

# ***Prisma Access Administrator's Guide (Panorama Managed)***

***Version 2.0 Innovation***

---

## Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

[www.paloaltonetworks.com/company/contact-support](http://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 [www.paloaltonetworks.com/documentation](http://www.paloaltonetworks.com/documentation).
- To search for a specific topic, go to our search page [www.paloaltonetworks.com/documentation/document-search.html](http://www.paloaltonetworks.com/documentation/document-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](mailto:documentation@paloaltonetworks.com).

## Copyright

Palo Alto Networks, Inc.

[www.paloaltonetworks.com](http://www.paloaltonetworks.com)

© 2017-2021 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](http://www.paloaltonetworks.com/company/trademarks.html). All other marks mentioned herein may be trademarks of their respective companies.

## Last Revised

April 26, 2021

---

# Table of Contents

<b>Prisma Access Overview.....</b>	<b>9</b>
Prisma Access.....	11
Prisma Access Infrastructure Management.....	13
Prisma Access Release and Infrastructure Updates.....	14
Prisma Access Scheduled and Unscheduled Upgrades.....	14
Prisma Access and Panorama Version Compatibility.....	16
Schedule Your Prisma Access Dataplane Upgrade Using the Prisma Access App.....	17
Cadence for Software and Content Updates for Prisma Access.....	18
Manage Upgrade Options for the GlobalProtect App.....	21
Select the Active GlobalProtect App Version.....	21
Manage Users' Access to GlobalProtect App Updates.....	23
Perform Staged Updates of the GlobalProtect App.....	23
Notifications and Alerts for Panorama, Cloud Services Plugin, and PAN-OS Dataplane Versions.....	28
Prisma Access Licensing.....	30
Prisma Access Licenses.....	30
License Enforcement for Mobile User and Remote Network Deployments.....	30
Other Required Licenses.....	31
Add-On Licenses.....	31
Determine Your License Type from Panorama.....	31
Monitor Your Data Transfer Usage.....	32
Retrieve the IP Addresses for Prisma Access.....	35
Prisma Access Infrastructure IP Addresses.....	35
Run the API Script Used to Retrieve IP Addresses.....	37
API Command Examples.....	42
Pre-Allocate IP Addresses for Mobile User Locations.....	43
Be Notified of Changes to IP Addresses.....	47
Legacy Scripts Used to Retrieve IP and Loopback Addresses.....	47
Plan for IP Address Changes for Mobile Users, Remote Networks, and Service Connections.....	53
Service IP and Egress IP Address Allocation for Remote Networks.....	62
How to Calculate Remote Network Bandwidth.....	63
Prisma Access APIs.....	65
<b>Activate and Install the Prisma Access Components.....</b>	<b>67</b>
Activate and Install Prisma Access (Panorama Managed).....	69
Installation Prerequisites.....	69
Hub Roles and Prisma Access Installation.....	70
Activate and Install Prisma Access.....	70
Transfer or Update Prisma Access Licenses.....	76
Supported Update Paths.....	76
Reset Your Prisma Access License.....	77
Transfer or Update Prisma Access Licenses Between Panorama Appliances.....	78
Configure Panorama Appliances in High Availability for Prisma Access.....	82
HA Prerequisites.....	82
Configure HA.....	82

---

<b>Prepare the Prisma Access Infrastructure and Service Connections.....</b>	<b>85</b>
Set Up Prisma Access.....	87
Prisma Access Onboarding and Configuration Workflow.....	87
Proxy Support for Prisma Access and Cortex Data Lake.....	89
Plan the Service Infrastructure and Service Connections.....	90
Configure the Service Infrastructure.....	94
Create a Service Connection to Allow Access to Your Corporate Resources.....	100
Verify Service Connection Status.....	107
Verify Service Connection BGP Status.....	110
Create a Service Connection to Enable Access between Mobile Users and Remote Networks.....	112
Deployment Progress and Status.....	115
How BGP Advertises Mobile User IP Address Pools for Service Connections and Remote Network Connections.....	120
Use Traffic Steering to Forward Internet-Bound Traffic to Service Connections.....	122
Default Routes.....	122
Traffic Steering.....	123
Traffic Steering Requirements.....	124
Traffic Steering Examples.....	125
Zone Mapping and Security Policies for Dedicated Connections.....	131
Configure Traffic Steering.....	133
Routing Preferences for Service Connection Traffic.....	138
Routing Modes for Service Connections.....	138
Mobile User and Remote Network Routing to Service Connections Overview.....	138
Prisma Access Default Routing.....	140
Hot Potato Routing.....	143
Configure Routing Preferences.....	145
Create a High-Bandwidth Network Using Multiple Service Connections.....	146
Create a High-Bandwidth Connection to a Headquarters or Data Center Location.....	147
Configure More than Two Service Connections to a Headquarters or Data Center Location.....	154
List of Prisma Access Locations.....	158
List of Locations by Compute Location.....	158
List of Locations by Region.....	161
Map of North America Locations.....	165
 <b>Secure Mobile Users with Prisma Access.....</b>	 <b>167</b>
Plan To Deploy Prisma Access for Mobile Users.....	169
Plan to Secure Mobile Users.....	169
Secure Mobile Users with GlobalProtect.....	169
Secure Mobile Users With an Explicit Proxy.....	171
Secure Mobile Users With GlobalProtect.....	173
Secure Mobile Users with an Explicit Proxy.....	189
Explicit Proxy Workflow.....	189
Explicit Proxy System Guidelines and Requirements.....	190
Set Up an Explicit Proxy to Secure Mobile Users.....	193
PAC File Guidelines and Requirements.....	199
Security Policy Guidelines and Requirements.....	201
Verify and Monitor the Explicit Proxy Deployment.....	202

Zone Mapping.....	205
Specify IP Address Pools for Mobile Users.....	206
How the GlobalProtect App Selects a Prisma Access Location for Mobile Users.....	207
View Logged In User Information and Log Out Current Users.....	208
View Mobile Users from the Status Tab.....	208
View Mobile Users from the Monitor Tab.....	209
How Prisma Access Counts Users.....	210
Quick Configs for Mobile User Deployments.....	212
Prisma Access with On-Premises Gateways.....	212
Manage Priorities for Prisma Access and On-Premises Gateways.....	214
DNS Resolution for Mobile Users and Remote Networks.....	223
Sinkhole IPv6 Traffic From Mobile Users.....	228
Identification and Quarantine of Compromised Devices With Prisma Access.....	232
Report Website Access Issues.....	243

## Use Remote Networks to Secure Branches..... 245

Plan to Deploy Remote Networks.....	247
Remote Network Planning Prerequisites.....	247
Aggregate Bandwidth Upgrade Considerations.....	249
Onboard and Configure Remote Networks.....	251
Configure Prisma Access for Networks—Configure Bandwidth by Compute Location.....	251
Configure Prisma Access for Networks Allocating Bandwidth by Location.....	269
Verify Remote Network Connection Status.....	285
Verify Remote Connection BGP Status.....	288
Quick Configs for Remote Network Deployments.....	290
Remote Network Locations with Overlapping Subnets.....	290
Remote Network Locations with WAN Link.....	291
Use Predefined IPSec Templates to Onboard Service and Remote Network Connections.....	293
Onboard Remote Networks with Configuration Import.....	299
Configure Quality of Service in Prisma Access.....	303
Create a High-Bandwidth Network for a Remote Site.....	312
Provide Secure Inbound Access to Remote Network Locations.....	319

## Configure User-ID and User-Based Policies with Prisma Access.....333

Configure User-ID in Prisma Access.....	335
Configure User-ID for Remote Network Deployments.....	336
Configure User-ID for Prisma Access Using the PAN-OS Integrated User-ID Agent.....	337
Configure Your Prisma Access Deployment to Retrieve Group Mapping.....	341
Retrieve Group Mappings Using a Master Device.....	341
Implement User-ID in Security Policies For a Standalone Prisma Access Deployment.....	346
Redistribute User-ID Information Between Prisma Access and On-Premises Firewalls.....	348
Redistribute User-ID Information From Prisma Access to an On-Premise Firewall.....	348
Redistribute User-ID Information From an On-Premises Firewall to Prisma Access.....	350
Get User and Group Information Using Directory Sync.....	353

