルの管理用ロールのサンプルと、それらのロールを作成するための手順を次の表に示します。

サンプルのテナントレベル設定	設定作業
ネットワークに特化したユーザーを作成します。 • プラグイン設定を編集できるユーザー • Panoramaにコミットできるユーザー	テナントレベルの管理ユーザーを作成し、**Admin Role Profile**（管理用ロールプロファイル）で**Save**（保存）および**Commit**（コミット）権限を有効にして、テナントレベルの管理ユーザーに与えたくない権限を無効にするか、または**Read Only**（読み取り専用）にします。

©2025 Palo Alto Networks, Inc.

サンプルのテナントレベル設定	設定作業
• 設定をPrisma Accessにプッシュできるユーザー	
セキュリティに重点を置いたユーザーを作成します。 • セキュリティポリシーの表示と変更ができるユーザー • Panama にコミット可能なユーザー • クラウドサービスプラグインの表示や変更ができないユーザー • 設定をPrisma Accessにプッシュできないユーザー (設定をプッシュするにはスーパーユーザーが必要です)	テナントレベルの管理ユーザーがプラグインを表示、またはプラグインにアクセスすることを防止するために、テナントレベル管理者に対するプラグインアクセスを削除してください。他のPanorama関連権限については、そのユーザーの管理用ロール権限を変更してください。
以下の権限を持つハイブリッドユーザーを作成します: • クラウドサービスプラグインへの読み取り専用アクセス権を持つユーザー • セキュリティポリシーへの読み取り/書き込みアクセス権を持つユーザー • 構成をPrisma Accessにプッシュできないユーザー (設定をプッシュするにはスーパーユーザーが必要です)	この設定は不可能です。Cloud Servicesプラグインを読み取り専用にはできません。管理者ユーザーのみにアクセス権を付与して、それを表示して構成変更を行うようにするか、管理者による表示を禁止することができます。

テナントレベル管理ユーザーのプラグインアクセスの削除

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)での複数のテナントを管理する方法については、Prisma SASEを参照してください。	☐ Prisma Accessのライセンス

通常のマルチテナント構成では、アクセス ドメインテナントをPrisma Accessに追加するを使用して、各アクセス ドメインをテナントに関連付けます。テナント レベルの管理ユーザー

©2025 Palo Alto Networks, Inc.

がPrisma Accessを表示または構成変更できないようにする場合、アクセス ドメインを作成しても、そのドメインをテナントとは関連付けないようにします。

テナントのデバイスグループとテンプレートスタックにアクセスドメインを関連付けるため、テナントレベルの管理ユーザーはテナントレベルのRBACアクセスを保有しており、テナントの設定のみを行えます。アクセスドメインをPrisma Access内のテナントに関連付けていないため、アクセス ドメインはPrisma Accessへのアクセスを提供する、Cloud Servicesプラグインを参照できません。このように、Prisma Accessへのアクセス、表示、設定の変更を禁止しながら、テナント レベルの設定作業を行えるユーザーを作成します。

管理レベルユーザーのPrisma Accessへのアクセスを削除するには、次の作業を行ってください。

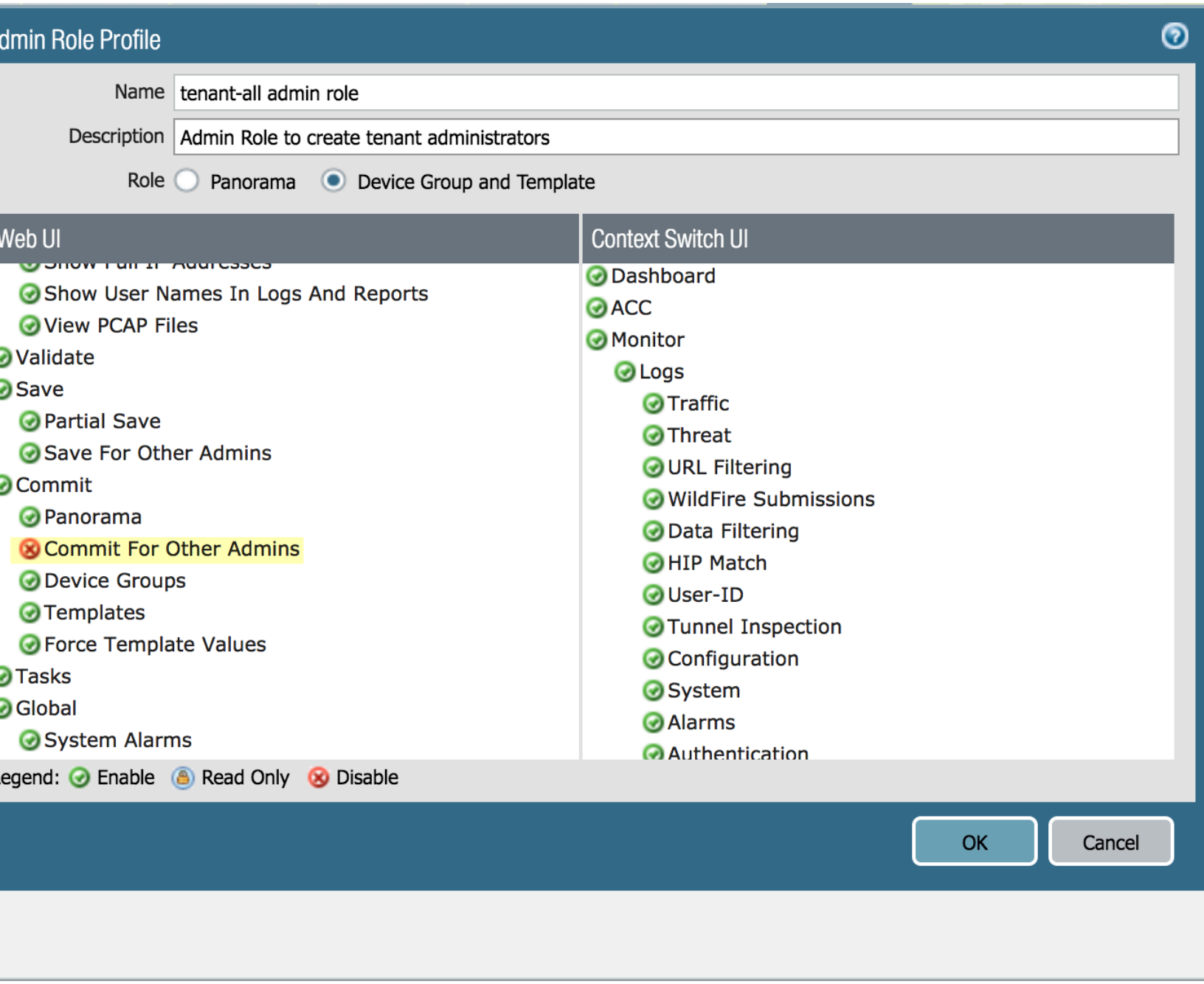
このタスクは、テナントをPrisma Accessに追加するテンプレート、テンプレートスタック、およびデバイスグループを保有していることを前提にしています。これらは、テナントレベルの管理ユーザーと関連付けます。

©2025 Palo Alto Networks, Inc.

STEP 1 | タイプが**Device Group and Template**（デバイスグループとテンプレート）の、管理用ロールを作成します。

1. **Panorama** > **Admin Roles**（管理者ロール）の順に選択します。
2. **Role**（ロール）が**Device Group and Template**（デバイスグループとテンプレート）の、管理者ロール プロファイルを**Add**（追加）します。
3. **OK** をクリックします。

   単一の管理者ロールプロファイルを作成し、それを複数のテナントで共有することができます。

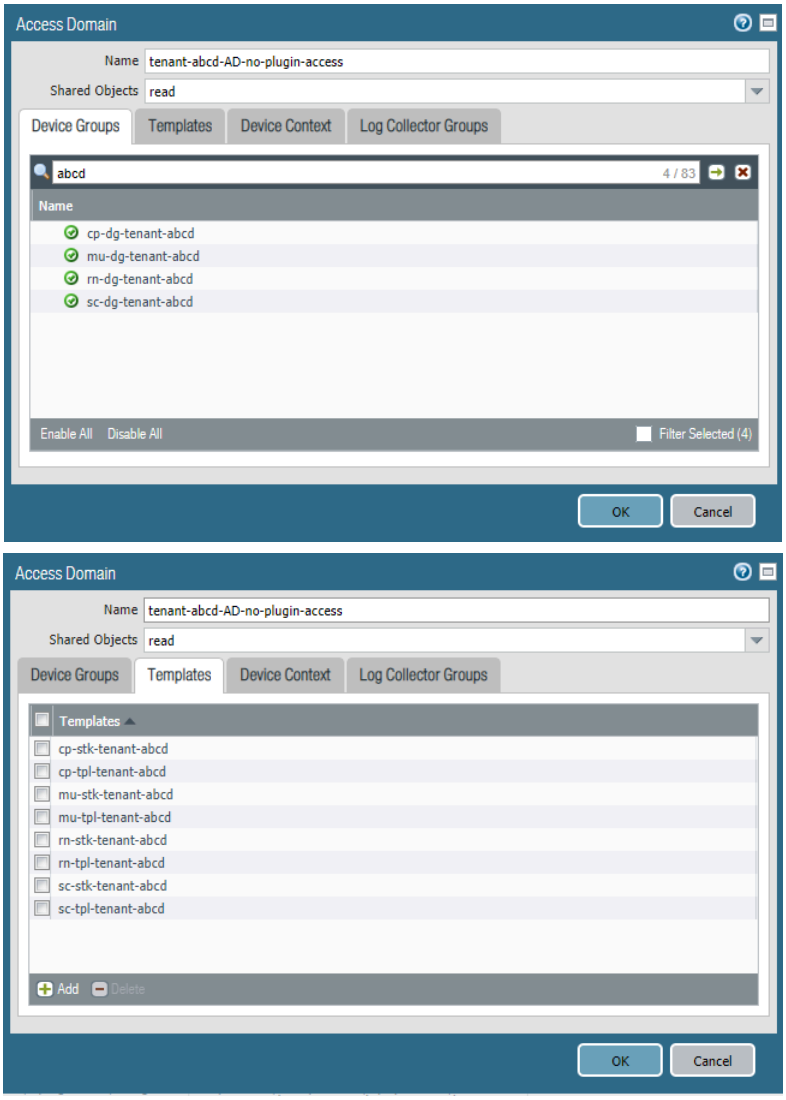


 ©2025 Palo Alto Networks, Inc.

STEP 2 | **Panorama > Access Domain**（アクセスドメイン）の順に選択して、アクセスドメインを**Add**（追加）します。

STEP 3 | テナントに関連付ける**Device Groups**（デバイスグループ）と**Templates**（テンプレート）を指定します。

Shared（共有）親デバイスグループ下の他のデバイスグループの子または孫となるデバイスグループを作成している場合、最下位の階層レベルにあるデバイスグループのみを選択してください。親は選択しないでください。親を選択すると、コミット時にエラーが発生します。

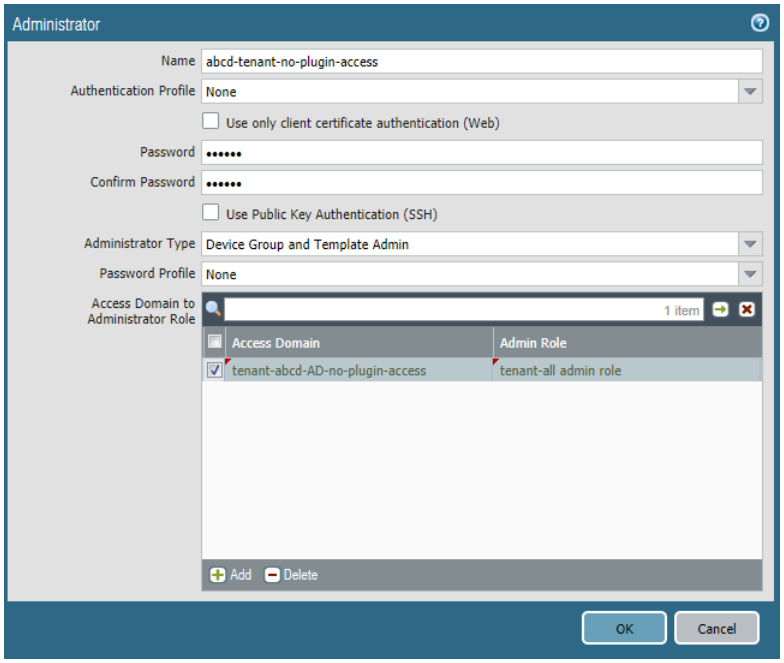


 ©2025 Palo Alto Networks, Inc.

STEP 4 | テナントレベル管理ユーザー用の管理者を作成、設定し、先ほど作成したアクセスドメインを指定します。

1. **Panorama** > **Administrators** [管理者]
2. 管理者を**Add**（追加）します。
3. 新しい管理者の**Password**（パスワード）を入力、再入力します。
4. **Administrator Type**（管理者タイプ）に**Device Group and Template Admin**（デバイスグループとテンプレート）を指定します。
5. テナントのデバイスグループと関連する**Access Domain**（アクセスドメイン）を指定します。
6. 手順1でテナントに作成した管理者ロールを指定します。

   この例を完了すると、**abcd-tenant-no-plugin-access**管理ユーザーには、管理用ロールプロファイルの定義内容に基づいた権限が与えられますが、Cloud Servicesプラグイン（Prisma Accessを含む）を参照、編集することはできません。また、クラウドに対して行った変更をプッシュできないことに注意してください。



STEP 5 | **Commit**（コミット） > **Commit to Panorama**（**Panorama** へのコミット）の順に選択し、変更を **Commit**（コミット）します。

©2025 Palo Alto Networks, Inc.

マルチテナント デプロイメントでのデバイス グループIDによるログのソート

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)での複数のテナントを管理する方法については、Prisma SASEを参照してください。	❑ Prisma Access ライセンス

Panoramaでテナント別にログを手動でソートするには、**[Monitor**（監視）**]** > **[Logs**（ログ）**]**の順に選択して、そのテナントに関連する**[Device Group**（デバイスグループ）**]**を選択し、そのデバイスグループのログを表示します。ただし、ログを外部デバイスに転送している場合、それらのログをテナントレベルでソートしなければならないことがあります。そのためには、デバイスグループに関連しているデバイスグループIDを探して、そのグループIDとデバイスグループのマッピングを使ってログをテナントと関連付けます。

ログには、デバイスグループに関連する4つのフィールドがあります。**DG** 階層レベル **1**、**DG** 階層レベル **2**、**DG** 階層レベル **3**、および **DG** 階層レベル **4**。これらのフィールドが、その階層内でのデバイスグループIDを表しています。共有デバイス グループ (レベル 0) はこの構造には含まれません。

DG 階層レベル **1** は、 階層内の最初のデバイス グループ レベルを指します。子または孫デバイス グループを追加した場合、**DG Hierarchy Level 2**～**DG Hierarchy Level 4**のフィールドが、それぞれ子～ひ孫グループの階層を表します。

テナント別にログを検索するには、以下のタスクを実行します。

STEP 1 | デバイスグループに関連するデバイスグループIDを探します。

- CLIコマンドを使ってこの情報を探すには、Panoramaにsuperuser（管理者レベルのユーザー）としてログインし、設定モードで`show readonly`コマンドを入力して、見出

©2025 Palo Alto Networks, Inc.

し**device-group**の値を参照します。デバイスグループのIDは、デバイスグループ名の下に表示されます。次の例で、デバイスグループ**acme-sc**のデバイスIDは、**20**です。

これらのデバイスグループは、階層内の第1レベル（**DG Hierarchy Level 1**）にあることに注意してください。この情報は、次のステップでクエリに使用します。

```
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 {
```

- APIクエリを使用するには、次のAPIコマンドを入力します：

```
/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>
```

ログへの*API*の使用の詳細は、ログの取得（API）を参照してください。

STEP 2 | ログをテナントと関連付けるには、デバイスグループIDとデバイスグループ名のマッピングを使用します。

STEP 3 | 転送するログを選択する、**Forwarding**（転送）パラメータを**Add**（追加）します。

©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

FedRAMP環境でのPrisma Access

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス ❑ クラウド サービス プラグイン バージョン 3.2.1-h94+、4.0.0-h88+、4.1.0-h58+、5.0.0-h31+

Federal Risk and Authorization Management Program（FedRAMP）は、米国政府全体のプログラムであり、政府ユーザー向けにクラウド製品およびサービスのセキュリティ評価、認可、継続的な監視のための標準化されたアプローチを提供しています。Palo Alto Networksは、Prisma Access (Managed by Panorama)向けのFedRAMP Moderate準拠を実証しています。FedRAMP Moderateに準拠するためのPrisma Accessの設定方法については、以下のトピックをお読みください。

Prisma Accessのようなクラウドベースのサービスについて、米国政府は、機密性、完全性、および可用性が失われた場合に、省庁の業務、資産、または個人に深刻な悪影響が及ぶような、*[Moderate (中程度)]*と呼ばれる特定の保証レベルを要求しています。深刻な悪影響には、代理店の資産に対する重大な運用上の損害、金銭的損失、または人命や身体の損失ではない個人への危害が含まれる可能性があります。

Prisma AccessはFedRAMP Moderateの要件に準拠しており、連邦政府からAuthorization to Operate（ATO）を取得しています。FedRAMP Moderate準拠を保証するために、以下のトピックに記載されている要件とガイドラインを使用してPrisma Accessをインストールおよび設定する必要があります。

Prisma Access FedRAMP要件

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス ❑ クラウド サービス プラグイン バージョン 3.2.1-h94+、4.0.0-h88+、4.1.0-h58+、5.0.0-h31+

FedRAMPは、米国政府が使用するプログラムであり、クラウド サービス オファリング (CSO) のコンプライアンスに対する標準的なアプローチを提供します。Prisma Access (Managed by Panorama) AccessがFedRAMP Moderateに準拠していることを確認するために、インストール、アク ティブ化、初回設定、およびPrisma Accessの設定を行う際には、以下のガイドラインと要件にならってください。

事前インストールおよび製品アクティベーションの要件

Prisma Accessのデプロイメントがコンプライアンスに適合していることを確認するために、以下のインストー ルおよび製品のアクティベーション要件に従ってください。

- インストール前の要件:
  - デプロイメント タイプ（新規または既存）- 新規のPrisma Accessデプロイメントはは FedRAMP Moderate環境でサポートされています。既存のPrisma Accessデプロイメントから FedRAMP ModeratePrisma Accessデプロイメントへのアップグレードはサポートされていません。
  - 必要な**SKU**- FedRAMP Moderateデプロイメントのために Prisma Accessを購入する場合、Prisma AccessはFedRAMP環境に特化したSKUを必要とします。認定され Palo Alto Networks担当者またはパートナーと協力して、FedRAMP Moderateデプロイメントに適切なSKUを購入していることを確認してください。
  - 必要なPanorama、プラグイン、PAN-OS データプレーンのバージョンに記載されているPanoramaバージョン、GlobalProtectバージョン、Cloud Servicesプラグインバージョンのみを使用してください。
  - 許可リスト**Strata Logging Service**パブリック**IP**アドレス- Strata Logging Service連邦地域が使用しているIPアドレスブロックは34.67.50.64/28です。企業で許可リストを使用している場合は、以下のIPアドレスを許可リストに追加し、Strata Logging ServiceがPrisma Accessからログを受信できるようにしてください。
  - **API URL**の変更-Prisma Accessが使用するパブリック IP アドレスを取得するために APIスクリプトを実行する場合、APIのURLを **`https://api.gpcloudservice.com/GetPrismaAccessIP/v2`** から **`https://api.fed.prismaaccess.com/GetPrismaAccessIP/v2`** に変更します。

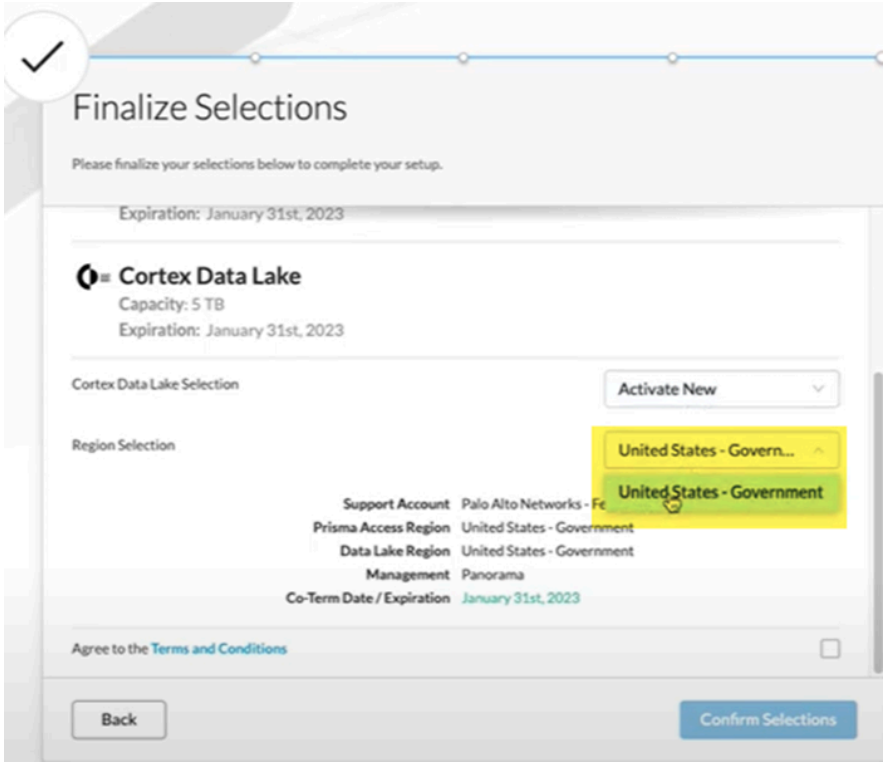
    Panoramaアプライアンスが プロキシサーバー （**Panorama** > セットアップ > サービス > プロキシサーバー）を使用している場合、またはPrisma AccessでSSLフォワード プロ

©2025 Palo Alto Networks, Inc.

キシ復号化を使用している場合は、 プロキシまたはプロキシ サーバーの許可リストに api.fed.prismaaccess.com URL を必ず追加してください。

- **GlobalProtect**ポータル名の変更- Prisma Access FedRAMP Mobile Users-GlobalProtectデプロイメントのデフォルトのポータルホスト名は、FedRAMP以外のデプロイメントとは異なります。ポータル名は*<portal-name>*.fed.prismaaccess.com. の代わりに*<portal-name>*.gpcloudservice.com です。
- サポート要件—Prisma AccessFedRAMP Moderateには、米国国内の米国人職員に対する24時間365日のサポートを含む Palo Alto Networks米国政府サポート サービスが必要です。

- アクティベーション要件- Prisma Accessデプロイメントのアクティベーションとインストールは、FedRAMP以外のデプロイメントと同様です。ただし、製品のアクティベーション中に、**Strata Logging Service**リージョンとして米国政府 を選択する必要があります。



必要なPanorama、プラグイン、PAN-OS データプレーンのバージョン

Prisma AccessがFedRAMP Moderate要件に準拠していることを確認するために、Prisma Access (Managed by Panorama)のデプロイメントで次のPanorama、Cloud Servicesプラグイン、およびGlobalProtectのバージョンを使用していることを確認してください。

コンポーネント	必要なバージョン
Panorama PAN-OS バージョン	10.2.8-h3またはそれ以降の10.2.8ホットフィックスPAN-OSバージョン

©2025 Palo Alto Networks, Inc.

コンポーネント	必要なバージョン
	10.2.9-h1またはそれ以降の10.2.9ホットフィックスPAN-OSバージョン Prisma Accessを管理するPanorama上で処理基準とコモンクライテリア（FIPS-CC）を有効にすることは、FedRAMPの 管理に沿った推奨されるベストプラクティスである。PanoramaでFIPS-CCサポートを有効にするには メンテナンス リカバリ ツール (MRT)にアクセスする必要があります。 インストールとアクティベーションのプロセスを簡素化するために、*Panorama* を登録し、ライセンスをインストールし、カスタマー サポート ポータル (CSP)でサポート ライセンスをアクティベートしている場合は、*FIPS* モードで既に構成済みの既存の *Panorama* を選択できます。*Panorama*のシリアルナンバーを*Prisma Access*をデプロイするのと同じ*CSP*アカウントに追加している場合は、インストール中にこの*Panorama*アプライアンスのシリアル番号を選択できます。 別のPrisma AccessまたはStrata Logging Serviceデプロイメントの管理に使用されたPanoramaは使用できません。
Cloud Servicesプラグインのバージョン	• 3.2.1-h94+ • 4.0.0-h88+ • 4.1.0-h58+ • 5.0.0-h31+
GlobalProtectバージョン	5.1.4+ and 6.0.7+ 5.1.4はFIPS認定されており、連邦政府ベースのデプロイメントで使用するデフォルトのバージョンです。デフォルトのGlobalProtectバージョンを5.1.4から変更した 場合、Panorama UIからバージョン5.1.4を選択することはできません。再度追加するに

©2025 Palo Alto Networks, Inc.

コンポーネント	必要なバージョン
	は、Palo Alto Networksテクニカル サポートにサポート ケースを発行してください。

Prisma AccessがサポートするFedRAMPロケーション

以下の場所は、FedRAMP Moderate環境でPrisma Accessを使用することが許可されており、米国本土（CONUS） および米国本土外（OCONUS）の場所に対するサポートも含まれています：

- オーストラリア南東部
- ベルギー
- Brazil South（ブラジル南部）
- Canada East（カナダ東部）
- フィンランド
- Germany Central（ドイツ中部）
- India West（インド西部）
- Japan Central（日本中部）
- Japan South（日本南部）
- Netherlands Central（オランダ中部）
- シンガポール
- スイス
- 台湾
- 英国
- US Central（米国中部）
- US East（米国東部）
- US Northwest（米国北西部）
- US Southeast（米国南東部）
- US Southeast（米国南西部）

Prisma Access FedRAMPデプロイメントにおけるサポートされる機能とサポートされない機能

プライベートアプリアクセスのIPv6サポートは、Prisma AccessFedRAMP Moderate環境でサポートされています。

以下のアプリと機能は、Prisma Access FedRAMP Moderate環境での使用はサポートされていません。

- Prisma Access インサイト（知見）

©2025 Palo Alto Networks, Inc.

- 自律型 DEM
- 明示型プロキシ
- Clean_Pipe用のPrisma Access
- Enterprise DLP
- IoTセキュリティ
- SaaSセキュリティ インライン サポート - 可視性

©2025 Palo Alto Networks, Inc.

FedRAMP環境でPrisma Accessを設定する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス ❑ クラウド サービス プラグイン バージョン 3.2.1-h94+、4.0.0-h88+、4.1.0-h58+、5.0.0-h31+

要件が完了したら、次のステップを実行して FedRAMP Moderate 環境のPrisma Accessデプロイメント設定を完了します。

開始する前に、*Panorama*アプライアンスを*FIPS-CC*モードで構成することや、*Panorama*、クラウド サービス プラグイン、*GlobalProtect*に必要な特定のバージョンなど、*Prisma Access FedRAMP*デプロイメントに固有の要件とガイドラインをメモしておきます。

STEP 1 | FedRAMPデプロイメント専用のカスタマー サポート ポータル（CSP）アカウントがあることを確認してください。

単一のCSPアカウントでFedRAMPと非FedRAMPのデプロイメントを行うことはできません。このため、Palo Alto Networksでは、FedRAMPアカウント専用に 新しい CSP アカウントを作成する ことをお勧めします。

STEP 2 | Prisma Access FedRAMP環境で使用できるようにPanoramaアプライアンスを準備します。

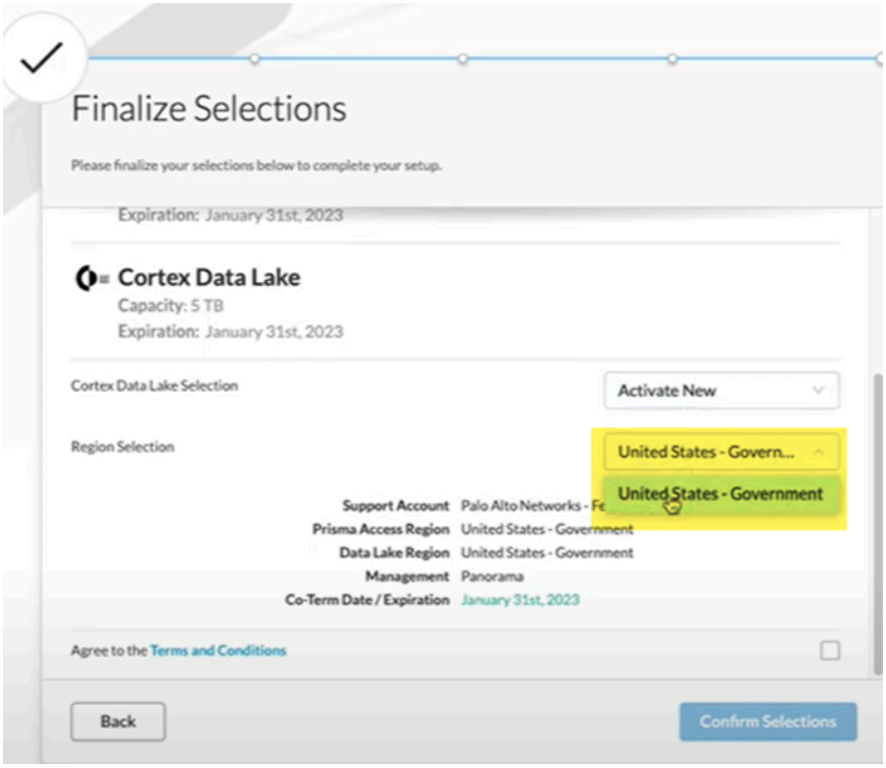
1. Panoramaアプライアンス (M-Seriesアプライアンス または 仮想アプライアンス)をインストールします。
2. (任意、推奨) Panorama アプライアンスでFederal Information Processing Standard (連邦情報処理標準 - FIPS)および共通基準 (FIPS-CC) のサポートを有効にします。

   FIPSサポートを有効にするには、メンテナンス リカバリ ツール (MRT)にアクセスする必要があります。
3. Panoramaのバージョンを必要なPanorama、プラグイン、PAN-OS データプレーンのバージョンに記載されているバージョンにアップグレードします。

©2025 Palo Alto Networks, Inc.

STEP 3 | ライセンス要件を確認し、Prisma Accessライセンスコンポーネントをアクティベートしてインストールします。

製品のアクティベーション時に、**Strata Logging Service**の地域を**United States-Government (米国政府)** から選択します。



STEP 4 | Prisma Accessを管理するPanoramaアプライアンスと一緒に使用する、任意のセキュリティアプライアンスの許可リストに、次のURLとポート、IPアドレスを追加します。

また、Panoramaアプライアンスがプロキシサーバーを使用している場合（**[Panorama] > [Setup**（セットアップ）**] > [Service**（サービス）**] > [Proxy Server**（プロキシサーバー）**]**）、またはPrisma AccessでSSLフォワード プロキシを使用している場合、プロキシまたはプロキシサーバーの許可リストに、次のURLとポート、およびIPアドレスを忘れずに追加してください。

- api.gpcloudservice.com （Prisma Access用）
- api.paloaltonetworks.com （Prisma Access用）
- api.fed.prismaaccess.com （Prisma Access用）
- apitrusted.paloaltonetworks.com （Prisma Access用）
- Strata Logging Serviceに必要なFQDNとポート
- 34.67.50.64/28

  使用されるIPアドレスブロックは、 Strata Logging Service連邦地域は34.67.50.64/28です。これらのIPアドレスを許可リストに追加し、Strata Logging ServiceがPrisma Accessからログを受信できるようにします。
- Panoramaで使用されるポート。

©2025 Palo Alto Networks, Inc.

STEP 5 | カスタマー サポート ポータル（CSP）でケースを開き、Palo Alto NetworksにStrata Logging Serviceの送信元ポートと宛先ポートのリストを許可してもらいます。

Prisma Access環境でStrata Logging Serviceを使用するには、Palo Alto Networksがソースおよび宛先ポートを内部的にリストすることを許可するように、ケースを作成する必要があります。

STEP 6 | デバイス > セットアップ > **WildFire** 選択し、**`wildfire.gov.paloaltonetworks.com`**と入力します。

FedRAMPのデプロイメントでは、WildFire U.S.を使用する必要があります。政府専用クラウド。

STEP 7 | デプロイメントに必要な場合は、モバイル ユーザーをオンボードし、GlobalProtect 使用して保護します。

サービスがセットアップされており、ユーザーがインターネットにアクセスできることを検証する最初のステップとして、ローカル認証を使用することをお勧めします。後ほど、ご自分の企業の認証手段に切り替えることができます。

1. GlobalProtectモバイル ユーザーをセットアップします。
2. モバイルユーザー向けにゾーンを設定します。
   1. Mobile User Template（モバイルユーザーテンプレート）で、2つのゾーンを作成します。たとえば、Mobile-Users（モバイルユーザー）とInternet（インターネット）を設定します。
   2. ゾーンをマップします。Prisma Access接続ユーザ、HQまたはブランチ オフィス以外のゾーンを[Untrust (信頼できない)]にマッピングします。

      Panorama > **Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Mobile Users**（モバイルユーザー）下で、[Internet (インターネット)]を[Untrust (信頼できない)]に、[Mobile-Users (モバイルユーザー)]を[Trust (信頼できる)]にマッピングします。
3. デバイスグループのセキュリティポリシーを設定します。

   インターネットへのトラフィックを許可するセキュリティポリシーを作成するには、Mobile_User_Device_Groupを選択し、**Policies**（ポリシー） > **Security**（セキュリティ） > **Prerules**（プレルール） > **Add**（追加）を選択して、ルールを追加します。以下に例を示します。Mobile-Users to Internet。
4. サービスを開始するには、変更をコミットしてプッシュします。
   1. Panoramaでローカルに**Commit**（コミット）します。
   2. Prisma Accessに**Commit and Push**（コミットしてプッシュ]します。
   3. **[Panorama]** > **[Cloud Services**（クラウドサービス）**]** > **[Status**（ステータス）**]** > **[Monitor**（監視）**]** > **[Mobile Users**（モバイルユーザー）**]**の順に選択し

 ©2025 Palo Alto Networks, Inc.

て、**[Status**（ステータス）**]**を参照し、ポータルのFQDNにpingできることを確認します。

5. Prisma Accessがモバイルユーザーのインターネットトラフィックを保護していることを確認します。
   1. GlobalProtectアプリをダウンロード、インストールします。
   2. アプリを使って、ポータルにモバイルユーザー（ローカルユーザー）として接続します。
   3. インターネット上のいくつかのWebサイトを参照して、Panoramaのトラフィックログを確認します。

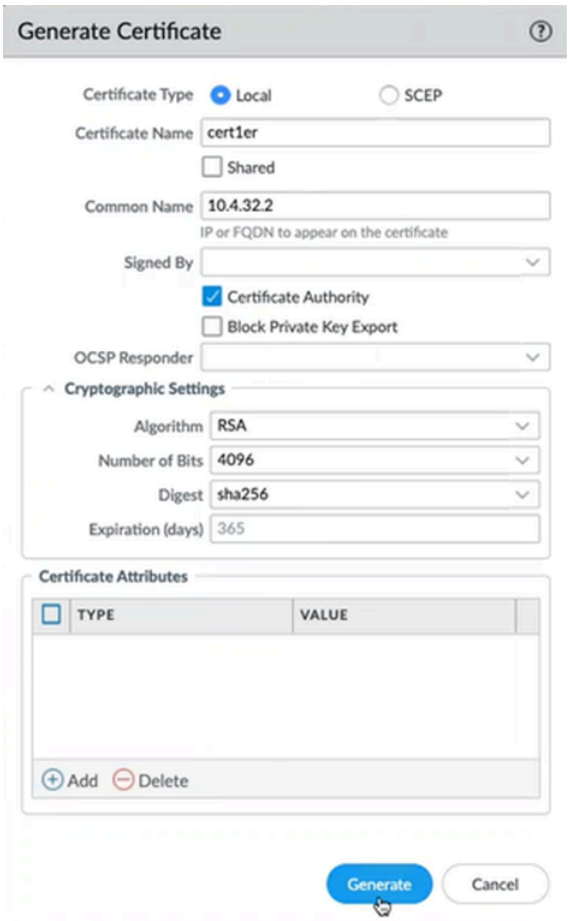
©2025 Palo Alto Networks, Inc.

STEP 8 | (モバイル ユーザー - GlobalProtectデプロイメントのみ) FIPS モードで実行されるPanoramaの要件を満たすモバイル ユーザー - GlobalProtectデプロイメントで認証オーバーライド証明書を作成し、その証明書をデプロイメントに適用します。

モバイル ユーザーのデフォルト証明書 (GlobalProtect、 認証 **Cookie CA**は、FIPS-CC モードで実行されているPanoramaの最小暗号スイート要件を満たしていないため、新しい証明書を生成します。

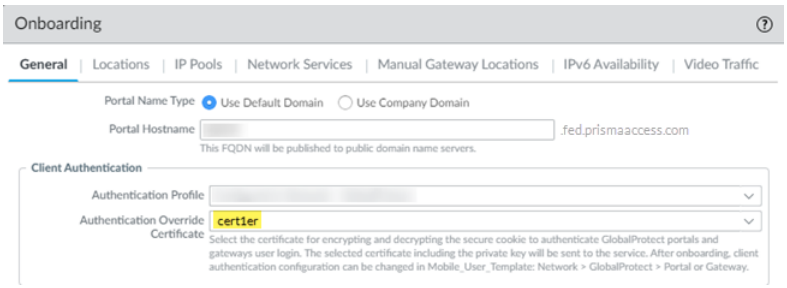
1. Prisma Accessを管理しているPanoramaから、**[Device (デバイス)]** > **[Certificate Management (証明書の管理)]** > **[Certificates (証明書)]** > **[Device Certificates (デバイス証明書)]**を順に選択します。

   Mobile_User_Templateにいることを確認してください。
2. FIPS-CCモードのPanoramaの最小暗号スイート要件を満たす証明書を生成します 。



3. **[Panorama]** > **[Cloud Services]** > **[Configuration (設定)]** > **[モバイル ユーザー - GlobalProtect]**を選択し、 **[ホスト名]**を選択して、 **[クライアント認証]** 領域で、作成した**[認証オーバーライド証明書]** を選択します。

 ©2025 Palo Alto Networks, Inc.



モバイル ユーザー - *GlobalProtect*設定をすでに作成している場合、この領域はグレー表示になります。認証オーバーライド証明書を変更するには、*[*ネットワーク*]* > ***[GlobalProtect]*** > *[*ポータル*]* > を選択します。 ***<portal-config>*** > *[*エージェント*]* > *[*デフォルト*]* > 認証を 選択し、***Cookie*** の暗号化/復号化に使用する証明書の下でこの証明書を選択します。

STEP 9 | Prisma Accessエレメント間の通信を可能にする、サービスインフラとサービス接続を有効にします。

1. サービスインフラとサービス接続の有効化を計画します。
2. サービスインフラを有効にします。
3. 会社のリソースへのアクセスを可能にするサービス接続を作成します。

   会社のリソースへのアクセスが不要な場合でも、モバイルユーザーとリモートネットワーク間のアクセスを有効にするために、サービス接続を作成してください。

STEP 10 | リモートネットワーク接続を計画、作成、および設定します。

1. Prisma Accessに1つまたは複数のリモートネットワークを追加します。

   1つのロケーションをオンボーディングした後、次に一括インポート機能を使ってその他のロケーションを追加することができます。
2. リモートネットワークから本社へのトラフィックを許可するセキュリティポリシーを作成します（例：Trust to Trust）。Trust to Trust (信頼から信頼へ)。
3. サービス接続、リモートネットワーク接続、およびモバイルユーザー間の接続性を確認します。

STEP 11 | Prisma Accessパブリックおよびプライベート IP アドレスを取得します。

企業ネットワーク/アプリケーションへのインバウンドアクセスを制限するために、組織のネットワークの許可リストに、これらのアドレスを追加します。

*Mobile User-GlobalProtect*をデプロイメントしている場合、このAPIの代わりに*Prisma Access*UIを使用してパブリックIPアドレスの割り当てを管理し、*Prisma Access*がIPアドレスを解放する前にIPアドレスが許可リストに追加されていることを確認することができます。このようにして、 *Prisma Access*は許可リストに登録されたIPアドレスのみをプロビジョニングします。

©2025 Palo Alto Networks, Inc.

STEP 12 | （任意） 認証方法をローカル認証から、ご自分の組織の認証方法に変更します。

モバイル ユーザーのSAML認証を設定するには、次のいずれかの方法を使用します。

- モバイル ユーザーデプロイメント用のAzure AD SAML認証を構成する

  この構成のGlobalProtect部分のみを構成し、明示型プロキシ構成は省略します。
- モバイルユーザー向けのIdPとしてOktaを使用してSAML認証を構成する
- モバイルユーザー向けのSAMLプロバイダーとしてADFSを構成する

認証を設定した後、Cloud Identity Engineを使用してユーザーおよびグループ情報を取得することはできますが、Cloud Identity Engine のみを使用してユーザーを認証することはできません。

STEP 13 | （任意） Strata Logging Serviceから外部Syslogレシーバーにログを転送するために、ログ転送アプリをセットアップします。

 ©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

Prisma Access高度なデプロイメント

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

Prisma Accessルーティングとネットワーキングの導入によっては、組織のトポロジとルーティングデバイスを完全に理解し、Prisma Accessルーティングの仕組みを理解する必要があります。このセクションでは、これらの高度なデプロイメントとその設定方法についてお読みください。

サービス接続、モバイルユーザー、およびリモートネットワークに適用される高度な導入:

- デプロイされたPrisma Accessロケーションに新しいコンピュート ロケーションを追加する。
- IPv6 サポート
- モバイルユーザーのためのDNS解決—GlobalProtectとリモートネットワークデプロイメント
- サービス接続およびリモートネットワーク接続用にBGPがモバイルユーザーIPアドレスプールをアドバタイズする仕組み
- Prisma AccessとStrata Logging Serviceのプロキシサポート
- 特定の国からの着信接続をブロックする
- AWS WorkSpaceからの安全なインターネットトラフィック
- デフォルトルートなしネットワークのPrisma Access

サービス接続の高度なデプロイメント:

- サービス接続マルチクラウド冗長性
- トラフィックステアリングを使用したインターネット宛てのトラフィックのサービス接続への転送
- サービス接続トラフィックのルーティング
- 送信元NATを使用したサービス接続のユーザーIDとデバイスIDのマッピングを保持する

モバイルユーザー - GlobalProtect高度なデプロイメント

- Prisma Accessで複数のポータルを構成する
- リモートトラブルシューティングとアップデートのためのダイナミックDNS登録サポート
- モバイルユーザー向けの動的DNS登録サポート - GlobalProtect
- Prisma Access GlobalProtectのデプロイメントにおける侵害されたデバイスの識別と隔離

- モバイル ユーザーのIPv6トラフィックのシンクホール - GlobalProtectのデプロイメント
- Prisma Accessを使用したHIP情報の再配信
- HIPレポートの表示
- クライアントレスVPNでのGzipエンコーディングのサポート
- Prisma Accessでのトラフィック レプリケーション

リモートネットワークの高度なデプロイメント:

- リモートネットワークのロケーションへの安全なインバウンドアクセスの提供
- リモートサイト向けの高帯域幅ネットワークの作成

©2025 Palo Alto Networks, Inc.

デプロイされたPrisma Accessロケーションに新しいコンピュート ロケーションを追加する。

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス

パフォーマンスを最適化し、レイテンシーを改善するために、Prisma Accessは、プラグインのアップグレードの一環として既にデプロイしたロケーションに新しいコンピューティングロケーションをデプロイできます。プラグインをアップグレードしても、既存のコンピューティングロケーションからロケーションへのマッピングは変更されませんが、新しいコンピューティングロケーションを利用することを選択できます。コンピュートロケーションを変更すると、Prisma Accessは、新しいコンピュートロケーションが関連付けられ ているロケーションのゲートウェイおよびポータルIPアドレス（モバイルユーザー用）、およびサービスIPアドレスのサービスエンドポイントアドレス（リモートネットワーク用）を変更します。ネットワークで許可リストを使用して、SaaS アプリケーションや一般にアクセス可能なパートナーアプリケーションなどのインターネットリソースへのアクセスをユーザーに提供する場合は、これらの新しいIPアドレスを許可リストに追加する必要があります。

利用可能になった後、新しいコンピューティング ロケーションにアップグレードするには、次の作業を行ってください。

既存のロケーションの削除と追加、許可リスト (モバイルユーザー用) またはピアIPsecトンネルIPアドレス (リモートネットワークデプロイメント用) の変更には時間をかける必要があるため、Palo Alto Networks では、メンテナンスの時間帯またはピーク時以外にコンピューティングロケーションの変更をスケジュールすることを推奨しています。

モバイル・ユーザー・デプロイメントのダウンタイムを短縮するには、以下の手順を実行する前に、APIを使用して新しいモバイル・ユーザー・ゲートウェイとポータルのIPアドレスを事前に割り当ててください。

STEP 1 | 新しいリモートネットワークコンピューティングロケーションの帯域幅を追加します。

1. (リモートネットワーク帯域幅をコンピューティングロケーションごとにのみ割り当てるリモートネットワークデプロイメント) **[Panorama]** > **[Cloud Services (**クラウドサービス**)]** > **[Configuration (**設定**)]** > **[Remote Networks (**リモートネットワーク**)]** を選択します。
2. 帯域幅割り当て領域の歯車アイコンをクリックし、新しいコンピューティングロケーションの帯域幅割り当て **(Mbps)** を追加します。
3. ページ上部の [割り当てられた合計]フィールドに帯域幅が反映されるまで待ってから、**[OK]**をクリックします。

STEP 2 | (モバイルユーザーデプロイメントのみ) APIスクリプトを使用して新しいゲートウェイとポータルIPアドレスを取得し、許可リストに追加します。

©2025 Palo Alto Networks, Inc.

STEP 3 | 新しいコンピュートロケーションに関連付けられているサービス接続、リモートネットワーク接続、またはモバイルユーザーロケーションを削除します。

STEP 4 | 変更をコミット、プッシュ配信します。

STEP 5 | 削除したロケーションを再度追加します。

STEP 6 | 変更をコミット、プッシュ配信します。

STEP 7 | (リモート ネットワークおよびサービス接続デプロイメントのみ) リモート ネットワーク接続またはサービス接続用のIPsecトンネルの新しいIPアドレスを指すようにCPEを変更します。

リモート ネットワーク接続の場合、**Panorama** > **Cloud Services** (クラウド サービス) > **Status** (ステータス) > **Network Details** (ネットワーク詳細) > **Remote Networks** (リモートネットワーク) を選択し、**Service IP Address** (サービスIPアドレス) をメモし、新しい **Service IP Address** (サービスIPアドレス) をCPE上のリモート ネットワークIPSecトンネルのピアアドレスとして設定します。

サービス接続の場合は、**Panorama** > **Cloud Services** (クラウドサービス) > **Status** (ステータス) > **Network Details** (ネットワーク詳細) > **Service Connection** (サービスコネクション) を選択し、**Service IP Address** (サービスIPアドレス) をメモし、新しい **Service IP Address** (サービスIPアドレス) をCPE上のサービス接続IPSecトンネルのピアIPアドレスとして設定します。

STEP 8 | **Panorama** > **Cloud Services** (クラウド サービス) > **Status** (ステータス) > **Network Details** (ネットワーク詳細) > **Remote Networks** (リモート ネットワーク) を選択し、**Service IP Address** (サービスIPアドレス) をメモし、新しい **Service IP Address** (サービスIPアドレス) をCPE上のリモート ネットワークIPSecトンネルのピアアドレスとして設定します。

リモートネットワーク接続を削除して再度追加すると、Prisma Access側のIPsecトンネルのIPアドレスが変更されます。

STEP 9 | (モバイルユーザーデプロイメントのみ) ロケーションを再マップしたら、新しいGateway FQDNを取得してSAMLプロバイダーの認証設定に追加します。

モバイルユーザーの場所が再マップされると、インフラストラクチャのアップグレード後にゲートウェイのFQDNが変更され、再マッピングが発生し、SAML認証で問題が発生する可能性があります。ゲートウェイ名を検索するには:

- Prisma Access (Managed by Strata Cloud Manager)で、**Workflows** (ワークフロー) > **Prisma Access**セットアップ > **GlobalProtect** > **GlobalProtect**セットアップ > **Infrastructure** (インフラストラクチャ) > **Infrastructure Settings** (インフラストラクチャ設定) を選択し、歯車をクリックしてInfrastructure Settings (インフラストラクチャ設定) を表示し、Gateway FQDNs エリアで名前を変更したゲートウェイをコピーします。
- Prisma Access (Managed by Panorama)で、**Panorama** > **Cloud Services** (クラウドサービス) > **Status** (ステータス) > **Network Details** (ネットワーク詳細) > **Mobile Users — GlobalProtect** を選択し、名前を変更したゲートウェイを [ゲートウェイ] 領域にコピーします。

 ©2025 Palo Alto Networks, Inc.

IPv6 サポート

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンスバージョン2.2以降を推奨 ❑ パブリックおよびプライベートアプリへのネイティブIPv6アクセスには、以下の最小リリースが必要です: • Prisma Access (Managed by Strata Cloud Manager):2024年6月のリリース • Prisma Access (Managed by Panorama):Prisma Access5.1.1は新規デプロイメントのみ。 その他のデプロイメント（既存のPrisma Access (Managed by Panorama)デプロイメントを含む）は、プライベート アプリ アクセスのみをサポートします。

あなたの組織がIPv6アドレスを使用している場合、Prisma Accessによって、IPv6アドレスの背後にある内部（プライベート）アプリにアクセスすることが可能になります。お使いのPrisma Accessバージョンでは、IPv6を使用してプライベート (内部) アプリにアクセスするか、GlobalProtectとリモート ネットワークの両方の内部アプリとパブリック (外部) アプリの両方にアクセスすることができます。

外部アプリへのアクセスについては、いくつかの*Prisma Access*コンポーネントでは、デフォルトでは*IPv6*機能が有効になっていません。パブリックアプリアクセス用にネイティブ*IPv6*を有効にする前に、*Palo Alto Networks*アカウントチームに連絡し、有効化プロセスを開始するための*TAC*チケットをオープンしてください。

ネイティブIPv6サポートの利点の1つは、IPv6のみおよびデュアルスタックエンドポイントのモバイルユーザーが、GlobalProtectを使用してIPv6接続を介してPrisma Accessに接続できることです。もう 1 つの利点は、GlobalProtectとリモート ネットワークが、インターネットの宛先でIPv6接続が必要な場合に、インターネット経由でインターネットおよびパブリック SaaS アプリケーションにアクセスできることです。

IPv6はIPv4よりも大幅に広いアドレス空間を提供し、ほぼ無制限の数の一意のIPアドレスを許可します。同時に、デュアル スタックは、ネットワークとデバイスがIPv4とIPv6の両方を同時に使用して動作できるようにする移行アプローチです。ネイティブIPv6サポートにより、Prisma AccessはIPv6接続とデュアルスタック接続の両方に対応し、IPv4からIPv6への移行プロセスを容易にし、下位互換性を確保し、クラウドとIPv6対応ネットワークへの移行を促進します。

以下のPrisma Accessネットワーク・コンポーネントでIPv6を設定します。

©2025 Palo Alto Networks, Inc.

- IPv6を有効にし、インフラストラクチャ サブネットでIPv6サブネットを指定してIPv6ネットワーク インフラストラクチャを確立し、リモート ネットワーク (ブランチ ロケーション)、モバイル ユーザー、およびサービス接続 (データセンターまたは本社ロケーション) 間の通信を可能にします。

  最良の結果を得るには、プレフィックス長が/64の独自のIPv6 (パブリックまたはプライベート) アドレス プール (例: 3005:10:209:55::/64) を指定します。

- モバイル ユーザー - GlobalProtectデプロイメントの場合、モバイル ユーザーの場所に関連付けられているコンピューティングのロケーションでIPv6ネットワークを使用するかどうかを指定します。

  必要に応じて、IPv6モバイル ユーザーIPアドレス プールとIPv6 DNSサーバー アドレスを指定できます。

  最良の結果を得るには、プレフィックス長が /64（3001:192:168:32::/64 など）で、ワールドワイド レベルに適用された独自のIPv6（パブリックまたはプライベート）アドレス プールを提供します。

  Prisma Accessは各コンピューティング リージョンに/80サブネットからのプールを割り当て、各場所 (ゲートウェイ) に/112サブネットからのプールを割り当てます。各GlobalProtect接続はプールから1つのIPアドレスを使用するため、この割り当てにより、場所ごとに 65,000 を超える利用可能なIPv6アドレス(/128)をユーザーのエンドポイントに割り当てることができます。

- サービス接続およびリモート ネットワーク接続の場合、接続で使用するルーティングの種類 (スタティックルートまたはBGPルート) にIPv6アドレスを指定できます。
  - スタティック ルートの場合は、スタティック ルートに使用されるサブネットのIPv6アドレスを指定します。
  - BGPルートの場合は、 IPv6ピア アドレスとローカル アドレスを指定します。

    BGPピアリング情報の交換に使用する転送方法を指定することもできます。IPv4を使用してすべてのBGPピアリング情報 (IPv4とIPv6 を含む) を交換するか、IPv6を使用してすべてのBGPピアリング情報を交換するか、IPv4を使用してIPv4 BGPピアリング情報を交換し、IPv6を使用して IPv6 BGPピアリング情報を交換するかを指定できます。

    最良の結果を得るには、最大プレフィックス長が/64である独自のIPv6 (パブリックまたはプライベート) アドレス プール (例: 2005:10:209:79::/64) を指定します。

- リモート ネットワークの場合、DNSサーバーのIPv6アドレスを追加できます。

  最良の結果を得るには、最大プレフィックス長が/64である独自の IPv6 (パブリックまたはプライベート) アドレス プール (例: 2001:10:209:65::/64) を用意してください。

  各ブランチ オフィスでは、65,000を超える一意のホストを許可する一意の/112 (最大長) サブネットを使用する必要があります。

©2025 Palo Alto Networks, Inc.

- 提供するIPv6アドレスは、*Prisma Access BYOIP*のパブリック*IPv6*アドレス空間と重複してはいけません。
- *IP*プール、ブランチ オフィス (リモート ネットワーク) サブネット、企業 (サービス接続) サブネット、インフラストラクチャ サブネットは、互いに重複してはなりません (相互に排他的である必要があります)。

次のコンピューティング ロケーションは IPv6をサポートしていません:

- 韓国
- アジア北東部
- 南アメリカ東部
- バーレーン
- South Africa West（南アフリカ西部）
- 北ヨーロッパ（ストックホルム）
- 中東中部（UAE）

次のロケーションではIPv6がサポートされていません。

- すべてのローカルゾーンのロケーション
- Canada West（カナダ西武）
- South Africa Central（南アフリカ中部）

次のデプロイメントではIPv6アドレス指定はサポートされません。

- リモート ネットワーク–ハイ パフォーマンス
- IP最適化

  IP最適化デプロイメントでは、パブリック (外部) アプリへのアクセスに IPv6はサポートされていません。プライベートアプリアクセスはサポートされています。新しいPrisma Accessデプロイメント環境でIPv6を有効にするには、Palo Alto Networksのアカウントチームに連絡してください。弊社担当者がリクエストに対応するためのTACケースを作成します。
- Clean Pipe (クリーンパイプ)のデプロイメント
- トラフィック ステアリング (トラフィック ステアリング ルールを使用して、サービス接続を使用してインターネットへのトラフィックをリダイレクトする)
- サービス接続およびリモート ネットワーク接続のためのサービスのアウトバウンドルート

*Prisma Access*は、*IPv6* デフォルト ルートをアドバタイズしません。

 ©2025 Palo Alto Networks, Inc.

ネイティブIPv6サポートの概要

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンスバージョン2.2以降を推奨 ❑ パブリックおよびプライベートアプリへのネイティブIPv6アクセスには、以下の最小リリースが必要です: • Prisma Access (Managed by Strata Cloud Manager):2024年6月のリリース • Prisma Access (Managed by Panorama):Prisma Access5.1.1は新規デプロイメントのみ。 その他のデプロイメント（既存のPrisma Access (Managed by Panorama)デプロイメントを含む）は、プライベート アプリ アクセスのみをサポートします。

Prisma Accessはプライベート アプリケーションへのアクセスを超えてIPv6のサポートを拡張し、GlobalProtectとリモート ネットワークのIPv6をネイティブにサポートします。

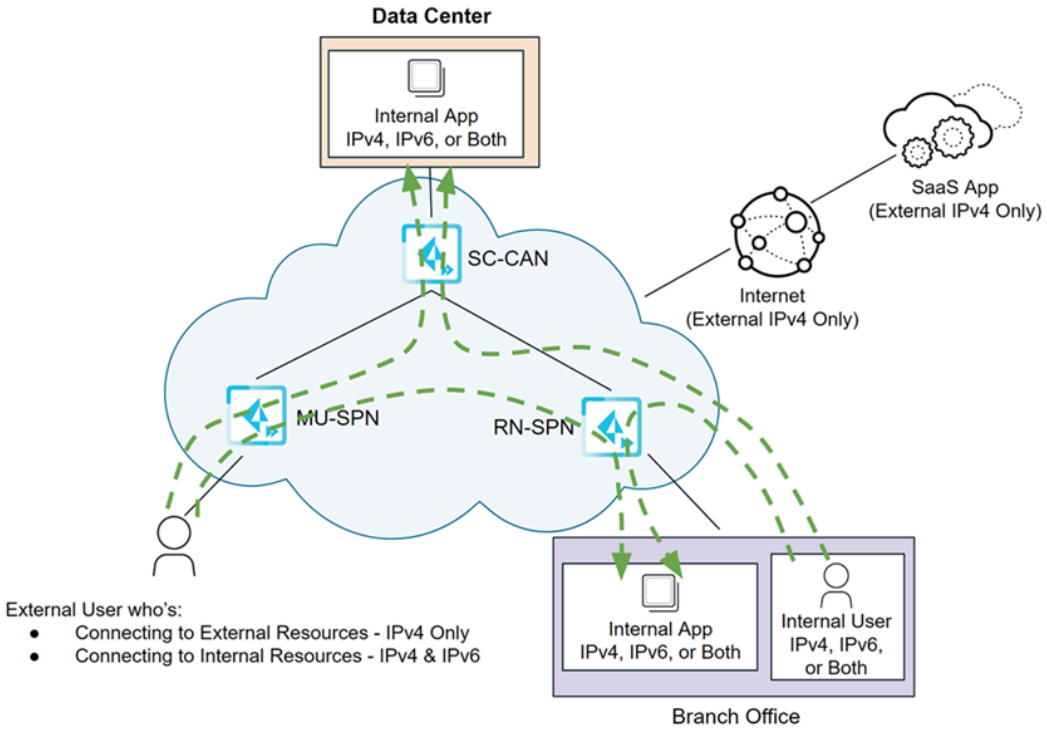
ネイティブIPv6サポートの利点の1つは、IPv6のみおよびデュアルスタックエンドポイントのモバイルユーザーが、GlobalProtectを使用してIPv6接続を介してPrisma Accessに接続できることです。もう 1 つの利点は、GlobalProtectとリモート ネットワークが、インターネットの宛先でIPv6接続が必要な場合に、インターネット経由でインターネットおよびパブリック SaaS アプリケーションにアクセスできることです。

IPv6はIPv4よりも大幅に広いアドレス空間を提供し、ほぼ無制限の数の一意のIPアドレスを許可します。同時に、デュアル スタックは、ネットワークとデバイスがIPv4とIPv6の両方を同時に使用して動作できるようにする移行アプローチです。ネイティブIPv6サポートにより、Prisma AccessはIPv6接続とデュアルスタック接続の両方に対応し、IPv4からIPv6への移行プロセスを容易にし、下位互換性を確保し、クラウドとIPv6対応ネットワークへの移行を促進します。

プライベートアプリのサポート

いくつかのPrisma Accessデプロイメントでは、内部の「プライベート」アプリへのIPv6接続がサポートされます。Prisma Accessは、アンダーレイを使用してデータ センター (サービス接続) およびブランチ オフィス (リモート ネットワーク) に接続し、IPv6トラフィックはIPv4トンネルをパススルーします。

©2025 Palo Alto Networks, Inc.



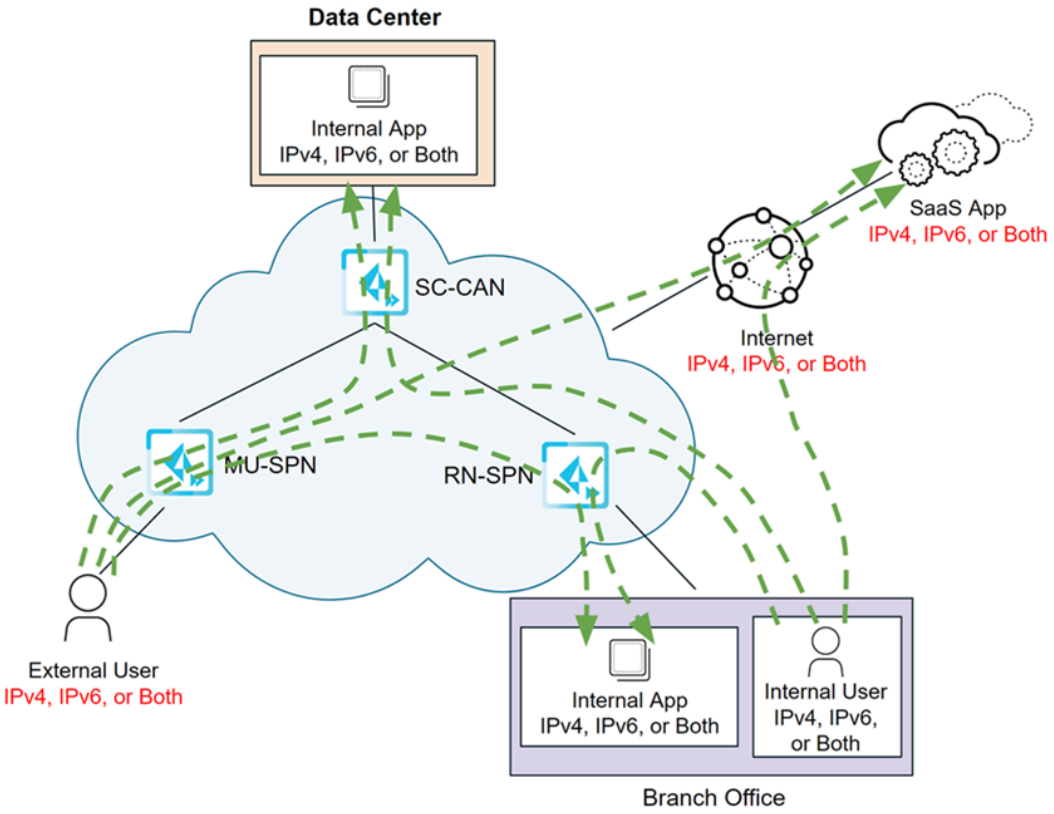
Prisma AccessのネイティブIPv6

Prisma Access

- Prisma AccessへのデュアルスタックIPv4/IPv6インバウンド接続
- デュアルスタックIPv4/IPv6インターネットへのアウトバウンド接続とインターネット経由のSaaSアプリ

現在、ユーザーはIPv6を使用してインターネット経由でインターネットおよび「パブリック」SaaS アプリに接続できます。

©2025 Palo Alto Networks, Inc.



ネイティブ *IPv6*が機能するには、外部ユーザー *(*モバイル ユーザー*)* が次のサポートされている *GlobalProtect* バージョンのいずれかを使用している必要があります。

- *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)*

以下の表は、IPv4 および IPv6 Prisma Accessのデプロイメントでサポートされる接続性を示したものです。チェックマークは、この接続がサポートされていることを示し、ダッシュは、サポートされていないことを示します。

©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

設定でIPv6を有効にするには、次のワークフローに従ってください。

- Prisma Accessインフラストラクチャ でIPv6ネットワークとIPプールを有効にして設定する
- モバイルユーザー向けIPv6ネットワークの有効化 - GlobalProtectのデプロイメント
- サービス接続のためのIPv6ネットワーキングを有効にする
- リモートネットワークのIPv6ネットワーキングの有効化

Prisma Accessインフラストラクチャにおける IPv6 ネットワーキングと IP プールの有効化と設定

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンスバージョン2.2以降を推奨

©2025 Palo Alto Networks, Inc.

どこで使用できますか?	何が必要ですか?
	❑ パブリックおよびプライベートアプリへのネイティブIPv6アクセスには、以下の最小リリースが必要です: • Prisma Access (Managed by Strata Cloud Manager):2024年6月のリリース • Prisma Access (Managed by Panorama):Prisma Access5.1.1は新規デプロイメントのみ。 その他のデプロイメント（既存のPrisma Access (Managed by Panorama)デプロイメントを含む）は、プライベート アプリ アクセスのみをサポートします。

Prisma Accessデプロイメントの場合は、グローバルにIPv6を有効にし、インフラストラクチャ サブネットにIPv6サブネットを指定して、Prisma Accessがリモート ネットワーク ロケーション、モバイルユーザー、およびサービス接続間でIPv6ネットワーク インフラストラクチャを確立できるようにする必要があります。そのためには、次の手順を行ってください。

- Strata Cloud Manager
- Panorama

Prisma Accessインフラストラクチャにおける IPv6 ネットワーキングと IP プールの有効化と設定 （Strata Cloud Manager）

STEP 1 | [ワークフロー] > **[Prisma Access** セットアップ] > **[Prisma Access]** を選択し、歯車アイコンを選択して設定を編集します。

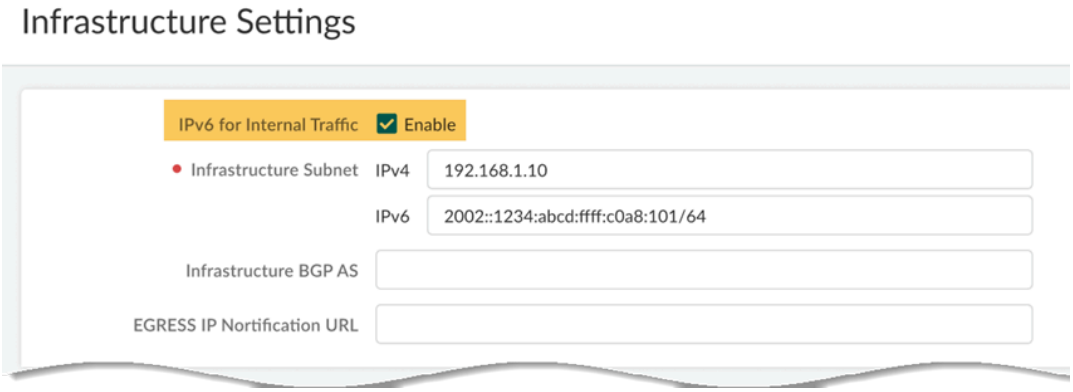
STEP 2 | 内部トラフィックに対して IPv6 を 有効にする には、チェック ボックスをオンにします。

IPv6を有効または無効にすると、データプレーンがPrisma Accessバックボーン上でIPv6ルートの受け入れまたは拒否を準備する間、短時間のトラフィック中断（最大120 秒）が発生し

©2025 Palo Alto Networks, Inc.

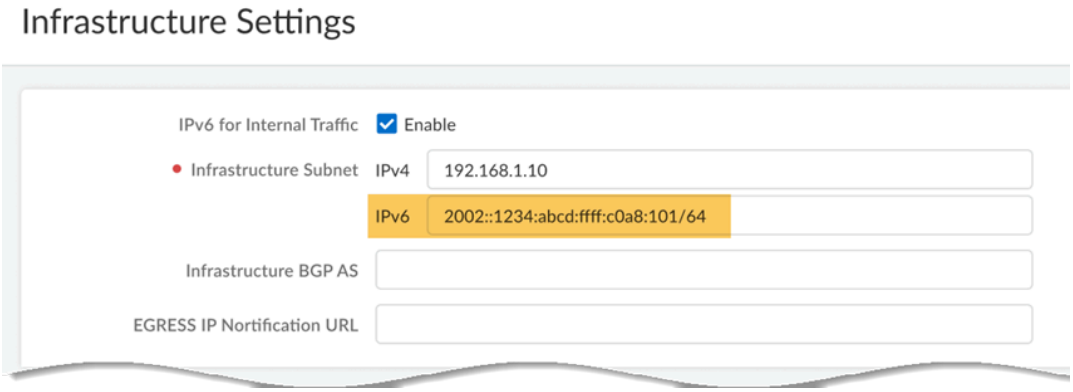
ます。Palo Alto Networksは、メンテナンス時間帯またはオフピーク時にこの設定変更をコミットすることを推奨しています。

IPv6 を削除する必要がある場合は、内部トラフィックに *IPv6* を有効にするチェック ボックスの選択を解除する前に、すべての構成 (該当する場合はモバイル ユーザー、リモート ネットワーク、およびサービス接続を含む) を削除します。



STEP 3 | **IPv6**インフラストラクチャ サブネットと インフラストラクチャ**BGP AS**を指定します。

- 最小サブネット/96を指定します。
- IPv4サブネットも入力する必要があります。 Prisma AccessはIPv6を使用するのに、ネットワーク インフラストラクチャ内のIPv4およびIPv6サブネットが必要です。詳細は Prisma Access インフラストラクチャ管理 を参照してください。
- Palo Alto Networksでは、プライベート (パブリックではない) IPv4およびIPv6アドレスを使用することをお勧めします。
- IPv6リンク ローカル アドレス (fe80::/10) を使用しないでください。



STEP 4 | Prisma Accessインフラ内で使用する**Infrastructure BGP AS**（インフラ**BGP AS**）を入力します。

ダイナミック ルーティングを使用して、Prisma Accessがリモート ネットワークおよびHQ/データセンター上のリソースへの経路を動的に検出できるようにしたい場合は、自律シ

 ©2025 Palo Alto Networks, Inc.

ステム（AS）番号を指定します。AS番号を指定しない場合、デフォルトのAS番号65534が使用されます。

STEP 5 | まだ追加していない場合は、内部DNSサーバーを追加して、Prisma Accessが内部ドメインを解決して、企業ネットワーク上のLDAPやDNSサーバーなどのサービスにアクセスで きるようにすることを検討してください。

詳細は Prisma Access インフラストラクチャ管理 を参照してください。

STEP 6 | (モバイル ユーザーデプロイメントのみ) モバイル ユーザー - GlobalProtectデプロイメントにIPv6 IPアドレス プールを追加します。

モバイル ユーザー - GlobalProtect のデプロイメントには IP アドレス プールが必要です。IPv6機能を有効にするには、IPv4とIPv6の両方のIPアドレス プールが必要です。IPv4アドレスは地域レベルまたは世界レベルで適用し、IPv6アドレスは世界レベルで適用します。最小の/80サブネットを指定します。

Prisma Accessは、以下の方法を使用して、ワールドワイド IPv6 アドレスを細分化します。

- Prisma Accessは、各場所 (ゲートウェイ) に /112 サブネットからプールを割り当てます。各GlobalProtect接続はプールから1つのIPアドレスを使用するため、この割り当てによ

 ©2025 Palo Alto Networks, Inc.

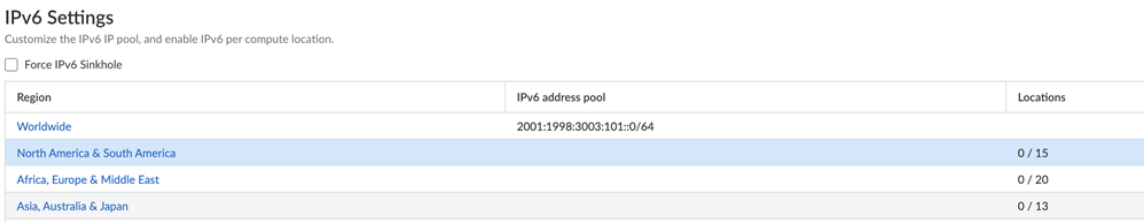
り、場所ごとに 65,000 を超える利用可能なIPv6アドレスをユーザーのエンドポイントに割り当てることができます。

オートスケール・イベント（多数のユーザが 1 つのPrisma Accessロケーションにログインする場合）が発生した場合、Prisma Accessは別の /112 サブネットを持つ別のロケーションを追加することができます。

- 場所でIPv6の使用を有効にすると、 Prisma Accessはロケーションが属するリージョンにIPv6アドレス プールを割り当て、IPv6が有効になっているリージョンの合計数間でプールを分割します。

*IP*アドレス プールではローカル リンク アドレス *(fe80::/10)* を使用しないでください。

1. [ワークフロー] > **[Prisma Access** セットアップ] > **[GlobalProtect]** を選択し、歯車アイコンを選択してインフラストラクチャ設定を編集します。
2. [クライアントIPプール] セクションで、 リージョン を選択するか、**[IP**ポータルの追加]を選択します。
3. **IPv6**アドレス プールを入力します。
   - モバイル ユーザーの場合は、IPv4とIPv6の両方のIPアドレスを入力する必要があります。 Prisma Accessは、IPv6を使用する場合、内部インフラストラクチャをサポートするために IPv4 およびIPv6アドレスが必要です。
   - 最小IPv6サブネット /80 を入力します。
   - Prisma Accessは各サブネットをリージョンごとに細分化します。



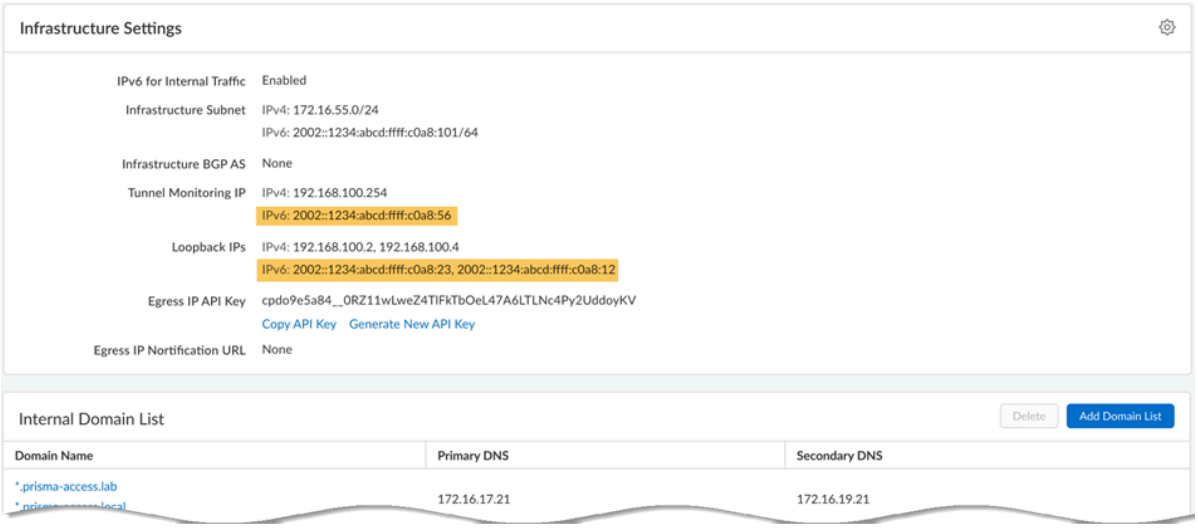
STEP 7 | 保存 して、 **[Push Config (**設定をプッシュ**)]**します

©2025 Palo Alto Networks, Inc.

STEP 8 | [ワークフロー] > **[Prisma Access]** > [セットアップ] を選択し、インフラストラクチャ設定で次の IPv6 アドレスをメモします。

- キャプティブ ポータル リダイレクト**IP**アドレス- 認証ポータルベースのユーザーIDアドレスマッピングで使用します
- トンネルモニター**IP**アドレス- トンネル監視に使用します

GlobalProtectモバイル ユーザーは VPN トンネルにIPv4アドレスを必要とするため、IPアドレスがインフラストラクチャ サブネットから取得される ループバック アドレスでは引き続きIPv4アドレスが使用されます。



Prisma Accessインフラストラクチャにおける IPv6 ネットワーキングと IP プールの有効化と設定 （Panorama）

STEP 1 | **Panorama** > **Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Service Setup**（サービスのセットアップ）の順に選択し、歯車型アイコンをクリックして設定を編集します。

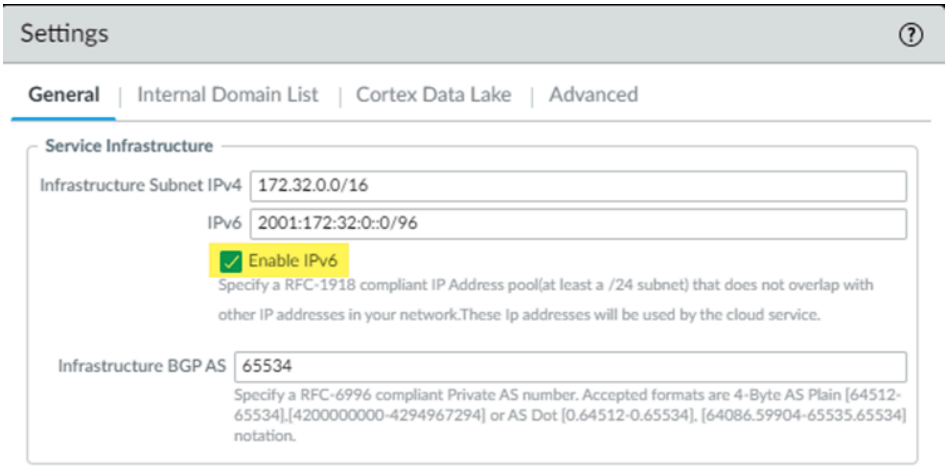
STEP 2 | 全般 タブで、 **IPv6** を有効にします。

IPv6を有効または無効にすると、データプレーンがPrisma Accessバックボーン上でIPv6ルートの受け入れまたは拒否を準備する間、短時間のトラフィック中断（最大120 秒）が発生し

©2025 Palo Alto Networks, Inc.

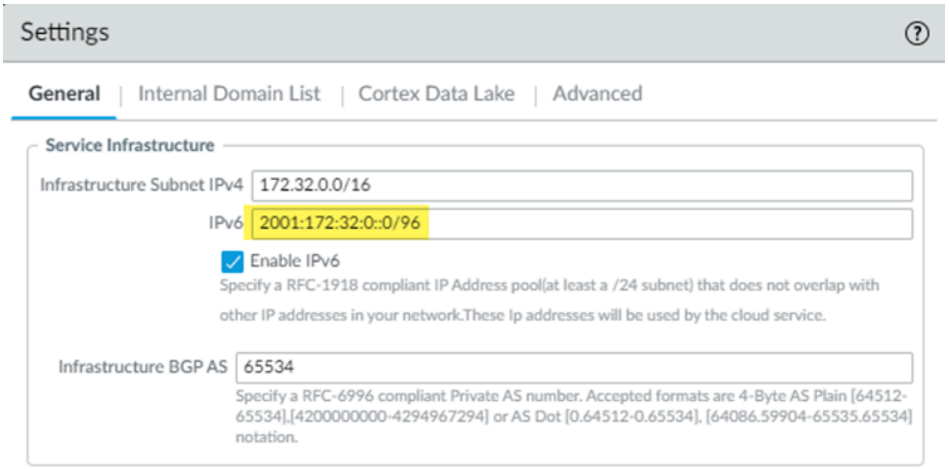
ます。Palo Alto Networks は、メンテナンス時間帯またはオフピーク時にこの設定変更をコミットすることを推奨しています。

IPv6 を削除する必要がある場合は*IPv6* を有効にする チェック ボックスの選択を解除する前に、すべての構成 (該当する場合はモバイル ユーザー、リモート ネットワーク、およびサービス接続を含む) を削除します。



STEP 3 | **IPv6**インフラストラクチャ サブネットと インフラストラクチャ**BGP AS**を指定します。

- 最小サブネット/96を指定します。
- IPv4サブネットも入力する必要があります。 Prisma AccessはIPv6を使用するのに、ネットワーク インフラストラクチャ内のIPv4およびIPv6サブネットが必要です。詳細は Prisma Accessサービスインフラの設定 (Panorama) を参照してください。
- Palo Alto Networksでは、プライベート (パブリックではない) IPv4およびIPv6アドレスを使用することをお勧めします。
- IPv6リンク ローカル アドレス (fe80::/10) を使用しないでください。



 ©2025 Palo Alto Networks, Inc.

STEP 4 | Prisma Accessインフラ内で使用する**Infrastructure BGP AS**（インフラ**BGP AS**）を入力します。

ダイナミック ルーティングを使用して、Prisma Accessがリモート ネットワークおよびHQ/データセンター上のリソースへの経路を動的に検出できるようにしたい場合は、自律システム（AS）番号を指定します。AS番号を指定しない場合、デフォルトのAS番号65534が使用されます。

STEP 5 | サービスのセットアップ設定をまだ完了していない場合は、**[Internal Domain List (**内部ドメイン一覧**)]**、**[Strata Logging** サービス**]**そして **[**詳細**]** 設定を入力します。

詳細は Prisma Accessサービスインフラの設定 (Panorama) を参照してください。

STEP 6 | (モバイル ユーザーデプロイメントのみ) モバイル ユーザー - GlobalProtectデプロイメントにIPv6 IPアドレス プールを追加します。

モバイル ユーザー - GlobalProtectのデプロイメントには IPアドレス プールが必要です。IPv6機能を有効にするには、IPv4とIPv6の両方のIPアドレス プールが必要です。IPv4アドレスは地域レベルまたは世界レベルで適用し、IPv6アドレスは世界レベルで適用します。最小の/80サブネットを指定します。

Prisma Accessは、以下の方法を使用して、ワールドワイド IPv6 アドレスを細分化します。

- Prisma Accessは、各場所 (ゲートウェイ) に /112 サブネットからプールを割り当てます。各GlobalProtect接続はプールから1つのIPアドレスを使用するため、この割り当てによ

 ©2025 Palo Alto Networks, Inc.

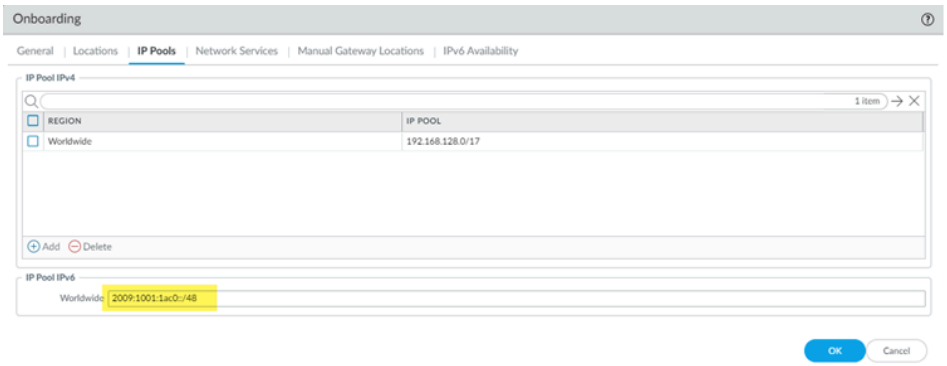
り、場所ごとに 65,000 を超える利用可能なIPv6アドレスをユーザーのエンドポイントに割り当てることができます。

オートスケール イベント（多数のユーザーが 1 つのPrisma Accessロケーションにログインする場合）が発生した場合、Prisma Accessは別の /112 サブネットを持つ別のロケーションを追加することができます。

- 場所でIPv6の使用を有効にすると、 Prisma Accessはロケーションが属するリージョンにIPv6アドレス プールを割り当て、IPv6が有効になっているリージョンの合計数間でプールを分割します。

*IP*アドレス プールでローカル リンク アドレス *(fe80::/10)* を使用しないでください。

1. **[Panorama]** > **[**クラウド サービス**]** > **[**構成**]** > **[**モバイル ユーザー **- GlobalProtect]**を選択します。
2. [オンボード] セクションで、ポータル**[Hostname (**ホスト名**)]** を選択するか、**[Configure (**設定**)]**を選択します 。
3. **IP** プール タブを選択します。
4. **IP** プール **IPv6**を入力します。
   - モバイル ユーザーの場合は、IPv4とIPv6の両方のIPアドレスを入力する必要があります。 Prisma Accessは、IPv6を使用する場合、内部インフラストラクチャをサポートするために IPv4 およびIPv6アドレスが必要です。
   - 最小IPv6サブネット /80 を入力します。
   - Prisma Accessは各サブネットをリージョンごとに細分化します。



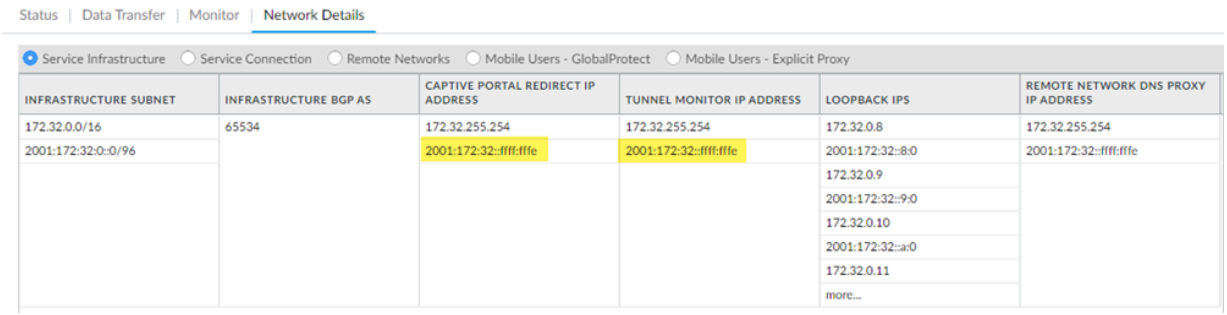
STEP 7 | 変更を **Commit and Push**（コミットしてプッシュ）します。

©2025 Palo Alto Networks, Inc.

STEP 8 | **[Panorama]** > [クラウドサービス] > [ステータス] > [ネットワークの詳細] > [サービスインフラストラクチャ]を選び、 次に、次のIPv6アドレスをメモします。

- キャプティブ ポータル リダイレクト**IP**アドレス- 認証ポータルベースのユーザーIDアドレスマッピングで使用します
- トンネルモニター**IP**アドレス- トンネル監視に使用します

GlobalProtectモバイル ユーザーは VPNトンネルにIPv4アドレスを必要とするため、IPアドレスがインフラストラクチャ サブネットから取得される ループバック アドレスでは引き続きIPv4アドレスが使用されます。



モバイルユーザー向けIPv6ネットワークの有効化 - GlobalProtectのデプロイメント

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンスバージョン2.2以降を推奨 ❑ パブリックおよびプライベートアプリへのネイティブIPv6アクセスには、以下の最小リリースが必要です: • Prisma Access (Managed by Strata Cloud Manager):2024年6月のリリース • Prisma Access (Managed by Panorama):Prisma Access5.1.1は新規デプロイメントのみ。 その他のデプロイメント（既存のPrisma Access (Managed by Panorama)デプロイメントを含む）は、プライベート アプリ アクセスのみをサポートします。

モバイル ユーザーの IP アドレス プールを指定することに加えて、モバイル ユーザー - GlobalProtectデプロイメントに対して **IPv6** の可用性 を設定する必要があります。ネットワークで内部ドメインを解決するため IPv6 DNSサーバーを使用する場合は、次のセクションに示すよ

 ©2025 Palo Alto Networks, Inc.

うに、プライマリDNSサーバーとセカンダリDNSサーバーのIPv6アドレスを指定することもできます。

- Strata Cloud Manager
- Panorama

モバイルユーザー向けIPv6ネットワークの有効化 - GlobalProtectのデプロイメント (Strata Cloud Manager)

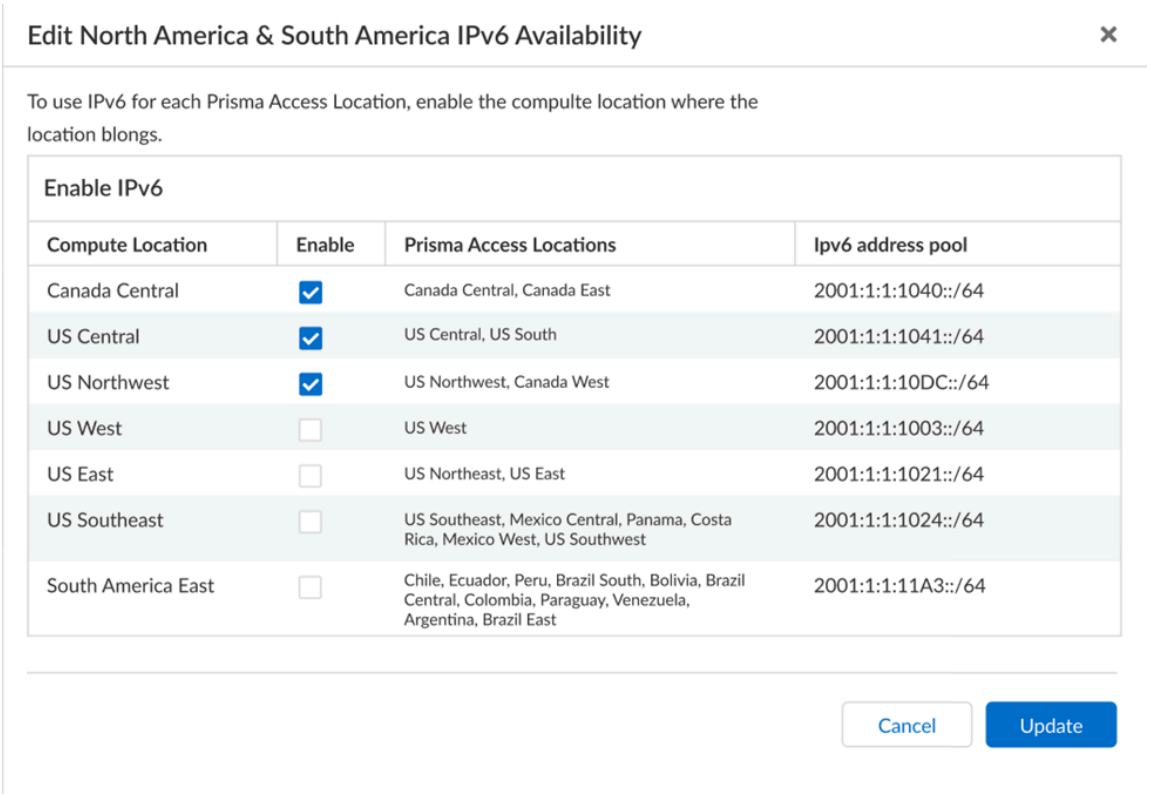
モバイル ユーザーの IP アドレス プールを指定することに加えて、モバイル ユーザー - GlobalProtectデプロイメントに対して **IPv6** の可用性 を設定する必要があります。ネットワークで内部ドメインを解決するため IPv6 DNSサーバーを使用する場合は、次のセクションに示すように、プライマリDNSサーバーとセカンダリDNSサーバーのIPv6アドレスを指定することもできます。

STEP 1 | Prisma Accessデプロイメント全体にIPv6をデプロイするか、または特定のコンピュート ロケーションのみにIPv6をデプロイするかを計画します。

STEP 2 | IPv6をデプロイするリージョンのIPv6の可用性を構成します。

1. [ワークフロー] > **[Prisma Access** セットアップ] > **[GlobalProtect]** を選択し、歯車アイコンを選択してインフラストラクチャ設定を編集します。
2. **IPv6** 設定 セクションで、IPv6 を 有効にするロケーションを選択します。

   すべての場所はコンピューティング場所に関連付けられています。コンピューティング ロケーション内の場所で IPv6 が有効になっていない場合は、そのコンピューティング ロケーションの選択を解除したままにします。



 ©2025 Palo Alto Networks, Inc.

STEP 3 | (任意) 内部 DNS サーバーがIPv6アドレスでアクセスできる場合は、[クライアント **DNS**]セクションから[リージョンの追加] を選択し、[内部ドメインの解決] チェック ボックスをオンにして、ルールを追加するか、デフォルト ルールを指定して、 プライマリ **DNS** サーバーとセカンダリ **DNS**サーバーのカスタムDNS サーバーIPv6アドレスを指定します。

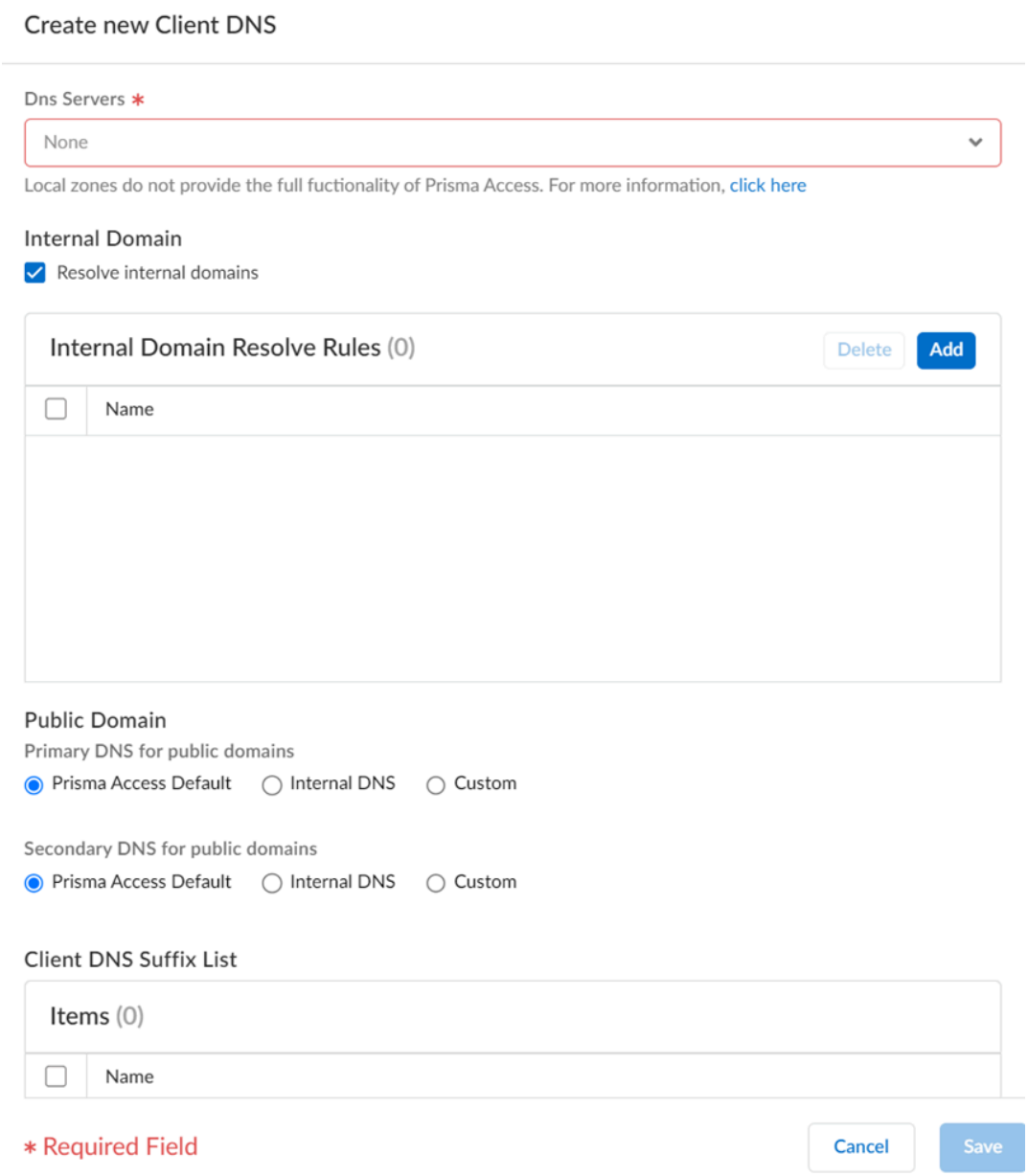
DNSサーバーのIPv6アドレスを入力する場合は、モバイル ユーザーのIPアドレス プールにもIPv6アドレスが必要です。

プライマリDNSサーバーとセカンダリDNSサーバーのIPv4またはIPv6アドレスの任意の組み合わせを入力できます。プライマリDNSサーバーのIPv6アドレスとセカンダリDNSサーバーのIPv4アドレスを入力し、**IPv6**可用性 が有効になっていないコンピューティング場所

 ©2025 Palo Alto Networks, Inc.

からDNSクエリを受信した場合、 Prisma AccessはIPv4アドレスを使用するため、セカンダリDNSサーバーを使用します。

*IPv4*アドレスは*A*レコードを使用し、*IPv6*アドレスは*AAAA*レコードを使用します。一部の*DNS*サーバーは*IPv4*トランスポート経由で*AAAA DNS*検索を実行できるため、*IPv6 IP*アドレスを持つサーバーは必要ない場合もあります。



STEP 4 | (任意) モバイル ユーザーの設定をまだ完了していない場合は、今すぐ完了してください。詳細については、「GlobalProtect モバイル ユーザーの設定」 を参照してください。

STEP 5 | **[Push Config (設定をプッシュ)]**を 実行して、変更をネットワークにデプロイします。

©2025 Palo Alto Networks, Inc.

モバイルユーザー向けIPv6ネットワークの有効化 - GlobalProtectのデプロイメント (Panorama)

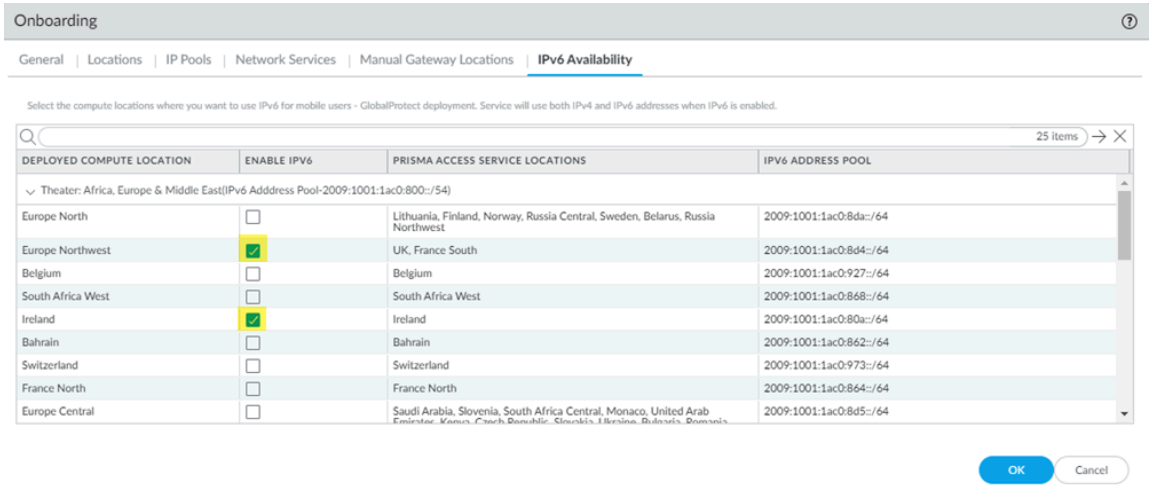
モバイル ユーザーの IP アドレス プールを指定することに加えて、モバイル ユーザー - GlobalProtectデプロイメントに対して **IPv6** の可用性 を設定する必要があります。ネットワークで内部ドメインを解決するため IPv6 DNSサーバーを使用する場合は、次のセクションに示すように、プライマリDNSサーバーとセカンダリDNSサーバーのIPv6アドレスを指定することもできます。

STEP 1 | <ph keyref="pa"/>デプロイメント全体にIPv6をデプロイするか、または特定のコンピュート ロケーションのみにIPv6をデプロイするかを計画します。

STEP 2 | IPv6をデプロイするリージョンのIPv6の可用性を構成します。

1. **[IPv6** の可用性]タブで、IPv6 を有効にする場所に対して**IPv6** を有効にします。

   すべての場所はコンピューティング場所に関連付けられています。コンピューティング ロケーション内の場所で IPv6 が有効になっていない場合は、そのコンピューティング ロケーションの選択を解除したままにします。



STEP 3 | (任意) 内部DNSサーバーがIPv6アドレスでアクセスできる場合は、[ネットワーク サービス]タブをクリックし、ルールを追加するか、既定のルールを指定して、 プライマリ**DNS**サーバーと セカンダリ **DNS** サーバーの カスタム**DNS**サーバー IPv6 アドレスを指定します。

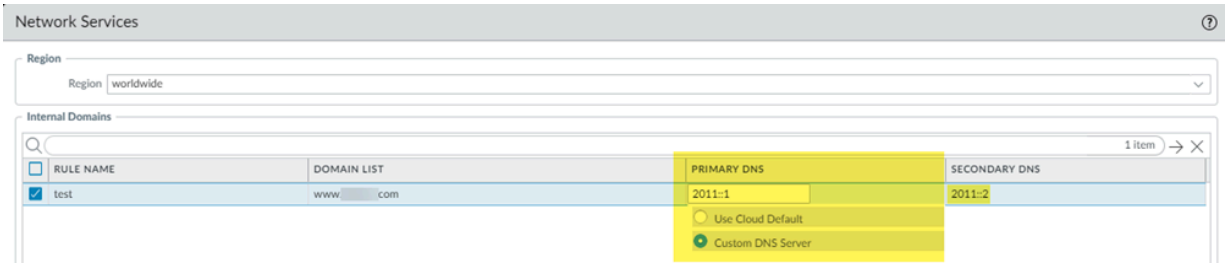
DNSサーバーのIPv6アドレスを入力する場合は、モバイル ユーザーのIPアドレス プールにもIPv6アドレスが必要です。

プライマリDNSサーバーとセカンダリDNSサーバーのIPv4またはIPv6アドレスの任意の組み合わせを入力できます。プライマリDNSサーバーのIPv6アドレスとセカンダリDNSサーバーのIPv4アドレスを入力し、**IPv6**可用性 が有効になっていないコンピューティング場所か

 ©2025 Palo Alto Networks, Inc.

らDNSクエリを受信した場合、 <ph keyref="pa"/>はIPv4アドレスを使用するため、セカンダリDNSサーバーを使用します。

*IPv4*アドレスは*A*レコードを使用し、*IPv6*アドレスは*AAAA*レコードを使用します。一部の*DNS*サーバーは*IPv4*トランスポート経由で*AAAA DNS*検索を実行できるため、*IPv6 IP*アドレスを持つサーバーは必要ない場合もあります。



STEP 4 | (任意) モバイル ユーザーの設定をまだ完了していない場合は、ここで完了してください。詳細については、「GlobalProtect モバイル ユーザーのセットアップ」 を参照してください。

STEP 5 | 変更を **Commit and Push**（コミットしてプッシュ）します。

サービス接続のためのIPv6ネットワーキングを有効にする

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンスバージョン2.2以降を推奨 ❑ パブリックおよびプライベートアプリへのネイティブIPv6アクセスには、以下の最小リリースが必要です: • Prisma Access (Managed by Strata Cloud Manager):2024年6月のリリース • Prisma Access (Managed by Panorama):Prisma Access5.1.1は新規デプロイメントのみ。 その他のデプロイメント（既存のPrisma Access (Managed by Panorama)デプロイメントを含む）は、プライベート アプリ アクセスのみをサポートします。

サービス接続では、スタティックまたはBGPルーティングにIPv6サブネットを使用できます。BGPルーティングでは、IPv6ピア アドレスを入力し、IPv4およびIPv6ルーティング オプションを指定できます。

サービス接続用にIPv6ネットワークを構成するには、次のタスクを実行します。

©2025 Palo Alto Networks, Inc.

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

サービス接続のためのIPv6ネットワーキングを有効にする (Strata Cloud Manager)

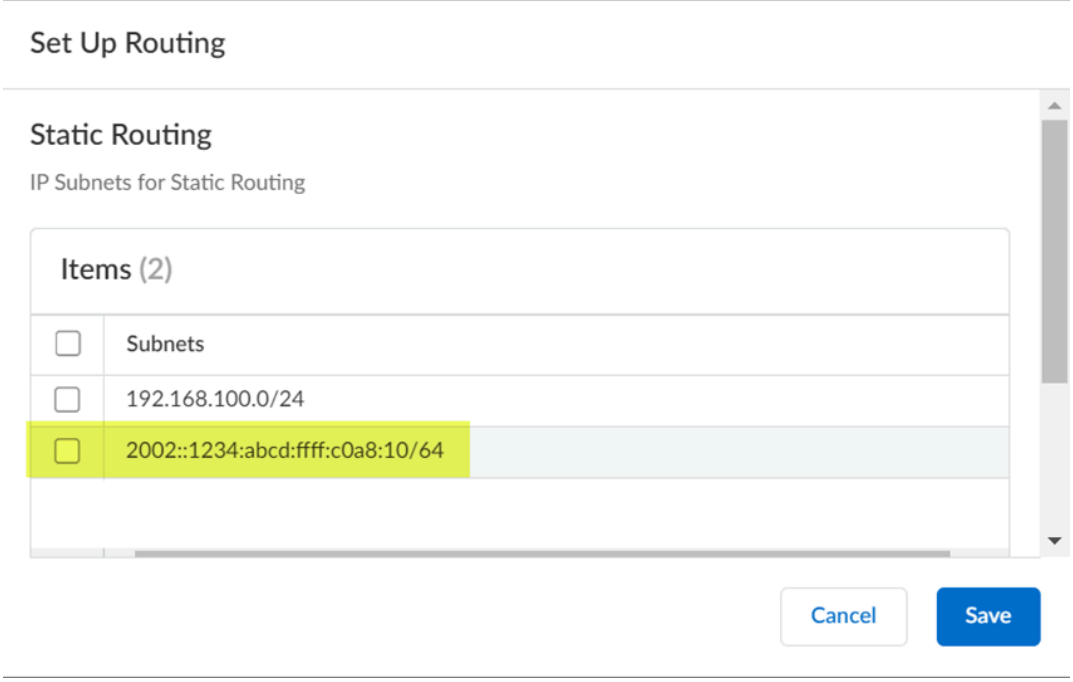
STEP 1 | **[Workflows (ワークフロー)] > Prisma Accessセットアップ)] > [Service Connections (サービスコネクション)]**を選択し、次に**[Add Service Connection (サービス接続を追加)]**を選択します。

STEP 2 | 新しいサービス接続を追加するか、既存のサービス接続を選択して編集します。

©2025 Palo Alto Networks, Inc.

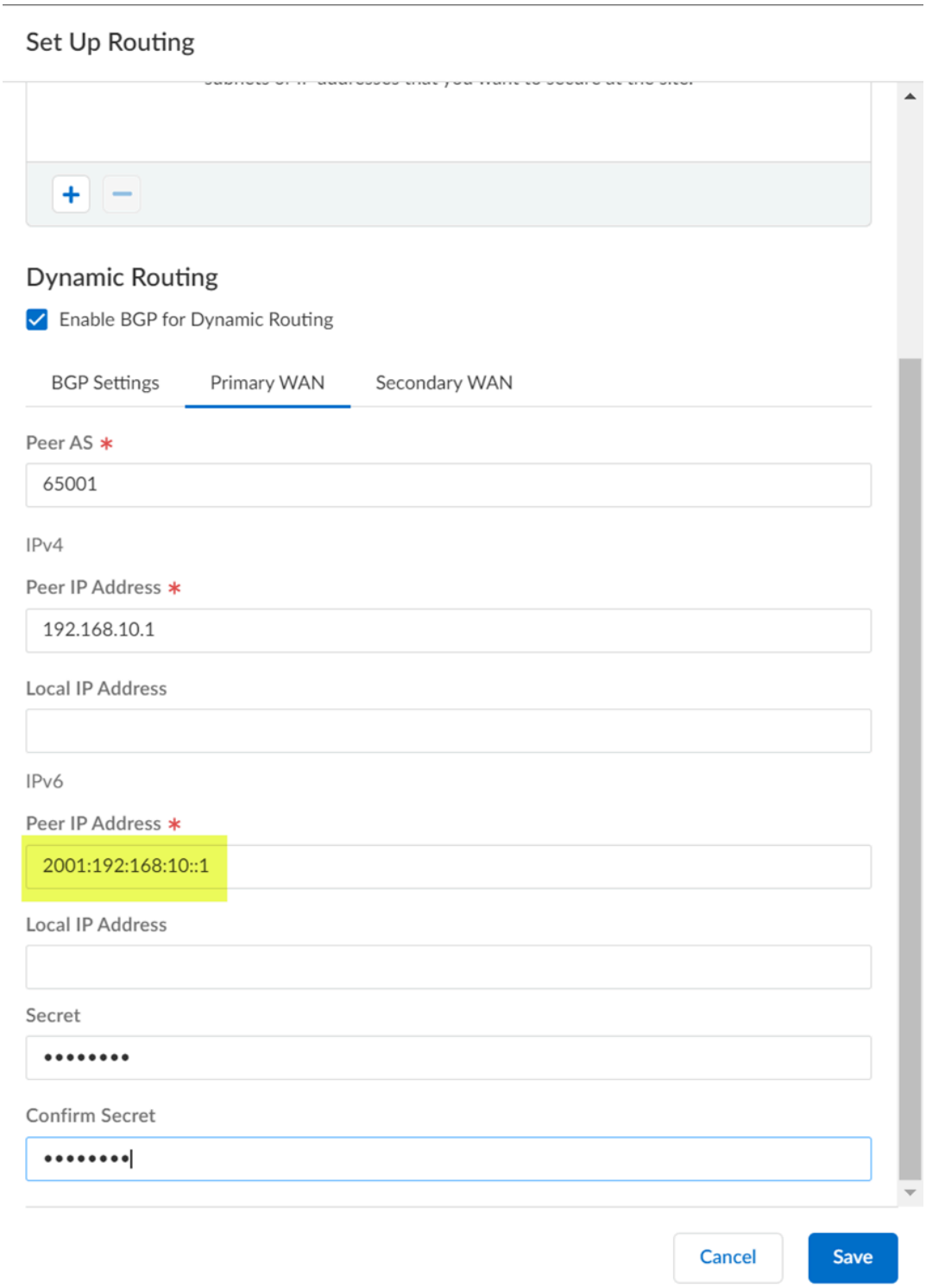
STEP 3 | サービス接続のためにIPv6ルーティングを設定します。

1. (スタティック ルーティング デプロイメントのみ) 1 **[Corporate Subnets (**企業サブネット**)]** の **[Static Routes (**スタティック ルート**)]** タブを 1 つ以上入力します。



2. (BGPルーティングデプロイメントのみ) IPv4およびIPv6 BGPルートの交換方法を指定します。次に、IPv6 ピアアドレス そして ローカルアドレスを入力します。。
   - 単一の IPv4 BGPセッションを使用してIPv4とIPv6の両方のBGPピアリング情報を交換するには、**IPv4** ピアリング経由で**IPv4**ルートと**IPv6**ルートの両方を交換します。
   - IPv4 BGPピアリング情報を交換するIPv4 BGPセッションと、IPv6 BGPピアリング情報を交換するIPv6セッションの場合は、**IPv4**ピアリング経由の**IPv4**ルートと**IPv6**ピアリング経由の**IPv6**ルートの交換します。
   - 単一のIPv6 BGPセッションを使用してIPv6 BGPピアリング情報を交換するには、**[IPv6** ピアリング経由の **IPv6** ルートの交換**]**を選択します。
3. セカンダリWANが異なるピアアドレスまたはローカルアドレスを使用する場合は、［プライマリ**WAN**と同じ］の選択を解除し、セカンダリWANのIPv6ピアアドレスとローカルアドレスを入力します。

©2025 Palo Alto Networks, Inc.



STEP 4 | サービス接続のセットアップをまだ完了していない場合は、ここで完了します。詳細については、「Prisma Accessでサービス接続を設定する」を参照してください。

サービス接続のための*IPv6*インターネットアクセスは、*IPv6*トラフィックが*IPv4*トンネルを通過するアンダーレイ接続によって有効になります。

©2025 Palo Alto Networks, Inc.

STEP 5 | **[Push Config (設定をプッシュ)]**を 実行して、変更をネットワークにデプロイします。

STEP 6 | モバイル ユーザーの設定をまだ完了していない場合は、ここで完了してください。

サービス接続のための**IPv6**ネットワーキングを有効にする **(Panorama)**

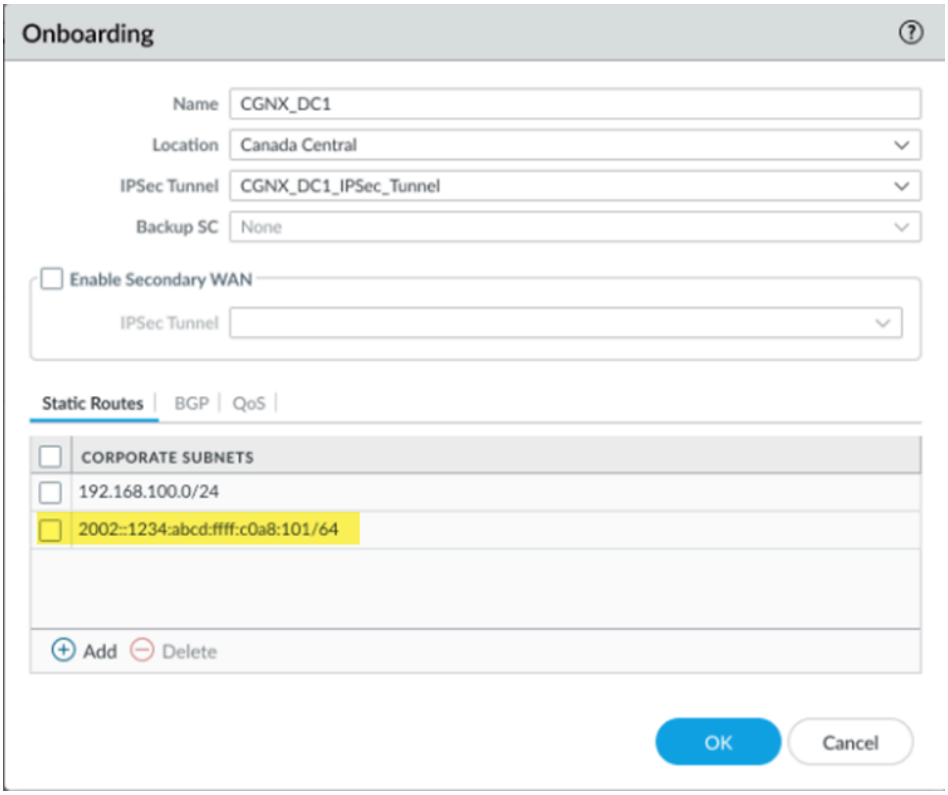
STEP 1 | **Panorama** > **Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Service Connection**（サービス接続）を選択します。

STEP 2 | 新しいサービス接続を追加するか、既存のサービス接続を選択して編集します。

 ©2025 Palo Alto Networks, Inc.

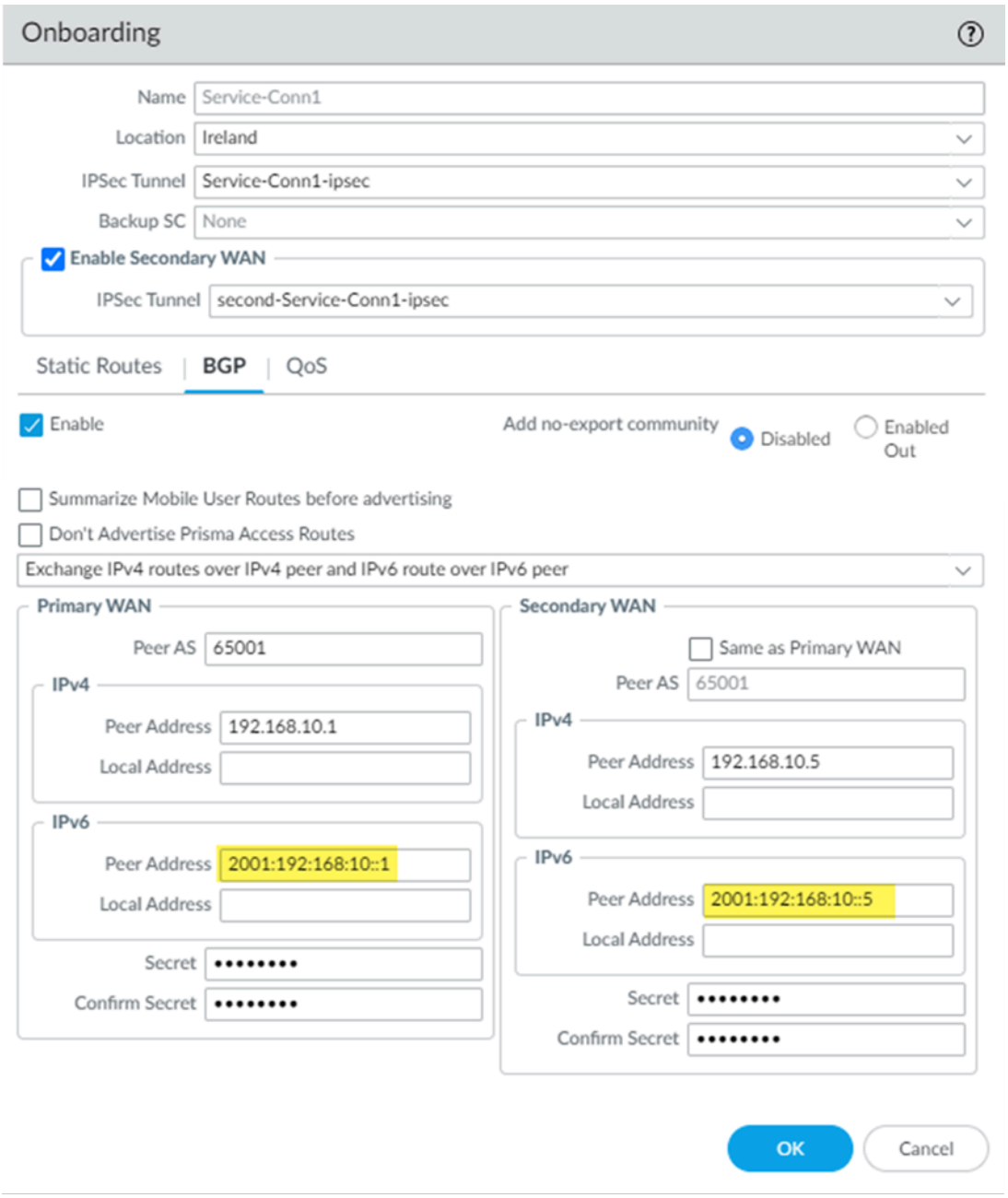
STEP 3 | サービス接続のためにIPv6ルーティングをセットアップします。

1. (スタティック ルーティング デプロイメントのみ) 1 **[Corporate Subnets (**企業サブネット**)]** の **[Static Routes (**スタティック ルート**)]** タブを 1 つ以上入力します。



2. (BGPルーティングデプロイメントのみ) IPv4およびIPv6 BGPルートの交換方法を指定します。次に、IPv6 ピアアドレス そして ローカルアドレスを入力します。。
   - 単一の IPv4 BGPセッションを使用してIPv4とIPv6の両方のBGPピアリング情報を交換するには、**IPv4** ピアリング経由で**IPv4**ルートと**IPv6**ルートの両方を交換します。
   - IPv4 BGPピアリング情報を交換するIPv4 BGPセッションと、IPv6 BGPピアリング情報を交換するIPv6セッションの場合は、**IPv4**ピアリング経由の**IPv4**ルートと**IPv6**ピアリング経由の**IPv6**ルートの交換します。
   - 単一のIPv6 BGPセッションを使用してIPv6 BGPピアリング情報を交換するには、**[IPv6** ピアリング経由の **IPv6** ルートの交換**]**を選択します。
3. セカンダリWANが異なるピアアドレスまたはローカルアドレスを使用する場合は、［プライマリ**WAN**と同じ］の選択を解除し、セカンダリWANのIPv6ピアアドレスとローカルアドレスを入力します。

©2025 Palo Alto Networks, Inc.



STEP 4 | サービス接続のセットアップをまだ完了していない場合は、ここで完了します。詳細については、「Prisma Access でサービス接続を設定する」 を参照してください。

STEP 5 | 変更を **Commit and Push**（コミットしてプッシュ）します。

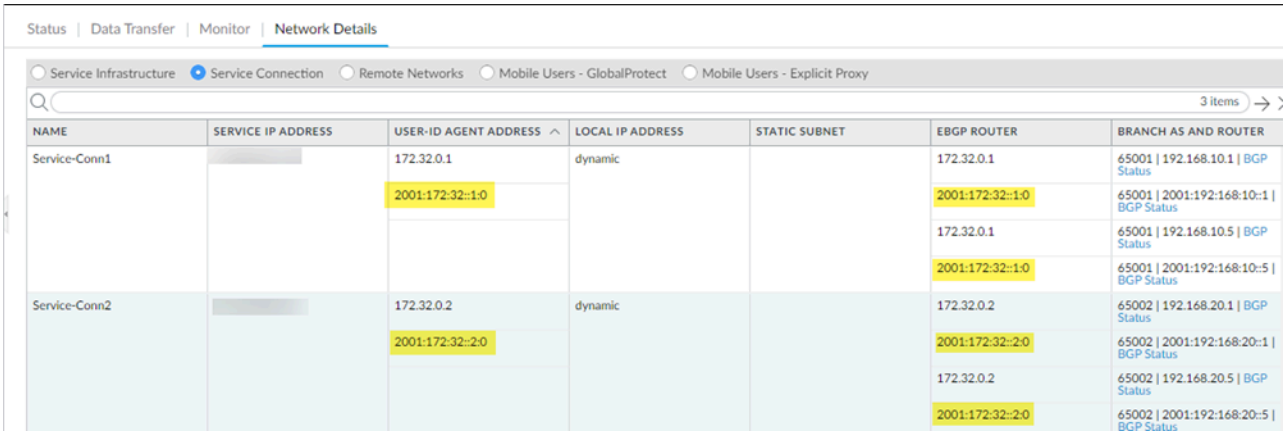
©2025 Palo Alto Networks, Inc.

STEP 6 | **[Panorama]** > **[クラウド サービス]** > **[ステータス]** > **[ネットワーク詳細]** > **[サービス接続]** を選択し、IPv6**[ユーザーUser-IDエージェントアドレス]** と **[EBGPルーター]** アドレスをメモします。

変更をコミットすると、サービス接続用のIPv6**User-ID**エージェントアドレス (ユーザーIDの取得と配信に使用) と **EBGP**ルーター アドレスが作成されます。

サービス接続に使用されるIPSecトンネルはIPv4アドレスを使用するため、 **[サービスIPアドレス]**はIPv4アドレスになります。

サービス接続のためのIPv6インターネットアクセスは、IPv6トラフィックがIPv4トンネルをパススルーするアンダーレイ接続によって有効になります。



STEP 7 | モバイル ユーザーの設定をまだ完了していない場合は、ここで完了してください。

リモートネットワークのIPv6ネットワーキングの有効化

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンスバージョン2.2以降を推奨 ❑ パブリックおよびプライベートアプリへのネイティブIPv6アクセスには、以下の最小リリースが必要です: • Prisma Access (Managed by Strata Cloud Manager):2024年6月のリリース • Prisma Access (Managed by Panorama):Prisma Access5.1.1は新規デプロイメントのみ。 その他のデプロイメント（既存のPrisma Access (Managed by Panorama)デプロイメントを含む）は、プライベート アプリ アクセスのみをサポートします。

©2025 Palo Alto Networks, Inc.

リモート ネットワーク接続の場合、スタティック ルートにIPv6サブネットを使用できます。BGPルーティングの場合、IPv6ピア アドレスを入力し、BGPがIPv6ルーティングのみを使用するか、IPv4と IPv6の両方のルーティングを使用するかを指定できます。

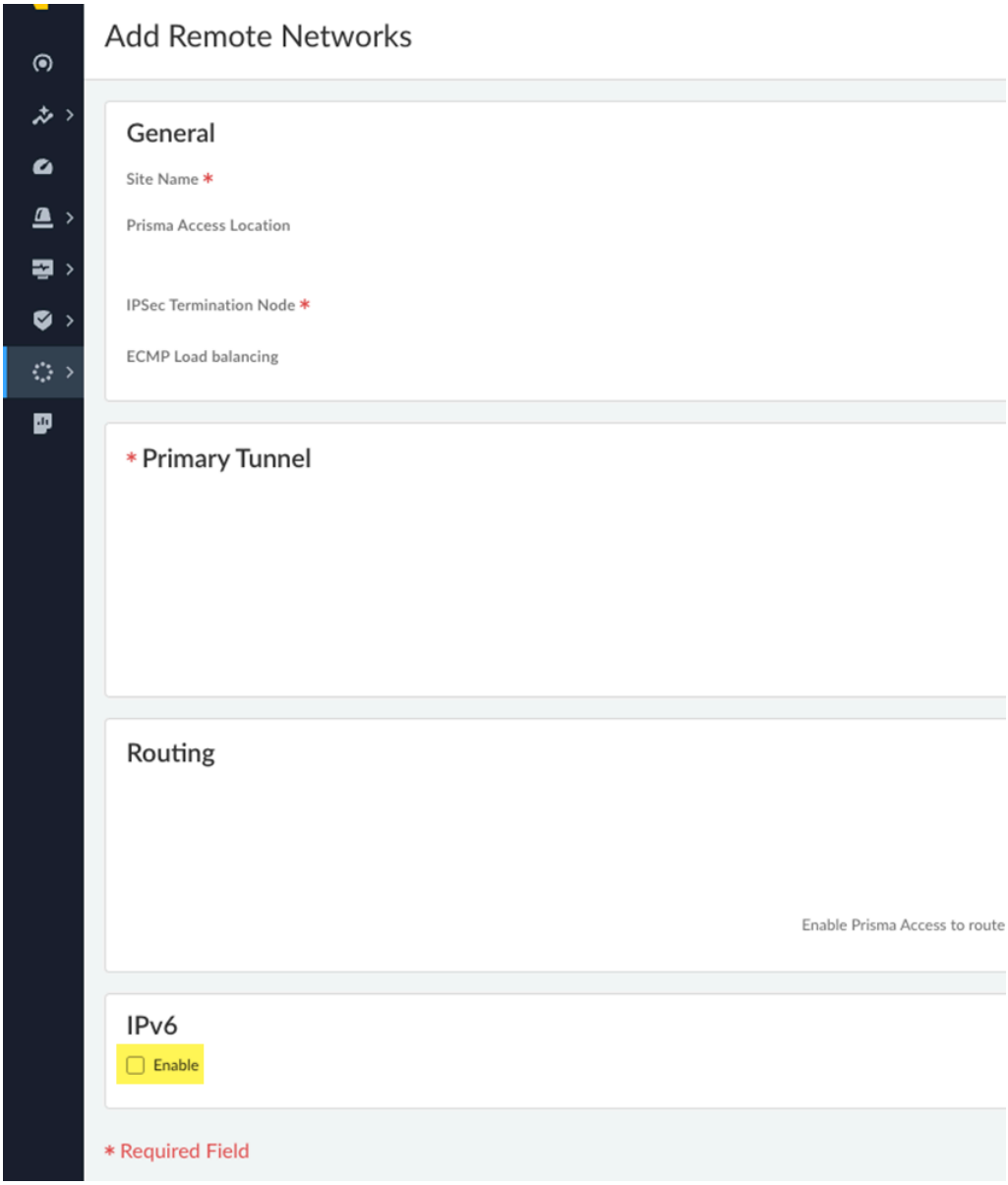
リモート ネットワーク接続用にIPv6ネットワークを構成するには、次のタスクを実行します。

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

リモートネットワークのIPv6ネットワーキングの有効化 (Strata Cloud Manager)

STEP 1 | [ワークフロー] > [Prisma Accessのセットアップ] > [リモートネットワーク]を選択し、[リモートネットワークの追加]を行います。

STEP 2 | IPv6を有効にします。



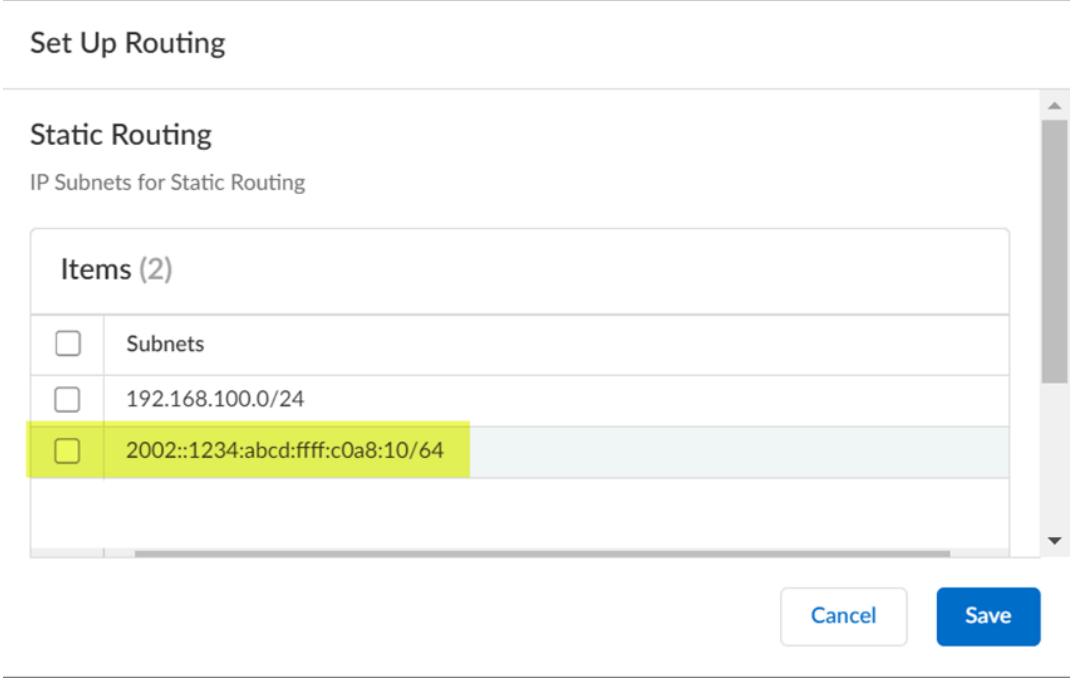
 ©2025 Palo Alto Networks, Inc.

STEP 3 | 新しいリモートネットワーク接続を追加するか、既存のリモートネットワーク接続を選択して編集します。

 ©2025 Palo Alto Networks, Inc.

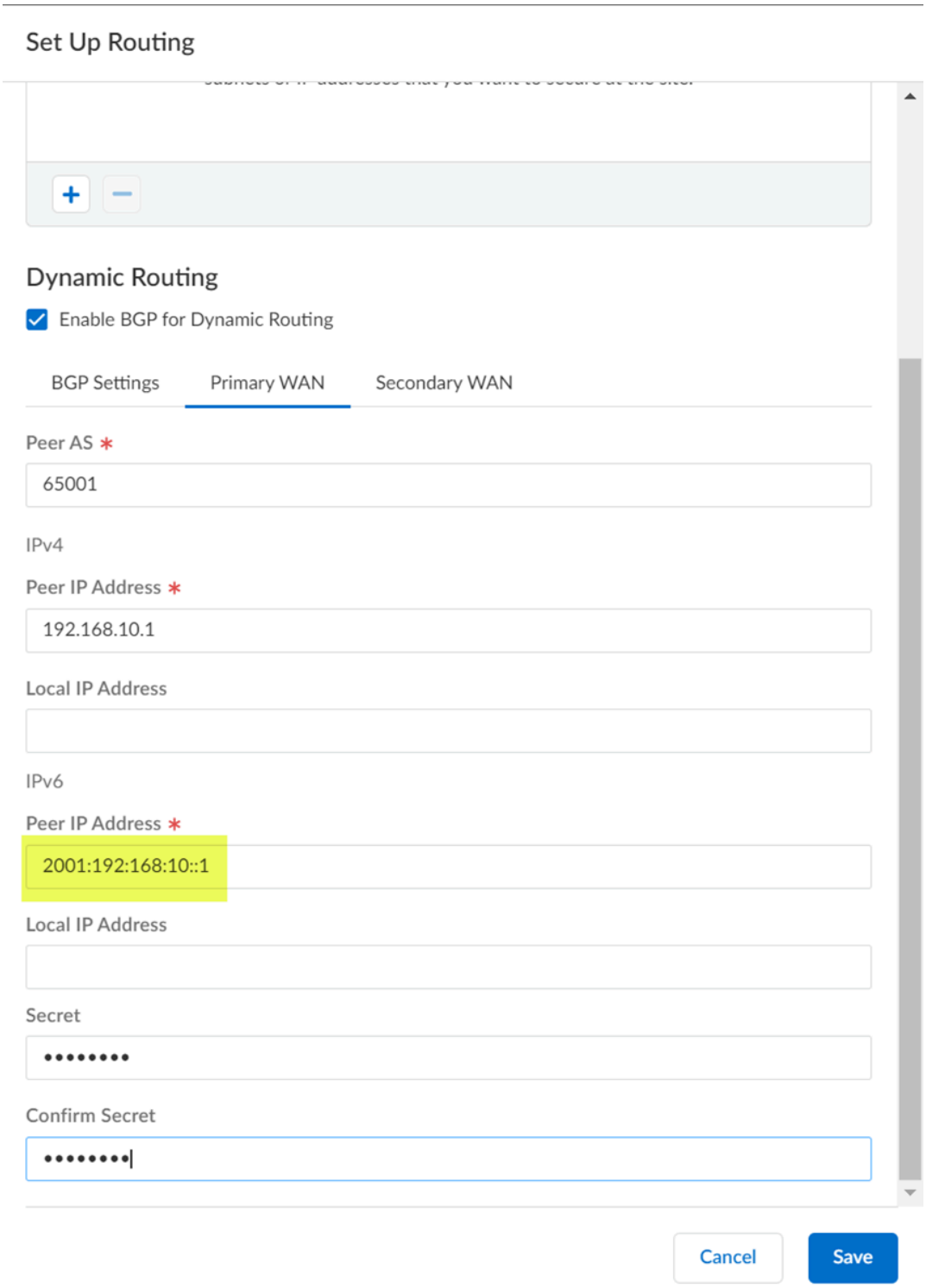
STEP 4 | リモート ネットワークのIPv6ルーティングをセットアップします。

1. (スタティック ルーティング デプロイメントのみ) 1 **[Corporate Subnets (**企業サブネット**)]** の **[Static Routes (**スタティック ルート**)]** タブを 1 つ以上入力します。



2. (BGPルーティングデプロイメントのみ) IPv4およびIPv6 BGPルートの交換方法を指定します。次に、IPv6 ピアアドレス そして ローカルアドレスを入力します。。
   - 単一の IPv4 BGPセッションを使用してIPv4とIPv6の両方のBGPピアリング情報を交換するには、**IPv4** ピアリング経由で**IPv4**ルートと**IPv6**ルートの両方を交換します。
   - IPv4 BGPピアリング情報を交換するIPv4 BGPセッションと、IPv6 BGPピアリング情報を交換するIPv6セッションの場合は、**IPv4**ピアリング経由の**IPv4**ルートと**IPv6**ピアリング経由の**IPv6**ルートの交換します。
   - 単一のIPv6 BGPセッションを使用してIPv6 BGPピアリング情報を交換するには、**[IPv6** ピアリング経由の **IPv6** ルートの交換**]**を選択します。
3. セカンダリWANが異なるピアアドレスまたはローカルアドレスを使用する場合は、［プライマリ**WAN**と同じ］の選択を解除し、セカンダリWANのIPv6ピアアドレスとローカルアドレスを入力します。

©2025 Palo Alto Networks, Inc.



STEP 5 | (任意) 使用している内部DNSサーバにIPv6アドレスで到達可能な場合は、 [ワークフロー] > **[Prisma Accessのセットアップ]** > [リモートネットワーク] > [詳細設定]を選択し、 **[DNSプロキシ]**を見つけ、ルールの[追加]をするか、デフォルトのルールを指定し、 [カスタ

©2025 Palo Alto Networks, Inc.

ムDNSサーバー] [プライマリDNS]のIPv6 アドレスおよび[セカンダリDNS] サーバーを指定します。

Prisma Accessでは、組織内部のドメインと外部のドメインの両方のドメインを解決する、DNSサーバーを指定することができます。指定しなかった場合、リモートネットワーク用のDNSリクエストのプロキシを行いません。また、 リージョンを選択する必要があります。

プライマリDNSサーバーとセカンダリDNSサーバーのIPv4またはIPv6アドレスの任意の組み合わせを入力できます。

- *IPv4*アドレスは*A*レコードを使用し、*IPv6*アドレスは*AAAA*レコードを使用します。一部の*DNS*サーバーは*IPv4*トランスポート経由で*AAAA DNS*検索を実行できるため、*IPv6 IP*アドレスを持つサーバーは必要ない場合もあります。

STEP 6 | リモートネットワーク接続の設定をまだ完了していない場合は、ここで完了します。

リモートネットワーク接続の*IPv6*インターネットアクセスは、*IPv6*トラフィックが*IPv4*トンネルを通過するアンダーレイ接続によって有効になります。

STEP 7 | **[Push Config (設定をプッシュ)]**を 実行して、変更をネットワークにデプロイします。

リモートネットワークのIPv6ネットワーキングの有効化 (Panorama)

STEP 1 | (任意) カスタムDNSサーバー プロキシ設定にIPv6アドレスを入力します。

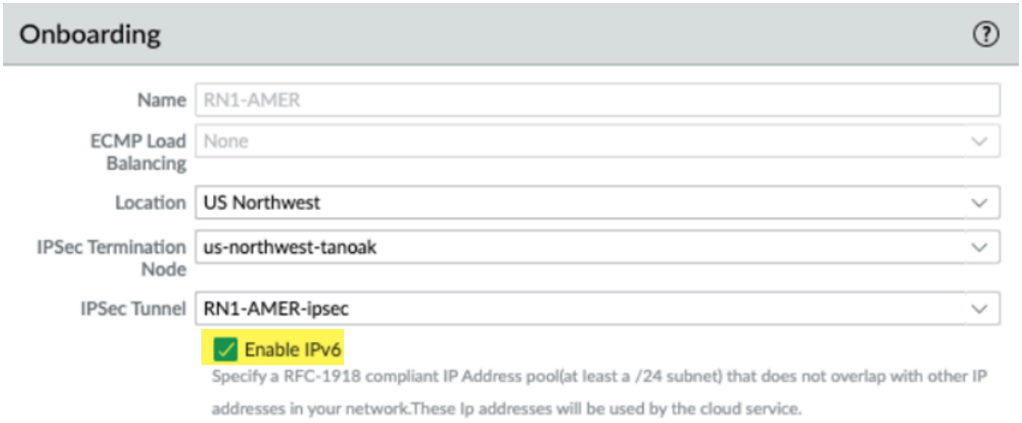
1. **Panorama** > **Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Remote Networks**（リモートネットワーク）の順に選択して、**Settings**（設定）エリアの歯車型アイコンをクリックして設定を編集します。
2. **DNS** プロキシ領域で、DNS プロキシ設定の IPv6 カスタムDNSサーバー アドレスを入力します。

STEP 2 | **[Panorama]** > **[Cloud Services**（クラウドサービス）**]** > **[Configuration**（設定）**]** > **[Remote Networks**（リモートネットワーク）**]**を選択します。

STEP 3 | 新しいリモートネットワーク接続を追加するか、既存のリモートネットワーク接続を選択して編集します。

©2025 Palo Alto Networks, Inc.

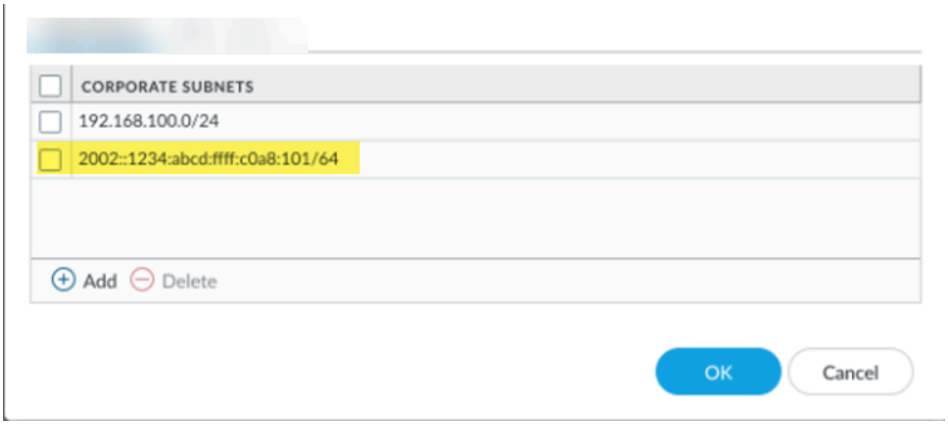
STEP 4 | **IPv6**を有効にします。



 ©2025 Palo Alto Networks, Inc.

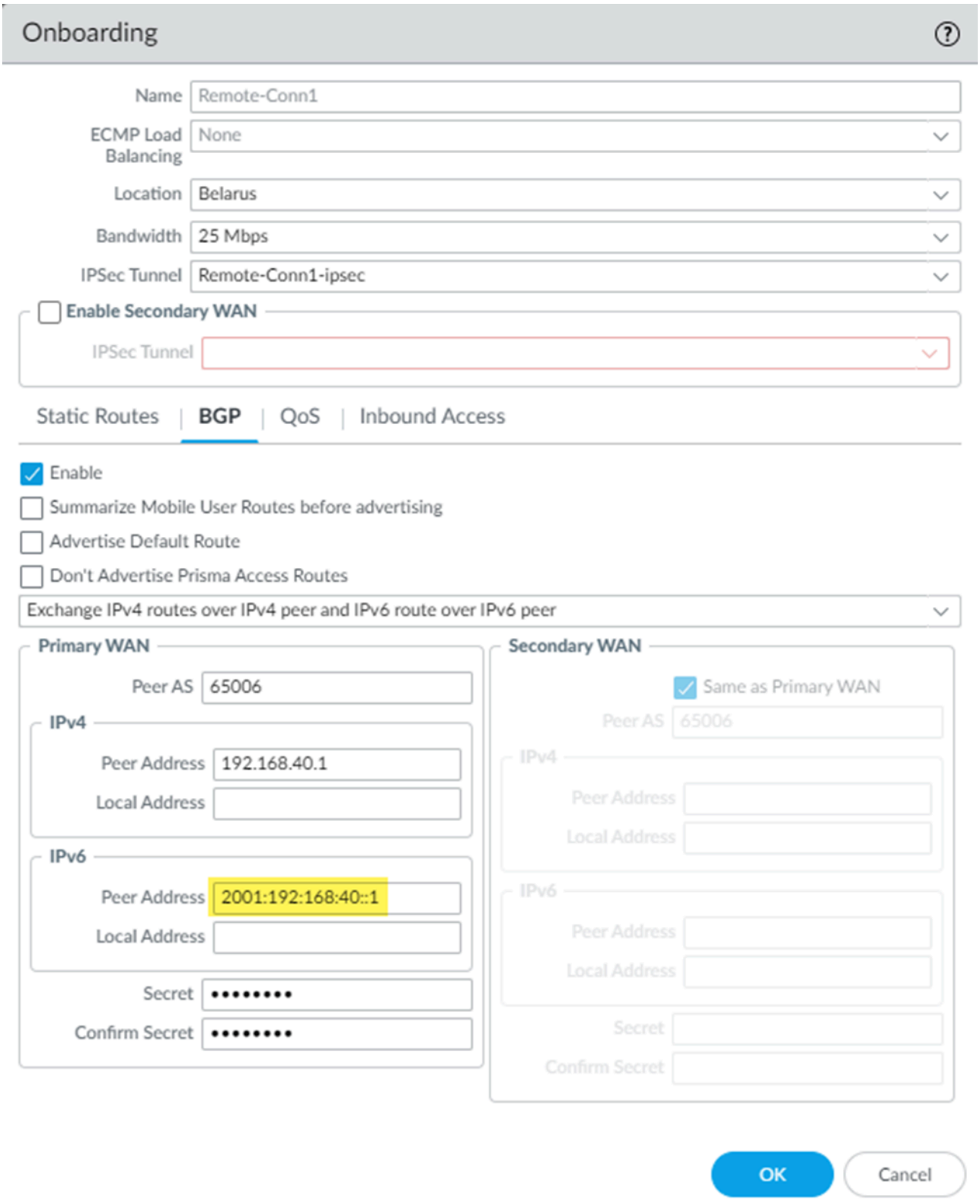
STEP 5 | リモート ネットワークのIPv6ルーティングをセットアップします。

1. (スタティック ルーティング デプロイメントのみ) 1 **[Corporate Subnets (**企業サブネット**)]** の **[Static Routes (**スタティック ルート**)]** タブを 1 つ以上入力します。



2. (BGPルーティングデプロイメントのみ) IPv4およびIPv6 BGPルートの交換方法を指定します。次に、IPv6 ピアアドレス そして ローカルアドレスを入力します。。
   - 単一の IPv4 BGPセッションを使用してIPv4とIPv6の両方のBGPピアリング情報を交換するには、**IPv4** ピアリング経由で**IPv4**ルートと**IPv6**ルートの両方を交換します。
   - IPv4 BGPピアリング情報を交換するIPv4 BGPセッションと、IPv6 BGPピアリング情報を交換するIPv6セッションの場合は、**IPv4**ピアリング経由の**IPv4**ルートと**IPv6**ピアリング経由の**IPv6**ルートの交換します。
   - 単一のIPv6 BGPセッションを使用してIPv6 BGPピアリング情報を交換するには、**[IPv6** ピアリング経由の **IPv6** ルートの交換]を選択します。
3. セカンダリWANが異なるピアアドレスまたはローカルアドレスを使用する場合は、［プライマリ**WAN**と同じ］の選択を解除し、セカンダリWANのIPv6ピアアドレスとローカルアドレスを入力します。

©2025 Palo Alto Networks, Inc.



STEP 6 | (任意) 内部DNSサーバーがIPv6 アドレスでアクセスできる場合は、**[Panorama]** > **[Cloud Services]** > **[Configuration (構成)]** > **[Remote Network (リモート ネットワーク)]** > **[Settings (設定)]**選択し、歯車アイコンをクリックして設定を編集し、**[DNS プロキシ]** タブを選択し

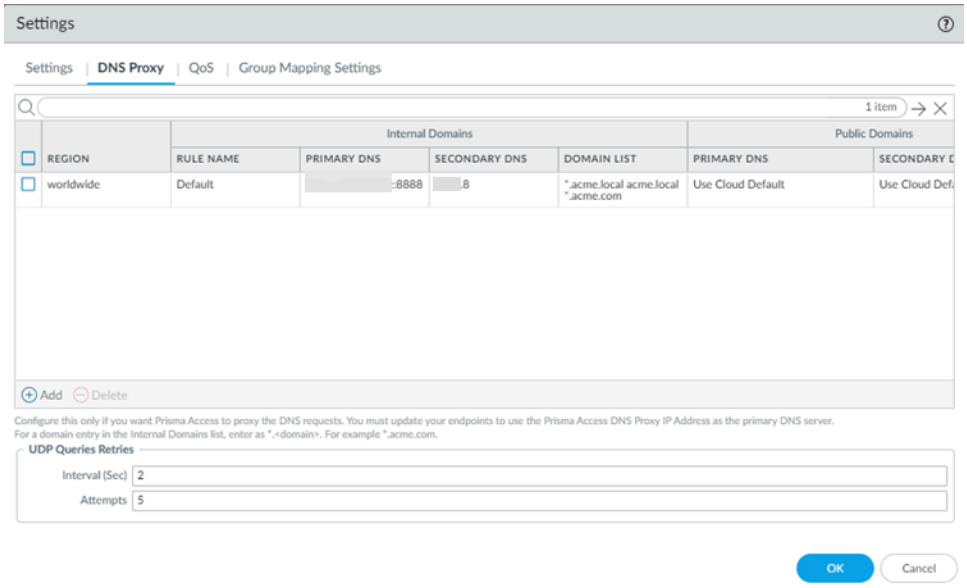
©2025 Palo Alto Networks, Inc.

てルール を追加する か、既定のルールを指定して、 プライマリ **DNS** サーバー と セカンダリ **DNS** サーバーの [カスタム **DNS** サーバー] IPv6 アドレスを指定します。

Prisma Accessでは、組織内部のドメインと外部のドメインの両方のドメインを解決する、DNSサーバーを指定することができます。指定しなかった場合、Prisma Accessはリモートネットワーク用のDNSリクエストのプロキシを行いません。また、 リージョンを選択する必要があります。

プライマリDNSサーバーとセカンダリDNSサーバーのIPv4またはIPv6アドレスの任意の組み合わせを入力できます。

*IPv4*アドレスは*A*レコードを使用し、*IPv6*アドレスは*AAAA*レコードを使用します。一部の*DNS*サーバーは*IPv4*トランスポート経由で*AAAA DNS*検索を実行できるため、*IPv6 IP*アドレスを持つサーバーは必要ない場合もあります。



STEP 7 | リモートネットワーク接続の設定をまだ完了していない場合は、ここで完了します。

STEP 8 | 変更を **Commit and Push**（コミットしてプッシュ）します。

STEP 9 | **Panorama** > **Cloud Services**（クラウドサービス） > **Status**（ステータス） > **Network Details**（ネットワーク詳細） > **Remote Networks**（リモートネットワーク）を選択して、**EBGP Router**（**EBGP**ルーター）のアドレスを書き留めておきます。

変更をコミットすると、サービス接続用のIPv6**EBGP** ルーターアドレスが作成されます。

リモート ネットワーク接続に使用されるIPSecトンネルはIPv4アドレスを使用するため、サービス**IP**アドレス はIPv4アドレスのままになります。

リモートネットワーク接続のIPv6インターネットアクセスは、IPv6トラフィックがIPv4トンネルをパススルーするアンダーレイ接続によって有効になります。

©2025 Palo Alto Networks, Inc.

モバイルユーザーのためのDNS解決—GlobalProtectとリモートネットワークデプロイメント

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンスバージョン2.2以降を推奨 ❑ パブリックおよびプライベートアプリへのネイティブIPv6アクセスには、以下の最小リリースが必要です: • Prisma Access (Managed by Strata Cloud Manager):2024年6月のリリース • Prisma Access (Managed by Panorama):Prisma Access5.1.1は新規デプロイメントのみ。 その他のデプロイメント（既存のPrisma Access (Managed by Panorama)デプロイメントを含む）は、プライベート アプリ アクセスのみをサポートします。

Prisma Accessでは、組織内部のドメインと外部のドメインの両方のドメインを解決する、DNSサーバーを指定することができます。Prisma Accessは、DNSサーバーの設定に基づいて、DNSリクエストのプロキシを行います。サポートされている内部および外部ドメインに対するDNS解決方法、およびPrisma AccessがDNSリクエストのプロキシを行う場合を次の表に示します。

内部DNS解決方法	外部DNS解決方法	Prisma AccessがDNSリクエストのプロキシを行う（はい/いいえ）
内部ドメイン用に構成されたDNSサーバーの単一ルール	クラウドデフォルト（IPv6用のGoogle Public DNS64）	あり
内部ドメイン用に構成されたDNSサーバーの単一ルール	内部ドメインと同じ	いいえ
内部ドメイン用に構成されたDNSサーバーの単一ルール	カスタムDNSサーバー（IPv6用のGoogle Public DNS64）	あり
ドメインのための単一ルール、クラウドデフォルト設定	クラウドデフォルト（IPv6用のGoogle Public DNS64）	あり

©2025 Palo Alto Networks, Inc.

内部DNS解決方法	外部DNS解決方法	Prisma AccessがDNSリクエストのプロキシを行う（はい/いいえ）
ドメインのための単一ルール、クラウドデフォルト設定	内部ドメインと同じ (IPv6 用の Google Public DNS64)	あり
ドメインのための単一ルール、クラウドデフォルト設定	カスタムDNSサーバー（IPv6用のGoogle Public DNS64）	あり
内部ドメイン用に構成されたDNSサーバーの複数のルール	クラウドデフォルト（IPv6用のGoogle Public DNS64）	あり
内部ドメイン用に構成されたDNSサーバーの複数のルール	内部ドメインと同じ	あり
内部ドメイン用に構成されたDNSサーバーの複数のルール	カスタムDNSサーバー（IPv6用のGoogle Public DNS64）	あり
設定なし	カスタムDNSサーバー（IPv6用のGoogle Public DNS64）	あり
設定なし	クラウドデフォルト（IPv6の場合、プライマリ = Google Public DNS64、セカンダリ = クラウドデフォルト）	いいえ
設定なし	設定なし	いいえ
DNSサーバーが指定されていない（デフォルト設定が存在しており、その場合クラウドのデフォルトが使用される）	DNS解決が指定されていない	いいえ
ZTNAコネクタ（*DNS*解決方法に関係なく）	該当なし	あり
ZTNA Connectorを有効にすると、Prisma Accessは、リモートネットワークおよびモバイルユーザー-GlobalProtect用に設定されたDNSルールを使用して、すべてのDNSリクエストをプロキシします。		

©2025 Palo Alto Networks, Inc.

DNSリクエストのソースIPアドレスは、Prisma AccessがDNSリクエストのプロキシを行うかどうかによって異なります。

- Prisma AccessがDNSリクエストのプロキシを行わない場合、DNSリクエストのソースIPアドレスがDNSルックアップをリクエストしたデバイスのIPアドレスに変更されます。このソースIPアドレスにより、ソースIPアドレスベースのDNSポリシーの採用、または悪意のあるドメインと通信しているエンドポイントの識別を行うことができます。この動作は、モバイルユーザーおよびリモートネットワークデプロイ環境の両方に適用されます。
- Prisma AccessがDNSリクエストのプロキシを行う場合、DNSリクエストのソースIPアドレスは、次のアドレスに変更されます。
  - モバイルユーザーデプロイ環境–DNSリクエストの送信元IPアドレスは、内部リクエストの場合モバイルユーザーIPアドレスプールから、外部リクエストの場合モバイルユーザーのロケーションのゲートウェイIPアドレスから取得されたIPアドレスになります。
  - リモートネットワークデプロイ環境–DNSリクエストの送信元IPアドレスは、内部リクエストの場合は**EBGP**ルーターアドレス、外部リクエストの場合はリモートネットワーク接続のサービスIPアドレスです。

Prisma AccessでDNS解決を使用する際のガイドラインと制限は以下の通りです:

- Prisma Accessがサポートする TCP DNSリクエストの最大同時保留数（**Max Pending Requests**）は64です。
- UDPクエリの場合、DNSプロキシは2秒以内に応答を受け取らなかった場合、別のリクエストを送信し、次のDNSサーバーを試す前に最大5回再試行します。
- Prisma Accessは、300秒の有効期限（TTL）値を持つDNSエントリをキャッシュします。EDNSの応答もキャッシュされます。

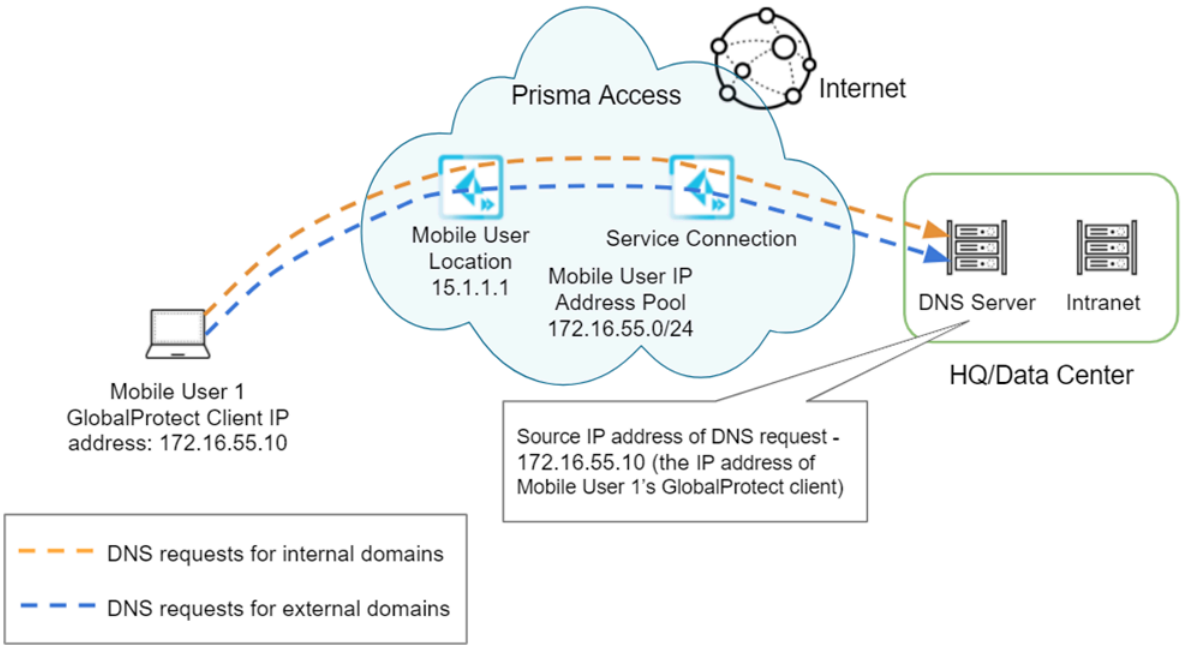
モバイルユーザー向けのDNS解決 – GlobalProtectデプロイメント

どこで使用できますか?	何が必要ですか?
• Panorama	• Prisma Accessライセンス

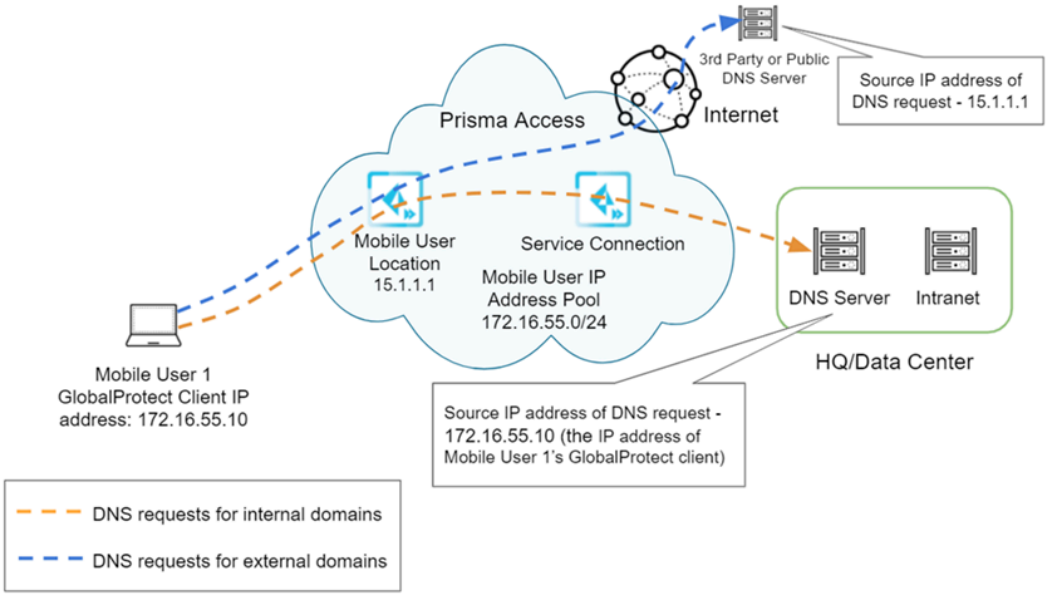
次のセクションは、モバイルユーザー向けおよびリモートネットワーク向けのDNS解決を設定後の、DNSリクエストの送信元IPアドレスをPrisma Accessがどのように処理するかを例で説明しています。

内部ドメインと外部ドメインの両方を解決する、内部DNSサーバーを割り当てたデプロイ環境を次の図に示します。この場合、Prisma AccessはDNS要求をプロキシせず、DNS要求はモバイルユーザー1のGlobalProtectクライアントIPアドレスからです。GlobalProtectクライアントは、このIPアドレスをモバイルユーザーに割り当てます。このアドレスは、モバイルユーザーロケーションのゲートウェイIPアドレスから取得されます。

 ©2025 Palo Alto Networks, Inc.

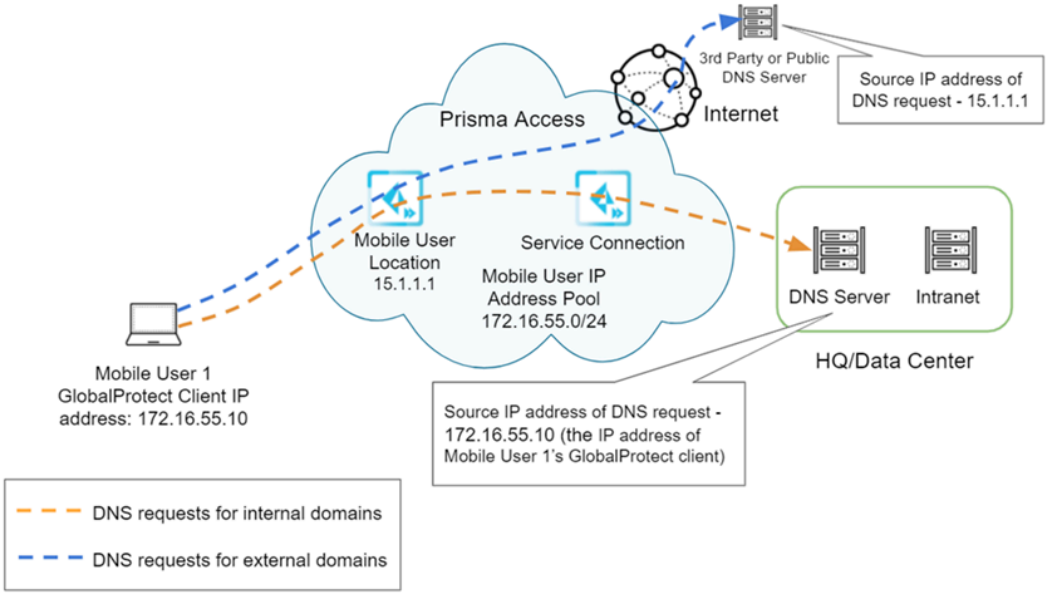


本社またはデータセンター内のDNSサーバーが、内部ドメインのDNSリクエストを解決している例を次の図に示します。外部ドメインのリクエストは、Prisma Accessのクラウドのデフォルトの DNSサーバーが解決します。この場合、Prisma Accessは外部要求に対する要求をプロキシし、送信元IPアドレスはPrisma Accessゲートウェイ IPアドレス（この例では 15.1.1.1）になるが、内部送信元IPはモバイルユーザー1のGlobalProtect クライアントIPアドレスのままとなります。



外部ドメインへのリクエスト用に、インターネット経由でアクセス可能なサードパーティまたはパブリックDNSサーバーを使用している組織の例を次の図に示します。Prisma Accessはこれらのリクエストもプロキシします。

 ©2025 Palo Alto Networks, Inc.



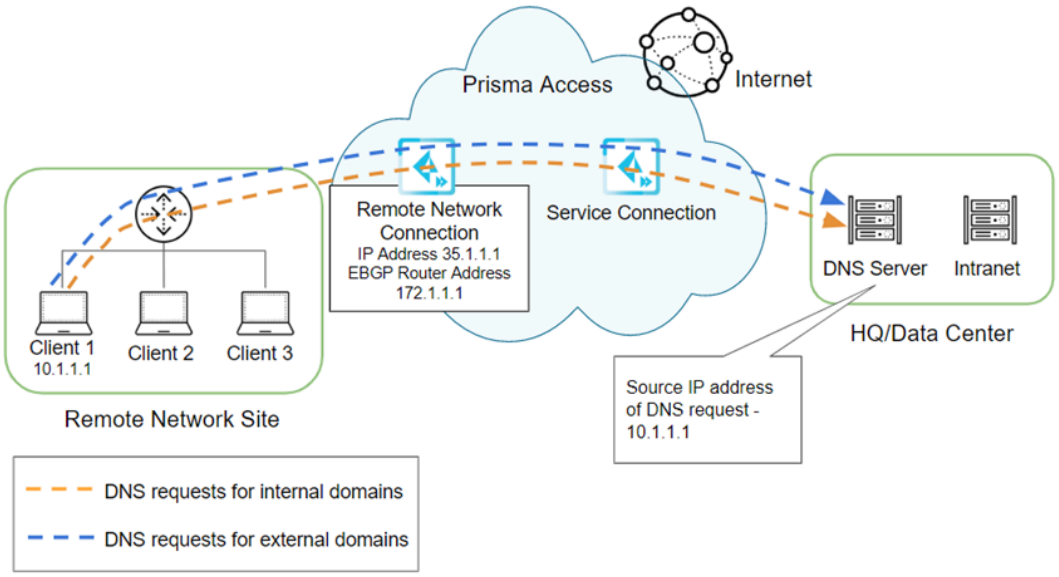
リモートネットワークのDNS解決

どこで使用できますか?	何が必要ですか?
• Panorama	• Prisma Accessライセンス

既存のリモートネットワークデプロイ環境がある場合、すでに存在しているDNS解決手段を利用することも、Prisma AccessにDNSリクエストのプロキシを行わせることも可能です。DNSリクエストのプロキシを行うことで、パブリックドメインのDNSリクエストをあるサーバーに送信し、内部ドメインのDNSリクエストを別のサーバーに送信することができます。

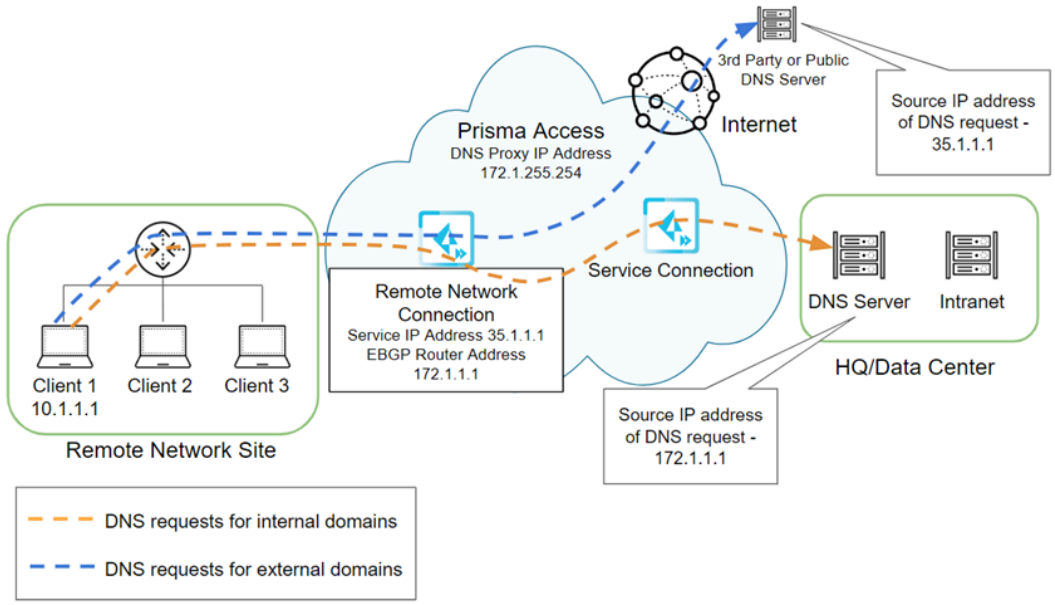
内部および外部ドメインの両方のリクエストを処理するために使われる、内部DNSサーバーが存在するデプロイ環境へのDNSリクエストを次の図に示します。リモートネットワークIPアドレスは35.1.1.1、**EBGP Router**のIPアドレスは172.1.1.1になります。この場合、Prisma Accessはリクエストのプロキシを行いません。また、内部DNSサーバーがNATを使用していない場合、DNSリクエストのソースIPは10.1.1.1（リモートネットワークサイト内のクライアント1のデバイスのIPアドレス）になります。

©2025 Palo Alto Networks, Inc.



Prisma AccessがDNSリクエストのプロキシを行う場合、プロキシされたDNSリクエストのソースIPアドレスは内部リクエストの場合**EBGP Router Address**（**EBGP**ルーターアドレス）に、外部リクエストの場合はリモートネットワーク接続のService IP Address（サービスIPアドレス）になります。次の図を参照してください。

*Prisma Access*がプロキシを行う外部リクエストに対して、ネットワークが使用する*DNS*アドレスを設定する場合、***Remote Network DNS Proxy IP Address***（リモートネットワーク***DNS***プロキシ***IP***アドレス）（***[Panorama]*** > ***[Cloud Services***（クラウドサービス）***]*** > ***[Status***（ステータス）***]*** > ***[Service Infrastructure***（サービスインフラ）***]*** > ***[Remote Network DNS ProxyIP Address***（リモートネットワーク***DNS***プロキシ***IP***アドレス））***]***を指定します。次の例では、*DNS*サーバーに対してネットワーク内の*172.1.255.254*を指定します。



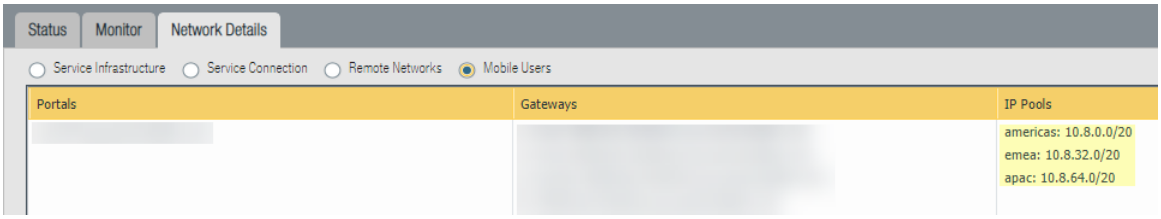
©2025 Palo Alto Networks, Inc.

サービス接続およびリモートネットワーク接続用にBGPがモバイルユーザーIPアドレスプールをアドバタイズする仕組み

どこで使用できますか?	何が必要ですか?
• Panorama	• Prisma Accessライセンス

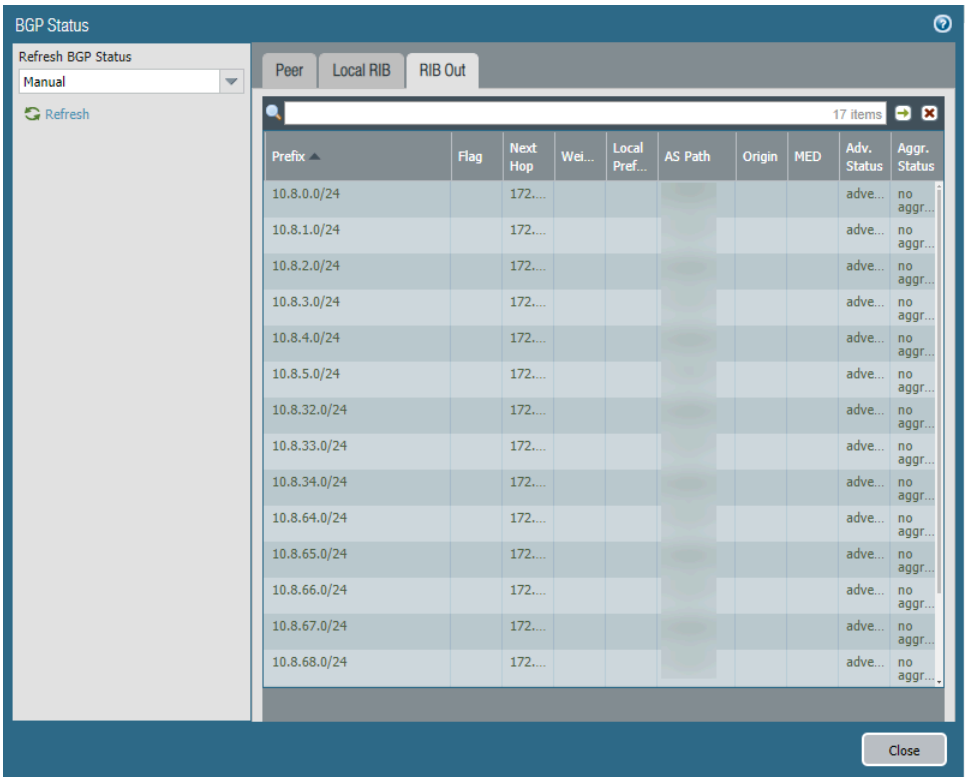
サービス接続またはリモートネットワーク接続のためにBGPを有効にする場合、GlobalProtectモバイルユーザーの設定 (Panorama)の後、Prisma Accessはクラスc（/24）アドレスブロックを使用して指定したモバイルユーザーIPアドレスプールを割り当てます。そのためBGPは、その地域に関連付けられているプール全体ではなく、「/24」のブロックで割り当てられたモバイルユーザーサブネットにアドバタイズします。Prisma AccessがPrisma Accessゲートウェイ用に「/24」サブネットを追加すると、自動的にBGPアドバタイズメントが送信されます。サブネットが追加、削除されていくにつれて、Prisma AccessはそのBGPアドバタイズメントを自動的に更新します。この割り当て方法は、BGPルートをアドバタイズする場合、特に地域ごとにプールを割り当てる代わりに、**Worldwide**プールを設定した場合に、柔軟性が向上します。IPアドレスプールを小さなサブネットに分割することで、割り当てられたアドレス空間を使い切った時に、同じサブネットを追加、削除したり、削除した後に別の地域でそれを再利用したりすることができます。

Panorama > **Cloud Services**（クラウドサービス） > **Status**（ステータス） > **Network Details**（ネットワーク詳細） > **Mobile Users**（モバイルユーザー）**—GlobalProtect**の順に選択して表示される次の画面は、地域別に分割したモバイルユーザー向けの、3つの「/20」IPプールを表しています。



Panorama > **Cloud Services**（サービス） > **Status**（ステータス） > **Network Details**（ネットワーク詳細） > **Service Connection**（サービス接続） > **Show BGP Status**（**BGP**ステータスを表示）の順に選択して表示される**RIB Out**テーブル（**Branch AS and Router**エリア内）は、BGPルートアドバタイズメント用に「/24」サブネットのブロックに分割されたモバイルユーザーアドレスプールを表しています。「/20」サブネット全体にはアドバタイズされないことに注意してください。

©2025 Palo Alto Networks, Inc.



©2025 Palo Alto Networks, Inc.

Prisma AccessとStrata Logging Serviceのプロキシサポート

どこで使用できますか?	何が必要ですか?
• Panorama	• Prisma Accessライセンス

Panorama、Prisma Accessインフラストラクチャ、およびStrata Logging Serviceの間にプロキシサーバーをデプロイする場合、予期 される動作の詳細については、以下の表を参照してください：

機能	SSL復号化を実施しないプロキシサーバーを介したサポート	SSL復号化を実施するプロキシサーバーを介したサポート
OCSPを使った**Certificate Revocation Status**（証明書失効ステータス）チェックによる、**Strata Logging Service**への初期オンボーディング	サポート	パススループロキシのみがサポートされています。SSL復号化を使用するプロキシはサポートされていません。
レポートおよびログに対する**Strata Logging Service**への**Panorama**クエリ	プロキシサーバーがPanoramaのデフォルトルートである場合、ACCおよび**Monitor**（監視） > **Logs**（ログ）ページのデータを参照することはできません。 PanoramaにStrata Logging Serviceへの代替ルートが存在しており、プロキシサーバーをバイパスできる場合、ACCおよび**Monitor**（監視） > **Logs**（ログ）ページのデータを参照することはできます。	

©2025 Palo Alto Networks, Inc.

特定の国からの着信接続をブロックする

Prisma Accessは、指定した国からのリモート ネットワーク、モバイル ユーザー - GlobalProtect、およびモバイル ユーザー - 明示的なプロキシのデプロイメントに対するログイン試行をブロックするセキュリティ ポリシー ルールを作成できます。 Prisma Accessは、クライアントの送信元IPアドレスからの地理的位置情報に基づいて、指定した国からの着信接続をブロックします。

これらの国からの着信接続をブロックするには、次のタスクを完了します。

STEP 1 | 特定のルール名のいずれかを使用して、セキュリティ ポリシーの事前ルールを作成します。

このルールは必ず事前ルールとして設定してください。

- モバイル ユーザー - GlobalProtectデプロイメントに対して国をブロックするには、**Mobile_User_EMBG_Source_Countries**という名前のルールを作成します。
- モバイル ユーザー - 明示的プロキシデプロイメントに対して国をブロックするには、**Explicit_Proxy_EMBG_Source_Countries**という名前のルールを作成します。
- リモート ネットワークのデプロイメントで国をブロックするには、**Remote_Network_EMBG_Source_Countries**という名前のルールを作成します。

STEP 2 | **PA_predefined_embargo_rule**という名前のルールのタグを追加します。

STEP 3 | ソースでブロックする国を1つ以上追加します。

STEP 4 | **Drop**のアクションを指定します。

©2025 Palo Alto Networks, Inc.

AWS WorkSpaceからの安全なインターネットトラフィック

組織は、Amazon WorkSpaceクラウドベースの仮想マシンを介してインターネットにアクセスするリモートワーカー、請負業者、病院スタッフ、コールセンターユーザーを保護するためのアプローチを再考する必要があります。これらのユーザーは、インターネットに安全にアクセスでき、インターネットベースの脅威から保護された状態を保ちながら、組織がこれらのクラウドホスト型仮想マシンを通じて発生するインターネットトラフィックを完全に可視化できる必要があります。

ワークフォース、データ、クラウドアプリケーションの分散が進む今日の複雑で革新的な経済では、リモートワーカーやリソース向けに設計された従来のネットワーキングモデルではもはや十分ではありません。組織はクラウドサービスの柔軟性とスケーラビリティを必要としていますが、これらのサービスには独自のニーズを満たすように設計されたクラウドセキュリティソリューションが必要です。

Prisma SASE と AWS WorkSpace の詳細をご覧ください。

Palo Alto NetworksのStrata Cloud Managerを使用すると、以下の方法で AWS WorkSpaceのインターネットへの安全なアクセスを提供できます。

- AWS WorkSpaceクライアントでPACファイルを設定する
- AWSとPrisma Access間のサイト間トンネルの設定

AWS WorkSpaceクライアントでPACファイルを設定する

Amazon WorkSpacesからのインターネットトラフィックを保護する1つの方法は、プロキシ自動設定 (PAC) ファイルを使用することです。PACファイルは、Webブラウザにプロキシ サーバーに接続する方法を指示するJavaScriptコードです。エンタープライズ環境では、PACファイルを使用してWebトラフィックを制御し、セキュリティ ポリシー ルールを適用します。通常、WebサーバーはPACファイルを保存し、Webブラウザーは起動時にPACファイルをダウンロードします。

STEP 1 | まだ設定していない場合は、Prisma SASE Explicit Proxy を設定します。

PACファイルをPrisma SASEまたはWebサーバーでホストできます。Webブラウザを使用してPAC URLにアクセスし、WorkSpaceクライアントからPACサーバーにアクセスできることを確認します。

STEP 2 | Prisma SASE Explicit Proxy PACファイルをカスタマイズして、プロキシFQDNを更新し、除外を定義します。

1. Strata Cloud Managerから**[Workflows (ワークフロー)]** > **Prisma Access [Setup (セットアップ)]** > **[Explicit Proxy (明示型プロキシ)]** > **[Forwarding Rules (転送ルール)]**を選択します。
2. PAC ファイルのガイドラインに従ってPACファイルを編集します。

STEP 3 | Prisma SASE Explicit Proxyルート証明書をダウンロードして、AWS WorkSpaceにインストールします。

©2025 Palo Alto Networks, Inc.

STEP 4 | ユーザーベースのポリシー ルール、トラフィック検査、レポートを適用するには、AWS WorkSpaceクライアントに証明書をインストールします 。

これにより、WorkSpaceクライアントはPrisma SASE Explicit Proxyと通信できるようになります。

STEP 5 | AWS WorkSpaceでPACファイルを設定します。

これを行う方法は、使用しているブラウザによって異なります。

- Google Chrome:
  1. Chromeを開きます。
  2. ウィンドウの右上隅にある 3 つのドットを選択します。
  3. [設定]を選択します。
  4. [詳細]を選択します。
  5. [システム]の下で、[プロキシ設定を開く]を選択します。
  6. [ローカル エリア ネットワーク (LAN) の設定] ウィンドウで、[自動構成スクリプトを使用する]を選択します。
  7. [アドレス] フィールドに、PACファイルのURLを入力します。
  8. 変更を保存するには、**[OK]** を選択します。
- Firefox
  1. Firefox を開きます。
  2. ウィンドウの右上隅にある 3 本の線を選択します。
  3. [オプション]を選択します。
  4. [詳細]を選択します。
  5. [ネットワーク]で [設定]を選択します。
  6. [接続設定] ウィンドウで、[自動プロキシ構成 **URL**]を選択します。
  7. **URL** フィールドにPACファイルのURLを入力します。
  8. 変更を保存するには、**[OK]** を選択します。

PACファイルを適用すると、ChromeとFirefoxはそれを使用して、各Webサイトに使用するプロキシ サーバーを決定します。

STEP 6 | AWS WorkSpaceブラウザを再起動します。

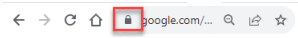
WorkSpaceブラウザが再起動すると、新しいPACファイルが選択され、Prisma SASEプロキシを介してトラフィックのルーティングが開始されます。

©2025 Palo Alto Networks, Inc.

STEP 7 | トラフィックフローをテストして検証します。

WorkSpaceクライアントがPrisma SASE Explicit Proxyを使用するように設定したら、ブラウザで証明書を検証し、Prisma Accessでログを表示して、トラフィックフローをテストできます。

1. Google Chromeを使用している場合は、アドレスバーの南京錠を選択します。



   1. **[Connection is secure (**接続は安全です**)]**を選択します。
   2. **[Certificate is valid (**証明書が有効です**)]**を選択します。
   3. ポップアップに表示される正しい証明書の詳細を確認します。
2. Safariを使用している場合は、アドレスバーの南京錠アイコンを選択します。
   1. **[Connection secure (**接続のセキュリティ保護**)]**を選択します。
   2. [詳細情報]を選択します。
   3. [証明書の表示]を選択します。
   4. ポップアップに表示される正しい証明書の詳細を確認します。

AWSとPrisma Access間のサイト間トンネルの設定

ビジネスの規模が拡大し、AWS WorkSpaceクライアントをいくつか実行している場合でも、Prisma AccessRemote Networksを使用すると、WorkSpaceを迅速にオンボードし、ユーザーに最高水準のセキュリティを提供できます。WorkSpaceの構成と管理を簡素化する便利なオプションを提供します。

組織は、AWSとPrisma Accessの間にIPSecトンネルを確立することで、AWS WorkSpaceユーザーをPrisma Accessにオンボードすることができる。

リモート ネットワークを使用する利点は、インターネットにアクセスするためにPrisma Access経由で接続するユーザーのアウトバウンド インターネット トラフィックを保護できることです。

STEP 1 | Amazon WorkSpaceにバーチャル プライベート クラウド（VPC）を設定するか、既存のVPCをAmazon WorkSpaceに使用します。

STEP 2 | AWSトランジットゲートウェイをVPCに接続して、AWSとPrisma Access間のサイト間IPSecトンネルを構成します。

STEP 3 | AWSトランジットゲートウェイとPrisma Accessリモートネットワーク間のIPSec VPNを設定します。

STEP 4 | Prisma Accessリモートネットワークでは、AWS WorkSpaceユーザーを保護するために、インターネットトラフィックを制限するセキュリティルールを定義できます。

 ©2025 Palo Alto Networks, Inc.

デフォルトルートなしネットワークのPrisma Access

どこで使用できますか?	何が必要ですか?
• Prisma Access	❑ Prisma Accessライセンス

デフォルトルートなしネットワークとは？

デフォルトルートなしネットワークとは、デフォルトルートが設定されていないネットワークです。ネットワークにデフォルトルートが設定されていない場合、未知の宛先宛てのパケットはドロップされます。エンタープライズでは、ユーザーのアクセスを制限するためにデフォル トルート ネットワークを使用しないことがよくあります。デフォルトルートがないネットワーク上のデバイスが特定の宛先 (IPアドレスまたはサブネット) にアクセスする必要がある場合、管理者はその宛先のルートを手動で設定する必要があります。エンタープライズはまた、デフォルトルートのないブランチ ネットワーク上のユーザー、サーバー、およびデバイスに、制限付きで安全なインターネットアクセスを必要としています。

誰かがデフォルト ルートなしのネットワークを設定したいと思う理由はいくつかあります。

- ネットワーク上の侵害されたエンドポイントからランダムな宛先へのアウトバウンドの悪意のあるトラフィックやDDoSトラフィックをブロックすることでセキュリティを強化し、Denial-Of-Service (サービス拒否 - DOS)攻撃やその他の悪意のあるトラフィックから保護します。
- 処理するルートの数を減らすことで、ルーティングデバイスのパフォーマンスを向上させます。
- 特定の宛先に特定のルートを設定することにより、ユーザーの特定のニーズを満たすルーティングポリシーを実装します。

デフォルトルートネットワークに関する考慮事項なし

デフォルトではないネットワークからのインターネットトラフィックを保護する場合、エンタープライズはインターネットと通信している可能性のあるブランチネットワーク内のユーザー、エンドポイント、サーバー、およびデバイスを明確に評価する必要があります。

デフォルトルートブランチがない場合、さまざまなオペレーティングシステムを搭載したデバイス、VDIなどのマルチユーザーまたは共有エンドポイント、およびサーバーやIoTデバイスなどのヘッドレスデバイスが存在する可能性があります。これらすべてのデバイスからのインターネットトラフィックにはセキュリティが必要です。これらすべてのユースケースに対応し、さまざまな接続方法に柔軟に対応し、デバイスの種類に関係なくインターネット アクセスを一貫して保護する統合型プラットフォームを提供するソリューションが不可欠です。

©2025 Palo Alto Networks, Inc.

デフォルトルートがないネットワークのインターネットアクセスを保護するためのデプロイメント上の推奨事項

デフォルトルートがないネットワークを使用している場合、インターネットトラフィックを保護するための推奨事項は次のとおりです。

デバイス	推奨事項
Windows、MacOS	プロキシモードのGlobalProtectエージェント
Chrome OS、VDI	エージェントレスPACファイル
iOS、Android	エージェントレスPACファイル
Linux	エージェントレスPACファイル
Servers（サーバー）	エージェントレスPACファイル
IoTデバイス (プロキシ対応)	エージェントレスPACファイル
IoTデバイス (プロキシ非対応)	リモートネットワーク (IPsec)

主な考慮事項

デフォルトルートがないネットワークにGlobalProtectを導入する場合は、次の点を考慮してください。

- 境界デバイスにルートを追加し、ユーザーのインターネット トラフィックをPrisma Access Explicit Proxy IPアドレスにルーティングします。
- PACファイルを内部でホストして、IdP URLとPrisma AccessポータルURLを明示型プロキシに転送して、GlobalProtectがポータルとIdPに接続できるようにします。
- デフォルトルートがないネットワークのDNSサーバーが外部FQDNを解決できない場合は、内部DNSレコードを追加して明示型プロキシ、PACファイル、Prisma AccessポータルFQDNを解決します。
- 内部のPrisma Access明示型プロキシIPアドレスとPrisma AccessPortal IPアドレスのDNATを、実際の明示型プロキシIPアドレスとポータルIPアドレスに設定します。

*PAC*ベースのデプロイメントでは、*Prisma Access*ポータル*URL*を明示型プロキシに転送して、*Prisma Access*明示型プロキシ設定の認証設定から除外する必要はありません。

©2025 Palo Alto Networks, Inc.

Prisma Accessサービス接続の高度なデプロイメント:

どこで使用できますか?	何が必要ですか?
• Panorama	• Prisma Accessライセンス

以下のセクションでは、Prisma Accessサービス接続で利用可能な高度なデプロイメントについて説明します：

- サービス接続マルチクラウド冗長性
- トラフィックステアリングを使用したインターネット宛てのトラフィックのサービス接続への転送
- サービス接続トラフィックのルーティング
- 複数のサービス接続を使用して高帯域幅ネットワークを作成する

サービス接続マルチクラウド冗長性

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	☐ Prisma Accessのライセンス

サービス接続のマルチクラウド冗長性は、*Prisma Access 3.1 Innovation*からサポートされています。

Prisma Accessサービス接続を使用する場合は、モバイル ユーザーやリモート サイトのユーザーに、HQ またはデータ センター内の内部リソースやアプリへのアクセスを提供するには、異なるクラウド プロバイダーでアクティブ サービス接続とバックアップ サービス接続を作成することで、それらのリソースへのより回復力のあるアクセスを確保できます。これらのアクティブ サービス接続とバックアップ サービス接続を同じ場所または異なる地理的リージョンの異なる場所に指定できるため、クラウド プロバイダーまたはリージョンが利用できなくなった場合でも、サービス接続を介してリソースにアクセスできます。

サイト内のアクティブなサービス接続とバックアップ サービス接続を指定します。サイトとは、1 つ以上のサービス接続が終了する顧客データ センターまたは本社の場所 (オンプレミスまたはパブリック クラウド内) です。サービス接続を作成したら、 サイトを作成し、そのサイトにサービス接続を追加して、追加したサービス接続をアクティブまたはバックアップとして指定します。

クラウドプロバイダーまたは地域の停止により、サイト内のアクティブなサービス接続がダウンした場合、 Prisma Accessはこれらのルールを使用してトラフィックを再ルーティングし、モバイル ユーザーが引き続きその HQ またはデータ センター内のリソースにアクセスできるようにします。

- サイト内にアクティブなサービス接続が1つだけある場合、 Prisma Accessは トラフィックをルーティングするために、そのサイト内のバックアップ サービス接続を選択します。

©2025 Palo Alto Networks, Inc.

- サイト内に複数のアクティブなサービス接続がある場合、 Prisma Accessはトラフィックをルーティングするために別のアクティブなサービス接続を選択し、バックアップ サービス接続は、すべてのアクティブなサービス接続がダウンした場合にのみトラフィックをルーティングするために使用されます。

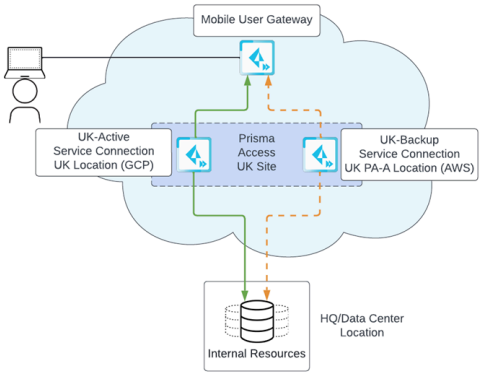
同じ国内のアクティブな場所とバックアップの場所を使用するサイトを利用するには、 国内の優先場所と代替場所を使用してサービス接続をオンボードし、サイトを作成して、それらの国内の場所をサイトに追加します。

Prisma Accessはサイトにオンボードしたサービス接続に関するステータス メッセージも提供します (たとえば、サイト内のすべてのサービス接続が単一のリージョンに展開されている場合など)。

次の例は、サイトを作成し、そこにサービス接続を追加することを活用する方法を示しています。

- 同じ地理的地域内の異なるクラウド プロバイダー- 特定の国でデータにアクセスする必要がある組織 (銀行など) の場合は、その国から優先場所を選択し、同じ国から代替場所を選択できます。次の例は、データの場所に関する規制に従うために英国でサービス接続をオンボードする英国の組織を示しています。この場合、組織の管理者は、英国の場所の UK-Active と英国の PA-A の場所の UK-Backup の 2 つのサービス接続を英国にオンボードします。英国のロケーションは英国の優先クラウド プロバイダー (GCP) によってホストされ、英国の PA-A ロケーションは、その国の代替クラウド プロバイダー (AWS) によってホストされます。国内の場所のリストには、 その国の優先クラウド プロバイダーと代替クラウド プロバイダーが表示されます。次に、管理者はサイトを作成し、そのサイト内のアクティブな場所として UK-Active を指定し、バックアップの場所として UK-Backup を指定します。

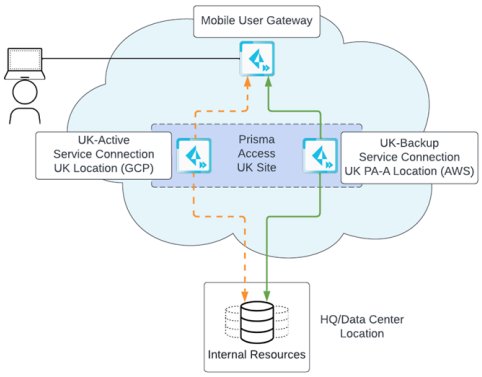
  通常の操作中、モバイル ユーザーは UK-Active サービス接続を使用して、HQ またはデータセンターの内部リソースにアクセスします。



  GCPの停止がUK-Activeサービス接続に影響する場合、 Prisma AccessはAWS でホストされている UK-Backup サービス接続にフェイルオーバーします。このようにして、クラウド プロ

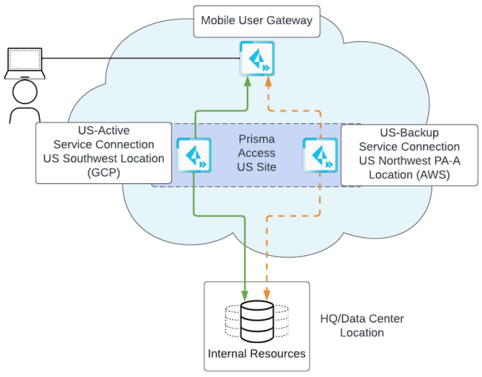
 ©2025 Palo Alto Networks, Inc.