## Redistribute HIP Information and View HIP Reports..... 359

Redistribute HIP Information with Prisma Access.....	361
HIP Redistribution Overview.....	361
Use Cases for HIP Redistribution.....	361
Configure HIP Redistribution in Prisma Access.....	367
View HIP Reports from Panorama.....	370
<b>Manage Multiple Tenants in Prisma Access.....</b>	<b>373</b>
Multitenancy Overview.....	375
Multitenancy Configuration Overview.....	376
Plan Your Multitenant Deployment.....	380
Enable Multitenancy and Migrate the First Tenant.....	381
Add Tenants to Prisma Access.....	387
Delete a Tenant.....	391
Create a Tenant-Level Administrative User.....	392
Control Role-Based Access for Tenant-Level Administrative Users.....	394
Remove Plugin Access for a Tenant-Level Administrative User.....	395
Sort Logs by Device Group ID for External Logging.....	399
<b>Use DLP With Prisma Access.....</b>	<b>403</b>
DLP Integration with Prisma Access.....	405
What is Enterprise DLP?.....	406
Register and Activate DLP on Prisma Access.....	407
Preinstallation Requirements.....	407
Install the Enterprise DLP Plugin—New DLP Deployments.....	407
Upgrade to the Enterprise DLP Plugin—Existing Enterprise DLP on Prisma Access Deployments.....	408
Monitor DLP Status With the DLP Health and Telemetry App.....	410
Access the DLP Health and Telemetry Dashboard.....	410
Monitor DLP Service Status.....	410
Save Evidence for Investigative Analysis with Enterprise Data Loss Prevention (DLP).....	412
Set Up Cloud Storage to Save Evidence.....	412
Download Files for Evidence Analysis.....	417
<b>IoT Security Integration with Prisma Access.....</b>	<b>419</b>
Use IoT Security with Prisma Access.....	421
IoT Security Integration with Prisma Access.....	422
IoT Security Integration Status with Prisma Access.....	425
<b>Create and Configure Prisma Access for Clean Pipe.....</b>	<b>429</b>
Prisma Access for Clean Pipe Overview.....	431
Clean Pipe Use Cases.....	431
Clean Pipe Examples.....	431
Clean Pipe and Partner Interconnect Requirements.....	432
Configure Prisma Access for Clean Pipe.....	434
Enable Multitenancy and Create a Tenant.....	434
Complete the Clean Pipe Configuration.....	438
<b>Cloud Management Logs and Reports.....</b>	<b>441</b>
Logs.....	443
Reports.....	447

---

Available Reports.....	448
Download, Share, and Schedule Reports.....	452
<b>Insights in Prisma Access.....</b>	<b>455</b>
First Look at Insights in Prisma Access.....	457
Go to Insights in Prisma Access.....	458
Give the Right People Access to Prisma Access.....	459
Learn About Prisma Access Alerts.....	461
All Prisma Access Alerts.....	461
Investigate Alerts in Prisma Access.....	466
Turn on Alert Notifications.....	467
Choose a Preferred Window for Certain Prisma Access Upgrades.....	470
Release Updates.....	471
What's New.....	471
Known Issues.....	479
<b>Autonomous DEM in Prisma Access.....</b>	<b>481</b>
Autonomous DEM.....	483
ADEM Monitoring and Tests.....	484
Get Started with Autonomous DEM.....	485
Enable Autonomous DEM for Your Mobile Users.....	487
Go to Autonomous DEM in Prisma Access.....	490
First Look at Autonomous DEM in Prisma Access.....	492
Set up an Autonomous DEM Application Test.....	495
Manage Autonomous DEM Users.....	497
Known Issues—Autonomous DEM.....	499





# Prisma Access Overview

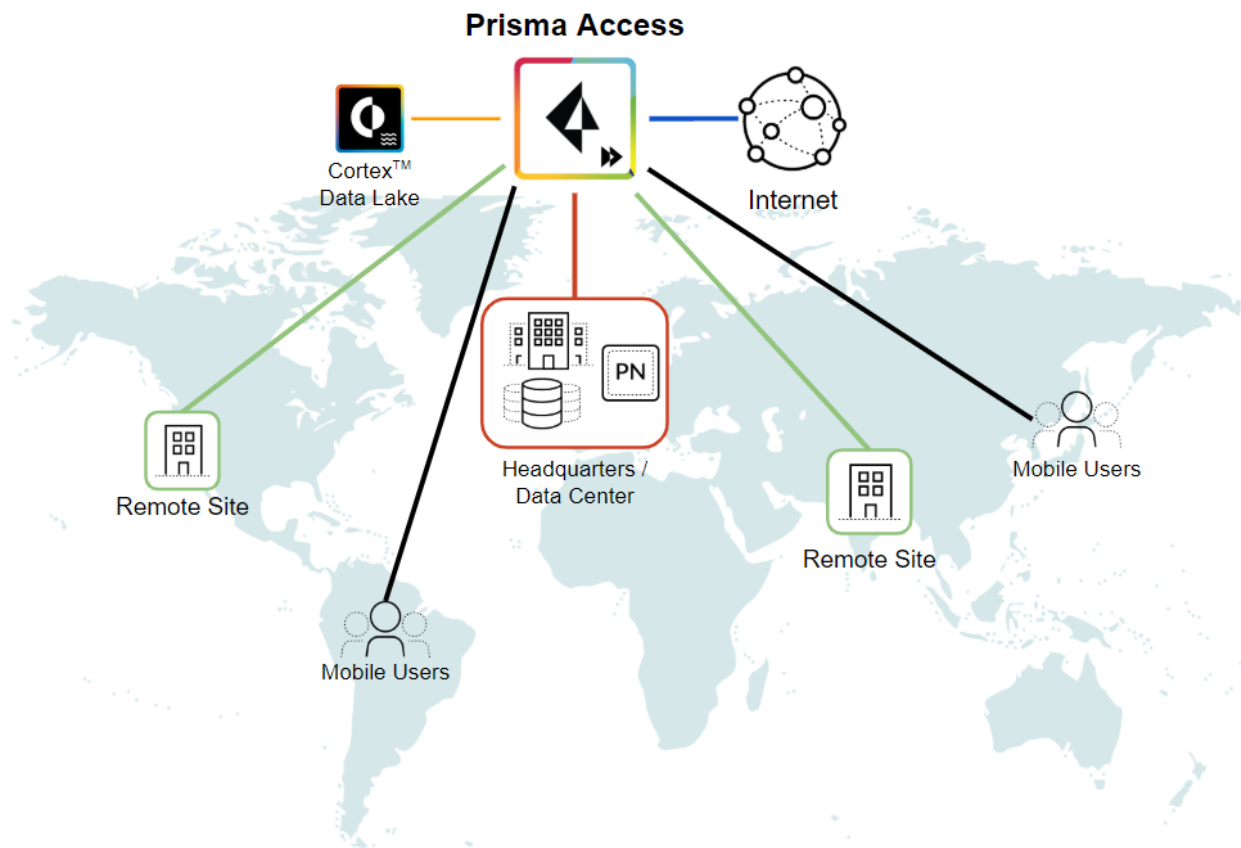
Read the following section to get an overview of what Prisma Access is, how it can secure your organization's resources, who owns and manages the infrastructure and network components.

- > Prisma Access
- > Prisma Access Infrastructure Management
- > Prisma Access Release and Infrastructure Updates
- > Manage Upgrade Options for the GlobalProtect App
- > Notifications and Alerts for Panorama, Cloud Services Plugin, and PAN-OS Dataplane Versions
- > Prisma Access Licensing
- > Retrieve the IP Addresses for Prisma Access
- > Plan for IP Address Changes for Mobile Users, Remote Networks, and Service Connections
- > Service IP and Egress IP Address Allocation for Remote Networks
- > How to Calculate Remote Network Bandwidth
- > Prisma Access APIs



# Prisma Access

As your business expands globally with new remote network locations popping up around the globe and mobile users roaming the world, it can be challenging to ensure that your business remains connected and always secure. Prisma Access uses a cloud-based infrastructure, allowing you to avoid the challenges of sizing firewalls and compute resource allocation, minimizing coverage gaps or inconsistencies associated with your distributed organization. The elasticity of the cloud scales as demand shifts and traffic patterns change. The cloud service operationalizes next-generation security deployment to remote networks and mobile users by leveraging a cloud-based security infrastructure managed by Palo Alto Networks. The security processing nodes deployed within the service natively inspect all traffic in order to identify applications, threats, and content. Prisma Access provides visibility into the use of SaaS applications and the ability to control which SaaS applications are available to your users.



With Prisma Access, Palo Alto Networks deploys and manages the security infrastructure globally to secure your remote networks and mobile users. Prisma Access is comprised of the following components:

- **Cloud Services Plugin**—Panorama plugin that enables both Prisma Access and [Cortex Data Lake](#).  
This plugin provides a simple and familiar interface for configuring and viewing the status of Prisma Access. You can also create Panorama templates and device groups, or leverage the templates and device groups you may have already created, to push configurations and quickly enforce consistent security policy across all locations.
- **Service Infrastructure**—Prisma Access uses an internal service infrastructure to secure your organization's network. You supply a subnet for the infrastructure, and Prisma Access uses the IP addresses within this subnet to establish a network infrastructure between your remote network

---

locations and mobile users, and service connections to your internal network resources (if applicable). Internal communication within the cloud is established using dynamic routing.

- **Service Connections**—Your Prisma Access [license](#) includes the option to establish IPSec tunnels to allow communication between internal resources in your network and mobile users and users in your remote network locations. You could, for example, create a service connection to an authentication server in your organization's HQ or data center.

Even if you don't require a service connection, we recommend that [you create one](#) with placeholder values to allow network communication between mobile users and remote network locations and between mobile users in different geographical locations.