バイダーが停止した場合でも、 Prisma Accessではモバイル ユーザーはデータ センターまたは本社のリソースにアクセスできます。次の図はトラフィックの流れを示しています。



- 異なる地理的リージョン- 地域的な停止が発生した場合に冗長性を確保する場合は、異なるコンピューティング場所と異なるクラウド プロバイダーで 2 つ以上のサービス接続を指定して、地理的なリージョンで停止が発生した場合にバックアップ アクセスを提供することができます。次の図では、管理者は米国の場所 (米国南西部の場所の US-Active と米国北西部の PA-A の場所の US-Backup) からサービス接続をオンボードし、サイト内で US-Active をアクティブなサービス接続にし、US-Backup をバックアップにするサイトを作成しました。

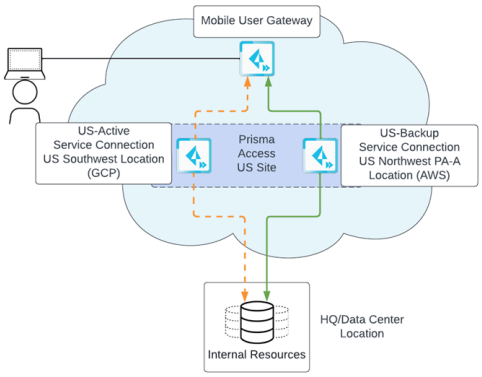
  異なる コンピューティング場所 と異なるクラウド プロバイダーにあるサービス接続をオンボードしたため、地理的冗長性とクラウド プロバイダー冗長性の両方を提供するサイトが構成されました。



  US-Active ロケーションがダウンした場合 (クラウド プロバイダーまたは地域の停止が原因)、サービス接続は US-Backup ロケーションにフェールオーバーします。US-Backup ロケーショ

 ©2025 Palo Alto Networks, Inc.

ンでは、次の図に示すように、US-Active サービス接続とは異なるクラウド プロバイダーとコンピューティング ロケーションが使用されます。

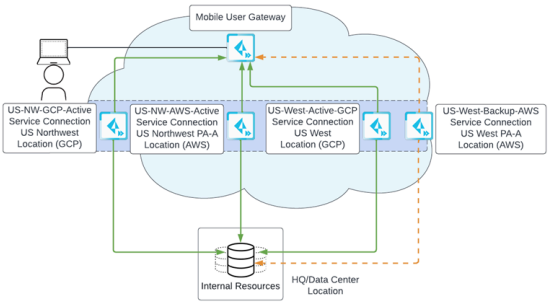


- 複数のサービス接続を使用した高帯域幅接続- 内部リソースへの高帯域幅接続が必要な場合は、複数のアクティブな接続を持つサイトを作成できます。次の図は、GCP と AWS のクラウド プロバイダーを組み合わせてオンボードされている 4 つのサイトを示しています。
  - US-NW-GCP-Active、米国北西部 (GCP) ロケーションを使用
  - US-NW-AWS-Active、米国北西部 PA-A (AWS) ロケーションを使用
  - US-West-Active-GCP、米国西部 (GCP) ロケーションを使用
  - US-West-Backup-AWS、米国西部 PA-A (AWS) ロケーションを使用

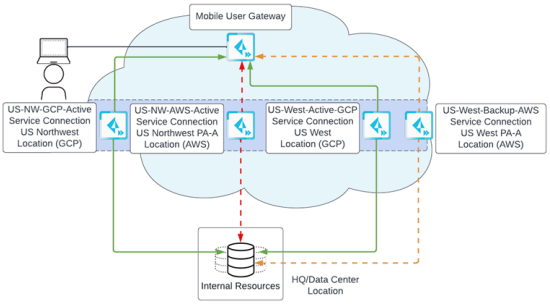
  このサイトでは、3 つのサービス接続がアクティブ サービス接続として指定され、4 つ目のサービス接続がバックアップとして指定されています。3 つのサービス接続をアクティブと

©2025 Palo Alto Networks, Inc.

して指定すると、単一のサービス接続と比較して、内部リソースへの帯域幅が実質的に 3 倍になります。

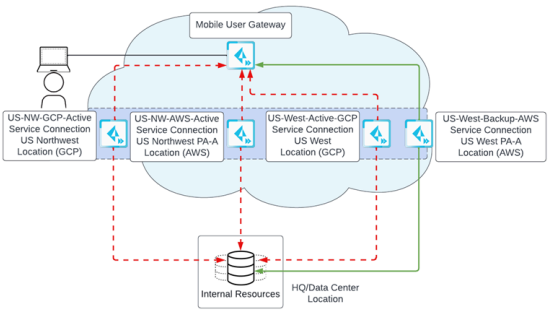


アクティブなサービス接続の1つがダウンした場合、バックアップ接続は使用されず、代わりに、次の図に示すように、Prisma Accessはトラフィックを稼働中の残りのアクティブなサービス接続に転送します。



すべてのアクティブなサービス接続がダウンした場合、バックアップ サービス接続が使用され、アクティブな接続になります。

複数のサービス接続をバックアップサービス接続として構成する場合、 *Prisma Access*はすべてのバックアップ サービス接続を使用し、サービス接続トラフィックを負荷共有します。



冗長クラウド プロバイダー サービス接続を構成するときは、次のガイドラインに従ってください。

 ©2025 Palo Alto Networks, Inc.

- サイト内の優先場所または代替場所を使用してサービス接続を追加できます。

  Palo Alto Networks では、サイト内のアクティブなサービス接続として、優先クラウド プロバイダーを使用することを強くお勧めします。
- サイト内のすべてのサービス接続は、同じ HQ またはデータ センターの場所にある同じリソースを指す必要があります。サイト内で、異なる場所にある異なるリソースを指すサービス接続を持つことはできません。
- サイト内で少なくとも 1 つのアクティブなサービス接続を選択する必要がありますが、1 つのサイト内で複数のアクティブなサービス接続を持つこともできます。次のサイト構成が有効です:
  - 米国中部（アクティブ）
  - 米国中部 PA-A (バックアップ)
  - 米国東部（アクティブ）
  - 米国東部 PA-A (バックアップ)
- サイトに複数のアクティブなサービス接続があり、アクティブなサービス接続の 1 つがダウンした場合、トラフィックは他のアクティブなサービス接続に転送されます (つまり、アクティブなサービス接続の 1 つが稼働している限り、バックアップ サービス接続は使用されません)。
- 静的および動的サービス接続ルーティングには、次のガイドラインを使用します。
  - サービス接続に静的ルーティングを使用する場合は、サービス接続に指定するサブネットが同じサブネットを指していることを確認してください。

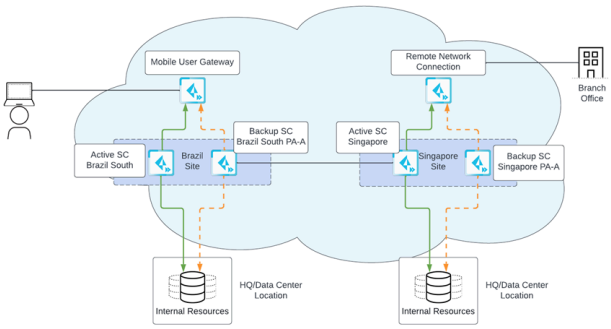
    たとえば、アクティブ サービス接続のサブネットとして 192.168.41.0/24、192.168.44.0/24、および 192.168.47.0/24 を使用するサイトがある場合は、バックアップ サービス接続に同じサブネットを指定するようにしてください。
  - サービス接続に動的 (BGP) ルーティングを使用する場合は、すべてのサービス接続が同じデータ センターまたは HQ に同じプレフィックスをアドバタイズするようにしてください。
- 次の表に示すように、Prisma AccessはBGP Multi Exit Discriminator (MED) 値を使用して、サイト内のアクティブなサービス接続とバックアップ サービス接続を区別します。アクティブ サービス接続の MED 値は、アクティブ サービス接続に対してセカンダリ IPSec トンネルを有効にしているかどうかによって変わることに注意してください。 Prisma Accessはこれらの MED 値を CPE (BGP ピア) にアドバタイズします。

接続タイプ	MED値
サイト内のアクティブな **IPSec** サービス接続	
アクティブなサービス接続、セカンダリ IPSec トンネルは構成されていません	0
アクティブなサービス接続、セカンダリ IPSec トンネルが構成済み、プライマリ トンネル	100

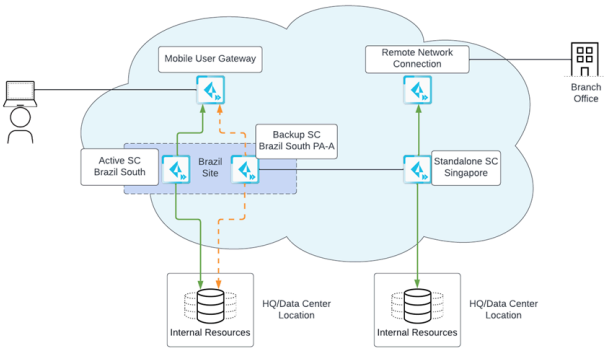
©2025 Palo Alto Networks, Inc.

接続タイプ	MED値
アクティブなサービス接続、セカンダリ IPSec トンネルが構成済み、セカンダリ トンネル	200
サイト内の **IPSec** サービス接続のバックアップ	
バックアップ サービス接続、プライマリ トンネル (セカンダリ IPSec トンネルが構成されているかどうかに関係なく)	500
バックアップ サービス接続、セカンダリ IPSec トンネルが構成済み、セカンダリ トンネル	600

- 以下の図に示すように、1 つのPrisma Accessデプロイメントで複数のサイトを追加することができます。



- 単一のスタンドアロン サービス接続を使用して内部リソースにアクセスすることもできます。次の図に示すように、スタンドアロン サービス接続とアクティブ サービス接続およびバックアップ サービス接続を混在させることもできます。



- サービス接続に Hot Potato ルーティングを 使用する場合、サービス接続のマルチクラウド冗長性はサポートされません。
- サービス接続のオンボードと構成にはCLIを使用しないでください。サービス接続をオンボードするためにCLIを使用する必要がある場合は、Palo Alto Networksチームにお問い合わせください。

©2025 Palo Alto Networks, Inc.

サービス接続クラウドプロバイダーの冗長性の構成と有効化

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

クラウド プロバイダーの複数のサービス接続を構成するには、次の手順を実行します。

STEP 1 | （既存のPrisma Accessデプロイメントのみ) プラグインをクラウド プロバイダーの冗長性をサポートするバージョンにアップグレードした場合は、サポートされているプラグインにアップグレードした後、 コミットおよびプッシュ 操作を実行します。

サービス接続のマルチクラウド冗長性は、Prisma Access 3.1 Preferred and Innovationからサポートされています。Cloud Services プラグインをアップグレードした後、クラウド冗長性の変更を UI に表示するには コミットとプッシュを 実行する必要があります。

新しいデプロイメント（アップグレードではない）がある場合は、この手順をスキップしてください。

©2025 Palo Alto Networks, Inc.

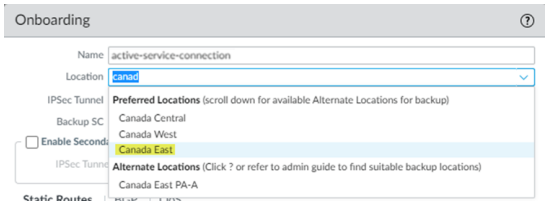
STEP 2 | サイト内のアクティブ サービス接続およびバックアップ サービス接続として使用するサービス接続を作成します 。

優先場所と代替場所を作成し、変更をコミットしてプッシュした後は、これらの場所を変更することはできません。たとえば、優先場所を*Canada East*から*Canada East PA-A*に変更したり、代替場所を*Canada East PA-A*から*Canada East*に変更したりすることはできません。

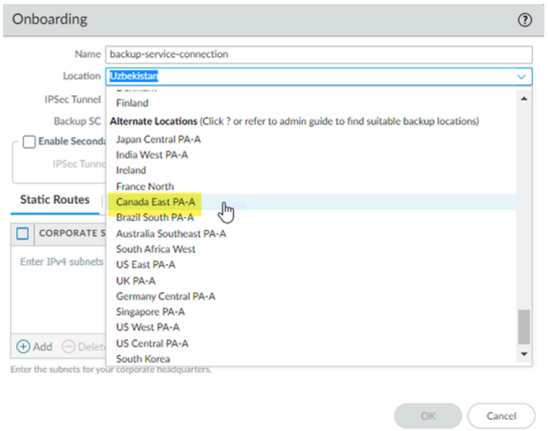
1. **Panorama** > **Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Service Connection**（サービス接続）を選択します。
2. サイト内でアクティブなサービス接続として指定するサービス接続を追加します 。

   優先場所または代替場所のリストから選択します。

   ロケーションを検索するには、 ロケーション の名前を入力します。



3. サイト内でバックアップ サービス接続として指定するサービス接続を追加します 。



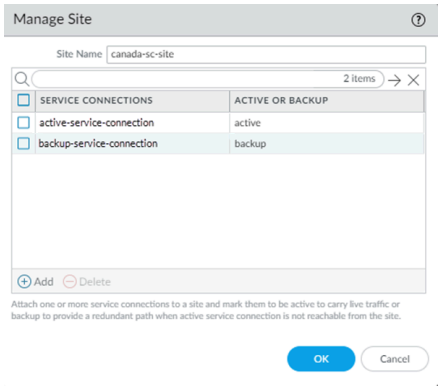
4. (任意) 必要に応じて、アクティブ サイトおよびバックアップ サイトとして指定されるサービス接続のオンボードを続行します。

 ©2025 Palo Alto Networks, Inc.

STEP 3 | サイトを作成し、追加したサービス接続をサイト内のアクティブ サービス接続またはバックアップ サービス接続として指定します。

1. 「サイトの管理」で、新しいサイト を追加します 。
2. オンボードしたサービス接続を追加します 。
3. 追加したサービス場所をサイト内で アクティブ および バックアップ として指定します。

   複数のアクティブ サイトとバックアップ サイトを作成できます。アクティブ サイトとして少なくとも1つのサイトを指定します。
4. **OK** をクリックします。
5. (任意) 必要に応じて、アクティブ サービス接続とバックアップ サービス接続のサイトの追加を続けます。



STEP 4 | 変更を **Commit and Push**（コミットしてプッシュ）します。

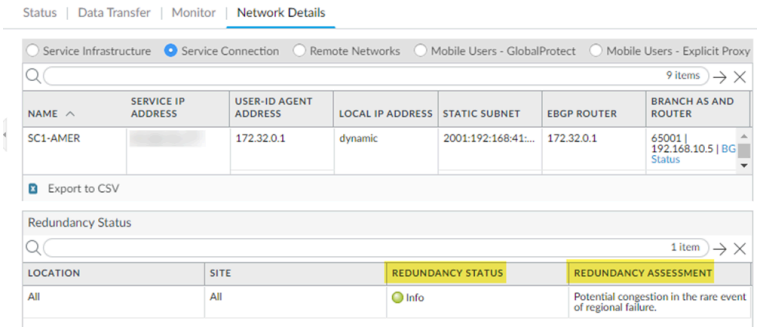
STEP 5 | サイトのステータスを確認します。

1. **[Panorama]** > **[クラウド サービス]** > **[ステータス]** > **[ネットワークの詳細]** > **[サービス接続]** > **[冗長性ステータス]**を選択します。
2. 冗長性ステータス および 冗長性評価 フィールドの情報を確認します。冗長性ステータスでは、展開するサイトのステータスが提供され、冗長性評価では、サイトに展開されたサービス接続に関する詳細情報が提供されます。

冗長性ステータス	冗長性評価
情報	地域的な障害が発生した場合、サービス接続が混雑する可能性があります。
警告	すべてのサービス接続は単一のリージョンにデプロイされます。お近くの場所への展開をご検討ください。 このメッセージは、すべてのサービス接続が単一のリージョンにデプロイされていることを通知します。

©2025 Palo Alto Networks, Inc.

冗長性ステータス	冗長性評価
注意	サイトに接続するすべてのサービス接続は、単一のリージョンにデプロイされます。お近くの場所への展開をご検討ください。 このメッセージは、サイトに接続するすべてのサービス接続が単一のリージョンにデプロイされていることを通知します。



サポートされている国内のアクティブおよびバックアップクラウドプロバイダー冗長ロケーション

どこで使用できますか?	何が必要ですか?
• Panorama	• Prisma Accessライセンス

アクティブおよびバックアップのロケーションが同じ国にあるデプロイメントを構成したい場合は、この国内の優先および代替の場所のリストから選択してください。

希望するロケーション	代替ロケーション
オーストラリア南東部	オーストラリア南東部PA-A
バーレーンPA-A	バーレーン
ブラジル南部	ブラジル南部PA-A
カナダ東部	カナダ東部PA-A
フランス北部PA-A	フランス北部
ドイツ中部	ドイツ中部 PA-A
インド西部	インド西部PA-A

©2025 Palo Alto Networks, Inc.

希望するロケーション	代替ロケーション
アイルラン PA-A	アイルランド
日本中部	日本中部PA-A
シンガポール	シンガポールPA-A
南アフリカ西部PA-A	南アフリカ西部
韓国PA-A	韓国
イギリス	イギリスPA-A
アラブ首長国連邦PA-A	アラブ首長国連邦
米国中部	米国中部PA-A
米国東部	米国東部PA-A
米国北西部	米国北西部PA-A
米国西部	米国西部PA-A

トラフィックステアリングを使用したインターネット宛てのトラフィックのサービス接続への転送

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス ❑ 証明書失効リスト (CRL) とオンライン証明書状態プロトコル (OCSP) をインターネットに直接送信する機能には、最低でもPrisma Access バージョン 5.1.1 が必要です。

Prisma Accessでは、モバイルユーザーおよびリモートネットワーク接続からインターネット宛てのトラフィックのターゲットを指定する、トラフィックステアリングルールを作成することができます。トラフィックをインターネットに送信する前にサービス接続にリダイレクトするように指定する、またはトラフィックを直接インターネットへの出口へと指定することができます。この機能は、トラフィックステアリングとして知られています。

あるいは、CPEからPrisma Accessへのデフォルトルートを受け入れるようにPrisma Accessを構成し、Prisma Accessがインターネットに接続するモバイルユーザートラフィックをデプロイメント内の最適なサービス接続に転送するようにすることもできます。

©2025 Palo Alto Networks, Inc.

Prisma Accessトラフィックステアリング付きデフォルトルート

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

Prisma Accessのデフォルト ルート機能を使用して、CPEからサービス接続にアドバタイズされるデフォ ルト ルートを受け入れます。BGPまたはスタティックルートを使って、デフォルトルートをアドバタイズすることができます。Prisma AccessはBGPを使ってこれらのルートを複数のサービス接続に渡ってアドバタイズします。そうすることで、Prisma Accessでモバイルユーザーのトラフィックを当該モバイルユーザーロケーションに対する最善のサービス接続経由でルーティングすることが可能になります。サービス接続がデフォルトルートを受け入れるようにするには、Prisma Accessでのトラフィック ステアリングの設定時に**[Accept Default Route over Service Connections (**サービス接続上のデフォルトルートを受け入れる**)]**を指定します。

デフォルトルートを有効にすると、インターネット宛てのトラフィックは、モバイルユーザーロケーションの出口ではなく、サービス接続へと誘導されます。インターネット宛てのトラフィックをデータセンターにリダイレクトしたいような場合に、この機能が役立ちます。たとえば、データセンター内にサードパーティのセキュリティスタックが存在しており、そのスタックにスクリーニングや検査を実施させたいような場合などに利用できます。

デフォルトルートの導入時には、次のガイドラインを使用してください。

- デフォルトルートは、モバイルユーザーデプロイ環境にのみ適用されます。リモートネットワーク接続は通常通りに動作し、デフォルトルートを有効にしても何も変更されません。
- デフォルトルートを許可する場合、ターゲットサービス接続やトラフィックスクリーニングルールを指定する必要はありません。ただし、デフォルトルートとともに使用することは可能です。
- **Accept Default Route over Service Connections**（サービス接続経由のデフォルトルートを受け入れ）を指定する場合、専用のサービス接続を除いて、すべてのPrisma Accessサービス接続がデフォルトルートを受け入れて、トラフィック ステアリングの判断にそのルートを使用します。
- この設定を有効にする前に、データセンターがデフォルトルートを送信していることを確認してください。そうしないと、サービス接続経由のルーティングが失敗してしまいます。
- すべてのデータセンターにデフォルトルートをアドバタイズさせることをお勧めします。Prisma Accessがルートを受信すると、リモートネットワークロケーション向けに使用する最良のサービス接続を選択できるようになります。
- サービス接続を設定する場合、接続に対してスタティックルートのみ、またはBGPのみを使用するようにしてください。デフォルトルートの使用時には、BGPを使用するサービス接続とスタティックルートを使用するサービス接続の混在はお勧めできません。
- (Prisma Access (Managed by Panorama)デプロイメント専用)マルチテナントデプロイ環境では、デフォルトルートの使用がサポートされています。

©2025 Palo Alto Networks, Inc.

- Prisma Accessは、クライアントレスVPN、ポータル、またはゲートウェイのSAML認証トラフィッ クを、デフォルトのルートを使用してパブリックIDプロバイダ（IDP）に転送しません。

トラフィックステアリングを使ったデフォルトルートの詳細と導入例については、トラフィックステアリングを使用したデフォルトルートの例、トラフィックステアリングを使って直接インターネットに送信するデフォルトルートの例およびトラフィックステアリングと専用のサービス接続を使ったデフォルトルートの例を参照してください。

Prisma Accessでのトラフィック ステアリング

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス

標準のPrisma Accessデプロイメント環境で、サービス接続は本社やデータセンター内の、認証サービスおよびプライベートアプリケーションなどの、内部ネットワークリソースへのアクセスを提供しています。サービス接続が内部トラフィックを処理します。インターネットアクセスは必要ありません。場合によっては、インターネット宛てのトラフィックをデータセンターにリダイレクトしたい場合もあります。トラフィックステアリングにより、モバイルユーザーまたはリモートネットワークトラフィックを、インターネットに送信する前にサービス接続にリダイレクトすることができます。

モバイルユーザーデプロイ環境、リモートネットワークデプロイ環境、または両者の組み合わせに対して、トラフィックステアリングを使用できます。インターネット宛てのネットワークトラフィックを、IPアドレス、ユーザー、URL、カスタムURLカテゴリ、サービスタイプ（HTTPまたはHTTPS）、User-ID、ダイナミック アドレス グループ（DAG）、ダイナミック ユーザー グループ (DUG) およびIPベースの外部ダイナミックリスト（EDL）など、さまざまな条件に基づいてリダイレクトするには、トラフィックステアリングを使用します。

トラフィックステアリングでは、2種類のアクションタイプがサポートされています。

- **Forward to the target**（ターゲットに転送）–トラフィックステアリングルールでこの条件を使用して、作成した1つまたは複数のサービス接続を使用するターゲット経由で、インターネット宛てのトラフィックを転送します。
- **Forward to the internet**（インターネットに転送）–トラフィックステアリングルールでこの条件を使用して、サービス接続に転送することなく、ソース（モバイルユーザーロケーションまたはリモートネットワーク接続）からインターネットに直接トラフィックを転送します。

ターゲットに転送する場合、専用および非専用の2種類のターゲットグループの作成を選択することができます。

- トラフィックステアリング関連トラフィックに対してのみ使用されるサービス接続は、専用のサービス接続になります。サービス接続を専用のサービス接続として使用するには、PanoramaでPrisma Accessでのトラフィック ステアリングの設定を実行する際に**[Dedicated for Traffic Steering Only (**トラフィック ステアリング専用**)]**を選択

 ©2025 Palo Alto Networks, Inc.

します。Strata Cloud Managerでトラフィック ステアリング ルールを設定するときは、**[Dedicated for PBF Only (PBF専用)]**を選択します。

組織の内部ネットワーク外にあるサードパーティのセキュリティスタックを使って、トラフィックをパブリックSaaSアプリケーションまたはインターネットに送信する前に処理する場合に、専用のサービス接続を設定したいこともあります。セキュリティスタックは組織ネットワークに属していないため、このサービス接続には内部ネットワークトラフィックを処理させたくはありません。

- トラフィックステアリングに使用されるサービス接続、および標準のサービス接続関連トラフィック（データセンター内の認証サーバーに送信されるトラフィックなど）に使用されるサービス接続は、非専用サービス接続になります。

専用のサービス接続としてサービス接続を設定すると、デプロイ環境に次のような変更が行われます。

- (Prisma Access (Managed by Strata Cloud Manager) デプロイメントのみ) サービス接続は、転送されたトラフィックに送信元NATを適用します。送信元IPアドレスは、インフラストラクチャサブネットから取得されるサービス接続の**EBGP**ルーターアドレスです。
- このターゲットに関連するすべてのサービス接続のゾーンが、TrustからUntrustに変更されます。ゾーンマッピングとトラフィックステアリング専用接続のゾーンマッピングとセキュリティポリシーの設定をチェックして、ネットワークがこの変更内容を反映していることを確認してください。
- 専用のサービス接続として設定されているサービス接続は、内部的にも外部的にもBGPルーティングには参加しません。
- (Prisma Access (Managed by Panorama) デプロイメントのみ) ステータス ページ (**[Panorama]** > [クラウドサービス] > [ステータス] > [監視] > [サービス接続])で、リージョンを選択し、[ステータス] タブを選択すると、専用サービス接続で BGP を使用している場合BGP ステータスは **[Not Enabled (無効)]** を示します。サービス接続のBGPステータスをチェックするには、サービス接続設定ページ（**[Panorama]** > **[Cloud Services ()]** > **[Configuration (設定)]** > **[Service Connection (サービス接続)]**）を確認します。
- (Prisma Access (Managed by Panorama) デプロイメントのみ)デフォルトでは、サービス接続は転送されたトラフィックに送信元NATを適用します。送信元IPアドレスは、サービス接続の**User-ID**エージェントアドレス(**[Panorama]** > **[Cloud Services (クラウドサービス)]** > **[Status (ステータス)]** > **[Network Details (ネットワーク詳細)]** > **[Service Connection (サービス接続)]** > **[User-ID Agent Address (User-IDエージェントアドレス)]**)です。これはインフラストラクチャサブネットから取得されます。(**[Panorama]** > **[Cloud Services (クラウドサービス)]** > **[Status (ステータス)]** > **[Network Details (ネットワーク詳細)]** > **[Service Infrastructure (サービスインフラストラクチャ)]**。

  (Prisma Access (Managed by Panorama) デプロイメントのみ) 送信元NATを無効にし、組織の送信元IP アドレスを専用サービス接続に使用できます。これを行うには、[トラフィックステアリングのターゲットサービス接続]領域で[ターゲットの追加を実行するときに、**[Disable Source NAT for Dedicated SC (専用SCの送信元NATを無効にする)]**を選択します。

 ©2025 Palo Alto Networks, Inc.

トラフィックステアリングの要件

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス

Prisma Accessデプロイメントにトラフィックステアリングを導入する前に、ご利用のネットワーク環境が次のインフラ要件を満たしていることを確認してください。

- Prisma Accessは、組織がサービス接続の終端に使用しているIPSec対応CPE（ルーターやSD-WANデバイスなど）に接続できなければなりません。また、デバイスのIPアドレスは、Prisma Accessから到達可能でなければなりません。

  スタックの場所とPrisma Access間には、標準のIPSecおよびIKE暗号化プロファイルを使ってサービス接続を作成します。サービス接続の作成時には、スタティック ルート、BGP、または両方を組み合わせて使用することができます。また、トラフィックステアリングを使用することができます。デフォルトルートとトラフィックステアリングを使用する場合、BGPのみまたはスタティックルートのみを使用することをお勧めします。スタティックルーティングを使用する場合は、IKEゲートウェイの作成時に、組織のCPEが使用しているパブリックIPアドレスを、**Peer Address**（ピアアドレス）として指定します。
- Prisma Access は、トラフィック ステアリング ルールの URL カテゴリからの URL の最初の数パケットと一致しない可能性があります。つまり、ネットワーク セッション (TCP ハンドシェイクなど) の最初の数パケットがルールと一致しない可能性があります。トラフィックステアリングルールで使用するURLに対して、Untrustゾーン経由でそれらを許可するセキュリティポリシールールを作成して、新しいセッション開始時にハンドシェイクが完了できるようにすることをお勧めします。
- セキュリティスタックでこの設定を使用している場合、スタックのロケーションは標準のIPSecトンネル設定によるサービス接続から到達可能でなければなりません。

トラフィックステアリングを設定する場合は、以下のガイドラインを使用してください。

- トラフィック ステアリング構成では、 カスタム URL カテゴリ内の通常の URL とワイルドカード (*.example.com) URL を含め、最大 1,000 個の URL (集約) を指定できます。

  この数字には、手動入力したURL、ワイルドカードを使用したURL、およびカスタムURLカテゴリに入力したURLが含まれます。
- トラフィックステアリングのルールでカスタムURLカテゴリを使用する場合、カテゴリ内のURLにはアスタリスクが付加されます。トラフィックステアリングルールとその他のセキュリティポリシールールの両方に、同じURLカテゴリポリシーを使用する場合、これらの変更はトラフィックステアリングルールとその他のセキュリティポリシールールの両方に適用されます。

  トラフィック ステアリング ルールで使用しないカスタムURLカテゴリがある場合、Prisma Accessはそれらのカテゴリの URLを変更しない。
- トラフィック転送ルールにURLを入力する、またはカスタムURLカテゴリにURLを追加する際には、すべて小文字でURLを指定してください。

©2025 Palo Alto Networks, Inc.

- 最大100件のトラフィック転送ルールを設定できます。
- プライマリ トンネルとバックアップ トンネルが設定されている場合、プライマリ (アクティブ) トンネルからバックアップ トンネルへのフェイルオーバー後は、トラフィック ステアリング ルールを使用したトラフィック ステアリングは機能しません。 Prisma Accessトラフィックステアリング付きデフォルトルートは、プライマリ トンネルとバックアップ トンネルを使用したフェイルオーバー シナリオで機能します。

トラフィック ステアリングを使用したデフォルトルートの例

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス

以下の例は、次のようなコンポーネントで構成されるサンプルPrisma Accessデプロイ環境を表しています。

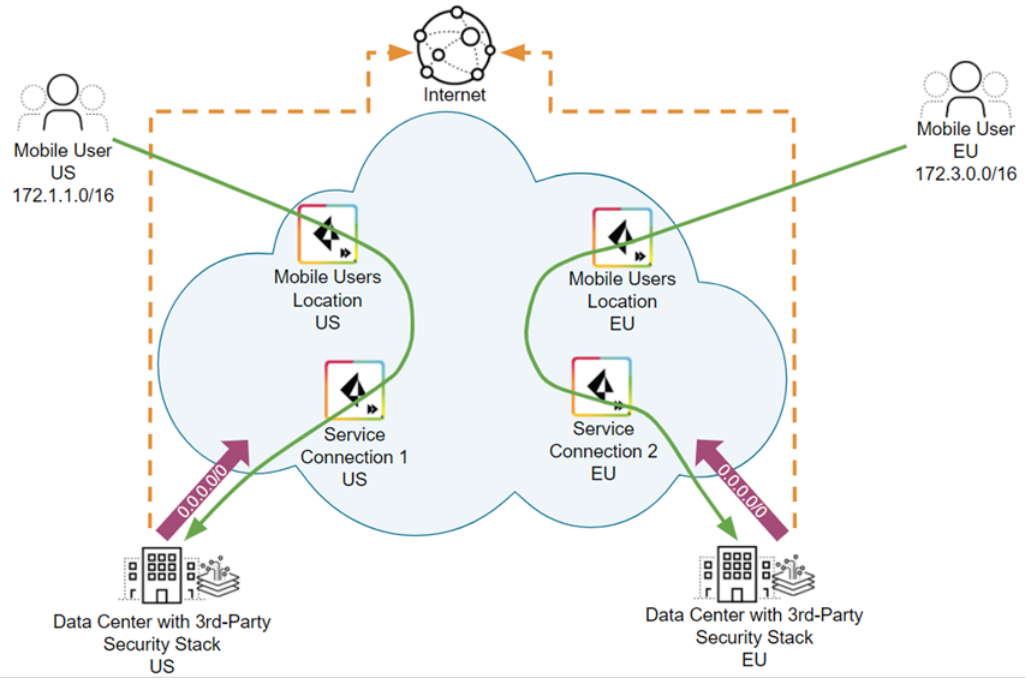
- United States（US:米国）およびEurope（EU:欧州）の2つのPrisma Accessモバイルユーザーロケーション。
- 2つのPrisma Accessサービス接続（1つは米国、もう1つはEU）。両方のデータセンターがサービス接続にデフォルト ルートを送信（**[Accept Default Route over Service Connections (サービス接続上のデフォルトルートを受け入れる)]**が有効）。
- USとEUにそれぞれ1つ、合計2つのデータセンター。

  各データセンターにはサードパーティのセキュリティスタックが存在している。そのため、インターネット宛てのすべてのトラフィックを、インターネットへの出口に送信する前にデータセンターを経由させたい。

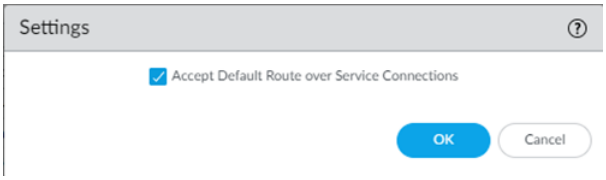
モバイルユーザーがデータセンタートラフィックを送信する場合、Prisma Accessはルーティングテーブルをチェックして、最も近いサービス接続を判断し、そのサービス接続にトラフィックを転送します。次の例で、Prisma AccessはUSのモバイルユーザーからのデータセンタートラフィックをService Connection 1に送信し、EUのモバイルユーザーからのトラフィックをService Connection 2に送信します。

デフォルト ルートで トラフィック ステアリング専用 のサービス接続を使用しないでください。専用サービス接続は*BGP*ルーティングに参加しないため、*HQ*またはデータセンターから*BGP*アドバタイズメントを受信できません。

©2025 Palo Alto Networks, Inc.



デフォルトルートを有効にするには、トラフィックステアリングの設定時に、**Accept Default Route over Service Connections**（サービス接続経由のデフォルトルートを受け入れ）を選択します。この設定を構成し、変更をコミットしてプッシュすると、Prisma Accessはインターネット接続トラフィックをサービス接続経由で送信します。

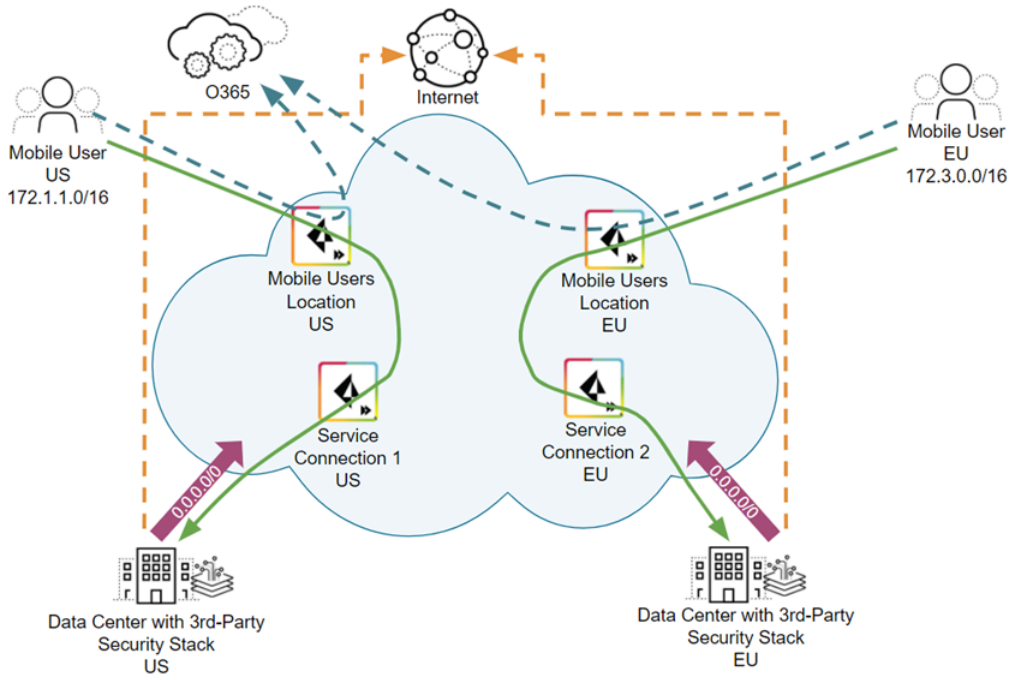


トラフィックステアリングを使って直接インターネットに送信するデフォルトルートの例

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

外部SaaSアプリケーション宛てのトラフィックをきめ細かく調整する例を次に示します。この場合、Office 365トラフィックをデータセンターに送信して処理するのではなく、モバイルユーザーロケーションから直接インターネットへの出口に送信します。この設定では、トラフィックステアリングとデフォルトルートを使用します。

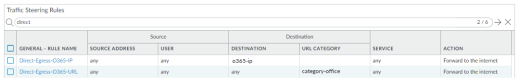
©2025 Palo Alto Networks, Inc.



Prisma AccessでOffice 365トラフィックを直接インターネットにルーティングするには、次の作業を行ってください。

- Office 365アドレスと一致するIPアドレスを使って、EDL（**Object** > **External Dynamic Lists**）を作成します。
- Office 365のURLと一致するURLを使って、カスタムURLカテゴリ（**Objects** > **Custom Objects** > **URL Category**）を作成します。
- Prisma Accessでのトラフィック ステアリングの設定し、作成したEDLとURLカテゴリを宛先一致条件として指定し、**Action**（アクション）を**Forward to the internet**（インターネットに転送）に設定します。

この設定では、Office 365トラフィックが直接インターネットに送信されます。その他のインターネット宛てトラフィックは、インターネットへの出口に送信する前にデータセンターに送信され、さらなる処理が行われます。



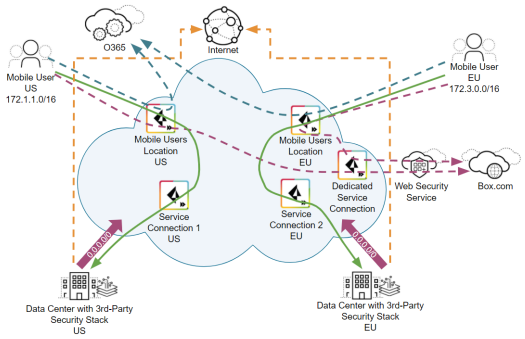
トラフィックステアリングと専用のサービス接続を使ったデフォルトルートの例

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	☐ Prisma Accessライセンス

この例では前の設定に加えて、サードパーティのインターネットセキュリティサービスを保有しており、box.comからのトラフィックをインターネットへの出口に送信する前に、セキュリティサービスを利用して処理を行います。その他のインターネット宛てトラフィックはセキュリティ

©2025 Palo Alto Networks, Inc.

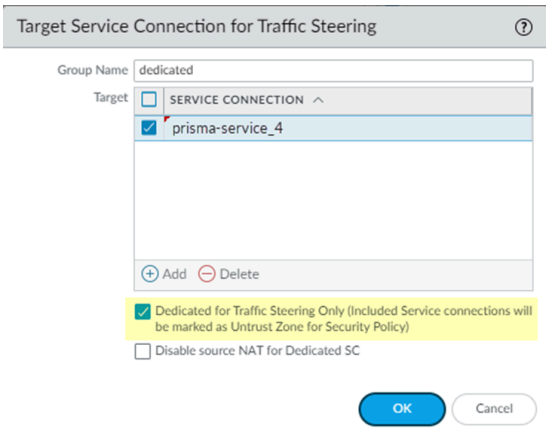
サービスに送信したくないため、box.comトラフィック専用のサービス接続を作成します。設定が完了したら、Prisma Accessは*.box.com宛先トラフィックをスタックに送信します。



デプロイメント環境を有効にするために、Traffic Steering（トラフィックステアリング）タブで次の作業を行います。

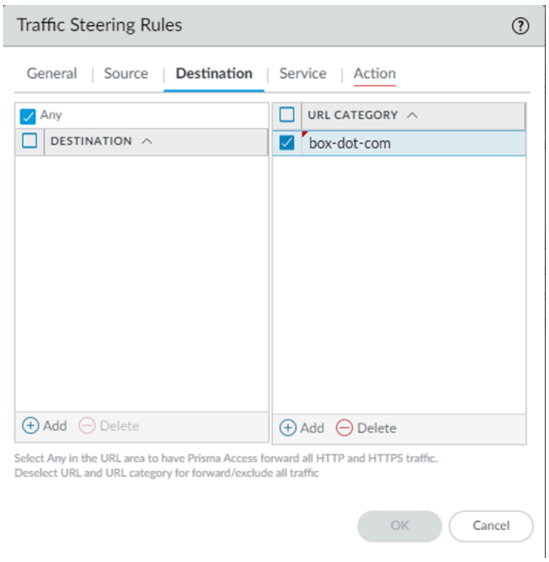
- 1つまたは複数のサービス接続をターゲットに割り当てるTarget Service Connection（ターゲットサービス接続）グループを作成し、**Dedicated for Traffic Steering Only**（トラフィックステアリング専用）を選択します。これにより、ターゲットサービス接続が専用のものになります。

> 複数のサービス接続を持つターゲットを作成した場合、*Prisma Access*はインターネット行きのトラフィックを転送するために最適なサービス接続を選択します。

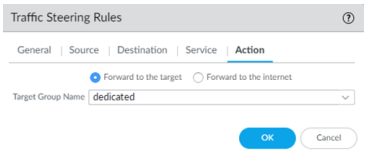


©2025 Palo Alto Networks, Inc.

- トラフィックをURLに転送するトラフィック ステアリング ルールを作成します。次のスクリーンショットは、URL *.box.comを含むカスタムURLカテゴリが割り当てられているトラフィックの宛先を示しています。



- トラフィック ステアリングルールの**Actio (**アクション)に**[Forward to the target (**ターゲットに転送**)]**を作成し、作成したターゲットグループ名（この場合は**dedicated (**専用**)**）を指定します。



Prisma Accessトラフィック ステアリング ルール ガイドライン

どこで使用できますか?	何が必要ですか?
• Panorama	• Prisma Accessライセンス

トラフィックステアリングは、さまざまな設定を処理できます。ただし、維持管理が簡単なルールを作成できるように、Prisma Accessがどのようにルールを処理するのかを理解しておくことが重要になります。デプロイ環境で適切に機能するルールを作成するためには、これらのガイドラインに従ってください。

- Prisma Accessは作成した順序 (上から下) でルールを評価します。より固有のルールは上部に、全般的なルールは下部に指定します。
- 複数の種類の条件を持つ少数のルールを作成するのではなく、一致する条件の数が少ない複数のルールを作成します。単純なルールを作成すると、ルールの作成速度が向上し、ルールの変更も簡単に行えます。
- ルールの作成後、リスト内でルールを上下に移動することはできないため、ルールの作成前に入念にルールのプランニングを行ってください。

©2025 Palo Alto Networks, Inc.

- **Any**（任意）のソースアドレスおよびユーザーを指定するルール、**Any**（任意）のソース宛先、およびURLカテゴリを指定するルール、および**Any**（任意）のサービスを指定するルールはサポートされていません。より特有のルールを使用してください。たとえば、**Any**（任意）のソースまたは宛先トラフィック、および**service-http**および**service-https**のサービスを指定したルールを作成します。
- ユーザーのルールを指定する場合は、 ソースユーザー フィールドで、 Prisma Access は、ローカルで認証するユーザーと LDAP を使用して認証するユーザー間で同じユーザー名が共有されている場合、LDAP ユーザーを次の形式で認証することでユーザーを区別できます。ドメイン/ユーザー名 また、次の形式でローカルユーザーを認証します。 ユーザー名 (ドメイン名なし)。
- オンプレミスの次世代ファイアウォールをマスターデバイスとして設定している場合は、トラフィックステアリングおよびセキュリティ ポリシー ルールでモバイルユーザーデバイスグループのユーザー情報とグループ情報を自動入力できます。 **[Panorama] > [Cloud Services (クラウドサービス)] > [Configuration (構成)] > [モバイルユーザー]**をクリックし、歯車アイコンをクリックして設定を編集し、 [デバイスグループ]領域でマスターデバイスを選択します。これにより、すべてのデバイス グループのマスター デバイスが入力されますが、セキュリティ ポリシー ルールのモバイル ユーザーのユーザーとグループの情報のみが入力されます。
- トラフィック ステアリング ルールで EDL(タイプ IP リスト)が使用され、EDL の EDL ソース URL がアクセスできない URL に更新された場合、 Prisma Accessは、前のURLからキャッシュされたIPリストを引き続き使用できます。
- Prisma Accessは、TCPポート80および443のアプリケーションオーバーライドポリシーを使用している場合、サービスタイプがHTTPまたはHTTPSのルールのトラフィックステアリングをバイパスします。

  また、TCP ポート 80 または 443 のアプリケーション オーバーライド ポリシーを設定している場合、トラフィック ステアリング ルールで参照される URL カテゴリの URL に対しては、トラフィック ステアリングは機能しません。
- 宛先 IP アドレスと URL カテゴリを同じルールで指定できます。指定した場合、Prisma Accessではルール内の宛先条件の処理には論理演算子のORが使用されますが、URLとURLカテゴリトラフィックは、HTTPの場合TCPポート80および8080、HTTPSの場合TCPポート443に基づいて処理されます。

  IPアドレスおよびURLカテゴリを使用したルールの場合、IPアドレスまたはURLカテゴリのいずれかに一致するトラフィックがルールに一致しますが、URLカテゴリトラフィックはポート80、443、8080のみに基づいて処理が行われます。このタイプのルールを作成することはお勧めできません。単純なルールを作成してください。

たとえば、ネットワークトラフィックに次のルールを適用します:

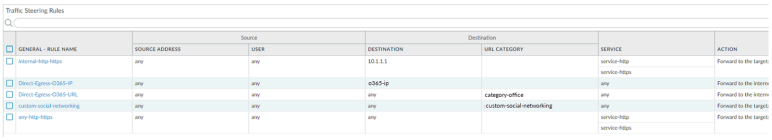
- データセンター内には、IPアドレスが10.1.1.1の内部HTTPサーバーが存在しており、内部HTTPおよびHTTPSトラフィックをこのサーバーにリダイレクトしたいと考えています。サーバーのIPアドレスは10.1.1.1です。

  このサーバーへのトラフィックはインターネット送信せずに、内部的に処理する必要があります。そのため、このトラフィックには非専用のターゲットを選択します。このタイプのターゲットは、内部トラフィックとインターネット宛てのトラフィックを処理できます。

 ©2025 Palo Alto Networks, Inc.

- office365.comのトラフィックを、インターネットに直接ルーティングしたいと考えています。
- *.example.comからのトラフィック、またはしカスタムURLカテゴリ**custom-social-networking**に定義されている任意のトラフィックを、専用の接続にルーティングします。
- その他のHTTPおよびHTTPSトラフィックは、内部HTTPサーバーに対して使われている、非専用のサービス接続ターゲットを使用するようにします。

この例では、次の画面に表示されているように、もっとも特有のルールから、特有ではないルールへとルールを作成していきます。すべてのHTTPおよびHTTPSトラフィックを許可するルールを最初に追加しないようにしてください。そうしないと、すべてのHTTPおよびHTTPSトラフィックが、その他のルールに対して評価されることなく、非専用の接続に転送されてしまいます。



トラフィックステアリング専用接続のゾーンマッピングとセキュリティポリシーの設定

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

専用のサービス接続を使用するターゲットを作成する場合、専用サービス接続のゾーンが**Trust**（信頼）から**Untrust**（信頼しない）に変更されます（非専用のサービス接続ターゲットはゾーンを変更しません）。サービス接続に対してゾーンの作成またはゾーンマッピングの設定は行えないため、モバイルユーザーおよびデバイスグループへの専用サービス接続用に、ゾーンマッピングおよびセキュリティポリシーの変更を行います。専用接続のゾーンマッピングを設定するには、以下の手順に従ってください。

これらの手順はサンプルの設定です。ご自分のデプロイ環境に合わせて、この例の内容を調整してください。

STEP 1 | **[Network]** > **[ゾーン]** の順に選択します。

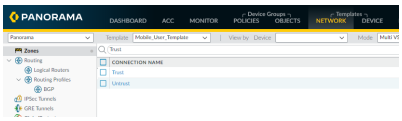
STEP 2 | ドロップダウンリストから正しい**Template**（テンプレート）を選択します（モバイルユーザーの場合**Mobile_User_Template**、リモートネットワークの場合**Remote_Network_Template**）。

モバイルユーザーとリモートネットワークデプロイが存在している場合、これらの手順を**Mobile_User_Template**に対して1回、**Remote_Network_Template**に対して1回の、合計2回繰り返す必要があります。

©2025 Palo Alto Networks, Inc.

STEP 3 | 信頼するゾーンと信頼しないゾーンの、2つのゾーンを**Add**（追加）します。

この例では、**Trust**（信頼する）および**Untrust**（信頼しない）の2つのゾーンを作成します。

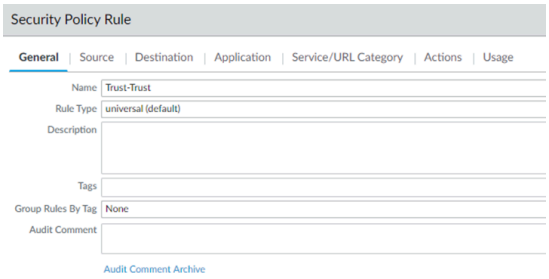


STEP 4 | 作成したゾーンのデフォルトポリシーを作成します。

1. **Policies**（ポリシー） > **Security**（セキュリティ） > **Post Rules**（ポストルール）の順に選択します。
2. ドロップダウンリストから正しい**Device Group**（デバイスグループ）を選択します（リモートネットワークの場合**Remote_Network_Device_Group**、モバイルユーザーの場合**Mobile_User_Device_Group**）。

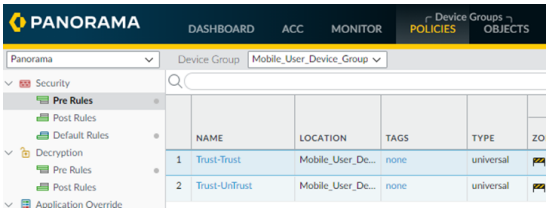
   モバイルユーザーおよびリモートネットワークのデプロイ環境が存在している場合、これらの手順を**Mobile_User_Device_Group**に対して1回、**Remote_Network_Device_Group**に対して1回の、合計2回繰り返す必要があります。
3. Trustゾーン間トラフィックに使用するデフォルトのポリシーを**Add**（追加）します。

   このポリシーは、**Source**（ソース）、**User**（ユーザー）、**Destination**（宛先）、**Application**（アプリケーション）、および**Service/URL Category**（サービス/URLカテゴリ）トラフィックすべてに対して、**Any**（任意）トラフィックの通過を許可します。



4. Trust-to-Trustポリシーで使用したのと同じパラメータを使って、TrustゾーンからUntrustゾーンへのトラフィックに使用するデフォルトポリシーを**Add**（追加）します。

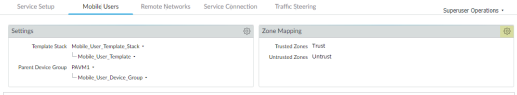
   作業が完了したら、Trust-to-Trustトラフィック用とTrust-to-Untrustトラフィック用の2つのセキュリティポリシーが存在することになります。



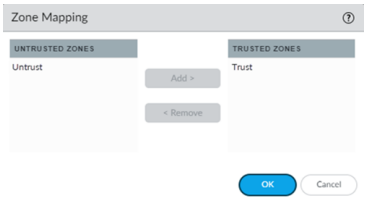
 ©2025 Palo Alto Networks, Inc.

STEP 5 | デプロイメントの必要に応じて、リモートネットワーク、モバイルユーザー、またはその両方のゾーンマッピングを定義します。

1. リモートネットワーク、モバイルユーザー、または両方のゾーンマッピングを設定します。
   - モバイルユーザーの場合、**Panorama** > **Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Mobile Users**（モバイルユーザー）を選択します。
   - リモートネットワークの場合、**Panorama** > **Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Remote Networks**（リモートネットワーク）を選択します。
2. 設定を編集するには、**Zone Mapping**（ゾーンマッピング）の隣にあるアイコンをクリックします。



3. デプロイ環境の**Zone Mapping**（ゾーンマッピング）を設定し、信頼するトラフィックのゾーンを**Trusted Zones**（信頼するゾーン）に、信頼しないトラフィックを**Untrusted Zones**（信頼しないゾーン）に移動して、**OK**をクリックします。



Prisma Accessでのトラフィック ステアリングの設定

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス ❑ 証明書失効リスト（CRL）とオンライン証明書状態プロトコル（OCSP）をインターネットに直接送信するには、最低Prisma Accessバージョン5.1.1が必要です。

トラフィック ステアリングでは、Prisma Access Accessを設定してトラフィック ステアリング ルールを作成し、モバイル・ユーザーおよびリモート ネットワーク接続からのインターネット接続トラフィックのターゲットを指定することができます。トラフィックをインターネットに送信する前にサービス接続にリダイレクトするように指定する、またはトラフィックを直接インターネットへの出口へと指定することができます。次の手順を実行して、Prisma Accessのデプロイメントにトラフィックステアリングを設定します。

- Strata Cloud Manager
- Panorama

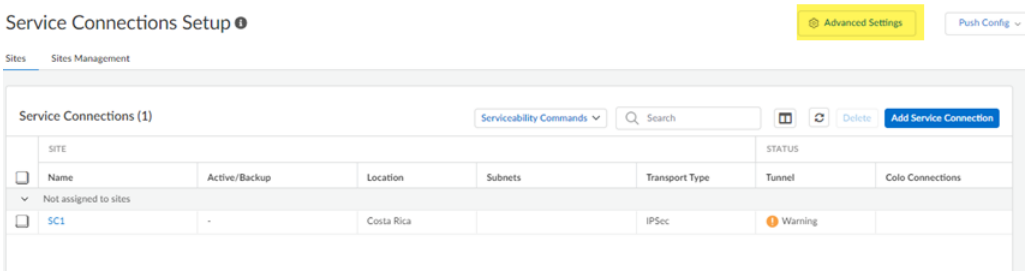
©2025 Palo Alto Networks, Inc.

Prisma Access (Strata Cloud Manager) でトラフィック ステアリングを設定する

Prisma Accessデプロイ環境で、サービス接続は本社やデータセンター内の、認証サービスおよびプライベートアプリケーションなどの、内部ネットワークリソースへのアクセスを提供しています。サービス接続が内部トラフィックを処理します。インターネットアクセスは必要ありません。場合によっては、インターネット宛てのトラフィックをデータセンターにリダイレクトしたい場合もあります。トラフィックステアリングにより、モバイルユーザーまたはリモートネットワークトラフィックを、インターネットに送信する前にサービス接続にリダイレクトすることができます。次の手順を実行して、Prisma Accessの展開にトラフィックステアリングを設定します。

STEP 1 | ご自分のデプロイ環境に合わせて、サービス接続、モバイルユーザー、およびリモートネットワークをオンボーディングします。

STEP 2 | **[Workflows (ワークフロー)]** > **[Prisma Accessセットアップ]** > **[Service Connections (サービス接続)]** > **[Advanced Settings (詳細設定)]**に移動します。



STEP 3 | トラフィック ステアリングルールを設定します。

1. （任意、モバイルユーザーデプロイメント環境のみ）CPEからの、1つまたは複数のサービス接続経由でアドバタイズされているデフォルトルートの受け入れとインストールをPrisma Accessに許可するために、歯車アイコンをクリックしてSettings（設定）を表示して、**[Accept Default Route over Service Connections**（サービス接続経由のデフォルトルートを受け入れ）**]**を選択します。

   デフォルトルートを使用する場合、遵守する必要があるガイドラインが存在しています。たとえば、もデフォルトルートはモバイルユーザーデプロイ環境に対してのみサポートされており、リモートネットワークデプロイ環境には何の影響もありません。トラフィックステアリングを使ったデフォルトルートを導入する前に、これらのガイドラインを必ず確認してください。

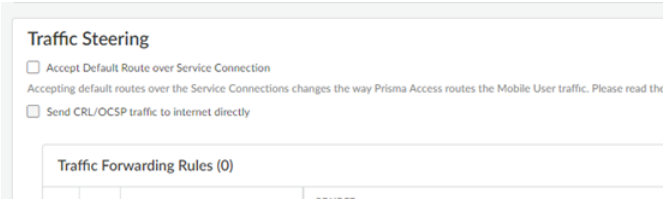
STEP 4 | （任意）CRL/OCSP トラフィックをインターネットに直接送信]を選択することにより、Prisma Accessが証明書失効リスト（CRL）とオンライン証明書ステータスプロトコル（OCSP）トラフィックをインターネットに直接送信できるようにします。

パブリック インターネットにOCSPまたはCRPサーバーがあり、そのトラフィックをアントラスト ゾーンを使用してインターネットに直接送信する場合は、この選択肢を選択します。

 ©2025 Palo Alto Networks, Inc.

この選択肢を選択しない場合は、 Prisma Accessはこのトラフィックをサービス接続に送信します。

*[CRL/OCSP*トラフィックをインターネットに直接送信*]*を選択する前に、*Prisma Access*デプロイメントを最小バージョン*5.1.1*にアップグレードしていることを確認してください。



STEP 5 | 作成したターゲットのルールを作成し、それをターゲットに適用します。

1. ルールを追加します。
2. ルールの一意の名前を入力します。
3. **Source (**送信元**)** エリアで：
   - 一致するユーザーのリストを指定します。

     [任意のユーザーに一致]、[ログオン前に一致]、[既知のユーザーに一致]、[不明に一致]、または [ユーザーの追加] を選択して、一致させるユーザーを選択できます。
   - 送信元アドレスエンティティを選択します。次のオブジェクトを1つ以上選択できます。
     - IP アドレス
     - アドレス グループ
     - IPアドレスまたはURLを使用した 外部動的リスト (EDL)
4. [宛先] 領域で、次の宛先アドレス エンティティのいずれかを指定するか、[URL カテゴリ] フィールドのルールでトラフィックを処理する場合は **[Any]** を選択します：
   - IPアドレス
   - アドレスグループ
   - IPアドレスまたはURLを使用した外部動的リスト (EDL)
5. **URL** カテゴリを指定します。

   カスタムURLカテゴリを作成する場合は、URLをすべて小文字で入力します。トラフィック ステアリングは、カスタムURLと定義済みURLカテゴリをサポートしま

©2025 Palo Alto Networks, Inc.

す。URLカテゴリ内のURLにはワイルドカードを使用できます。次のワイルドカード形式がサポートされています。

- *.example.com
- *.fqdn.example.com

次の形式はサポートされていません:

- *
- *.*
- *example.com
- example.com/ (トラフィック ステアリングで使用される URL カテゴリでは、URLの末尾のスラッシュはサポートされていません)
- example.com/path (ドメイン名のみがサポートされます)
- *fqdn.example.com
- fqdn.example.*

宛先オプションを構成するときは、次のガイドラインに従ってください。

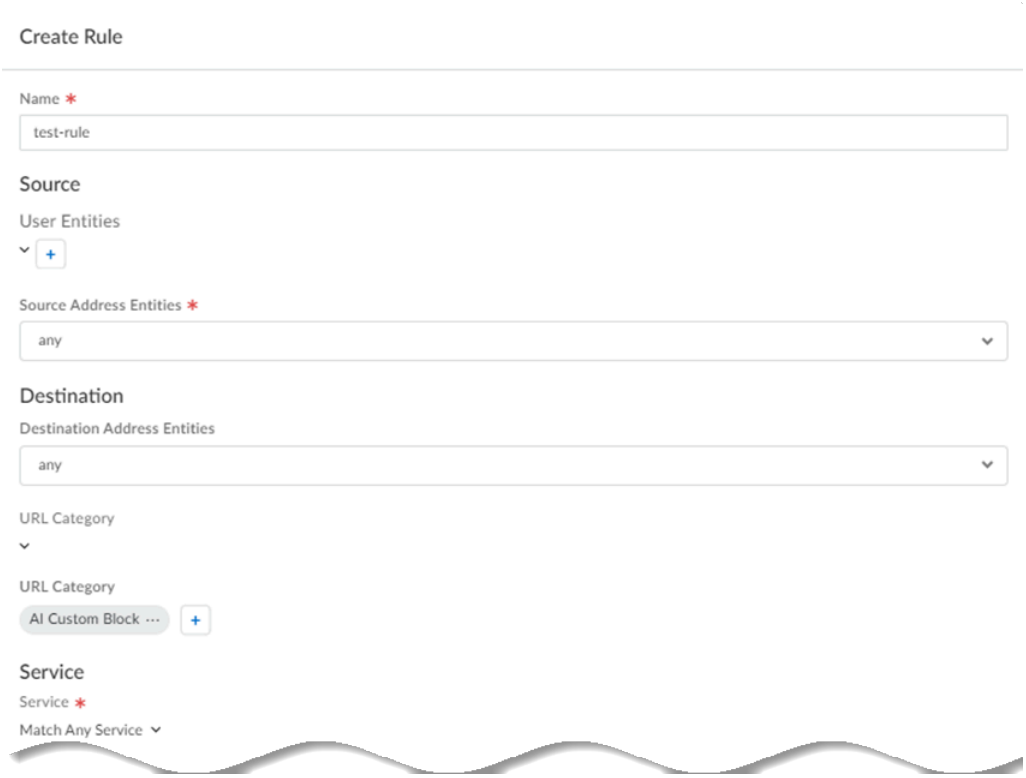
- URL カテゴリを指定すると、サービスが **Any**に設定されている場合でも、Prisma Access は HTTP および HTTPS トラフィックのみを照合します。
- カテゴリ一致タイプのカスタムURLカテゴリを作成しないでください。

Custom_URL_Category_TFRという名前のカスタムURLカテゴリを作成しないでください。

6. サービスタイプを指定して、 サービスを追加します。

   HTTPトラフィックを転送する場合は**service-http**を、HTTPSトラフィックを転送する場合は**service-https**を指定します。任意のサービス タイプのトラフィックを転送するには、[任意のサービスに一致] を選択します。

©2025 Palo Alto Networks, Inc.



7. サービス接続グループを作成し、アクションを指定します。
   1. 新規グループを作成する か、グループを管理して一意の名前を付けます。
   2. ターゲットで使用するサービス接続を指定します。

      Palo Alto Networksでは、トラフィック ステアリング ルールで参照されるターゲット サービス接続グループで複数のサービス接続 (専用か非専用かに関係なく) を使用することは推奨されません。加えて、当該サービス接続は1つのターゲットに対してのみ存在しており、単一のサービス接続を複数の異なるターゲットに追加することはできません。
   3. (任意) 専用のサービス接続を使用して、トラフィックをサードパーティのセキュリティスタックまたは構内にはないクラウドに誘導することができます。ルーティングに参加する必要はありません。専用のサービス接続として使用するようにサービス接続を設定するには、**[Dedicated for Traffic Steering Only**（トラフィックステアリング専用）**]**を選択します。

      専用サービス接続は ゾーンを変更し 、セキュリティ ポリシー ルールのアントラスト ゾーンとしてマークされます。

      サービス接続経由で、標準のサービス接続関連トラフィックとトラフィックステアリングトラフィックの両方を送信する場合は、**Dedicated for Traffic Steering**

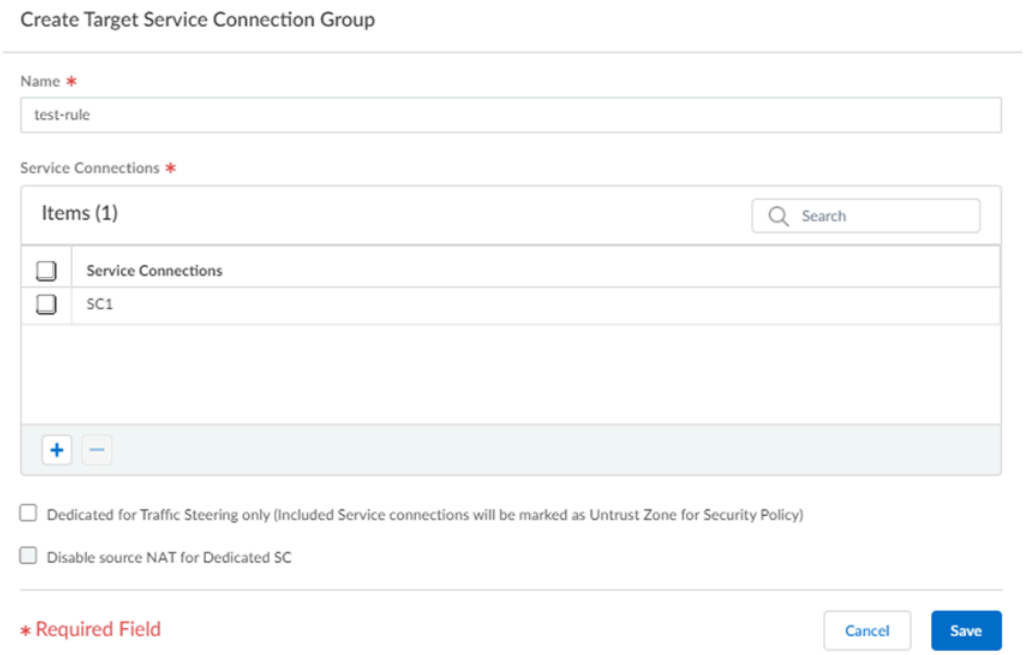
 ©2025 Palo Alto Networks, Inc.

Only（トラフィックステアリング専用）の選択を解除してください。この場合、サービス接続のゾーンはTrustになります。

4. 専用サービス接続の送信元NATを選択で無効にするには、**[専用SCの送信元NATを無効にする]**を選択します。送信元NATはデフォルトで有効になっています (チェックボックスはオフになっています)。

   送信元NATを無効にすると、 Prisma Accessは専用サービス接続には組織の送信元IPアドレスを使用します。送信元NAT を有効にすると、専用サービス接続((**[Panorama]** > **[Cloud Services (クラウドサービス)]** > **[Status (ステータス)]** > **[Network Details (ネットワーク詳細)]** > **[Service Connection (サービス接続)]** > **[EBGP Router (EBGPルーター)]**))からトラフィックが排出された後でも、 Prisma Accessはサービス接続の**EBGP**ルータアドレスを送信元IPアドレスとして使用します。

5. 変更を保存します。



8. トラフィックを指定したサービス接続ターゲットに転送するか、またはサービス接続を経由しないで直接インターネットにトラフィックを送信します。

   - Prisma Accessにトラフィックをサービス接続ターゲットに転送させるには、**[Forward to target (ターゲットに転送)]**を選択し、次に**[Target Service Connection Group (ターゲットサービス接続グループ)]**を選択します。

     SaaSアプリケーションの許可リストの制限により、既存または従来の環境にトラフィックを送信する必要がある場合、または指定されたインターネット トラフィッ

©2025 Palo Alto Networks, Inc.

クをオンプレミス ネットワークに戻すトラフィック フローを作成する場合は、この選択を指定します。

- Prisma Accessに、最初にサービス接続にトラフィックを送信することなく、インターネットに直接トラフィックを転送させるには、**[Forward to internet (**インターネットに転送**)]**を選択します。

  Prisma Accessにデフォルト ルートを送信しており、一部のトラフィックを直接インター ネットに送りたい場合は、この選択肢を指定します。



STEP 6 | 変更を保存するには、 **[Push Config (**設定をプッシュ**)]** を実行します 。

Prisma Accessでのトラフィック ステアリングの設定 (Panorama)

STEP 1 | ご自分のデプロイメント環境に合わせて、サービス接続、モバイルユーザー、およびリモートネットワークをオンボーディングします。

STEP 2 | **Panorama > Cloud Services**（クラウドサービス） **> Configuration**（設定） **> Traffic Steering**（トラフィックステアリング）を選択します。

STEP 3 | （任意、モバイルユーザーデプロイメント環境のみ）CPEからの、1つまたは複数のサービス接続経由でアドバタイズされているデフォルトルートの受け入れとインストールをPrisma Accessに許可するために、歯車アイコンをクリックしてSettings（設定）を表示して、**[Accept Default Route over Service Connections**（サービス接続経由のデフォルトルートを受け入れ）**]**を選択します。

デフォルトルートを使用する場合、遵守する必要があるガイドラインが存在しています。たとえば、もデフォルトルートはモバイルユーザーデプロイ環境に対してのみサポートされており、リモートネットワークデプロイ環境には何の影響もありません。トラフィックステアリングを使ったデフォルトルートを導入する前に、これらのガイドラインを必ず確認してください。

©2025 Palo Alto Networks, Inc.

STEP 4 | （任意）CRL/OCSP トラフィックをインターネットに直接送信]を選択することにより、Prisma Accessが証明書失効リスト（CRL）とオンライン証明書ステータスプロトコル（OCSP）トラフィックをインターネットに直接送信できるようにします。

パブリック インターネットにOCSPまたはCRPサーバーがあり、そのトラフィックを非信頼ゾーンを使用してインターネットに直接送信する場合は、この選択肢を選択します。この選択肢を選択しない場合は、 Prisma Accessはこのトラフィックをサービス接続に送信します。

*[CRL/OCSP*トラフィックをインターネットに直接送信*]*を選択する前に、*Prisma Access*デプロイメントを最小バージョン*5.1.1*にアップグレードしていることを確認してください。



STEP 5 | （任意）ターゲットグループを作成して、それにサービス接続を割り当てます。

1. **Target Service Connections for Traffic Steering**（トラフィック ステアリングのターゲットサービス接続）エリアで、グループを**Add**（追加）して、それの**Group Name**（グループ名）を指定します。
2. トラフィックの**Target**（ターゲット）を**Add**（追加）して、ターゲットで使用する**Service Connection**（サービス接続）を指定し、次に**OK**をクリックします。

   Palo Alto Networksでは、トラフィック ステアリング ルールで参照されるターゲットサービス接続グループで複数のサービス接続 (専用か非専用かに関係なく) を使用することは推奨されません。加えて、当該サービス接続は1つのターゲットに対してのみ存在しており、単一のサービス接続を複数の異なるターゲットに追加することはできません。
3. このターゲットに関連するサービス接続を専用のサービス接続にするかどうかを選択します。

   - 専用のサービス接続を使用して、トラフィックをサードパーティのセキュリティスタックまたは構内にはないクラウドに誘導することができます。ルーティングに参加する必要はありません。専用のサービス接続として使用するようにサービス接続を設定するには、**[Dedicated for Traffic Steering Only**（トラフィックステアリング専用）**]**を選択します。

     専用サービス接続のゾーンが変更されます。

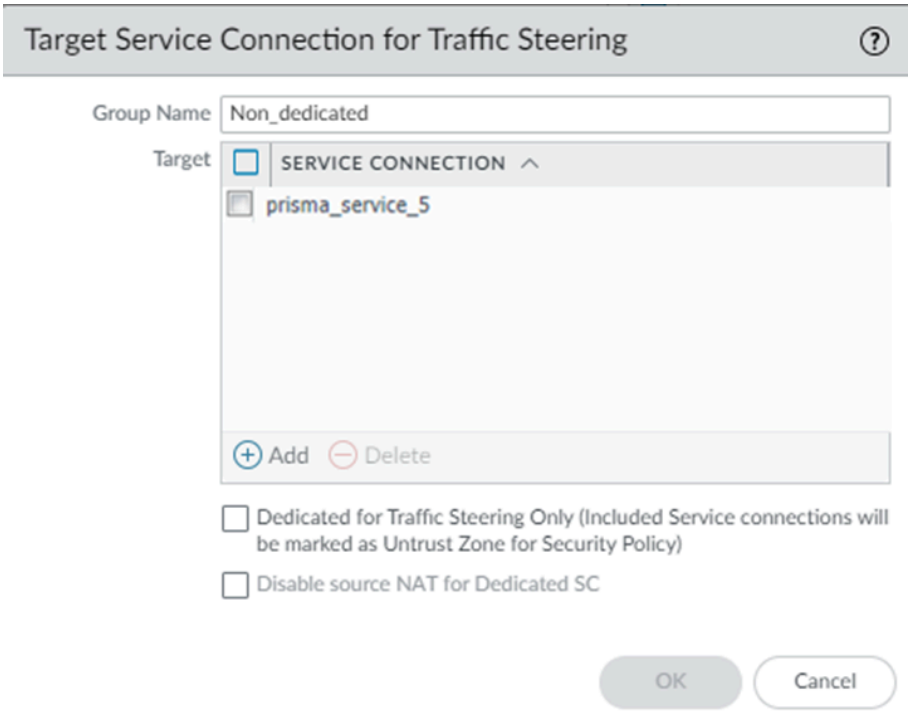
   - サービス接続経由で、標準のサービス接続関連トラフィックとトラフィックステアリングトラフィックの両方を送信する場合は、**Dedicated for Traffic Steering Only**（トラフィックステアリング専用）の選択を解除してください。この場合、サービス接続のゾーンはTrustになります。

©2025 Palo Alto Networks, Inc.

4. 送信元NATを有効にするか無効にするかを選択します。

   専用サービス接続の送信元NATを無効にするには、[専用**SC**の送信元**NAT**を無効にする]を選択します。送信元NATはデフォルトで有効になっています (チェックボックスはオフになっています)。

   送信元NATを無効にすると、 Prisma Accessは専用サービス接続には組織の送信元IPアドレスを使用します。送信元NAT を有効にすると、専用サービス接続((**[Panorama]** > **[Cloud Services (**クラウドサービス**)]** > **[Status (**ステータス**)]** > **[Network Details (**ネットワーク詳細**)]** > **[Service Connection (**サービス接続**)]** > **[EBGP Router (EBGP**ルーター**)]**))からトラフィックが排出された後でも、 Prisma Accessはサービス接続の**EBGP**ルータアドレスを送信元IPアドレスとして使用します。



 ©2025 Palo Alto Networks, Inc.

STEP 6 | 作成したターゲットのルールを作成し、それをターゲットに適用します。

1. **[トラフィック ステアリング ルール]** 領域で、トラフィック ステアリング ルールを 追加します 。
2. **General**（全般）タブで、トラフィック ステアリング ルールの**Name**（名前）を指定します。
3. **Source**（ソース）タブで、ソーストラフィックのルールを指定します。
   - **Source Address**（ソースアドレス）フィールドで、次の1つまたは複数のオブジェクトを指定するか、または**Any**（任意）を選択して任意のソースからのトラフィックがこのターゲットに送信されるようにします。
     - IPアドレス
     - Panoramaで作成したアドレスオブジェクト（**Objects** > **Addresses**）。
     - ダイナミックアドレスグループ（DAG）
     - IPアドレスまたはURLを使用した外部動的リスト (EDL)
   - **Source User**（ソースユーザー）フィールドで、ソースユーザートラフィックのルールを指定します。次のユーザー情報を指定できます。
     - ユーザー

       ユーザーを、ドメイン/ユーザーまたはユーザー@ドメインの形式で入力します。
     - ユーザーグループ

       ユーザーグループの入力時には、完全識別名（DN）を使用します。
     - Panoramaで設定されたユーザー（**[Device (デバイス)]** > **[Local User Database (ローカルユーザーデータベース)]** > **[Users (ユーザー)]**）
     - Panoramaで設定されたユーザーグループ（**[Device (デバイス)]** > **[Local User Database (ローカルユーザーデータベース)]** > **[User Groups (ユーザーグループ)]**）

   アドレスオブジェクト、DAG、EDL、ユーザー、またはユーザーグループを使用する場合、それに**Shared**（共有）を設定して、Prisma Access内のすべてのデバイス グ

©2025 Palo Alto Networks, Inc.

ループと共有してください。また、アドレス オブジェクト、DAG、または EDL に 0.0.0.0/0 を入力せず、代わりにルールに 0.0.0.0/0 を直接入力します。

*Prisma Access*は、モバイルユーザーデバイス グループからのユーザーのみを、自動的に入力します。

4. **Destination**（宛先）タブで、次の値を指定します。
   - **Destination**（宛先）エリアで、次のいずれかの条件を指定するか、または**Any**（任意）を選択して、**URL Category**（**URL**カテゴリ）フィールド内のルールにトラフィックを処理させるようにしてください。
     - IPアドレスまたはプレフィックス
     - Panoramaで作成したアドレスオブジェクト（**Objects** > **Addresses**）。
     - ダイナミックアドレスグループ（DAG）
     - IPアドレスベースの外部ダイナミックリスト（EDL）

     アドレス オブジェクト、*DAG*、または*EDL*に *0.0.0.0/0* を入力しないでください。代わりに、ルールに *0.0.0.0/0* を直接入力してください。

     すべてのトラフィックを**URL Category**（**URL**カテゴリ）エリア内のルールで処理するために、**Any**（任意）は選択した状態にします。**Destination (**宛先**)**、および**URL Category (URL**カテゴリ**)**領域にルールを指定した場合、Prisma Accessは**Destination (**宛先**)**カテゴリのルールを最初に処理します。
   - **URL Category**（**URL**カテゴリ）フィールドで、カスタムURLカテゴリ（**Objects** > **Custom Objects** > **URL Category**）を入力します。カスタムURLカテゴリを作成する

©2025 Palo Alto Networks, Inc.

場合、URLはすべて小文字で入力してください。トラフィック ステアリングは、カスタムURLと定義済みURLカテゴリをサポートします。

URLカテゴリ内のURLにはワイルドカードを使用できます。次の形式のワイルドカードがサポートされています。

- *.example.com
- *.fqdn.example.com

次の形式はサポートされていません。

- *
- *.*
- *example.com
- example.com/ (トラフィック ステアリングで使用されるURLカテゴリでは、URLの末尾のスラッシュはサポートされていません)
- example.com/パス (ドメイン名のみがサポートされます)
- *fqdn.example.com
- fqdn.example.*

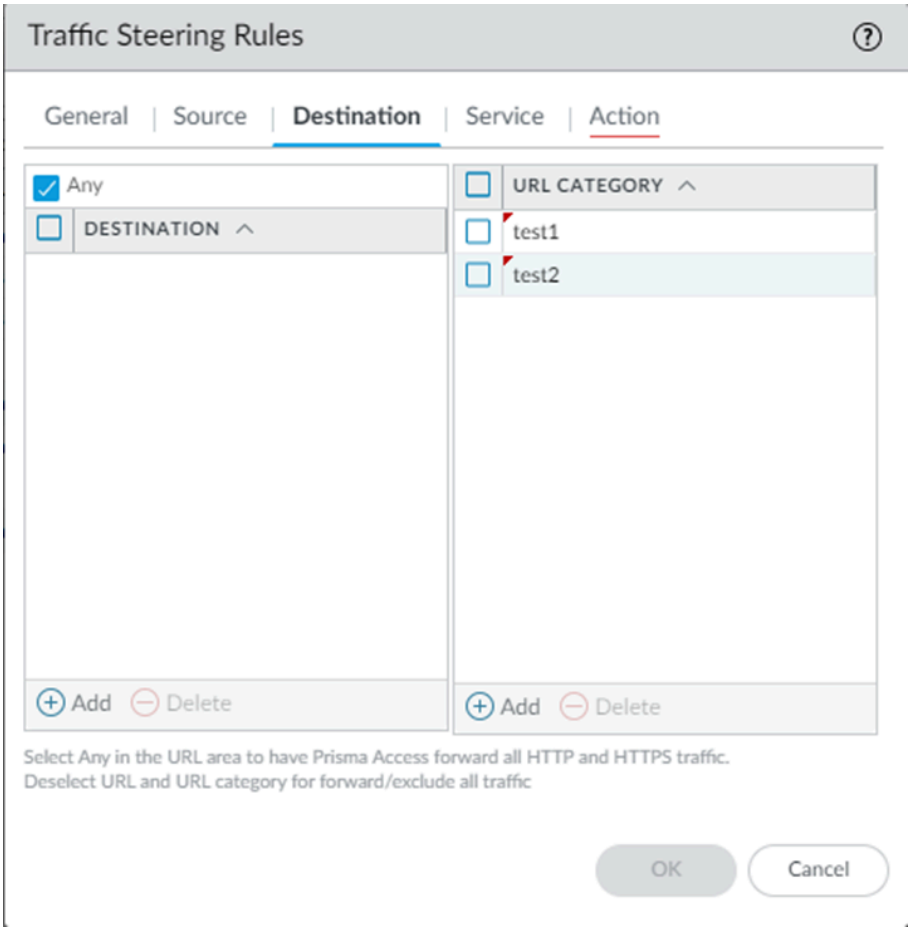
カスタムURLカテゴリ内のURLは、次世代ファイアウォールで使用されるものと同じURLパターン マッチングを使用します。

宛先オプションを設定する場合は、次のガイドラインを使用してください。

- URLカテゴリを指定すると、サービスが［Any (任意)］に設定されている場合でも、Prisma AccessはHTTPおよびHTTPSトラフィックにのみ一致します。
- カテゴリ一致タイプのカスタムURLカテゴリを作成しないでください。
- Prisma Access 1.7から2.0に移行されたデプロイメントでは、1.7からURL領域に入力されたURLは、**Custom_URL_Category_TFR number**（*number*はカスタムURLカテゴリに付加された番号）という名前のカスタムURLカテゴリに移動されるた

©2025 Palo Alto Networks, Inc.

め、**Custom_URL_Category_TFR**という名前のカスタムURLカテゴリを作成しないでください。



5. **Service**（サービス）タブで、サービスタイプを指定します。

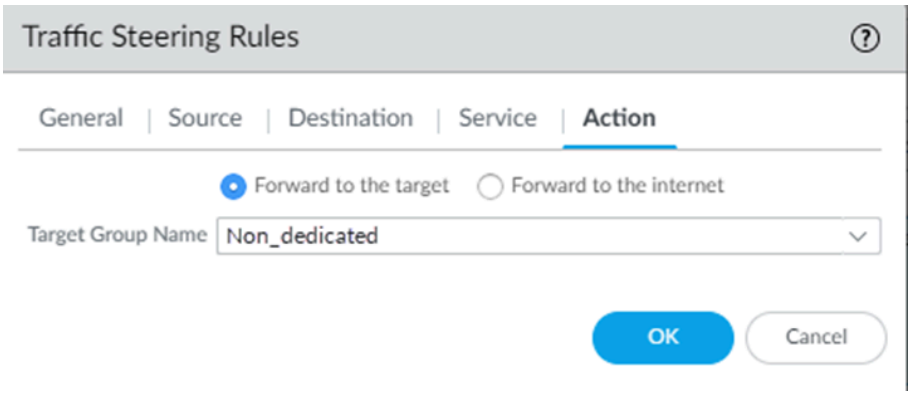
   HTTPトラフィックを転送する場合は**service-http**を、HTTPSトラフィックを転送する場合は**service-https**を指定します。任意のサービスタイプのトラフィックを転送する場合は、**Any**（任意）を選択します。

6. **Action**（アクション）タブで、トラフィック ステアリング ルールに適用する**Target Group Name**（ターゲットグループ名）を選択します。

7. トラフィックを指定したサービス接続ターゲットに転送するか、またはサービス接続を経由しないで直接インターネットにトラフィックを送信します。

   - Prisma Accessにトラフィックをサービス接続ターゲットに転送させるには、**[Forward to target (**ターゲットに転送**)]**を選択し、次に**[Target Group Name (**ターゲットグループ名**)]**を選択する。
   - Prisma Accessに、最初にサービス接続にトラフィックを送信することなく、インターネットに直接トラフィックを転送させるには、**[Forward to internet (**インターネットに転送**)]**を選択します。

©2025 Palo Alto Networks, Inc.



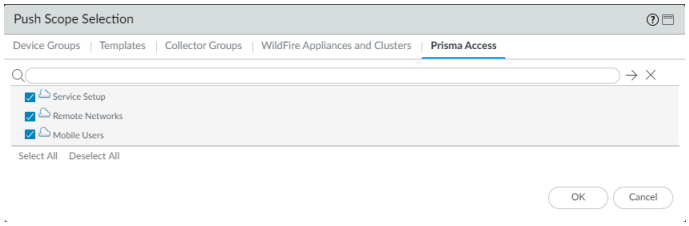
8. **OK** をクリックして変更内容を保存します。

STEP 7 | （任意）その他のトラフィックステアリングルールを指定します。

Prisma Accessでは、複数のルールは、作成した順番に処理されます（上から下へ）。

STEP 8 | Prisma Accessで変更内容をアクティブにするために、変更内容をコミット、プッシュします。

1. **Commit**（コミット） > **Commit and Push**（コミットしてプッシュ）の順に選択し、Push Scope（プッシュ スコープ）で **Edit Selections**（選択内容の編集）を行います。
2. **Prisma Access**を選択し、**[Service Setup**（サービスセットアップ）**]**、**[Remote Networks**（リモートネットワーク）**]**、および**[Mobile Users**（モバイルユーザー）**]**を選択します。



3. **OK** をクリックして、プッシュ スコープに対する変更を保存します。
4. 変更をコミットしてプッシュします。

サービス接続トラフィックのルーティング

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

Prisma Accessはダイナミック ルーティングにBGPを使用しており、BGPパス選択を使ってルーティングテーブルにルートをインストールします。Prisma Accessは、サービス接続を使用して本社またはデータセンターにトラフィックをルーティング するとき、そのトラフィックを効果的に誘導するルーティング方法を使用します。 Prisma Accessは、大半のネットワーク配

 ©2025 Palo Alto Networks, Inc.

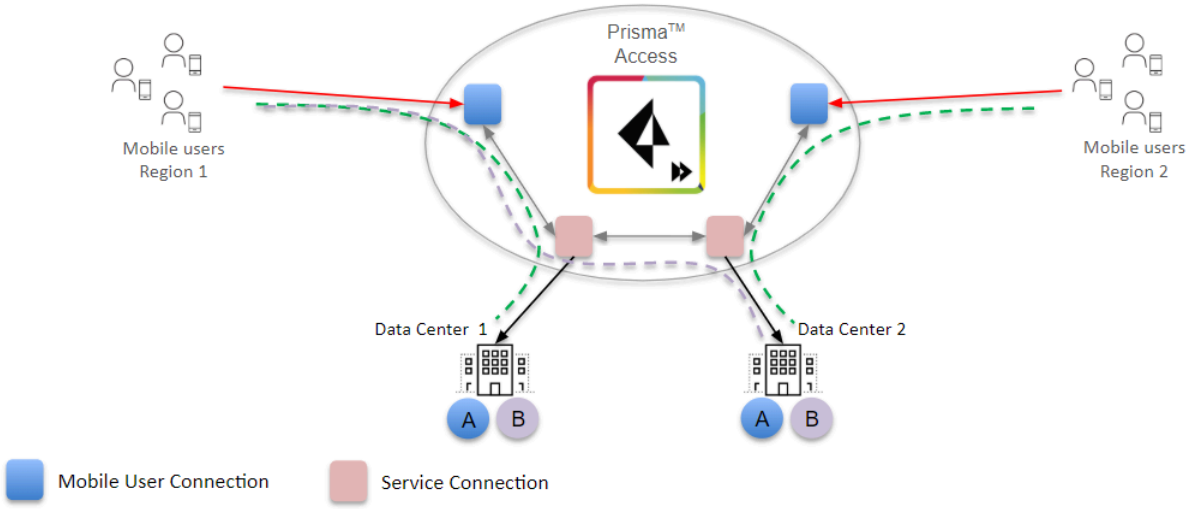
備に適合するように設計されたデフォルトのルーティング・モデルを 使用するが、すべての組織のネットワークが同じとは限りません。幅広いデプロイメントに対応するために、Prisma Accessではサービス接続のルーティングについて他のモードを選択することも可能です。

*Prisma Access*サービス接続のルーティング方法を変更するには、組織のトポロジーとルーティングデバイス、および*Prisma Access*の仕組みをこのセクションで説明している通りに完全に理解しておく必要があります。ルーティング方法をデフォルト設定から変更する前に、このセクションをよくお読みください。

Prisma Accessは、スタティック ルーティングと、サービス接続とリモート ネットワーク接続のためのBGPを使用したダイナミック ルーティングをサポートしています。接続にBGPルーティングを使用する場合、お使いの組織のネットワークはPrisma AccessからBGP情報を学習します。

どのサービス接続ルーティングを使用するかを決定する前に、Prisma Accessがモバイル ユーザー、リモート ネットワーク、およびサービス接続間のトラフィックをどのようにルーティングするかを理解する必要があります。なぜなら、サービス接続間のモバイル ユーザ トラフィックとリモート ネットワーク トラフィックで使用されるルーティングは異なるからです。

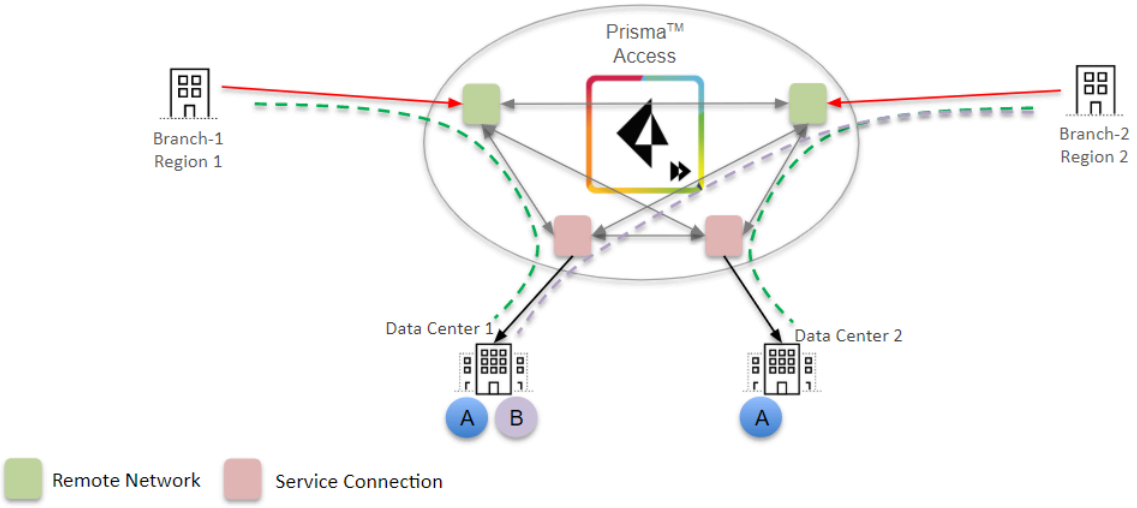
モバイル ユーザー サービス接続ルーティング- モバイル ユーザー接続は、最も近いサービス接続とのIPSecトンネルを形成します。 Prisma Accessは内部ルーティングにはiBGPを使用し、データセンターの顧客構内機器とのピアリングにはeBGPを使用します。Regions 1および2のモバイルユーザーが、それぞれのリージョンのサービス接続にルーティングされている図を次に示します。Region 1のモバイルユーザーは、Data Center 1にあるアプリケーション**A**と**B**にアクセスしています。組織ネットワークがサービス接続に対してBGPルーティングを使用しており、Data Center 1でサービス接続にISP障害が発生した場合、Prisma Accessは障害を検知して、BGPコンバージェンス後にアプリケーション**A**と**B**のトラフィックをData Center 2にルーティングすることで、ネットワークのデータセンターの冗長性を確保しています。



©2025 Palo Alto Networks, Inc.

*Prisma Access*は障害を検出すると、*BGP*で次のタイミングを使用します。*BGP*ルーティングを設定し、トンネル監視を有効にしている場合、セキュリティパラメータインデックス（*SPI*）が失敗していると判断するまでの、デフォルトのホールドタイムがもっとも短いのが、*Tunnel Monitor*です。これは、連続した*15*秒間のトンネル障害を検出すると、ピアへのすべてのルートを削除します。このように、*Tunnel Monitor*が*BGP*ルートの動作を判断します。トンネルモニタリングを設定しない場合、ホールドタイマーはルートを削除する前にトンネルがダウンしている時間を決定します。 *Prisma Access*は、*RFC 4271*で定義されているデフォルトの*BGP HoldTime*値*90*秒を使用します。これは、*Prisma Access*が非アクティブな*SPI*のルートを削除するまでの最大待機時間です。ピア*BGP*デバイスに短いホールドタイムが設定されている場合、*BGP*ホールドタイマーはより小さい方の値を使用します。セカンダリトンネルが正常にインストールされた場合、プライマリトンネルが復旧するまでの間、セカンダリルートが優先されます。プライマリとセカンダリの両方が機能している場合は、プライマリルートが優先されます。

リモートネットワーク-サービス接続ルーティング—Prisma Accessは、他のリモートネットワークおよびサービス接続との、フルメッシュネットワークを作成します。モバイルユーザーのように、Prisma Accessは内部ルーティングにiBGPを、カスタマ構内設備とのピアリングによるルートの交換にeBGPを使用します。Branch 1のユーザーが組織のデータセンター内のData Center 1からアプリケーション**A**にアクセスしており、Branch 1とData Center 1間のリンクがダウンした場合、Prisma AccessはBGPコンバージェンス後にアプリケーション**A**のトラフィックをData Center 2にルーティングします。



Prisma Accessサービス接続のルーティングと、それがネットワークにどのように関係するかを理解したら、サービス接続のルーティング モードとして、以下のいずれかを選択することができます。

- デフォルト ルーティング - これはPrisma Accessが使用するデフォルトのルーティング モデルです。

  Prisma AccessがBGP属性を調整せずにBGPベストパス選択メカニズムを使用したい場合は、このルーティン グモードを使用する。このモードでPrisma Accessは、カスタマ構内設備（CPE）がアドバタイズする任意の属性を使用します。

©2025 Palo Alto Networks, Inc.