- **Mobile Users—GlobalProtect**—You select locations in Prisma Access that function as cloud-based GlobalProtect gateways to secure your mobile users. To configure this service, you designate one or more [IP address pools](#) to allow the service to assign IP addresses for the client VPN tunnels.
- **Mobile Users—Explicit Proxy**—You can configure an explicit proxy using a proxy URL and a Proxy Auto-Configuration (PAC) file. The GlobalProtect app is not required to be installed on the users' endpoints. The explicit proxy method allows you to retrofit and replace an existing set up to send all traffic to the Prisma Access infrastructure and enforce security in the cloud. In addition, if your organization requires an explicit proxy design for regulatory or auditing compliance, you can meet those requirements using an explicit proxy with Prisma Access.
- **Remote Networks**—Use remote networks to secure remote network locations, such as branches, and users in those branches with cloud-based next-generation firewalls. You can enable access to the subnetworks at each remote network location using either static routes, dynamic routing using BGP, or a combination of static and dynamic routes. All remote network locations that you onboard are fully meshed.
- **Prisma Access for Clean Pipe**—The [Prisma Access for Clean Pipe](#) service allows organizations that manage the IT infrastructure of other organizations, such as service providers, MSSPs, or Telcos, to quickly and easily protect outbound internet traffic for their tenants.


Prisma Access for Clean Pipe uses its own license and has its own [requirements](#). However, it requires the same [Panorama and Cortex Data Lake licenses](#) as the other Prisma Access products described in this section.

Prisma Access forwards all logs to [Cortex Data Lake](#). You can view the logs, ACC, and reports from Panorama for an aggregated view into your remote network and mobile user traffic. To enable logging for Prisma Access, you must purchase a Cortex Data Lake license. Log traffic does not use the licensed bandwidth you purchased for Prisma Access.

---

# Prisma Access Infrastructure Management

It is important to understand who owns and manages the components in the Prisma Access infrastructure. To see when Prisma Access updates the components of the cloud infrastructure, see [Prisma Access Release and Infrastructure Updates](#).

 To see the features that Prisma Access supports, see [What features does Prisma Access support?](#)

Prisma Access uses a shared ownership model. Palo Alto Networks manages the underlying security infrastructure, ensuring it is secure, resilient, up-to-date and available to you when you need it. Your organization's responsibility is to onboard locations and users, push policies, update them, query logs, and generate reports.

Your organization manages the following components of the security infrastructure:

- **Users**—You manage the onboarding of mobile users.
- **Authentication**—You manage the authentication of those users.
- **Mobile device management (MDM)**—You can control your organization's mobile devices that are protected with Prisma Access using your own MDM software.
- **Panorama and Cloud Services plugin**—You make sure that the Panorama on which the Cloud Services plugin is installed is [running a Panorama version that supports the Cloud Services plugin](#). In addition, you [upgrade the Cloud Services plugin](#) in Panorama after we inform you that a new plugin is available.
- **Policy creation and management**—You plan for and create the policies in Panorama to use with Prisma Access.
- **Log analysis and forensics**—Prisma Access provides the logs, you provide the analysis and reporting, using integrated tools provided by us or by another vendor.
- **On-premises security**—You provide the on-premises security between micro-segmentations of your on-premises network. In some deployments, you can also direct all traffic to be secured with Prisma Access.
- **Networking**—You provide the network connectivity to Prisma Access.
- **Monitoring**—You monitor the on-premises network's status.
- **Service Connectivity**—You provide the connectivity to the Prisma Access gateway for mobile users (for example, provide an ISP), and you also provide the on-premises devices used as the termination points for the IPsec tunnels used by service connections and remote network connections.
- **Onboarding**—You onboard the mobile users, HQ/Data center sites, and branch sites.

Palo Alto Networks manages the following parts of the security infrastructure:

- **Prisma Access**
- **Cortex Data Lake**—We manage the delivery mechanism for logs.
- **Content updates**—We [manage the updating of the Prisma Access infrastructure](#), including PAN-OS updates. For your mobile users, Prisma Access hosts several versions of the GlobalProtect app and you can [select the active GlobalProtect app version](#) from that list.
- **Fault tolerance**—We manage the availability of the service.
- **Auto scaling**—We automatically scale the service when you add service connections or remote networks, or when additional mobile users log in to one or more gateways in a single region.
- **Provisioning**—We provision the infrastructure with everything that is required.
- **Service monitoring**—We monitor the service status and keep it functioning.

---

# Prisma Access Release and Infrastructure Updates

Learn about the different types of Prisma Access releases and updates that you need to stay up-to-date and secure your users. Some of the updates are managed by Palo Alto Networks, such as Prisma Access infrastructure updates and you will receive advance notification so you can plan around them. Other updates are your responsibility and you must schedule the specified version of the content update, software update, and plugin version (as required), at your earliest convenience.



*You can retrieve the status of all cloud services, including Prisma Access and Cortex Data Lake, along with a historical record of the uptime of each service, by accessing the <https://status.paloaltonetworks.com/> website. You can also sign up for email or text message updates at this site to be notified in advance when infrastructure updates are planned and real-time notifications when updates occur, and when Palo Alto Networks creates, updates, or resolves an incident.*

- [Prisma Access Scheduled and Unscheduled Upgrades](#)
- [Prisma Access and Panorama Version Compatibility](#)
- [Schedule Your Prisma Access Dataplane Upgrade Using the Prisma Access App](#)
- [Cadence for Software and Content Updates for Prisma Access](#)

## Prisma Access Scheduled and Unscheduled Upgrades

Prisma Access has scheduled upgrades, including major (x.0 and 1.x) and minor (2.0.x) releases, that include new features and optimizations to deliver best-of-breed security for your remote networks and mobile users. Prisma Access might also need to occasionally make unscheduled upgrades for hotfixes and emergency bug fixes. The following sections define the releases, list the types of upgrades that Palo Alto Networks include for each release, and show you the advance notification and maintenance windows for each release type.

- [Release Definitions](#)
- [Upgrade Types](#)

### *Release Definitions*

The following list defines scheduled and unscheduled releases, along with the advance notification we provide you for each release. To make sure that you receive notifications for all releases, register for email or text notifications for Prisma Access at the <https://status.paloaltonetworks.com/> website.

- **Scheduled Release**—Prisma Access divides scheduled releases into major and minor releases.
  - **Major Release**—A major release typically includes significant new features and optimizations that require a maintenance window.

**Notification**—Palo Alto Networks provides you with a notification 21 days before a major release, including a feature preview document that lists features that are available with the release and any changes to default behavior.
  - **Minor Release**—A minor release includes incremental features and optimizations. In some cases, Palo Alto Networks may combine a hotfix with a minor release.

**Notification**—Palo Alto Networks provides you with a notification 10 days before a scheduled minor release upgrade, including a feature preview document that lists the new features that are available with the release.

- **Unscheduled Release**—Unscheduled Prisma Access upgrades include hotfixes or emergency bug fixes (for example, fixes for zero-day threats or plugin changes).

**Notification**—Palo Alto Networks will make every effort to give you 48 hours' notice before an unscheduled upgrade. On occasion, you may receive a shorter notice for an unscheduled upgrade.

## Upgrade Types

Palo Alto Networks upgrades its cloud-based infrastructure without any intervention required from you. Some upgrades require that you perform an action, such as install a new plugin.

The following list includes the different types of scheduled and unscheduled upgrades for Prisma Access:

- **Infrastructure Upgrade**—Palo Alto Networks upgrades the Prisma Access infrastructure, which includes the underlying service backend, orchestration, and monitoring infrastructure.
- **Dataplane Upgrade**—Palo Alto Networks upgrades the Prisma Access dataplane that enables traffic inspection and security policy enforcement on your network and user traffic.

You [use the Prisma Access Insights app](#) to sign up for dataplane upgrade email alert notifications and indicate your upgrade preferences.

- **Cloud Services Plugin Upgrade**—Your network administrator will need to [upgrade the Cloud Services plugin](#) on the Panorama appliance that manages Prisma Access.
- **Panorama Software Upgrade**—A [Prisma Access and Panorama Version Compatibility](#) might be required to ensure compatibility with Prisma Access.

The following table shows you what is included with each release, including the maintenance window we provide and any impact to your Prisma Access service.