- Hot Potatoルーティング—Prisma Accessは、できる限り早く組織ネットワークにトラフィックを渡します。

  組織ネットワークに、大部分のルーティング決定を行わせたい場合に、このルーティング手法を使用します。

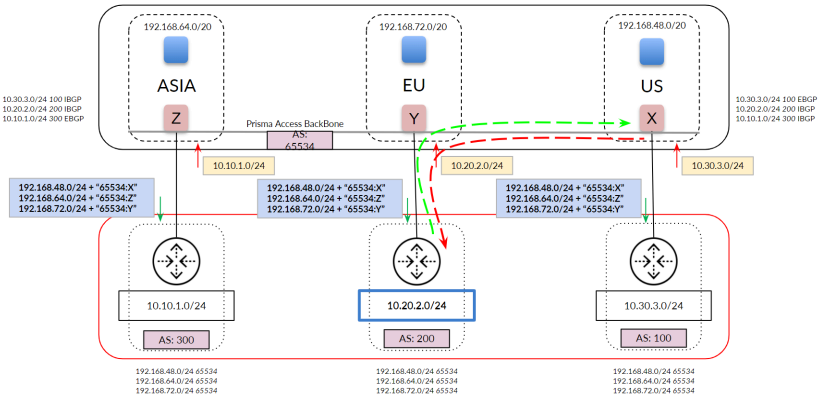
Prisma Access デフォルトルーティング

デフォルトのルーティングモードで、Prisma Accessがサービス接続トラフィックをルーティングする例を次の図に示します。組織ネットワークには、3つのデータセンター内に3つの個別のネットワークが存在しており、ネットワークに接続するバックボーンは存在していません。図の下部に示されているように、デフォルトのルーティングモードで、モバイルユーザープールは3つのネットワークに均等にアドバタイズされます。

Prisma Accessがモバイルユーザールートをアドバタイズする場合、アドバタイズ前にサブネットがClass C /24アドレスブロックに分割されることに注意してください。つまり、プレフィックスがゲートウェイで消費されるにつれて、/20モバイルユーザーサブネットが、/24単位でアドバタイズされます。

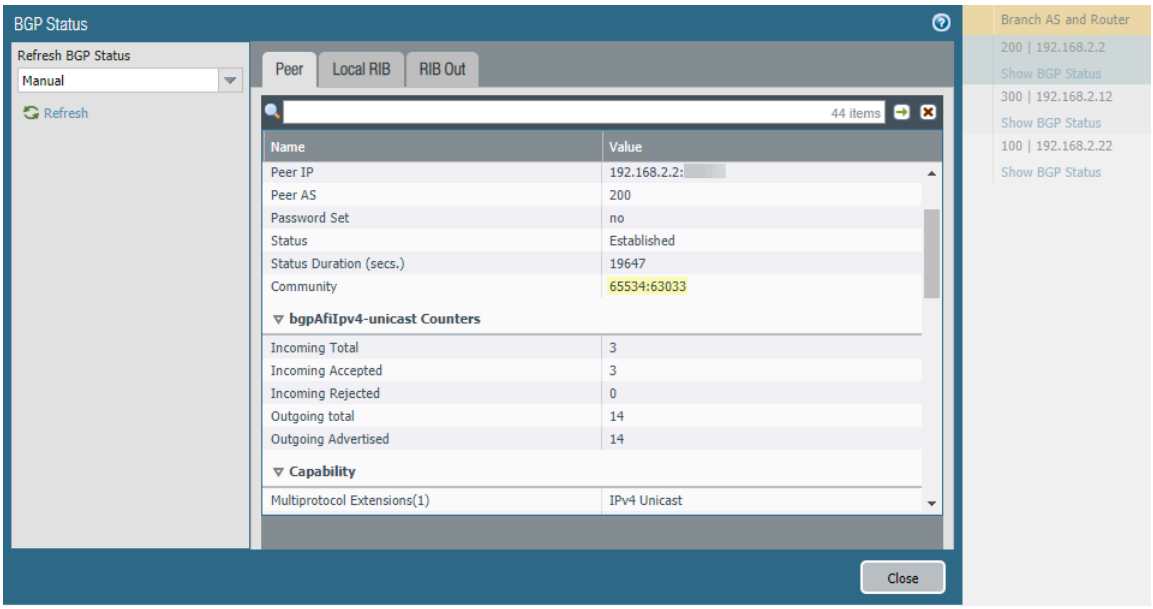
Prisma AccessがBGPルートアドバタイズを使用する仕組みについて書き留めてください:

- Prisma Accessは、モバイルユーザーがアドバタイズしたルートのデフォルトBGP属性を調整しません（Prisma Accessは、ルートアドバタイズにAS番号を追加します）。
- Prisma Accessは、モバイルユーザールートを/24のサブネットブロックでアドバタイズして、サービス接続経由でアドバタイズするルートにBGPコミュニティ値を追加します。次の図は、モバイル ユーザーIPアドレス プール 3つのサービス接続と3つの異なるIPアドレス ブロックが指定されたモバイル ユーザーのデプロイメントを示したものです。アジア、オーストラリア、日本 地域では`192.168.64.0/20`、 アフリカ、ヨーロッパ、中東 地域では`192.168.72.0/20`、 北米および南米 地域では `192.168.48.0/20` です 。 Prisma Access これらのルートを /24 のブロックに分割し、AS番号 **65534**でアドバタイズしますが、アドバタイズに BGP コミュニティ値 (アジアの場合は**Z**、EU の場合は **Y**、米国の場合は **X**) も追加します。これらのルートは、図の中央に表示されています。このようにすることで、Prisma Accessが同じAS番号を割り当てる場合でも、サービス接続を区別することができます。



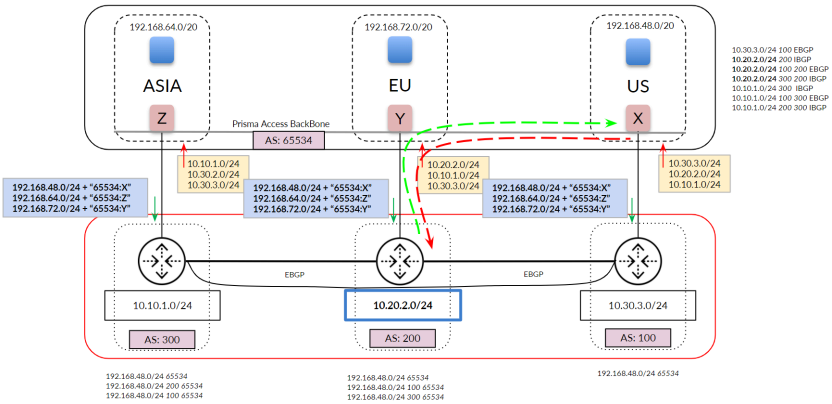
コミュニティ文字列を参照するには、**Panorama** > **Cloud Services**（クラウドサービス） > **Status**（ステータス） > **Network Details**（ネットワーク詳細） > **Service Connection**（サービス接続） > **Show BGP Status**（BGPステータスの表示）を選択して、**Peer**（ピア）タブの**Community**（コミュニティ）フィールドを探します。

©2025 Palo Alto Networks, Inc.



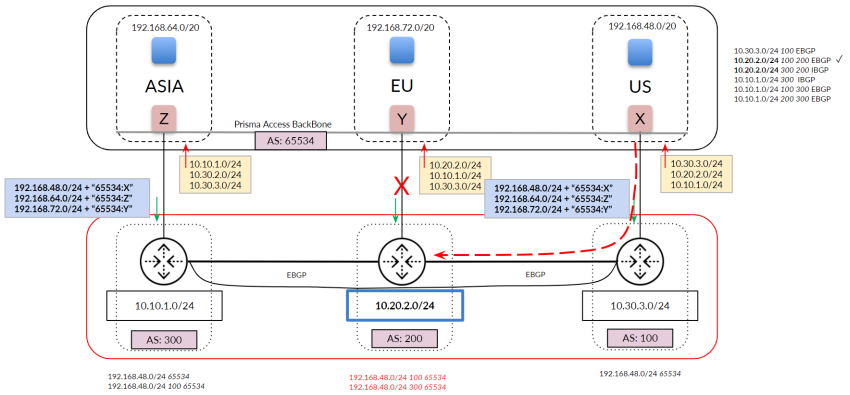
フルメッシュeBGPバックボーンを持つ、一般的なネットワークを次の図に示します。この図は、Prisma Accessが右上にある組織ネットワークから学習したルートを表しています。Prisma Accessのバックボーン（iBGP）および組織のバックボーン（eBGP）を介してPrisma Accessが学習した、追加のルートに注意してください。

North America & South America（北米と南米）リージョン（図のUS）のモバイルユーザーと組織の**Africa, Europe & Middle East**（アフリカ、欧州、中東）リージョン（図のEU）のデータセンター間のトラフィックに対して、Prisma AccessはAS-PATHが短いルートを優先するため、EUサービス接続経由のパスが選択されます。



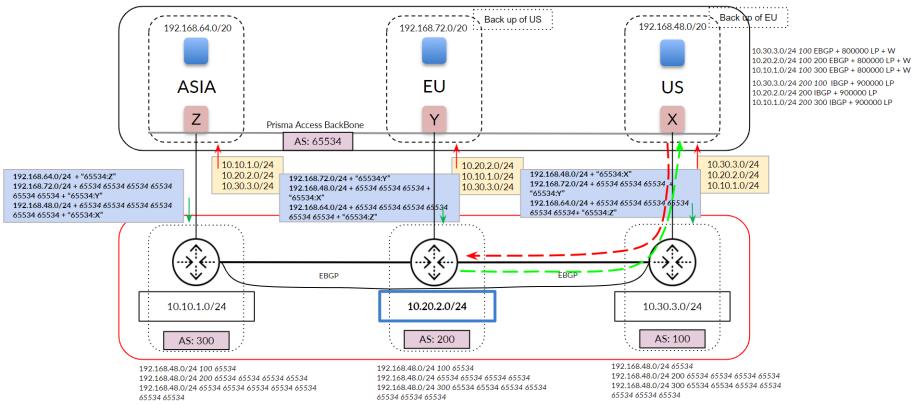
フルメッシュeBGPバックボーンを持つデプロイ環境の場合、顧客のデータセンターのISP/CPE障害により、Prisma Accessが特定のデータセンターに到達できないと、非対称が発生する可能性があります。EUサービス接続へのリンクがダウンした場合に、何が起きるのかを次の図に示します。ネットワークはリンク障害を検出して、AS 200用の新しいルートテーブルを作成します。USサービス接続からAS 200へのトラフィックは、AS 200とAS 100間のバックボーンに対するeBGPルートの方が、サービス接続EUおよびUS間のiBGPルートよりも好ましいため、AS 200はAS 100経由のルートを使用します。ただし、オンプレミスCPEがWriterトラフィックに対してどちらかのパスを選択する可能性があるため（赤で表示）、リターントラフィックで同じパスが使用されることは保証されません。

 ©2025 Palo Alto Networks, Inc.



前の例では、ルートが集約されていないネットワークを表していました（Prisma AccessにBGPルートアドバタイズを送信する前に、ルートの要約を実施していない）。次の例は、ルートをPrisma Accessに送信する前に、10.0.0.0/8で要約するネットワークを表しています。デフォルトのルーティングを選択した場合、Prisma Accessが要約されたルートから正しいリターンパスを判断できないため、この設定では非対称ルーティングの問題が発生する可能性があります。

*Prisma Access*デプロイ環境にリモートネットワークが存在している場合、サービス接続でルート要約を使用することはお勧めできません。サービス接続でのルート要約は、モバイルユーザーデプロイ環境専用です。



モバイルユーザーに対してルート集約を使用する場合、デフォルトのルーティングではなくhot potato(ホットポテト)ルーティングを使用することを強くお勧めします。この場合、Prisma Accessは組織のネットワークにできる限り早くトラフィックを渡します。また、各サービス接続に確定的ルーティングを行わせるように、次のセクションで説明している**Backup SC**を選択することをお勧めします。

Prisma AccessHot Potato (ホットポテト)ルーティング

Hot Potato Routing（ホットポテトルーティング）を選択すると、Prisma Accessは内部ネットワークからサービス接続/データセンターに向けたトラフィックを、できる限り早く送信します。

ホットポテトルーティングで、Prisma Accessはゲートウェイから送信されるBGPプレフィックスアドバタイズの先頭にASパス（AS-PATH）を追加します。この先頭への追加は、プレフィッ

 ©2025 Palo Alto Networks, Inc.

クスが組織のオンプレミスCPEへのサービス接続からアドバタイズされるときに実行されます。Prisma AccessはAS-PATHを先頭に追加して、CPEがプライマリ トンネルとセカンダリ トンネルに適切な優先順位を与えるようにします。これにより、プライマリ トンネルがダウンした場合に、CPEがセカンダリ トンネルをバックアップとして選択できるようになります。

セカンダリ（バックアップ）BGPピアに異なるIPアドレスを指定した場合、次の表に示すように、Prisma Accessはトンネル・タイプに基づいてさらにプリペンドを追加します。

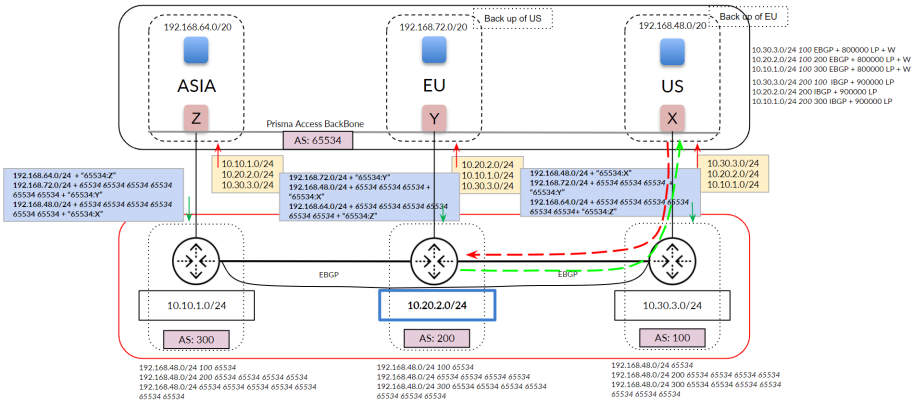
プレフィックスタイプ	サービス接続トンネルタイプ	AS-PATH付加数	CPEで見られるAS-PATH合計
プライマリサービス接続からのゲートウェイプレフィックス	同じBGPピアIPアドレスを持つプライマリまたはセカンダリトンネル	0	1
バックアップサービス接続からのゲートウェイプレフィックス	同じBGPピアIPアドレスを持つプライマリまたはセカンダリトンネル	3	4
その他のすべてのサービス接続からのゲートウェイプレフィックス	同じBGPピアIPアドレスを持つプライマリまたはセカンダリトンネル	6	7
プライマリサービス接続からのゲートウェイプレフィックス	異なるBGPピアIPアドレスを持つセカンダリトンネル	1	2
バックアップサービス接続からのゲートウェイプレフィックス	異なるBGPピアIPアドレスを持つセカンダリトンネル	4	5
その他のすべてのサービス接続からのゲートウェイプレフィックス	異なるBGPピアIPアドレスを持つセカンダリトンネル	7	8

hot potato(ホットポテト)ルーティングモードでは、Prisma Accessはオンボーディング時にバックアップ・サービス接続を指定できます。**Backup SC**を指定することでPrisma Accessに、サービス接続リンクの障害発生時に、このサービス接続をバックアップとして使用することを指示します。

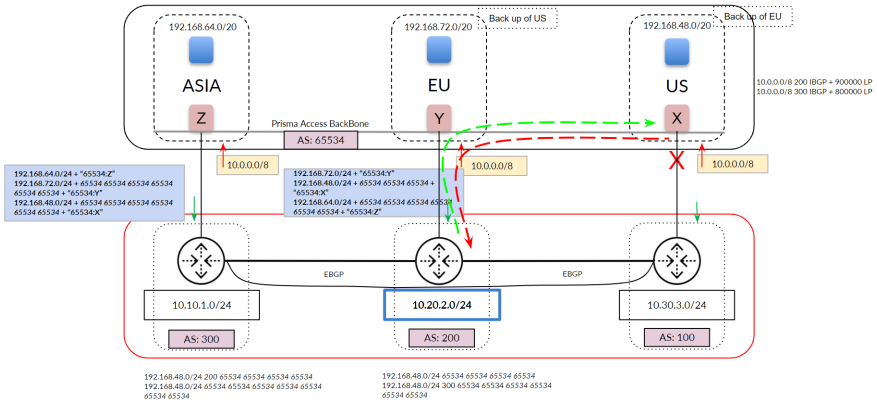
USサービス接続とAS 200間のホットポテトルーティング設定を次の図に示します。ここで、EUサービス接続はUS接続の**Backup SC**として設定されています。Prisma Accessはホットポテトルーティングを使用して、USサービス接続経由でトラフィックをもっとも近い出口パスから送信します。戻りトラフィックはAS100を通る同じパスをたどります。これは、このパスの方が米国のモバイル ユーザー プールへのAS-PATHが短いためです。 Prisma Accessは、 トン

 ©2025 Palo Alto Networks, Inc.

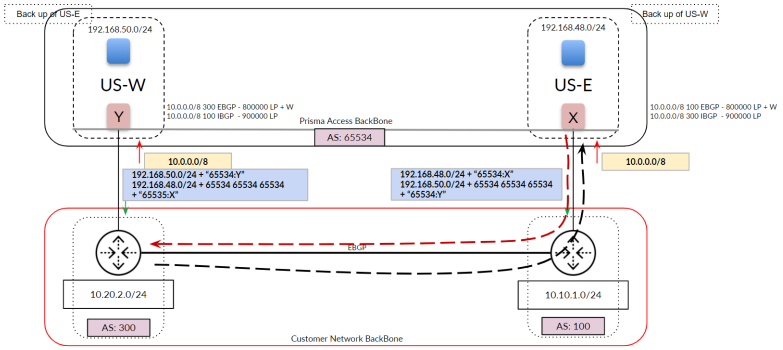
ネルがプライマリ トンネルであるか、バックアップ トンネルであるか、あるいはプライマリにもバックアップにも使用されていないかに応じて、プレフィックス アドバタイズメントの先頭にAS-PATHを追加します。



バックアップサービス接続を設定しているため、USサービス接続へのリンクがダウンした場合、ホットポテトルーティングは、EUサービス接続経由のもっとも短いルートを使ってトラフィックを送信します。このルーティングの例は、ルート集約を使用しているネットワークにも適用されます。



単一のリージョン内の複数のサービス接続に対して、バックアップサービス接続を使用することも可能です。North America（北米）リージョンに2つのサービス接続を持つ、Prisma Accessデプロイ環境を次の図に示します。この場合、US-Wの**Backup SC**としてUS-Eを設定し、またその逆の設定を行って、対称ルーティングを維持しています。



 ©2025 Palo Alto Networks, Inc.

ルーティングの優先度の設定

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

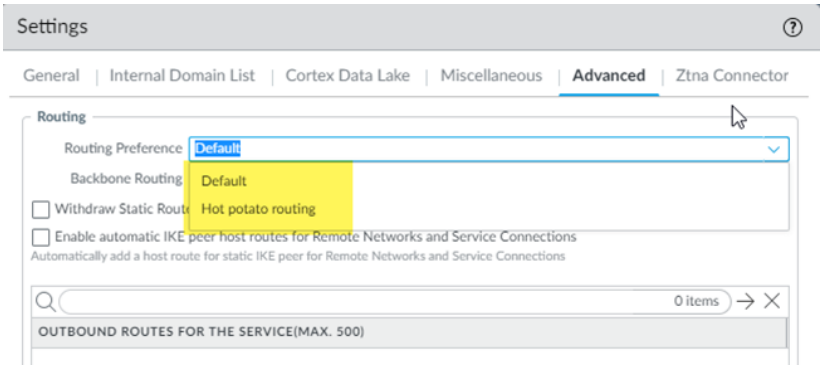
ルーティングの優先度を有効にするには、次の作業を行ってください。

これらのルーティング設定を構成するには、サービス接続に静的ルーティングではなくBGPルーティングを使用する必要があります。

STEP 1 | サービス接続を構成します。

STEP 2 | (任意) サービス接続に使用するルーティングを選択します。

1. Prisma Accessを管理するPanoramaから 、**[Panorama]** > **[Cloud Services]** > [設定] > [サービス セットアップ] に移動し、歯車をクリックして 設定を編集します。
2. 詳細設定で、**[Routing Preference (**ルーティングの設定**)]**（デフォルトまたは**[Hot Potato (**ホットポテト**)]**）を選択します。



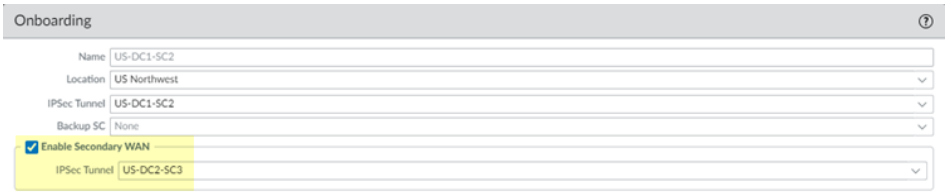
STEP 3 | (任意、 Hot Potatoルーティングのデプロイメントのみ) リンク障害発生時に優先的に使用するサービス接続を指定するには、サービス接続の作成時にBackup SCを設定します。

すでに追加している任意のサービス接続を選択することができます。リンク障害発生時、Prisma Accessは選択した**Backup SC**を、優先するサービス接続として使用します。バックアップサービス接続を選択することで、3つ以上のサービス接続をオンボーディングしている場合の、非対称ルーティングの問題を防止することができます。この選択肢は、Hot potato routing（ホットポテトルーティング）モードでのみ利用できます。

1. **[Panorama]** > **[Cloud Services**（クラウドサービス）**]** > **[Configuration**（設定）**]** > **[Service Connection**（サービス接続）**]**へと移動します。
2. 構成するサービス接続を選択するか、新しいサービス接続を追加します 。

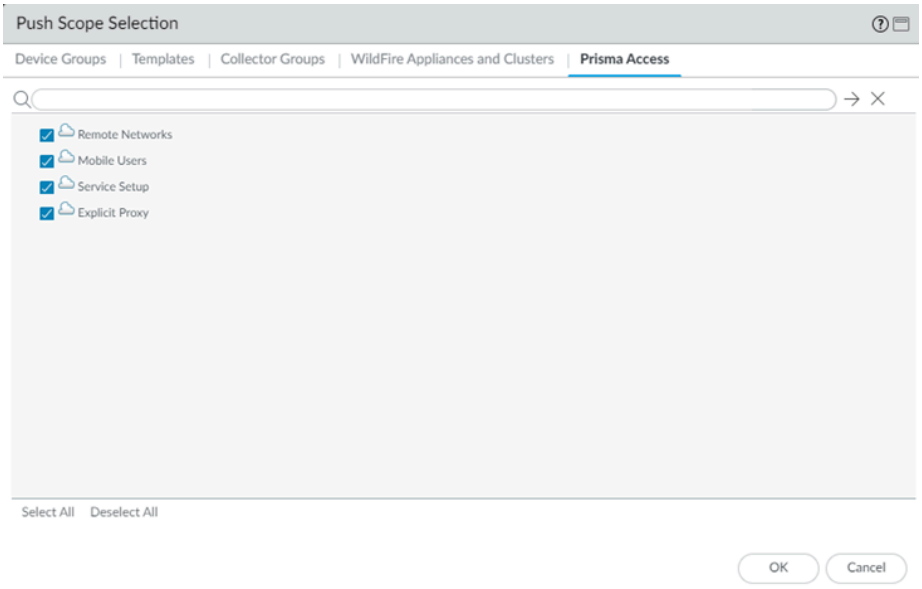
©2025 Palo Alto Networks, Inc.

3. 優先バックアップとして使用するサービス接続 (**Backup SC**) を選択します。



STEP 4 | Panoramaに変更をコミットし、その設定変更をPrisma Accessにプッシュします。

1. **Commit**（コミット） > **Commit and Push**（コミットしてプッシュ）をクリックします。
2. [選択内容を編集]をクリックし、Prisma Accessタブで**[Push Scope (**スコープをプッシュ**)]**に**[Service Setup (**サービスのセットアップ**)]**が選択されていることを確認し、**[OK]**をクリックする。

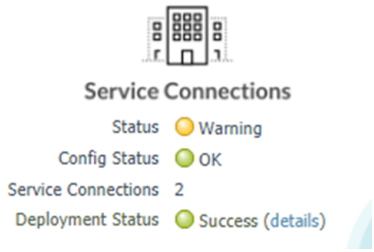


3. **[Commit and Push (**コミットしてプッシュ**)]** をクリックします。

©2025 Palo Alto Networks, Inc.

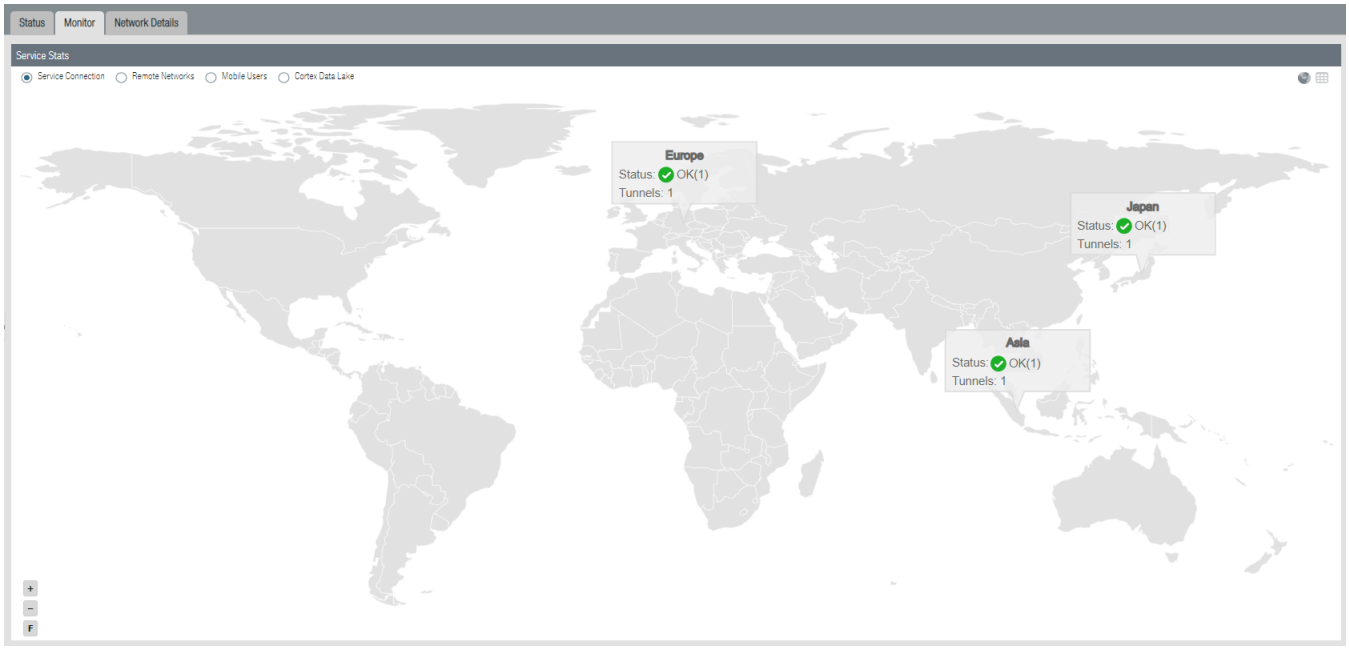
STEP 5 | **Panorama** > クラウド サービス > ステータス > ステータス を選択し、ステータスが **OK**であることを確認して、サービス接続が確立されていることを確認します。

Deployment Status（デプロイステータス）では、オンボーディングおよびデプロイジョブのステータスを参照することができます。また、完了したジョブのステータスに関する詳細情報も参照することができます。



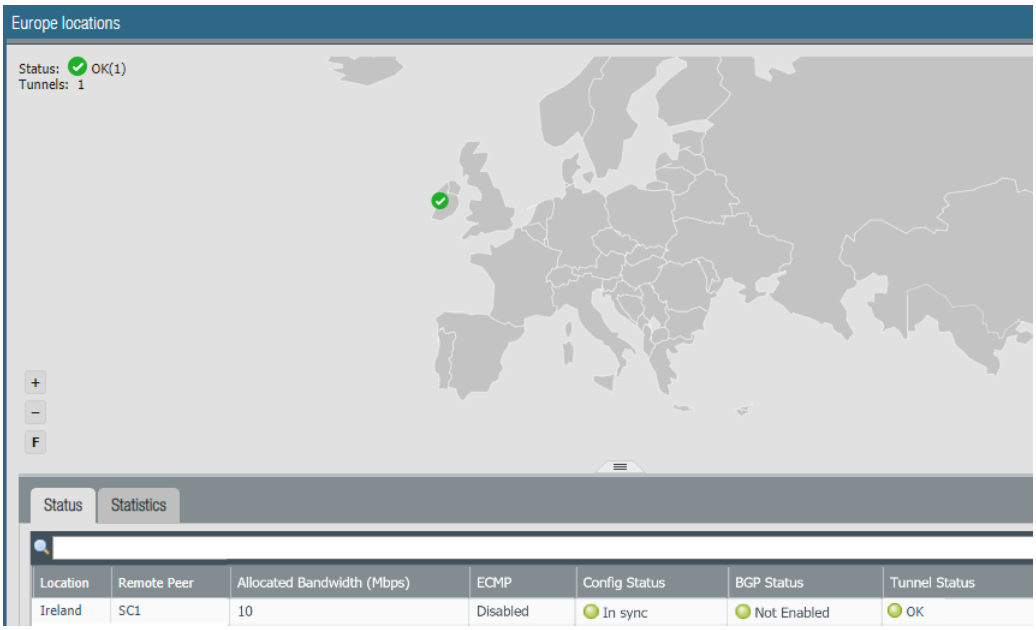
ステータスが**OK**になっていない場合は、Statusアイコン上にカーソルを移動して、エラーがあるかどうかを確認してください。

サービス接続のグラフィカル表示とステータス詳細を参照するには、**Monitor**（監視）タブで**Service Connection**（サービス接続）を選択します。



地域を選択すると、その地域の詳細情報が表示されます。

©2025 Palo Alto Networks, Inc.



マップの下にあるタブをクリックすると、サービス接続に関するその他の情報が表示されます。

Status（ステータス）タブ：

- **Location**（ロケーション）–サービス接続がデプロイされたロケーション。
- **Remote Peer**（リモートピア）–このサービスインフラが、IPSecトンネルをセットアップしている、企業のロケーション。
- **Allocated Bandwidth**（割当たられている帯域幅）–割り当てられたサービス接続数に300 Mbpsを乗じた値。

  この数値は、利用可能なサービス接続帯域幅を表しているものではありません。

  各サービス接続は約*1Gbps* のスループットを提供しますが、実際のスループットは次のようないくつかの要因に依存します。

  - トラフィックミックス（例:フレームサイズ）
  - サービス接続と本社またはデータセンター間のレイテンシとパケットロス
  - サービスプロバイダのパフォーマンス制限
  - 顧客の終端デバイスのパフォーマンス制限
  - その他の顧客データセントートラフィック
- **ECMP**–このサービス接続に対してECMP（Equal Cost Multipath）を設定している場合。サービス接続ではECMPが使用されないため、このステータスは**Disabled**（無効）になります。

©2025 Palo Alto Networks, Inc.

- **Config Status**（設定ステータス）–サービスへの設定の最後のプッシュのステータス。ローカル設定とクラウド内の設定が一致する場合、Config Statusは**In sync**（同期）になります。ローカルで変更を行ったけれども、まだクラウドに設定をプッシュしていない場合、ステータス**Out of sync**（非同期）が表示される可能性があります。ステータスインジケータ上にカーソルを移動すると、詳細情報が表示されます。設定をPrisma Accessにコミットしてプッシュすると、Config Statusが**In sync**になります。
- **BGP Status**（**BGP**ステータス）–企業/本社のロケーションのファイアウォールまたはルーターとサービス接続が確立されているPrisma Access間のBGP状態に関する情報が表示されます。一時的にステータスが各種BGP状態（**Idle**、**Active**、**Open send**、**Open pend**、**Open confirm**）に切り替わることがありますが、一般的にBGPステータスには次のような項目が表示されます。
  - **Connect**（接続）–データセンター/本社のルーターが、Prisma AccessとのBGPピアリレーションシップの確立を試みています。
  - **Established**（確立済み）–BGPピアリレーションシップが確立されています。

  このフィールドには、BGP接続がエラー状態にあるかどうかも表示されます。
  - **Warning**（警告）–8分間以上に渡ってBGPステータスの更新がありません。ファイアウォールが機能停止している可能性があります。
  - **Error**（エラー）–BGPステータスが不明です。
- **Tunnel Status**（トンネル ステータス）–Prisma Accessとサービス接続間の接続の運用ステータス。

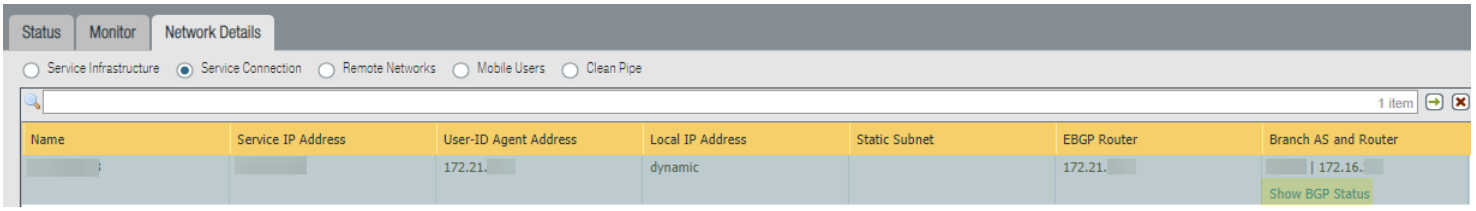
Statistics（統計）タブ：

- **Location**（ロケーション）–サービス接続がデプロイされたロケーション。
- **Remote Peer**（リモートピア）–このサービス接続が、IPSecトンネルをセットアップしている、企業のロケーション。
- **Ingress Bandwidth (Mbps)**（着信帯域幅）–本社/データセンターのロケーションからPrisma Accessへの帯域幅。
- **Ingress Peak Bandwidth (Mbps)**（着信ピーク帯域幅）–本社/データセンターのロケーションからクラウドサービスへのピーク負荷。
- **Egress Bandwidth (Mbps)**（出力帯域幅）–Prisma AccessからHQ/データセンターへの帯域幅。
- **Egress Peak Bandwidth (Mbps)**（発信ピーク帯域幅）–Prisma Accessから本社/データセンターのロケーションへのピーク負荷。
- **QoS**–このボタンを選択すると、クラスあたりの破棄パケット数を含めた、リアルタイムの、および過去のQoS統計情報を表したグラフが表示されます。このグラフには、QoSが有効になっているサービス接続またはリモートネットワーク接続のみが表示されます。

BGPを設定した場合、**Panorama** > **Cloud Services**（クラウドサービス） > **Status**（ステータス） > **Network Details**（ネットワーク詳細） > **Service Connection**（サービス接続） >

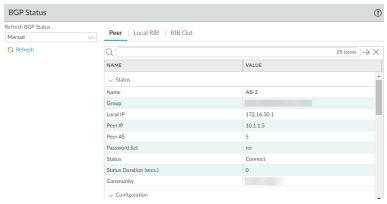
 ©2025 Palo Alto Networks, Inc.

Show BGP Status（**BGP**ステータスの表示）の順に選択して、そのステータスを確認することができます。



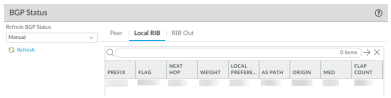
BGP Status（BGPステータス）ダイアログが表示されます。このタブには、次の情報が表示されます。

- **Peer**（ピア）–ステータス、ルート数合計、設定、およびランタイム統計とカウンタを含む、BGPピアのルーティング情報。ルート数合計は**bgpAfiIpv4-unicast Counters**エリアの、**Incoming Total**（着信合計）および**Outgoing Total**（発信合計）フィールドに表示されます。



- ローカル**RIB**- Prisma Accessがローカルで使用する BGP ルート。Prisma Accessは、隣接するネットワーキングデバイスから送信された情報を保管する、BGP RIB-Inテーブルからこの情報を選択し、ローカルBGPインポートポリシーおよびルーティング決定を適用し、ルーティング情報ベース（RIB）にローカルのRIB情報を保管します。

  最初の256件のエントリのみが表示されることに注意してください。その他のエントリを表示するには、Filter（フィルタ）フィールドにサブネットまたはIPアドレスを入力して、Apply Filter（フィルタの適用）をクリックします。最大256件の、ルーティングエントリのサブセットが表示されます。



- **RIB Out**–BGP更新メッセージを利用して、Prisma Accessがピアにアドバタイズするルーティング情報。

複数のサービス接続を使用して高帯域幅ネットワークを作成する

追加のサービス接続帯域幅が必要な本社またはデータセンターの場所がある場合は、その場所への複数のサービス接続を構成できます。

各Prisma Accessサービス接続には帯域幅の上限はありませんが、Palo Alto Networksでは、各サービス接 続が約1 Gbpsのスループットを提供できると見込んでいます。この帯域幅は通常、本社またはデータ センター内の内部リソースにアクセスするには十分ですが、データセンターで内部またはプライベートのSaaSアプリケーションをホストしている場合など、追加の帯域幅が必要な展開がある場合もあります。

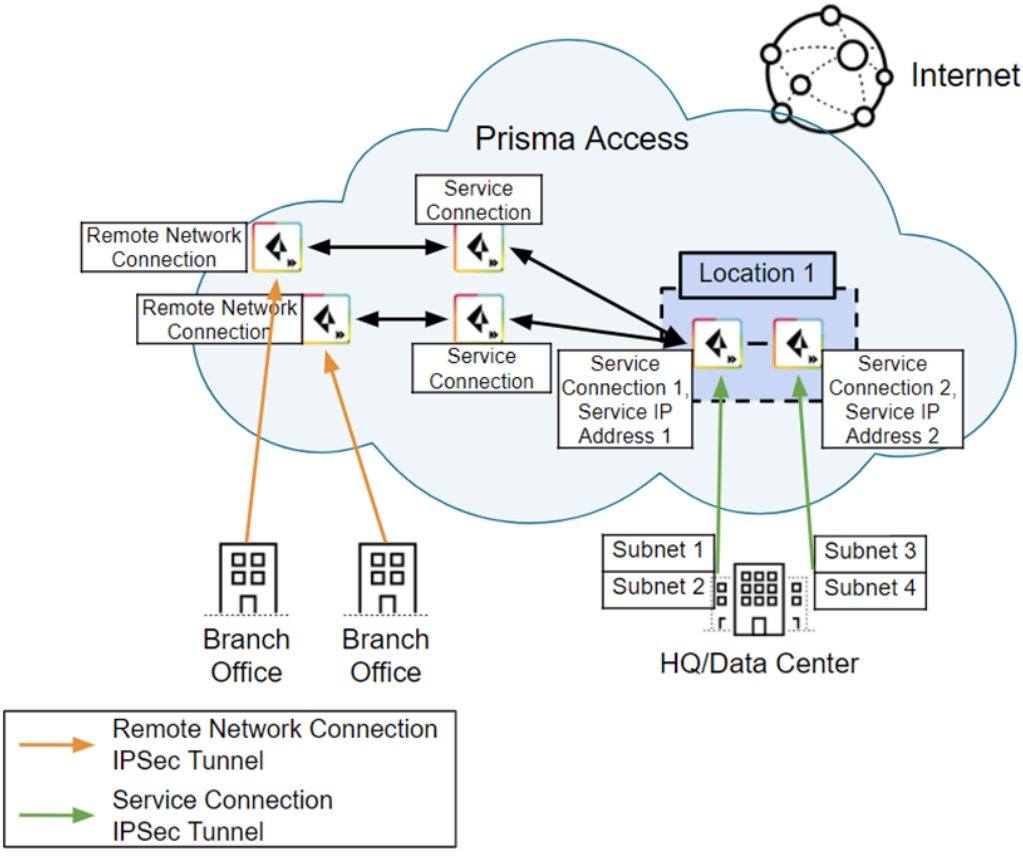
©2025 Palo Alto Networks, Inc.

本社またはデータセンター サイトへの広帯域サービス接続を作成するには、同じPrisma Accessロケーショ ンへの複数のサービス接続を使用してサイトをオンボーディングします。

*Prisma Access*は、*1*つの本社またはデータセンター リモート ネットワーク ロケーションにオンボードで接続で きるサービス接続の最大数を制限しませんが、*Palo Alto Networks*は、高帯域幅のデプロイメントで*4*つを超えるサービス接続を使用しないことを推奨します。社内アプリにアクセスするためにより多くの帯域幅が必要な場合は、複数のサービス接続の代わりにZTNA ConnectorまたはColo-Connectを使用してください。

次の図は、同じPrisma Accessロケーションから2つのサービス接続を持つ本社またはデータセンター サイトによるPrisma Accessリモート ネットワークの展開を示しており、サイトとPrisma Accessロケーションの間で実質的に2Gbpsの帯域幅を提供しています。

高帯域幅アクセス用に展開されているサービス接続に加えて、図には別のサービス接続のセットが示されています。これらのサービス接続は、Prisma Accessに通常のルーティング機能を提供します (この図では、リモート ネットワーク接続と高帯域幅サービス接続間の内部ルーティングアクセスを提供します)。Palo Alto Networksでは、高帯域幅接続をデプロイする場合、本社またはデータ センターの場所にあるリソースへのアクセスのみを提供するサービス接続を予約し、リモート ネットワーク、モバイル ユーザー、およびデータセンター内のリソース間の内部ルーティングに使用する追加のサービス接続をデプロイすることをお勧めします。



©2025 Palo Alto Networks, Inc.

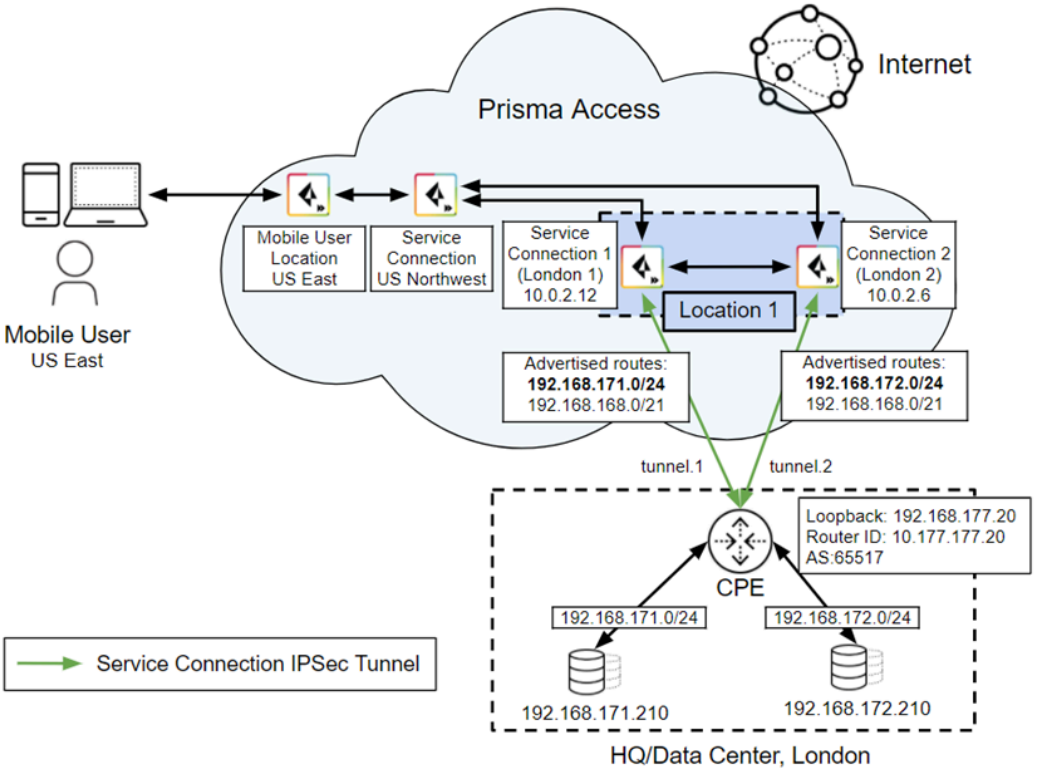
各サービス接続はアクティブで、独自の**Service IP Address (サービスIPアドレス)** を持っています。 サービス エンドポイント アドレスは、各サービス接続のIPSecトンネルを終了するために使用します。

本社またはデータセンターへの高帯域幅接続を確立する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

単一の本社またはデータセンターの場所への複数のサービス接続を構成するには、次の手順を実行します。

このセクションの手順では、次の図に示すようなデプロイメント例を使用します。この例では、ロンドン本社は、2つの異なる顧客構内設備 (CPE) インターフェース (tunnel.1 と tunnel.2) で終了する2つの異なるIPSecトンネルを使用して、2つの異なるサービス接続 (ロンドン1とロンドン2) に接続します。



この例とこのセクションの手順では、次世代ファイアウォールを使用してCPE上のサービス接続を終了します。ただし、対称ルーティングとPBFまたはポリシーベース ルーティングをサポートする任意のCPEをCPEとして使用できます。

これらの手順はガイダンスとして使用してください。各ユース ケースでは、このドキュメントの範囲を超える追加の設計と計画が必要になる場合があります。

©2025 Palo Alto Networks, Inc.

STEP 1 | 単一のPrisma Accessロケーションから単一のサイトに複数のサービス接続を展開する前に、ネットワークに以下の前提条件があることを確認してください:

- 本社またはデータセンターの場所でサブネットを分割し、各サービス接続で一意のサブネットをアドバタイズする必要があります。
- 顧客宅内機器 (CPE) は次のネットワーク機能をサポートし、設定できる必要があります。
  - ポリシーベース転送 (PBF) またはポリシーベース ルーティング -CPEは、特定のローカル ソース IP アドレスとサブネットに対して特定のパスを選択できる必要があります。
  - 対称リターン- 特定の IP アドレスとサブネットとの間で対称トラフィック フローが確実に行われるようにCPEを構成し、トンネルの1つがダウンした場合にフェールオーバー トンネルの対称リターンを構成できる必要があります。

STEP 2 | サービス接続を作成し、サービス接続に使用されるIPSecトンネルの接続を確立します。

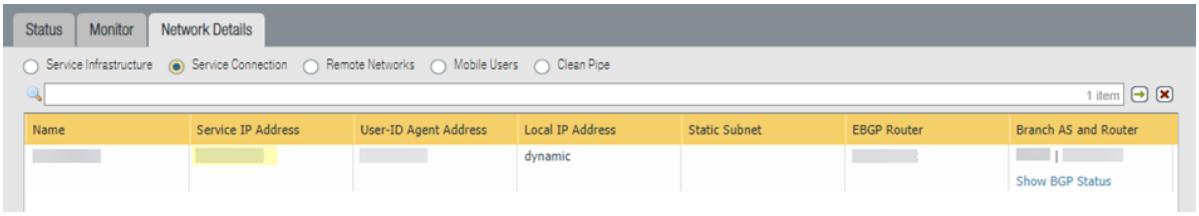
1. Prisma Accessを管理するPanoramaで、サービス接続の設定を行います。これにはIPSec Tunnel (IPSecトンネル)設定、IKE Gateway (IKEゲートウェイ) IPSec Crypto Profile (IPSec暗号プロファイル)、 およびTunnel Monitoring (トンネルモニタリング)設定が含まれます。

   *Prisma Access*は、*IPSec*トンネルの作成プロセスを簡素化するために使用できる、事前定義済みのIPSecテンプレートを提供しています。

2. CPE からPrisma AccessへのIPSecトンネルのリモート側として使用するIPアドレスを見つけます。 **[Panorama]** > **[Cloud Services (クラウドサービス)]** > **[Status (ステータス)]** > **[Network Details (ネットワークの詳細)]**を選択し、**[Service Connection (サービス接**

©2025 Palo Alto Networks, Inc.

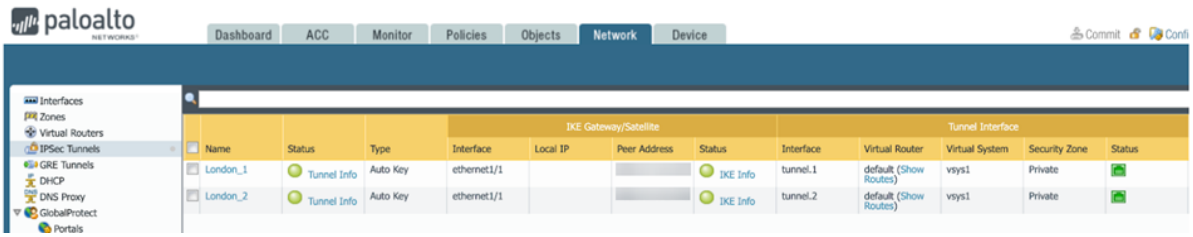
続)]ラジオボタンをクリックし、サイトの[Service IP Address (サービスIDアドレス)]をメモします。



3. CPEでサービス接続へのIPSecトンネルを作成します

   1. IKEトンネルとIPSecトンネルがピア間の認証と暗号化に同じ暗号化プロファイルを使用していることを確認します。
   2. ピアFQDNとしてトンネル用にサービスIPアドレスを使用します。またはIPアドレスを使用します。

   次世代ファイアウォールをCPEとして使用する場合は、[ネットワーク] > [IPSecトンネル] を選択し、サービス接続用に2つのトンネルを作成します (次のスクリーンショットのtunnel.1 と tunnel.2)。



STEP 3 | CPE の仮想ルーター設定を作成します。

1つのトンネルで1つのサブネットをアドバタイズし、別のトンネルで別のサブネットをアドバタイズするBGPルーティング インスタンスを作成します。これにより、2つのアクティブなトンネルでの負荷分散が保証されます。

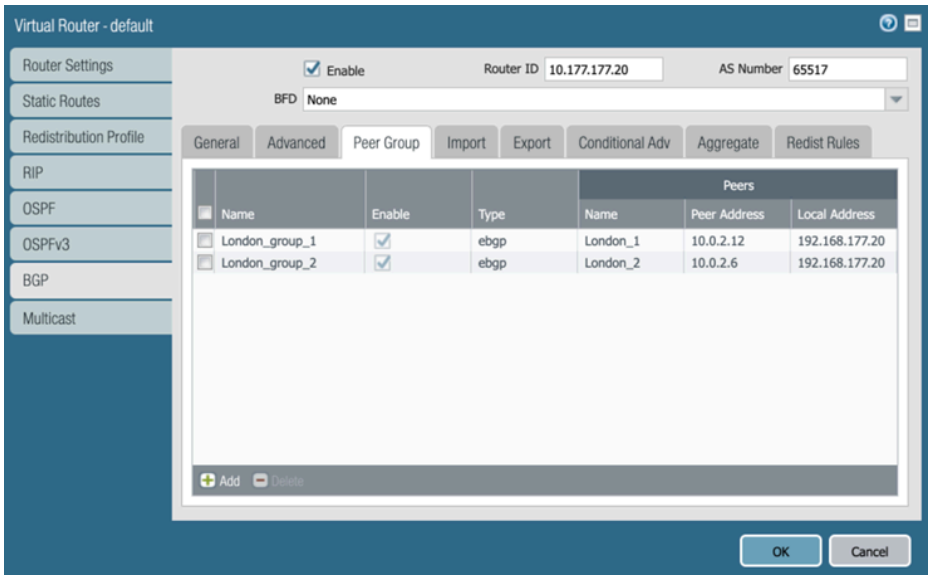
次世代ファイアウォールを CPE として使用している場合は、[ネットワーク] > [仮想ルーター]を選択し、仮想ルーター設定を追加して、各トンネルの [BGP][ピア グループ]の追加を選択し 、次の設定を指定します。

- CPEルーターのルーターIDとAS番号を指定します (この例ではそれぞれ 10.177.177.20 と 65517)。
- サービス接続のピア アドレス として、サービス接続のEBGP ルーターアドレス ([Panorama] > [Cloud Services (クラウドサービス)] > [ステータス] > [ネットワーク詳細] >

 ©2025 Palo Alto Networks, Inc.

[サービス接続] > [**EBGP** ルーター]) を指定します (この例では、サービス接続 1 の場合は 10.0.2.12、サービス接続 2 の場合は 10.0.2.6)。

- ローカル アドレスには、CPE のループバック アドレス (この例では 192.168.177.20) を指定できます。



STEP 4 | 両方のトンネルに使用されるIPアドレスの要約されたサブネットを作成します。

要約されたサブネットを提供することで冗長性が保証されます。両方のトンネルが稼働している場合、トラフィックは最も具体的なルートを使用して宛先に到達します。たとえば、192.168.171.0/24 は、宛先に到達するために tunnel.1 を使用します。アドバタイズされたすべてのサブネット (この例では 192.168.168.0/21) をカバーする要約サブネットを追加すると、tunnel.1 がダウンした場合でも 192.168.171.0/24 からのトラフィックが tunnel.2 から到達可能になり、tunnel.2 がダウンした場合でも 192.168.172.0/24 からのトラフィックが tunnel.1 から到達可能になります。

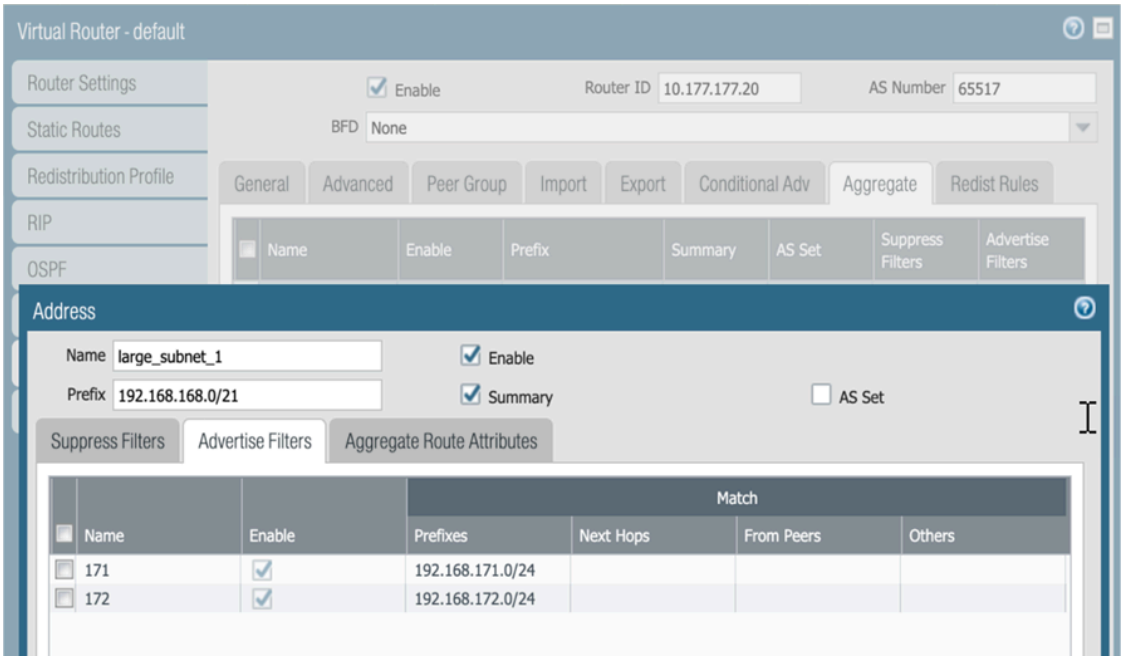
次世代ファイアウォールを CPE として使用している場合は、次の手順を実行します。

1. 仮想ルータ プロファイルの変更を続行し、ルート集約パラメータを追加します ([ネットワーク] > [仮想ルーター] > **[BGP]** > [集約])。

©2025 Palo Alto Networks, Inc.

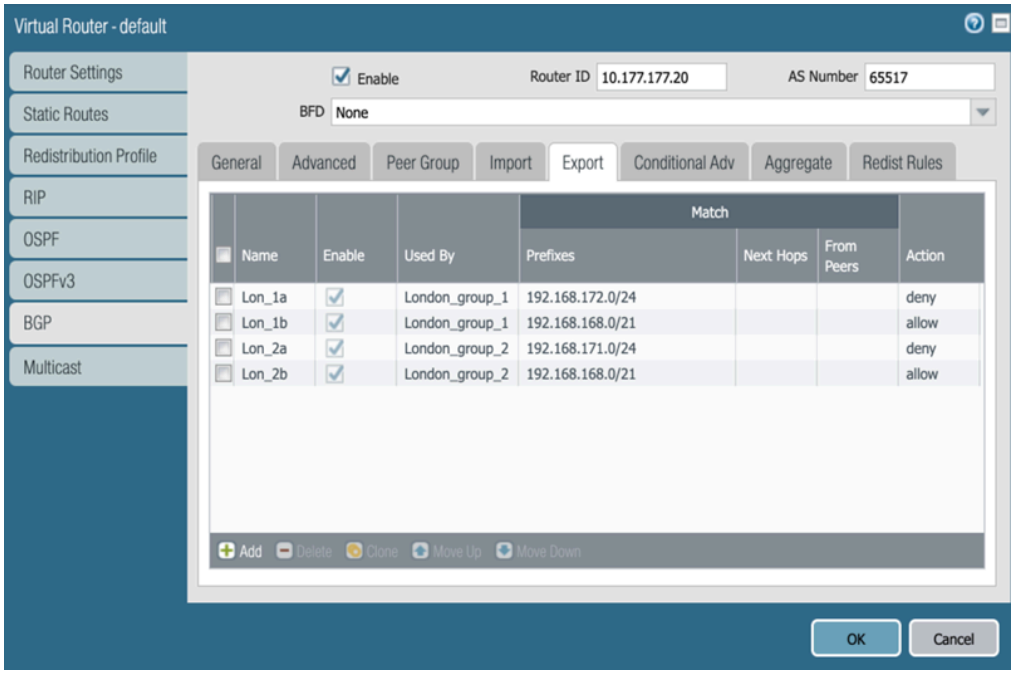
2. サービス接続用にアドバタイズするサブネットの概要サブネットを入力します。

   この例では、2つのデータセンター サブネットを要約する プレフィックス**192.168.168.0/21**を入力します。



3. トンネルが正しいサブネットをアドバタイズするように、エクスポート設定を入力します。

   この例では、最初のサブネット (192.168.171.0/24) が tunnel.1 から到達可能になり、2番目のサブネット (192.168.172.0/24) が tunnel.2 から到達可能になるように、サブネットに対して **deny (**拒否**)** と **allow (**許可**)** の アクション を指定します。



©2025 Palo Alto Networks, Inc.

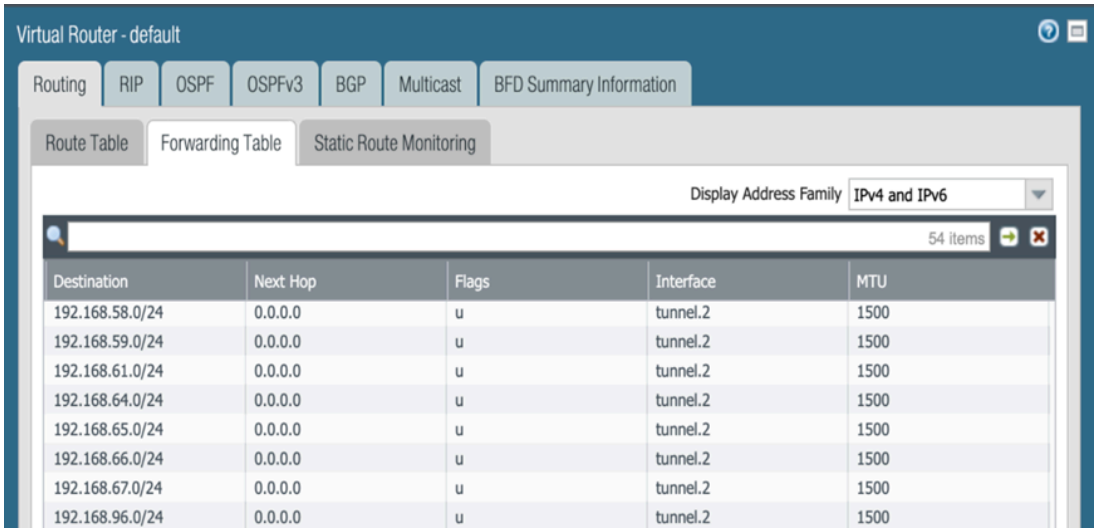
STEP 5 | (2 つ以上のサービス接続があるデプロイメントのみ)2 Gbpsを超える帯域幅でユーザーをプライベート リソースに接続するために2つ以上のサービス接続が必要な場合は、エクスポートされたルートの先頭にAS-PATHを追加して、フェイルオーバーの発生時にサービス接続がデータセンターとの間で対称ルーティングを使用するようにします。詳細は 本社またはデータセンターの場所へのサービス接続を3つ以上設定する を参照してください。

STEP 6 | 対称的なリターンを確保するには（192.168.171.0/24 からのトラフィックが常に tunnel.1 を使用し、192.168.172.0 からのトラフィックが常に tunnel.2 を使用するようにするには）、PBF またはポリシーベースのルーティング ルールを入力します。

デフォルトでは、BGPは優先トンネルに関係なく、すべての異なる宛先のルートをルーティング テーブルにインストールします。次のスクリーンショットは、BGPが192.168.168.0/21サブネットからtunnel.2のすべての宛先をアドバタイズ

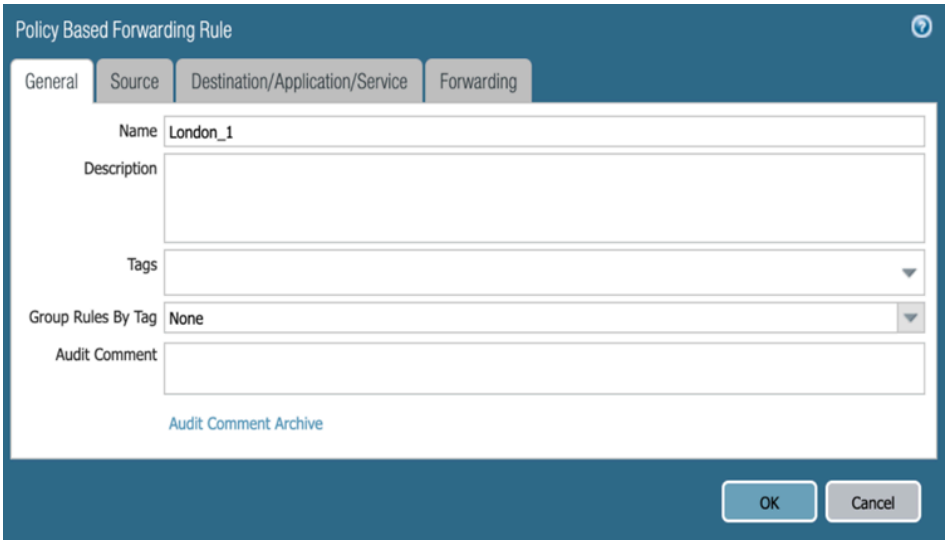
 ©2025 Palo Alto Networks, Inc.

し、192.168.171.0/24からのトラフィックに対して非対称ルーティングが発生する可能性があることを示しています。



対称ルーティングを確実にするには、PBF またはルートベースの転送ルールのセットを構成します。次世代ファイアウォールを CPE として使用している場合は、次の手順を実行します。

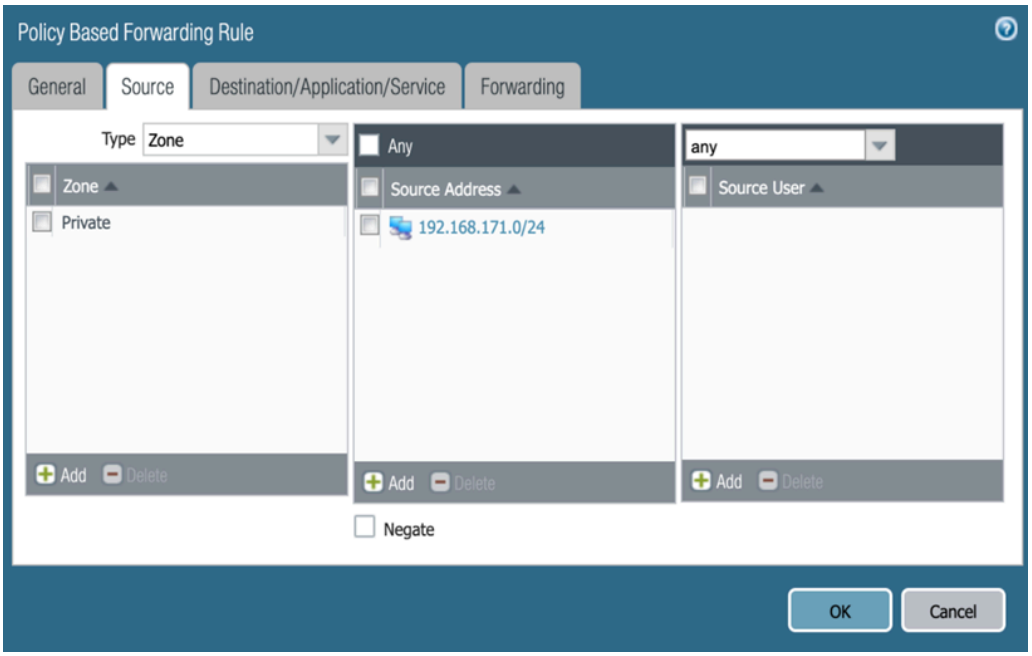
1. **Policies (**ポリシー**) > Policy Based Forwarding (**ポリシーベース フォワーディング**)** を選択して、PBF ポリシー ルールを **Add (**追加**)** します。



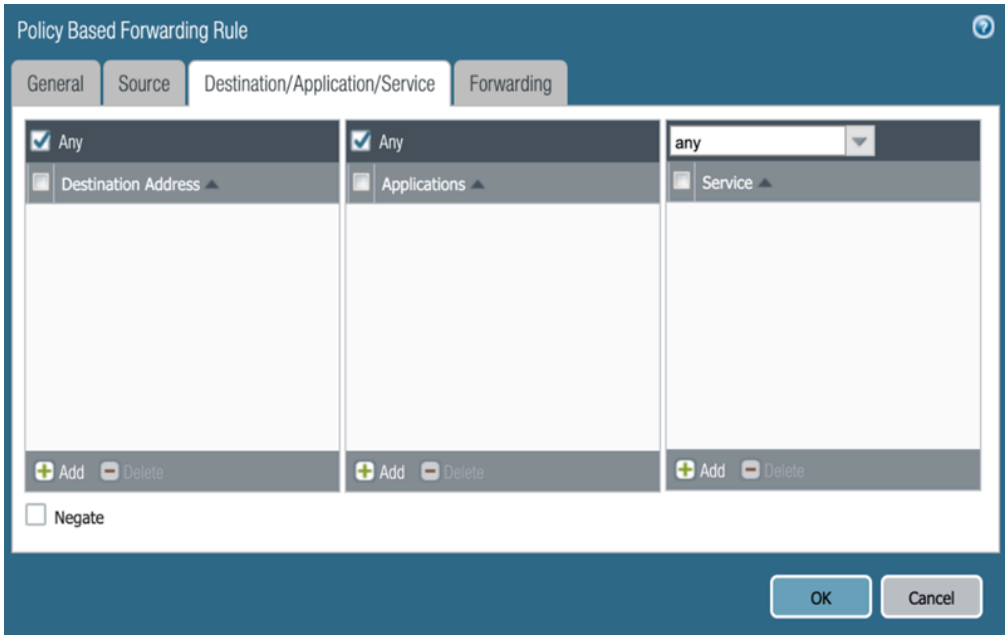
2. [送信元] を選択し、PBF に使用する 送信元アドレスを追加します 。

   この場合、tunnel.1 の PBF を作成するため、192.168.171.0/24 サブネットを入力します。

 ©2025 Palo Alto Networks, Inc.



3. 宛先/アプリケーション/サービス を選択し、 任意 の宛先アドレスと 任意のアプリケーションを選択します。

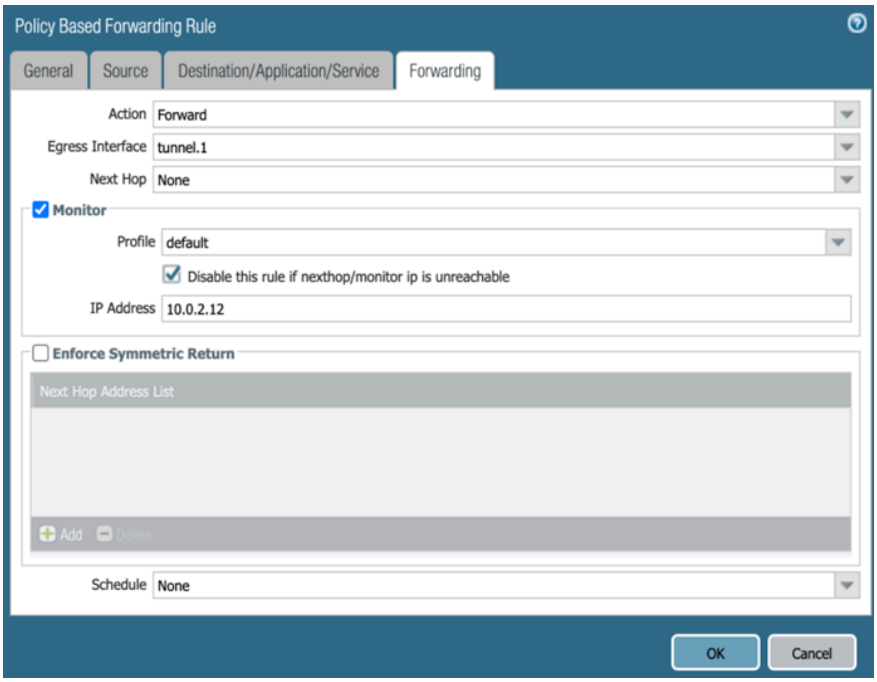


4. **[転送]** を選択し、次のパラメータを指定して、**[OK]**をクリックします。
   - 「転送」の アクション を選択します。
   - IP サブネットを転送するトンネルの 出力インターフェイス を選択します (この場合は**tunnel.1**)。
   - **[Monitor (監視)]** を 選択し、次の監視プロファイルを選択します。
     - デフォルトのプロファイルを選択します。

©2025 Palo Alto Networks, Inc.

- **Disable this rule if nexthop/monitor ip is unreachable** (ネクストホップ/監視 **IP** に到達できない場合にこのルールを無効化)を選択します。
- サービス接続の**[EBGP** ルーター**]**アドレス (**[Panorama]** > **[Cloud Services** (クラウドサービス**)]** > [ステータス] > [ネットワーク詳細] > [サービス接続] > **[EBGP** ルーター**]**) の **IP** アドレス を指定します。

監視を有効にし、サービス接続のEBGPルーター アドレスを選択すると、tunnel.1 がダウンした場合にファイアウォールがPBFポリシーを無効にし、まだ稼働しているトンネル (tunnel.2) にトラフィックをルーティングするようになります。



5. サービス接続1のEBGPルータアドレスをサービス接続2のEBGPルータアドレスに置き換え、tunnel.1のサブネットをtunnel.2のサブネットに置き換えて、ステップ6を繰り返します。

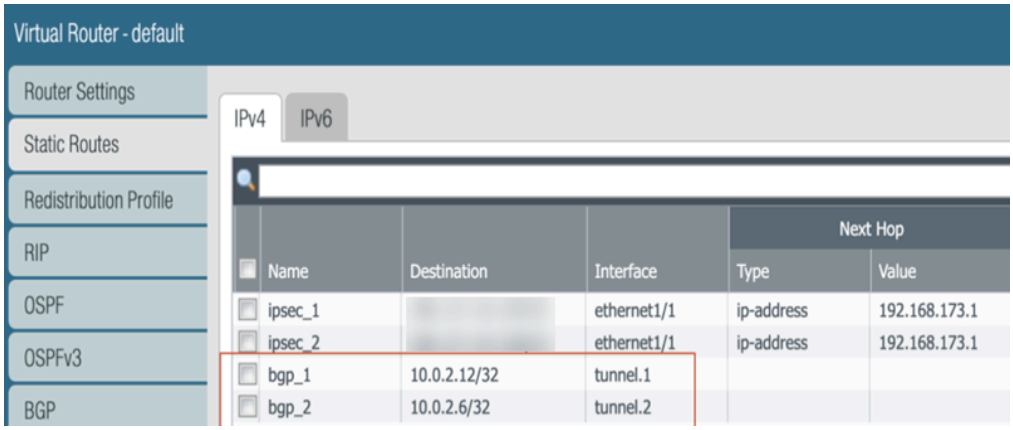
   完了すると、tunnel.1 用と tunnel.2 用の2つのPBFポリシーが作成されます。



 ©2025 Palo Alto Networks, Inc.

STEP 7 | [ネットワーク] > [仮想ルータ] > [スタティック ルート] を選択し、サービス接続1の**[EBGP**ルータ]アドレスを **[tunnel.1]**の[インターフェース] に割り当てます。次に、サービス接続2の**EBGP**ルータアドレスを **tunnel.2**の インターフェース に割り当てます。

各ルータBGPアドレスに特定の静的ルートを入力すると、サービス接続1のEBGPルーターIPアドレスはtunnel.1でのみ到達可能であり、サービス接続2のEBGPルータIPアドレスはtunnel.2でのみ到達可能であるため、トンネル監視が正しく機能することが保証されます。



本社またはデータセンターの場所へのサービス接続を3つ以上設定する

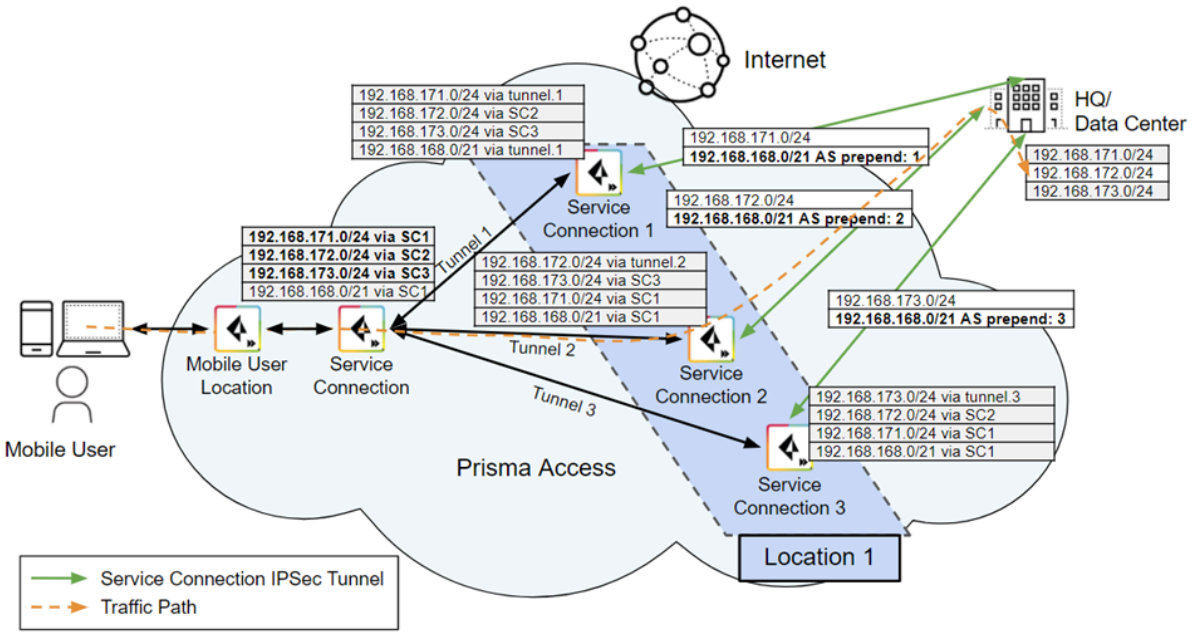
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

高帯域幅のサービス接続に2つのトンネルを使用する場合、トンネルに障害が発生した場合に使用できるトラフィックパスは1つだけになり、フェイルオーバー パスの設定が簡単になります。高帯域幅接続に3つ以上の接続を使用する場合は、トンネルフェールオーバーの一貫した動作を確保するために追加の設定を行う必要があります。

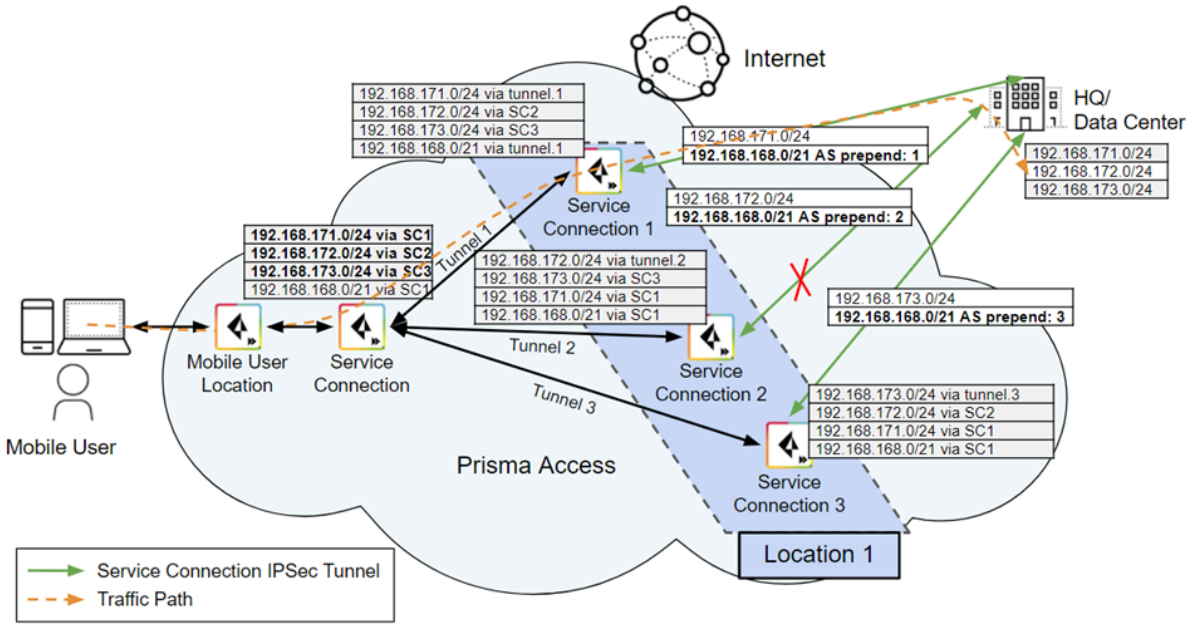
トンネルフェイルオーバーには集約サブネットを使用するため、フェイルオーバーが発生した場合に使用するサービス接続トンネルを明示的に指定する必要があります。BGPルーティングでは、ルートのASパスの数が最も少ないため、フェールオーバーが発生した場合にBGPがトンネルを優先するようにルートの先頭にASパスを追加できます。

次の例は3つのサービス接続を使用する高帯域幅サービス接続のルーティングテーブルを示しています。3つのトンネルがすべて稼働している場合は、Prisma Accessより具体的なルートを使用して本社またはデータセンターのサブネットに到達します。ユーザーは192.168.172.0/24サブネット内のリソースにアクセスしているため、モバイルユーザーに最も近いサービス接続はルーティングテーブルを確認し、データセンターリソースへのパスとしてトンネル2を選択します。

©2025 Palo Alto Networks, Inc.



トンネル2がダウンすると、192.168.172.0/24サブネット内のリソースへのより具体的なルートが使用できなくなるため、ユーザに最も近いサービス接続は、集約された192.168.168.0/21サブネットを使用します。サービス接続1にはAS-PATHプリペンドが1つしか設定されていません。そのため、Prisma AccessはAS-PATHプリペンドの数が少ないため、トンネル1をフェールオーバーパスとして選択します。

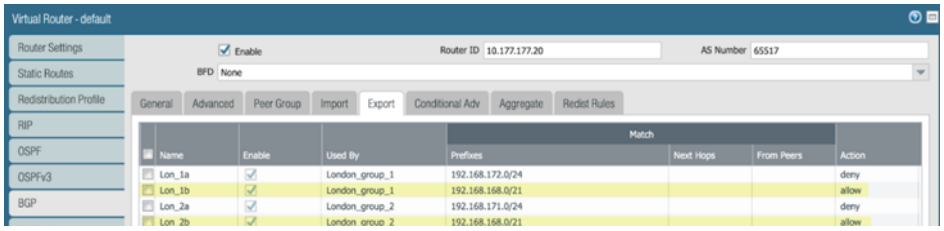


CPEとして次世代ファイアウォールを使用している場合にルートにプリペンドを追加するには、次のタスクを実行します。

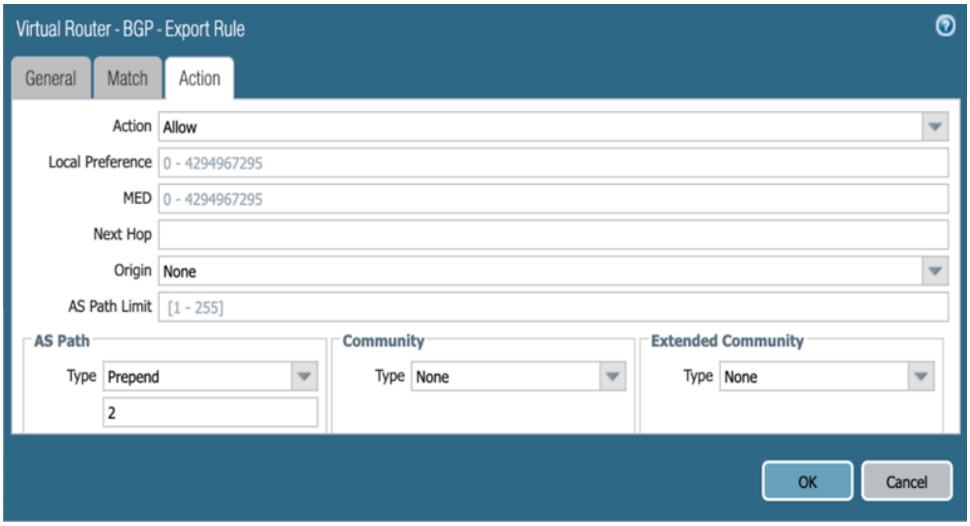
STEP 1 | 仮想ルーターBGPエクスポートプロファイル ([ネットワーク] > [仮想ルーター] > **[BGP]** > [エクスポート]) を選択します。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | **Action (アクション)** が **Allow (許可)** のサービス接続を設定したときに作成したエクスポートルールを変更します。



STEP 3 | [AS Path (AS経路)]領域にプリペンドを追加し、追加する AS-PATH プリペンドの数（この例では**2**）を入力します。



STEP 4 | 手順2と3を繰り返し、**Action (アクション)** が **Allow (許可)** のエクスポートルールごとに、デプロイメントで計画したフェイルオーバーシナリオに合わせてAS-PATHプリペンドを追加します。

このセクションで使用する例では、サービス接続 1（トンネル1）のデータセンターロケーションへのトンネルのAS-PATH プレペンドを 1、サービス接続 2 に使用されるトンネル（トンネル2）に AS-PATH プリペンドを 2、サービス接続 3（トンネル3）に使用するトンネルに AS-PATH プリペンド3 を追加します。

完了すると、この例ではフェイルオーバーが発生した場合に次のトンネルを使用します。

- トンネル2またはトンネル3がダウンすると、対応するサブネットのトラフィックは、アドバタイズされたAS-PATHが最も短いトンネル1にフェールオーバーします。
- トンネル1がダウンすると、そのサブネット（192.168.171.0/24）のトラフィックは、アドバタイズされたAS-PATHが最も短いトンネル2にフェールオーバーします。

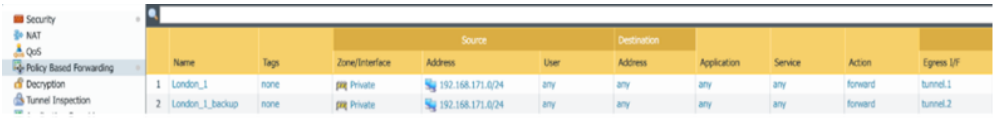
STEP 5 | バックアップPBFまたはポリシーベースのルーティングポリシーを追加して、トンネルに障害が発生した場合のリターントラフィックが対称になるようにします。

AS-PATH プリペンドは、フェイルオーバー時にPrisma Accessからデータセンターへのトラフィックが特定のトンネルを使用することを保証するが、データセンターからPrisma Accessへのトラフィックの対称リターンパスも保証する必要があります。対称リターンを確保するには、Prisma Accessからデータセンターへのトラフィック用に作成したフェイルオー

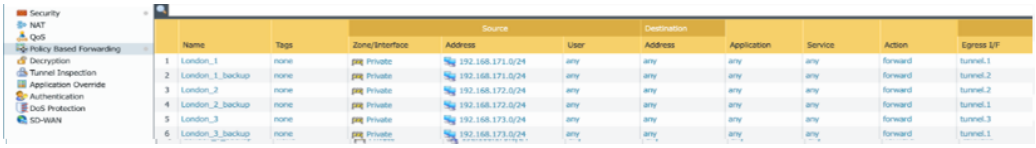
 ©2025 Palo Alto Networks, Inc.

バー シナリオをミラーリングするPBFまたはポリシーベースのルーティング ポリシーを使用する。

この例では、送信元IPが192.168.171.0/24 の トンネル1トラフィックに対して、フェールオーバーが発生した場合にリターントラフィックに トンネル2 を使用するように強制するバックアップPBFポリシーを作成します。トンネルモニターのIPアドレスにアクセスできない場合、最初のPBFルールは無効になります。このフェイルオーバーが発生すると、CPE（この例では次世代ファイアウォール）がリスト内の次のルールを評価します。



次に、Prisma Accessからデータセンターへのトラフィック用に作成したフェイルオーバー シナリオに合わせて、さらにPBFルールを追加します。



送信元NATを使用したサービス接続のユーザーIDとデバイスIDのマッピングを保持する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス ❑ 次世代ファイアウォール（NGFW）で、最小バージョンのPAN-OS 11.2を実行しています。 ❑ この機能はGeneveカプセル化を使用します。NGFW（PAN-OS 11.2以降）に加えて、下流のファイアウォールがGeneveカプセル化をデカプセル化できることを確認してください。 この機能はDynamic Privilege Access (ダイナミック特権アクセス)ではサポートされていません。

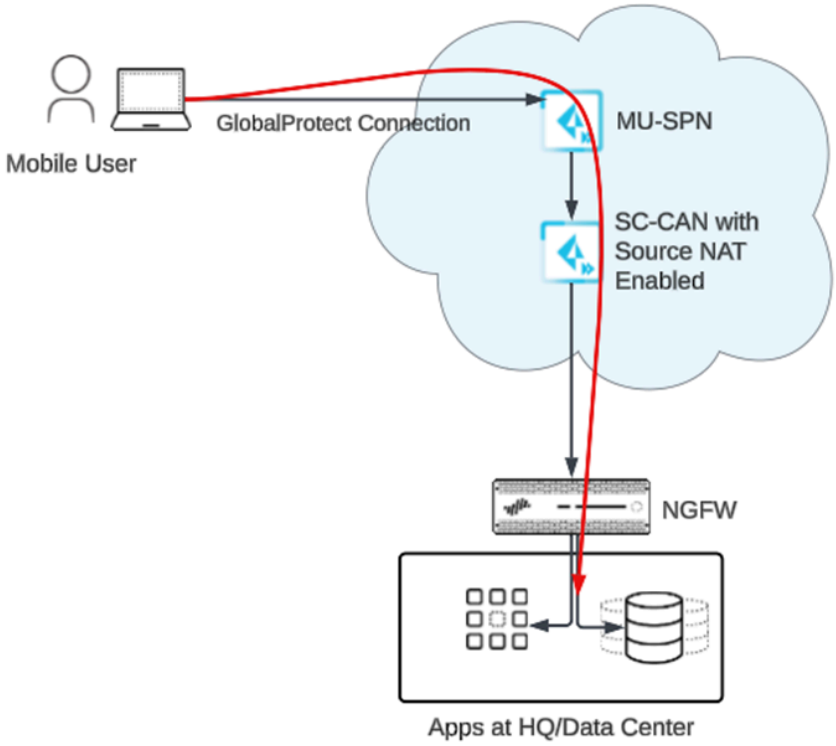
プライベート アプリケーションを保護するには、Prisma Accessでサービス接続(企業アクセス ノード(SC-CAN)とも呼ばれる)を使用します。ユーザーIDまたはデバイスIDに基づいてアプリへのアクセスを制限するには、プライベート アプリケーションが配置されているデータセンターまたは本社に次世代ファイアウォール(NGFW)を導入し、ユーザーIDマッピング、デバイスIDマッピング、またはその両方に基づいてNGFWでポリシー ルールを設定します。

これらのルールを使用するには、NGFWはSC-CANからユーザーID またはデバイスIDのマッピングを受信する必要があります。ただし、ユーザーがGlobalProtectを使用してPrisma Accessに

 ©2025 Palo Alto Networks, Inc.

接続し、SC-CAN でデータ トラフィック送信元**NAT**が有効になっている場合、NGFW はこのマッピングを取得できません。SC-CAN でデータ トラフィック送信元**NAT**が有効になっている場合、モバイル ユーザーIPアドレス プールでNATが実行され、データセンターまたは本社の場所でそれらのIPアドレスはアドバタイズされません。

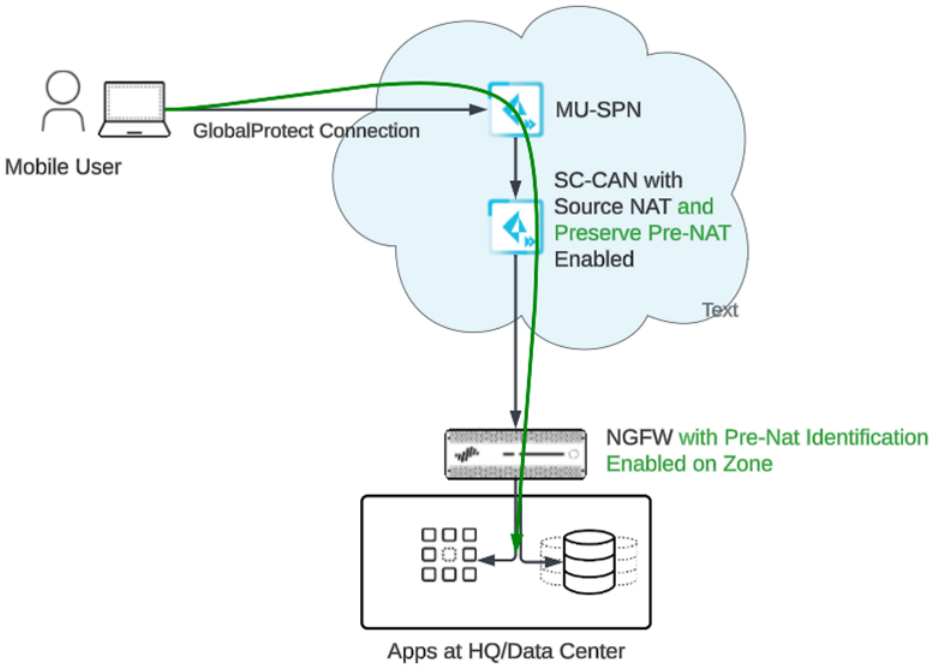
この場合、NGFWはGlobalProtectユーザーのユーザーIDまたはデバイスIDを取得できないため、ユーザーIDまたはデバイスIDに基づいてポリシーを適用することはできません。



ネットワークがユーザーIDまたはデバイスIDのマッピングを本社またはデータセンターに必ず配布するようにするには、以下のセクションのいずれかに記載されている手順を完了します。これにより、NGFWはGlobalProtectから学習したユーザーIDのマッピングに基づいてセキュリティ ポリシー ルールを適用できるようになります。

*NGFW*には、最小*PAN-OS*バージョン*11.2*が必要です。サービス接続は*NGFW*で終了する必要はなく、サービス接続が終了する場所の下流に*NGFW*がある限り、別の*IPSec*対応デバイスで終了することができます。

©2025 Palo Alto Networks, Inc.



- Strata Cloud Manager
- Panorama

送信元NATを使用したサービス接続のユーザーとデバイスIDのマッピングを保持する (Strata Cloud Manager)

Prisma AccessがGlobalProtectユーザーからPrisma Access (Managed by Strata Cloud Manager)にある本社またはデータセンターのNGFWにユーザーIDマッピングを配信するには、以下の手順を実行します。

この手順では、次のネットワーク構成が確立されていることを前提としています。

- サービス接続でデータ トラフィック送信元NATが有効になっています。
- プライベート アプリが配置されている本社またはデータ センターにNGFWを導入しました。
- NGFWで作成したゾーンに基づいて、NGFW上のPrisma Accessのセキュリティ ポリシー ルールを適用しました。

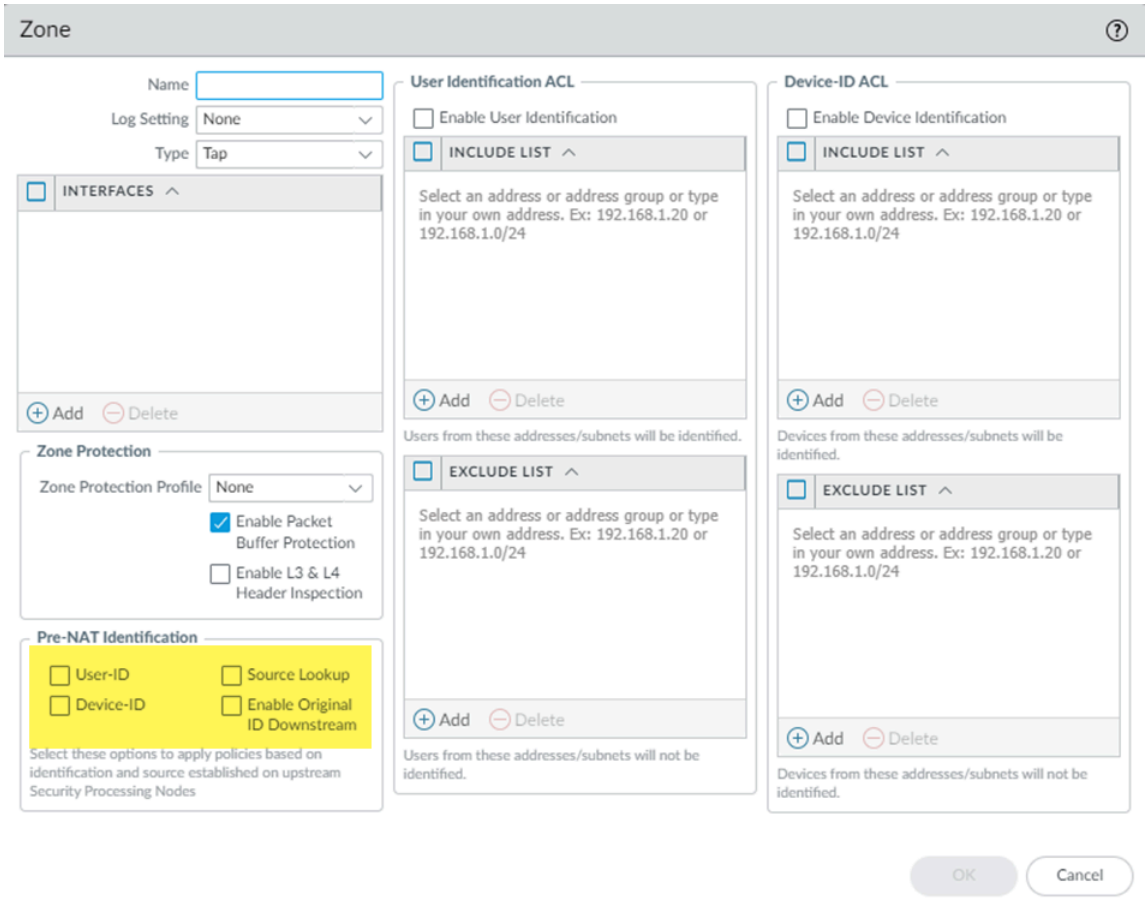
©2025 Palo Alto Networks, Inc.

STEP 1 | NGFWでPre-NAT(NAT 導入前の)識別パラメータを入力します。

1. NGFWにログインするか、NGFWを管理するSCMまたはPanoramaにログインして、[ネットワーク > ゾーン]に移動します。
2. ゾーンを追加するか、既存のゾーンを選択します。
3. 1つ以上の**Pre-NAT(NAT**導入前の)識別パラメータを選択します。
   - ユーザー**ID**- IPアドレスがNATされる前に使用されたモバイル ユーザーのユーザーIDマッピングを保持します。セキュリティ ポリシー ルールでユーザーID を使用している場合は、これを有効にします。
   - デバイス**ID**- IPアドレスがNATされる前に使用されたモバイル ユーザーのデバイスIDマッピングを保持します。セキュリティ ポリシー ルールでデバイスIDを使用している場合は、これを有効にします。
   - 送信元検索- GlobalProtectから受信した元の送信元IPアドレスを照合できます。QoSまたはPolicy-Based Forwarding (ポリシー ベース フォワーディング - PBF)ポリシーで送信元検索を使用している場合、送信元IPの比較はNAT前の送信元IPアドレスに基づいて行われます。たとえば、送信元IPアドレス1.1.1.1と宛先IPアドレスAnyを許可するセキュリティ ポリシーがある場合、1.1.1.1はパケット ヘッダー内のNAT前の送信元IPアドレスと比較されます。
   - 元の**ID**ダウンストリームを有効にする- 2つのNGFWが連続して存在する場合、このオプションを指定すると、最初のNGFWがトラフィックを検査してポリシーを適用

 ©2025 Palo Alto Networks, Inc.