Upgrade Type		Scheduled Upgrades		Unscheduled Upgrades
		Major	Minor	
Infrastructure Upgrade	<b>Maintenance Window</b>	2-8 hours (always required)	2-8 hours (always required)	2-8 hours (if required)
	<p><b>Impact:</b> No impact to network traffic; however you cannot perform commits during the maintenance window.</p> <p>Palo Alto Networks schedules the upgrades at a local time that is minimally disruptive to business functions.</p>			
Dataplane Upgrade	<b>Maintenance Window</b>	72 hours (always required)	— (not required)	72 hours (if required)
	<p><b>Impact:</b> Palo Alto Networks uses this window to upgrade the dataplane for all customers. You can make configuration changes and commits during this window. Our goal is to minimize impact to network traffic, but in some cases there may be a brief interruption.</p>			

Upgrade Type	Scheduled Upgrades		Unscheduled Upgrades
	Major	Minor	
	You use the <a href="#">Prisma Access Insights app</a> to sign up for dataplane upgrade email alert notifications and indicate your upgrade preferences, including the preferred time window for your upgrade.		
Cloud Services Plugin Upgrade	<b>Maintenance Window</b>	(always required)	(if required)
	<p><b>Impact:</b> Palo Alto Networks notifies you in advance if an upgrade to the Cloud Services plugin is required, and when the plugin will be available, using the notification schedule as defined in <a href="#">Release Definitions</a>. During the plugin upgrade, you cannot make configuration changes and commits in Panorama.</p> <p>After Palo Alto Networks provides you with the advance notification, you must plan to schedule a maintenance window to <a href="#">upgrade the plugin</a> and complete the plugin upgrade within five days of its availability. <b>You cannot use the previous version of the plugin to perform changes to configuration and commits in Panorama after the three-day upgrade window.</b></p>		

## Prisma Access and Panorama Version Compatibility

When Prisma Access upgrades its infrastructure and dataplane after a major release, the upgrades can be incompatible with earlier Panorama versions. Because of the fast-paced release of Prisma Access and the Cloud Services plugin, the software compatibility (end-of-support) dates for Panorama are shorter than the software end-of-life dates for Panorama releases and apply to Panorama version compatibility with Prisma Access only.

If the Panorama appliance that manages Prisma Access is running a software version that is incompatible (not supported) with the upgrades, you must upgrade Panorama to a compatible version to take full advantage of the capabilities of the infrastructure and dataplane upgrades. It is Palo Alto Networks' goal to make this process as seamless as possible; for this reason, we make every effort to provide you with adequate notice of Panorama and Prisma Access version compatibility requirements.

Use the dates in the following table to learn when the software version of the Panorama that manages Prisma Access is no longer compatible with Prisma Access. Before the end-of-support date, you should plan to perform an upgrade to a supported Panorama version.



*To find the latest EoS compatibility information for your Panorama with Prisma Access, log in to the Panorama appliance that manages Prisma Access, select the Service Setup page (Panorama > Cloud Services > Configuration > Service Setup), and view the information in the Panorama Alert section. See [Notifications and Alerts for Panorama, Cloud Services Plugin, and PAN-OS Dataplane Versions](#) for details.*

Panorama Software Version	End-of-Support Dates for Prisma Access Deployments
9.1	February 1, 2022  Before this date, you must upgrade your Panorama to a version that is later than 9.1.x. Palo Alto Networks will update this document



---

Panorama Software Version	End-of-Support Dates for Prisma Access Deployments
	with more specific upgrade guidelines as newer Panorama software releases become generally available.

---

For more information about Prisma Access and Panorama software version compatibility, see [Prisma Access and Panorama Version Compatibility](#) in the [Palo Alto Networks Compatibility Matrix](#).

The Panorama upgrade is required, regardless of the Cloud Services plugin version you are running at the end-of-support date. You cannot continue using an earlier version of the Cloud Services plugin with an earlier, unsupported Panorama version.

## Schedule Your Prisma Access Dataplane Upgrade Using the Prisma Access App

Prisma Access now provides you the flexibility to schedule the dataplane upgrade for your Prisma Access tenant, when upgrades become available. To stay informed about the dataplane upgrade schedule and to select your preference, you must use the Prisma Access app to subscribe to Prisma Access notifications.

To sign up for email alert notifications through the Prisma Access app and indicate your upgrade preferences, complete the following steps.

**STEP 1** | Log into the [Hub](#).

**STEP 2** | Click the **Prisma Access** app.

**STEP 3** | Select **Insights** to expand the choices; then, select **Alerts > Alert Subscription** and enter the email address to receive notifications from the Prisma Access app.

The email accounts to which Prisma Access sends alerts must be the same email accounts associated with users in your Palo Alto Networks support account.

**STEP 4** | **Add Users**.

**STEP 5** | Enter the email addresses of the users to whom you want to send notifications.

To add multiple users, separate each user with a comma.

**STEP 6** | In a multi-tenant deployment, **Select Sub-Tenants** for which you want users to receive notifications or select **All Sub-Tenants** if you want them to receive notifications from all sub-tenants.

**STEP 7** | **Add** the users.

**STEP 8** | Check your notifications.

Prisma Access sends an upgrade notification 21 days before your dataplane upgrade is scheduled.

- Log in to the Prisma Access app and view the banner for your scheduled upgrade.
- Check your email for notifications for your scheduled upgrade.

**STEP 9** | After you receive notification that the upgrade is available, select your upgrade preferences.

1. Select the Prisma Access locations you would like to upgrade first.
2. Select a preferred time window, from the list of available options, for the upgrade.

Palo Alto Networks uses your preference to begin the roll out at the selected Prisma Access locations and the remaining locations, if any will be upgraded seven days later based on the time preference you provided. See [Choose a Preferred Window for Certain Prisma Access Upgrades](#) for more details about the upgrade and notification process. Prisma Access Insights [provides you with notifications](#) that inform you of the progress of the upgrade and when it is complete.



*If you do not provide your upgrade preferences three days before the scheduled upgrade window, Palo Alto Networks will automatically select the first set of your deployed Prisma Access locations, notify you of the selection, and upgrade the selected locations on the scheduled date. The remaining Prisma Access locations, if any, in your deployment will be upgraded seven days after the selected time window.*

## Cadence for Software and Content Updates for Prisma Access

The following table informs you of the software and content updates that you must install to get the latest applications and threat signatures and leverage the threat prevention capabilities provided by Palo Alto Networks.

Component	Update Schedule	Cloud Controlled? (Yes/No)	Comments
Upgrades to Panorama software for compatibility with Prisma Access	<p>For major Prisma Access releases, you might need to upgrade your Panorama version for the following use cases:</p> <ul style="list-style-type: none"> <li>• <b>Required Upgrade</b>—On occasion, you will be required to upgrade the software version on Panorama <a href="#">Prisma Access and Panorama Version Compatibility</a> with Prisma Access.</li> <li>• <b>Maintenance Window</b>—Your organization will need to schedule a maintenance window to upgrade the Panorama software version.</li> <li>• <b>Impact</b>—You cannot use the new plugin version until you upgrade your Panorama version.</li> <li>• <b>Notification</b>—Palo Alto Networks will provide you with a notification 100 days before the scheduled major release upgrade.</li> <li>• <b>Optional Upgrade</b>—In other cases, you might need to</li> </ul>	No	See <a href="#">Prisma Access and Panorama Version Compatibility</a> to learn when a Panorama version becomes incompatible with Prisma Access. See <a href="#">Upgrade the Cloud Services Plugin</a> for the currently supported Panorama versions to use with Prisma Access. To upgrade your Panorama to a new version, see <a href="#">Install Content and Software Updates for Panorama</a> .

Component	Update Schedule	Cloud Controlled? (Yes/No)	Comments
	<p>upgrade the Panorama software version to use the new features that Prisma Access supports in the major release.</p> <ul style="list-style-type: none"> <li>• <b>Maintenance Window</b>—Your organization will need to schedule a maintenance window to upgrade the Panorama software version.</li> <li>• <b>Impact</b>—You cannot use the new features that Prisma Access supports until you upgrade your Panorama.</li> <li>• <b>Notification</b>—Palo Alto Networks will notify you of any Panorama requirements 21 days before a scheduled major release upgrade as defined in <a href="#">Release Definitions</a>.</li> </ul>		
Cloud Services plugin version	Available after the plugin release.	No	You perform the tasks to upgrade the plugin. See <a href="#">Prisma Access Scheduled and Unscheduled Upgrades</a> for details about when Prisma Access updates its plugin version. See <a href="#">Upgrade the Cloud Services Plugin</a> to upgrade the plugin in the Panorama appliance.
GlobalProtect app	<ul style="list-style-type: none"> <li>• <b>Major GlobalProtect App Releases (for example, x.0 or 5.x)</b>—Prisma Access updates the agent on the portal with the latest major release 7-10 days after the general availability of the x.0.1 version of that release.</li> </ul> <p>For example, given an agent release of 5.1, Prisma Access updates the agent on the</p>	Yes	The cloud controls the versions of the app that is available for upgrade; however you can choose between several different hosted versions of the app and can control how and when to roll out GlobalProtect app updates to the end users. See <a href="#">Manage Upgrade Options for the</a>

Component	Update Schedule	Cloud Controlled? (Yes/No)	Comments
	<p>portal 7-10 days after the release of 5.1.1.</p> <ul style="list-style-type: none"> <li>• <b>Minor GlobalProtect App Releases (for example, 5.1.x)</b> –Prisma Access updates the agent on the portal with the latest minor release 7-10 days after the general availability of that release.</li> </ul>		<p><a href="#">GlobalProtect App</a> for details.</p> <p>If your Prisma Access deployment requires a hotfix of the GlobalProtect app, open a <a href="#">Support Case</a> with Palo Alto Networks Technical Support for assistance.</p>
<a href="#">Applications and threat updates</a>	<p>Daily with a threshold of 24 hours.</p> <p>We release New App-IDs on the third Tuesday of every month. Plan to review and incorporate these new App-IDs within the 24 hour threshold. Use the <a href="#">New App-ID filter</a> to minimize this possible traffic impact.</p>	Yes	<p>We will provide an update via the <a href="https://status.paloaltonetworks.com">status.paloaltonetworks.com</a> page 48 hours prior to a cloud upgrade, and 24 hours prior to release of new App-ID version.</p>
<a href="#">Antivirus protection</a>	Every hour, 10 minutes after the hour	Yes	Prisma Access is always up-to-date with the latest Antivirus release.
<a href="#">WildFire</a>	Every 5 minutes	Yes	Prisma Access is always up-to-date with the latest WildFire release.
<a href="#">GlobalProtect Data File</a>	Every hour	Yes	Prisma Access is always up-to-date with the latest GlobalProtect data file release.
<a href="#">Clientless VPN application signatures</a>	Every hour	Yes	Prisma Access is always up-to-date with the latest Clientless VPN application signature release.