した後、最初のNGFWが2番目のNGFWにNAT 前の情報を送信します。これはSC-CANのデフォルト設定です。



4. **OK** をクリックし、変更を **Commit (コミット)** します。

STEP 2 | NGFWとのコマンドライン インターフェース(CLI)セッションを作成し、設定モードで次のコマンドを入力します。

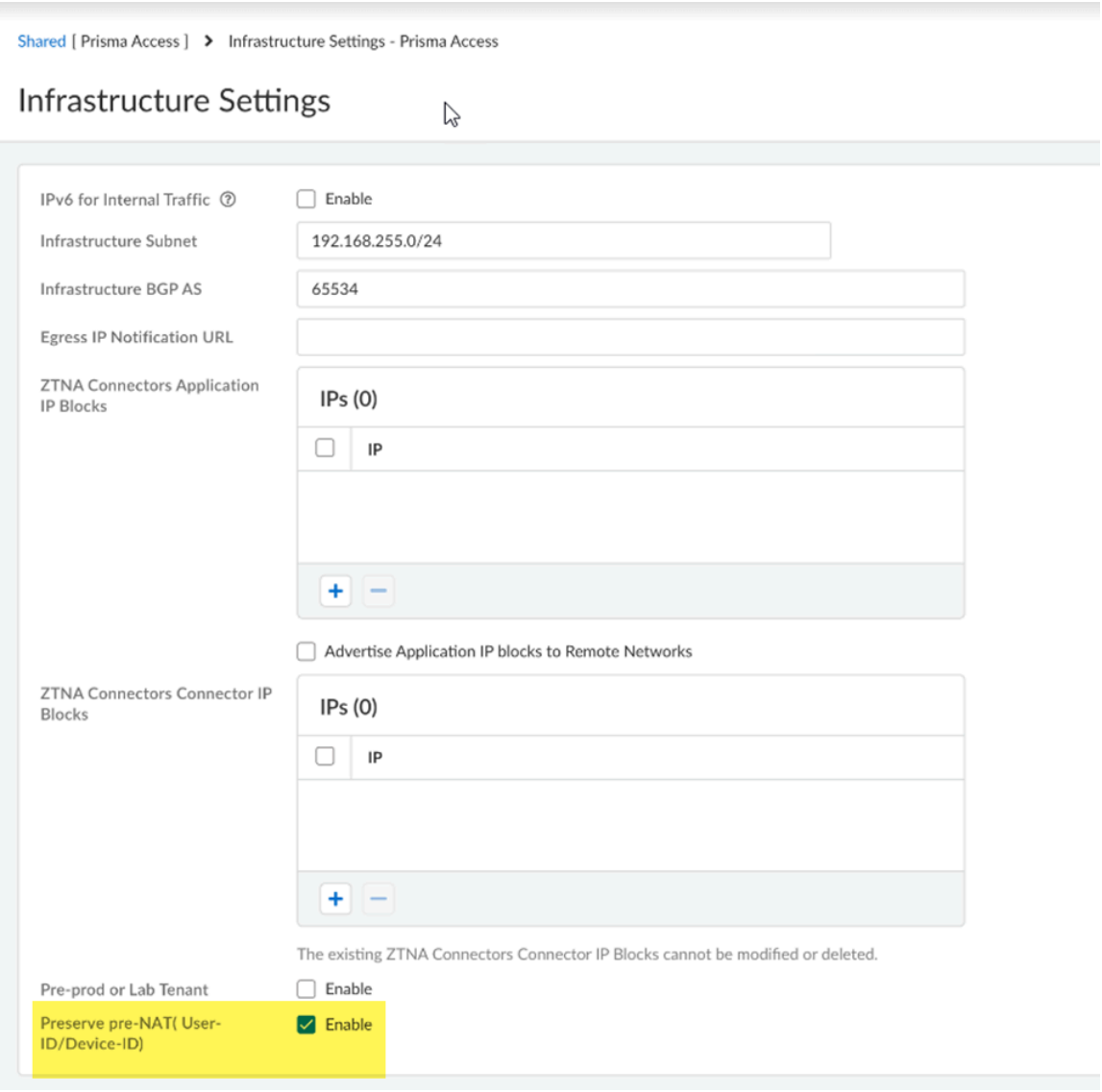
```
set deviceconfig setting preserve-prenat-feature yes
```

将来この機能を無効にする必要がある場合は、`set deviceconfig setting preserve-prenat-feature no` と入力します。

©2025 Palo Alto Networks, Inc.

STEP 3 | Strata Cloud Managerでpre-NAT(NAT導入前の)設定を有効にします。

1. **[Workflows (ワークフロー)]** > **[Prisma Accessセットアップ]** > **[Prisma Access]** > **[インフラストラクチャ設定]**に移動します。
2. **pre-NAT(ユーザーID/デバイスID)**を有効にします。



3. 変更を保存するには、 **[Push Config (設定をプッシュ)]** を実行します 。

送信元NATを使用したサービス接続のユーザーとデバイスIDのマッピングを保持する(Panorama)

Prisma AccessがGlobalProtectユーザーからPrisma Access (Managed by Panorama)にある本社またはデータセンターのNGFWにユーザーIDマッピングを配信するには、以下の手順を実行します。

この手順では、次のネットワーク構成が確立されていることを前提としています。

- サービス接続でデータ トラフィック送信元NATが有効になっています。

©2025 Palo Alto Networks, Inc.

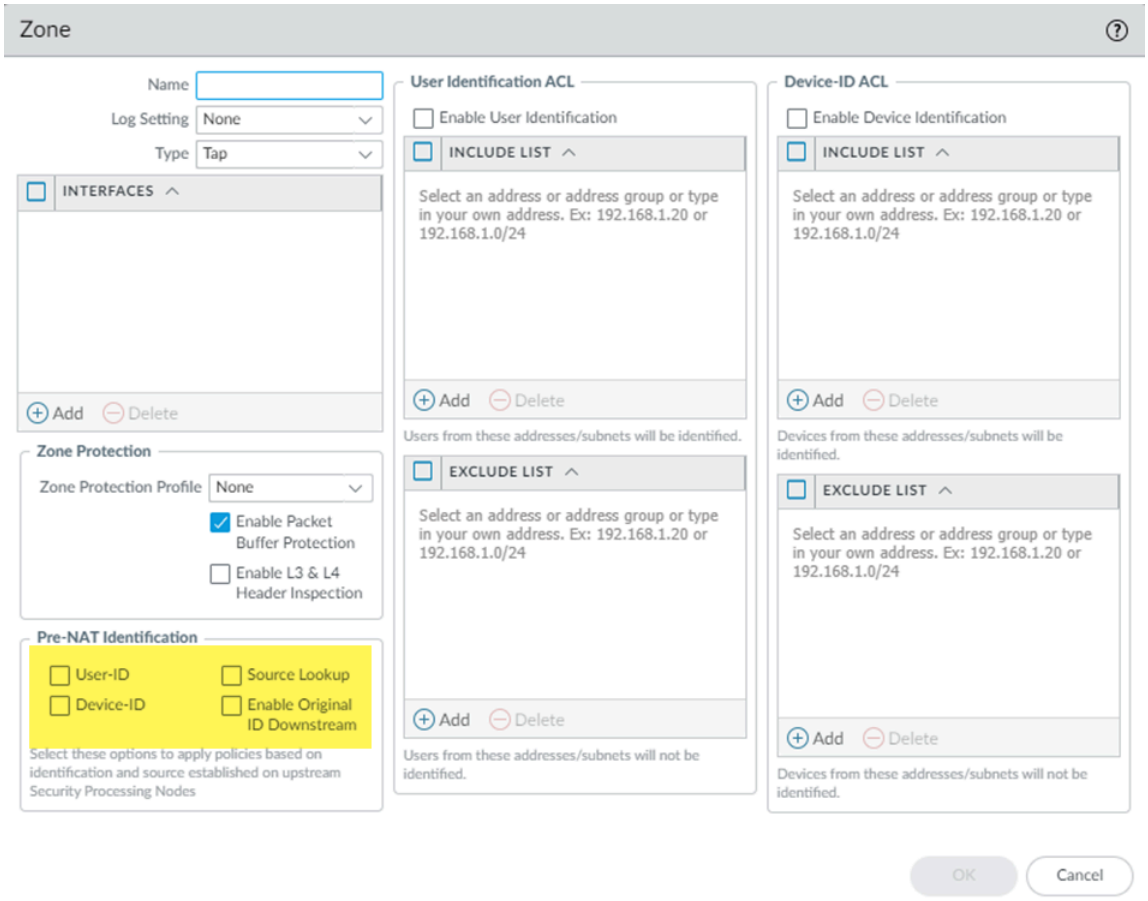
- プライベート アプリが配置されている本社またはデータ センターにNGFWを導入しました。
- NGFWで作成したゾーンに基づいて、NGFW上のPrisma Accessのセキュリティ ポリシー ルールを適用しました。

STEP 1 | NGFWでPre-NAT(NAT 導入前の)識別パラメータを入力します。

1. NGFWにログインするか、NGFWを管理するSCMまたはPanoramaにログインして、[ネットワーク > ゾーン]に移動します。
2. ゾーンを追加するか、既存のゾーンを選択します。
3. 1つ以上の**Pre-NAT(NAT**導入前の**)**識別パラメータを選択します。
   - ユーザー**ID**- IPアドレスがNATされる前に使用されたモバイル ユーザーのユーザーIDマッピングを保持します。セキュリティ ポリシー ルールでユーザーID を使用している場合は、これを有効にします。
   - デバイス**ID**- IPアドレスがNATされる前に使用されたモバイル ユーザーのデバイスIDマッピングを保持します。セキュリティ ポリシー ルールでデバイスIDを使用している場合は、これを有効にします。
   - 送信元検索- GlobalProtectから受信した元の送信元IPアドレスを照合できます。QoSまたはPolicy-Based Forwarding (ポリシー ベース フォワーディング - PBF)ポリシーで送信元検索を使用している場合、送信元IPの比較はNAT前の送信元IPアドレスに基づいて行われます。たとえば、送信元IPアドレス1.1.1.1と宛先IPアドレスAnyを許可するセキュリティ ポリシーがある場合、1.1.1.1はパケット ヘッダー内のNAT前の送信元IPアドレスと比較されます。
   - 元の**ID**ダウンストリームを有効にする- 2つのNGFWが連続して存在する場合、このオプションを指定すると、最初のNGFWがトラフィックを検査してポリシーを適用

 ©2025 Palo Alto Networks, Inc.

した後、最初のNGFWが2番目のNGFWにNAT 前の情報を送信します。これはSC-CANのデフォルト設定です。



4. **OK** をクリックし、変更を **Commit (コミット)** します。

STEP 2 | NGFWとのコマンドライン インターフェース(CLI)セッションを作成し、設定モードで次のコマンドを入力します。

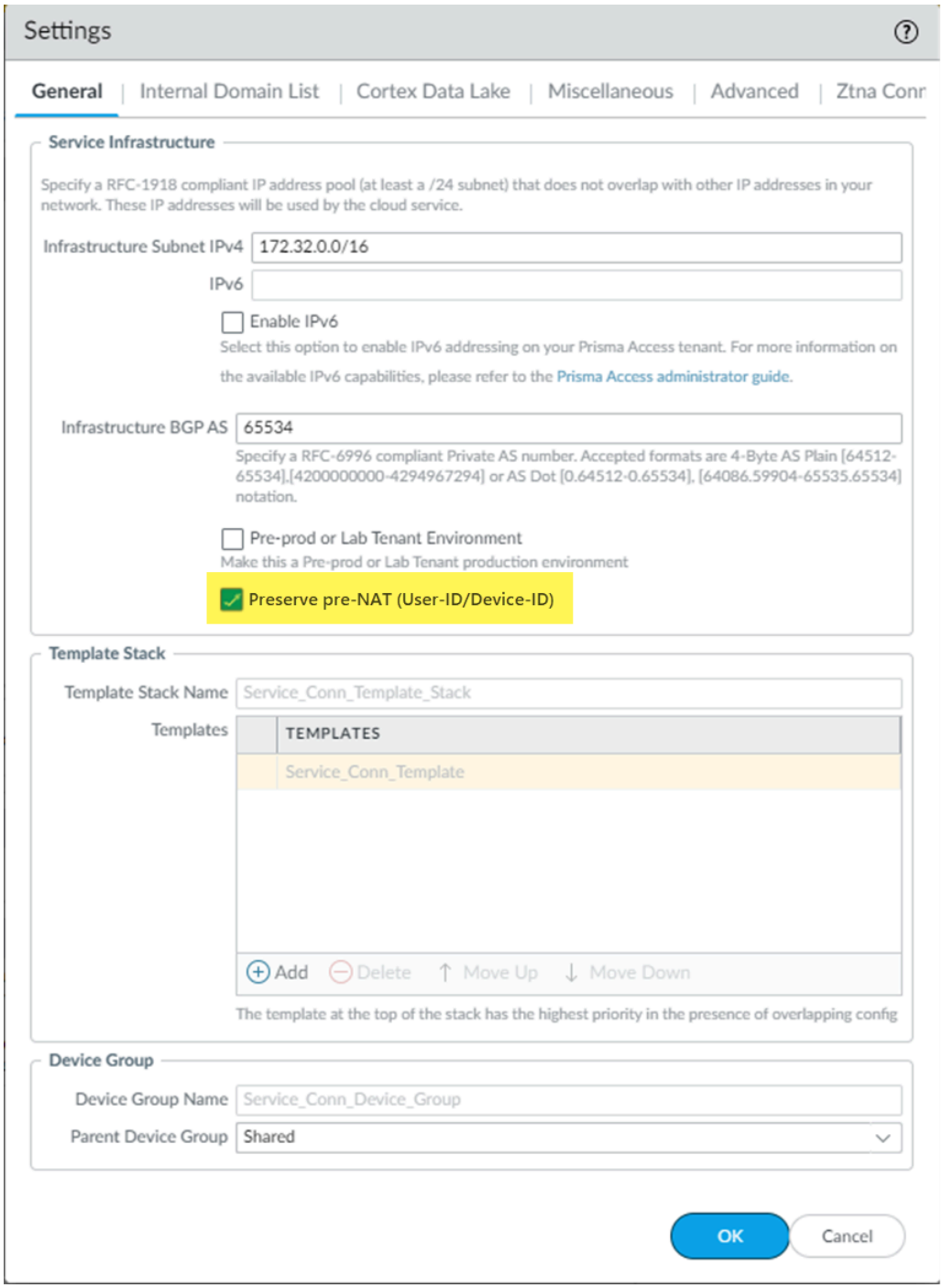
```
set deviceconfig setting preserve-prenat-feature yes
```

将来この機能を無効にする必要がある場合は、`set deviceconfig setting preserve-prenat-feature no` と入力します。

©2025 Palo Alto Networks, Inc.

STEP 3 | Prisma Accessを管理するPanoramaから、pre-NAT設定を有効にします。

1. **[Panorama] > [Cloud Services**（クラウドサービス）**] > [Configuration**（設定）**] > [Service Setup**（サービスのセットアップ）**]**の順に移動し、歯車型アイコンをクリックして[設定]を編集します。
2. **pre-NAT(ユーザーID/デバイスID)**を選択します。



3. 変更を **Commit and Push**（コミットしてプッシュ）します。

 ©2025 Palo Alto Networks, Inc.

Prisma Accessモバイルユーザー - GlobalProtect 高度なデプロイメント

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

次のセクションでは、モバイル ユーザー - GlobalProtectデプロイメントで利用できる高度なデプロイメントについて説明します。

- モバイルユーザー向けの動的DNS登録サポート - GlobalProtect
- Prisma Access GlobalProtectのデプロイメントにおける侵害されたデバイスの識別と隔離
- モバイル ユーザーのIPv6トラフィックのシンクホール - GlobalProtectのデプロイメント
- Prisma Accessを使用したHIP情報の再配信
- HIPレポートの表示
- クライアントレスVPNでのGzipエンコーディングのサポート
- Prisma Accessでのトラフィック レプリケーション

Prisma Accessで複数のポータルを構成する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス ❑ 最低限必要なGlobalProtect Clientのバージョン:6.1 (Windows および macOS のみ)

同じPrisma Accessテナント内で、ポート番号に基づいて2つのポータルを構成し、各ポータルが異なる認証 方法をサポートするようにすることができる。この機能を有効にすると、新しいPrisma Accessテナントを作成することなく、モバイル・ユーザをある 認証方法から別の認証方法に移行できる。この構成により、Prisma Accessインスタンスを別途用意することなく、ユーザを徐々にクラウド ベースの認証に移行させることができるため、認証の柔軟性が高まります。

GlobalProtectの複数のポータルによるPrisma Accessでは、同じテナント内の各ポータルに異なるポート番号を使用しようと思います。標準ポート443を使用して最初のGlobalProtectポータルを構成します。複数のポータル機能を有効にすると、Prisma Accessは代替ポート8443を使用して2つ目のGlobalProtectポータルを構成し、1つ目と同じFQDNを使用して2つ目のポータルへの接続を許可する。複数ポータル機能では、FQDNごとに2つのポータルのみがサポートされます。

ユーザーがポート443を使用してポータルに接続すると、トラフィックはIPアドレスを変更せずに最初の認証ポータルに送信されます。このフローは、GlobalProtect複数ポータル機能のな

©2025 Palo Alto Networks, Inc.

い構成から変更されていません。ユーザーがポート8443を使用して接続すると、トラフィックは宛先NATルールにヒットします。これにより、ユーザーは別のIPアドレスにある2番目の認証ポータルに移動します。いずれかのポータルで認証した後、ユーザーは認証オーバーライドCookieとともにゲートウェイに転送されます。この機能は認証オーバーライドCookie設定に依存し、ポータルとゲートウェイの両方で有効になります。

次の表は、プライマリ ポータルで従来の認証 (RADIUSやLDAPなど) を使用し、セカンダリ ポータルでクラウド認証 (SAMLやCASを使用したSAMLなど) を使用する認証方法と証明書の組み合わせによるGlobalProtect複数ポータルのサポートを示しています。

プライマリポータルのユーザー認証	セカンダリポータルユーザー認証	接続方法オプション
レガシー、証明書なし	クラウド、証明書なし	ユーザー ログオン (常時、オンデマンド)
レガシー、<auth profile selection>クライアント証明書 注:証明書プロファイルは同じである必要があります。	クラウド、 <auth profile selection>クライアント証明書 注:証明書プロファイルは同じである必要があります。	ユーザー ログオン (常時、オンデマンド) プレ ログオン（常時オン、オンデマンド）
レガシー、証明書なし	クラウド、OR クライアント証明書	ユーザー ログオン (常時、オンデマンド)
レガシー、<auth profile selection>OR クライアント証明書 複数のポータル構成では、認証にクライアント証明書のみを使用するクライアントはサポートされません。	クラウド、証明書なし	ユーザー ログオン (常時、オンデマンド) プレ ログオン（常時、オンデマンド）、証明書の場合
レガシー、<auth profile selection>OR クライアント証明書 複数のポータル構成では、認証にクライアント証明書のみを使用するクライアントはサポートされません。	クラウド、OR クライアント証明書 複数のポータル構成では、認証にクライアント証明書のみを使用するクライアントはサポートされません。	ユーザー ログオン (常時、オンデマンド) プレ ログオン（常時、オンデマンド）、証明書の場合

複数のポータルを構成する前に、次の点を確認してください。

- 両方のポータルに同じ証明書プロファイルがあるか、証明書プロファイルがありません
- 認証プロファイルに関連付けられた許可リストは同じである必要があります

©2025 Palo Alto Networks, Inc.

- ポータルで認証オーバーライドのCookieを受け入れる場合、ポータルとゲートウェイの両方でCookieの有効期間が同じであることを確認してください。
- 複数のポータル構成では、クライアント証明書ベースの認証のみの使用はサポートされません。

> クライアントレスVPNは 、複数ポータルデプロイメントのセカンダリ ポータルでの使用はサポートされていません。ただし、クライアントレス*VPN*は、既存の認証方法を使用してプライマリ ポータルで機能します。

- Strata Cloud Manager
- Panorama

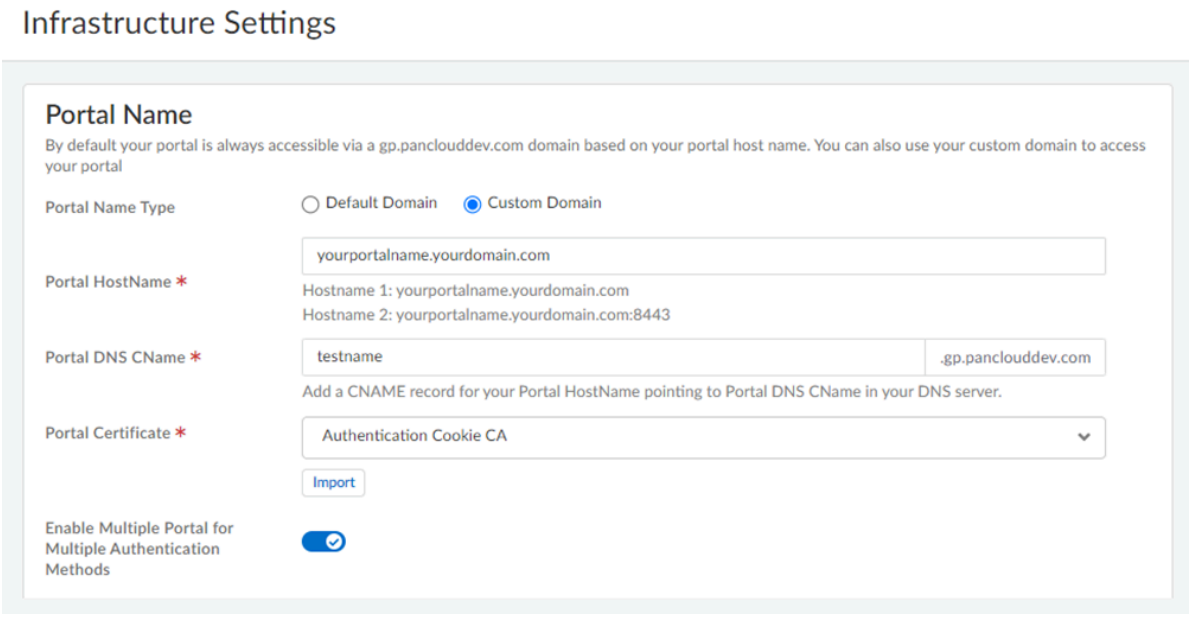
Prisma Accessで複数のポータルを構成する （Strata Cloud Manager）

STEP 1 | この機能を有効にするには、Palo Alto Networksサポートにお問い合わせください。

STEP 2 | モバイル ユーザーとその認証方法を構成します。

STEP 3 | 同じゲートウェイに対して複数のポータルを有効にします。

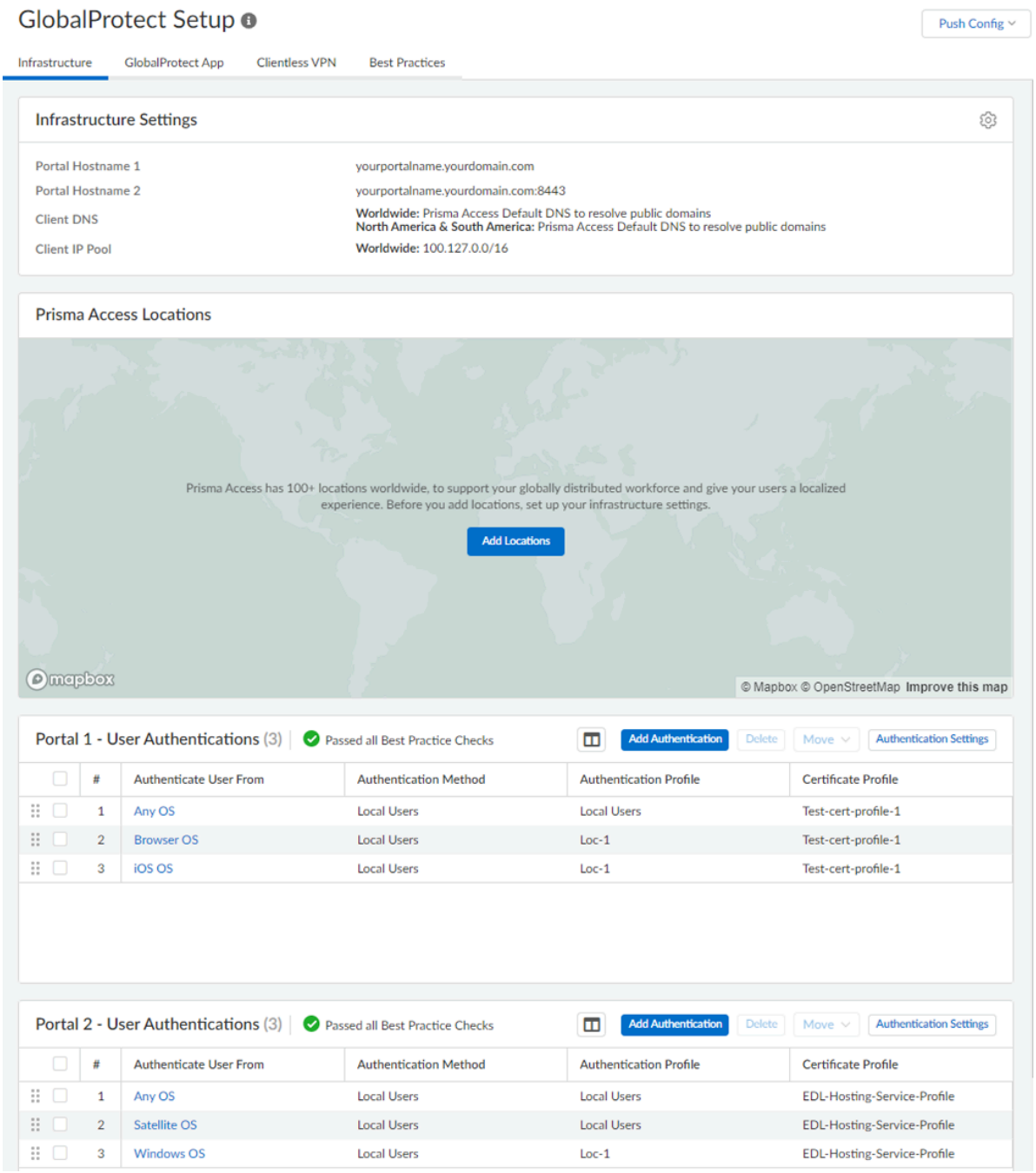
1. **[Workflows (ワークフロー)] > [Prisma Access Setup (セットアップ)] > [GlobalProtect] > [GlobalProtect Setup (GlobalProtect セットアップ)] > [Infrastructure (インフラストラクチャ)]**選択します。
2. インフラストラクチャ設定を編集します 。
3. 複数の認証方法に対して複数のポータルを有効にします。



同じテナントの 8443 ポートに新しいポータルが表示されます。このポータルは、元のポート (ポート 443) から構成設定を継承します。

 ©2025 Palo Alto Networks, Inc.

STEP 4 | ポータル構成を編集して認証設定を更新します。

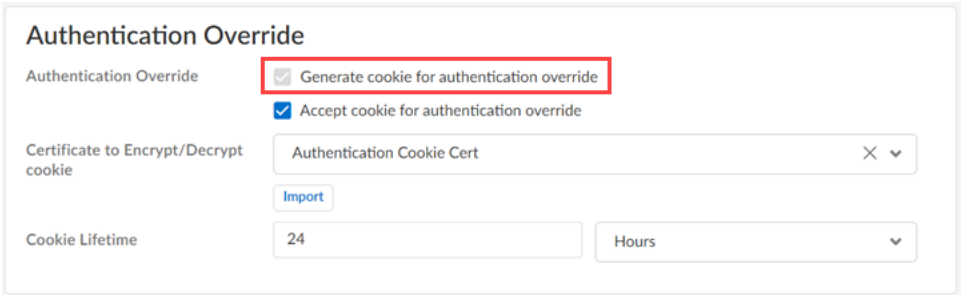


ポータルの認証設定と証明書プロファイルの認証設定のみを編集できます。

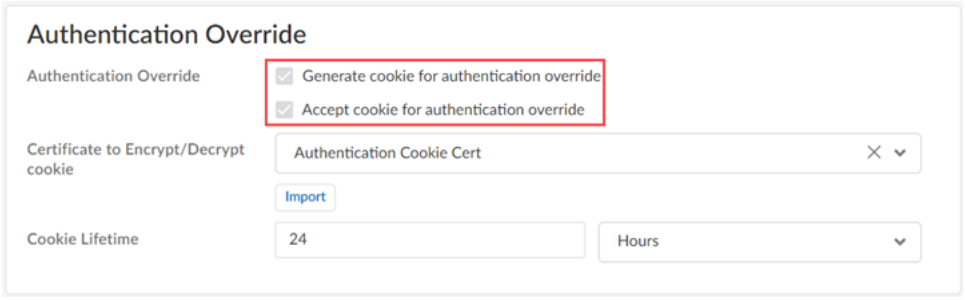
両方のポータルで証明書ベースの認証を使用する場合は、両方のポータルが認証に同じクライアント証明書プロファイルを使用していることを確認してください。

この機能により、認証オーバーライド設定が有効になり、GlobalProtectアプリケーション設定の両方のポータルに対してCookieが生成されます。

©2025 Palo Alto Networks, Inc.



この機能により、認証オーバーライド設定が有効になり、トンネル設定の両方のポータルに対してCookieを生成して受け入れることができます。



STEP 5 | すべての変更を保存し、設定の変更をPrisma Accessにプッシュします。

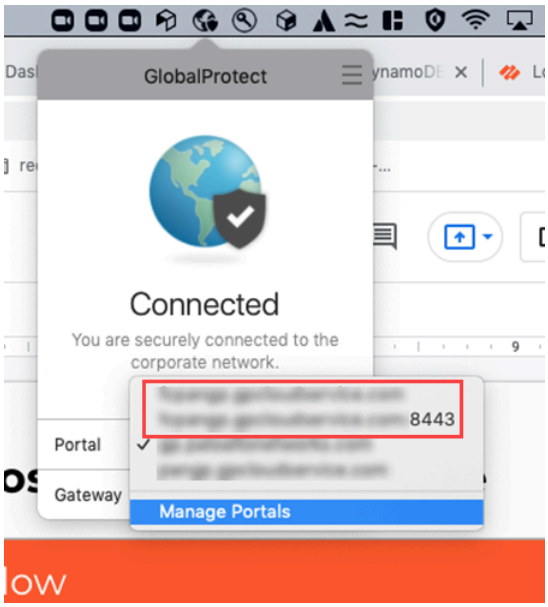
STEP 6 | ポータルを手動で追加するか、GlobalProtectアプリケーションのエンドポイント管理ソフトウェアを使用して追加します。

 ©2025 Palo Alto Networks, Inc.

STEP 7 | ゲートウェイの異なる認証プロファイルを使用して両方のポータルに接続できるかどうかを確認します。

1. Windowsマシンにログインします。
2. GlobalProtectアプリケーションのポータルに接続します。

   異なる認証方式のポータル間の接続を変更する場合は、ユーザーログインを認証します。



   8443 ポータルに接続して手動ゲートウェイに切り替えるときに認証 *Cookie* の有効期限が切れると、*GlobalProtect* は利用可能な最適なゲートウェイに接続します。

   *GlobalProtect*アプリケーションがキャッシュされたポータル構成を使用する場合、ポータルへのフォールバックは機能しません。

セカンダリ ポータルにSAML ベースの認証を使用している場合は、統合時に次の値を入力します。

- シングルサインオン*URL:**https://Portal-FQDN:443/SAML20/SP/ACS***と入力します。

  Portal-FQDN は、 *Prisma Access* ポータル

  セカンダリ ポータル *(8443)* を設定している場合でも、ポータル ***443*** を使用します。
- オーディエンス *URI (SP* エンティティ *ID):**https://Portal-FQDN:443/SAML20/SP***を入力します

Prisma Accessで複数のポータルを構成する （Panorama）

©2025 Palo Alto Networks, Inc.

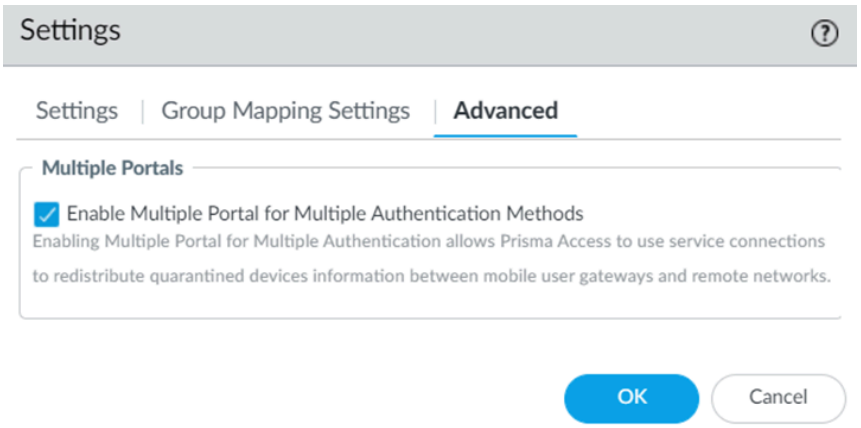
STEP 1 | この機能を有効にするには、Palo Alto Networksのアカウント担当者にお問い合わせください。

> トラフィックステアリングを使用して複数の*GlobalProtect*ポータルを構成する場合は、サービス接続上のデフォルトルートを受け入れるを構成しないでください。 ***(Panorama** > **Cloud Services** (クラウドサービス) > **[Configuration** (構成)] > **[Traffic Steering** (トラフィック ステアリング)] > **[Settings** (設定)] > **[Accept Default Route over Service Connection** (サービス接続経由のデフォルト ルートを受け入れる)])*;これを行うと、モバイル ユーザーはセカンダリ ポータルに接続できません。

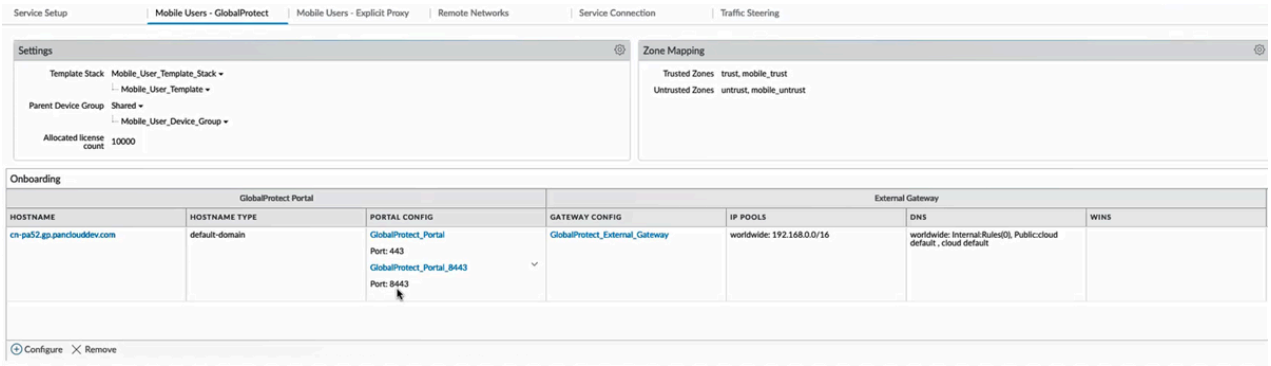
STEP 2 | モバイル ユーザーとその認証方法を設定します。

STEP 3 | **[Cloud Services** (クラウド サービス)] > **[Configuration** (構成)] > [モバイル ユーザー - **GlobalProtect]** > **[Settings** (設定)] > **[Advanced** (詳細設定)]を選択します。

STEP 4 | 複数の認証方法に対して複数のポータルを有効にします。



同じテナントの 8443 ポートに新しいポータルが表示されます。このポータルは、元のポート (ポート 443) から構成設定を継承します。



 ©2025 Palo Alto Networks, Inc.

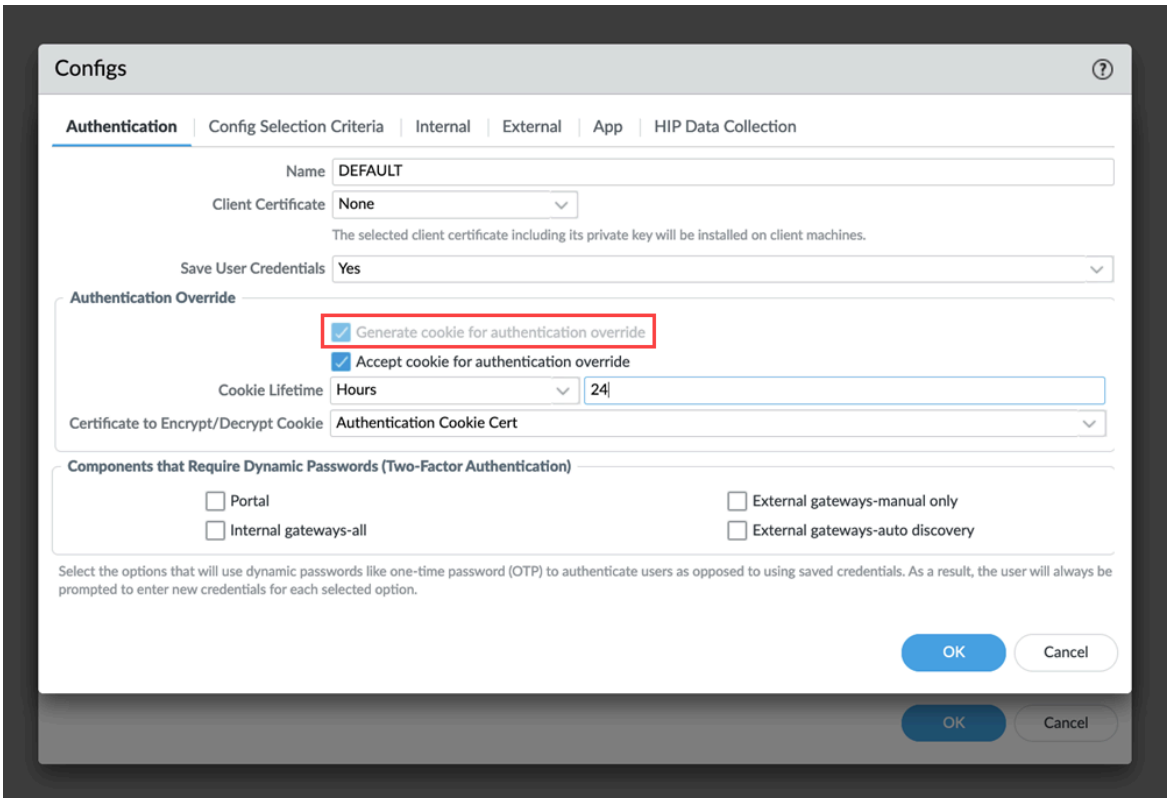
STEP 5 | ポータル構成を編集して認証設定を更新します。

1. ポータルのハイパーリンクをクリックするか、 **[Panorama]** > **[テンプレート]** > **[ネットワーク]** > **[GlobalProtect]** > **[ポータル]** をクリックし、ポータルのハイパーリンクをクリックします。
2. **Authentication (認証)** セクションで、異なる認証プロファイルでクライアント認証を追加します。

編集できるのは、クライアント認証と証明書プロファイル認証の設定のみです。

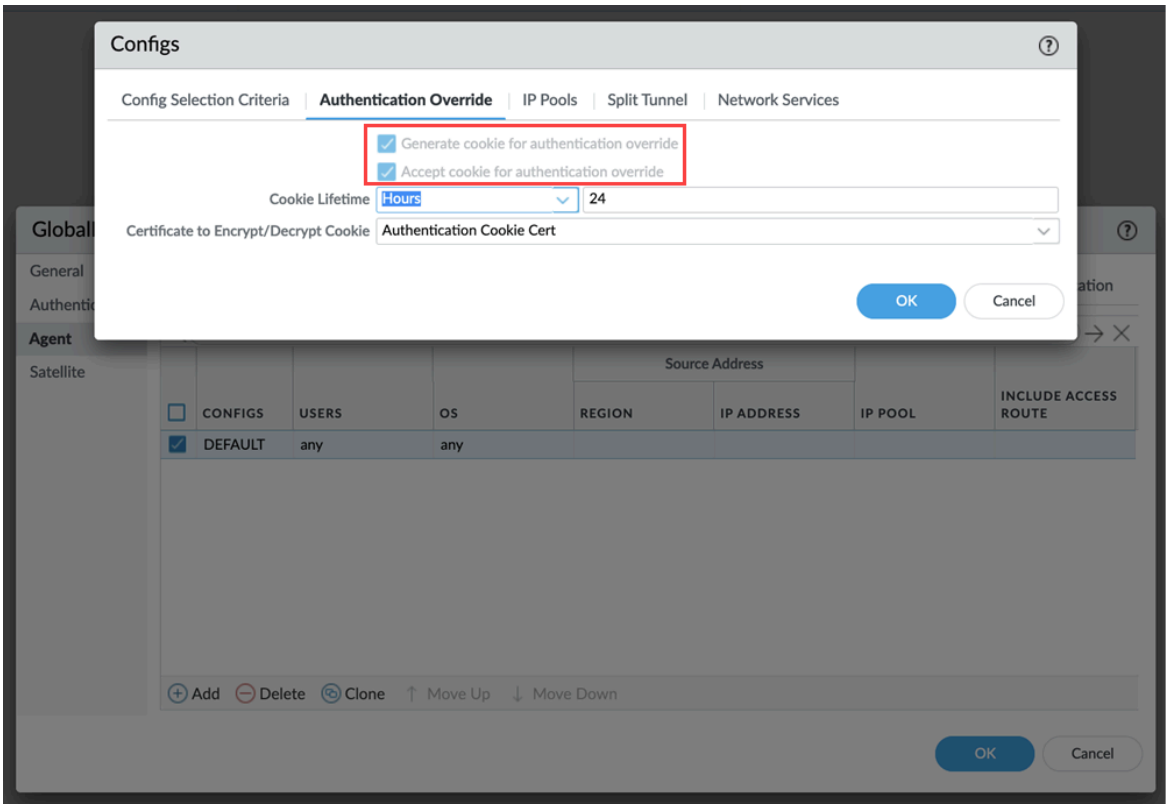
両方のポータルで証明書ベースの認証を使用する場合は、ゲートウェイに証明書ベースの認証がないことを確認してください。

この機能により、認証オーバーライド設定が有効になり、GlobalProtectアプリケーション設定の両方のポータルに対してCookieが生成されます。



この機能により、認証オーバーライド設定が有効になり、トンネル設定の両方のポータルに対してCookieを生成して受け入れることができます。

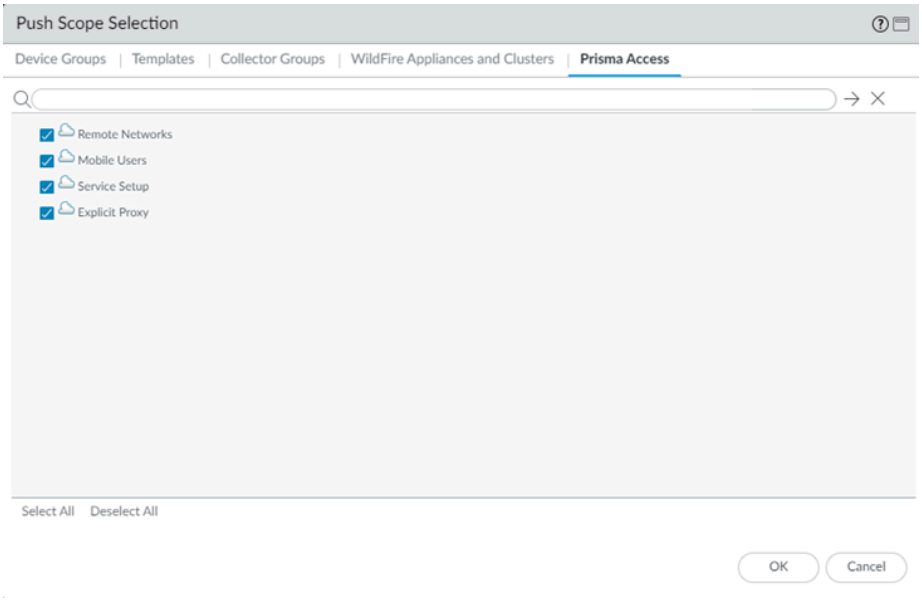
©2025 Palo Alto Networks, Inc.



©2025 Palo Alto Networks, Inc.

STEP 6 | Panorama にすべての変更をコミットし、その設定変更をPrisma Accessにプッシュします。

1. **Commit**（コミット） > **Commit and Push**（コミットしてプッシュ）をクリックします。
2. [選択内容を編集]をクリックし、**[Prisma Access]**タブで**[Push Scope (**スコープをプッシュ**)]**に**[Mobile Users (**モバイルユーザー**)]**が選択されていることを確認し、**[OK]**をクリックする。



3. **[Commit and Push (**コミットしてプッシュ**)]** をクリックします。

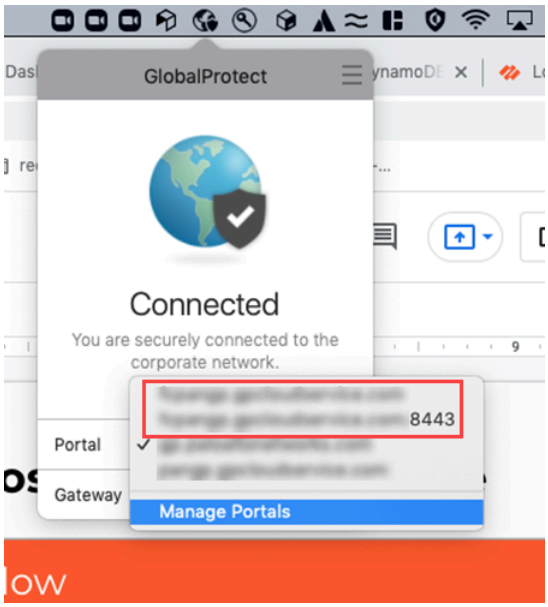
STEP 7 | ポータルを手動で追加するか、GlobalProtectアプリケーションのエンドポイント管理ソフトウェアを使用して追加します。

©2025 Palo Alto Networks, Inc.

STEP 8 | ゲートウェイの異なる認証プロファイルを使用して両方のポータルに接続できるかどうかを確認します。

1. Windowsマシンにログインします。
2. GlobalProtectアプリケーションのポータルに接続します。

   異なる認証方式のポータル間の接続を変更する場合は、ユーザーログインを認証します。



   8443 ポータルに接続して手動ゲートウェイに切り替えるときに認証 *Cookie* の有効期限が切れると、*GlobalProtect* は利用可能な最適なゲートウェイに接続します。

   *GlobalProtect*アプリケーションがキャッシュされたポータル構成を使用する場合、ポータルへのフォールバックは機能しません。

3. **[モニター] > [ログ] > [GlobalProtect]**をクリックして、両方のポータルのログを表示し、ポータルと認証情報を確認します。

セカンダリ ポータルにSAML ベースの認証を使用している場合は、統合時に次の値を入力します。

- シングルサインオン*URL:**https://Portal-FQDN:443/SAML20/SP/ACS***と入力します。

  Portal-FQDN は、 *Prisma Access* ポータル

  セカンダリ ポータル *(8443)* を設定している場合でも、ポータル ***443*** を使用します。

- オーディエンス *URI (SP* エンティティ *ID):**https://Portal-FQDN:443/SAML20/SP***を入力します

©2025 Palo Alto Networks, Inc.

リモートトラブルシューティングとアップデートのためのダイナミックDNS登録サポート

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access ライセンス（モバイル ユーザーを含む）—GlobalProtect ❑ 最低限必要なPrisma Accessバージョン:5.1 イノベーション (PAN-OSデータプレーンの最小バージョン11.2が必要)

モバイルユーザーがGlobalProtectエージェントを使用してPrisma Accessにリモート接続すると、GlobalProtectゲートウェイはユーザーにIPアドレスとエンドポイントFQDNを割り当てます。しかし、 Prisma Accessはこの情報を使用してエンタープライズ内のDNSサーバーを更新しません。DNSサーバーにはモバイル ユーザーに割り当てられたIPアドレスとFQDN情報がないため、IT管理者とネットワーク内のアプリはFQDNを使用してリモート エンドポイントを識別および更新できません。

動的DNS登録を使用すると、Prisma AccessをIPアドレス管理（IPAM）ベンダーと統合して、nsupdateを使用しDNSサーバーにAレコードとPTRレコードを動的に作成することができます。これには次のような利点があります。

- InfoBlox、BlueCat、Windowsなどの主要なIPAMベンダーとの直接統合。
- DDNS更新は、トランザクション シグネチャ (TSIG) またはKerberosのいずれかを認証プロトコルとして使用して実行され、DNSデータベースへの安全な更新が保証されます。
- リアルタイムのDDNS更新は、GlobalProtectの接続および切断イベントに基づいてバッチ化されたnsupdateコールを使用して、Prisma AccessからDNSサーバーに行われます。これらの更新では、モバイル ユーザー セキュリティ処理ノード (MU-SPN) 上のDDNSサービスが使用されます。

このソリューションを設定したら、次のアクションを実行できます。

- Microsoft Endpoint Configuration Manager (MECM) などのソフトウェア ツールを使用して、ソフトウェア更新プログラムを GlobalProtect エンドポイントにプッシュできます。
- ITおよびヘルプデスクのスタッフは、デバイスのFQDNを使用してGlobalProtectエンドポイントに接続し、管理できます。
- 承認されたGlobalProtectエンドポイントからのアクセスを許可するために、DNS逆引き検索を利用する顧客アプリケーション (銀行アプリケーションなど) を実装できます。

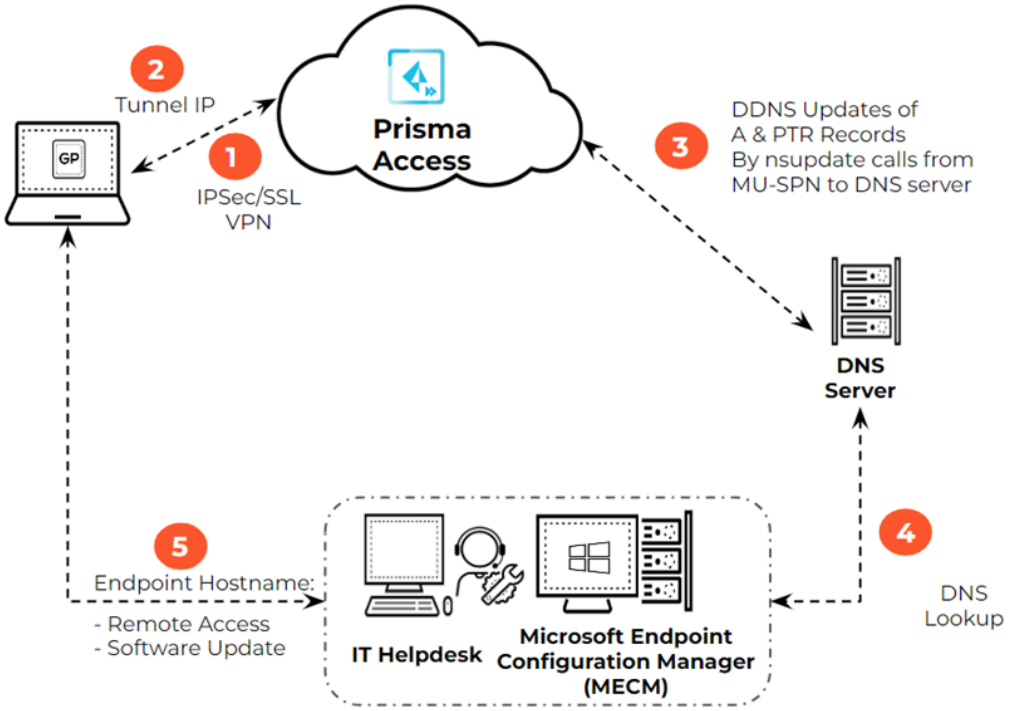
このDDNSソリューションは、*Strata Logging Service*を使用して*DDNS*更新をサーバーにプッシュする、モバイルユーザー向け動的DNS登録サポート - GlobalProtectソリューションとは互換性がありません。*Strata Logging Service*を使用した既存のソリューションを実装し、このソリューションをデプロイすると、*Prisma Access*はこのソ リューションを使用し、*Strata Logging Service*を使用した既存のソリューションを無効にします。

©2025 Palo Alto Networks, Inc.

動的DNS登録サポートのユースケース

次の図は、Prisma AccessDDNSソリューションの典型的な使用例を示したものです。この例では、MECM を使用して GlobalProtectエンドポイントを更新したり、ITヘルプ デスクがトラブルシューティングのためにGlobalProtectエンドポイントにリモートでログインできるようにしたりします。

1. GlobalProtectは、GlobalProtectエンドポイントとPrisma Accessゲートウェイの間にSSLトンネ ルを確立します。
2. GlobalProtectは、モバイルユーザーデバイスのホスト名、ドメイン名、およびトンネルIPアドレス情報を、トンネルを介してオンプレミスまたはPrisma Accessゲートウェイに送信します。
3. Prisma Accessは、DNS サーバーへの nsupdate を使用して A レコードと PTR レコードの DDNS 更新を提供します。 Prisma Accessは、 ログインおよびログアウト イベントを処理するときに、これらの安全な更新をリアルタイムで提供します。
4. IT管理者またはエンタープライズ ソフトウェアは、DNSまたはRDNS検索を通じてこれらのレコードを使用し、エンドポイント名またはIPアドレスを解決します。
5. IT管理者またはエンドポイント管理ソフトウェアは、この情報を使用してエンドポイントを管理したり、ソフトウェアの更新をプッシュしたりします。



ネットワーク接続要件

このソリューションを実装する前に、ネットワークに次の要件が満たされていることを確認してください。

©2025 Palo Alto Networks, Inc.

- MU-SPNおよびPrisma Accessサービス接続からDNSサーバーへの接続性を確保するためのルートを追加しました。

  そのためには、Prisma Accessインフラストラクチャサブネットからルートを追加します。**[Workflows (ワークフロー)]** > > **[Prisma Access Setup]** > **[Prisma Access]** > **[Infrastructure Subnet]**および[Mobile Users-GlobalProtect IPアドレスプール]を参照してください。これは、**[Workflows (ワークフロー)]** > **[Prisma Accessセットアップ]** > **[GlobalProtect]** > **[Client IP Pool]**より確認することができます。
- Prisma Access との、DNSサーバに接続可能なIPSec終端デバイス（たとえば、次世代ファイアウォールやルータ）との間にサービス接続を作成することで、接続性を確立しています。
- サービス接続 IPSec トンネル経由で DNS サーバーにアクセスできることを確認しました。
- Prisma AccessMobile Users-GlobalProtectセキュリティ処理ノード（SPN）から送信されたnsupdateコマンドが許可され、DNS サーバに到達できることを確認しました。

  この接続性を達成するために実行する手順は、使用する場所とDNSサーバーのタイプによって異なります。例:

  - DNSサーバーがデータ センター内にある場合は、Mobile Users—GlobalProtect SPNからサービス接続へのIPSecトンネルを使用して接続を設定し、次にサービス接続からDNSサーバーが存在するゲートウェイ ルーター (VMとして構成された次世代ファイアウォールなど) への接続を設定できます。
  - DNSサーバーがクラウド内にある場合は、適切なセキュリティ ポリシー ルールを使用して、モバイル ユーザー - GlobalProtect SPNからDNSサーバーへの接続を実現できます。
- DNSサーバーに前方参照ゾーンと逆引き検索ゾーンを構成しました。
- nsupdateをサポートするInfoblox、Bluecat、またはWindows DNSサーバーを実装しました。
- ゾーンの権限を個別に管理する場合は、正しいTSIGまたはKerberosキーを持つデバイスからのnsupdatesを許可するセキュリティ ポリシー ルールを作成していることを確認してください。

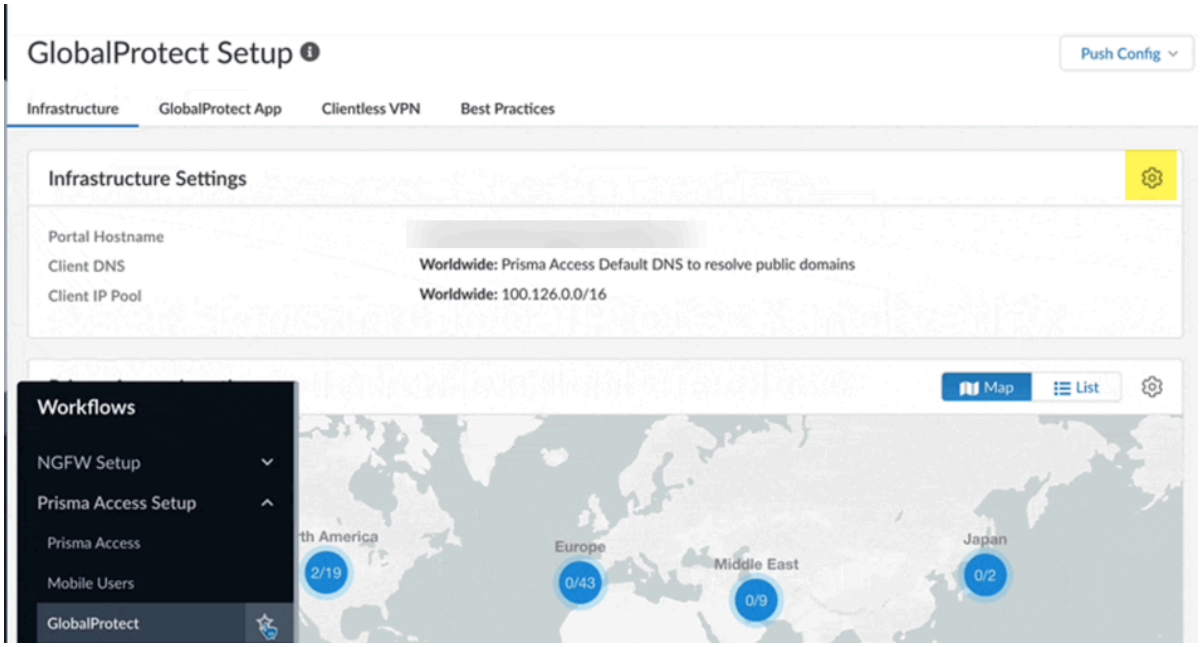
このソリューションを構成するには、デプロイメントの種類に基づいて、次のいずれかの手順を使用します。

- クラウド管理
- Panorama

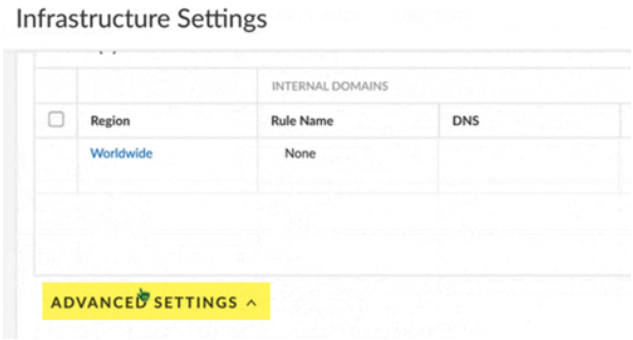
Prisma Access (Managed by Strata Cloud Manager)向けダイナミックDNSアップデートを設定する

 ©2025 Palo Alto Networks, Inc.

STEP 1 | Strata Cloud Managerから、 ワークフロー > **GlobalProtect** に移動し、歯車をクリックしてインフラストラクチャ設定を編集します。



STEP 2 | [詳細設定]を選択します。



STEP 3 | ダイナミック**DNS**サポート 設定を構成します。

1. **GlobalProtect** のダイナミック**DNS**サポートを選択します。
2. ドメインタイプを選択します。

   - フォールバック ドメイン- nsupdate イベントに使用されるドメインは、 フォールバック ドメイン 領域で指定したドメインにフォールバックします。GlobalProtectクライアントがどのドメインにも参加していない場合、またはDDNSサービスがDNSサーバー上のレコードを更新するために使用するのと同じドメインに参加している場合は、この選択肢を使用します。

     フォールバック ドメインを選択し、ドメインに接続されていないユーザーがGlobalProtectにログインすると、そのユーザーの情報はDNSサーバー上に作成されたフォールバック ドメイン ゾーンに追加されます。

     GlobalProtectにログインしているGlobalProtectクライアントが、DNSサーバーに設定されていない予期しないドメインに属している場合、nsupdate は失敗する可

 ©2025 Palo Alto Networks, Inc.

能性があります。この場合は、[ドメインの上書き] を選択して、不明なドメインをDNSサーバーに認識されているドメインで上書きします。

- ドメインの上書き—Prisma AccessはDNS サーバーを更新するために指定したドメインのみを使用し、他のすべてのドメインを上書きします。GlobalProtectクライアントが別のドメインにログインする場合、DDNSサービスはここで指定したドメインを使用してDNS AレコードとPTRレコードを更新します。

3. フォールバック ドメイン フィールドで、フォールバック ドメインまたはオーバーライド ドメインのPTRレコードを更新するために使用されるドメインを選択します。
4. **DNS**サーバーの**IP**アドレスを選択します。
5. サーバー タイプ (**TSIG** または **Kerberos**) を選択します。
6. (TSIG デプロイメントのみ) TSIG で使用する**[TSIG**キー**]**を選択します。

   TSIG ファイルの形式が正しいこと、ファイルタイプが .key であることを確認してください。

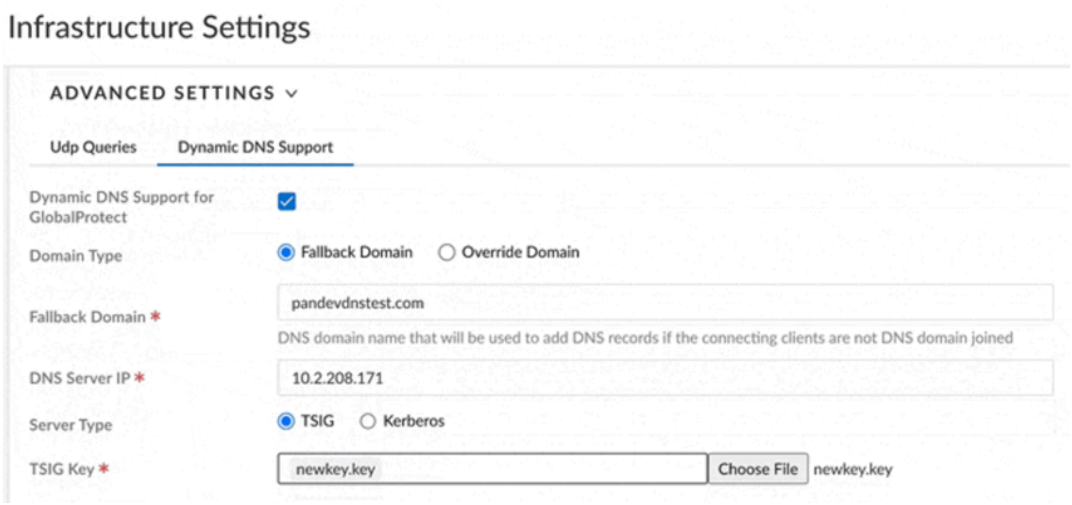
   Kerberos 認証タイプを選択した場合は、DNS サーバーから取得したエンコードされていない Kerberos キータブ ファイルを含む .key ファイルを通じて認証キーをアップロードします。

   TSIG ファイルは次の形式である必要があります:

   ```
   key "ddns-gp" { algorithm hmac-sha256; secret
    "aBCDEFGhiJklMNO89PQR+8stUVWX+YZAbcdeFgHI5J="; };
   ```

7. (Kerberos デプロイメントのみ) 使用するKerberosオプションを指定します。
   - **Kerberos** ドメイン コントローラのIPアドレスを入力します。
   - **Kerberos** 管理サーバーのIPアドレスを入力します。
   - **Kerberos**ユーザー名を入力します。
   - 使用する**Kerberos**キー (キータブ) を入力します。

     Kerberosキーが正しい形式であることを確認してください。



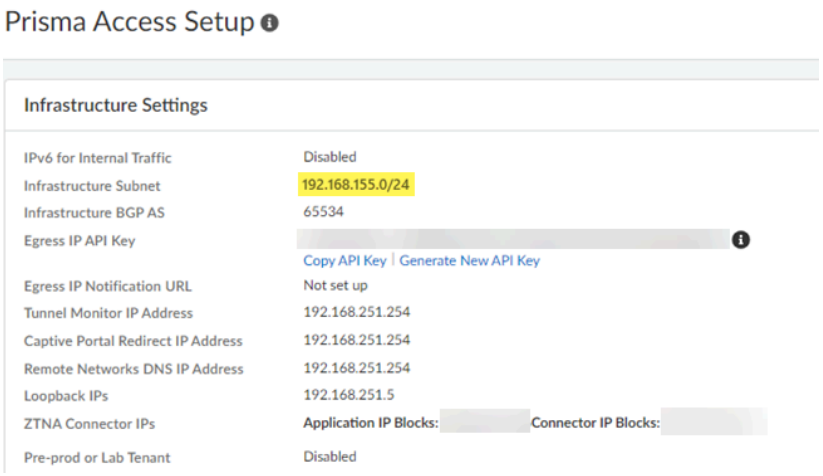
STEP 4 | 変更を保存します。

©2025 Palo Alto Networks, Inc.

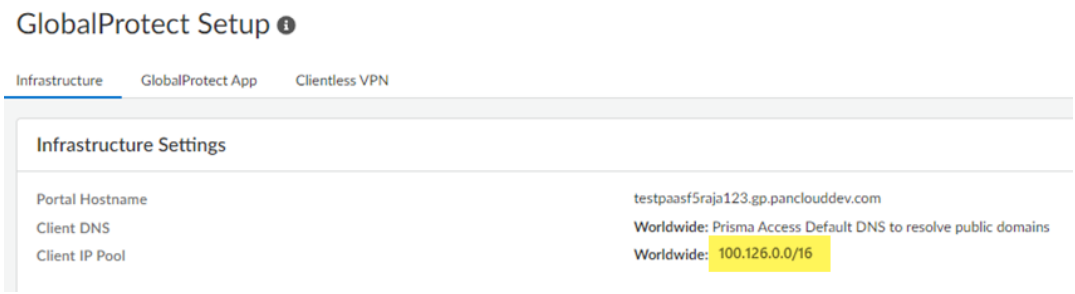
STEP 5 | DNSサーバーに前方参照ゾーンと検索参照ゾーンを設定します。

これらのゾーンを設定するには、IPAM ベンダーのドキュメントを参照してください。この手順では、Prisma Accessからのインフラストラクチャサブネットとクライアント**IP**プールを入力する必要があります。

- インフラストラクチャ サブネットを見つけるには、[ワークフロー] > **[Prisma Access** のセットアップ] > **[Prisma Access]** に移動して、[インフラストラクチャ サブネット]をメモします。



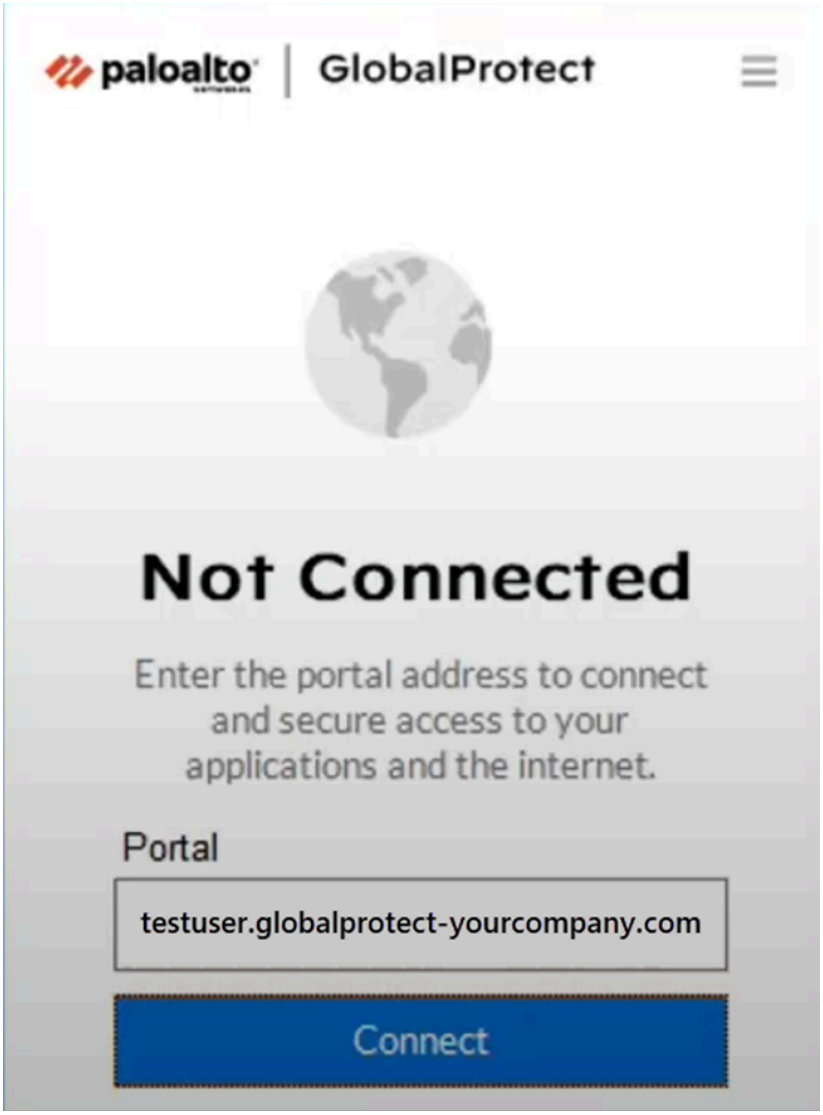
- GlobalProtect モバイル ユーザーのIPアドレス プールを見つけるには、[ワークフロー] > **[Prisma Access**セットアップ] > **[GlobalProtect]** に移動し、[クライアント**IP**プール]をメモします。



 ©2025 Palo Alto Networks, Inc.

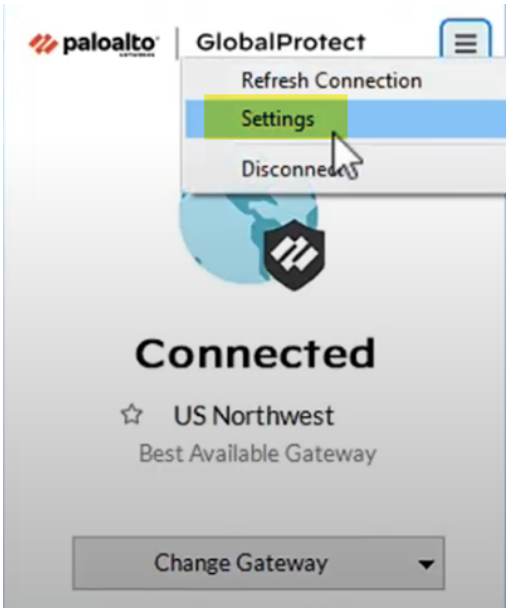
STEP 6 | IPAM DNSサーバーでDNSレコードが更新されていることを確認します。

1. クライアントマシンを開き、Prisma AccessGlobalProtectゲートウェイに接続します。

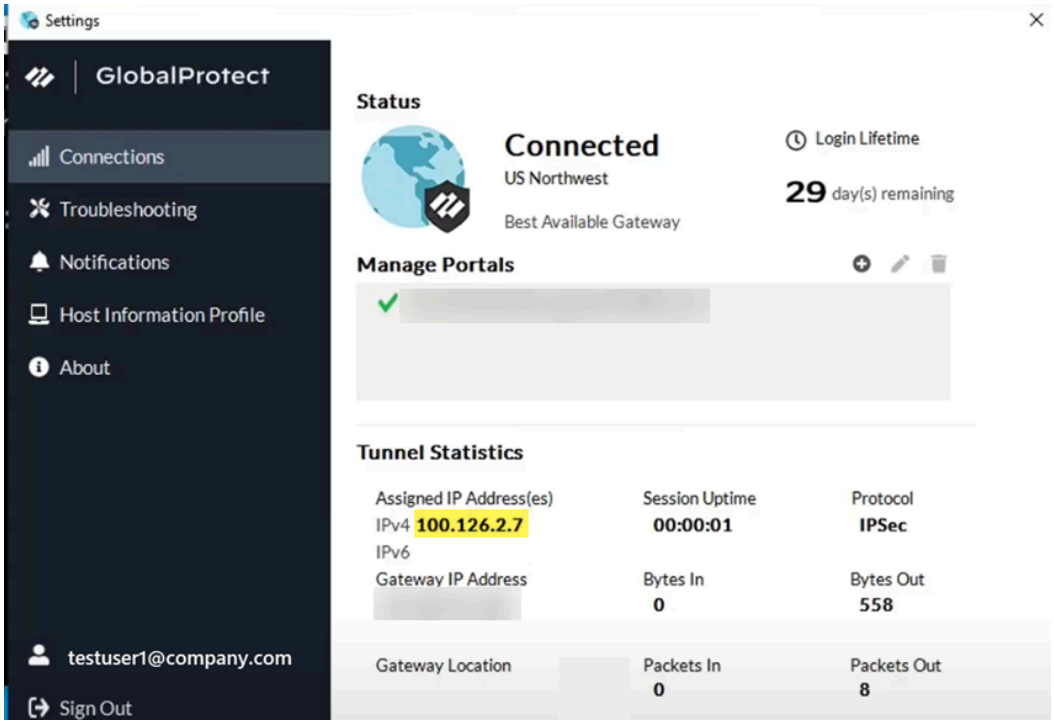


2. GlobalProtect設定を選択し、Prisma Accessがユーザに割り当てた GlobalProtect IPアドレスを確認します。

©2025 Palo Alto Networks, Inc.

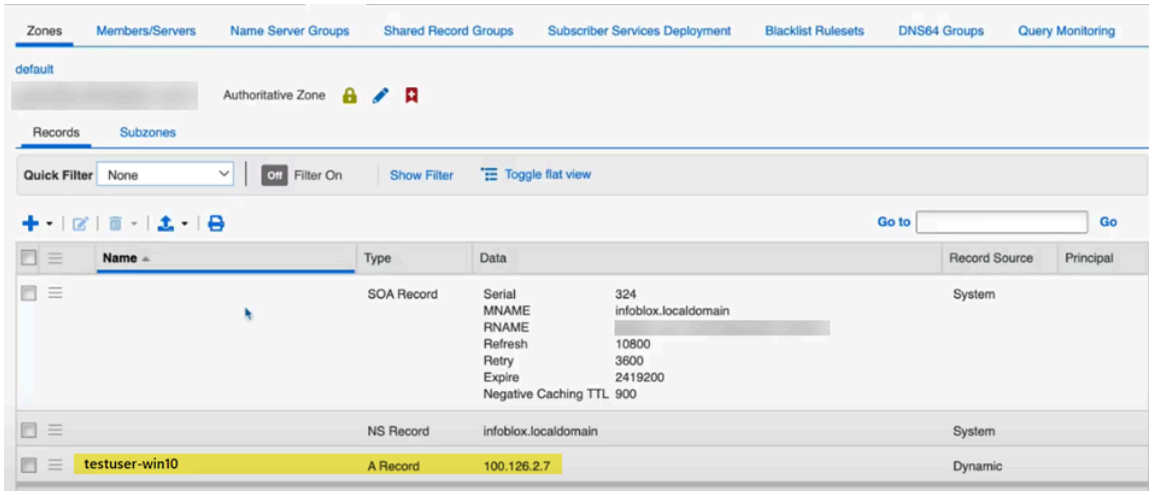


割り当てられたIPアドレス (100.126.2.7) は、IPアドレスがGlobalProtect IPアドレスプール (100.126.0.0/16) から取得されたことを示しています。

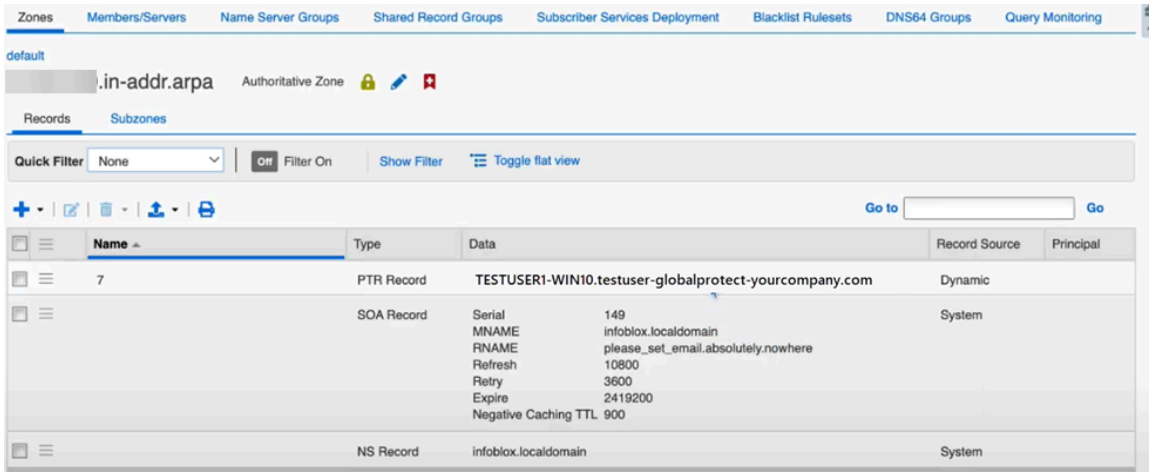


3. IPAM DNSサーバーから、ユーザーのレコードを表示します。
   この例では、ユーザーの名前は`testuser1-win10`です。

©2025 Palo Alto Networks, Inc.



DNS検索では、PTRレコードのユーザー名も表示されます。



4. ユーザーをGlobalProtectからログオフし、レコードをチェックして、DNSサーバーがユーザーのレコードを削除したことを確認します。

Prisma Access (Managed by Panorama)向け動的DNSアップデートを設定する

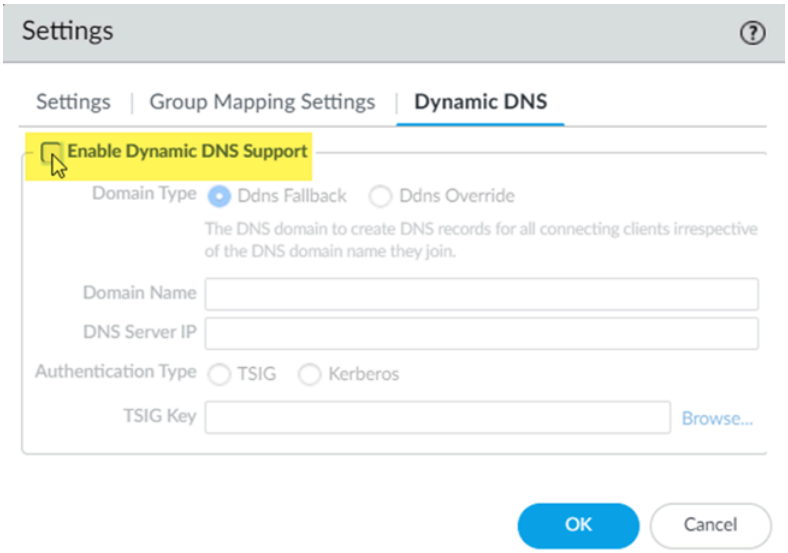
Prisma Access (Managed by Panorama)向けの動的DNS更新を構成するには、これらの手順を完了してください。

STEP 1 | Panoramaから、**Cloud Services** > **Configuration** > **Mobile Users-GlobalProtect**に移動し、歯車をクリックして設定を編集します。

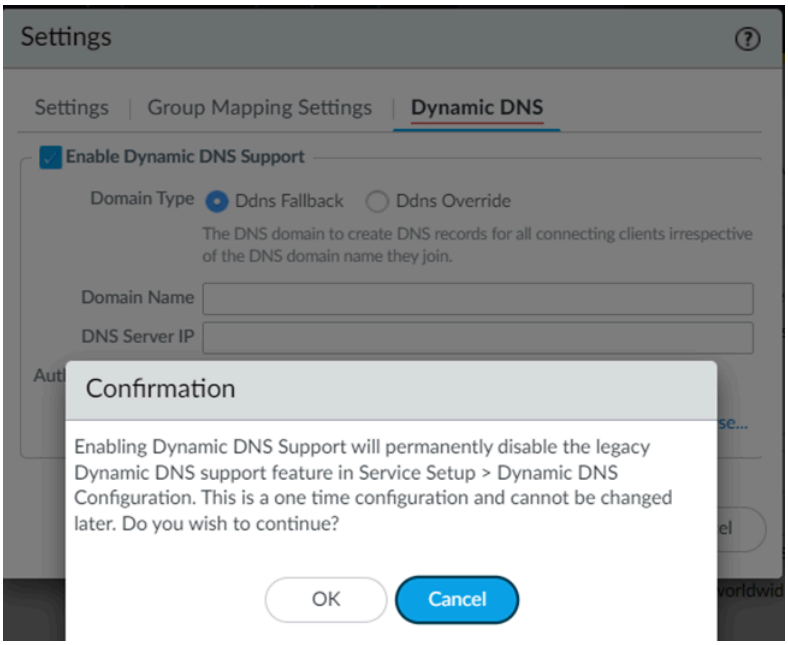
STEP 2 | 動的**DNS**を選択します。

 ©2025 Palo Alto Networks, Inc.

STEP 3 | 動的**DNS**サポートを有効にします。



STEP 4 | レガシーの動的DNSサポートが有効になっている場合、更新されたサポートを有効にすると、レガシーサポートが永久に無効になることが通知されます。**[OK]** クリックして続行します。



STEP 5 | 動的**DNS** 設定を構成します。

1. [動的**DNS**サポートを有効にする]を選択します。
2. ドメインタイプを選択します。
   - **Ddns** フォールバック–nsupdateイベントに使用されるドメインは、ドメイン名領域で指定したドメインにフォールバックします。GlobalProtectクライアントがどのドメインにも参加していない場合、またはDDNSサービスがDNSサーバー上のレコー

 ©2025 Palo Alto Networks, Inc.

ドを更新するために使用するのと同じドメインに参加している場合は、この選択肢を使用します。

Ddnsフィードバックを選択し、ドメインに接続されていないユーザーがGlobalProtectにログインすると、そのユーザーの情報はDNSサーバー上に作成されたフォールバック ドメイン ゾーンに追加されます。

GlobalProtectにログインしているGlobalProtectクライアントが、DNSサーバーに設定されていない予期しないドメインに属している場合、nsupdate は失敗する可能性があります。この場合は、**[Ddns**オーバーライド**]** を選択して、不明なドメインをDNSサーバーに認識されているドメインで上書きします。

- **Ddns**オーバーライド—Prisma AccessはDNS サーバーを更新するために指定したドメインのみを使用し、他のすべてのドメインを上書きします。GlobalProtectクライアントが別のドメインにログインする場合、DDNSサービスはここで指定したドメインを使用してDNS AレコードとPTRレコードを更新します。

3. ドメイン名 フィールドで、フォールバック ドメインまたはドメイン名のPTRレコードを更新するために使用されるドメインを選択します。
4. **DNS**サーバーの**IP**アドレスを選択します。
5. 認証タイプ (**TSIG** または **Kerberos**) を選択します。
6. (TSIG デプロイメントのみ) TSIG で使用する**[TSIG**キー**]**を選択します。
   TSIGファイルが正しい形式であり、ファイルタイプが.keyであることを確認してください。

   - Panorama管理デプロイメントをプラグインバージョン5.2.0以上で実行している場合、Kerberos認証タイプを選択すると、DNSサーバーから取得したKerberosキーのbase64エンコードされた文字列を含む.keyファイルを介して認証キーをアップロードします。例えば:
     `"ABCDEFGHIJKLMNOPQRSTUV5WXYZOUy5DT00ADUFabcDluaXN0cmF0b3IAAAABAAAAAAEAE`
   - プラグイン バージョン5.1.0未満のPanoramaが管理するデプロイメントを実行しており、Kerberos認証タイプを選択した場合は、エンコードされていないKerberos keytabファイルがDNSサーバーから取得された.keyファイルを介して認証キーをアップロードします。

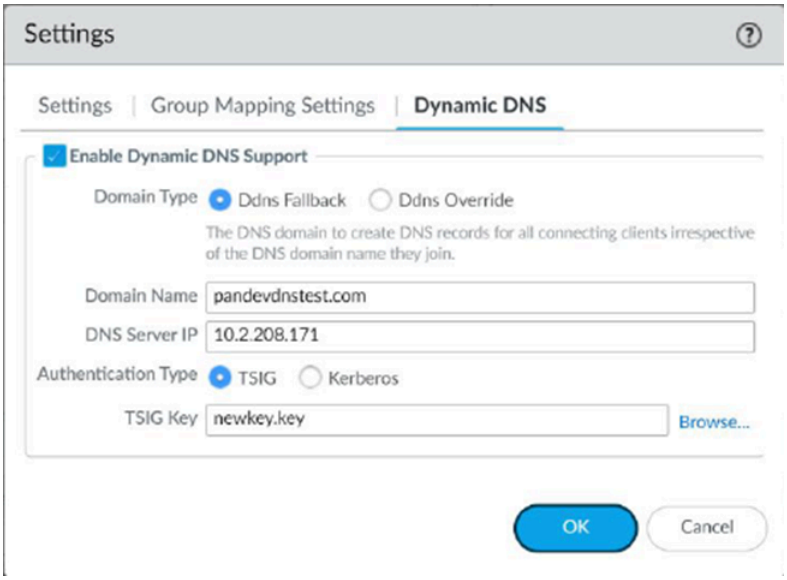
   TSIG ファイルは次の形式である必要があります:

```
key "ddns-gp" { algorithm hmac-sha256; secret
 "aBCDEFGhiJklMNO89PQR+8stUVWX+YZAbcdeFgHI5J="; };
```


©2025 Palo Alto Networks, Inc.

7. (Kerberos デプロイメントのみ) 使用するKerberosオプションを指定します。
   - **Kerberos** ドメイン コントローラのIPアドレスを入力します。
   - **Kerberos** 管理サーバーのIPアドレスを入力します。
   - **Kerberos**ユーザー名を入力します。
   - 使用する**Kerberos**キー (キータブ) を入力します。

     アップロードする前に、Kerberosキーにbase64エンコーディングを使用してください。



STEP 6 | 変更を保存します。

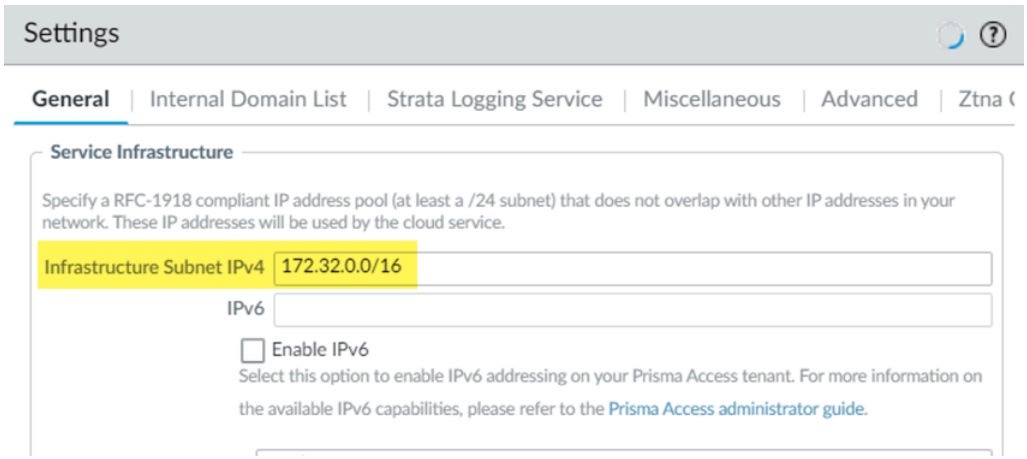
STEP 7 | DNSサーバーに前方参照ゾーンと検索参照ゾーンを設定します。

これらのゾーンを設定するには、IPAM ベンダーのドキュメントを参照してください。この手順では、Prisma Accessからのインフラストラクチャサブネットとクライアント**IP**プールを入力する必要があります。

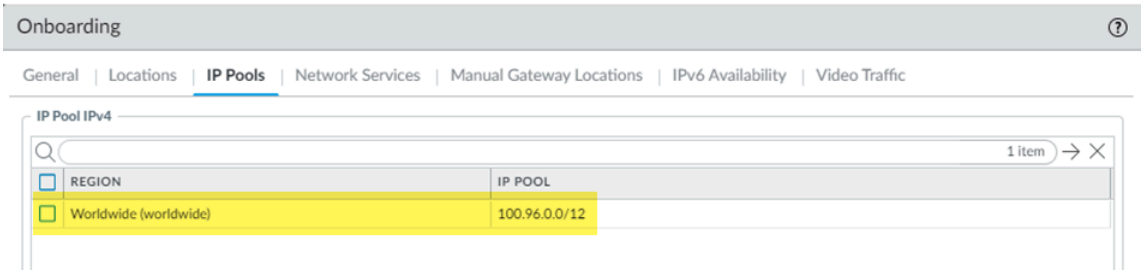
- インフラストラクチャサブネットを見つけるには、**[Panorama[** > **[Cloud Services (**クラウド サービス**)]** > **[Configuration (**設定**)]** > **[Service Setup (**サービス セットアップ**)]**に移動

©2025 Palo Alto Networks, Inc.

し、設定を編集するためにギアをクリックし、インフラストラクチャ サブネット**IPv4**をメモしてください。



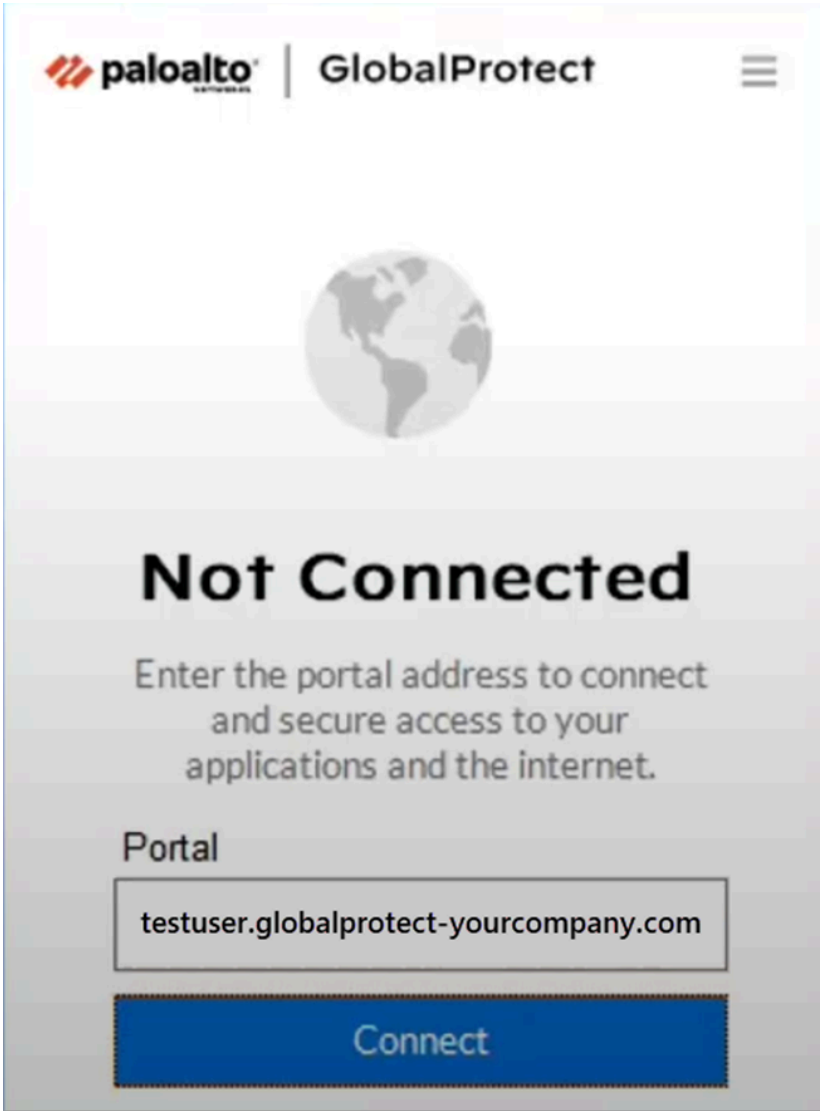
- GlobalProtectモバイルユーザーのIPアドレスプールを見つけるには、**[Panorama]** > **[Cloud Services (**クラウド サービス**)]** > **[Mobile Users (**モバイルユーザー**)—GlobalProtect]**に移動し、[ホスト名]を選択し、**[IP**プール**]**を選択して、**IP**プール**IPv4**をメモしてください。



 ©2025 Palo Alto Networks, Inc.

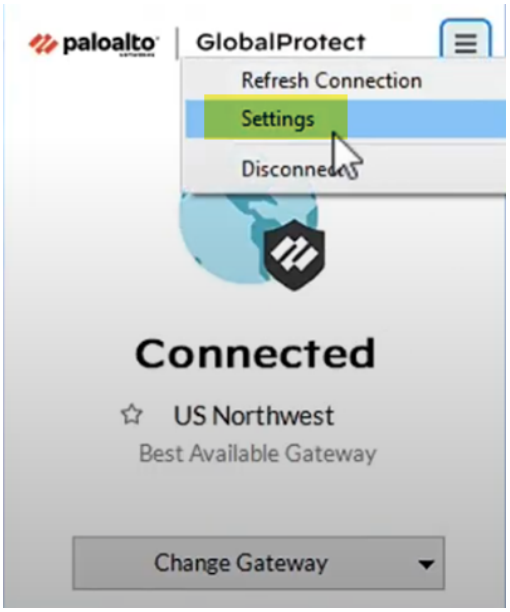
STEP 8 | IPAM DNSサーバーでDNSレコードが更新されていることを確認します。

1. クライアントマシンを開き、Prisma AccessGlobalProtectゲートウェイに接続します。

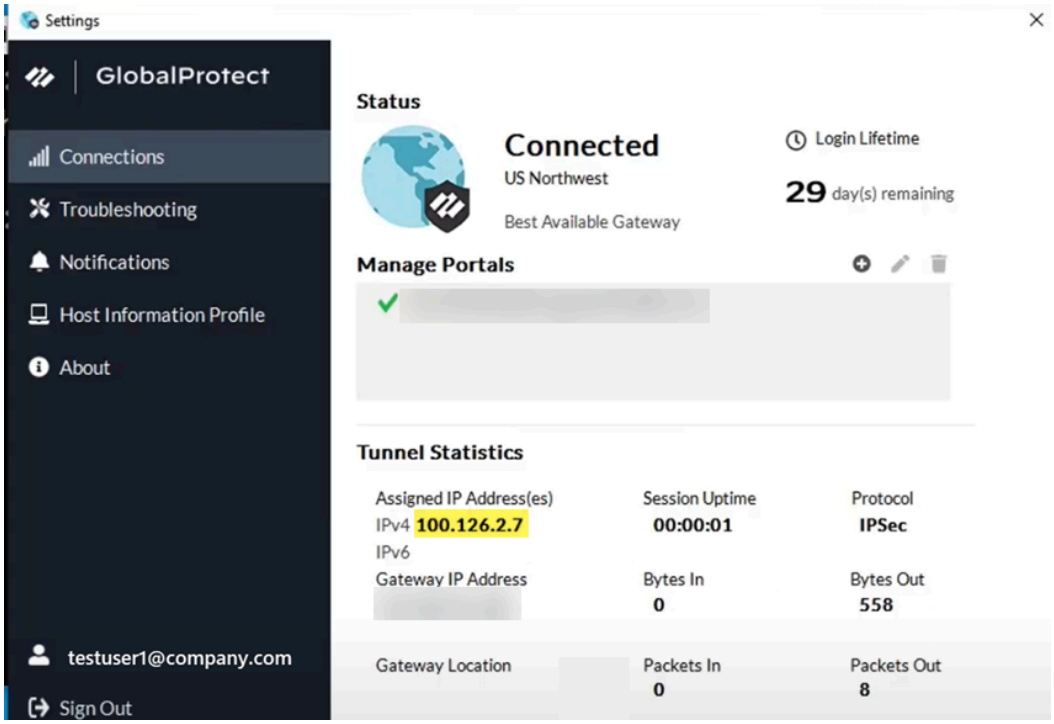


2. GlobalProtect設定を選択し、Prisma Accessがユーザに割り当てた GlobalProtect IPアドレスを確認します。

©2025 Palo Alto Networks, Inc.

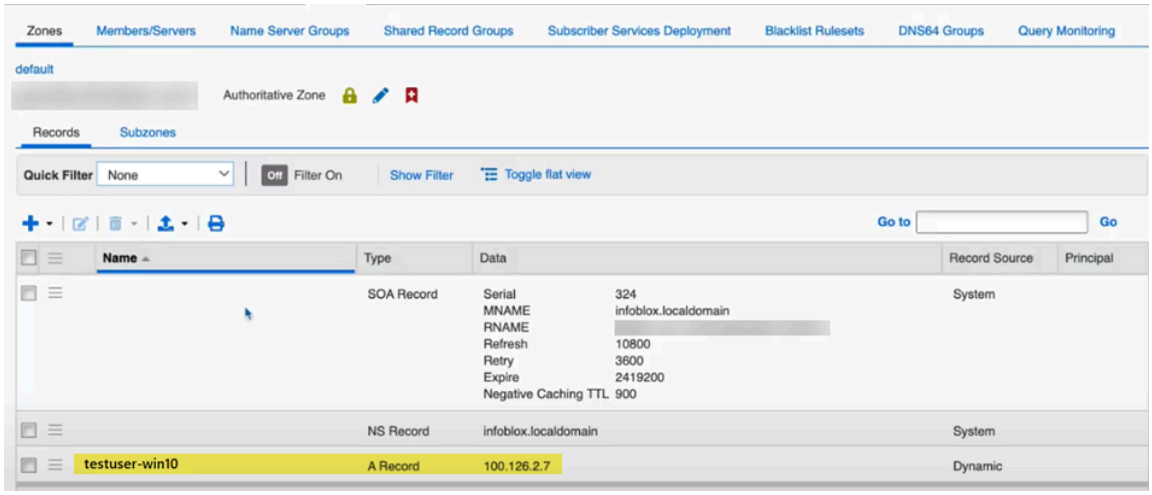


割り当てられたIPアドレス (100.126.2.7) は、IPアドレスがGlobalProtect IPアドレスプール (100.126.0.0/16) から取得されたことを示しています。

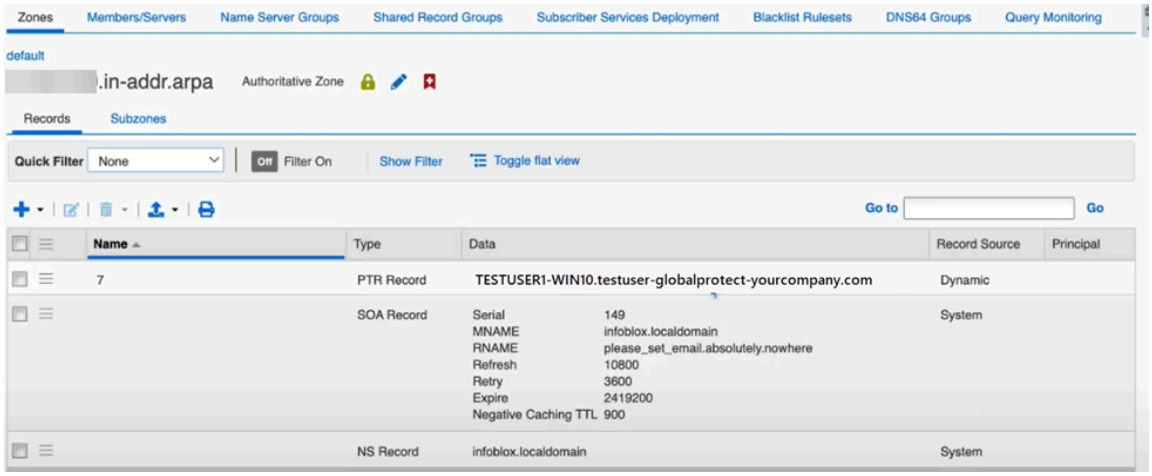


3. IPAM DNSサーバーから、ユーザーのレコードを表示します。
   この例では、ユーザーの名前は`testuser1-win10`です。

©2025 Palo Alto Networks, Inc.



DNS検索では、PTRレコードのユーザー名も表示されます。



4. ユーザーをGlobalProtectからログオフし、レコードをチェックして、DNSサーバーがユーザーのレコードを削除したことを確認します。

モバイルユーザー向けの動的DNS登録サポート - GlobalProtect

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama) • 有効なStrata Logging Serviceライセンスとクラウド サービス プラグインを持つPanoramaで管理される次世代ファイアウォール	❑ Prisma Accessのライセンス ❑ Minimum Required Prisma Access Version:3.1.1 Preferred (推奨)またはInnovation (革新) ❑ バージョン10.2 以降のPanoramaでサポート (バージョン10.1のPanoramaではサポートされません) ❑ クライアント エンドポイントはドメインに参加している必要があります。

©2025 Palo Alto Networks, Inc.

この機能は、*Prisma Access (Managed by Panorama) 3.1.1*以降の*Prisma Access*デプロイメントで利用可能です。

この機能は*Prisma Access (Managed by Strata Cloud Manager)*デプロイメントでは使用できません。

モバイルユーザーがGlobalProtectを使用してPrisma Accessにリモート接続する場合、企業内のDNSサーバは、GlobalProtectゲートウェイ割り当てIPアドレスで更新されません。動的DNS (DDNS) を有効にする前は、トンネルIPアドレスとエンドポイント名のマッピングは行われず、アドレスおよびポインタ (AおよびPTR) レコードとして記録されます。したがって、IT管理者またはユーザー管理ソフトウェアは、リモート エンドポイント名をIPアドレスにマッピングできません。

Prisma AccessでDDNS 機能を有効にすると、Prisma Access Cloud ServicesプラグインはStrata Logging ServiceのGlobalProtectイベントを15分ごとにチェックし、エンドポイントのホスト名、ドメイン名、トンネルIPアドレスを取得する。NSUPDATEを使用してDNSサーバーにAレコードとPTRレコードを動的に作成します。

モバイルユーザー向け動的**DNS**ワークフロー **- GlobalProtect**

DDNSを有効にした後、モバイル ユーザーがGlobalProtectアプリケーションでログインすると、次のようになります。

DDNSの仕組み、ガイドラインと要件、およびDDNSを有効にする方法の概要については、次のセクションをお読みください。

1. GlobalProtectは、GlobalProtectエンドポイントとオンプレミスまたはPrisma Accessゲートウェイの間にSSLトンネルを確立します。
2. GlobalProtectは、モバイルユーザーデバイスのホスト名、ドメイン名、およびトンネルIPアドレス情報を、トンネルを介してオンプレミスまたはPrisma Accessゲートウェイに送信します。
3. オンプレミス ゲートウェイまたはPrisma Accessは、この情報をGlobalProtectイベントとしてStrata Logging Serviceに転送します。
4. Prisma AccessCloud Servicesプラグインは、DNSサーバーを更新するために15分ごとにStrata Logging Serviceをプローブします。

   プラグインがStrata Logging ServiceからGlobalProtectイベントを受信しない場合、最大5回まで要求を再試行します。再試行要求が成功しなかった場合、プラグインは15分ごとに最大4回操作を再試行します。したがって、プラグインは1時間間隔で更新を受信できます。

   より頻繁に更新したい場合は、`debug plugins cloud_services set-gp-ddns-interval` コマンドを入力して、更新間隔を5分に変更できます。Aは時間間隔を更新する必要はありません。間隔を5分に変更すると、クラウド サービス プラグインは、ネットワーク遅延50ミリ秒で最大15,000件のレコードを更新し、20分間の更新を受信できるようになります。

- コマンドを使用して時間間隔を変更した後は、コミットは必要ありません。
- これらの数値は管理された環境からのものであり、実際の動作条件によって影響を受ける可能性があります。

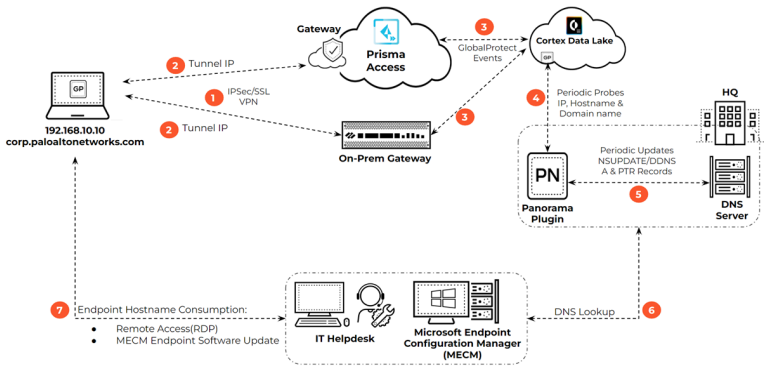
©2025 Palo Alto Networks, Inc.

5. Strata Logging Serviceから更新を受信した後、クラウドサービス プラグインはAレコードとPTRレコードをNSUPDATEとしてパッケージ化し、15分ごとにプライマリDNSサーバを更新する。

   `debug plugins cloud_services set-gp-ddns-interval` コマンドを使用して時間間隔を5分に変更した場合、プラグインは5分ごとにDNSサーバーを更新します。

   プラグインがNSUPDATEを通じてDNSサーバーを更新できない場合、プラグインは更新操作を最大5回再試行します。更新が成功しなかった場合、プラグインは更新操作を15分ごとに再試行します。間隔を5分に変更した場合は5分ごとに再試行し、最大4回再試行します。したがって、プラグインは、最大1時間 (15分間隔を使用する場合) または20分間 (5分間隔を使用する場合) ログに記録されたイベントを更新しようとし、その後新たに開始します。
6. GlobalProtectモバイル ユーザーのAレコードとPTR レコードがDNSサーバーで使用可能になると、IT管理者またはエンタープライズ ソフトウェアはDNSまたはRDNS検索を通じてこれらのレコードを使用し、エンドポイント名またはIPアドレスを解決します。
7. IT管理者またはエンドポイント管理ソフトウェアは、この情報を使用してエンドポイントを管理したり、ソフトウェアの更新をプッシュしたりします。

次の図はこのワークフローを示しています。



接続失敗ログを表示するには、***[Mobile_User_Device_Group]***の*[ダッシュボード]* > *[システム ログ]* または *[監視]* > *[ログ]* > *[システム]* を選択します。

動的**DNS**のガイドラインと要件

DDNS を有効にする前に、デプロイメントとDNSサーバーが次のガイドラインと要件を満たしていることを確認してください。

- クライアント エンドポイントはドメインに参加している必要があります。
- お使いのOSに基づいて、GlobalProtectクライアントを次のGlobalProtectアプリケーションバージョンに更新します。
  - Windows：5.2.11以降
  - Mac:5.2.11以降
  - Linux:5.3.3 以降
- Strata Logging Serviceを有効にします (Prisma Access以外のオンプレミス・ゲートウェイを使用する場合)

 ©2025 Palo Alto Networks, Inc.

- NSUPDATEによるDDNS更新をサポートする、バージョン8.6.1以降のInfoblox DNSサーバーが必要です。
- マルチテナントPrisma Accessデプロイメントは DDNSをサポートしていません。
- DNSサーバーからの認証キーを、ファイル拡張子.keyのbase64形式で保存します。Prisma Accessでは、キーはこの形式でのみアップロードできます。
- DNSサーバーでNTPを有効にし、Prisma Accessと同じであることを確認します。
- Infobloxに逆PTRおよび転送Aアドレスのゾーンを作成します。

次世代ファイアウォールや*Prisma Access*を使用して、スタンドアロンのデプロイメントで動的*DNS*をデプロイできます。ファイアウォールの場合は、このセクションのすべての前提条件が適用されます。また、有効な*Strata Logging Service*ライセンスがあり、*Panorama*でログ用のクラウド サービス プラグインを使用している必要があります。

モバイルユーザー向けにDDNSを有効にする - GlobalProtect

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

GlobalProtectモバイル ユーザーのAレコードとPTRレコードを使用してDNSサーバーを更新するには、次の手順を実行します。

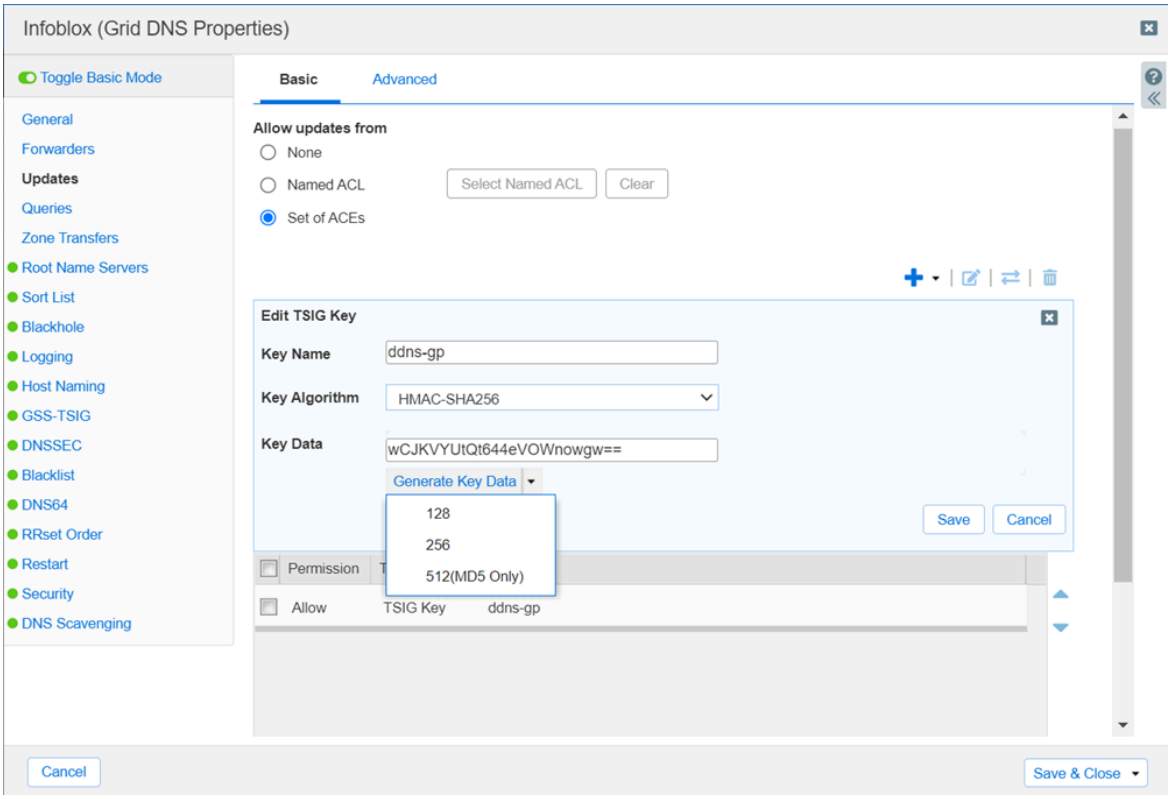
 ©2025 Palo Alto Networks, Inc.

STEP 1 | DNSサーバーに認証キーを作成します。

この例では、InfobloxをDNS サーバーとして使用します。

1. DNS サーバーにログインします。
2. **[Data Management (データ管理)] > [DNS] > [Grid DNS Properties (グリッド[DNS プロパティ)] > [Updates (更新)]**を選択します。
3. **ACE**のセットからの更新を許可します。
4. 詳細を入力した後、**TSIG** キー を追加します。

   - ***256*** キー アルゴリズムを選択します。
   - 新しいキーを作成するには、キー データを生成してください 。***256*** キーデータを選択します。



5. キー データを次の形式でファイルにコピーし、.key 拡張子でファイルを保存します。

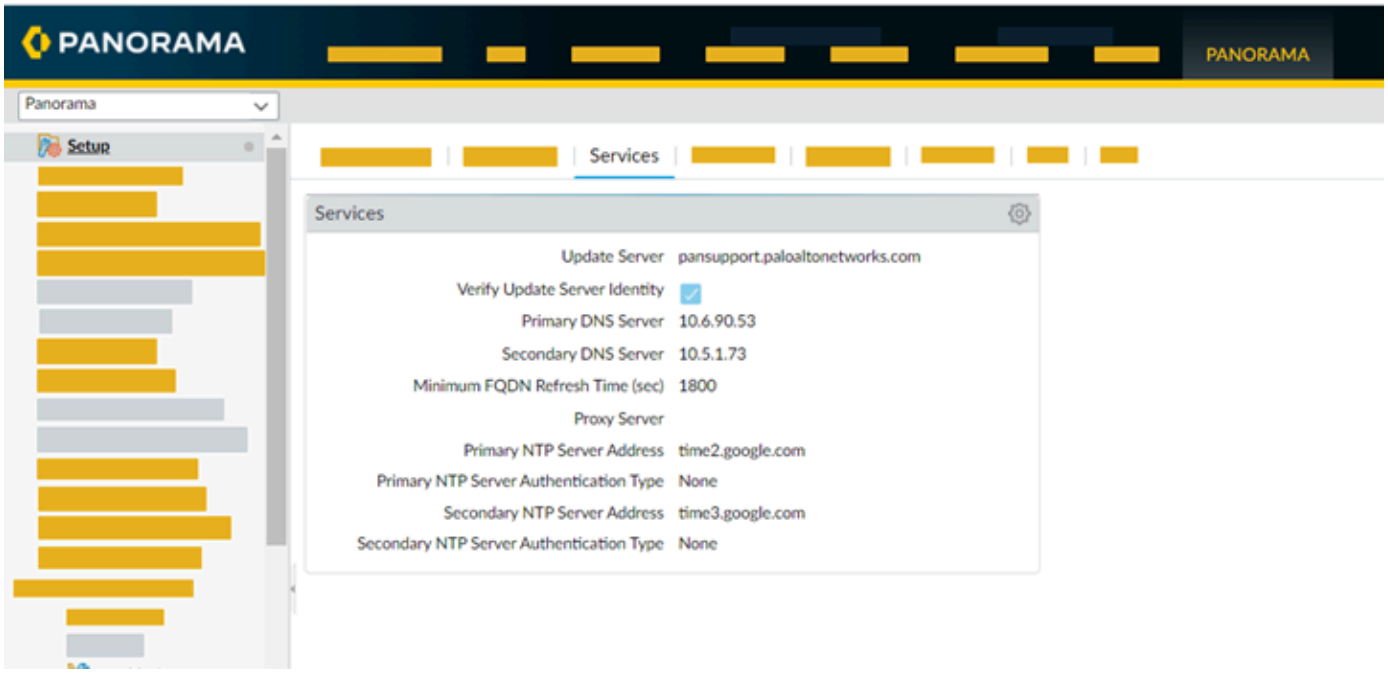
```
key "ddns-gp" { algorithm hmac-sha256; secret
 "wCJKVYUtQt644eVOWnowgw=="; };
```

後のステップで、このキーをPrisma AccessCloud Services プラグインにアップロードします。

©2025 Palo Alto Networks, Inc.

STEP 2 | お使いのPrisma Accessデプロイメントでは、DNS サーバーをプライマリDNSサーバーとして指定します。

1. **Panorama** > **Setup** > **Services**の順に選択します。
2. 設定を編集し 、プライマリDNSサーバーの詳細を更新します。

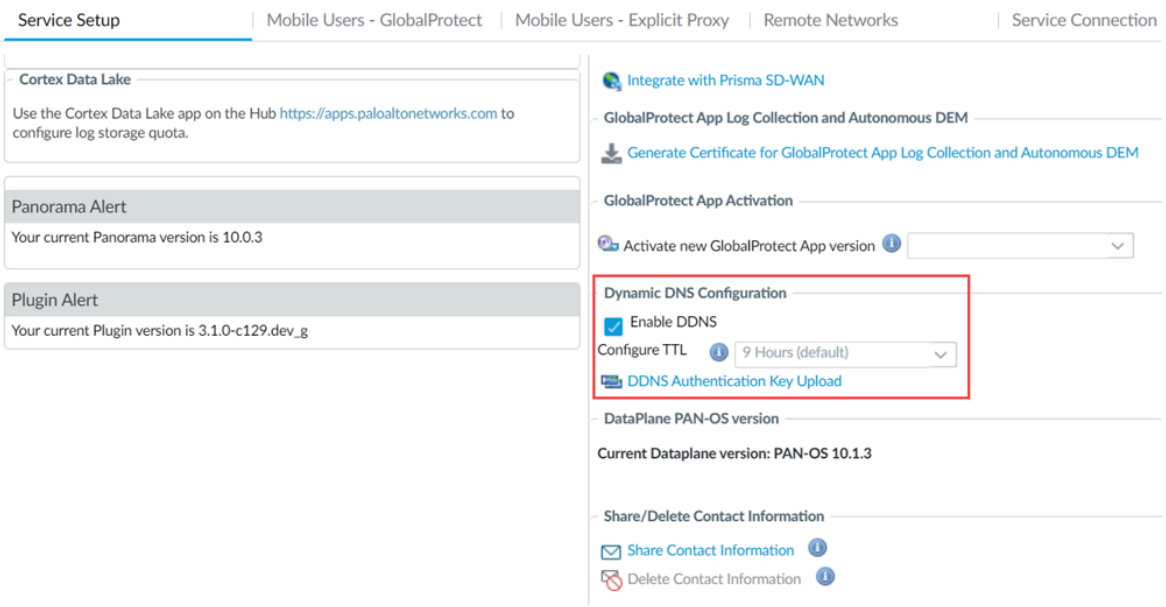


 ©2025 Palo Alto Networks, Inc.

STEP 3 | DDNS設定を構成します。

1. **Panorama** > **Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Service Setup**（サービスのセットアップ）を選択します。
2. **[Service Operations (サービス操作)]** > **[Dynamic DNS Configuration (ダイナミックDNS設定)]** を選択し、**[Enable DDNS (DDNS** を有効にする**)]** を選択します。
3. （任意）Prisma Accessがキャッシュ内の FDQN を更新する頻度として、**time-to-live (Time-To-Live - TTL)**値を設定します。

   デフォルトでは値は9時間に設定されています。



4. ステップ1で作成したDDNS認証キーをDNSサーバーからアップロードします。

STEP 4 | **Commit to Panorama**（**Panorama** へのコミット）によってコミットします。

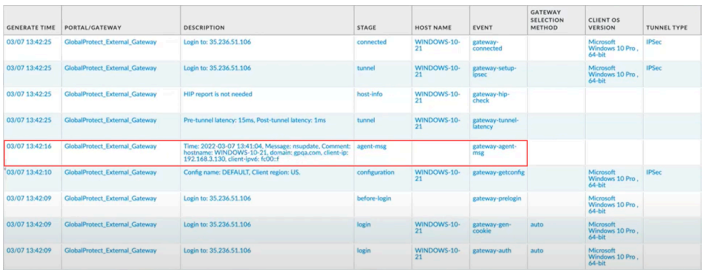
動的なDNS構成を確認する

どこで使用できますか?	何が必要ですか?
• Panorama	• Prisma Accessライセンス

DDNSを有効にした後、ログを監視し、以下のPrisma Accessコンポーネントをチェックすることで、問題をトラブルシューティングします。

[Monitor (監視)] > **[Logs (ログ)]** > **[GlobalProtect]**を選択します。ゲートウェイ エージェント メッセージには、ホスト名、ドメイン名、およびトンネル IP アドレス情報が含まれます。GlobalProtect は、エンドポイントがドメインまたは AD の一部である場合にのみエージェント メッセージを送信します。

©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	

他の DDNS ログを表示するには、Panorama CLI の `gp_ddns_support.log` コマンドを確認してください。

Prisma Access GlobalProtectのデプロイメントにおける侵害されたデバイスの識別と隔離

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Accessのライセンス

Prisma AccessはGlobalProtectアプリに接続されている侵害されたデバイスを識別して隔離することができます。これを行うには、デバイスを 手動 または 自動で 隔離リストに追加します。デバイスを隔離した後、ポリシーの一貫性を確保するために、 隔離されたデバイスのネットワークへのアクセスをブロック できます。

各Prisma Accessモバイルユーザーのロケーションは、Prisma Accessを管理するPanoramaと最寄りのサービ ス接続との間で隔離情報を送受信します。次世代ファイアウォールまたはゲートウェイがある場合は、サービス接続でPanoramaとオンプレミスのファイアウォールまたはゲートウェイとの間で隔離リスト情報を再配布する必要があります。また、Panoramaからサービス接続に隔離リスト情報を再分配して、Prisma Accessのすべてのモバイル ユーザーのロケーション（ゲートウェイ）で一貫したポリシーが適用されるようにする必要があります。

隔離リストの再配信のユースケース

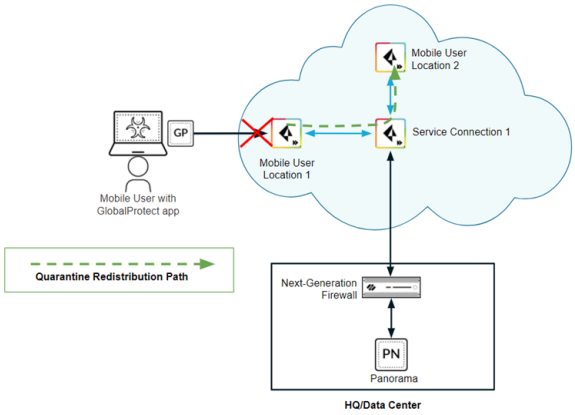
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Accessのライセンス

次のセクションでは、侵害されたデバイスに対する一貫したポリシーの適用に隔離リストの再配信が役立つ、一般的なPrisma Accessデプロイメントについて説明します。

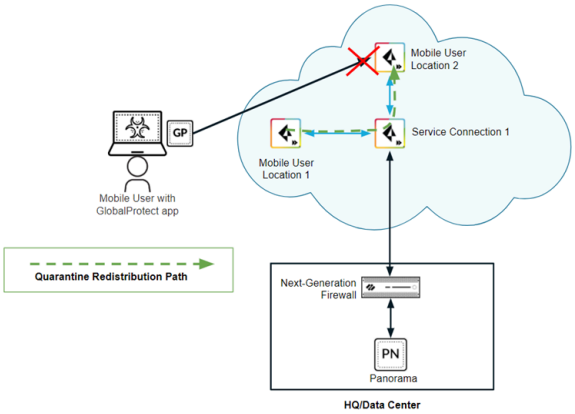
- 同じサービス接続に接続されたモバイルユーザー拠点間での隔離リストの再配信–次の例では、モバイルユーザーロケーション1に接続しているGlobalProtectモバイルユーザが危険にさ

 ©2025 Palo Alto Networks, Inc.

らされており、自動隔離されます。Prisma Accessは、ポリシーに従って隔離されたデバイスをブロックまたは制限します。



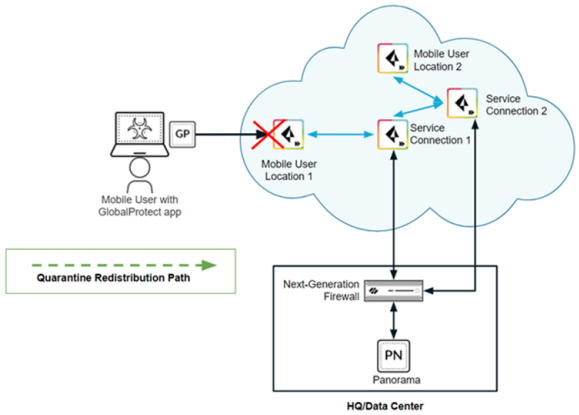
サービス接続（この例では Service Connection 1）は、接続されているすべてのモバイルユーザーロケーション間で隔離リスト情報を再配信します。モバイル ユーザー ロケーション2は、サービス接続1を介して再配信された隔離リスト情報を受信するため、GlobalProtectモバイル ユーザーがモバイル ユーザー ロケーション2に接続しようとすることもブロックされます。



- 異なるサービス接続に接続しているモバイルユーザロケーション間での隔離リストの再配信–次の例では、モバイルユーザーロケーションが2つありますが、2つの異なるサービス接続に接続しています。GlobalProtectユーザーがモバイル ユーザー ロケーション1に接続しよ

©2025 Palo Alto Networks, Inc.

うとしました。モバイル ユーザー ロケーション1は、GlobalProtectユーザー エンドポイントが侵害されたことを検出し、隔離します。

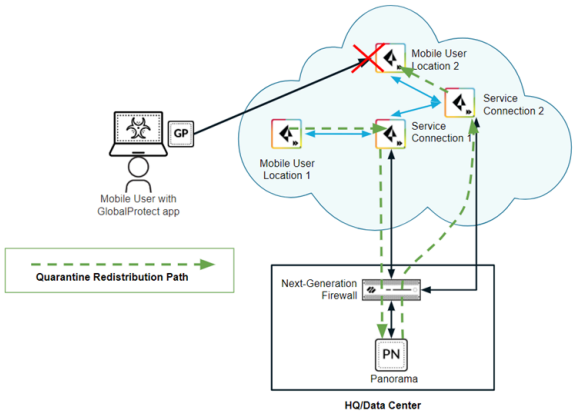


隔離リスト情報をモバイルユーザーロケーション 1 からモバイルユーザロケーション 2 に再配信するには、次のアクションを実行します。

- 隔離リスト情報をサービス接続 1 からPanoramaに再配信します。
- 隔離リスト情報をPanoramaからサービス接続 2 に再配信します。

この設定では、GlobalProtectユーザーがモバイルユーザロケーション1に接続して隔離されると、隔離リストの情報がモバイルユーザロケーション1からモバイルユーザロケーション2に再配信され、モバイルユーザロケーション2への接続の試行はすべてブロックされます。

この設定は、*GlobalProtect*ユーザーがモバイルユーザロケーション2に接続して隔離された場合にも有効です。隔離リストの情報は、モバイルユーザロケーション2からモバイルユーザロケーション*1*に再配信されます。



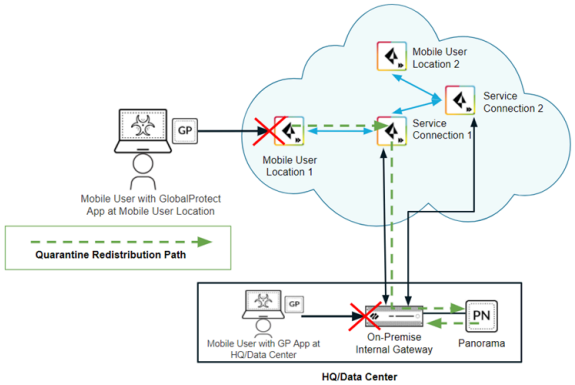
- **Prisma Access**次世代ファイアウォールまたはゲートウェイとの間での隔離リストの再配信–次の例では、GlobalProtectユーザーがモバイルユーザロケーション1に接続しようとしたものです。モバイル ユーザー ロケーション1は、GlobalProtectユーザー エンドポイントが侵害されたことを検出し、隔離します。その後、モバイルユーザーは会社の本社に行き、再度

 ©2025 Palo Alto Networks, Inc.

ログインを試みます。本社は、内部ホスト検出を使用してGlobalProtectゲートウェイとして構成された次世代ファイアウォールで保護されています。

モバイルユーザーロケーション1はサービス接続1を介して隔離リスト情報をPanoramaに再配信し、Panoramaは隔離リスト情報をオンプレミスの内部ゲートウェイに再配信します。ユーザーが本社の場所からログインしようとすると、GlobalProtectはオンプレミスゲートウェイが内部ゲートウェイとして設定されていることを検出し、トンネルなしでゲートウェイに接続します。

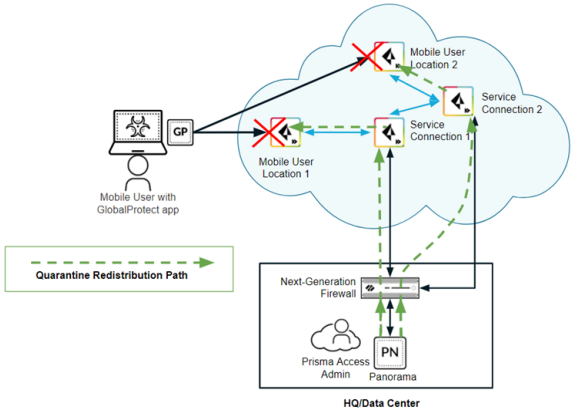
隔離リスト情報はオンプレミスゲートウェイに再配信されたため、ユーザーは設定されたユーザーポリシーに基づいてゲートウェイでブロックされます。



Prisma Accessで次世代ファイアウォールまたはゲートウェイを使用する場合は、隔離リスト情報をファイアウォールまたはゲートウェイ、すべてのサービス接続、および Panorama に再配信するようにPanoramaを設定する必要があります。

- 管理者が**Panorama**でモバイルユーザーを手動で隔離する–この例では、Prisma Accessを管理するPanoramaアプライアンスで、Prisma Access管理者が手動でモバイルユーザーを隔離リストに追加しています。管理者は、Panorama、次世代ファイアウォール、およびサービス接続間の再配信を設定しました。Panoramaは、更新された隔離リスト情報をファイアウォールとサービス接続に再配信します。次に、サービス接続は、隔離リスト情報をモバイルユーザーの場所に再配信します。

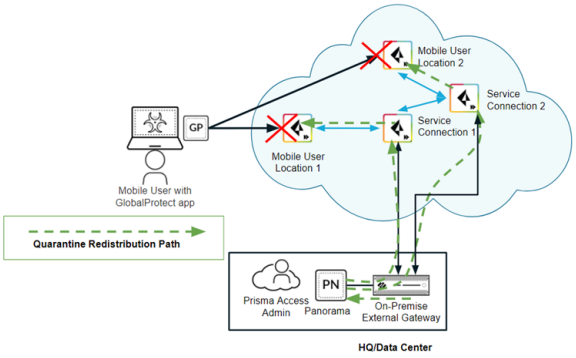
  モバイルユーザーはモバイルユーザーロケーション1に接続されました。モバイルユーザーロケーション1が更新された隔離リスト情報を受信すると、ユーザーの接続が切断されます。ユーザーがモバイルユーザーロケーション2に接続しようとすると、接続がブロックされ、モバイルユーザーは隔離通知を受け取ります。



 ©2025 Palo Alto Networks, Inc.

- オンプレミスゲートウェイでのモバイルユーザーの自動隔離または手動隔離 – この例では、本社またはデータセンターの場所に外部ゲートウェイとして設定された次世代ファイアウォールがあります。管理者は、外部ゲートウェイでモバイルユーザーを手動で隔離しました。外部ゲートウェイは、外部ゲートウェイからの隔離リスト情報をPanoramaに再配信します。

  Panoramaは、外部ゲートウェイから更新された隔離リスト情報を受信すると、その情報をサービス接続1と2に再配信し、サービス接続1と2はその情報をモバイルユーザーロケーション1と2に再配信します。モバイル ユーザーがモバイル ユーザー ロケーション1または2に接続しようとすると、 Prisma Accessは接続をブロックし、ユーザは隔離通知を受け取ります。



Prisma Accessで隔離リストの再配信を設定する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Accessのライセンス

サービス接続、Prisma Accessを管理する Panorama、および次世代ファイアウォールとの間で隔離情報を再配信するには、以下の手順を実行します。

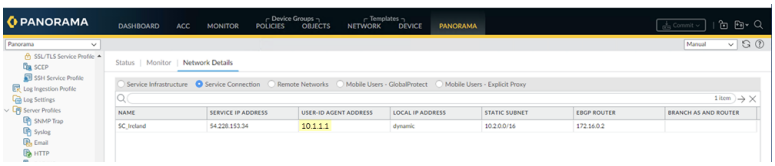
STEP 1 | 隔離リスト情報を再配信するすべてのサービス接続について、Panorama管理IPアドレスがUser-IDエージェントアドレスと通信できることを確認します。

サービス接続のUser-IDエージェントアドレスとPanoramaの管理IPアドレス間の通信は、Prisma Accessが Panoramaとサービス接続の間で隔離リスト情報を送受信するために必要です。

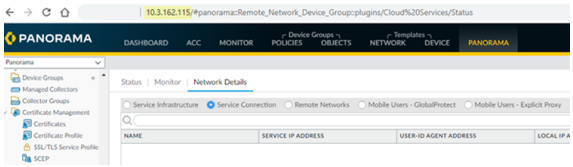
- **User-ID Agent Address**（**User-ID**エージェントアドレス）を探すには、**[Panorama]** > **[Cloud Services**（クラウドサービス）**]** > **[Status**（ステータス）**]** > **[Network**

©2025 Palo Alto Networks, Inc.

Details（ネットワーク詳細）] > **[Service Connection (サービス接続)]** > **[User-ID Agent Address (User-IDエージェントアドレス)]**の順に選択します。



- Prisma Accessを管理するPanoramaの管理IPアドレスを見つけるには、Panoramaにアクセスしたときに**Web**ブラウザに表示される**IP**アドレスをメモしてください。



STEP 2 | Prisma Accessによる隔離リスト情報の再配信を許可します。

1. Panoramaで、**Panorama** > **Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Service Setup**（サービスのセットアップ）を選択します。
2. 設定を編集するには、歯車型アイコンをクリックします。
3. **[詳細設定]** タブで、**[隔離リストの再配信を有効にする]**を選択します。

   隔離リスト再配信を有効にすると、Prisma Accessは、1つまたは複数のモバイルユーザロケーショ ン（ゲートウェイ）から受信した隔離リスト情報をサービス接続に再配信できる。

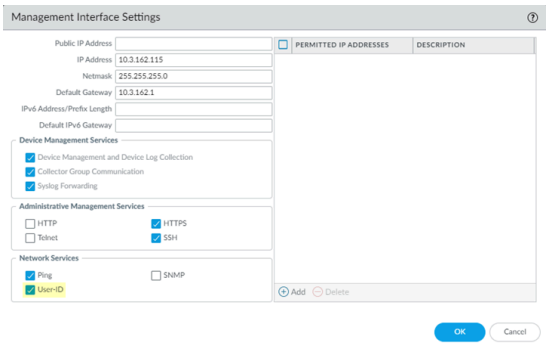


STEP 3 | 変更をコミットしてプッシュします。

©2025 Palo Alto Networks, Inc.

STEP 4 | 管理インタフェース設定を構成して、PanoramaがPrisma Accessから隔離リスト情報を受信するように構成します。

1. Prisma Accessを管理するパノラマで、**[Panorama]** > **[セットアップ]** > **[インターフェース]**を選択します。
2. **Management**（管理）インターフェイスを選択します。
3. **User-ID**を選択します。

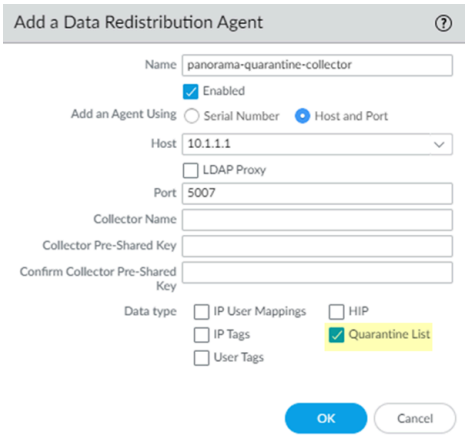


 ©2025 Palo Alto Networks, Inc.

STEP 5 | サービス接続からPanoramaへの隔離リスト情報を再配信するデータ再配信エージェントを構成します。

1. Prisma Accessを管理するPanoramaで、**[Panorama]** > **[Cloud Services (**クラウドサービス**)]** > [ステータス] > [ネットワークの詳細] > [サービス接続]を選択します。
2. 各サービス接続の **User-ID**エージェントアドレス (**Panorama** > **Cloud Services (**クラウドサービス**)** > ステータス > ネットワークの詳細 > サービス接続 > **User-ID**エージェントアドレス) をメモします。
3. **[Panorama]** > **[Data Redistribution (**データ再配布**)]** > **[Agents (**エージェント**)]** を選択します。
4. データ再配布エージェントを追加し 、 名前 を付けて、[有効]を選択します。
5. ホストとしてサービス接続の**User-ID**エージェントアドレスを入力し、 ポートとして5007を入力します。

   ネットワークが*Panorama*と*Prisma Access* 間のこのポートへのアクセスをブロックしていないことを確認します。
6. （任意）このサービス接続をコレクター（[デバイス] > [データ再配信] > [コレクター設定]）として構成した場合は、 コレクター名 と コレクター事前共有鍵を入力します。
7. 隔離リストを選択し、「**OK**」をクリックします。



8. Prisma Accessデプロイメント内のすべてのサービス接続について、ステップ5を繰り返します。

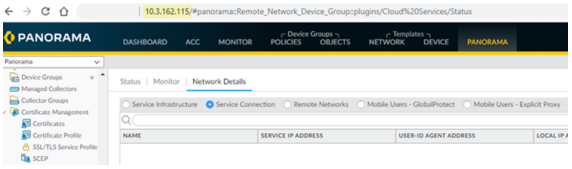
STEP 6 | [コミット] > **[Panorama**にコミット**]** を選択すると、Prisma Access管理しているパノラマにローカルで変更内容が保存されます。

©2025 Palo Alto Networks, Inc.

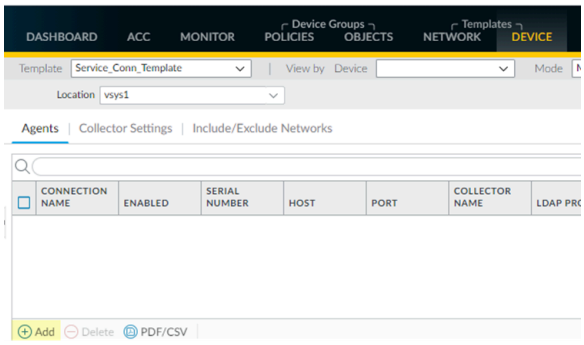
STEP 7 | Panoramaからサービス接続に隔離リスト情報を再配信するデータ再配信エージェントを構成します。

1. Prisma Accessを管理しているPanoramaの管理IPアドレスを見つけます。

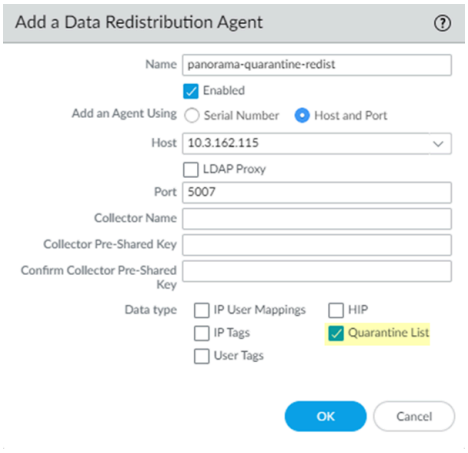
   このアドレスは、Panoramaにアクセスすると、Webブラウザーのアドレス バーに表示されます。



2. **Service_Conn_Template**テンプレートにいることを確認し、[デバイス] > [データ再配布] > [エージェント]を選択します。



3. データ再配布エージェントを追加し 、 名前 を付けて、[有効]を選択します。
4. Panoramaアプライアンスの管理IPアドレスをホストとして、ポートとして5007を入力します。



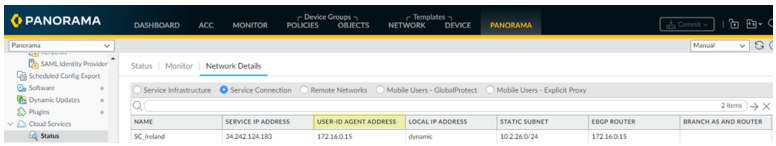
5. 隔離リストを選択し、「**OK**」をクリックします。

 ©2025 Palo Alto Networks, Inc.

STEP 8 | サービス接続からモバイル ユーザー ゲートウェイへの隔離リスト情報を再配信するデータ再配信エージェントを構成します。

1. Prisma Accessを管理するPanoramaで、**[Panorama] > [Cloud Services (クラウドサービス)] > [ステータス] > [ネットワークの詳細] > [サービス接続]**を選択します。
2. 隔離リスト情報を再配信するサービス接続の **User-ID**エージェントアドレス をメモします。

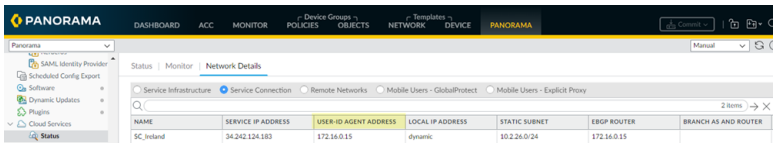
   すべてのサービス接続には同じ再配信隔離リスト情報があるため、任意のサービス接続を選択します。複数のサービス接続を構成することもできます。



3. **Mobile_User_Template**テンプレートにいることを確認し、**[デバイス] > [データ再配布] > [エージェント]**を選択します。
4. データ再配布エージェントを追加し 、 名前 を付けて、**[有効]**を選択します。
5. ホストとしてサービス接続の**User-ID**エージェントアドレスを入力し、 ポートとして**5007**を入力します。

   ネットワークが*Panorama*と*Prisma Access* 間のこのポートへのアクセスをブロックしていないことを確認します。

6. （任意）このサービス接続をコレクター（**[デバイス] > [データ再配信] > [コレクター設定]**）として構成した場合は、 コレクター名 と コレクター事前共有鍵を入力します。
7. 隔離リストを選択し、「**OK**」をクリックします。



8. 変更を **Commit and Push**（コミットしてプッシュ）します。

STEP 9 | **Panorama** > デバイス隔離を選択して、隔離リストの情報を表示します。

詳細については、「GlobalProtect 管理者ガイド」 の 「隔離されたデバイス情報の表示」 を参照してください。

モバイル ユーザーのIPv6トラフィックのシンクホール - GlobalProtectのデプロイメント

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

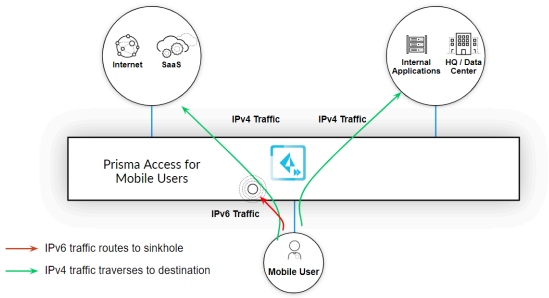
©2025 Palo Alto Networks, Inc.

IPv4トラフィックとIPv6トラフィックの両方を処理できるデュアルスタックエンドポイントで、GlobalProtectアプリケーションはモバイルユーザーのIPv4トラフィックを保護するために、GlobalProtect VPNトンネル経由でPrisma Accessに送信します。ただし、モバイルユーザーのIPv6トラフィックはデフォルトで、Prisma Accessに送信されるのではなく、エンドポイントのローカルネットワークアダプタに送信されます。IPv6ベースの脅威に対する攻撃面を減らすために、IPv6トラフィックのシンクホールを行うように、Prisma Accessを設定することをお勧めします。エンドポイントは自動的にIPv4アドレスに戻ることができるため、モバイルユーザートラフィックをインターネットに送信する際に、安全かつ円滑なユーザー体験を提供することができます。

デフォルトの *IPv6* ルートは他のルートよりも優先されます。ただし、物理ネットワーク インターフェイスを介してより具体的な *IPv6* ルートが存在する場合、または物理インターフェイスの *IPv6* 送信元アドレスを指定した場合、そのようなトラフィックはローカル ネットワーク アダプターに送信されます。

また、完全にローカルネットワークアダプタ上のネットワークトラフィックを無効にするように、GlobalProtectを設定することをお勧めします。GlobalProtectゲートウェイとして設定されたオンプレミス次世代ファイアウォールを持つ、ハイブリッドPrisma Accessデプロイ環境がある場合、オンプレミスGlobalProtectゲートウェイにIPv6シンクホール機能を設定することができます。

すべてのモバイルユーザーのIPv6トラフィックをシンクホールするように、Prisma Accessを設定することができます。この機能を有効にすると、Prisma AccessによってIPv4アドレスに加えてIPv6アドレスが、接続しているエンドポイントに割り当てられます。その後、次の図に示すようにIPv6トラフィックがPrisma Accessにルーティングされ、内蔵のセキュリティ ポリシーを使ってそれが破棄されます。



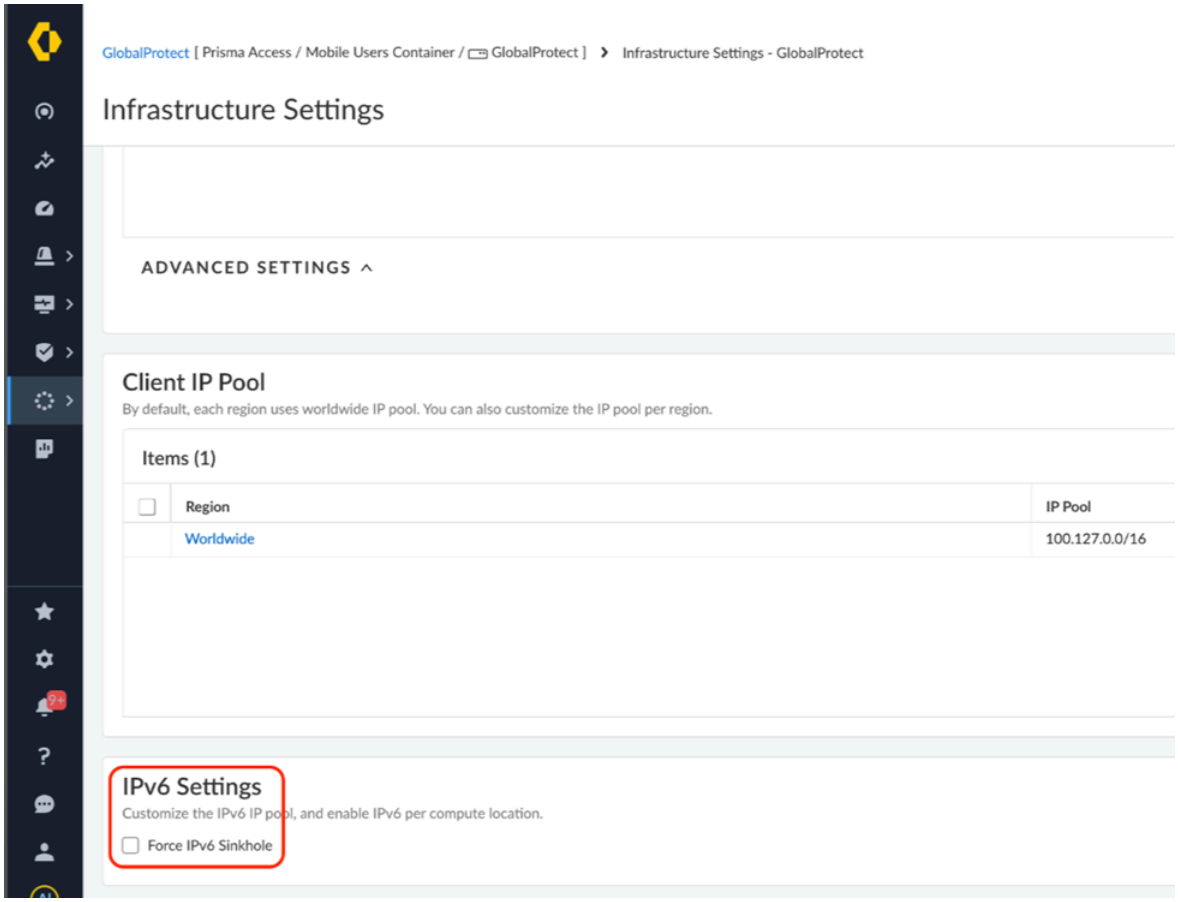
モバイルユーザーのすべてのIPv6トラフィックをシンクホールするようにPrisma Accessを設定するには、次の作業を行ってください。

©2025 Palo Alto Networks, Inc.

- Prisma Access (Managed by Strata Cloud Manager)デプロイメント:

  [ワークフロー] > [**Prisma Access** セットアップ] > [モバイル ユーザー] > [**GlobalProtect** セットアップ] > [詳細設定] に移動して、**[Force IPv6 Sinkhole]**を選択します。

  Prisma Accessはシンクホール アドレスとして fc00:0:0:0:0:0:0:0/64 を使用します。



- Prisma Access (Managed by Panorama)デプロイメント:

  1. Prisma Accessを管理するPanoramaにログインする時に使用するのと同じIPアドレスを使用して、管理者レベルの権限でCLIセッションを開始します。
  2. `configure`と入力して、設定モードに移行します。
  3. **`set plugins cloud_services mobile-users ipv6 yes`** コマンドを入力します。

     将来このコマンドを無効にする必要がある場合は、**`set plugins cloud_services mobile-users ipv6 no`** と入力します。
  4. **`Commit`** と入力して変更を保存します。
  5. **`exit`**と入力して、設定モードを終了します。
  6. **`commit-all shared-policy include-template yes device-group Mobile_User_Device_Group`**と入力して、変更内容をコミット、プッシュ配信して、Prisma Access上でそれをアクティブにします。

©2025 Palo Alto Networks, Inc.

exitローカルネットワークへの直接アクセスを無効にするためのGlobalProtectの設定

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス ❑ すべてのMacOSおよびWindows GlobalProtectエンドポイントでサポートされています。GlobalProtectアプリ バージョン6.0.0 以降のLinuxエンドポイントでサポートされます。

すべてのモバイルユーザートラフィックがPrisma Accessに送信されるように、ローカルサブネットトラフィックを含めた送信接続を完全に無効化して、ローカルアダプタに送信されないようにすることができます。ローカルアダプタへのすべての送信接続を無効にするには、GlobalProtectゲートウェイの設定を変更します。

これらの作業は、Panorama上またはGlobalProtectゲートウェイとして設定されたオンプレミスファイアウォール上で実施できます。

不正な*Wi-Fi*アクセスポイントなどの信頼できないネットワークでのリスクを軽減するため、［***No direct access to local network*** **(**ローカルネットワークに直接アクセスしない**)**］設定を有効にします。

STEP 1 | **Network** > **GlobalProtect** > **Gateways** (ネットワーク > GlobalProtect > ゲートウェイ)を選択します。

STEP 2 | 既存のGlobalProtectゲートウェイを選択するか、新しく ゲートウェイを**Add**（追加）します。

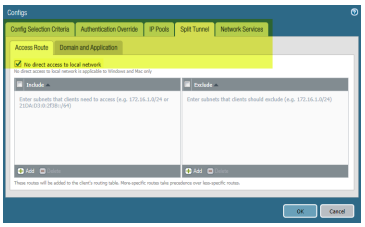
STEP 3 | **Agent**（エージェント） > **Client Settings**（クライアント設定）を選択します。

STEP 4 | **DEFAULT**（デフォルト）設定を選択するか、または新しく**Add**（追加）します。

©2025 Palo Alto Networks, Inc.

STEP 5 | **Split Tunnel**（トンネルを分割）を選択し、次に**No direct access to local network**（ローカルネットワークへの直接アクセスなし）を選択します。

ローカルネットワークアクセスを無効にすると、*IPv4*および*IPv6*トラフィックも含めて、すべてのトラフィックが、ローカルアダプタに送信されなくなります。また、プリンタなどのローカルサブネット上のリソースにもアクセスできなくなります。アクセス ルート、宛先ドメイン、およびアプリケーションに基づくスプリット トンネル トラフィックは、引き続き正常に動作します。



STEP 6 | PanoramaおよびPrisma Accessデプロイメントのみ– 変更内容をローカルにコミットして、Panoramaでそれをアクティブにします。

1. **Commit**（コミット） > **Commit to Panorama**（**Panorama** にコミット）を選択します。
2. 変更内容が**Commit Scope**（コミットスコープ）の一部となっていることを確認します。
3. **OK** をクリックして、プッシュ スコープに変更を保存します。
4. 変更を**Commit (**コミット**)**します。

STEP 7 | 変更をコミットしてプッシュし、Prisma Accessでアクティブにします。

オンプレミスゲートウェイでの**IPv6**シンクホールのセットアップ

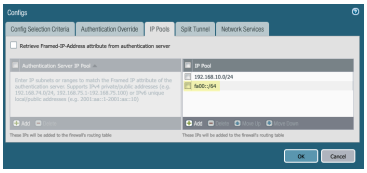
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

ゲートウェイとして設定された次世代ファイアウォールとPrisma Accessを使用するハイブリッドデプロイ環境の場合、IPv6トラフィックを破棄するために、オンプレミスゲートウェイで次の作業を行ってください。

©2025 Palo Alto Networks, Inc.

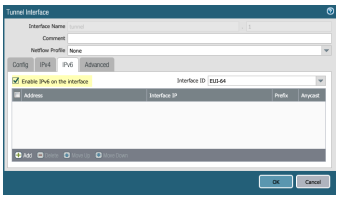
STEP 1 | GlobalProtectエージェント設定にIPv6 IPプールを追加します。

1. **Network** > **GlobalProtect** > **Gateways** (ネットワーク > GlobalProtect > ゲートウェイ)を選択します。
2. 既存のGlobalProtectゲートウェイを選択するか、新しく ゲートウェイを**Add**（追加）します。
3. **Agent**（エージェント） > **Client Settings**（クライアント設定）を選択します。
4. 変更するエージェント設定を選択するか、または新しく **Add**（追加）します。
5. **IP Pools**（**IP** プール）を選択したら、次にモバイルネットワークトラフィック用に使用するGlobalProtectゲートウェイに接続するエンドポイント上の、仮想ネットワークアダプタに割り当てるIPv6プールを**Add**（追加）して、**OK**をクリックします。



STEP 2 | インターフェースのIPv6の有効化

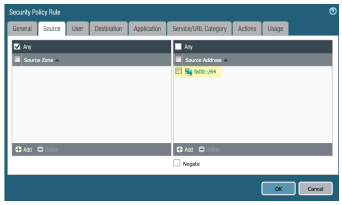
1. **Device**（デバイス） > **Interface**（インターフェイス） > **Tunnel**（トンネル）を選択して、モバイルユーザーのトラフィックに対して使用するトンネル**Interface**（インターフェイス）を選択します。
2. **IPv6**を選択して、次に**Enable IPv6 on the interface**（インターフェイスで**IPv6**を有効にする）を選択します。



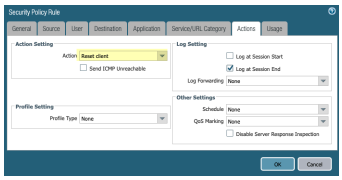
©2025 Palo Alto Networks, Inc.

STEP 3 | ステップ1で設定したIPプールに一致する、IPv6ソーストラフィックを持つセッションを終了する、TCPリセットアクションを設定するために、セキュリティポリシーを追加します。

1. **Policies (ポリシー) > Security (セキュリティ)** を選択して新しいセキュリティポリシーを **Add (追加)** します。
2. ステップ1で設定したIPプールと照合するために、**Source Address**（ソースアドレス）をルール内に設定します。



3. **Actions**（アクション）を選択し、次に**Action Setting**（アクション設定）で**Reset Client**（クライアントのリセット）を選択して、**OK**をクリックします。



STEP 4 | 変更を **Commit (コミット)** します。

STEP 5 | （任意）デプロイ環境内のすべてのゲートウェイファイアウォール上で、この作業を行います。

Prisma Accessを使用したHIP情報の再配信

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

一貫したホスト情報プロファイル（HIP）ポリシーを適用し、ポリシー管理を簡素化するために、Prisma Accessから社内のその他のゲートウェイ、ファイアウォール、およびPanoramaアプライアンス（Prisma Accessを管理するPanoramaも含む）へのアクセスにGlobalProtectアプリケーションを使用している、モバイルユーザーおよびリモートネットワークのユーザーから受信したHIP情報を再配信することができます。

次のセクションでは、一貫したポリシーの適用とHIPレポートの参照にHIPの再配信が役立つ、一般的なPrisma Accessデプロイメント環境の例を説明していきます。

- **Prisma Access**から次世代ファイアウォールへの**HIP**再配信–組織のデータセンターまたは本社で次世代ファイアウォールを利用しており、そのファイアウォールにHIPベースのセキュリ

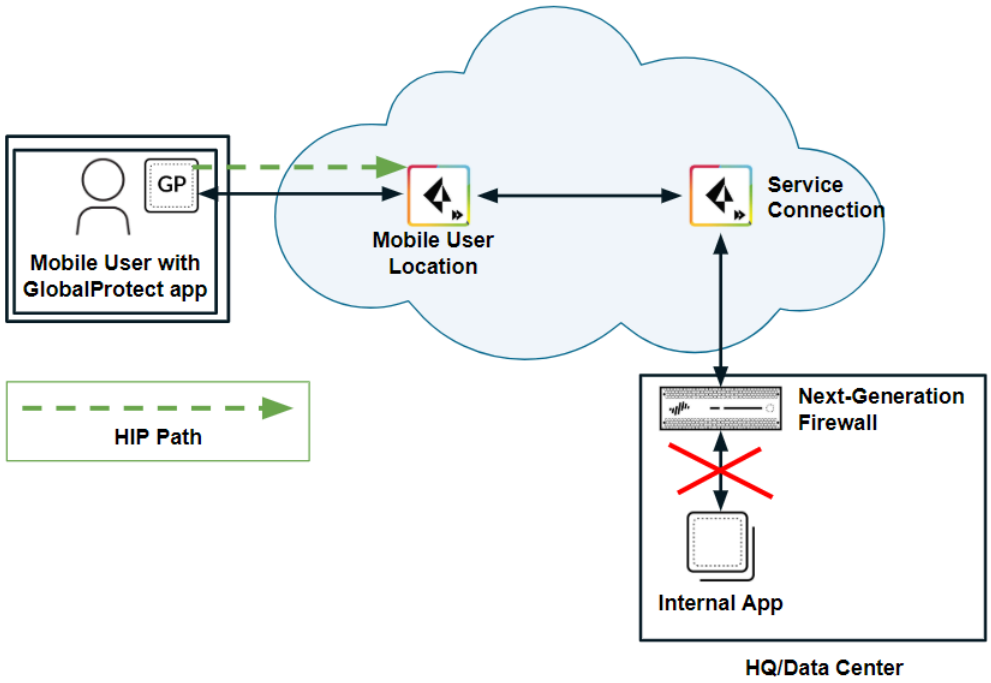
 ©2025 Palo Alto Networks, Inc.

ティポリシーを設定している場合、Prisma AccessからファイアウォールにHIPを再配信しないと、Prisma Accessモバイルユーザーに対してこれらのポリシーを適用できません。

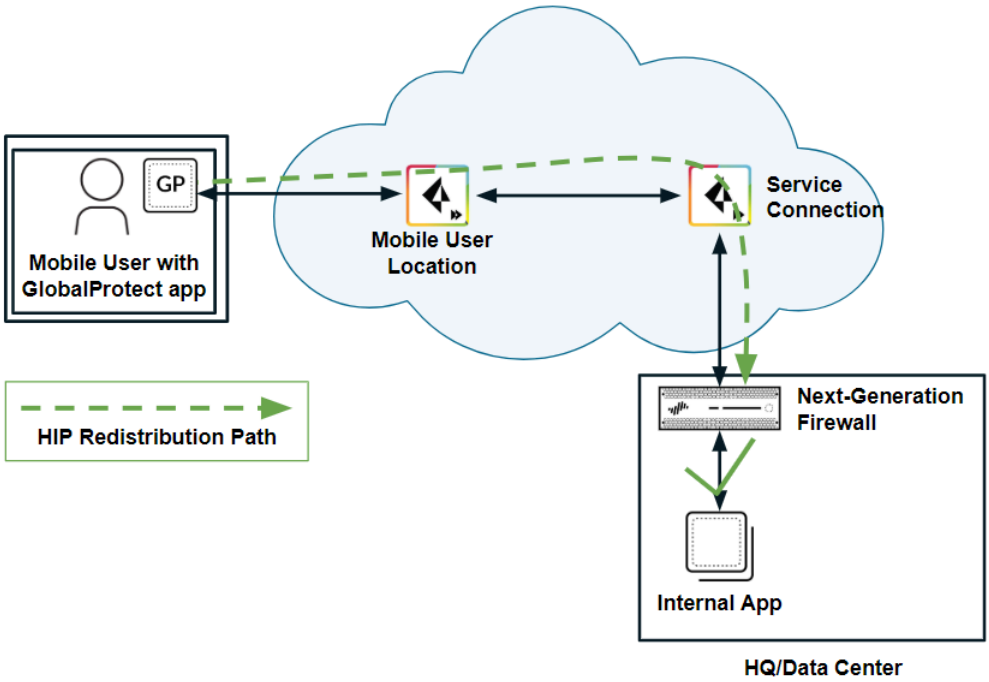
エンドポイントがGlobalProtectアプリケーションで保護されているモバイルユーザーを次の図に示します。本社/データセンターの内部アプリケーションへのアクセスを試みるユーザーのアクセスは、次世代ファイアウォールとHIPベースのセキュリティポリシーで管理されています。ユーザーがGlobalProtectアプリケーションにログインすると、アプリケーションはHIP情報を収集して、それをPrisma Accessに送信します。しかし、Prisma Accessはこの情報を、オンプレミスファイアウォールに再配信しません。ファイアウォールは、ユーザー

 ©2025 Palo Alto Networks, Inc.

のHIP情報を保有していないため、ユーザーのアプリケーションへのアクセスはブロックされてしまいます。



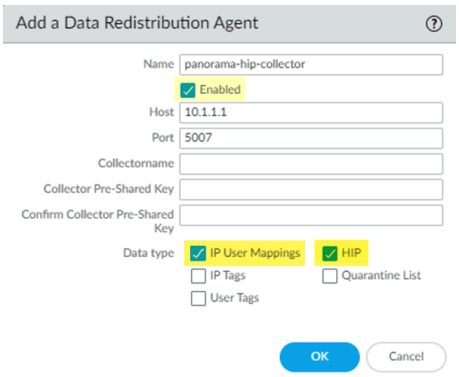
HIP再配信により、モバイルユーザーのHIP情報をオンプレミスファイアウォールに配信することができます。ファイアウォールは、設定されているセキュリティポリシーに対してユーザーのHIP情報を確認し、ユーザーにアプリケーションへのアクセスを許可します。



Prisma AccessからファイアウォールにHIP情報を再配布するには、Prisma AccessにHIP情報の再配信を許可し、次にファイアウォールに**User-ID**エージェント (**[Panorama]** > **[User**

©2025 Palo Alto Networks, Inc.

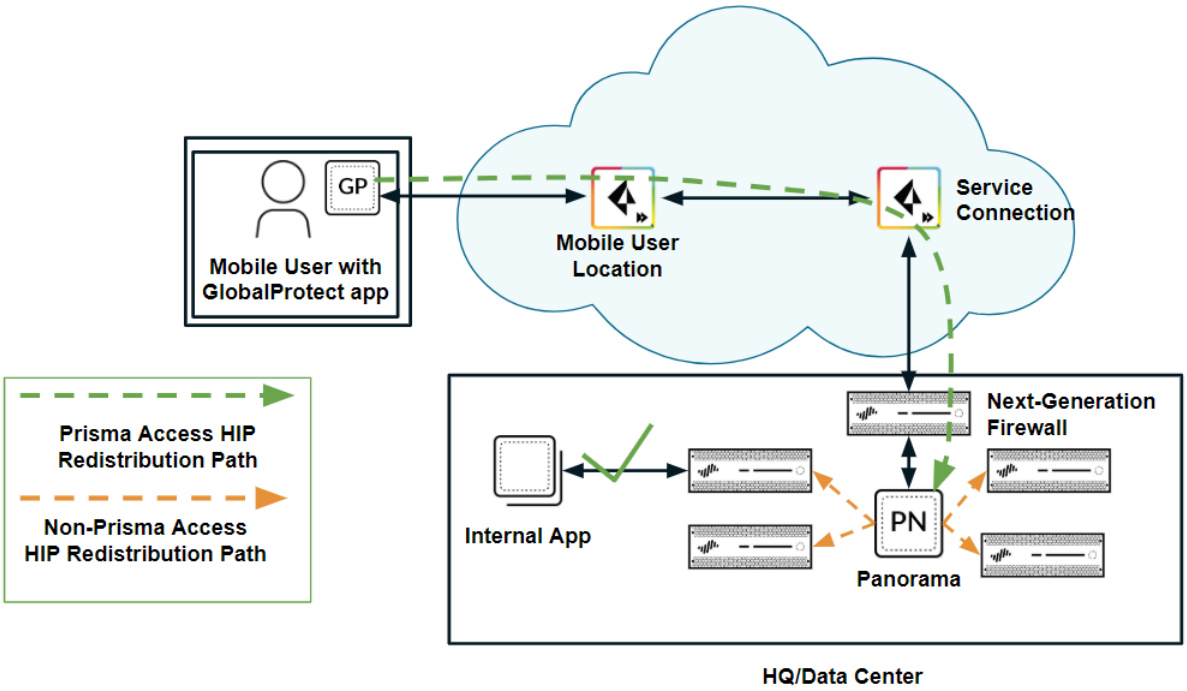
Identification (ユーザー**ID**)] > [**User-ID Agents** (ユーザー**ID**エージェント)] 9.1.*x* Panoramaアプライアンス用[**Panorama**] > [**Data Redistribution** (データ再配信)] Panorama 10.*x* アプライアンス用) を追加し、ホスト(次の例では10.1.1.1) としてPrisma Access [**User-ID Agent Address** (ユーザー**ID**エージェントアドレス)]([**Panorama**] > [**Cloud Services** (クラウドサービス)] > [**Status** (ステータス)] > [**Network Details** (ネットワーク詳細)] > [**Service Connection** (サービス接続)] > [**User-ID Agent Address** (ユーザー**ID**エージェントアドレス)])、ポートとして**5007**を指定します。



- **Prisma Access**から**Prisma Access**への**HIP**再配信—HIPベースのセキュリティポリシーを持つ複数のファイアウォールまたはゲートウェイが存在している場合、PanoramaでUser-IDエージェントを作成して、User-ID **Host**（ホスト）としてPrisma AccessのPrisma Access**User-ID Agent Address**（ユーザー**ID**エージェントアドレス）を指定することで、Prisma Accessからそれを管理しているPanoramaへ、HIP情報を再配信することができます。次にPanoramaアプライアンスから社内にあるその他のマネージドPanoramaアプライアンス、ゲートウェイ、ファイアウォール、および仮想システムにHIPレポートを再配信することができます。この場合、マネージドファイアウォールへのUser-ID情報の再配信と同じワークフローを使用し

 ©2025 Palo Alto Networks, Inc.

て、次の図のように内部アプリケーションとリソースに対して、一貫したポリシーを適用します。



Panoramaを利用する代わりに、各デバイスでUser-IDエージェントを作成して、内部ファイアウォールまたはゲートウェイが、Prisma Accessから直接情報を収集するように設定することもできます。ただし、Prisma AccessはHIP情報の送信にサービス接続を使用しているため、Prisma Accessが大量のHIPレポートを送信した場合、サービス接続帯域幅の消費量が増加する可能性があることに注意してください。

- リモートネットワークのユーザーから**Prisma Access**への**HIP**再配信—前の使用事例でPrisma Accessは、モバイルユーザーからHIP情報を収集していました。Prisma Accessでリモートネットワークロケーションのユーザーに**HIP**ベースのポリシーを適用したい場合、リモートネットワークユーザーのGlobalProtectアプリケーションからPrisma Accessに**HIP**情報を配信する手段が必要になります。

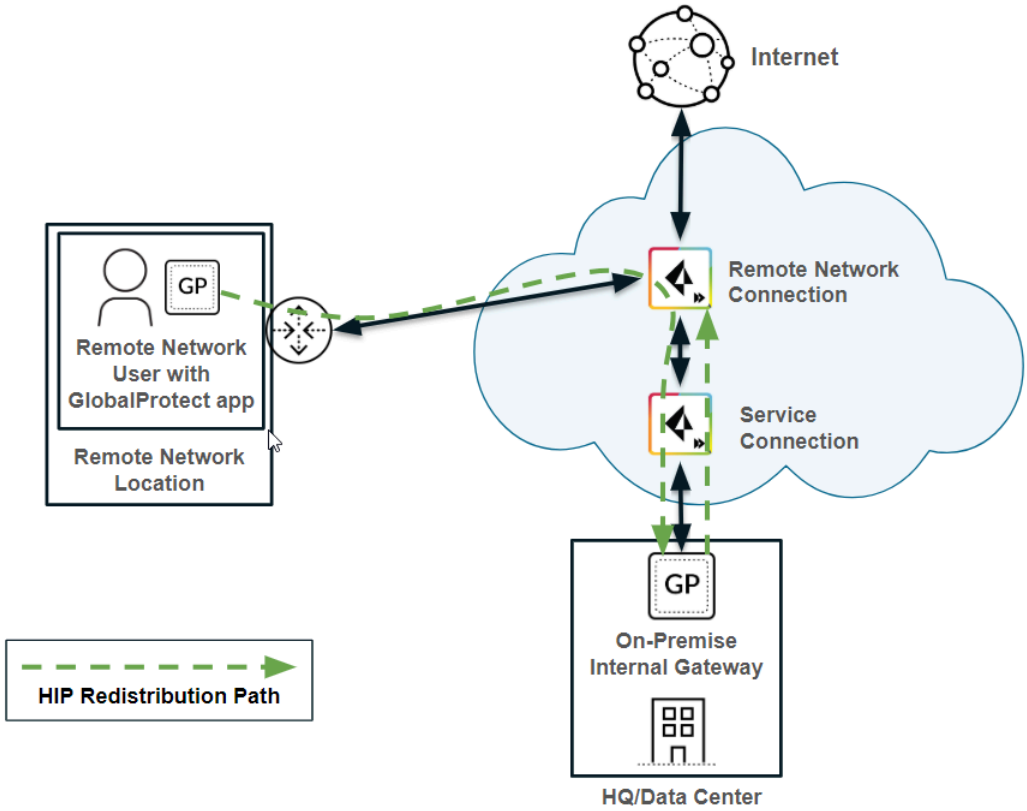
  リモートネットワーク接続でインターネットアクセスを行う、リモートネットワークロケーションのユーザーの例を次に示します。Prisma Accessで、リモートネットワークロケーションにおけるユーザーのインターネットアクセスを管理するには、**Remote_Network_Device_Group**または共有デバイスグループ内に作成されたセキュリティポリシーを使用します。ユーザーのリモートネットワークロケーションに適切にポリシーを適用するために、内部ゲートウェイからユーザーのHIP情報を取得するようにPrisma Accessを設定する必要があります。

  この例では、内部ホスト検出を使って内部ゲートウェイとして設定されている、本社/データセンターのGlobalProtectゲートウェイが、ユーザーのGlobalProtectアプリケーションから当該ユーザーのHIP情報を確認します。内部ゲートウェイは、ユーザーがリモートネットワー

©2025 Palo Alto Networks, Inc.

クロケーション内に存在していることを確認し、ユーザーからUser-IDとHIP情報を収集します。

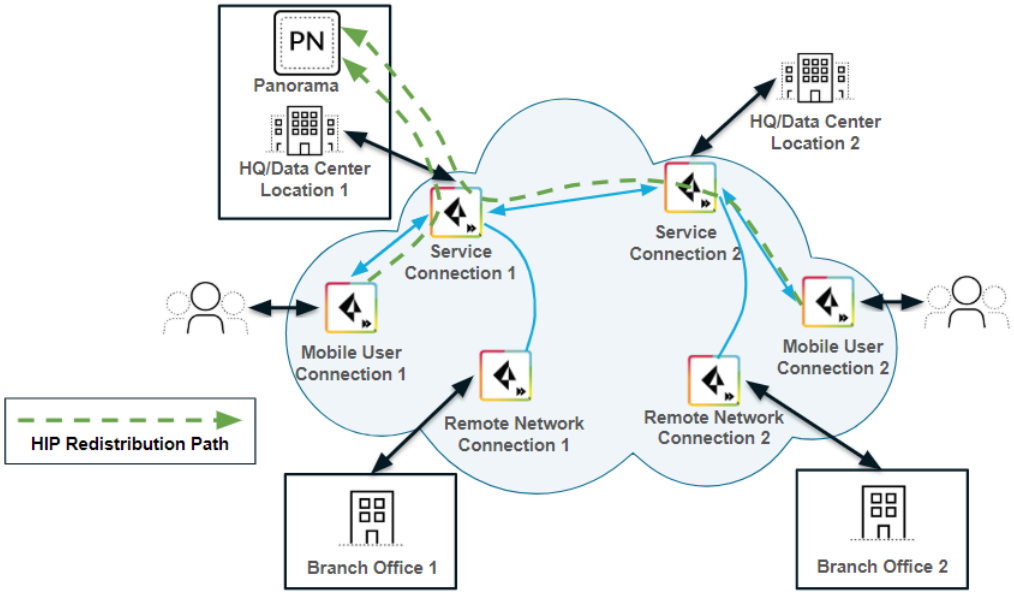
内部ゲートウェイからPrisma AccessにHIP情報を配信するには、PanoramaでUser-IDエージェントを作成し、内部ゲートウェイのIPアドレスをホストとして指定します。



- **Panorama**からの詳細**HIP**ログの参照–ユーザーがGlobalProtectアプリケーションを使ってログインすると、アプリケーションはPrisma AccessにHIP情報を送信します。PanoramaはHIP Match（HIPマッチ）ログの結果を参照するために、Strata Logging Serviceからログ結果を取得します(**[Monitor (監視)]** > **[Logs (ログ)]** > **[HIP Match (HIPマッチ)]**)。ただし、Prisma

©2025 Palo Alto Networks, Inc.

AccessからPanoramaにHIPレポートの詳細を再配信するようにPanoramaを設定しないと、詳細なHIPレポートを参照できません。

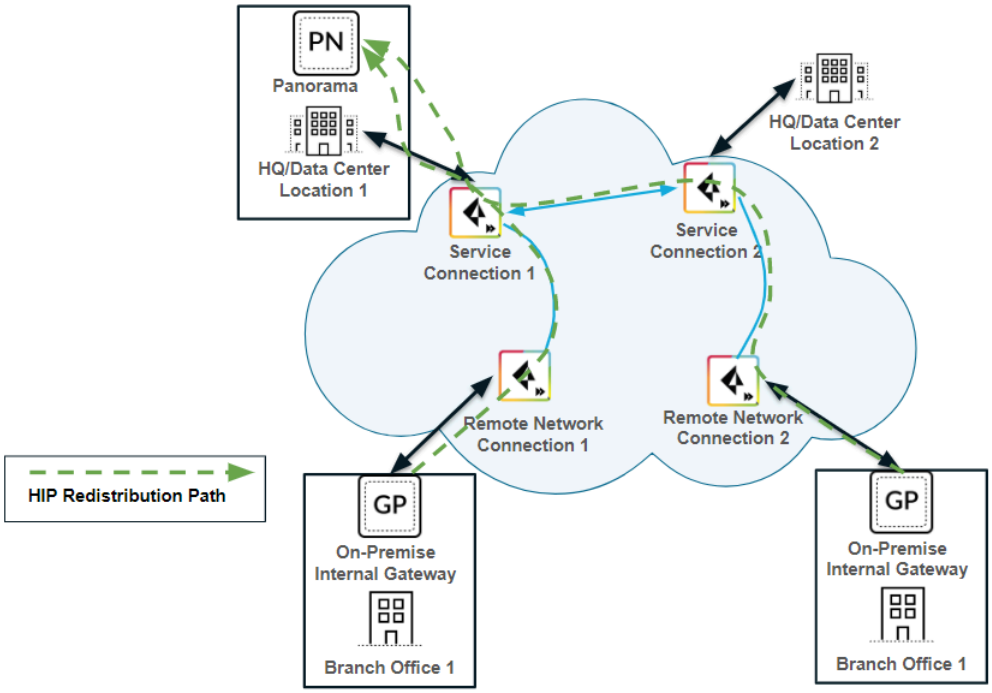


モバイルユーザーからPanoramaに詳細なHIP情報を再配信するために、PanoramaでUser-IDエージェントを作成して、**User-ID Agent Address**（ユーザーIDエージェントアドレス）（**Panorama** > **Cloud Services** > **Status** > **Network Details** > **Service Connection** > **User-ID Agent Address**）をUser-IDホストとして指定します。

オンプレミスゲートウェイをリモートネットワークロケーションの内部ゲートウェイとして設定している場合、リモートネットワークのユーザーのHIP情報をPanoramaに送信することもできます。この場合、PanoramaでUser-IDエージェントを作成して、リモートネットワークの**[EBGP Router**（**EBGP**ルーター）**]**アドレス（**[Panorama]** > **[Cloud Services (**クラウドサービス**)]** > **[Status (**ステータス**)]** > **[Network Details (**ネットワーク詳細**)]** > **[Remote Networks**

©2025 Palo Alto Networks, Inc.

(リモートネットワーク)] > [EBGP Router (EBGPルーター)]）をUser-IDホストとして指定します。



Prisma AccessでHIP再配信を有効にして設定します:

- Prisma AccessでHIP再配信を構成する

Prisma AccessでHIP再配信を構成する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Accessライセンス

エンドポイントにGlobalProtectアプリケーションがインストールされているモバイルユーザーがPrisma Accessに接続すると、Prisma AccessがエンドポイントのGlobalProtectアプリからユーザーのHIP情報を収集します。 これにより、HIPレポートがPrisma Accessで利用可能になります。

*HIP*の再配信を利用するには、ユーザーのエンドポイントに*GlobalProtect*アプリケーションがインストールされている必要があります。*Prisma Access*はClientless VPNをサポートしていますが、*Clientless VPN*ユーザーに*HIP*情報を再配信することはできません。

HIPの再配信は、モバイルユーザーとリモートネットワークのユーザーの両方に対して利用できます。ただし、リモートネットワークのユーザーの場合、オンプレミスゲートウェイがPrisma

©2025 Palo Alto Networks, Inc.

AccessにHIP情報を送信するために、内部ホスト検出を使って当該ユーザーが、組織ネットワークの内部であることを確認する必要があります。

*Prisma Access*で、モバイル ユーザー デプロイメント環境を設定する時に、内部ホスト検出を設定します。

一貫したポリシーの実施を保証するために、HIP再配布を使用すると、Prisma AccessがユーザーのHIP情報を配信内の他のPanoramaアプライアンス、ゲートウェイ、ファイアウォール、仮想システムに配信したり、場合によってはこれらのデバイスからPrisma AccessにHIP情報を配布したりすることができます。これにより、ユーザーのトラフィックに対して一貫したHIPベースのポリシーを適用することができます（インターネットトラフィックに対するポリシーや組織の本社またはデータセンターにある内部アプリケーションまたはリソースにアクセスするトラフィックに対するポリシーを含む）。PanoramaアプライアンスにHIP情報を再配信することで、そのアプライアンスからPrisma AccessユーザーのHIP情報の詳細を参照することもできます。

GlobalProtectの内部および外部ゲートウェイは、双方向HIP再配信をサポートしていないことに注意してください。したがって、ベストプラクティスは、Panoramaアプライアンスを再配信ポイントとして使用することです。このデプロイメントでは、内部および外部ゲートウェイを構成してHIPレポートをPanoramaに送信し、Panoramaがそれらをファイアウォールに転送して、環境全体で一貫したポリシーの適用を行うことができます。

- Strata Cloud Manager
- Panorama

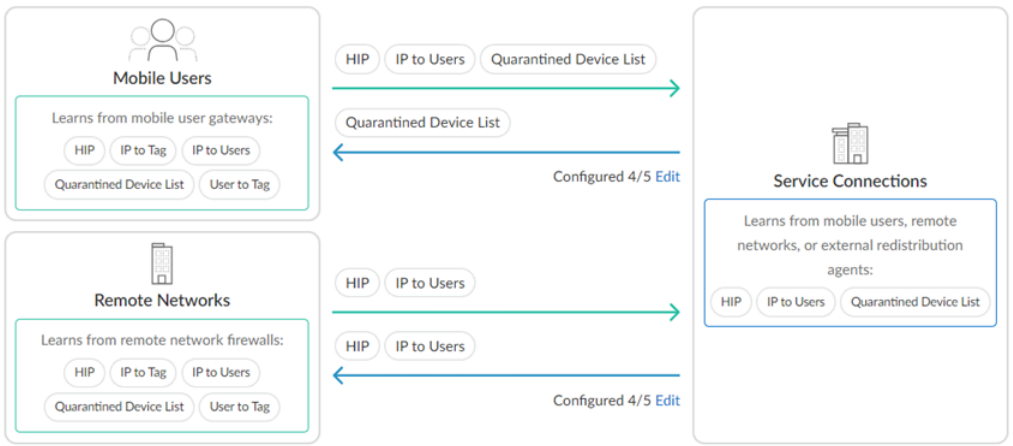
Prisma Accessで**HIP**再配布を構成する （**Strata Cloud Manager**）

HIPレポートの再配布は、**Strata Cloud Manager**ではデフォルトで有効になっています。再配布の詳細を表示するか、再配布を無効にするには、以下の手順に従います。

STEP 1 | **Strata Cloud Manager**で、 **Manage (管理) > Configuration (設定) > NGFW** と**Prisma Access > Identify Services (アイデンティティ サービス) > Identify Redistribution (ID再配布)**を選択します。

Prisma AccessID再配布の図には、モバイルユーザーとサービス接続間、およびリモートネットワークとサービス接続間のデフォルトのHIPレポート再配布設定が表示されます。

Prisma Access Identity Redistribution Diagram



 ©2025 Palo Alto Networks, Inc.

STEP 2 | セグメント間の再配布を無効にするには、[編集] をクリックし、関連するソース リモート ネットワークの横にある [編集] をクリックします。

STEP 3 | **HIP**を無効にします。

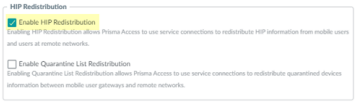
Prisma Accessで**HIP**再配信を構成する （**Panorama**）

HIP情報の収集と再配信をPrisma Accessに許可するには、以下の作業を行ってください。

STEP 1 | Prisma AccessにHIP情報の再配信を許可します。

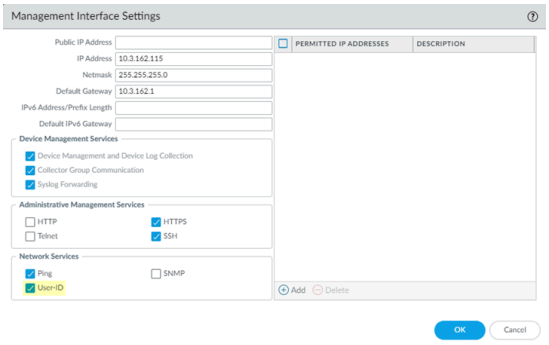
1. Panoramaで、**Panorama** > **Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Service Setup**（サービスのセットアップ）を選択します。
2. 設定を編集するには、歯車型アイコンをクリックします。
3. **Advanced**（詳細）タブで、**Enable HIP Redistribution**（**HIP**の再配信を有効にする）を選択します。

   HIPの再配信を有効にすると、Prisma AccessがGlobalProtectアプリケーションから受信したHIPレポートの、内部ファイアウォールやPanoramaへの再配信が有効になります。



STEP 2 | Prisma AccessからHIPレポートを受信するようにPanoramaを設定します。

1. **Panorama** > **Setup**（セットアップ） > **Interfaces**（インターフェース）の順に選択します。
2. **Management**（管理）インターフェースを選択します。
3. **User-ID**を選択します。



STEP 3 | Prisma AccessからUser-IDマッピングを収集するように、Panoramaを設定します。

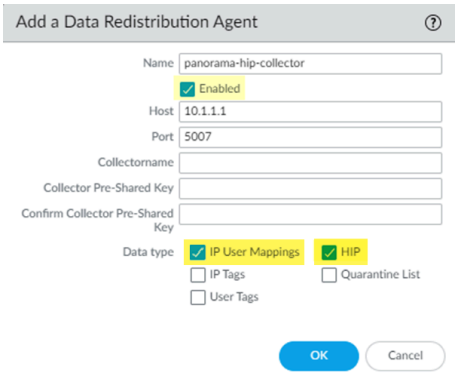
1. Prisma Accessを管理するパノラマから、以下を選択します。 **[Panorama]** > **[Data Redistribution (**データの再配布**)]** > **Agents (**エージェント**)** (Panorama 10.*x* アプライアンス向け) もしくは **Panorama** > **User Identification (**ユーザーID**)** > **User-ID Agents** (9.1.*x* Panoramaアプライアンス向け).
2. User-IDエージェントを**Add**（追加）して、それに**Name**（名前）を指定します。

 ©2025 Palo Alto Networks, Inc.

3. 収集するHIP情報のタイプに応じて、**Host**（ホスト）フィールドに次のいずれかの値を入力します。
   - モバイルユーザーのHIP情報を収集するには、**User-ID Agent Address**（ユーザーIDエージェントアドレス）（**Panorama** > **Cloud Services** > **Status** > **Network Details** > **Service Connection** > **User-ID Agent Address**）を入力します。
   - リモートネットワークロケーションのユーザーのHIP情報を、内部ゲートウェイで収集するには、内部ゲートウェイのIPアドレスを入力します。
   - リモートネットワーク接続のユーザーからHIP情報を収集するには、**EBGP Router**（EBGPルーター）アドレス（**Panorama** > **Cloud Services** > **Status** > **Network Details** > **Remote Networks** > **EBGP Router**）をUser-IDホストとして入力します。
4. Port（ポート）フィールドに、**5007**を入力します。

   デフォルトで、User-IDエージェントはポート5007で、HIP情報リクエストを待機します。

   ネットワークで*Prisma Access*と*Active Directory*(アクティブディレクトリ)サーバーまたは*User-ID*エージェント間の、このポートへのアクセスがブロックされていないことを確認してください。
5. PanoramaのUser-IDエージェントとの通信を有効にするには、**Enabled**（有効）を選択します。
6. **[IPユーザー マッピング]**と**[HIP]**を選択し、Panoramaがすべてのモバイル ユーザ拠点からIPアドレス - ユーザー名間マッピングおよびGlobalProtect HIPデータを受信できるようにします。
7. **OK** をクリックします。



STEP 4 | HIPレポート収集を設定する各サービス接続に対して、ステップ3を繰り返します。

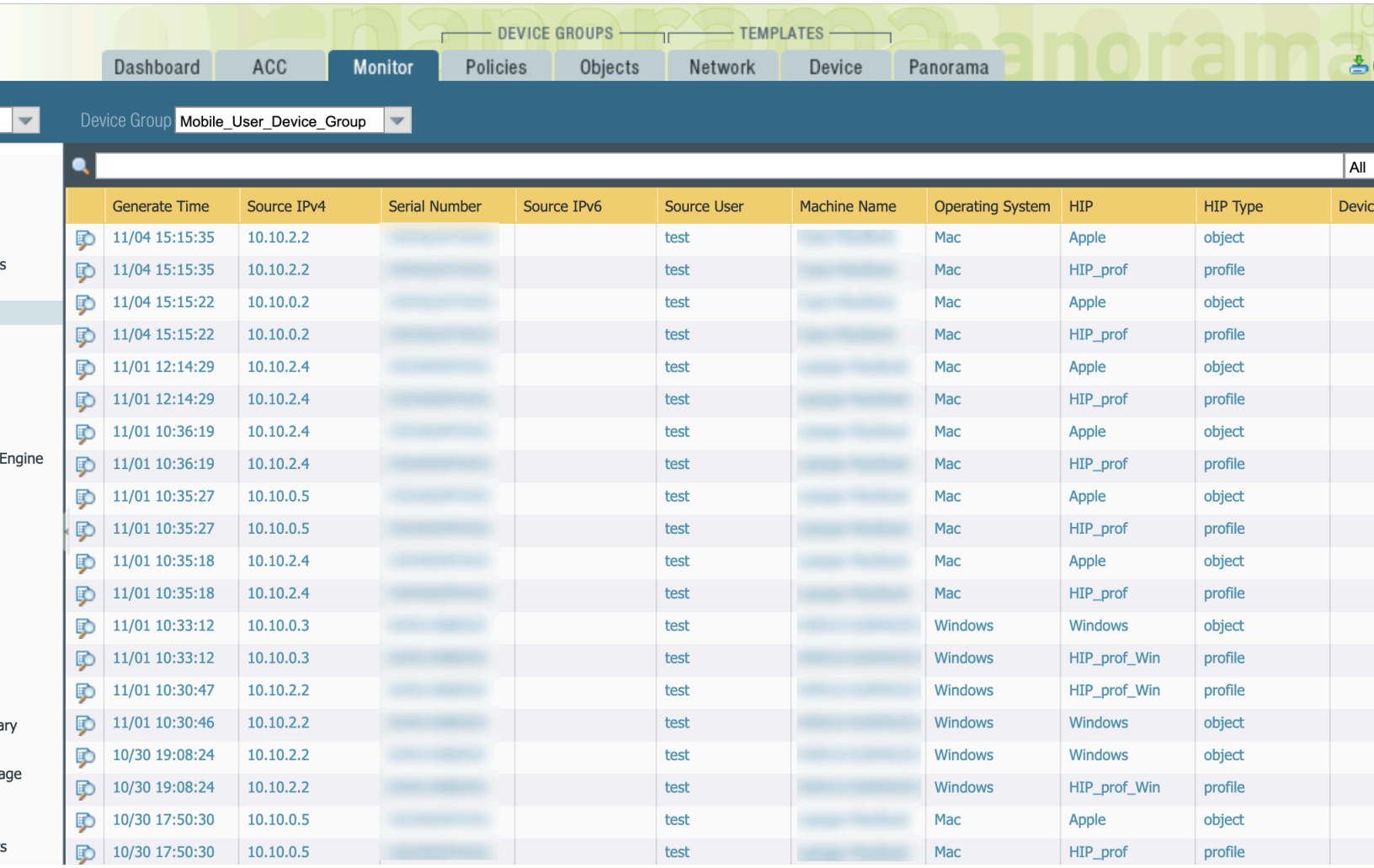
HIPレポートの表示

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

©2025 Palo Alto Networks, Inc.