---

# Manage Upgrade Options for the GlobalProtect App

Prisma Access hosts the GlobalProtect app version that macOS and Windows users in your organization can download from the Prisma Access portal. Prisma Access offers several versions of the GlobalProtect app, and you can choose to make one of those versions the active version. You can also manage mobile users' access to the GlobalProtect app, or perform staged upgrades.

- [Select the Active GlobalProtect App Version](#)
- [Manage Users' Access to GlobalProtect App Updates](#)
- [Perform Staged Updates of the GlobalProtect App](#)

## Select the Active GlobalProtect App Version

Prisma Access manages the GlobalProtect app version for Windows and macOS users in your organization. While Prisma Access hosts several GlobalProtect app versions, only one of the hosted versions is active. When mobile users log in to the Prisma Access portal, the active version is the one they download and use on their Windows and macOS devices.



*The System Status page also provides you information about your current Panorama version, Cloud Services plugin version, and dataplane version. You can receive notifications and alerts on this page when plugin or Panorama versions become end of support (EoS) for use with Prisma Access. See [Notifications and Alerts for Panorama, Cloud Services Plugin, and PAN-OS Dataplane Versions](#) for details.*

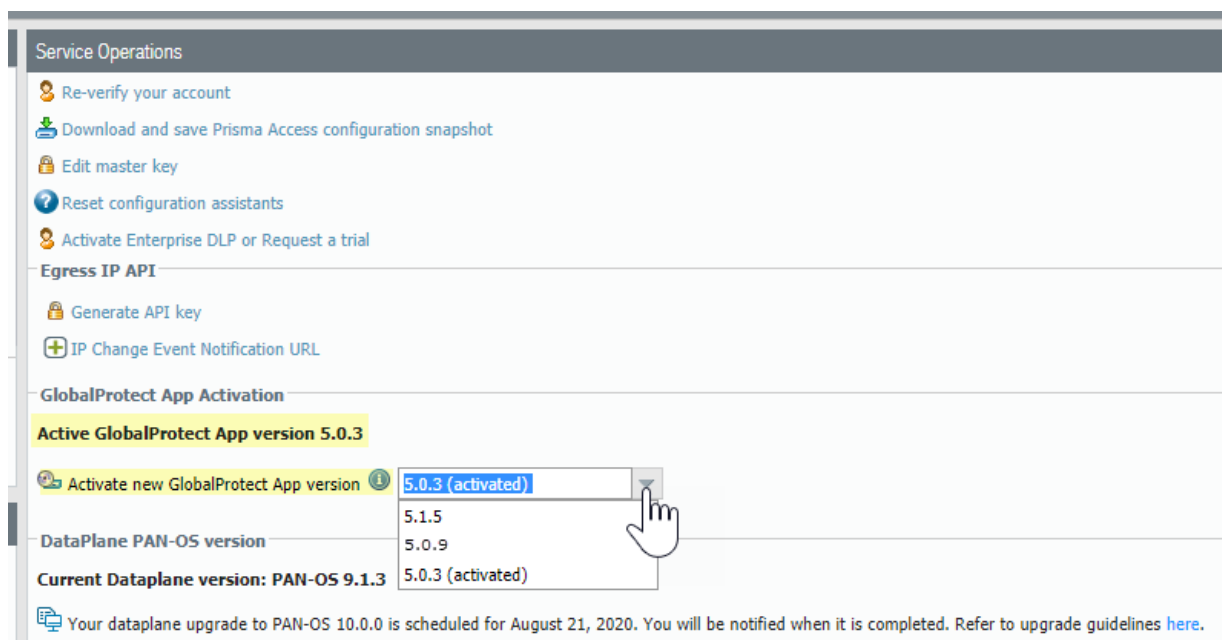
If your currently-active version is end-of-life, Prisma Access notifies you and requests that you activate a supported version.


You can select different GlobalProtect versions in a [multi-tenant deployment](#). The GlobalProtect app version settings you apply are per tenant and not global; you control the app version on a per-tenant basis.

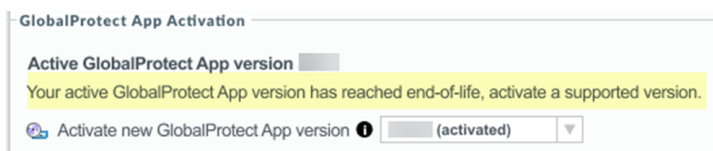
You can replace the current active version with another hosted version from the Service Setup page by completing the following steps.

**STEP 1** | Select **Panorama > Cloud Services > Configuration > Service Setup**.

**STEP 2** | Select **Activate new GlobalProtect App version** and compare it to the active GlobalProtect version.

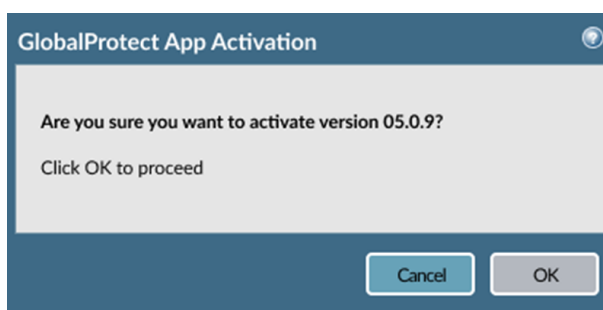


 *If your current GlobalProtect version is end-of-life (EoL), a message displays in this area on the Service Setup page; if you receive this message, upgrade your GlobalProtect app version by continuing to the next step.*

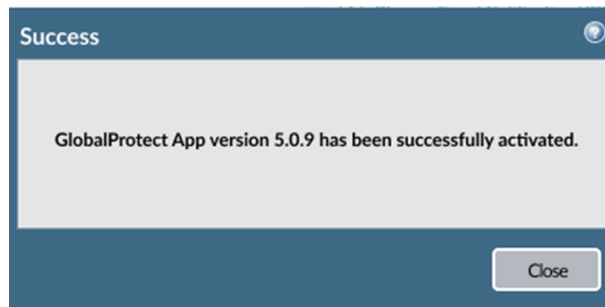


### STEP 3 | Select the version to which you want to upgrade.

A window displays to verify your choice.



After the app has been activated, you receive a success message.



**STEP 4** | View the System Status page to verify that the GlobalProtect app version you selected as active is the **Active GlobalProtect App version**.

## Manage Users' Access to GlobalProtect App Updates

To manage mobile users' access to the active GlobalProtect app version that is hosted by Prisma Access, complete the following steps.

**STEP 1** | In Panorama, select **Network > GlobalProtect > Portals**.

**STEP 2** | Select the **Mobile\_User\_Template** from the **Template** drop-down.

**STEP 3** | Select **GlobalProtect\_Portal** to edit the Prisma Access portal configuration.

**STEP 4** | Select the **Agent** tab and select the app configuration.

**STEP 5** | Select the **App** tab.

**STEP 6** | In the **App Configurations** area, select a choice in **Allow User to Upgrade GlobalProtect App** to specify whether mobile users can upgrade their GlobalProtect app version to the active version that is hosted on Prisma Access and, if they can, whether they can choose when to upgrade:

- **Allow with Prompt** (default)—Prompt users when a new version is activated and allow users to upgrade their software when it is convenient.
- **Disallow**—Prevent users from upgrading the app software.
- **Allow Manually**—Allow users to manually check for and initiate upgrades by selecting **Check Version** in the GlobalProtect app.
- **Allow Transparently**—Automatically upgrade the app software whenever a new version becomes available on the portal.
- **Internal**—Automatically upgrade the app software whenever a new version becomes available on the portal, but wait until the endpoint is connected internally to the corporate network. This prevents delays caused by upgrades over low-bandwidth connections.

## Perform Staged Updates of the GlobalProtect App

If you manage a large organization, you might want to update mobile users to the latest version of the GlobalProtect app in stages. For example, you could assign a smaller group to update their GlobalProtect app before rolling out the update to everybody in your organization. To do so, complete the following task.

**STEP 1** | If you have not yet created it, create a user group for the first group of users to which you want to roll out the GlobalProtect app update.

You can use [User-ID](#) to [map users to groups](#), or select **Device > Local User Database > User Groups** to manually create a group.

**STEP 2 |** Create a new [GlobalProtect agent configuration](#) to use for the first group of users.

1. In Panorama, select **Network > GlobalProtect > Portals**.
2. Select the **Mobile\_User\_Template** from the **Template** drop-down.
3. Select **GlobalProtect\_Portal** to edit the Prisma Access portal configuration.
4. Select the **Agent** tab.
5. Select the **DEFAULT** configuration and **Clone** it.

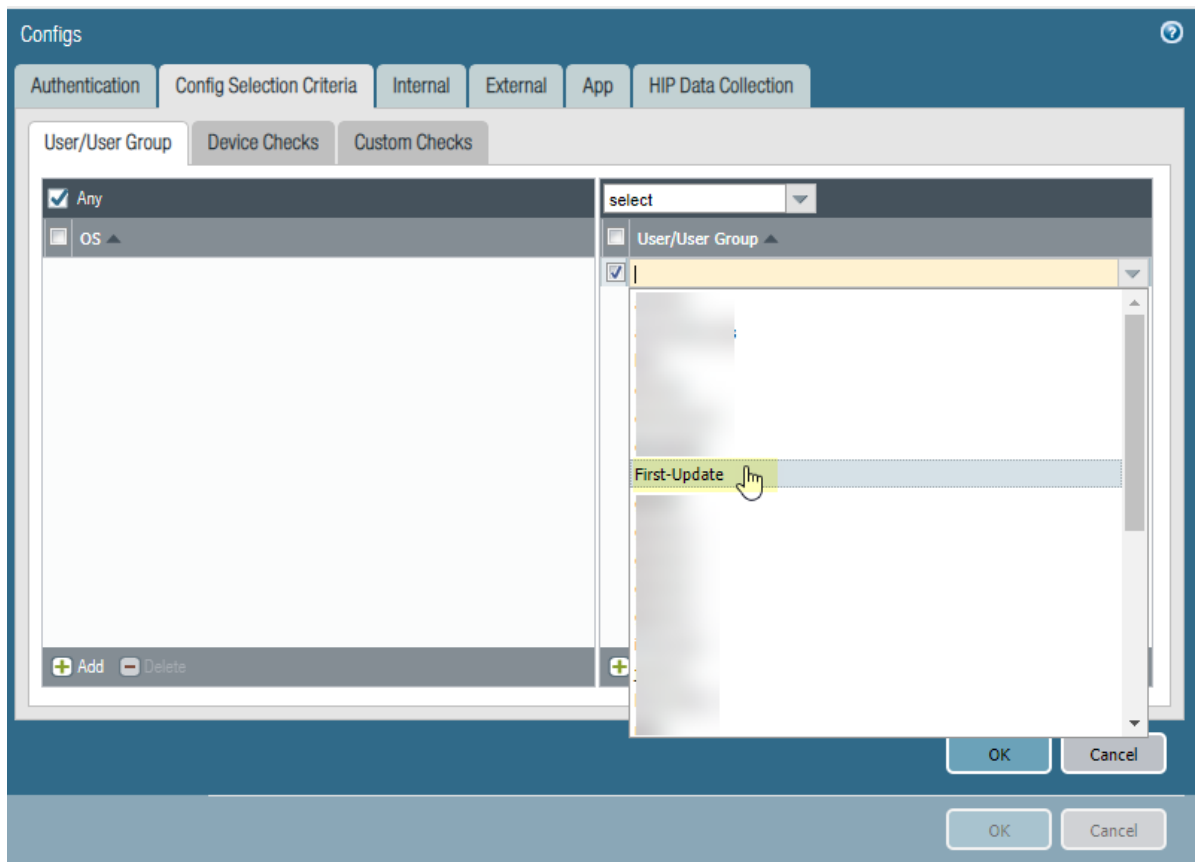
You can also **Add** a new configuration; but cloning the existing configuration copies over required information for the new configuration.

6. Specify a **Name** for the configuration.

The screenshot shows the 'Configs' dialog box for a GlobalProtect agent configuration. The 'Name' field is 'First'. The 'Client Certificate' is 'Local'. The 'Save User Credentials' is 'Yes'. Under 'Authentication Override', 'Generate cookie for authentication override' and 'Accept cookie for authentication override' are checked. The 'Cookie Lifetime' is 'Hours' with a value of '24'. The 'Certificate to Encrypt/Decrypt Cookie' is 't'. Under 'Components that Require Dynamic Passwords (Two-Factor Authentication)', 'Portal', 'Internal gateways-all', 'External gateways-manual only', and 'External gateways-auto discovery' are all unchecked. The dialog has 'OK' and 'Cancel' buttons at the bottom right.

7. Select the **Config Selection Criteria** tab.
8. In the **User/User Group** area, select the user you created in Step 1.