Prisma AccessへのHIP情報の収集と再配信を行うようにPrisma Accessを設定したら、次のワークフローを使ってPanoramaでHIP情報を参照することができます。

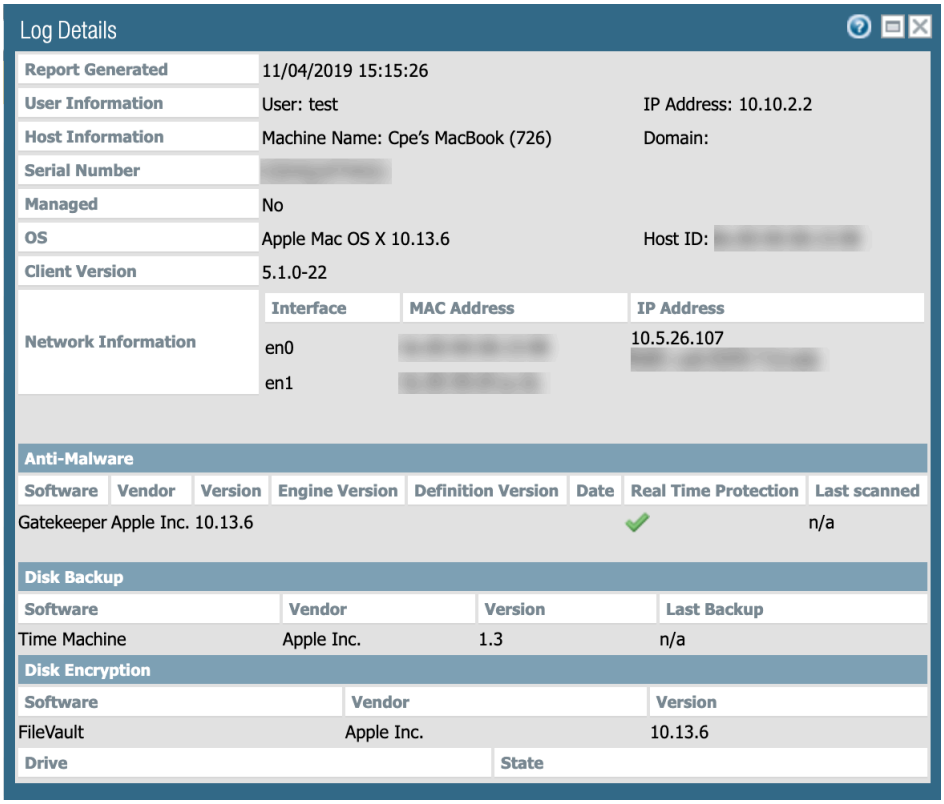
STEP 1 | HIP情報を参照するには、**Monitor**（監視） > **Logs**（ログ） > **HIP Match**（HIP照合）を選択します。



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 | レコードの左側にあるアイコンをクリックすると、詳細なHIP情報が表示されます。



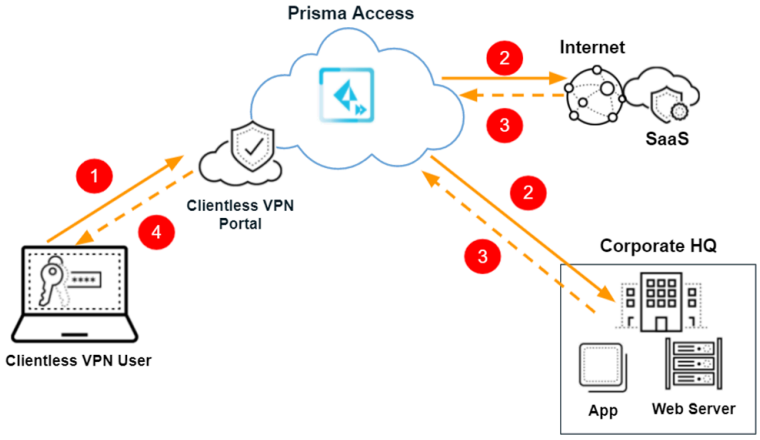
クライアントレスVPNでのGzipエンコーディングのサポート

どこで使用できますか?	何が必要ですか?
• Panorama	• Prisma Accessライセンス

GlobalProtect クライアントレス VPN を使用すれば、一般的なエンタープライズ Web アプリケーションに安全にリモート アクセスできます。Prisma Access クライアントレス VPN を使用すると、モバイル ユーザーは Gzip 圧縮された Web サイトにアクセスして、内部アプリケーションと SaaS アプリケーションの両方を使用できます。Gzip エンコーディングのサポートにより、HTTP ヘッダー内の Gzip エンコーディング要求がクライアントレス VPN ポータルによって受け入れられることが保証されます。これにより、クライアントレス VPN ポータルからアクセスしたときに、Gzip 圧縮された Web ページのコンテンツが正しくレンダリングされるようになります。

以下の図は、Prisma Accessのクライアントレス VPN を通じて、ユーザーが内部および SaaS アプリケーションにアクセスできるようにするための拡張サポートを示しているものです。

©2025 Palo Alto Networks, Inc.



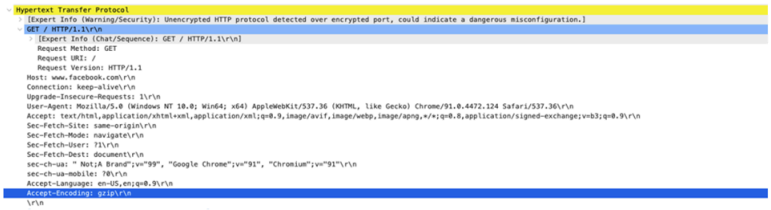
クライアントレス VPN は、クライアントからの HTTP 要求とアプリからの対応する応答に基づいて、Gzip エンコーディングを使用するかどうかを決定できます。**gzip** 値は、Clientless VPN によって受け入れられるように、Accept-Encoding ヘッダー値の 1 つとして含める必要があります。

たとえば、クライアントレス VPN が Gzip エンコーディングを使用する場合の次のシナリオを検討してください。

1. ブラウザは、次の例に示すように、 Accept-Encoding ヘッダーの値を **gzip**、**deflate**、**br**に設定して、Web サイトに HTTP 要求を送信します。



2. Prisma Accessのクライアントレス VPN ポータルは、ブラウザから送られてくる HTTP リクエストを解析し、以下の例に示すように、Gzip エンコーディングのサポートを示す Accept-Encoding ヘッダー値を **gzip** に設定します。

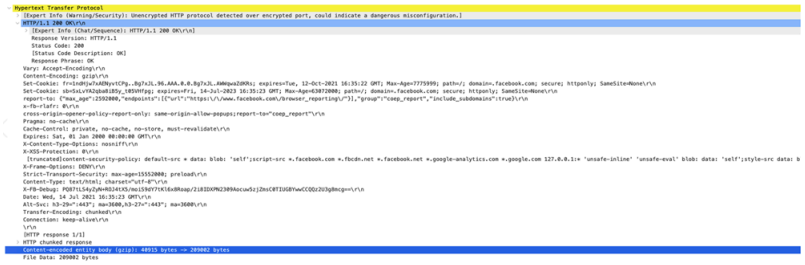


 ©2025 Palo Alto Networks, Inc.

3. Web サイトが HTTP 応答で Gzip エンコーディングをサポートしている場合、次の例に示すように、Web サイトはコンテンツが Gzip 形式であることを示す Content-Encoding ヘッダーを **gzip** として送信します。



4. クライアントレス VPN は、次の例に示すように、Web サイトから受信した応答を同じ形式で Web ブラウザーに転送します。



クライアントレス VPN が受信した HTTP 要求にエンコード方式の 1 つとして **gzip** が含まれていない場合、クライアントレス VPN は Gzip エンコードも受け入れません。

Prisma Accessでのトラフィック レプリケーション

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessライセンス ❑ トラフィックレプリケーションアドオンライセンス ❑ トラフィック レプリケーションには、モバイルユーザー トラフィック用に最低4.1のPrisma Accessリリースが必要です。 ❑ トラフィック レプリケーションには、モバイル ユーザーとリモート ネットワークの両方のトラフィック用に最低5.0 Prisma Access リリースが必要です。 ❑ リモート ネットワークの TLS 1.3 サポートには、最低 Prisma Access 5.2 リリースが必要です。

©2025 Palo Alto Networks, Inc.

どこで使用できますか?	何が必要ですか?
	❑ PubSubには最低限 Prisma Access 5.2.1 リリースが必要です。

オンプレミスのネットワーク レコーダーは、組織がフォレンジック分析や侵害分析を実行するための強力なツールです。オンプレミスのトポロジでは、このような帯域外分析に使用されるトラフィックのコピーを配信するタップ ポート、スパン ポート、またはパケット ブローカーの並列インフラストラクチャを実装するのが一般的です。

しかし、ハイブリッドワークとクラウドの導入が加速するにつれ、組織はこれらの課題に対処するために SASE アーキテクチャに移行しています。SASE クラウド セキュリティ ソリューションに準拠すると、これらのフォレンジック分析ツールに盲点が生じ、リモート ユーザーから SaaS アプリケーションへのトラフィックのコピーが利用できなくなります。

Prisma Access トラフィックのレプリケーションは、Prisma Accessを通過しているトラフィックのコピーを利用できるようにすることで、SASEアーキテクチャを含むフォレンジックおよび事後分析に完全な可視性を追加します。トラフィック レプリケーションが役立つ一般的なユースケースは次のとおりです。

- パケットキャプチャが攻撃と使用されたアプローチの反駁の余地のない証拠を提供するフォレンジックおよび脅威ハンティング分析
- パケットキャプチャを一定期間保存する必要がある特定の規制コンプライアンスを満たす
- 組織が投資したサードパーティの優先ツールを引き続き使用する
- パケットレベルのネットワークとアプリケーションのパフォーマンスのデバッグ

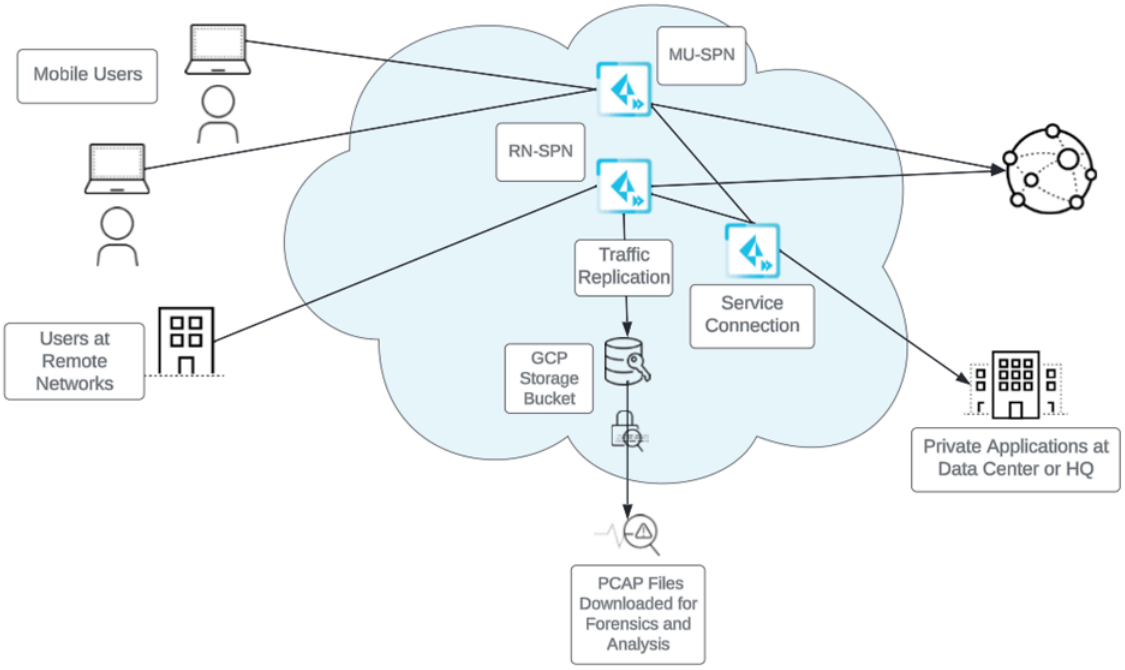
トラフィック レプリケーションは、ユーザーの実際のトラフィックのパケット キャプチャ (pcaps) へのアクセスを提供します。これにより、複数のセッションにまたがる可能性のある脅威を検出して修復したり、異常な動作を識別して対応したりして、リスクを軽減し、企業を安全に保つことが可能になります。

トラフィックのレプリケーションを有効にすると、Prisma Accessは、この機能が有効になっている各Prisma Accessコンピュートロケーションに専用のクラウドストレージバケットを作成し、Prisma Accessを通過するトラフィックのレプリカを含むpcapファイルを継続的に保存します。

新しい pcap ファイルがストレージ バケットにアップロードされたときに通知を受け取るには、Pub/Sub 通知をサブスクライブします。新しい pcap ファイルに Pub/Sub 通知を使用すると、バケットに新しいフォルダーや新しいファイルが追加されたときに通知するツールを開発する必要がなくなります。

これらのストレージ バケットへの読み取り専用権限を共有し、pcap ファイルへの安全なアクセスを可能にするために使用する Google Cloud サービス アカウント を提供する必要があります。Prisma Accessで証明書を介して共有される公開鍵を含む、静止時のpcapファイルの追加暗号化が適用されます。元の pcap ファイルを復号化して復元するための秘密鍵を持っているのはあなただけです。

©2025 Palo Alto Networks, Inc.



トラフィックレプリケーションの前提条件

トラフィック レプリケーションの構成を開始する前に、次の前提条件に注意してください。

- Google Cloud Platform (GCP) に サービス アカウント を作成していることを確認してください。
- SSL復号化に使用するために、[オブジェクト] > [証明書管理] > [証明書] > [カスタム証明書] > [生成] ページで証明書を介して共有される公開キーを作成したことを確認します。
- 推奨されるアーキテクチャでは、各ストレージ バケットから pcap ファイルを読み取るコンピューティングまたはサービスが、バケットの読み取り元と同じ GCP リージョンに存在する必要があります。別の GCP リージョンまたは GCP クラウド外部のストレージ バケットから pcap ファイルを読み取ることはできるかもしれませんが、これらはサポートされているデプロイメント モデルではありません。

トラフィック複製ガイドライン

トラフィックのレプリケーションについては、次のガイドラインに従ってください。

- **TLS** サポート- モバイル ユーザーの展開で使用されるトラフィック レプリケーションでは TLS 1.2 がサポートされ、リモート ネットワークの展開で使用されるトラフィック レプリケーションでは TLS 1.2 および 1.3 がサポートされます。
- **IPSec** トンネル アルゴリズム- モバイル ユーザーおよびリモート ネットワーク展開でサポートされているすべての IPSec トンネル アルゴリズムは、トラフィック レプリケーションでもサポートされます。

トラフィック レプリケーションを設定する方法については、以下をご覧ください。

- Strata Cloud Manager
- Panorama

©2025 Palo Alto Networks, Inc.

Prisma Accessでのトラフィックの複製 (Strata Cloud Manager)

トラフィック レプリケーションを構成し、パケット キャプチャ (pcap) ファイルにアクセスするには、次の手順を実行します。

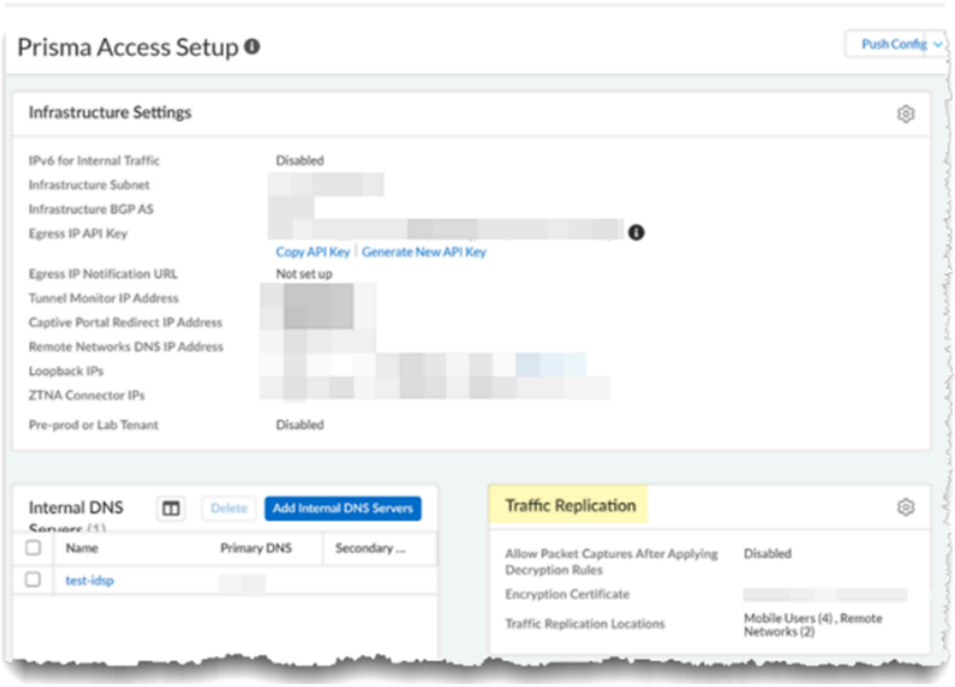
STEP 1 | トラフィック レプリケーションを有効にしたい場所にMobile Users—GlobalProtectをオンボーディングして構成し、変更をコミットしてプッシュします。

Mobile Users—GlobalProtectロケーションを有効にしてから、それらのロケーションのトラフィックレプリケーションを有効化する必要があります。

©2025 Palo Alto Networks, Inc.

STEP 2 | （任意）パケットキャプチャに SSL復号化を適用します。

1. Prisma Access (Managed by Strata Cloud Manager)へ移動して、 **[Prisma Access** 設定] > **Prisma Access** >]トラフィック レプリケーション] 選択し、歯車をクリックして [設定]を編集します。

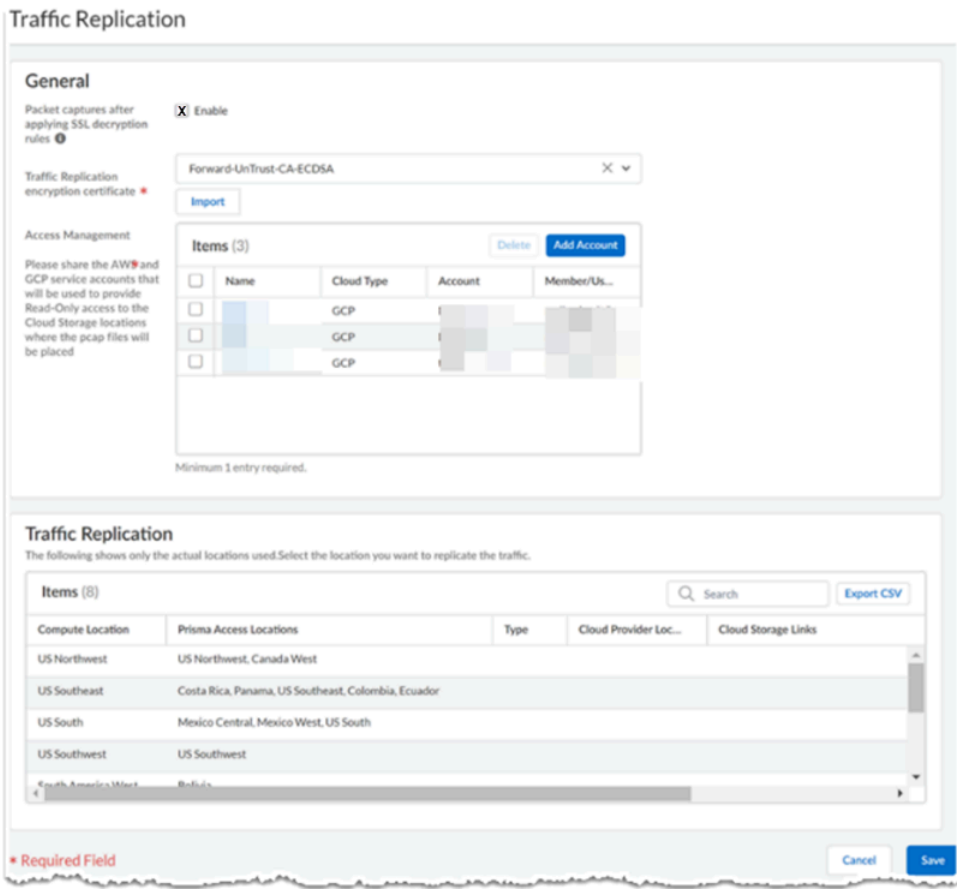


2. **SSL** 復号化ルールを適用した後にパケット キャプチャ を有効にして、既に構成されている SSL 復号化ポリシーを pcap ファイルに適用します。

   インライン SSL 復号化ポリシーに一致するトラフィックのみが復号化されます。

   このオプションを選択すると、PCAP ファイルはデプロイメントで指定したのと同じ復号ルールを使用します。このオプションを選択解除すると、設定した復号ルールに関係なく、PCAP ファイルの復号化は実行されません。

©2025 Palo Alto Networks, Inc.



STEP 3 | トラフィック レプリケーションの暗号化証明書の場合は、[オブジェクト] > [[証明書管理] > [証明書] > [カスタム証明書] > [生成] ページで追加した証明書を選択するか、SSL復号化に使用する証明書をインポートします 。

証明書は公開鍵と秘密鍵で構成されています。パブリックキーをPrisma Accessにアップロードします。プライベートキーは保持し、圧縮された PCAP ファイルをストレージバケットからダウンロードするときに復号化に使用します。これにより、PCAP ファイルが保存されているストレージバケットにアクセスできるのは組織だけであることを保証できます。

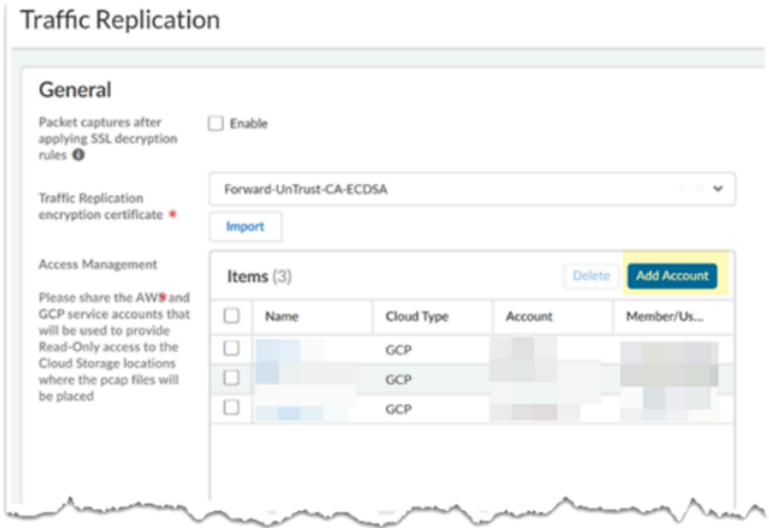
STEP 4 | ステップ 1で作成した GCP サービス アカウントを構成します。

トラフィックレプリケーションは GCP アカウントでのみサポートされています。このサービスアカウントは、トラフィックの複製を有効にした場所にある PCAP ファイルが保存されているストレージバケットへの読み取り専用アクセスを共有するために使用されます。通常のGCPサービスアカウント作成手順を使用して、GCPアカウントにこれらのサービスアカウントを作成することができます。どのユーザーがこれらのサービスアカウントにアクセスで

©2025 Palo Alto Networks, Inc.

きるかを管理するのはお客様の責任です。PCAPファイルと秘密鍵の両方にアクセスできるユーザーは、PCAPファイルにアクセスできます。

1. アクセス管理 領域で、 アカウントの詳細を追加して 、pcap ファイルが保存されているストレージ バケットへの読み取り専用アクセスを共有します。



2. 次のパラメータを入力します。
   - アカウントに一意のアカウント名を指定します。
   - アカウントの **Type** として **GCP** を指定します。
   - 作成した GCP サービスアカウントのアカウント情報を指定します。
   - GCP サービスアカウントのメンバー/ユーザー名を入力します。

©2025 Palo Alto Networks, Inc.

STEP 5 | （任意）バケットに新しいフォルダまたは新しいファイルが追加されたときに通知するPub/Sub 通知を追加する場合は、Google Cloudサービスアカウントで Pub/Sub 通知を設定します。

Prisma Accessはテナント内のすべての場所に対して、テナントごとに 1 つの Pub/Sub チャネルを作成します。

Pub/Sub 通知は*Prisma Access 5.2* 以降でサポートされています。既存のアカウントをお持ちで、*Pub/Sub* 通知を追加したい場合は、*Prisma Access 5.2* にアップグレードし、次のオプションのいずれかを選択して *Pub/Sub* 通知を追加します。

- *Prisma Access*で設定済みの既存の*Google*クラウド サービス アカウントを修正します。
- 既存のサービスアカウントに新しいアカウントを追加し、そのアカウントを*Prisma Access*設定で指定します。

  新しいアカウントを追加する場合、既存のアカウントのトラフィック複製を無効にし、新しいアカウントのトラフィック複製を有効にする必要があります。
- 既存の場所でのトラフィックレプリケーションを無効または有効にします。

Prisma Access `panw-traffic-replication-file-notifications-`という見出しの付いた Pub/Sub メッセージを送信します。ここでの*<tenantid>*は通知を送信しているテナントの*<tenantid>*ID です。メッセージは次の形式です。

```
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": "xxxxxxxxxxxxxxxx",
 "objectId": "instance-group-xxxxxxx/12345678_190000_xxxxx.zip",
 "payloadFormat":"NONE" } }
```

ここで:

- `objectGeneration (オブジェクト生成)`は、変更されたオブジェクトの世代番号です。
- `ObjectId (オブジェクトID)` は変更されたオブジェクトの名前です。

 ©2025 Palo Alto Networks, Inc.

STEP 6 | 1 つ以上のモバイル ユーザーの場所のトラフィックのレプリケーションを構成します。

1. **[トラフィック レプリケーション]** 領域で、トラフィック レプリケーションを有効にする場所を選択し、**[モバイル ユーザー]**を選択します。

   Prisma Accessロケーションに関連付けられているコンピュートロケーションを選択します。トラフィックの複製は、すべてのモバイルユーザ（選択した場所に接続しているクライアント）に対して有効です。

STEP 7 | 設定を保存します。

STEP 8 | 変更をコミット、プッシュ配信します。

1. **[Manage (管理)]** > **[Operations (オペレーション)]** > **[Push Config (設定をプッシュ)]**を選択します。
2. **[Push Scope (プッシュ スコープ)]**で モバイル ユーザー コンテナ を選択し、 プッシュ構成 を選択して変更を プッシュします 。
3. プッシュ ターゲットを確認して、 プッシュします。

STEP 9 | トラフィックレプリケーションのステータスを確認するには、**[Prisma Access**のセットアップ**]** > **Prisma Access** > **[**トラフィック レプリケーション**]**へ移動します。

STEP 10 | pcap ファイルをダウンロードします。

クラウドストレージリンクを使用して、GCP ストレージバケット内の PCAP ファイルにアクセスします。

- これらのストレージバケットは、他の GCP ストレージバケットと同じ通常の操作、コマンド、クエリをサポートします。
- PCAP データは最大 72 時間ダウンロードできます。72 時間が経過すると、ファイルは完全に削除されます。
- ファイルは公開鍵を使用して暗号化されます。
- 最大ファイルサイズは 200 MB または 5 分のパケットキャプチャ時間のうち、どちらか小さい方です。

1. 「`gsutil ls gs://<storage_bucket_link>/`」と入力して、サービス内のファイルを一覧表示します。ここでの*<storage_bucket_link>*は、ファイルが保存されている GCP サービスアカウントのストレージリンクです。
2. `gsutil cp gs://<storage_bucket_link>/<file_name> <destination folder>`と入力して、サービスアカウントからファイルをダウンロードします。ここでの、
   - *<storage_bucket_link>* は、ファイルが保存されている GCP サービスアカウントのストレージリンクです。
   - *<file_name>* は PCAP ファイルの名前です。
   - *<destination folder>* は、PCAP ファイルをダウンロードするフォルダです。
3. ダウンロードしたファイルを解凍します。
4. ダウンロードしたファイルを復号化します。

 ©2025 Palo Alto Networks, Inc.

Prisma Accessでのトラフィックの複製 (Panorama)

トラフィック複製を設定し、PCAP ファイルにアクセスするには、次の手順を実行します。

STEP 1 | Mobile Users—GlobalProtect（モバイル ユーザー用にトラフィック レプリケーションを設定する場合）、リモート ネットワーク（リモート ネットワーク用にトラフィック・レプリケーションを設定する場合）、または両方（モバイル ユーザーとリモート ネットワークの両方にトラフィック・レプリケーションを設定する場合）をオンボーディングし、設定します。

STEP 2 | （任意）パケットキャプチャに SSL復号化を適用します。

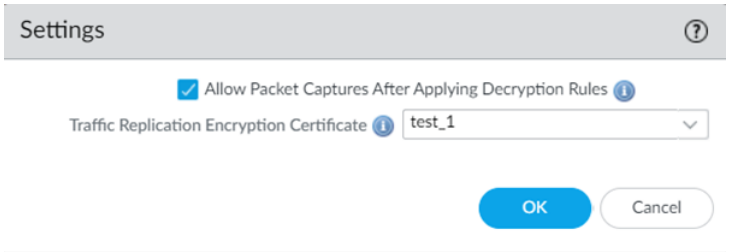
1. **[Panorama] > [Cloud Services**（クラウドサービス）**] > [Configuration**（設定）**] > [Traffic Replication**（トラフィック レプリケーション）**]**の順に移動し、歯車型アイコンをクリックして[設定]を編集します。
2. PCAP ファイルに設定済みの SSL復号化ポリシーを適用するには、[復号ルールを適用した後にパケットキャプチャを許可する] を選択します。

   このオプションを選択すると、PCAP ファイルはデプロイメントで指定したのと同じ復号ルールを使用します。このオプションを選択解除すると、設定した復号ルールに関係なく、PCAP ファイルの復号化は実行されません。

STEP 3 | **Mobile_User_Template**（モバイルユーザー導入の場合）または**Remote_Network_Template**（リモートネットワーク導入の場合）で、先の手順で作成した**Traffic Replication Encryption Certificate (**トラフィック レプリケーション暗号化証明書**)**（公開鍵）を選択し、SSL復号化に使用します。

このステップは必須です。**Mobile_User_Template** または **Remote_Network_Template** の**[Device (**デバイス**)] > [Certificate Management (**証明書管理**)] > [Certificates (**証明書**)] > [Device Certificates (**デバイス証明書**)]**エリアに追加した証明書を選択できます。モバイルユーザーとリモートネットワークの両方でトラフィックの複製を有効にする場合は、証明書を **Mobile_User_Template** と **Remote_Network_Template** の両方に配置してください。。

証明書は公開鍵と秘密鍵で構成されています。パブリックキーをPrisma Accessにアップロードします。プライベートキーは保持し、圧縮された PCAP ファイルをストレージバケットからダウンロードするときに復号に使用します。これにより、PCAP ファイルが保存されているストレージバケットにアクセスできるのは組織だけであることを保証できます。



STEP 4 | **Configuration (**設定**)**エリアでロケーションを選択し、トラフィックのレプリケーションを有効にするロケーションを選択し、**MU-GP**、**RN**、または両方を選択することで、1つまた

©2025 Palo Alto Networks, Inc.

は複数のMobile Users-GlobalProtectロケーション、リモートネットワークロケーション、またはその両方にトラフィックのレプリケーションを設定します。

Prisma Accessロケーションに関連付けられているコンピュートロケーションを選択します。トラフィックの複製は、選択した場所に接続しているすべてのモバイルユーザ（GlobalProtectクライアント、リモートネットワークユーザ、またはその両方）に対して有効です。

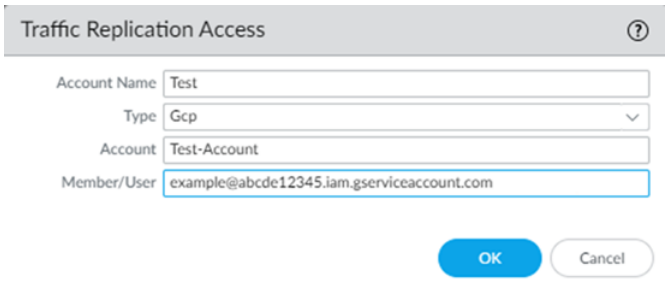


STEP 5 | トラフィックレプリケーションパケットキャプチャ (PCAP) データにアクセスできるアカウントを追加します。

このサービスアカウントは、トラフィックの複製を有効にした場所にある PCAP ファイルが保存されているストレージバケットへの読み取り専用アクセスを共有するために使用されます。通常のGCPサービスアカウント作成手順を使用して、GCPアカウントにこれらのサービスアカウントを作成します。どのユーザーがこれらのサービスアカウントにアクセスできるかを管理するのはお客様の責任です。PCAPファイルと秘密鍵の両方にアクセスできるユーザーは、PCAPファイルにアクセスできます。

1. **Traffic Replication Access (**トラフィック レプリケーション アクセス**)**エリアで、アカウントを追加します。
2. 次のパラメータを入力します。
   - アカウントに一意のアカウント名を指定します。
   - アカウントの **Type** として **Gcp** を指定します。

     トラフィックレプリケーションは GCP アカウントでのみサポートされています。
   - 作成した GCP サービスアカウントのアカウント情報を指定します。
   - GCP サービスアカウントのメンバー/ユーザー名を入力します。



 ©2025 Palo Alto Networks, Inc.

STEP 6 | （任意）バケットに新しいフォルダまたは新しいファイルが追加されたときに通知するPub/Sub 通知を追加する場合は、Google Cloudサービスアカウントで Pub/Sub 通知を設定します。

Prisma Accessはテナント内のすべての場所に対して、テナントごとに 1 つの Pub/Sub チャネルを作成します。

Pub/Sub 通知は*Prisma Access 5.2* 以降でサポートされています。既存のアカウントをお持ちで、*Pub/Sub* 通知を追加したい場合は、*Prisma Access 5.2* にアップグレードし、次のオプションのいずれかを選択して *Pub/Sub* 通知を追加します。

- *Prisma Access*で設定済みの既存の*Google*クラウド サービス アカウントを修正します。
- 既存のサービスアカウントに新しいアカウントを追加し、そのアカウントを*Prisma Access*設定で指定します。

  新しいアカウントを追加する場合、既存のアカウントのトラフィック複製を無効にし、新しいアカウントのトラフィック複製を有効にする必要があります。
- 既存の場所でのトラフィックレプリケーションを無効または有効にします。

Prisma Access `panw-traffic-replication-file-notifications-`という見出しの付いた Pub/Sub メッセージを送信します。ここでの*<tenantid>*は通知を送信しているテナントの*<tenantid>*ID です。メッセージは次の形式です。

```
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": "xxxxxxxxxxxxxxxx",
 "objectId": "instance-group-xxxxxxx/12345678_190000_xxxxx.zip",
 "payloadFormat":"NONE" } }
```

ここで:

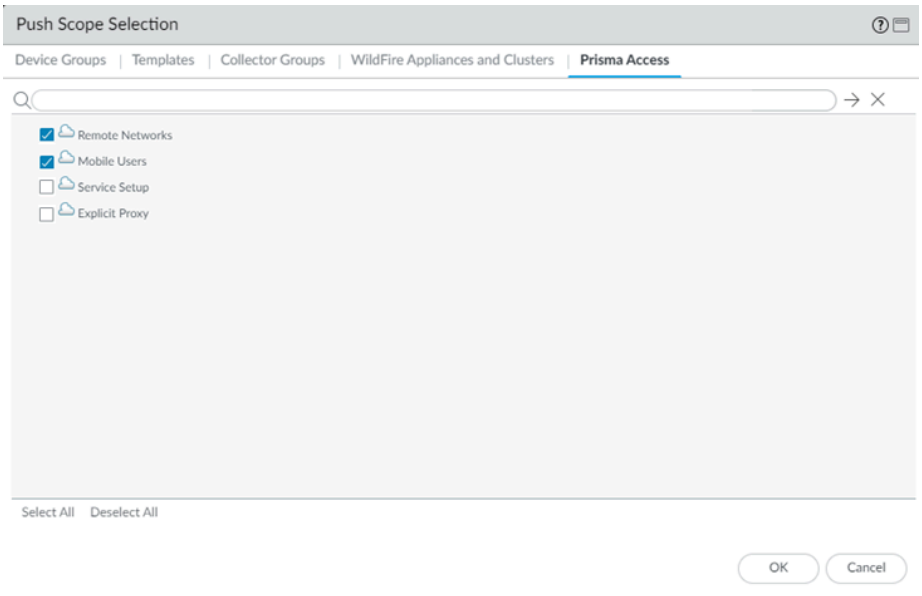
- `objectGeneration (オブジェクト生成)`は、変更されたオブジェクトの世代番号です。
- `ObjectId (オブジェクトID)` は変更されたオブジェクトの名前です。

©2025 Palo Alto Networks, Inc.

STEP 7 | 変更をコミットしてプッシュします。**[Push Scope (プッシュ範囲)]**で**[**モバイルユーザー**]**（モバイルユーザー配置の場合）、**[**リモートネットワーク**]**（リモートネットワーク配置の場合）、またはその両方が選択されていることを確認します。

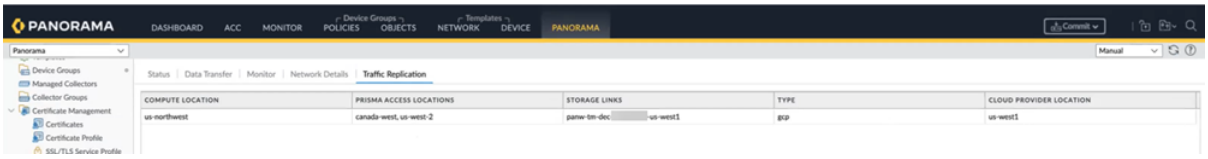
1. **Commit**（コミット） > **Commit and Push**（コミットしてプッシュ）をクリックします。
2. 選択項目を編集し、**Prisma Access**タブで**Push Scope (**プッシュ範囲**)**に**Mobile Users (**モバイルユーザー**)**と**Remote Networks (**リモートネットワーク**)**がことを確認し、**OK**をクリックします。

   プッシュ範囲が自動的に選択されない場合があります。



3. **[Commit and Push (**コミットしてプッシュ**)]** をクリックします。

STEP 8 | **Panorama** > **Cloud Services (**クラウドサービス**)** > ステータス > **Traffic Replication (**トラフィックレプリケーション**)**に移動して、トラフィック レプリケーションのステータスを確認します。



ストレージリンク はPCAP ファイルにアクセスできる GCP ストレージバケットの名前で、クラウドプロバイダーロケーションはGCP インスタンスがオンボーディングされる場所です。

 ©2025 Palo Alto Networks, Inc.

STEP 9 | 自分だけが所有する秘密鍵を使用して PCAP ファイルをダウンロードします。

ストレージリンクを使用して、GCP ストレージバケット内の PCAP ファイルにアクセスします。

- これらのストレージバケットは、他の GCP ストレージバケットと同じ通常の操作、コマンド、クエリをサポートします。
- PCAP データは最大 72 時間ダウンロードできます。72 時間が経過すると、ファイルは完全に削除されます。
- ファイルは公開鍵を使用して暗号化されます。
- 最大ファイルサイズは 200 MB または 5 分のパケットキャプチャ時間のうち、どちらか小さい方です。

1. 「`gsutil ls gs://<storage_bucket_link>/`」と入力して、サービス内のファイルを一覧表示します。ここでの*<storage_bucket_link>*は、ファイルが保存されている GCP サービスアカウントのストレージリンクです。
2. `gsutil cp gs://<storage_bucket_link>/<file_name> <destination folder>`と入力して、サービスアカウントからファイルをダウンロードします。ここでの、
   - *<storage_bucket_link>* は、ファイルが保存されている GCP サービスアカウントのストレージリンクです。
   - *<file_name>* は PCAP ファイルの名前です。
   - *<destination folder>* は、PCAP ファイルをダウンロードするフォルダです。
3. ダウンロードしたファイルを解凍します。
4. 自分だけが所有する秘密鍵を使用して、ダウンロードしたファイルを復号化します。

©2025 Palo Alto Networks, Inc.

Prisma Accessリモートネットワークの高度なデプロイメント:

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

以下のセクションでは、Prisma Accessリモート ネットワークで利用可能な高度なデプロイメントについて説明します：

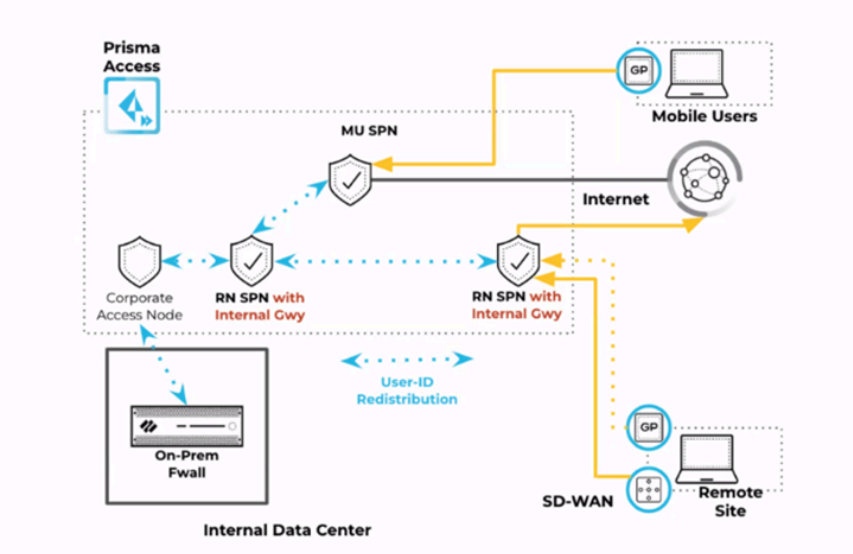
- リモートネットワークのロケーションへの安全なインバウンドアクセスの提供
- リモートサイト向けの高帯域幅ネットワークの作成

Prisma Access 内部ゲートウェイ

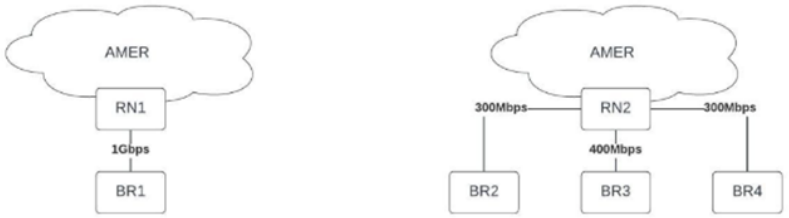
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Accessとモバイルユーザーライセンス ❑ Minimum Required Prisma Access Version:5.1 ❑ Prisma Access (Managed by Panorama)に最低限必要なデータプレーンバージョン:10.2.4 ❑ 最低限必要なGlobalProtect Clientのバージョン:6.0

以前は、Prisma AccessリモートネットワークでGlobalProtectクライアントソフトウェアを実行しているホストのIPユーザー マッピングとHIPを生成するには、内部ゲートウェイとしてオンプレミスのNGFWをデプロイする必要がありました。このソリューションはクラウドネイティブではありません。Prisma Accessクラウドネイティブの内部ゲートウェイを使用すると、オンプレミスの内部ゲートウェイを使用する必要がなくなり、Prisma Access内部ゲートウェイがリモートネットワークでIPユーザー マッピングとHIPをローカルに生成します。リモートネットワークは、他のファイアウォールから学習するのではなく、ポスチャチェックにローカルデータベースのIPユーザー マッピングやHIPを使用します。

©2025 Palo Alto Networks, Inc.

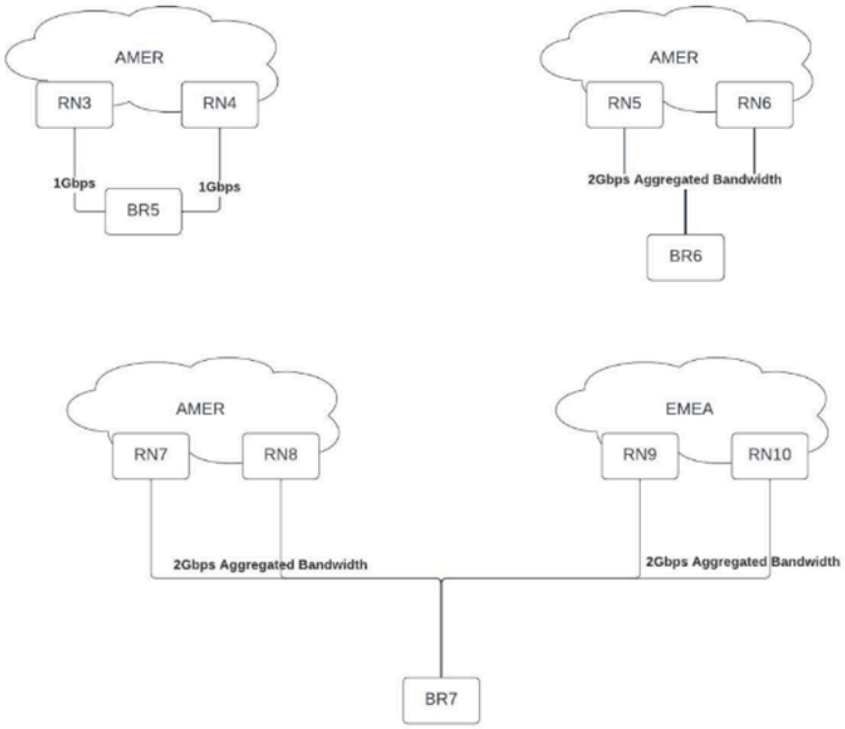


リモートサイトに複数のリモートネットワークサイト (たとえば、アクティブ/アクティブトンネル) または高帯域幅サイトへの複数のIPsecトンネルがある場合は、内部ゲートウェイをデプロイできないことに注意してください。次の図は、内部ゲートウェイ デプロイメントでサポートされる環境の例を示しています。



次の図は、内部ゲートウェイがサポートされていないデプロイメントの例を示しています。

 ©2025 Palo Alto Networks, Inc.



Prisma Access内部ゲートウェイをセットアップする前に、モバイル ユーザーをオンボー ドします。

- Strata Cloud Manager
- Panorama

Prisma Access 内部ゲートウェイ（Strata Cloud Manager）

Prisma Access内部ゲートウェイを設定するために、次の手順を完了してください。

STEP 1 | Strata Cloud Managerで、GlobalProtectをセットアップし、 アプリ設定を追加し、 リモート ネットワークをオンボードします。

現時点では内部ホスト検出と内部ゲートウェイ構成が存在しないことに注意してください。

STEP 2 | **[リモートネットワークのDNS IPアドレス]を、[Workflows (ワークフロー)] > [Prisma Accessセットアップ] > Prisma Accessからメモしてください。**

STEP 3 | **Gateway FQDN (ゲートウェイFQDN)をメモしてください。[Workflows (ワークフロー)] > [Prisma Accessセットアップ] > [GlobalProtect] > [Infrastructure (インフラストラクチャ)] > [Infrastructure Settings (インフラストラクチャ設定)] > [Gateway FQDNs (ゲートウェイFQDN)]から確認できます。**

STEP 4 | **Workflows (ワークフロー) > [Prisma Accessセットアップ] > Remote Networks (リモートネットワーク) > Advanced Settings (詳細設定)を選択します。**

©2025 Palo Alto Networks, Inc.

STEP 5 | **Prisma Access**内部ゲートウェイの設定を編集して、内部ゲートウェイを有効にし、変更を保存します。

(任意) 独自のDNSサーバーを使用しない場合は、IPv4の内部ホスト検出を有効にします 。内部ホスト検出を有効にするには、**[Enable Internal Gateway (**内部ゲートウェイを有効にする**)]**を選択します。

*Prisma Access*は***Always On (***常時オン**)**接続方式の場合のみ、内部ホスト検出をサポートします。

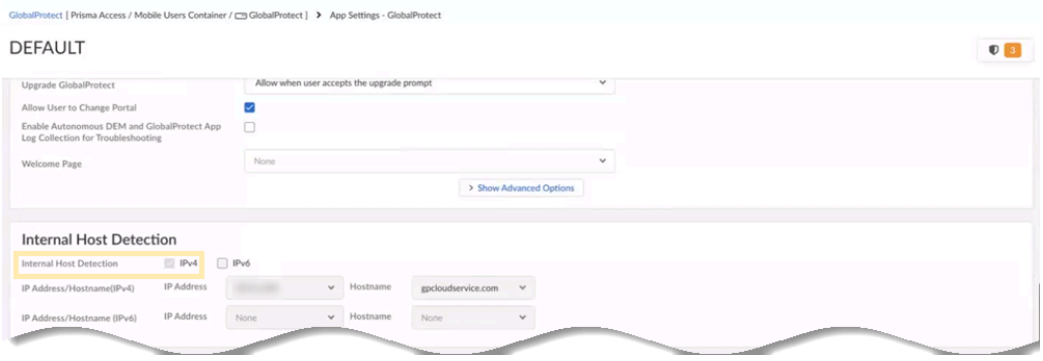


内部ゲートウェイを有効にすると、リモート ネットワーク インスタンスは内部ゲートウェイとして機能します。内部ホスト検出を有効にすると、Prisma Accessは内部ホスト検出処理のためにリモート・ネットワーク DNS プロキシ・サーバー上に PTR レコードを作成します。

STEP 6 | **[Workflows (**ワークフロー**)]** > **[Prisma Access**セットアップ**]** > **[GlobalProtect]** > **[GlobalProtect**アプリケーション**]** を選択します。

STEP 7 | アプリ設定を選択し、内部ホスト検出の詳細と内部ゲートウェイの詳細を表示します。

ステップ5で内部ゲートウェイと内部ホスト検出を有効にすると、Prisma Accessはここでもも IPv4内部ホスト検出と内部ゲートウェイを有効にします。Prisma Accessは、2手順で取得したリモートネットワーク**DNS IP**アドレス値をIPアドレスとして入力します。

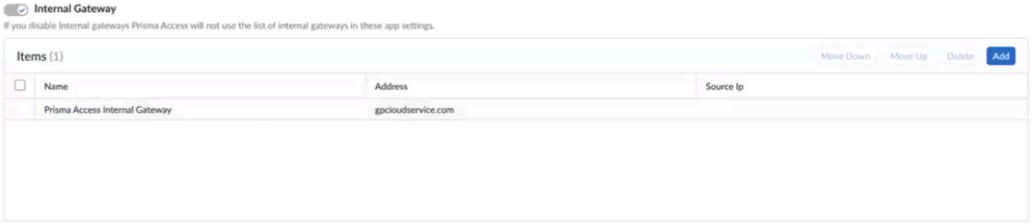


Prisma AccessDNSプロキシでのIPv6内部ホスト検出はサポートされていないことに注意してください。

この **Prisma AccessInternal Gateway (**内部ゲートウェイ**)** のエントリを削除することはできません。ただし、自己でデプロイした内部ゲートウェイを追加できます。Y内部ホスト検出のために、内部ネットワークに独自のDNSサーバーを配置することができますが、内部ホ

 ©2025 Palo Alto Networks, Inc.

スト検出が可能であるように、PTRレコードを追加してください。Prisma Accessは、ステップ3のゲートウェイ **FQDN** 値をアドレスに追加します。



NSプロキシサーバーのIPアドレスの詳細を表示するには、**Workflows** > **Prisma Access Setup** > **Prisma Access**を選択します。

内部ホスト検出を有効にした場合、DNS解決が機能していることを確認し、内部ネットワークからDNSプロキシサーバーIPへのDNS逆引きを実行し、**`any-igw`**で始まるFQDNを返すことを確認します。

STEP 8 | 変更をモバイル ユーザーとリモート ネットワークに同時にプッシュします 。

STEP 9 | エンドポイントにログインします。

GlobalProtectに接続すると、最初にGlobalProtectポータルで認証を行います。内部ホスト検出がGlobalProtectを内部ゲートウェイに接続させます。その後、GlobalProtectエージェントがトンネルモードで動作し続けると、2回目の認証が表示され、ホスト情報がリモートネットワークの内部ゲートウェイに送信されます。

Prisma Access 内部ゲートウェイ（Panorama）

STEP 1 | Panoramaで、GlobalProtectをセットアップし、 アプリ設定を追加し、 リモート ネットワークをオンボードします。

現時点では内部ホスト検出と内部ゲートウェイ構成が存在しないことに注意してください。

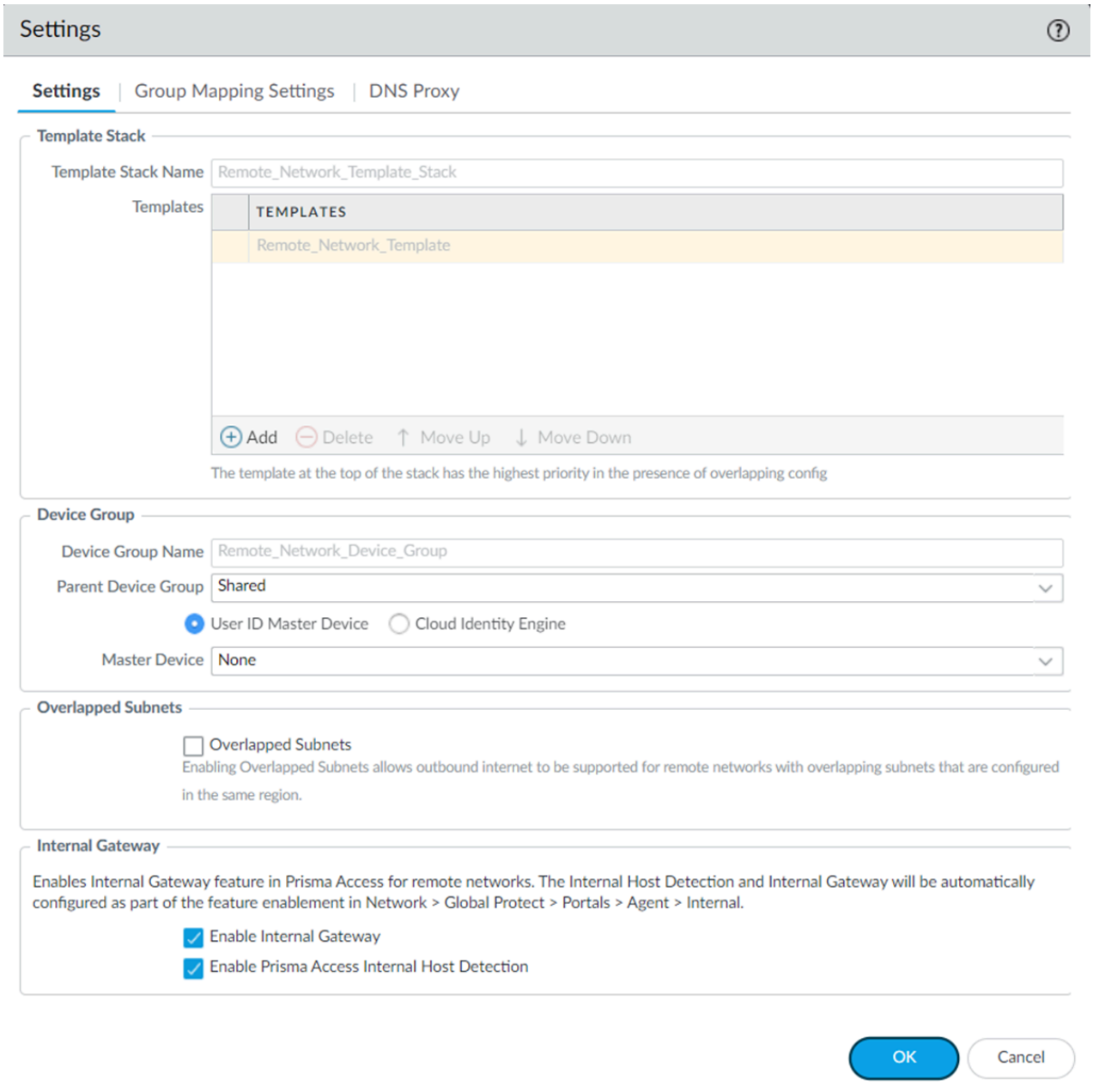
STEP 2 | **[Panorama]** > **[Cloud Services (クラウド サービス)]** > **[Configuration (構成)]** > **[Remote Networks (リモート ネットワーク)]** > **[Settings (設定)]**に移動します。

©2025 Palo Alto Networks, Inc.

STEP 3 | 内部ゲートウェイを有効にして変更を保存します。

(任意) 独自のDNSサーバーを使用しない場合は、IPv4 の**Prisma Access** 内部ホスト検出を有効にします 。内部ホスト検出を有効にするには、**[Enable Internal Gateway (**内部ゲートウェイを有効にする**)]**を選択します。

*Prisma Access*は***Always On* (**常時オン**)**接続方式の場合のみ、内部ホスト検出をサポートします。



内部ゲートウェイを有効にすると、リモート ネットワーク インスタンスは内部ゲートウェイとして機能します。内部ホスト検出を有効にすると、 Prisma Accessは内部ホスト検出プロセスのために、リモート ネットワークDNSプロキシ サーバーにPTRレコードを作成します。

©2025 Palo Alto Networks, Inc.

内部ゲートウェイを有効にすると、 Prisma Accessはリモート ネットワーク テンプレートに内部ゲートウェイ構成を作成します。

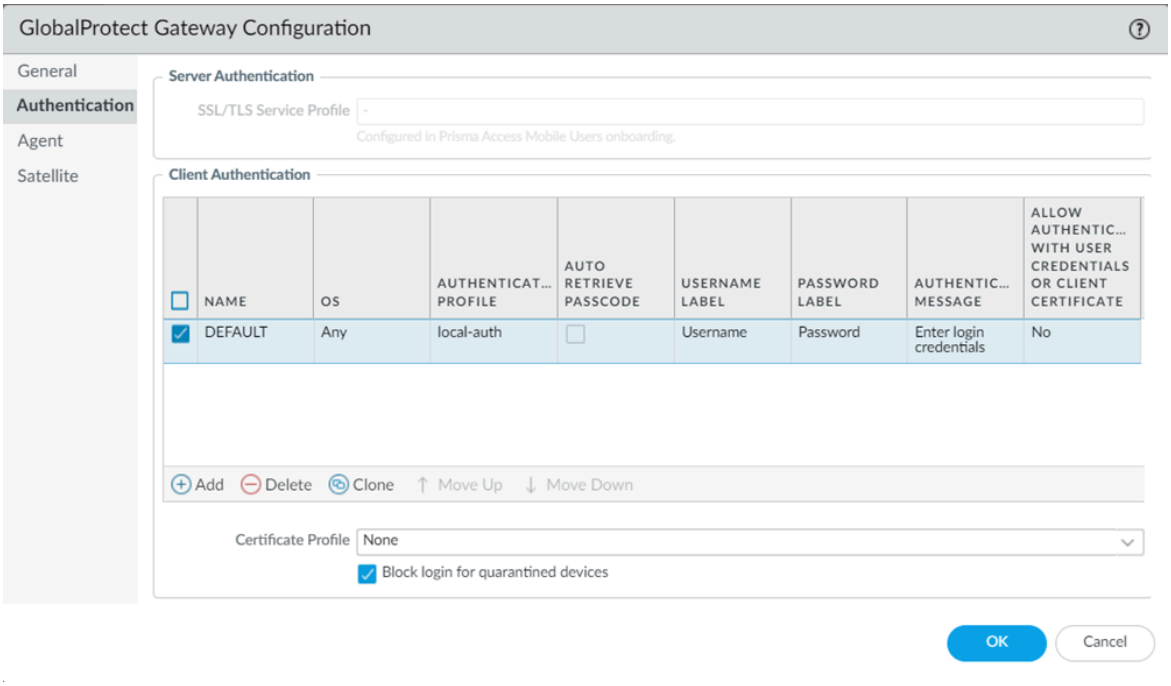
STEP 4 | **[テンプレート] > [ネットワーク] > > [GlobalProtect] > [ゲートウェイ]**に移動し、**[Remote_Network_Template]**を選択します。

内部ゲートウェイ用に作成された **GlobalProtect_Internal_Gateway** テンプレートが見つかります。

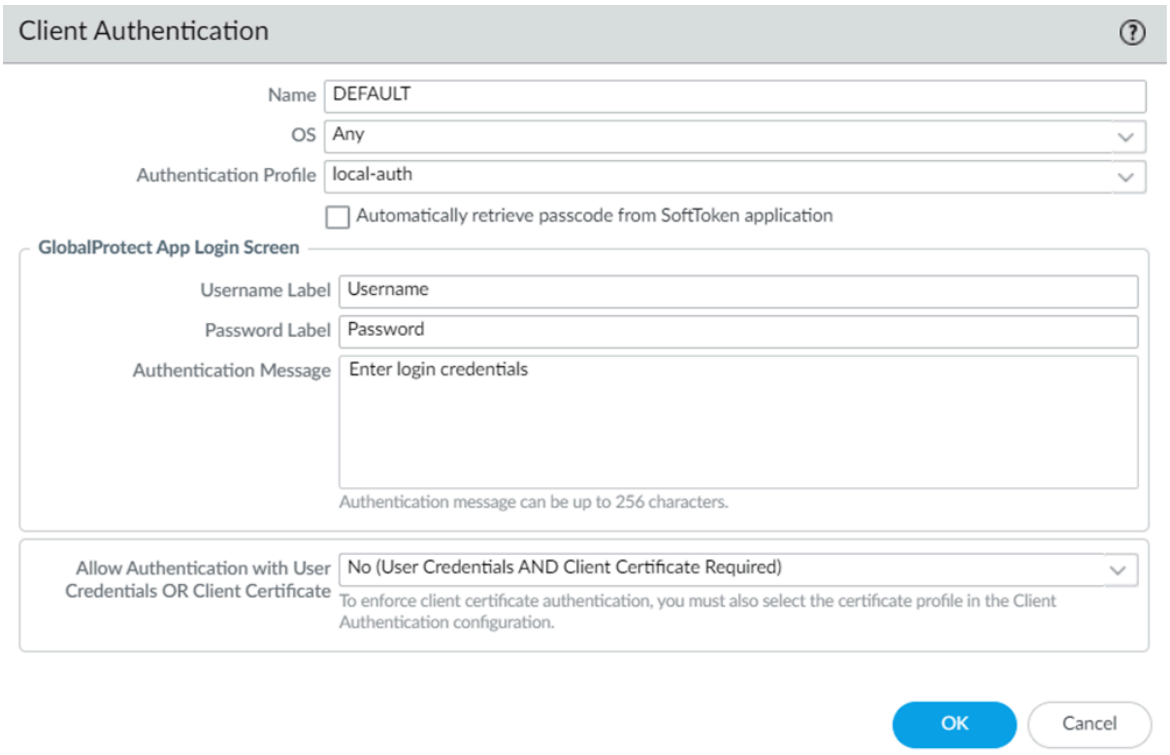
©2025 Palo Alto Networks, Inc.

STEP 5 | モバイル ユーザー テンプレートの認証プロファイルに似た、このリモート ネットワーク テンプレートの認証プロファイルを作成します。

1. リモート ネットワーク テンプレート、**GlobalProtect_Internal_Gateway**テンプレート、ハイパーリンクを選択します。
2. [認証] > [クライアント認証]に移動します。

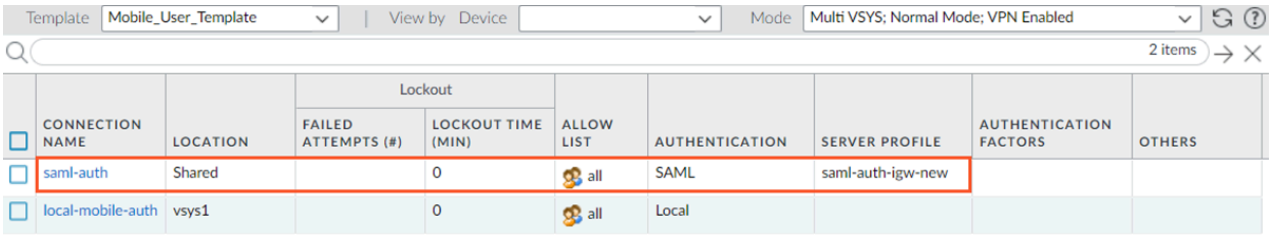


3. **DEFAULT** クライアント認証の認証プロファイルの詳細を編集します。

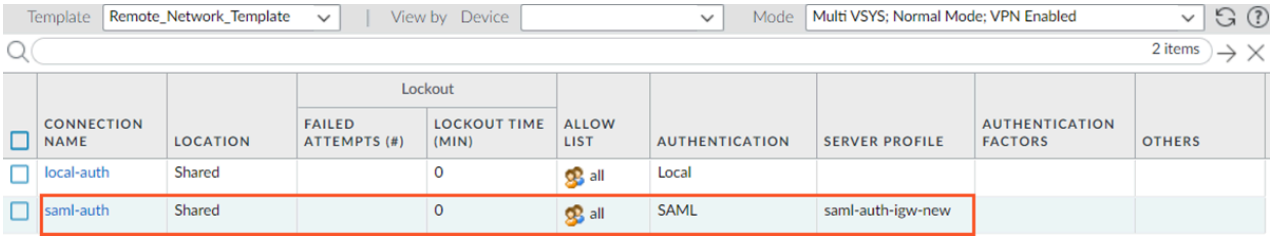


©2025 Palo Alto Networks, Inc.

モバイル ユーザー テンプレートと同じ認証プロファイルを作成します。モバイル ユーザー テンプレートで使用される認証プロファイルは [テンプレート] > [デバイス] > [認証プロファイル]の下にあります。必ず **Mobile_User_Template**を選択してください。



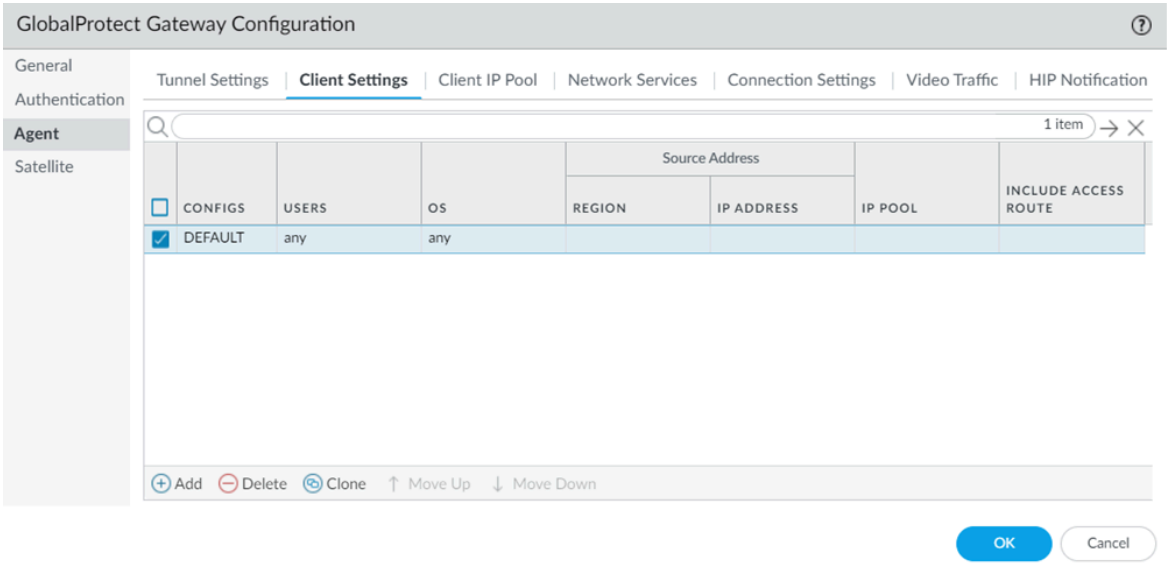
[テンプレート] > [デバイス] > [認証プロファイル] を選択して、リモート ネットワーク テンプレートの認証プロファイルを表示することもできます。***Remote_Network_Template***を選択します。



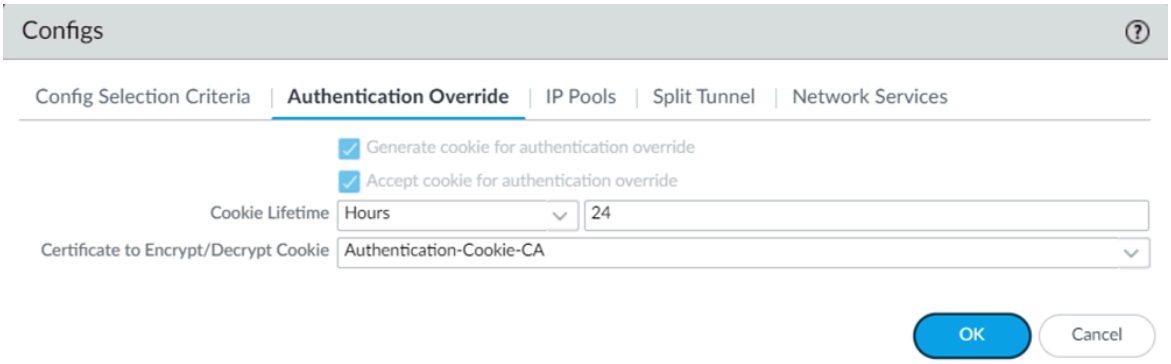
 ©2025 Palo Alto Networks, Inc.

STEP 6 | モバイル ユーザー テンプレートのデバイス証明書と同様に、リモート ネットワーク テンプレートのデバイス証明書を作成します。

1. リモート ネットワーク テンプレート **GlobalProtect_Internal_Gateway**のハイパーリンクを選択します。
2. **[Agent**（エージェント）**] > [Client Settings**（クライアント設定）**]**を選択します。



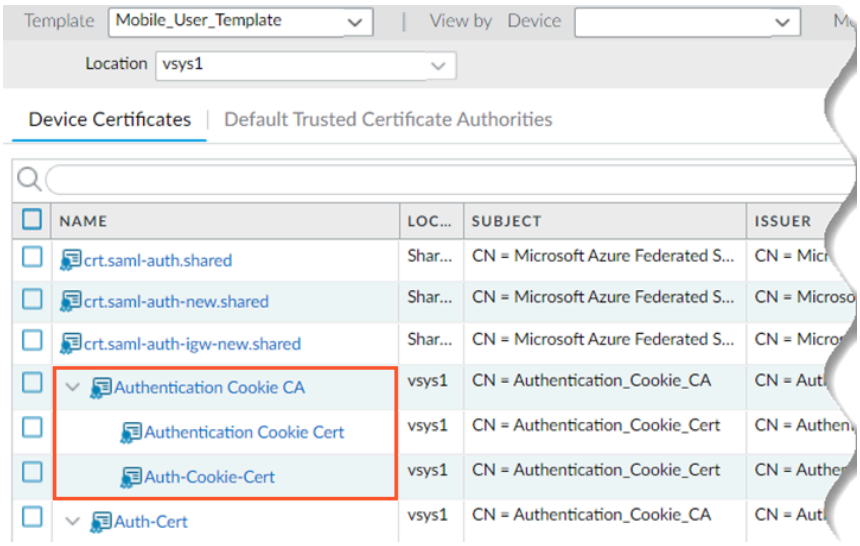
3. **DEFAULT** 構成を選択し、 **[Authentication Override (**認証オーバーライド**)]** 設定に移動します。
4. **[Certificate to Encrypt/Decrypt Cookie (Cookie**の暗号化/復号化のための証明書**)]** 設定を編集し、新しいデバイス証明書を作成します。



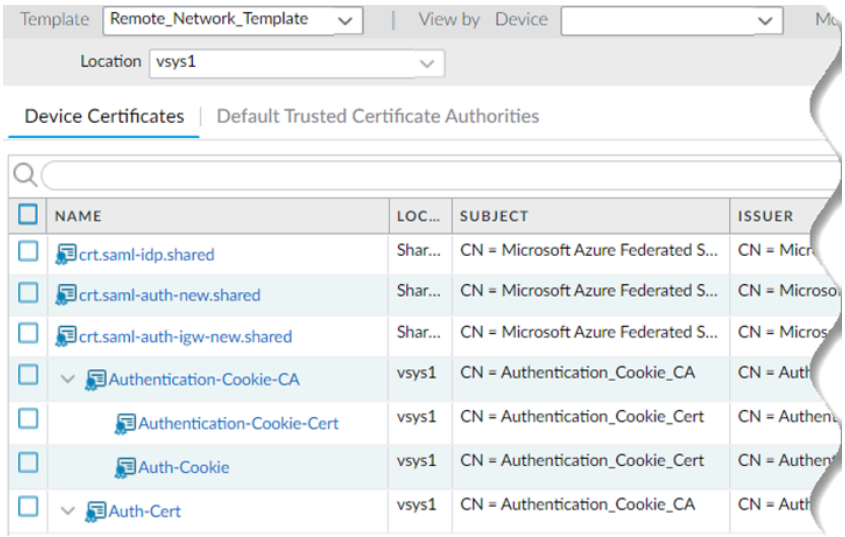
モバイル ユーザー テンプレートにあるものと同じデバイス証明書を作成します。モバイル ユーザー テンプレートで使用されるデバイス証明書は **[**テンプレート**]** > **[**デバイス > **[**証明書管理**]** > **[**証明書**]** > **[**デバイス証明書**]**で見つけることができます。必ず**Mobile_User_Template**を選択してください。**DEFAUL**設定では、

 ©2025 Palo Alto Networks, Inc.

[Authentication Cookie CA (認証Cookie CA)] 証明書を参照します。認証を成功させるには、**Mobile_User_Template** と同じ階層に従ってください。



[テンプレート] > *[デバイス]* > *[証明書管理]* > *[証明書]* > *[デバイス証明書]*を選択して、リモート ネットワーク テンプレートのデバイス証明書を表示することもできます。***Remote_Network_Template***を選択します。



STEP 7 | 変更をモバイル ユーザーとリモート ネットワークに同時にプッシュします 。

リモートネットワークのロケーションへの安全なインバウンドアクセスの提供

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager)	• サイト間およびユーザー間アクセス用のネット相互接続を含むPrisma Accessライセンス

©2025 Palo Alto Networks, Inc.

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	

リモートネットワークサイトでインターネットでアクセス可能なアプリケーションを提供している場合、それらのアプリケーションへのアクセスを提供することは、インターネットで発生するそれらの脅威すべてにネットワークが晒されます。このセクションでは、 Prisma Accessがこれらのアプリケーションへの安全なアクセスをどのように提供するのかを説明し、それをいつ実装するか、およびそれを構成する方法について説明します。

- リモートネットワークサイト用のインバウンドアクセスの保護
- 安全なインバウンドアクセスの例
- 安全なインバウンドアクセスを使用するためのガイドライン
- リモートネットワークサイト用の安全なインバウンドアクセスの設定

リモートネットワークサイト用のインバウンドアクセスの保護

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• サイト間およびユーザー間アクセス用のネット相互接続を含むPrisma Access ライセンス

Prisma Access リモート ネットワークでは、インターネットに接続されたアプリケーションへの発信アクセスを許可します。場合によっては、リモートサイトのアプリケーションまたはWebサイトへのインバウンドアクセスを提供し、Prisma Accessが保護するユーザーだけではなく、インターネットに接続している任意のユーザーに対してそのアプリケーションへの保護を提供する必要があります。以下に例を示します。

- リモートネットワークサイトで、一般的に公開されているカスタムアプリケーションまたはポータルを提供している。
- 安全なアクセスを提供したいと考えている、ラボやステージング環境が存在している。
- メンバーまたは組織ドメインではないユーザーに、アプリケーションまたはWebサイトへのアクセスを提供する必要がある。
- 内部のアセット管理、追跡、またはステータスアプリケーションにアクセスする必要があるIoTデバイスを保有している。

そのためには、インバウンドアクセスの保護を許可するリモートネットワークを作成してください。リモートネットワークサイトに対して、インバウンドアクセスだけではなくアウトバウンドアクセスも必要な場合は、インバウンドアクセス用とアウトバウンドアクセス用の、同じロケーションに2つのリモートネットワークサイトを作成してください。

この解決方法では、リモートネットワークあたり最大*50,000*件の同時インバウンドセッションを提供できますが、大容量のアプリケーションや*Web*サイトに対してこの方法を使用することはお勧めできません。

©2025 Palo Alto Networks, Inc.

安全なインバウンドアクセスの例

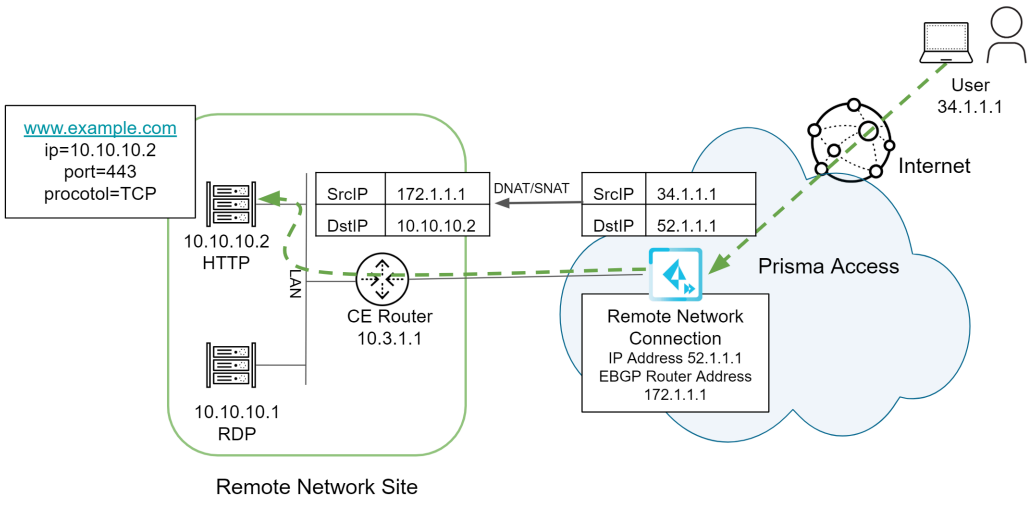
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• サイト間およびユーザー間アクセス用のネット相互接続を含むPrisma Accessライセンス

このセクションでは、さまざまなデプロイメントでPrisma Accessが割り当てるIPアドレスとともに、インバウンド・アクセ スの例を示します。

リモートネットワークサイトのアプリケーション（www.example.com）に対するインバウンドアクセスを有効にする、サンプル設定の例を次に示します。アプリケーションに対してIPアドレス10.10.10.2、ポート 443、およびプロトコルTCPを割り当てます。次に、インバウンドアクセスの設定時に、Prisma Accessにこれらの値を入力します。変更内容を保存してコミットしたら、Prisma Accessによって指定したアプリケーションにパブリックIPアドレスが割り当てられます（この場合52.1.1.1）。

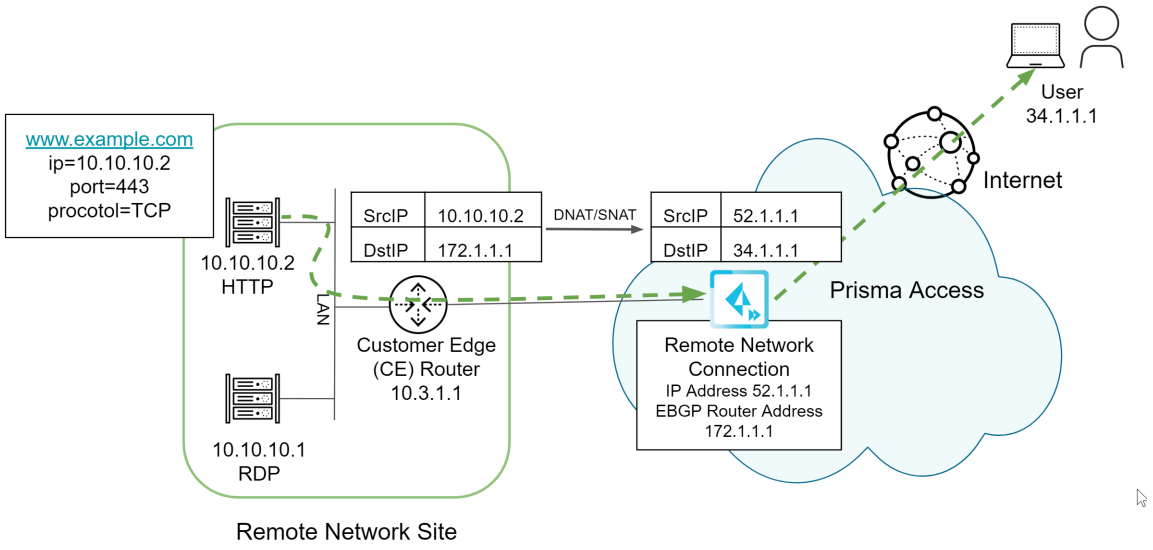
デフォルトでPrisma Accessは、パケットの送信元ネットワークアドレス変換（送信元NAT）を実行します。リモートネットワークサイトのIPSec対応デバイスがシンメトリックリターンを行える場合は（Palo Alto Networks次世代ファイアウォールなど）、送信元NATを無効にすることができます。

ユーザーからアプリケーションへのトラフィックフローを次の図に示します。ソースNATが有効になっているため、ルーティングテーブル内の送信元IPアドレスはユーザーのデバイスのIP（34.1.1.1）からリモートネットワークの**EBGP Router**アドレス（**Panorama** > **Cloud Services** > **Status** > **Network Details** > **Remote Networks** > **EBGP Router**）に変更されます。（172.1.1.1）。

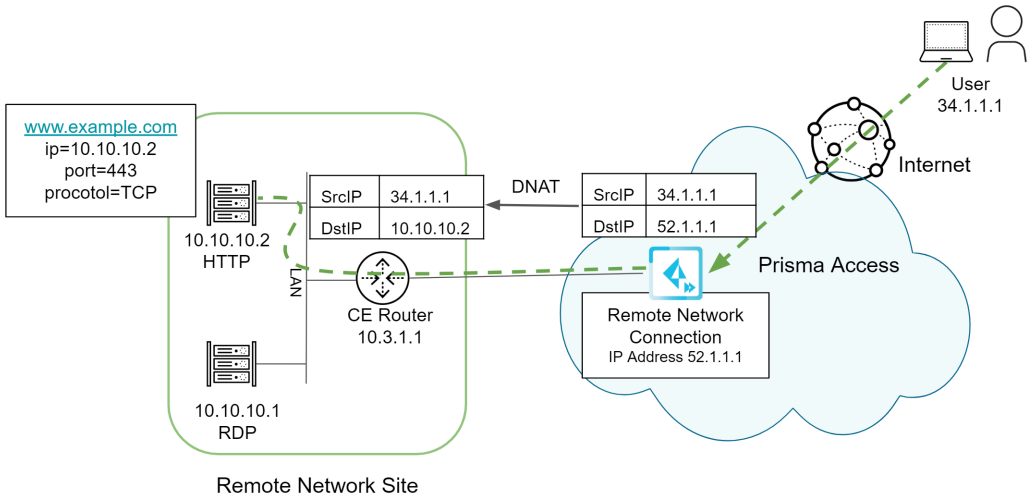


送信元NATを有効にしている、トラフィックのリターンパスを次の図に示します。

©2025 Palo Alto Networks, Inc.

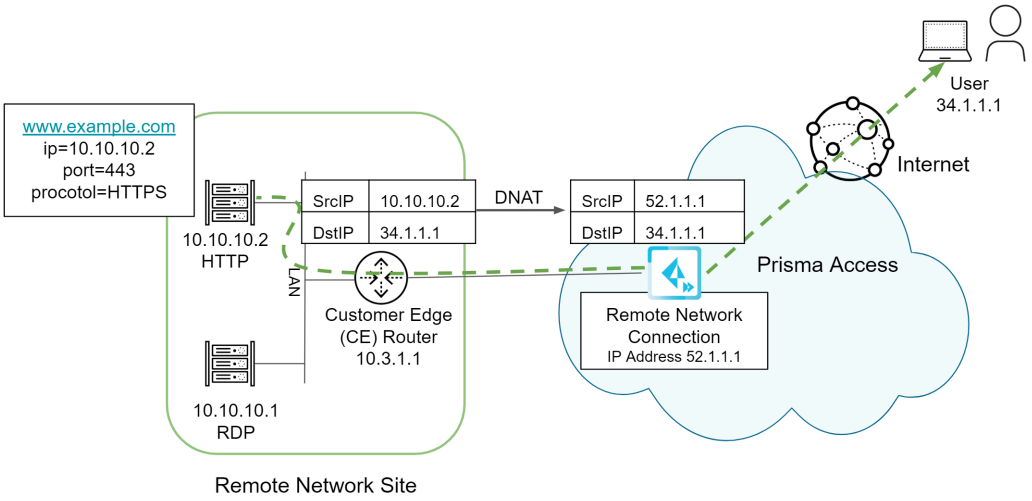


送信元NATを無効にした場合でも、Prisma Accessによって宛先NATは実行されますが、リクエストの送信元IPアドレスは変更されません。



リターントラフィックの場合、SNATは無効になっています。また、すべてのルーティングテーブルの宛先アドレスは、ユーザーのIPアドレス（34.1.1.1）になります。

©2025 Palo Alto Networks, Inc.



インバウンドアクセスが有効になっているリモートネットワークサイトのリソースがあり、非インバウンドアクセスサイトのユーザーにそのリソースへのアクセスを許可する場合、非インバウンドアクセスのリモートネットワークを構成するときに、**Prisma Access**バックボーンを介した他のリモートネットワークへのインバウンドフローを許可できます。

他のリモート ネットワークからのインバウンドフローを許可する場合は、送信元*NAT*を有効にする必要があります。



安全なインバウンドアクセスを使用するためのガイドライン

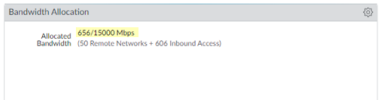
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• サイト間およびユーザー間アクセス用のネット相互接続を含むPrisma Access ライセンス

安全なインバウンドアクセスを使用するようにリモート ネットワークを構成する場合は、次のガイドラインと制限に従ってください。

- リモート ネットワークをインバウンドアクセス用に構成する場合、割り当てるIPアドレスのライセンスからユニット (Mbps) を追加します (5つのIPアドレスの場合は150 Mbps、10のIPアドレスの場合は300 Mbps)。このため、開始する前に、着信アクセス リモート ネットワークをオンボードするのに十分なライセンス帯域幅が残っていることを確認してください。利用可能な帯域幅を確認するには、**[Panorama]** > **[Cloud Services (**クラウドサービス**)]** > **[Configuration (**構成**)]** > [リモート ネットワーク] を選択し、ライセンスされた

 ©2025 Palo Alto Networks, Inc.

Bandwidth Allocation (帯域幅割り当て)を表示します。この領域には、すでに割り当てられている帯域幅と、ライセンスされている合計帯域幅が表示されます。



- セキュアなインバウンドアクセスは、Prisma Accessロケーションのサブセットを使用します。
- 安全なインバウンドアクセスを提供するために、既存のリモートネットワークを変更することはできません。新しいリモートネットワークを作成してください。
- ECMPロードバランシングを使用するリモートネットワークでは、インバウンドアクセス機能を利用できません。
- アプリケーションポート変換はサポートされていません。
- リモートネットワークをオンボーディングするための一括インポート機能は、インバウンドアクセスをサポートしていません。新しいインバウンドアクセスリモートネットワークをオンボーディングするには、Panoramaを使用してください。
- リモートネットワークインバウンドアクセスで、サービス接続によるトラフィック転送ルールは使用しないでください。
- インバウンドリモートネットワークで、支店からのアウトバウンドトラフィックは許可されていません。
- User-IDおよびアプリケーション認証はサポートされていません。
- Prisma Accessは、フラッド防御のために次のレート制限を採用しています。また、レートは秒あたりの接続数（CPS）で測定しています。

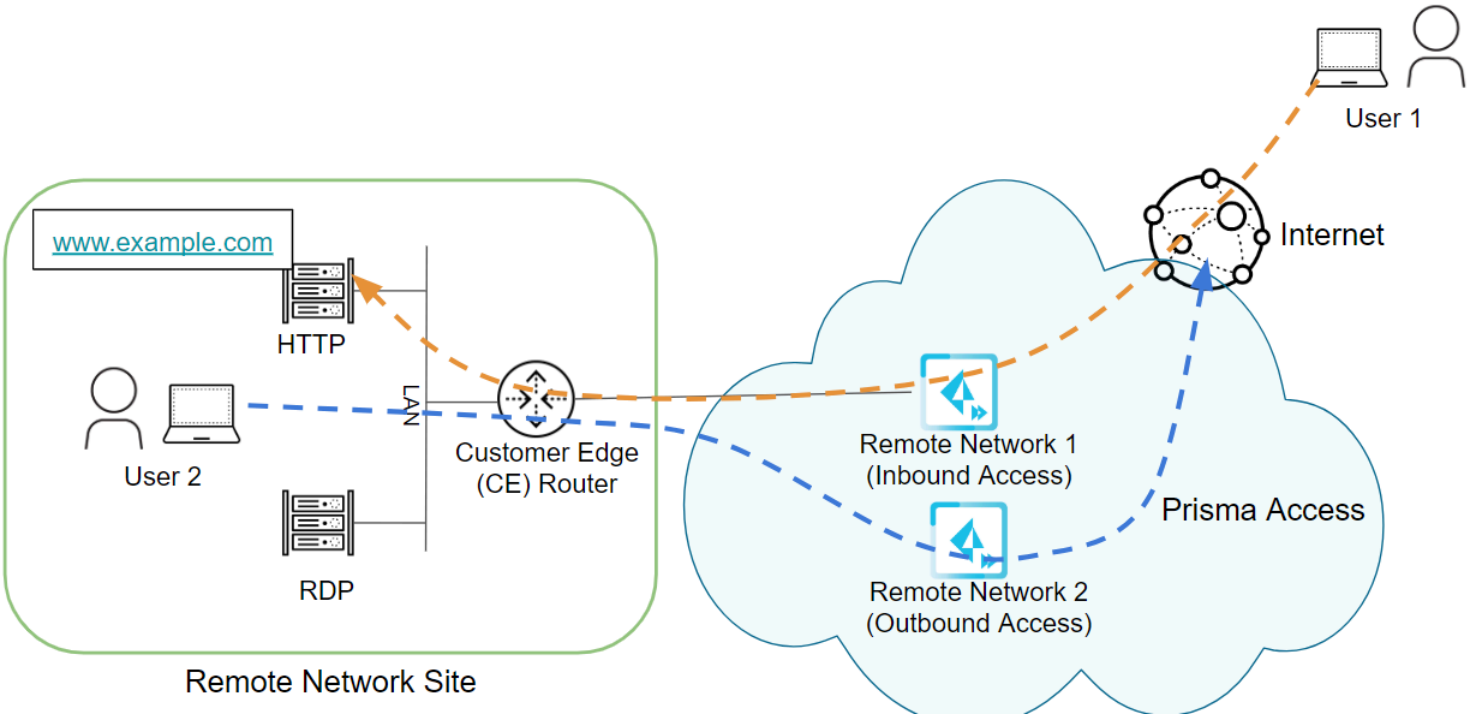
フラッド防御タイプ	アラームレート（CPS）	アクティベーションレート（CPS）
SYNフラッド	10000	15000
ICMPフラッド	20	20

新しいセッションのフラッディングに対するより強力な保護が必要な場合は、Palo Alto Networksチームにお問い合わせください。

- 安全なインバウンドアクセスが設定されているリモートネットワークは、その目的でのみ利用できます。リモートネットワークサイトに対して、インバウンドアクセスだけではなくアウトバウンドアクセスも必要な場合は、次の図のように、同じロケーションにインバウンドアクセス用とアウトバウンドアクセス用の、2つのリモートネットワークサイトを作成してください。この例でUser 1はwww.example.comへのインバウンドアクセス用にRemote

©2025 Palo Alto Networks, Inc.

Network 1を使用しており、User 2はリモートネットワークロケーションからのアウトバウンドインターネットアクセスにRemote Network 2を使用しています。



- いずれかのクラウドプロバイダが除外されているカスタムのPrisma Accessデプロイメント環境がある場合、リモートネットワークのオンボーディング時にロケーションを選択できないため、インバウンドアクセスがサポートされない場合があります。
- 評価版ライセンスでは、安全なインバウンドアクセスはサポートされていません。

リモートネットワークサイト用の安全なインバウンドアクセスの設定

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access サイト間およびユーザー間アクセス用のNet Interconnectを含むライセンス

お使いのデプロイメントでは、コンピュートロケーションまたはロケーションごとに帯域幅をオンボードすることができます。リモートネットワークのインバウンドアクセスを設定するには、どちらの方法もサポートされています。リモートネットワークのインバウンドアクセスを構成する際、コンピュートロケーションによって帯域幅が割り当てられる場合、ロケーションごとに帯域幅を指定します。安全なインバウンドアクセスを許可するリモートネットワークを作成するには、以下の手順に従ってください。

- リモートネットワーク デプロイメントのために、コンピューティング ロケーションによって帯域幅を割り当てる安全なインバウンドアクセスを構成するには、このワークフローを完了してください。

©2025 Palo Alto Networks, Inc.

- 場所によって帯域幅を割り当てるリモートネットワーク デプロイメントのためのセキュアなインバウンドアクセスを設定するには、次のワークフローを完了してください。

リモートネットワーク用の安全なインバウンドアクセスの設定

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access サイト間およびユーザー間アクセス用のNet Interconnectを含むライセンス

リモートネットワークサイトからインターネットにアクセス可能なアプリケーションを利用できるようにするには、まずアクセスさせるアプリケーションのリストを作成し、各アプリケーションに対してプライベートIP、ポート番号、およびプロトコルの組み合わせを割り当ててください。複数のアプリケーションに対して同じIPアドレスを使用する場合、各アプリケーションに対してポート/プロトコルの組み合わせは一意でなければなりません。複数のアプリケーションに対して同じポート/プロトコルの組み合わせを使用する場合は、各IPアドレスが一意でなければなりません。

設定を開始するには、アプリケーションに関連付けるパブリックIPアドレス数を選択します。リモートネットワークサイトあたり、5または10のパブリックIPアドレスを指定することができます。各パブリックIP割り当てでは、リモート ネットワークに関連付けられたコンピューティング ロケーションに割り当てた帯域幅に加えて、リモート ネットワーク ライセンスから帯域幅 (ユニット) が使用されます 。5件のIPアドレスでは、リモートネットワークライセンスから150 Mbpsが消費され、10件のIPアドレスでは300 Mbpsが消費されます。

パブリックIPアドレス数を選択した後、インバウンドアクセスを保護するアプリケーションとそれに関連するプライベートIP/ポート番号/プロトコルを指定します。

アプリケーションをパブリックIPアドレスにマップする方法を指定することができます。デフォルトでPrisma Accessは、指定されたアプリケーションに対してパブリックIPアドレスを割り当てます。単一のIPアドレスに複数のアプリケーションを割り当てることができます。単一のアプリケーションを単一のパブリックIPアドレスにマップする必要がある場合、システム設定時に**Dedicated IP**（専用の**IP**）を選択することができます。プロビジョニングされた各パブリックIPアドレスのグループに対して（5件または10件）、最高100件のインバウンドアプリケーションを設定することができます。

- Strata Cloud Manager
- Panorama

リモートネットワーク用の安全なインバウンドアクセスの設定 *(Strata Cloud Manager)*

ここでは、インターネットに接続しているすべてのユーザー (Prisma Accessユーザーだけでなく) がリモートネットワークサイトからアプリケーションにアクセスできるようにする方法を示します。

STEP 1 | インバウンドアクセスリモートネットワークのガイドラインをまだ読んでいない場合は、確認してください。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 始めるために必要なアプリケーションの詳細を収集します。

アクセスを提供するアプリケーションのリストを作成し、各アプリケーションにプライベートIP、ポート番号、およびプロトコルの組み合わせを割り当てます。複数のアプリケーションに対して同じIPアドレスを使用する場合、各アプリケーションに対してポート/プロトコルの組み合わせは一意でなければなりません。複数のアプリケーションに対して同じポート/プロトコルの組み合わせを使用する場合は、各IPアドレスが一意でなければなりません。

STEP 3 | Strata Cloud Manager で、[ワークフロー] > **[Prisma Access**セットアップ] > [リモートネットワーク] > [インバウンドアクセス] > [インバウンドアクセスの追加]に移動します。

STEP 4 | 必要な詳細を入力します。

アプリケーションに使用するパブリック**IP**の数を、5つまたは10のいずれかで選択します。

パブリックIPの割り当てごとに、リモートネットワークライセンスの帯域幅と、ライセンスコストが消費されます。5件のIPアドレスでは、リモートネットワークライセンスから150 MBが消費され、10件のIPアドレスでは300 MBが消費されます。

Prisma Accessバージョン4.1以降、インバウンドアクセスが有効になっているリモートネットワークサイトのリソースがあり、非インバウンドアクセスサイトのユーザーにそのリソースへのアクセスを許可する場合、非インバウンドアクセスのリモートネットワークを構成するときに、**Prisma Access**バックボーンを介した他のリモートネットワークへのインバウンドフローを許可できます。

Prisma Accessバージョン5.0以降では、非インバウンド アクセスのリモート ネットワークを設定する際に、サービス プロバイダー(SP)バックボーンを介して、他のリモート ネットワークへのインバウンド フローを許可します。

*SP*インターコネクトは、以下のもののみをサポートします。

- *GCP*リージョン
- 新しい*Prisma Access*デプロイメント
- 明示型プロキシ出口トラフィック

STEP 5 | アクセスを保護したいインバウンドアクセスアプリケーションを追加します。

アプリケーションに関連するプライベートIP/ポート番号 /プロトコルの組み合わせを追加します。

STEP 6 | アプリケーションをパブリックIPアドレスにどのようにマップするかを決定します。

デフォルトでPrisma Accessは、指定されたアプリケーションに対してパブリックIPアドレスを割り当てます。単一のIPアドレスに複数のアプリケーションを割り当てることができます。単一のアプリケーションを単一のパブリックIPアドレスにマップする必要がある場合、システム設定時に**Dedicated IP**（専用の**IP**）を割り当てることができます。プロビジョニングされた各パブリックIPアドレスのグループに対して（5件または10件）、最高100件のインバウンドアプリケーションを設定することができます。

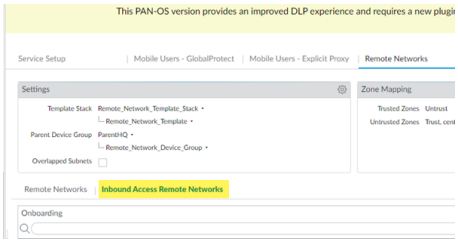
STEP 7 | 通常のリモート ネットワーク サイトと同様に、インバウンド アクセス リモート ネットワークの設定を完了します。

©2025 Palo Alto Networks, Inc.