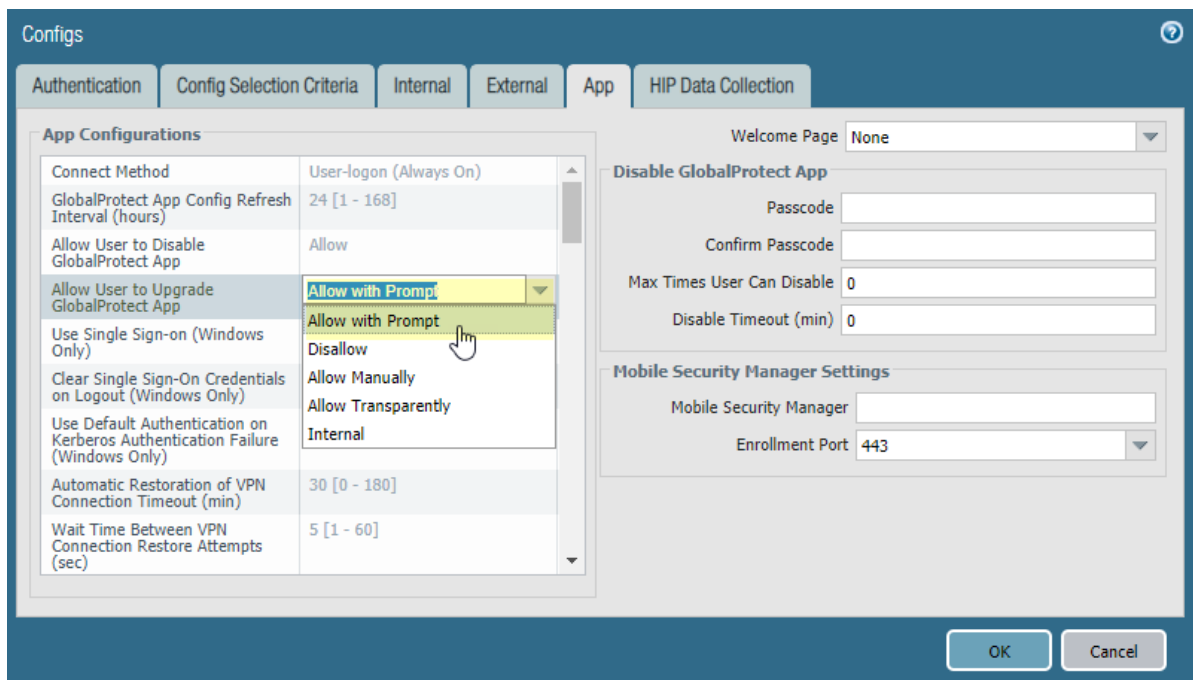




9. Select the **App** tab.

10. Change **Allow User to Upgrade GlobalProtect App** to either **Allow with Prompt** or **Allow Transparently**.

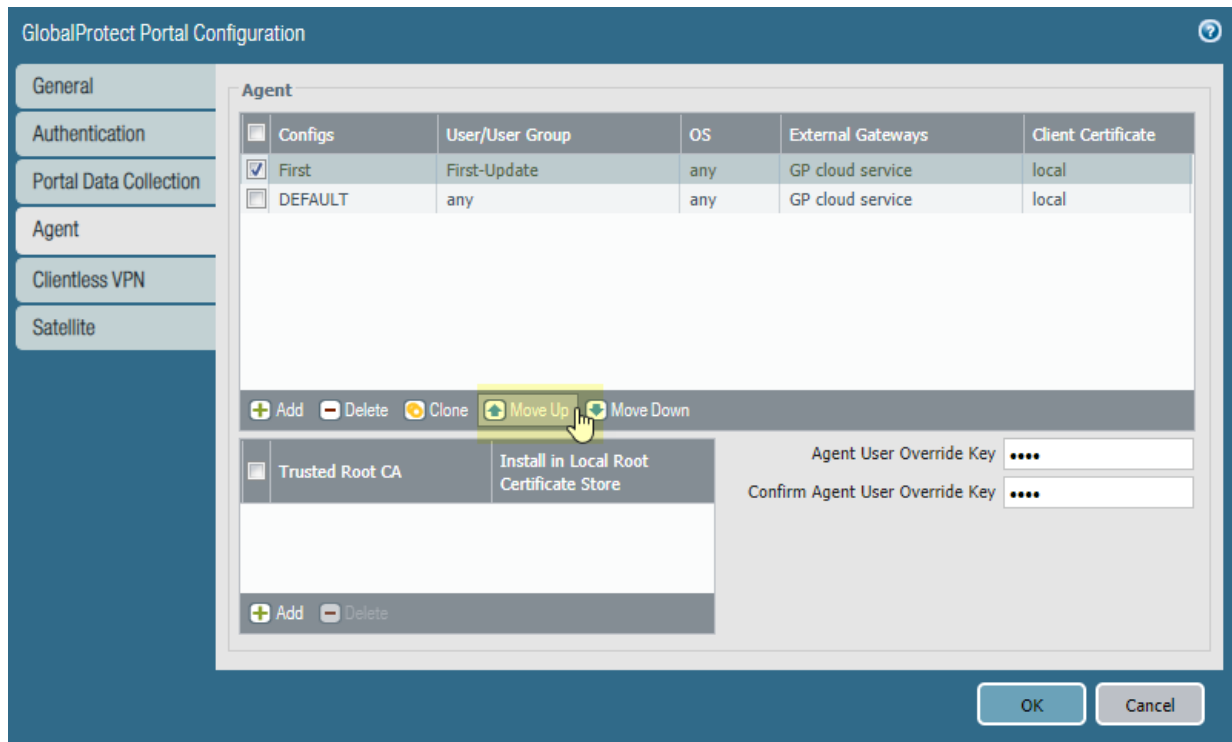
**Allow with Prompt** prompts users when a new version is activated and allows them to upgrade their software when it is convenient; **Allow Transparently** automatically upgrades the app software whenever a new version becomes available on the portal.



11. Click **OK** to save your changes.

### STEP 3 | Select **Move Up** to move your configuration above the default configuration.


When an app connects, the portal compares the source information in the packet against the agent configurations you have defined. As with security rule evaluation, the portal looks for a match starting from the top of the list. When it finds a match, it delivers the corresponding configuration to the app.



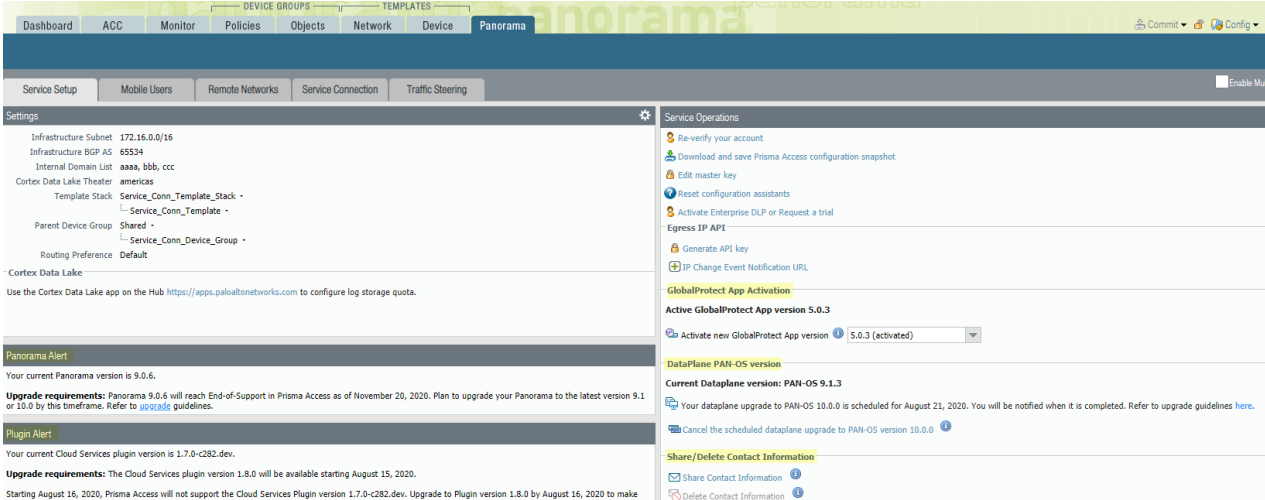
- 
- STEP 4** | Repeat these steps for the **DEFAULT** configuration, but change **Allow User to Upgrade GlobalProtect App** to **Disallow** to prevent users from updating to the latest GlobalProtect app software.
- STEP 5** | When you want to let the rest of the users update their apps, change **Allow User to Upgrade GlobalProtect App** in the **DEFAULT** configuration to a selection that allows it (either **Allow with Prompt** or **Allow Transparently**).

# Notifications and Alerts for Panorama, Cloud Services Plugin, and PAN-OS Dataplane Versions

Prisma Access consists of **components you manage** such as Panorama and the Cloud Services plugin, components that Prisma Access manages such as the dataplane version, and components that Prisma Access manages but whose version you can control (the **GlobalProtect app version** hosted on the Prisma Access portal). The Service Setup page (**Panorama > Cloud Services > Configuration > Service Setup**) shows you the status of these components in a single page. This page also contains notifications that show you when your current running Panorama version and plugin versions will be end of support (EoS) for use with Prisma Access. Palo Alto networks provides you with advance notice of EoS dates to give your organization sufficient time to plan the upgrade.

 *All dates are in Coordinated Universal Time (UTC).*

The Service Setup page provides you with the following information:



Area	Description
<b>Panorama Alert</b>	Displays the current Panorama version that you are running. The <b>Upgrade requirements</b> area provides you with information about Panorama versions, including dates when currently compatible Panorama versions reach their end of support (EoS) dates for managing Prisma Access. Use this information to plan your Panorama upgrade in advance of its EoS date.
<b>Plugin Alert</b>	Displays the current Cloud Services plugin that is installed on the Panorama that manages Prisma Access. The <b>Upgrade requirements</b> area provides you with dates when the next plugin version will be released, the deadline for upgrading to the next plugin, and the date when you will

Area	Description
	not be able to make changes and commits using the earlier plugin version. Use this information to plan for the next Cloud Services plugin upgrade.
<b>GlobalProtect App Activation</b>	Displays the currently-running (active) version of the GlobalProtect app that mobile users can download from the Prisma Access portal, and shows you the available GlobalProtect app versions to which you can upgrade. See <a href="#">Select the Active GlobalProtect App Version</a> for details.
<b>Dataplane PAN-OS version</b>	Displays the current PAN-OS version that your dataplane is running. The <a href="#">dataplane</a> is the component of the Prisma Access infrastructure that enables traffic inspection and security policy enforcement on your network and user traffic.
<b>Share/Delete Contact Information</b>	<p>Allows you to share contact information (Company name, contact name, email, and phone number) so that you can be contacted about Palo Alto Networks service upgrades.</p> <p>If you have previously entered contact information, you can delete the information you entered in this area.</p> <p>Do not use any of the following special characters in the contact information area:</p> <ul style="list-style-type: none"> <li>• " (Double quotes)</li> <li>• ' (Apostrophe)</li> <li>• &lt; (less than sign)</li> <li>• &gt; (greater than sign)</li> <li>• &amp; (ampersand)</li> </ul>

---

# Prisma Access Licensing

The following sections describe the licensing options for Prisma Access, as well as components that are required to use the service.

- [Prisma Access Licenses](#)
- [License Enforcement for Mobile User and Remote Network Deployments](#)
- [Other Required Licenses](#)
- [Add-On Licenses](#)
- [Determine Your License Type from Panorama](#)
- [Monitor Your Data Transfer Usage](#)

## Prisma Access Licenses

Prisma Access offers a licensing model that allows you to implement and use the capabilities of Prisma Access aligned to your business needs in a way that delivers the fastest return on investment. Whether your applications are migrating to the cloud, your users are working from anywhere, or if you are looking to gain operational efficiencies, Prisma Access offers the relevant type of license for your deployment.

You can choose from the following license editions:

- **Business**
- **Business Premium**
- **Zero Trust Network Access (ZTNA) Secure Internet Gateway (SIG)**
- **Enterprise**



*Your Prisma Access license edition determines the security capabilities you are allowed to use. If you use any capability in security rules or profiles that is unsupported based on your license type, Prisma Access removes those configurations and those capabilities are not enforced in your Prisma Access tenants until you update Prisma Access with a license edition that supports those capabilities. To find the capabilities included with your license, refer to the [Prisma Access Licensing Guide](#).*

All license editions are available for Local and Worldwide Prisma Access locations. When you purchase a license with Worldwide locations, you can deploy Prisma Access in all Prisma Access locations. When you purchase a license with Local locations, you can select up to 5 Prisma Access locations.