リモートネットワーク用の安全なインバウンドアクセスの設定 *(Panorama)*

コンピュートロケーションごとにリモートネットワーク帯域幅を割り当てるPrisma Accessをデプロイして いる場合は、以下の手順を実行して、インバウンドアクセスを構成します。

STEP 1 | **[Panorama] > [Cloud Services] > [設定] > [リモート ネットワーク]を選択し、 [Inbound Access Remote Networks (インバウンド アクセス リモート ネットワーク)]**を選択します。



STEP 2 | インバウンドアクセス用にリモート ネットワークを追加します 。

STEP 3 | インバウンドアクセス リモート ネットワーク接続の設定を指定します。

1. インバウンドアクセス接続の 名前 を入力します。
2. ロケーションを入力します。

   インバウンド アクセスは ロケーションのサブセットをサポートします。
3. インバウンドアクセス接続に使用する 帯域幅 を指定します。

   インバウンドアクセス接続の帯域幅は、ロケーションごとに割り当てます。
4. インバウンドアクセス接続に使用する パブリック**IP**の数 を指定します。

   5個または10個のパブリックIPアドレスを指定します。各パブリックIP割り当てでは、リモート ネットワークに関連付けられた コンピューティング ロケーション に割り当てた帯域幅に加えて、リモート ネットワーク ライセンスから 帯域幅 (ユニット) が使用されます 。
5. インバウンドアクセス接続で使用するIPSecトンネルを選択します。
6. **Prisma Access**バックボーンを介した他のリモート ネットワークへのインバウンド フローを許可するかどうかを選択します。

   インバウンドアクセスが有効になっているリモート ネットワーク サイトにリソースがあり、非 インバウンドアクセス サイトのユーザがそのリソースにアクセスできるようにしたい場合、非 インバウンドアクセス リモート ネットワークを構成するときに、**Prisma Access**バックボーンを介した他のリ モート ネットワークへのインバウンドフローを許可することができます。他のリモート ネットワークからのインバウンドフローを許可する場合は、送信元NATを有効にする必要があります。
7. (任意) この場所にセカンダリ WAN リンクがある場合は、[セカンダリ **WAN** を有効にする] を選択し、プライマリ IPSec トンネルとは異なる **IPSec** トンネル を指定します。

STEP 4 | デプロイメントに合わせて スタティック ルート、**BGP**、および **QoS** を設定します。

この設定は、非インバウンド アクセスのリモート ネットワーク接続と同じです。

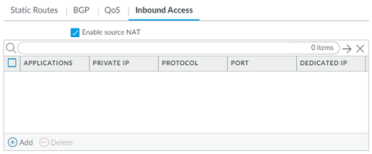
©2025 Palo Alto Networks, Inc.

STEP 5 | インバウンドアクセス オプションを構成するには、[インバウンドアクセス] タブをクリックします。

1. （任意）ソースNATを無効にするには、**Enable Source NAT**（ソース**NAT**を有効にする）の選択を解除します。

   デフォルトでは、ソースNATが有効になっています。リモート ネットワーク サイトのIPSec対応デバイスが対称リターンを実行できる場合（Palo Alto Networksの次世代ファイアウォールなど）、または **Prisma Access**バックボーンを介して他のリモート ネットワークへのインバウンド フローを許可するを選択していない場合は、送信元NATを有効にするの選択を解除します。

   このチェックボックスを選択した場合は、*[インバウンドアクセス]* タブで送信元***NAT*** を有効にする 必要があります。送信元*NAT* は、他のリモートネットワークへのインバウンドフローを許可するための要件です。

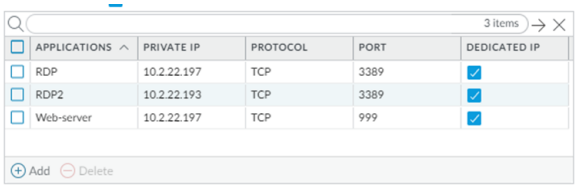


2. 安全なインバウンドアクセスを提供するために、アプリケーションを**Add**（追加）します。

   プロビジョニングされた各パブリックIPアドレスのグループに対して（5件または10件）、最高100件のインバウンドアプリケーションを設定することができます。各アプリケーションに対して、一意の**Private IP**（プライベート**IP**）アドレス、**Protocol**（プロトコル）、および**Port**（ポート）を入力します。2つのアプリケーションに対して重複したプライベートIPアドレスを使用することは可能ですが、その場合片方のアプリケーションに対して**TCP**を、もう一方のアプリケーションに対して**UDP**を選択する必要があります。

   以下の値を指定します。

   - **Application**（アプリケーション）の名前を指定します。
   - アプリケーションで使用する**Private IP**（プライベート**IP**）アドレスを指定します。
   - アプリケーションで使用する**Protocol**（プロトコル）を指定します（**TCP**または**UDP**）。
   - アプリケーションで使用する**Port**（ポート）を指定します。
   - 単一のアプリケーションに対して、専用のパブリックIPアドレスを使用するかどうかを選択します。使用する場合は、**Dedicated IP**（専用の**IP**）を選択します。



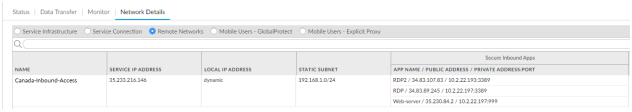
STEP 6 | **OK** をクリックして変更内容を保存します。

©2025 Palo Alto Networks, Inc.

STEP 7 | 変更を**Save**（保存）、**Commit**（コミット）します。

STEP 8 | Prisma Accessがパブリックアドレスを生成するまで30分ほど待ちます。その後**[Panorama]** > **[Cloud Services**（クラウドサービス）**]** > **[Status**（ステータス）**]** > **[Network Details**（ネットワーク詳細）**]** > **[Remote Networks**（リモートネットワーク）**]**を選択して、作成したアプリケーションの**App Name**（アプリケーション名）に関連する**Public Address**（パブリックアドレス）を書き留めておきます。

Dedicated IP（専用の**IP**）を選択している場合、**Public Address**（パブリックアドレス）と関連付ける単一のアプリケーションを探します。



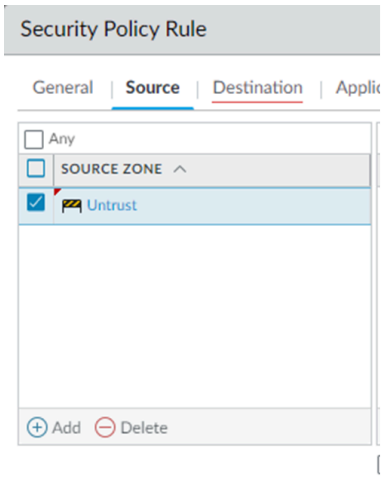
STEP 9 | インバウンドインターネットユーザーからのトラフィックを許可する、セキュリティポリシーを作成します。

Prisma Accessのデフォルトのセキュリティポリシーはuntrust-to-untrustトラフィックのみを許可しているため、インバウンドアクセスアプリケーション用にuntrust-to-trustトラフィックを許可するセキュリティポリシーを設定する必要があります。インバウンドアプリケーションへのアクセスを許可するアクセスタイプを制限することをお勧めします。SSHサーバー、Webポータル、およびRDPサーバーへのアクセスを提供する例を次に示します。

1. **Policies (**ポリシー**)** > **Security (**セキュリティ**)** の順に選択し、ポリシーを **Add (**追加**)** します。

   このポリシーは、**Remote_Network_Device_Group**デバイスグループ下に作成するようにしてください。

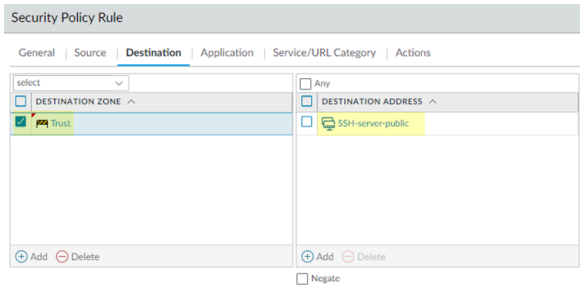
2. **Source**（送信元）トラフィックとして**Untrust**（信頼できない）を選択します。



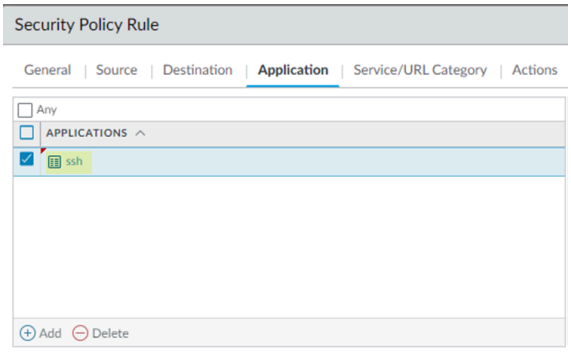
3. 宛先トラフィックの**Destination Zone**（宛先ゾーン）として**Trust**（信頼できる）を選択し、**SSH-server-public**の**Destination Address**（宛先アドレス）を指定して、SSHサーバートラフィックを許可するポリシーを作成します。これは、SSHログインに使用され

 ©2025 Palo Alto Networks, Inc.

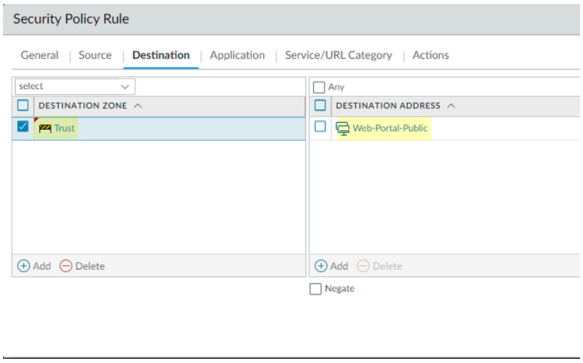
るすべてのパブリックIPアドレスのリストを含む、作成した アドレスまたはアドレス グループ オブジェクト です。



4. **Application**（アプリケーション）では**ssh**を選択します。

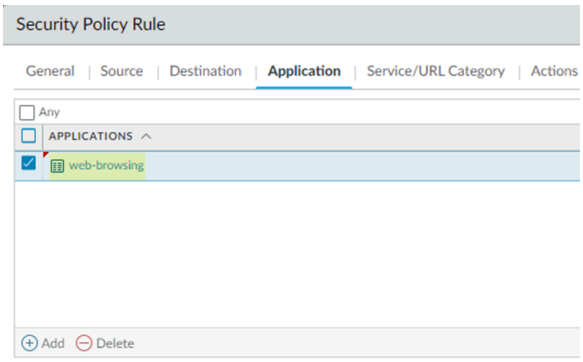


5. **Service/URL Category**（サービス/URLカテゴリ）では**application-default**を選択して、Palo Alto Networksが定義したデフォルトポートにのみ基づいて、アプリケーションを許可または拒否します。
6. **Actions** （アクション）で、**Allow**（許可）を選択します。
7. **OK** をクリックしてポリシーを保存します。
8. 前のステップの手順を利用して、Webポータルアクセスを許可するポリシーを作成します。ただし、**Destination**（宛先）および**Application**（アプリケーション）タブでは、次の設定を使用します。
   - Web ポータルのすべてのパブリック IP アドレスが含まれる **Web-Portal-Public**のアドレスまたはアドレス グループの 宛先アドレス を選択します。



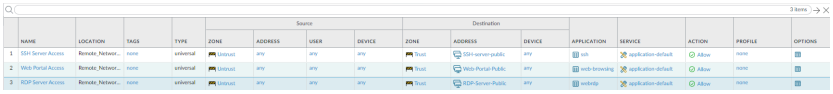
 ©2025 Palo Alto Networks, Inc.

- **Application**（アプリケーション）では**web-browsing**を選択します。



9. RDPサーバーアクセス用のセキュリティポリシーを作成する。他のポリシーと同じ設定を使用するが、**RDP-Server-Public**というAddressまたはアドレス グループ オブジェクトを作成し、**Destination Address (**宛先アドレス**)**にRDPサーバーのパブリックIPアドレス、**Application (**アプリケーション**)**に**webrdp**を指定します。

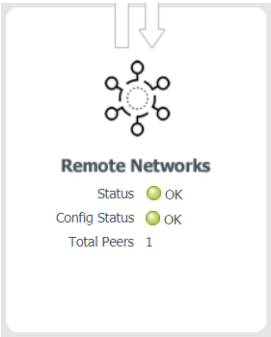
   作業が完了したら、SSHサーバーアクセス、Webポータルアクセス、およびRDPサーバーアクセス用の3種類のポリシーが完成します。



STEP 10 | 変更を**Save**（保存）、**Commit**（コミット）します。

STEP 11 | リモートネットワーク接続が機能しており、インバウンドトラフィックを正しく処理していることを確認します。

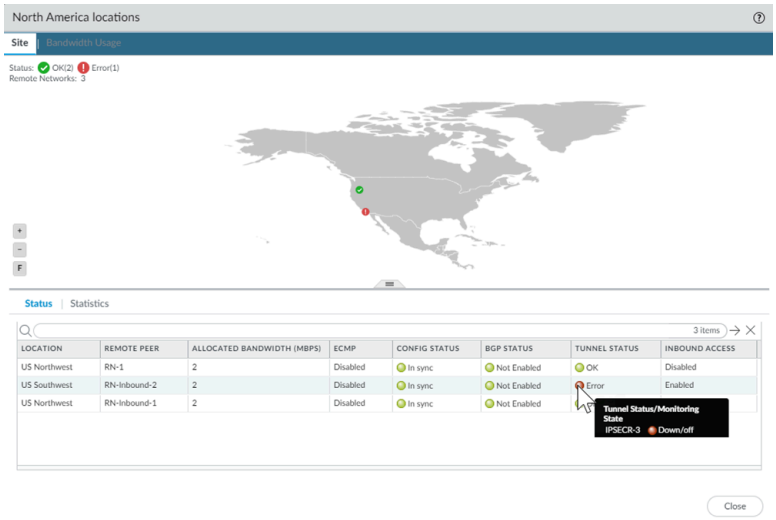
1. **Panorama** > **Cloud Services** （クラウドサービス） > **Status**（ステータス） > > **Status**（ステータス） > **Remote Networks**（リモートネットワーク）を選択した後、**Status**（ステータス）および**Config Status**（設定ステータス）エリア上にカーソルを移動して、トンネルのステータスを参照します。



2. 何か問題が見つかった場合は、**Panorama** > **Cloud Services**（クラウドサービス） > **Status**（ステータス） > > **Monitor**（監視） > **Remote Networks**（リモートネットワーク）を選択して、地図からリモートネットワークトンネルのロケーションを選択

 ©2025 Palo Alto Networks, Inc.

し、**Tunnel Status**（トンネルステータス）エリア上にカーソルを移動して、エラーの原因を判断します。



ロケーションごとに帯域幅を割り当てる場所のリモート ネットワーク サイトの安全なインバウンドアクセスを設定する

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	• Prisma Access サイト間およびユーザー間アクセス用のNet Interconnectを含むライセンス

場所によってリモートネットワークの帯域幅を割り当てるPrisma Accessデプロイメントを使用している場合は、次の手順を実行してインバウンドアクセスを設定します。

STEP 1 | **Panorama** > **Cloud Services** > 構成 > リモート ネットワークを選択し、接続 を追加して 、ルーティングやIPSecトンネル オプションなどのリモート ネットワークを設定します。

詳細は Prisma Accessリモートネットワーク を参照してください。デプロイメントでは、コンピューティング ロケーションまたはロケーションごとに帯域幅をオンボードする場合があります。どちらの方法も、インバウンド アクセスでサポートされています。

インバウンドアクセスで サポートされているロケーション の*1*つを選択していることを確認してください。

©2025 Palo Alto Networks, Inc.

STEP 2 | インバウンドアクセス オプションを構成するには、[インバウンドアクセス] タブをクリックします。

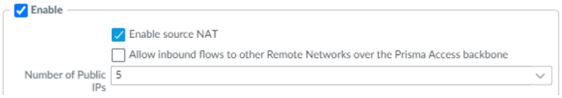
1. リモート ネットワークのインバウンドアクセスを有効にするには、[有効]を選択します。

   インバウンドアクセスでサポートされていない場所を選択した場合は、Prisma Accessはサポートされている場所を選択するようプロンプトが表示されます。

2. （任意）ソースNATを無効にするには、**Enable Source NAT**（ソース**NAT**を有効にする）の選択を解除します。

   デフォルトでは、ソースNATが有効になっています。リモート ネットワーク サイトのIPSec対応デバイスが対称リターンを実行できる場合（Palo Alto Networksの次世代ファイアウォールなど）、または **Prisma Access**バックボーンを介して他のリモート ネットワークへのインバウンド フローを許可するを選択していない場合は、送信元**NAT**を有効にするの選択を解除します。

   このチェックボックスを選択した場合は、*[インバウンドアクセス]* タブで送信元*NAT* を有効にする 必要があります。送信元*NAT* は、他のリモートネットワークへのインバウンドフローを許可するための要件です。

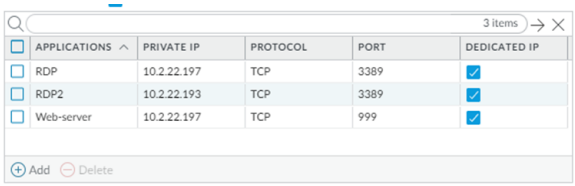


STEP 3 | 安全なインバウンドアクセスを提供するために、アプリケーションを**Add**（追加）します。

プロビジョニングされた各パブリックIPアドレスのグループに対して（5件または10件）、最高100件のインバウンドアプリケーションを設定することができます。各アプリケーションに対して、一意の**Private IP**（プライベート**IP**）アドレス、**Protocol**（プロトコル）、および**Port**（ポート）を入力します。2つのアプリケーションに対して重複したプライベートIPアドレスを使用することは可能ですが、その場合片方のアプリケーションに対して**TCP**を、もう一方のアプリケーションに対して**UDP**を選択する必要があります。

以下の値を指定します。

- **Application**（アプリケーション）の名前を指定します。
- アプリケーションで使用する**Private IP**（プライベート**IP**）アドレスを指定します。
- アプリケーションで使用する**Protocol**（プロトコル）を指定します（**TCP**または**UDP**）。
- アプリケーションで使用する**Port**（ポート）を指定します。
- 単一のアプリケーションに対して、専用のパブリックIPアドレスを使用するかどうかを選択します。使用する場合は、**Dedicated IP**（専用の**IP**）を選択します。



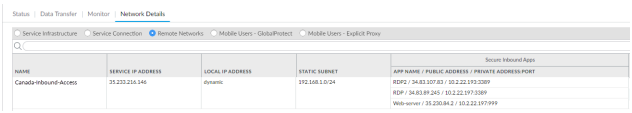
 ©2025 Palo Alto Networks, Inc.

STEP 4 | **OK** をクリックして変更内容を保存します。

STEP 5 | 変更を**Save**（保存）、**Commit**（コミット）します。

STEP 6 | Prisma Accessがパブリックアドレスを生成するまで30分ほど待ちます。その後**[Panorama] > [Cloud Services**（クラウドサービス）**] > [Status**（ステータス）**] > [Network Details**（ネットワーク詳細）**] > [Remote Networks**（リモートネットワーク）**]**を選択して、作成したアプリケーションの**App Name**（アプリケーション名）に関連する**Public Address**（パブリックアドレス）を書き留めておきます。

Dedicated IP（専用の**IP**）を選択している場合、**Public Address**（パブリックアドレス）と関連付ける単一のアプリケーションを探します。



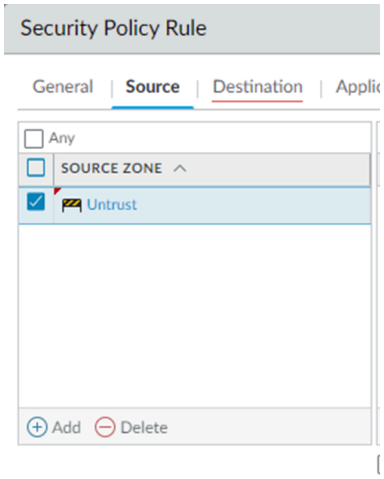
STEP 7 | インバウンドインターネットユーザーからのトラフィックを許可する、セキュリティポリシーを作成します。

Prisma Accessのデフォルトのセキュリティポリシーはuntrust-to-untrustトラフィックのみを許可しているため、インバウンドアクセスアプリケーション用にuntrust-to-trustトラフィックを許可するセキュリティポリシーを設定する必要があります。インバウンドアプリケーションへのアクセスを許可するアクセスタイプを制限することをお勧めします。SSHサーバー、Webポータル、およびRDPサーバーへのアクセスを提供する例を次に示します。

1. **Policies (**ポリシー**) > Security (**セキュリティ**)** の順に選択し、ポリシーを **Add (**追加**)** します。

   このポリシーは、**Remote_Network_Device_Group**デバイスグループ下に作成するようにしてください。

2. **Source**（送信元）トラフィックとして**Untrust**（信頼できない）を選択します。



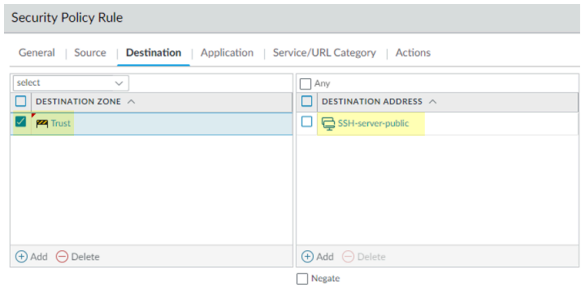
3. 宛先トラフィックの**Destination Zone**（宛先ゾーン）として**Trust**（信頼できる）を選択し、**SSH-server-public**の**Destination Address**（宛先アドレス）を指定して、SSHサー

 ©2025 Palo Alto Networks, Inc.

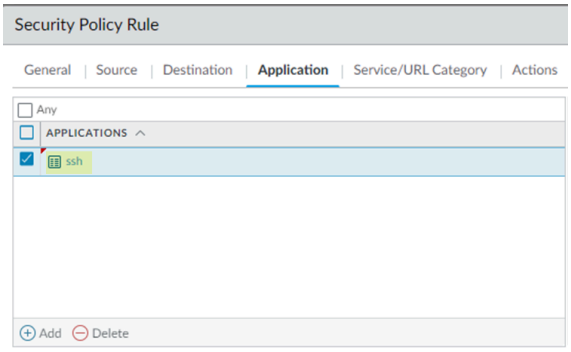
バートラフィックを許可するポリシーを作成します。これは、SSHログインに使用され

©2025 Palo Alto Networks, Inc.

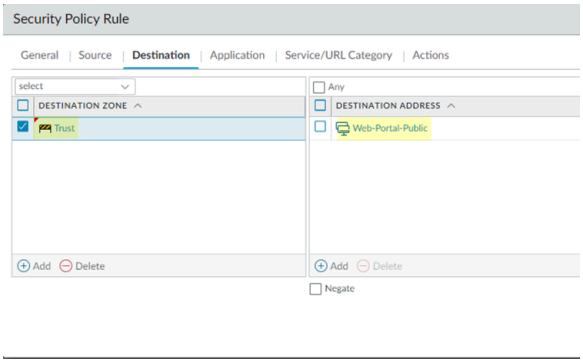
るすべてのパブリックIPアドレスのリストを含む、作成した アドレスまたはアドレス グループ オブジェクト です。



4. **Application**（アプリケーション）では**ssh**を選択します。

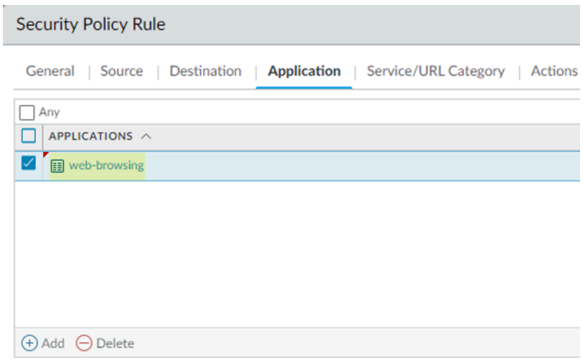


5. **Service/URL Category**（サービス/URLカテゴリ）では**application-default**を選択して、Palo Alto Networksが定義したデフォルトポートにのみ基づいて、アプリケーションを許可または拒否します。
6. **Actions** （アクション）で、**Allow**（許可）を選択します。
7. **OK** をクリックしてポリシーを保存します。
8. 前のステップの手順を利用して、Webポータルアクセスを許可するポリシーを作成します。ただし、**Destination**（宛先）および**Application**（アプリケーション）タブでは、次の設定を使用します。
   - Web ポータルのすべてのパブリック IP アドレスが含まれる **Web-Portal-Public**のアドレスまたはアドレス グループの 宛先アドレス を選択します。



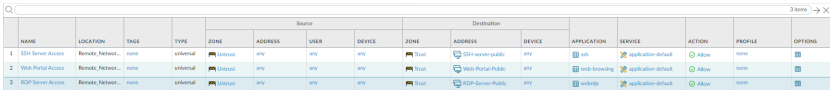
©2025 Palo Alto Networks, Inc.

- **Application**（アプリケーション）では**web-browsing**を選択します。



9. RDPサーバーアクセス用のセキュリティポリシーを作成する。他のポリシーと同じ設定を使用するが、**RDP-Server-Public**というAddressまたはアドレス グループ オブジェクトを作成し、**Destination Address (**宛先アドレス**)**にRDPサーバーのパブリックIPアドレス、**Application (**アプリケーション**)**に**webrdp**を指定します。

   作業が完了したら、SSHサーバーアクセス、Webポータルアクセス、およびRDPサーバーアクセス用の3種類のポリシーが完成します。



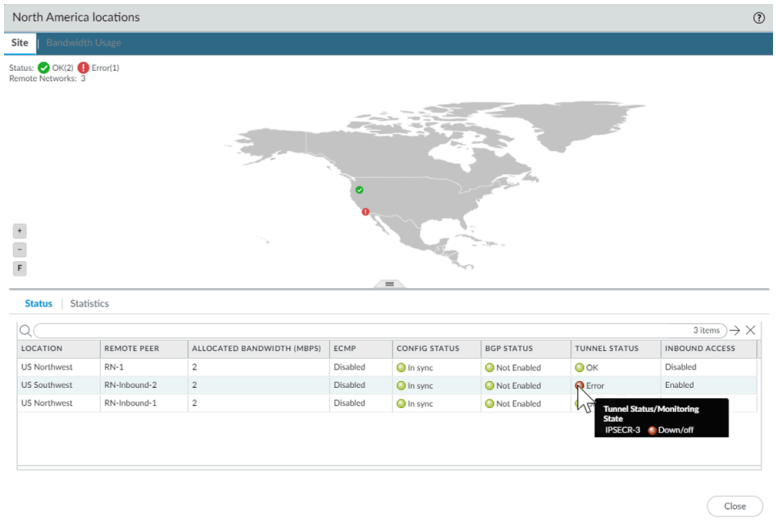
STEP 8 | 変更を**Save**（保存）、**Commit**（コミット）します。

STEP 9 | リモートネットワーク接続が機能しており、インバウンドトラフィックを正しく処理していることを確認します。

1. **Panorama** > **Cloud Services** （クラウドサービス） > **Status**（ステータス） > > **Status**（ステータス） > **Remote Networks**（リモートネットワーク）を選択した後、**Status**（ステータス）および**Config Status**（設定ステータス）エリア上にカーソルを移動して、トンネルのステータスを参照します。
2. 何か問題が見つかった場合は、**Panorama** > **Cloud Services**（クラウドサービス） > **Status**（ステータス） > > **Monitor**（監視） > **Remote Networks**（リモートネットワーク）を選択して、地図からリモートネットワークトンネルのロケーションを選択

©2025 Palo Alto Networks, Inc.

し、**Tunnel Status**（トンネルステータス）エリア上にカーソルを移動して、エラーの原因を判断します。



リモートサイト向けの高帯域幅ネットワークの作成

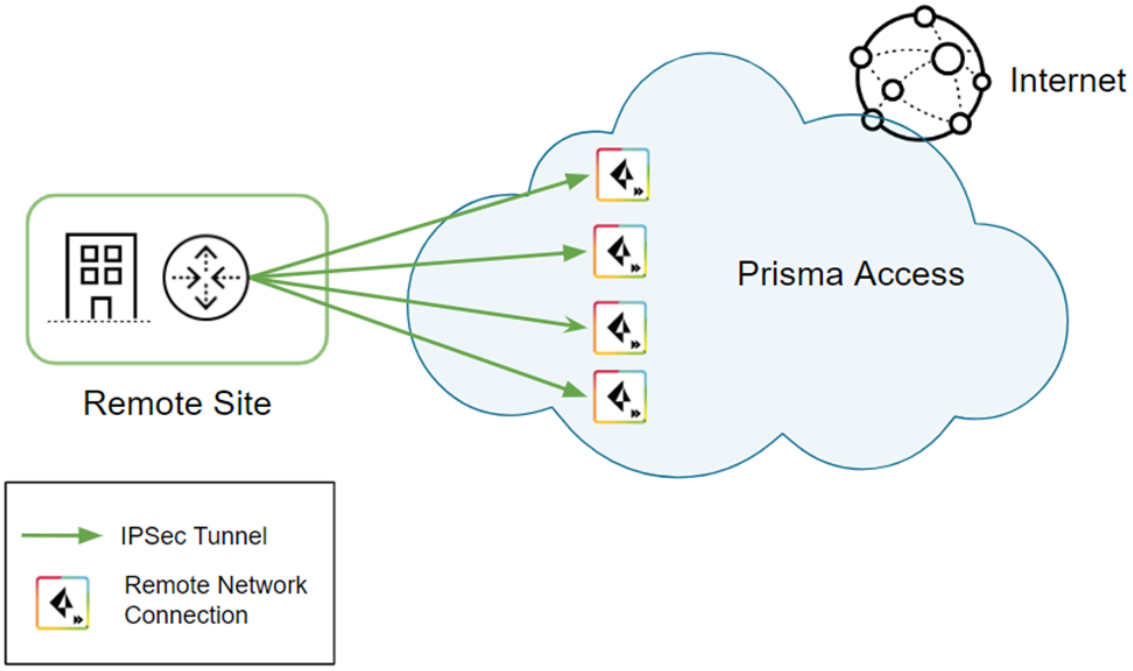
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

Prisma Accessへの高帯域幅接続を持つアウトバウンドインターネットアクセスに対して支店オフィスまたはサイトを保護するために、このセクションで説明している手順を実行して、複数のIPSecトンネルを使用して、支店オフィスまたはサイトからのトラフィックをロードバランシングすることができます。

次の図は、同じリモート サイトを使用する4つのリモート ネットワーク接続を示しています。オンボーディングの前に、コンピューティング場所（この例では韓国で、リモート サイトに対応）に4 Gbps (4000 Mbps) を割り当てます。4000 Mbpsでは4つのIPSec 終端ノードが提供され、各IPSec 終端ノードは最大1000 Mbpsの帯域幅を提供します。オンボーディング プロセス中に各リモート ネットワーク接続に独自のIPSec終端ノードを割り当てて、帯域幅全体を活用します。

この例では、*4*つのトンネルを使用しています。*Prisma Access*の高帯域幅接続に使用できるトンネルの最大数は、使用するロードバランシングプロトコル で顧客構内設備（*CPE*）がサポートする*IPSec*トンネルの最大数に基づいています。

©2025 Palo Alto Networks, Inc.



この設定をデプロイする前に、次の制限と推奨事項を考慮してください。

- IPSecトンネルには、BGPルーティングを使用してください。スタティックルーティングはサポートされていません。
- この設定はアウトバウンドインターネットアクセスにのみ使用してください。
- Prisma AccessまたはCPEのいずれかでトンネルモニタを使用しないでください。IPSecトンネルの可用性は、CPEとPrisma Accessリモートネットワーク間のBGPピアリングによって決まります。IPSecトンネルが停止して、BGP接続が中断された場合、そのトンネルにおいてBGP経由で学習されたルートは、ECMPから自動的に削除されます。
- トンネルの停止を判断するためにBGPを使用しているため、CPGに設定するHoldTimeの値を考慮してください。ホールド タイマーは、ルートを削除する前にトンネルがダウンしている時間を決定します。 Prisma AccessではRFC 4271で定義されているデフォルトのBGP HoldTime値90秒を使用します。リモートネットワークサイトのBGP CPEでこれより小さなHoldTime値を設定した場合、BGPはその値を使用します。Palo Alto Networksは、このデプロイ環境のCPEで、KeepAliveの値を10秒、HoldTimeの値を30秒に設定することをお勧めします。

高帯域幅のリモートネットワーク接続を作成するには、以下の手順に従ってください。

©2025 Palo Alto Networks, Inc.

STEP 1 | Panoramaで、Prisma Accessリモートネットワークトンネルを設定します。

1. （任意）まだ設定していない場合は、作成したリモートネットワークに対するIKEゲートウェイ、IKE暗号、およびIPSec暗号プロファイル、およびIPSecトンネルを設定します。

   IKEおよびIPSec暗号プロファイルを書き留めておきます。リモートネットワークロケーションのリモートネットワーク接続の終端として使用するCPEでも、同じ設定を指定する必要があります。

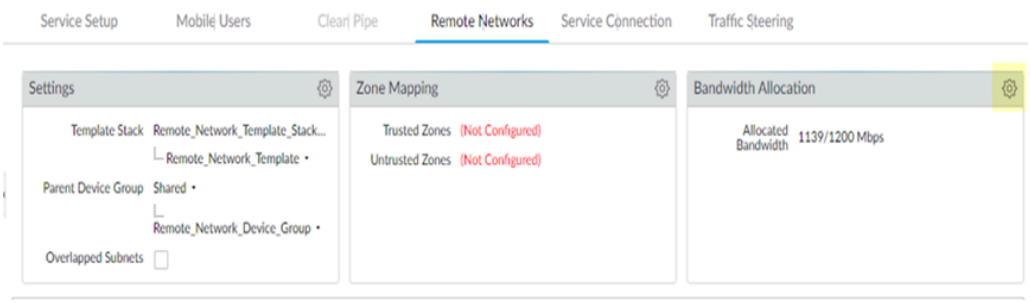
2. 使用しているリモート ネットワーク デプロイメントの種類を決定します。

   Prisma Accessデプロイメントでは、コンピューティング ロケーションごとに帯域幅を割り当てるか、ロケーションごとに帯域幅を割り当てることによって帯域幅を割り当てます。

3. リモート ネットワークをオンボードします。

   - コンピューティング ロケーションごとに帯域幅を割り当てるリモート ネットワークをオンボードするには:

     1. 帯域幅割り当て領域の歯車アイコンをクリックして、オンボードする場所に帯域幅を割り当てます。

     2. オンボーディングしたいPrisma Accessロケーションに関連する、各コンピュートロケーションに必要な帯域幅割り当てを入力します。
     3. ページ上部の [割り当てられた合計]フィールドに帯域幅が反映されるまで待ってから、[OK]をクリックします。

   - ロケーションごとに帯域幅を割り当てるリモート ネットワークをオンボードするには、次の手順に進みます。リモート ネットワークのオンボーディング中に帯域幅を割り当てます。

4. **Panorama** > **Cloud Services**（クラウドサービス） > **Configuration**（設定） > **Remote Networks**（リモートネットワーク）を選択して、次の設定を指定した4つのリモートネットワーク接続を作成します。

   - 各接続に対して同じ**Location**（ロケーション）を選択します。
   - **IPSec**終端ノードを選択します。

     リモート ネットワーク接続ごとに個別のIPSec終端ノードを選択します。

     ロケーションごとに帯域幅を割り当てるデプロイメントの場合は、***500 Mbps***の帯域幅を選択します。

©2025 Palo Alto Networks, Inc.

ライセンスされている帯域幅の総量を超える帯域幅を選択することはできません。この設定を使用して、このロケーションに割り当てる、ライセンスされた帯域幅の量を定義します。

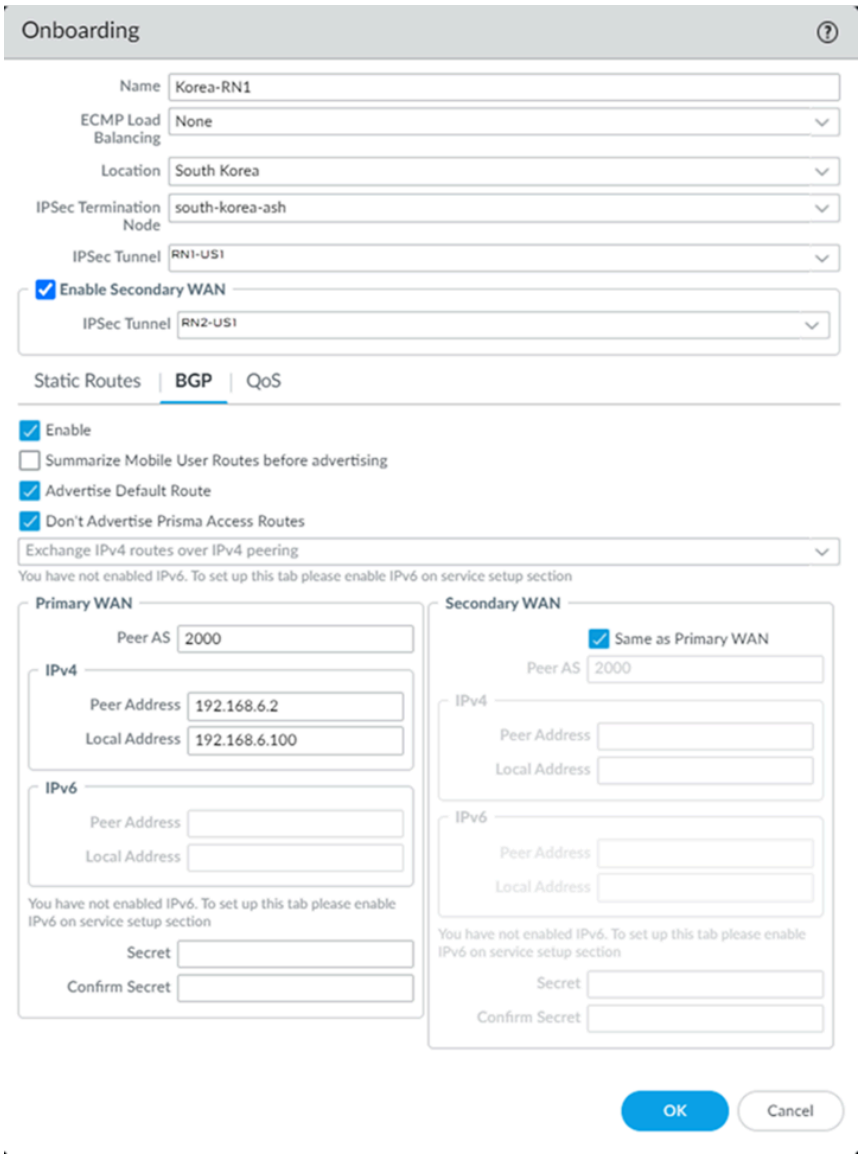
- BGPを有効にし 、 デフォルト ルートをアドバタイズし、**[Don't Advertise Prisma Access Routes (Prisma** アクセス ルートをアドバタイズしない**)]**を選びます。
- すべてのリモートネットワークに対して、同じ**Peer AS**を選択します。

  この例では、**Peer AS**として2000を指定しています。4つの接続すべてに対して、**Peer AS**に2000を指定してください。
- （任意）バックアップのリモートネットワークを作成する場合は、**Enable Secondary WAN**（セカンダリ**WAN**を有効にする）を選択して作成します。次に、バックアップトンネル用に作成した**IPSec Tunnel**（**IPSec**トンネル）を選択します。

セカンダリ WAN の設定は、次の展開ではサポートされていません。

- セカンダリ WAN がプライマリ IPsec トンネルを使用してアクティブ/アクティブモードに設定されている場合。
- 顧客宅内機器 (CPE) が、プライマリおよびセカンダリIPsecトンネルを使用する等コストマルチパス (ECMP) 構成で設定されている場合。

©2025 Palo Alto Networks, Inc.

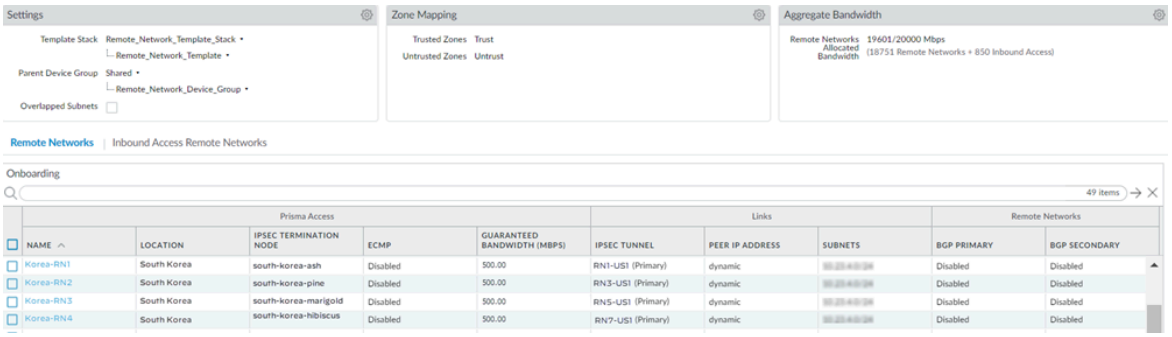


作業が完了したら、同じロケーションに対する4つの1000 Mbpsリモートネットワークができあがります。

ロケーションごとに帯域幅を割り当てるデプロイメントでは最大帯域幅が500 Mbpsであるため、この構成ではロケーションごとに500 Mbpsが提供されます。

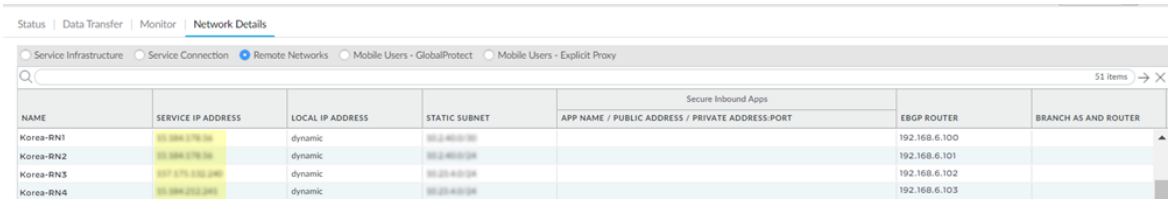
バックアップトンネルを設定した場合、フェイルオーバー目的で使用する4つのセカンダリトンネルも存在します。

©2025 Palo Alto Networks, Inc.



5. **[Panorama] > [Cloud Services**（クラウドサービス）**] > [Status**（ステータス）**] > [Network Details (**ネットワーク詳細**)] > [Remote Networks**（リモートネットワーク）**]**を選択して、**[Service IP Address (**サービス**IP**アドレス**)]** および **[EBGP**ルーター**]**アドレスのメモをとります。

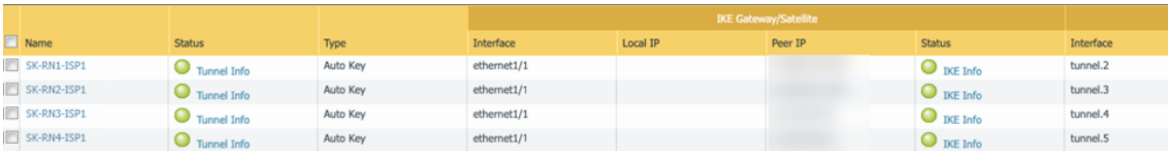
   リモートネットワークサイトのCPEで IPSecトンネルを構成する場合は、ピア またはIPアドレスとしてサービス**IP**アドレスを使用します。 CPEでスタティックルートを作成する場合は、これらのアドレスと**EBGP** ルーターのアドレスを使用します。



STEP 2 | リモートネットワークサイトのCPEで、リモートネットワークトンネルを設定します。

- これらのステップの設定作業では、*Palo Alto Networks*次世代ファイアウォールを使用しています。このデプロイの*IPSec*トンネルと*ECMP*をサポートしている任意の*CPE*デバイスを使用できます。
- 帯域幅のバランスは、*ECMP*の*CPE*ハッシュに依存します。しかし、*Prisma Access*はトラフィックの対称的なリターンを保証します。

1. アクティブなCPEから4つのネットワーク接続それぞれへの、4つのアクティブなトンネルを作成します。ピア**IP**アドレスには、前のステップでPrisma Accessから受け取ったリモート ネットワークのサービス**IP**アドレスを入力します。



2. （任意）バックアップトンネルを作成する場合、アクティブなCPEから4つのネットワーク接続それぞれへのトンネルを作成します。ピア**IP**アドレスには、前の手順

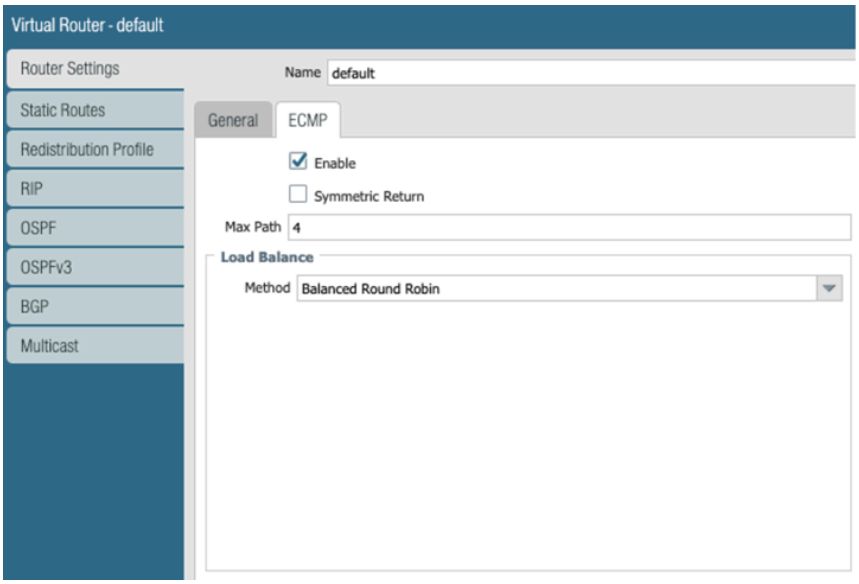
 ©2025 Palo Alto Networks, Inc.

でPrisma Accessから受け取ったリモートネットワークのサービス**IP**アドレスを入力します。

	Name	Status	Type	IKE Gateway/Satellite				
				Interface	Local IP	Peer IP	Status	Interface
	SK-RN1-ISP2	Tunnel Info	Auto Key	ethernet1/1			IKE Info	tunnel.2
	SK-RN2-ISP2	Tunnel Info	Auto Key	ethernet1/1			IKE Info	tunnel.3
	SK-RN3-ISP2	Tunnel Info	Auto Key	ethernet1/1			IKE Info	tunnel.4
	SK-RN4-ISP2	Tunnel Info	Auto Key	ethernet1/1			IKE Info	tunnel.5

STEP 3 | リモートネットワークサイトのCPEで、ECMPを設定します。

1. **Network (**ネットワーク**) > Virtual Routers (**仮想ルーター**)**を選択します。
2. **default**（デフォルト） の仮想ルーターを編集するか、新しい仮想ルーターを**Add**（追加）します。
3. **Router Settings**（ルーター設定） > **Enable**（有効） > **ECMP**を選択し、ECMPを**Enable**（有効）にして、**Max Path**（最大パス）に**4**を、ロードバランシングの**Method**（方法）に**Balanced Round Robin**（均等ラウンド ロビン）を指定します。



STEP 4 | リモート ネットワーク サイトのCPE上で、前の手順で取得したPrisma Access サービス**IP**アドレス と **EBGP**ルータIPアドレスへのスタティック ルートを作成します。

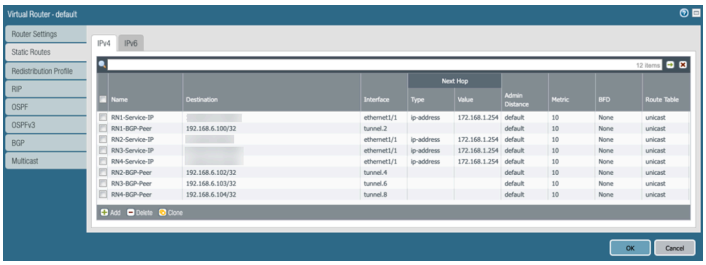
前述したように、この設定ではBGPによるダイナミックルーティングが必要です。CPEとPrisma AccessのeBGPルーター間のBGP接続を容易にするために、CPEのeBGPルーターIPアドレスに対するスタティックルートを追加する必要があります。また、次のホップはCPEのトンネルインターフェースでなければなりません。残りのト

 ©2025 Palo Alto Networks, Inc.

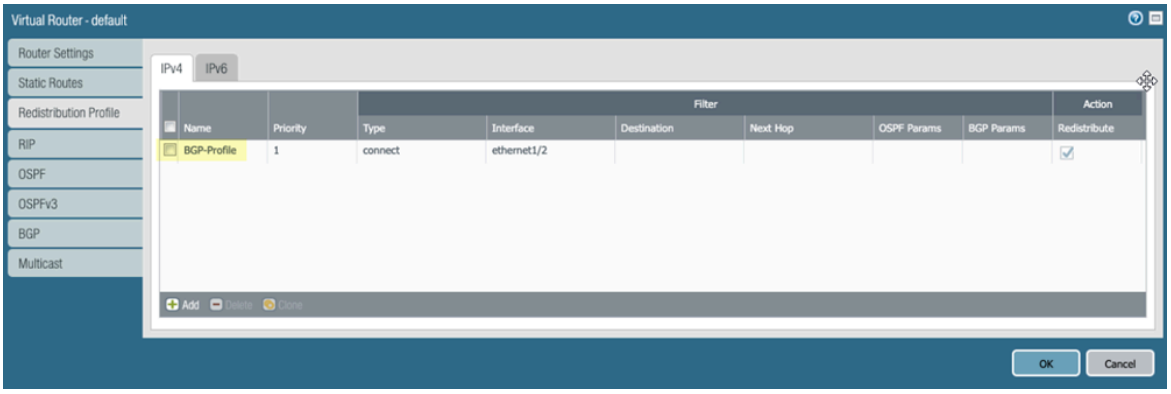
ンネルの他のすべてのリモートネットワークeBGPルーターIPアドレスに対しても、この手順を繰り返す必要があります。

アクティブなCPEのルートの例を次に示します。スタンバイCPEでバックアップトンネルを作成した場合は、スタンバイCPEでも同じルーティングを作成してください。

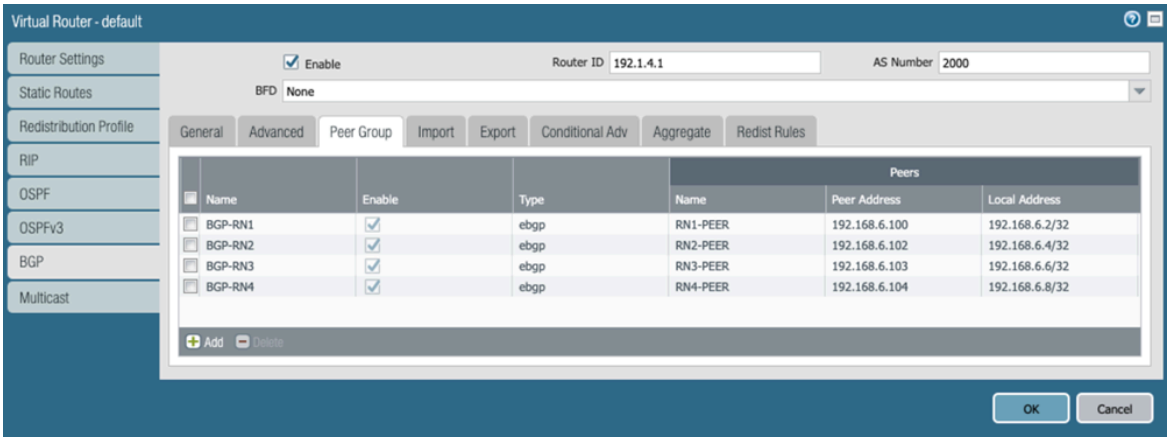
Palo Alto Networks次世代ファイアウォールを設定している場合、**Static Routes**（スタティックルート） > **IPv4**を選択してスタティックルートを追加します。



STEP 5 | [再配信プロファイル] > **[IPv4]**を選択し、IPv4ルート再配信プロファイルを追加して 、CPEでのルート再配信を有効にします。

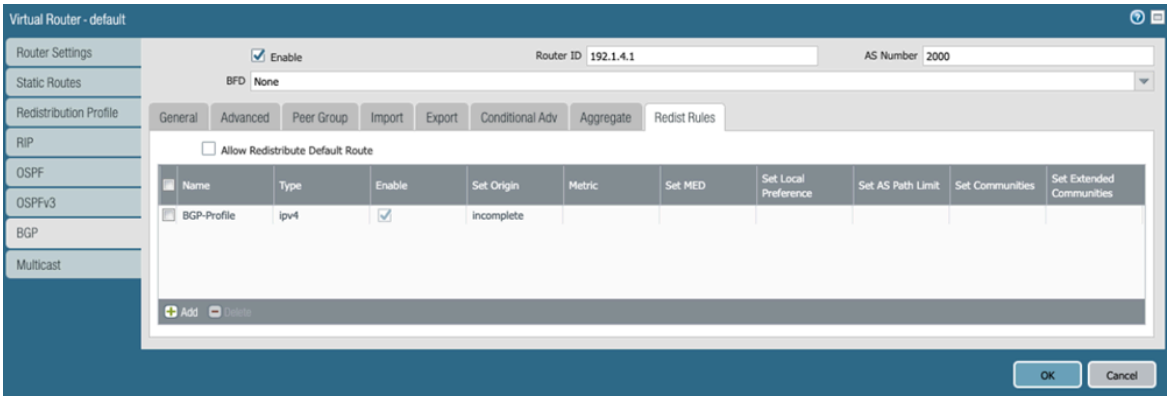


STEP 6 | **BGP** > **Peer Group**（ピアグループ）を選択し、仮想ルーターインスタンス上でBGPを**Enable**（有効）にしてから、リモートネットワークBGPピアを**Add**（追加）します。



 ©2025 Palo Alto Networks, Inc.

STEP 7 | **BGP** > **Redist Rules**（再配信ルール）を選択して、前のステップで作成したルート再配信プロファイルを添付します。

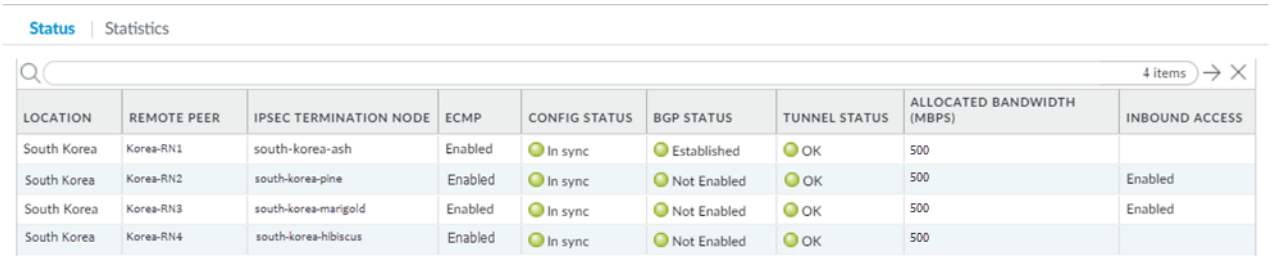


STEP 8 | CPEが4つのトンネルすべてで、トラフィックを通過させていることを確認します。

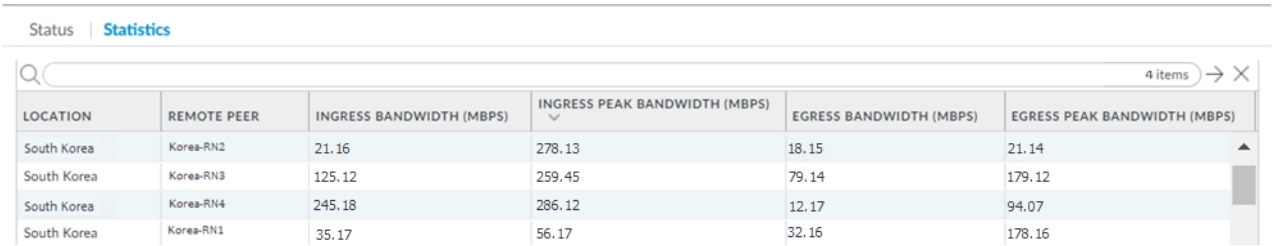
STEP 9 | Prisma Accessからの、ECMPを有効にした接続のステータスを確認します。

- **Panorama** > **Cloud Services**（クラウドサービス） > **Monitor**（監視） > **Remote Networks**（リモートネットワーク）を選択して、ECMP接続をデプロイしたリージョンを選択し、次に**Status**（ステータス）を選択します。

  - ここで、***ECMP***には***No***が表示されます。*Prisma Access*のECMP load balancing（ECMPロードバランシング）機能を設定していないため、これは想定通りの表示になります。
  - *ECMP*は*CPE*から*Prisma Access*への指向性であり、*Prisma Access*は*CPE*からのトラフィックの対称的な返送を保証する。



- **Statistics**（統計情報）を選択して、各リモートネットワークトンネルをトラフィックが通過していることを確認します。



このワークフローを完了したら、リモートネットワーク用高帯域幅設定の作成作業が終了します。このソリューションは、アウトバウンドトラフィックのみに対応していることを忘れないようにしてください。

©2025 Palo Alto Networks, Inc.

Clean Pipe向けPrisma Access

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

クリーンアウトバウンドインターネット接続の複数のインスタンスを素早く手軽に設定するには、 *Clean Pipe向けPrisma Access*を使用します。

これは、*Prisma Access (Managed by Strata Cloud Manager)*に対してサポートされていません。

Clean Pipe向けPrisma Accessの概要

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

サービスプロバイダ、MSSP、またはTelcosなどの、他の組織のITインフラを管理している組織を許可し、そのテナントのアウトバウンド インターネット トラフィックを素早く手軽に保護するために、Palo Alto NetworksはClean Pipe向けPrisma Accessを提供しています。サービスプロバイダ、MSSP、またはTelcoは、Partner Interconnectを使って、顧客（テナントとして設定）をClean Pipe向けPrisma Accessにルーティングできます。トラフィックがPartner Interconnectを通過すると、それはセキュリティ確保のためにテナント専用のClean Pipeインスタンスに送信され、次にインターネットにルーティングされます。

Clean Pipe向けPrisma Accessには、テナント用のClean Pipeを素早く手軽に作成するために使用できるAPIも用意されています。

Clean Pipeの使用事例

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

次の事項すべてに該当する場合は、Clean Pipe向けPrisma Accessを使用してください。

- 多数のテナントを持つネットワークデプロイ環境を管理している。

  たとえば、多数の異なる組織のネットワーク（最高数万件）を保守管理しているサービスプロバイダ、Telco、またはMSSPなどがこれに該当します。
- デプロイ環境内の各テナントの、アウトバウンド インターネット トラフィックを保護する手段を必要としている。
- ネットワークを管理している組織向けに、Clean Pipeをオンボーディングする素早くスケーラブルな方法を求めている。
- アウトバウンド インターネット セキュリティを例外として、管理しているネットワークのモバイルユーザー、本社、または支店のロケーションを保護する追加の要件はありません。

  追加のセキュリティ要件がある場合は、Clean Pipeを導入する代わりに、Prisma Accessで複数のテナントを作成することをお勧めします。そうすることで、個別のリモートネットワークおよびモバイルユーザーのグループに対する、セキュリティポリシーを作成して適用することができます。

©2025 Palo Alto Networks, Inc.

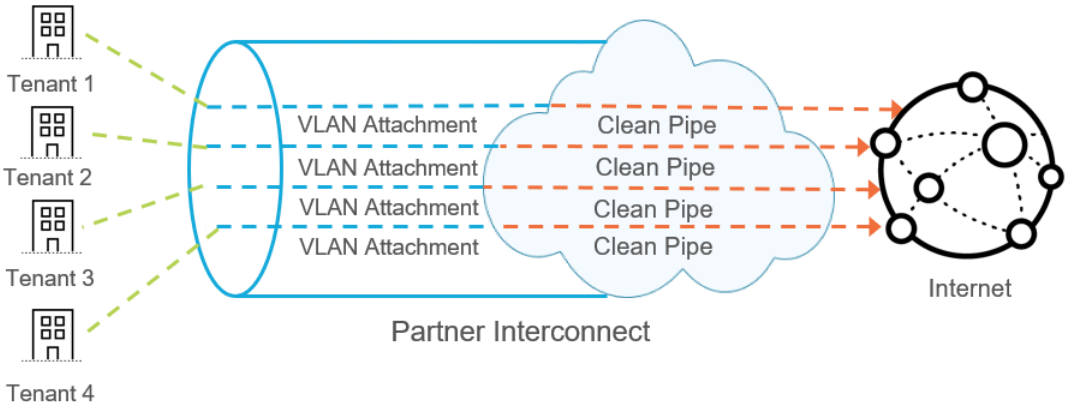
Clean Pipeの例

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

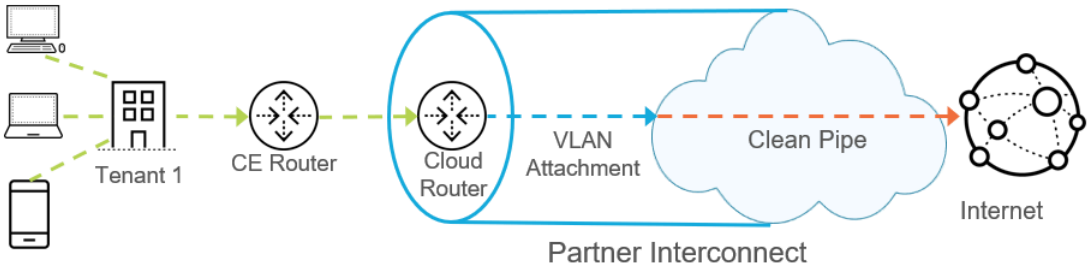
単一のテナントに対して設定されているClean Pipeの例を、次の図に示します。テナントに対して、複数のClean Pipeが設定されています。

この例で、サービスプロバイダは4つの組織のインターネット接続を管理しており、それらのアウトバウンド インターネットアクセスを保護したいと考えています。サービスプロバイダは、Google Cloud Platform（GCP）Partner Interconnectを作成して、各テナントに対してVLANアタッチメントを作成します。サービスプロバイダは、VLANアタッチメントのセキュリティを作成するために、Panoramaを使ってClean Pipe用のPrisma Accessを設定します。

この例では、テナントあたり1つのClean Pipeが用意されています。単一のテナント内に複数のClean Pipeを作成することもできます。テナントに対して指定する各Clean Pipeが、異なるロケーションを使用していることを確認してください。



インターネットへのクリーン接続を必要としているテナントに対する、単一のClean Pipeの詳細を次の図に示します。Customer Edge（CE）ルーターは、テナントにWAN接続を提供します。CEルーターはクラウドルーターに接続し、クラウドルータはPartner Interconnectに対する接続性を提供しています。サービスプロバイダはテナント用にVLANアタッチメントを作成し、VLANアタッチメントにセキュリティを提供するClean Pipe用のPrisma Accessを、Panoramaで設定します。そうすることで、テナントのインターネットベースのトラフィックを保護します。



©2025 Palo Alto Networks, Inc.

Clean PipeおよびPartner Interconnectの要件

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	❑ Prisma Accessのライセンス

開始する前に、次のClean Pipeデプロイメント要件を認識し、Clean Pipe のPrisma Accessと他のPrisma Accessデプロイメントの次の違いに注意してください。

- Clean Pipe用のPrisma Accessのライセンスが必要です。

  Clean Pipe用のPrisma Accessライセンスは、他のPrisma Access製品のライセンスとは個別のライセンスです。ただし、PanoramaおよびStrata Logging Serviceライセンスの購入およびインストールと同じ要件が、Clean Pipeにも適用されます。
- Clean Pipe用のPrisma Accessには、次のGCP Partner Interconnect要件があります：
  - GCPで、Partner Interconnectを作成できる必要があります。
  - GCPで、VLANアタッチメントを作成できる必要があります。
  - レイヤー2（L2）パートナーの相互接続の場合、MSSP側でCEルーターへのアクセスが必要で、それの設定を変更できる必要があります。

  GCP設定の詳細は、GCPのドキュメントを参照してください。
- Clean Pipeデプロイ環境の最低帯域幅要件に注意してください。

  購入できる最低ライセンスは、1000 Mbpsです。各Clean Pipeの最低帯域幅割り当ては、100 Mbpsです。

  テナントの作成後、そのテナントのClean Pipeを作成できます。各Clean Pipeは、最低100 Mbpsでなければなりません。各Clean Pipeは、テナントのアクセスドメイン、テンプレートとテンプレートスタック、およびデバイスグループを共有します。
- 単一のテナントに対して複数のClean Pipeを設定している場合、各Clean Pipeは個別のロケーションに配置する必要があります。同じゾーン（intrazone）内の冗長性用アクティブ/バックアップ構成のため、単一のClean Pipeロケーションに対して2つのVLANアタッチメントを設定したい場合、新しいClean Pipeインスタンスを追加する際に、**REDUNDANT**（冗長）を指定します。
- Clean Pipeテナント内で接続を作成する場合、VLANアタッチメントと同じ帯域幅を割り当ててください。接続の帯域幅より大きい、または小さい帯域幅を持つVLANアタッチメントを作成しないでください。
- マルチテナント機能を有効にした後、Configuration（設定）エリアの他のタブでClean Pipeデプロイ環境を設定しないでください。ただし、Clean PipeIP アドレスを取得するためのAPI鍵を生成する、**[Service Setup**（サービスのセットアップ）]タブの**[Generate API key**（**API**鍵の生成）]リンクは例外です。すべての構成は、クリーン パイプのPrisma Accessに固有のものであり、ネットワークのPrisma Accessやユーザーの Prisma Accessなどの他のPrisma Accessデプロイメントとは別です。
- Clean Pipe設定のコミット後は、それを変更しないでください。コミット後にClean Pipe設定を変更すると、それを再コミット時にコミットエラーが発生します。代わりに、既存のClean

©2025 Palo Alto Networks, Inc.

Pipeを削除してから、新しいClean Pipeを追加してください。この変更は、システムのダウンタイム期間中にスケジュールしてください。変更を行ってしまったけれども、まだコミットしていない場合は、Clean Pipe設定を編集して元の値に戻すことができます。

- Clean Pipe が使用する場所は、他のPrisma Accessデプロイメントとは異なることに注意してください。 Clean Pipe用のPrisma Accessは次のロケーションをサポートしています。
  - 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
- 次の、Clean Pipeネットワーク制限に注意してください。
  - Clean Pipe用のQoSは、入口（インターネットからClean Pipeへの方向）のみサポートされています。
  - User-IDはサポートされていません。
  - Clean Pipeは、ソース/宛先IPアドレスに基づくセッションアフィニティをサポートしています。設定を変更することはできません。
  - トラフィックは常にインターネット宛てのため、Clean Pipeに対してTrust-to-Trustポリシーは無効です。Trust-to-Untrustポリシーのみを使用してください。

©2025 Palo Alto Networks, Inc.

Clean Pipe設定の完了

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	• Prisma Accessのライセンス

Clean Pipe向けのPrisma Accessの設定を完了するには、Partner InterconnectおよびPanoramaで設定作業を行います。

*Partner Interconnect*の*Partner Interconnect*（*Prisma Access*ではない）側にある、*CE*およびクラウドルーターにアクセスでき、設定が可能であることを確認してください。

STEP 1 | Partner Interconnect側の設定で、Panoramaから取得した**Pairing Key**（ペアリングキー）を使用して、VLANアタッチメントを作成します。

Partner InterconnectでのVLANアタッチメントの作成、およびCEルーターのクラウドルーターとの通信設定の詳細は、https://cloud.google.com/interconnect/docs/にあるGoogle Cloudドキュメントを参照してください。

選択したロケーションと帯域幅が、Panoramaで指定した**Location**（ロケーション）と一致していることを確認してください。Partner Interconnectで使用するサービスプロバイダは、ペアリングキー、および要求された接続ロケーションと容量を使って、VLANアタッチメントの設定を完了します。

STEP 2 | 接続が有効になったら、Panoramaに戻って**Panorama** > **Cloud Services**（クラウドサービス） > **Status**（ステータス） > **Network Details**（ネットワーク詳細） > **Clean Pipe**の順に選択して、**MSSP CE**および**Cloud Router IP**（クラウドルーター**IP**）アドレスを記録しておいてください。

これらの値は、VLANアタッチメントのもう一方の側に**Pairing Key**（ペアリングキー）を入力した後に記入されます。



 ©2025 Palo Alto Networks, Inc.

STEP 3 | CEルーターにログインして、次の設定作業を行います。

1. **MSSP CE**アドレスを、ローカルIPアドレスとして入力します。
2. **Cloud Router IP**（クラウドルーター**IP**）アドレスを、ピアIPアドレスとして入力します。
3. PanoramaでのClean Pipeの設定時に入力した**BGP Peer ASN**と一致する、BGP ASNを入力します。

   正しい値を入力したことを確認してください。これらの値を後で変更することはできません。

STEP 4 | Clean Pipeステータスを確認します。

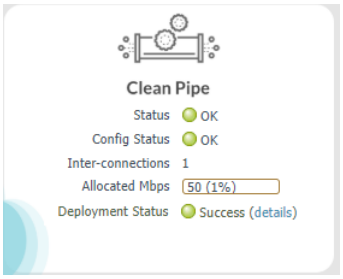
1. Panoramaで、**Panorama** > **Cloud Services**（クラウドサービス） > **Status**（ステータス）の順に選択して、ドロップダウンから**Tenant**（テナント）を選択して、Clean Pipeの**Status**（ステータス）を確認します。

   許容値については、Prisma Accessロケーションのリストを参照してください。

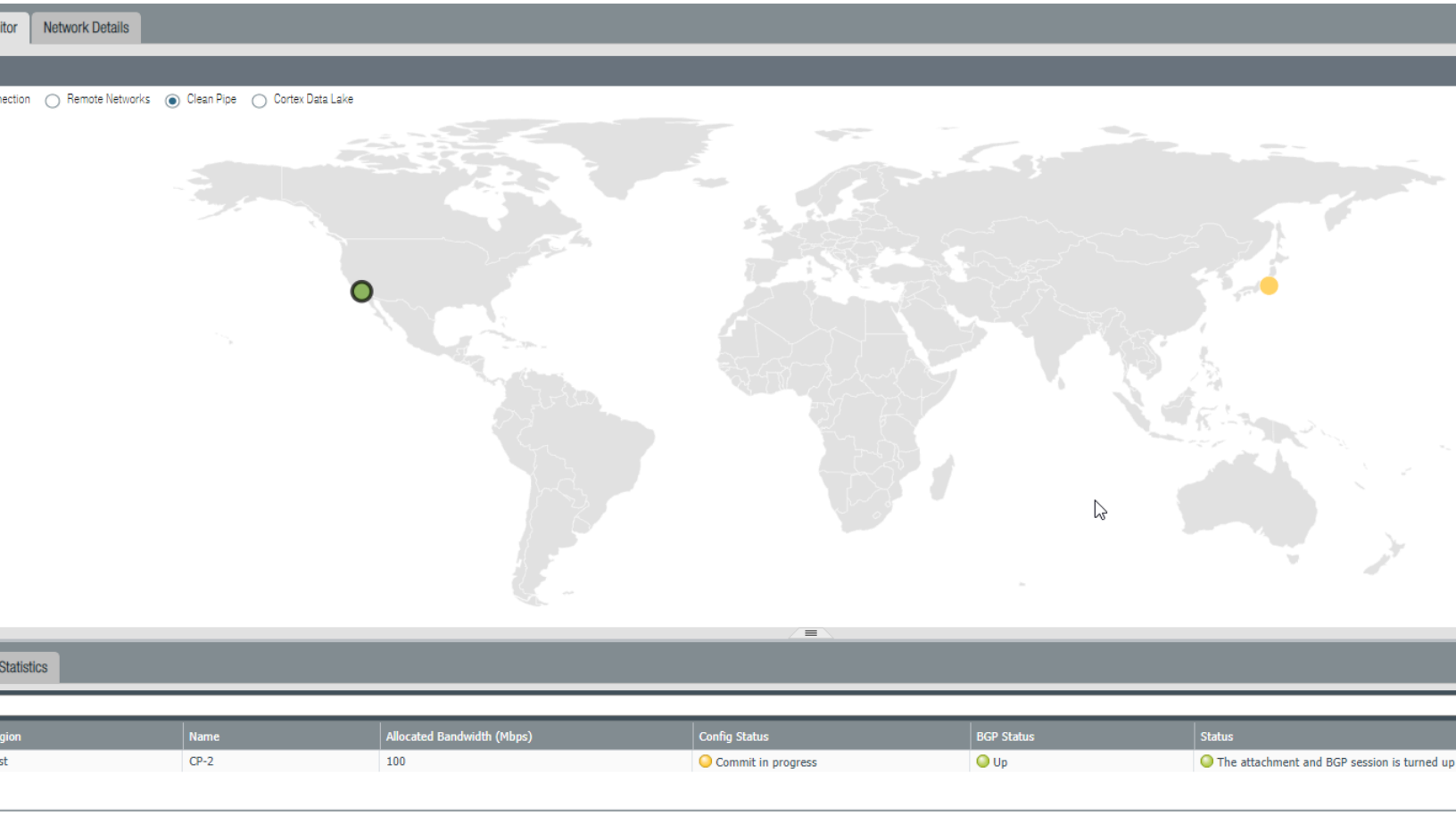
   Deployment Status（デプロイステータス）では、オンボーディングおよびデプロイジョブのステータスを参照することができます。また、完了したジョブのステータスに

©2025 Palo Alto Networks, Inc.

関する詳細情報も参照することができます。詳細については、「デプロイメントの進行状況とステータス」を参照してください。



2. **Panorama** > **Cloud Services**（クラウドサービス） > **Status**（ステータス） > **Clean Pipe**の順に選択して、**Monitor**（監視）タブをクリックして、デプロイされているClean Pipeのマップとステータスを参照します。



マップの下にあるタブをクリックすると、Clean Pipeに関するその他の統計情報が表示されます。

Status（ステータス）タブ：

- **Compute Region**—Clean Pipeインスタンスに対して、クラウドサービスインフラがデプロイされているCompute Region。
- **Name**（名前）—Clean Pipeインスタンスの名前。

©2025 Palo Alto Networks, Inc.

- **Allocated Bandwidth (Mbps)**（割り当てられている帯域幅）—Clean Pipeインスタンスに割り当てた帯域幅。
- **Config Status**（設定ステータス）—サービスへの設定の最後のプッシュのステータス。ローカルで変更を行ったけれども、まだクラウドに設定をプッシュしていない場合、ステータスには**Out of sync**（非同期）が表示されます。ステータスインジケータ上にカーソルを移動すると、詳細情報が表示されます。設定をPrisma Accessにコミットしてプッシュすると、Config Statusが**In sync**になります。
- **BGP Status**（**BGP**ステータス）—Clean Pipeインスタンスのファイアウォールまたはルーターと Prisma Access間の、BGP状態に関する情報を表示します。一時的にステータスが各種BGP状態（**idle**、**active**、**open send**、**open pend**、**open confirm**）に切り替わることがありますが、一般的にBGPステータスには次のような項目が表示されます。
  - **Connect**（接続）—Clean Pipeインスタンスのルーターが、クラウドファイアウォールとのBGPピアリレーションシップの確立を試みています。
  - **Established**（確立済み）—BGPピアリレーションシップが確立されています。

    このフィールドには、BGP接続がエラー状態にあるかどうかも表示されます。
  - **Warning**（警告）—8分間以上に渡ってBGPステータスの更新がありません。ファイアウォールが機能停止している可能性があります。

©2025 Palo Alto Networks, Inc.

  - **Error**（エラー）—BGPステータスが不明です。
- **Status**（ステータス）—Prisma AccessとClean Pipeインスタンス間の接続の運用ステータス。

Statistics（統計）タブ：

- **Region**（地域）—Clean Pipeインスタンスに対して、クラウドサービスインフラがデプロイされている地域。
- **Name**（名前）—Clean Pipeインスタンスの名前。
- **Allocated Bandwidth (Mbps)**（割り当てられている帯域幅）—リモートネットワークロケーションに割り当てた帯域幅。
- **QoS**— グラフィカルなQoS統計情報を表示するには、**QoS**を選択します。
- **Avg Egress Bandwidth 5 Min**（**Mbps**）（**5**分間の平均発信帯域幅）—5分間に渡るClean Pipe発信帯域幅の平均値。
- **Avg Egress Bandwidth 60 Min**（**Mbps**）（**60**分間の出口発信帯域幅）—60分間に渡るClean Pipe出口帯域幅の平均値。
- **Avg Ingress Bandwidth 5 Min**（**Mbps**）（**5**分間の平均着信帯域幅）—5分間に渡るClean Pipe着信帯域幅の平均値。
- **Avg Ingress Bandwidth 60 Min**（**Mbps**）（**60**分間の平均入口帯域幅）—60分間に渡るClean Pipe入口帯域幅の平均値。
- **Egress Peak Bandwidth 1 Hour**（**Mbps**）（**1**時間のピーク発信帯域幅）—過去1時間におけるClean Pipeインスタンスのピーク発信帯域幅。
- **Egress Peak Bandwidth 24 Hour**（**Mbps**）（**24**時間のピーク発信帯域幅）—過去24時間におけるClean Pipeインスタンスのピーク発信帯域幅。
- **Egress Peak Bandwidth 7 Days**（**Mbps**）（**7**日間のピーク発信帯域幅）—過去7日間におけるClean Pipeインスタンスのピーク発信帯域幅。
- **Egress Peak Bandwidth 30 Days**（**Mbps**）（**30**日間のピーク出口帯域幅）—過去30日間におけるClean Pipeインスタンスのピーク出口帯域幅。
- **Ingress Peak Bandwidth 1 Hour**（**Mbps**）（**1**時間のピーク着信帯域幅）—過去1時間におけるClean Pipeインスタンスのピーク着信帯域幅。
- **Ingress Peak Bandwidth 24 Hour**（**Mbps**）（**24**時間のピーク着信帯域幅）—過去24時間におけるClean Pipeインスタンスのピーク着信帯域幅。
- **Ingress Peak Bandwidth 7 Days**（**Mbps**）（**7**日間のピーク着信帯域幅）—過去7日間におけるClean Pipeインスタンスのピーク着信帯域幅。
- **Ingress Peak Bandwidth 30 Days**（**Mbps**）（**30**日間のピーク入口帯域幅）—過去30日間におけるClean Pipeインスタンスのピーク入口帯域幅。

©2025 Palo Alto Networks, Inc.

マルチテナント機能の有効化とテナントの作成

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Panorama)	• Prisma Accessのライセンス

Clean Pipe設定を開始する前に、Panoramaでマルチテナントデプロイ環境を作成し、1つまたは複数のテナントを作成します。

STEP 1 | Clean PipeのPrisma Accessをインストールしてアクティブにします。

Prisma Access向けのClean Pipeには個別のライセンスが必要で、アクティブ化するとCloud ServicesプラグインにClean Pipe固有のタブが作成されます。Clean Pipe用のPrisma Accessをインストールする手順は、Cloud Servicesプラグインのインストールを含め、Prisma Accessライセンスをアクティベートしてインストールする手順と同じです。

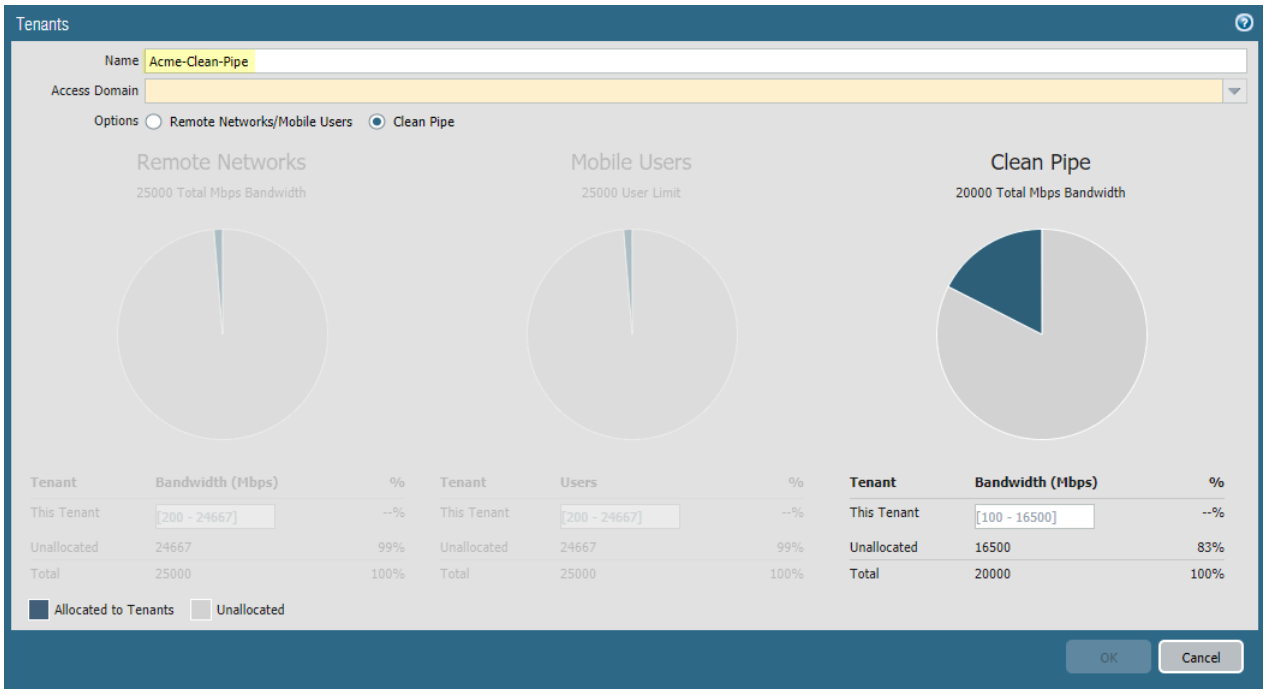
©2025 Palo Alto Networks, Inc.

STEP 2 | まだ有効化していない場合は、マルチテナント機能を有効にします。

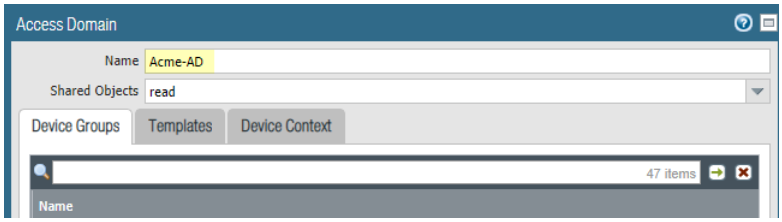
1. **Panorama** > **Cloud Services**（クラウドサービス） > **Configuration**（設定）を選択します。
2. **Enable Multitenancy**（マルチテナント機能を有効にする）（ページの右上にあります）を選択します。
3. **OK** をクリックします。

   Tenants（テナント）ページが表示されます。
4. **Options**（オプション）で、**Clean Pipe**を選択します。

   リモート ネットワーク、モバイルユーザー、またはその両方のためにテナントを構成するには、Prisma Access の「複数のテナントを管理する」を参照してください。



5. 最初のテナントの**Name**（名前）を入力します。
6. 最初のテナント向けの新しい**Access Domain**（アクセスドメイン）を作成、設定して、**OK**をクリックします。



7. **Clean Pipe**エリアで、**This Tenant**（このテナント）の**Bandwidth**（**Mbps**）（帯域幅）を入力します。

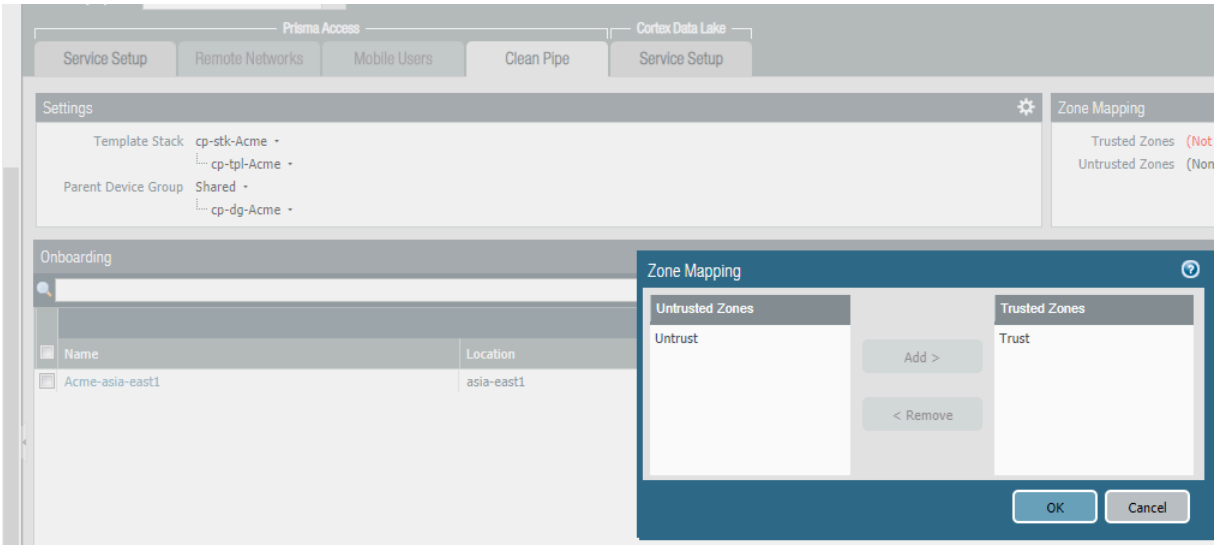
   作成する各テナントに対して、最低100 Mbpsの帯域幅を入力してください。
8. **OK** をクリックします。

©2025 Palo Alto Networks, Inc.

STEP 3 | テナントのゾーンを作成して、それらのゾーンをマップします。

1. **[Network] > [ゾーン]** の順に選択します。

   作成したテナントのClean Pipe **Template**（テンプレート）（**cp-tpl-***tenant*）を選択していることを確認します。
2. テナントのゾーンを作成します（例：**Trust**および**Untrust**）。
3. **Panorama > Cloud Services**（クラウドサービス） **> Configuration**（設定）の順に選択して、ドロップダウン リストから**Tenant**（テナント）を選択します。
4. **Clean Pipe**タブを選択します。
5. 設定を編集するには、**Zone Mapping**（ゾーンマッピング）の隣にあるアイコンをクリックします。
6. 作成したゾーンを**Add**（追加）および**Remove**（削除）して、それらをトラスト ゾーンおよび信頼しないアントラスト ゾーンにマップします。



STEP 4 | 新しいClean Pipeをオンボードします。

1. **Panorama > Cloud Services**（クラウドサービス） **> Configuration**（設定） **> Clean Pipe**の順に選択します。
2. テナントの新しいClean Pipeインスタンスを**Add**（追加）して、次の情報を入力します。

   - **Name**（名前） – Clean Pipeの名前を入力します。
   - **Bandwidth**（帯域幅）–Clean Pipeに割り当てる帯域幅を選択します。

     Clean Pipeインスタンスは、100 Mbps、200 Mbps、300 Mbps、400 Mbps、500 Mbps、1000 Mbps、2000 Mbps、5000 Mbps、および10000 Mbps単位でオンボーディングできます。指定する帯域幅は、ライセンスされている帯域幅割り当て以内

©2025 Palo Alto Networks, Inc.

でなければなりません。また、Partner Interconnectで作成するVLANアタッチメントの帯域幅と同じにする必要があります。

- **Edge Availability Domain**（エッジアベイラビリティドメイン）—Clean Pipe用のアベイラビリティドメインを選択します。**1**、**2**、**ANY**（任意）、または**REDUNDANT**（冗長）を選択できます。
  - 非冗長構成Clean Pipeデプロイの場合は、**ANY**（任意）を指定します。

    ご利用のクラウドプロバイダがこの選択項目をサポートしていることを確認してください。クラウドプロバイダ側のパートナー相互接続でも、**ANY**（任意）を選択する必要があります。ご利用のクラウドプロバイダで選択項目が利用できない場合は、別の項目を選択してください。
  - アクティブ/バックアップ構成で、同じロケーションの2つのVLANアタッチメントを指定する場合は、**REDUNDANT**（冗長）を選択します。

    REDUNDANT（冗長）構成用に2つのペアリングキーが作成され（各アベイラビリティゾーンに対してそれぞれ1つ）、最初のアベイラビリティゾーンの場合はzone1が、2番目のアベイラビリティゾーンにはzone2がClean Pipe名に追加されます。たとえば、**[Name (**名称**)]**に**[San Francisco]**を指定すると、Prisma

©2025 Palo Alto Networks, Inc.

Accessは**[San Francisco-zone1]** と **[San Francisco-zone2]**という 2 つのゾーンを作成します。

最初のアベイラビリティ ゾーン*(zone1)*を*CPE*のプライマリ ゾーンとして設定してください。

単一テナントの冗長性のために、異なるロケーションでClean Pipeのペアを作成することもできます。その場合、あるロケーションにある最初のClean Pipeには**1**を、別のロケーションにある2番目のClean Pipeには**2**を指定してください。

- **BGP Peer ASN**—BGP ASNを入力します。

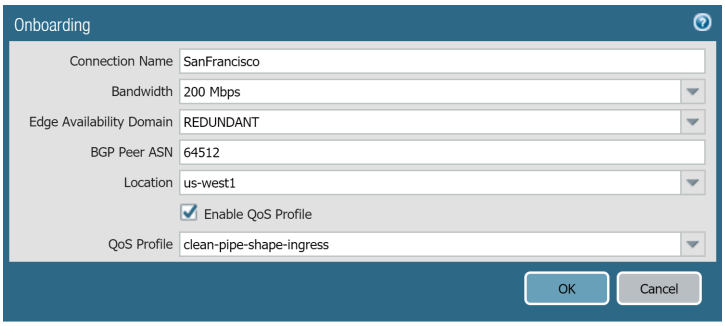
  プライベートまたはパブリックBGP ASNを指定できます。

  この値を記録しておいてください。Clean Pipe設定の完了時に、CEルーターにこの値を設定します。

- **Location**（ロケーション）–ロケーションを選択します。

  Partner Interconnect向けのVLANアタッチメントの作成時に使用するロケーションと、同じロケーションを使用することをお勧めします。

- QoSを有効にするには、**QoS**を選択して、次にClean Pipeで使用するQoS Profile（QoSプロファイル）を選択します。Clean Pipe QoSは、入口で形成されます。



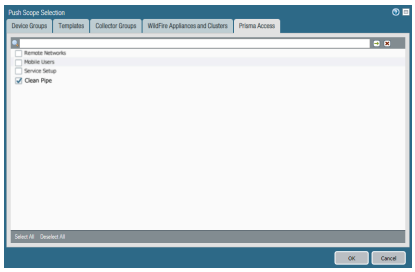
STEP 5 | 他のClean Pipeインスタンスを追加するには、ステップ4を繰り返してください。

追加の各Clean Pipeは、個別のロケーションを使用するようにしてください。

©2025 Palo Alto Networks, Inc.

STEP 6 | 変更をコミットしてプッシュし、Prisma Accessでアクティブにします。

1. **Commit**（コミット） > **Commit and Push**（コミットしてプッシュ）の順に選択し、Push Scope（プッシュ スコープ）で **Edit Selections**（選択内容の編集）を行います。
2. **Prisma Access**を選択し、次に**[Clean Pipe]**を選びます。



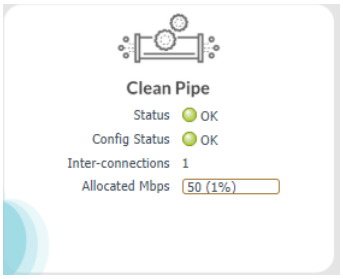
3. **OK** をクリックして、プッシュ スコープに対する変更を保存します。
4. 変更をコミットしてプッシュします。

STEP 7 | Clean Pipeがプロビジョニングされていることを確認します。

1. **Panorama** > **Cloud Services**（クラウドサービス） > **Status**（ステータス）を選択します。
2. ページ上部にあるドロップダウンリストから、**Tenant**（テナント）を選択します。
3. **Status**（ステータス）をクリックします。

   Clean Pipeのステータスが表示されます。
4. Clean Pipeの**Config Status**（設定ステータス）上にカーソルを移動して、ステータスが**Provisioning in Progress**（プロビジョニング中）から**Provisioned**（プロビジョニング完了）になるまで待機してください。待機してください。

   このプロビジョニングは、最高で30分かかる場合があります。



STEP 8 | **Network Details**（ネットワーク詳細）タブをクリックして、**Clean Pipe**ラジオボタンをクリックし、**Pairing Key**（ペアリングキー）を記録しておいてください。。

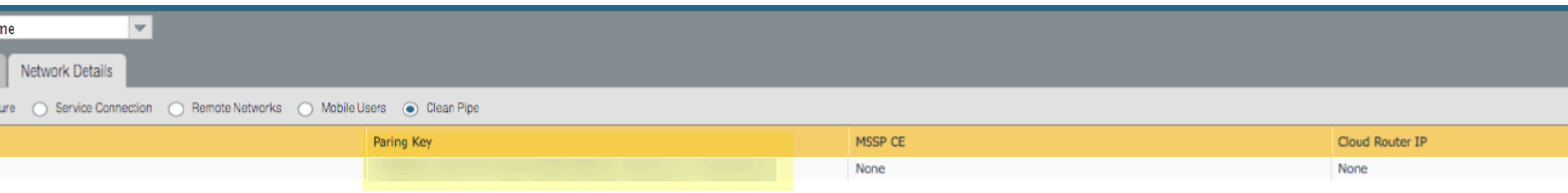
Clean Pipe設定の開始時に、**MSSP CE**および**Cloud Router IP**（クラウドルーター**IP**）フィールドは空欄になっています。これらのフィールドは、Clean Pipe設定が完了して、VLANアタッチメントを作成した後に記入されます。

REDUNDANT（冗長）接続を指定した場合、2つのペアリングキーが作成され（各アベイラビリティゾーンに対してそれぞれ1つ）、Clean Pipe名に最初のアベイラビリティゾーンの場合はzone1が、2番目のアベイラビリティゾーンにはzone2が追加されます。冗長構成の**SanFrancisco**（サンフランシスコ） Clean Pipeを次の画像に示します。Prisma Accessで

©2025 Palo Alto Networks, Inc.

は、**SanFrancisco-zone1**と**SanFrancisco-zone2**用にそれぞれ1つずつ、合計2つのペアリングキーが作成されます。

最初のアベイラビリティ ゾーン*(zone1)*を*CPE*のプライマリ ゾーンとして設定してください。



STEP 9 | Clean Pipe設定を完了します。

©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.