Prisma Access uses *units* in licenses, and uses the following definitions for a unit:

- For mobile user deployments, a *unit* is defined as one mobile user.
- For remote network and Clean Pipe deployments, a *unit* is defined as 1 Mbps of bandwidth.



*When a Prisma Access license expires, you can still use the service and collect logs for 15 days after license expiration. You cannot make changes to configuration. Prisma Access shuts down its instances 15 days after license expiration and completely deletes the instances and tenants 30 days after license expiration.*

## License Enforcement for Mobile User and Remote Network Deployments

Prisma Access uses the following enforcement policies for mobile user and remote network licenses:

- **Mobile User Deployments**—Though there is no strict policing of the mobile user count, the service does track the number of unique users over the last 90 days to ensure that you have purchased the proper

---

license tier for your user base, and stricter policing of user count may be enforced if continued overages occur.

In addition, if you use Prisma Access for users—GlobalProtect, the GlobalProtect app is required on each [supported](#) endpoint. The GlobalProtect app is not required for Mobile Users—Explicit Proxy deployments.

- **Remote Network Deployments**—To enable traffic peaks, the service allows you to go 10% over the allocated bandwidth for each site; traffic overages above this peak limit is dropped.

A remote network's bandwidth speed is enforced equally in both directions. If you assign a remote network with 50Mbps bandwidth, then 55 Mbps (50 Mbps plus 10% overage allocation) is enforced for both ingress and egress traffic. If you have an asymmetric internet connection (which is a common deployment), you should specify the higher of the two values to fully utilize the circuit.

## Other Required Licenses

In addition to the Prisma Access licenses, in order to run the service you must also have the following licensed components:

- **Panorama**—You deploy and manage Prisma Access using the Cloud Services plugin for Panorama. In order to use this plugin, you must have Panorama with a valid support license. See the [Palo Alto Networks Compatibility Matrix](#) for the Panorama versions that are supported with the Cloud Services plugin. When you license the Prisma Access components, you must tie the auth code to a licensed Panorama serial number.
- **Cortex Data Lake**—The Prisma Access infrastructure forwards all logs to [Cortex Data Lake](#). You can view the Prisma Access logs, ACC, and reports directly from Panorama for an aggregated view into your remote network and mobile user traffic. To enable logging for Prisma Access, you must purchase a Cortex Data Lake license.

## Add-On Licenses

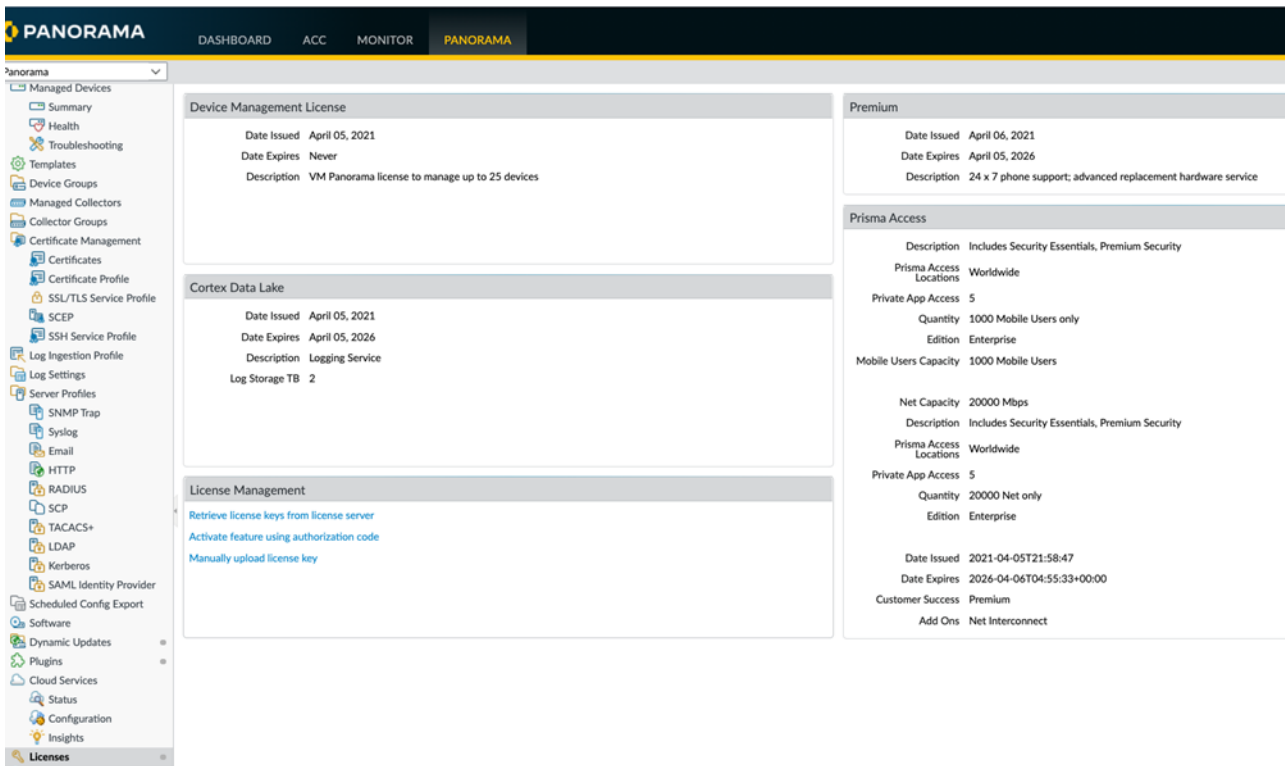
You can add the following capabilities to use with Prisma Access as an add-on license:

- [IoT Security](#)
- [Enterprise Data Loss Prevention \(DLP\)](#)

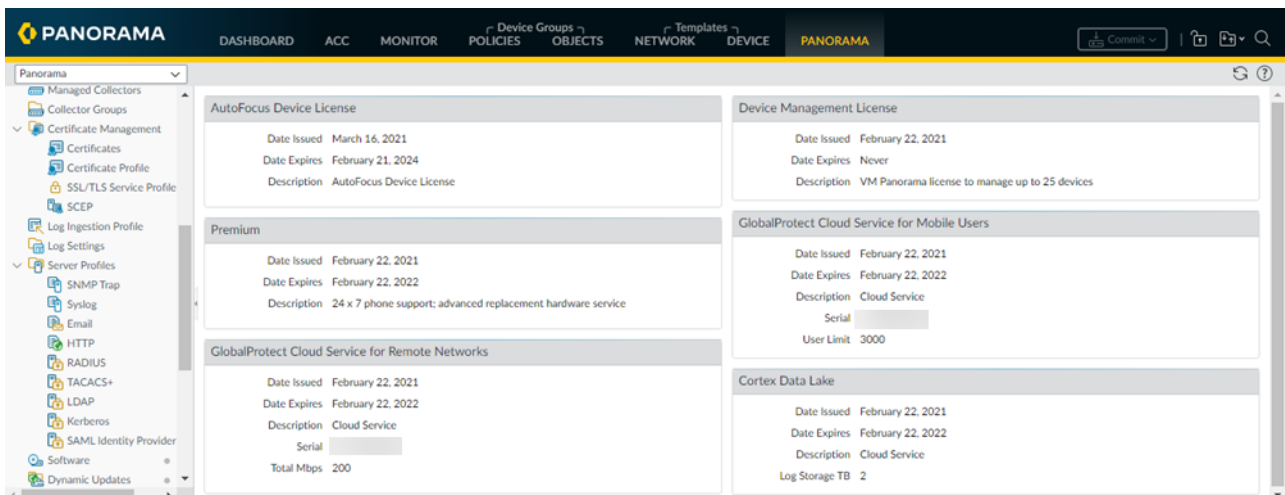
## Determine Your License Type from Panorama

Some license requirements, such as the requirements you need [to enable tenants in a multi-tenant configuration](#), are dependent on the type of Prisma Access license you have. To determine your license type, select **Panorama > Licenses** and find the information in the **Prisma Access** area.

Licenses available after November 17, 2020 include the license **Edition** and provide you with the type of **Prisma Access Locations** you can deploy (either **Local** or **Worldwide** locations).



Licenses available before November 17, 2020, contain the words **GlobalProtect Cloud Service** in the license areas and are divided by remote networks, mobile users, or Clean Pipe.



## Monitor Your Data Transfer Usage

You can view data transfer statistics for your mobile users, remote networks, and Clean Pipe deployments using the Data Transfer tab (**Panorama > Cloud Services > Status > Data Transfer**). This tab appears if you have the **Prisma Access Edition** licenses that became available after November 2020 along with the Prisma Access 2.0 Innovation version. If you have a legacy license that was available before November 2020 or a Prisma Access version that is not 2.0 Innovation, this tab does not display.

Prisma Access tracks this usage in a one-year period, starting with the date that you activate your license.



## Data Transfer (283 days remaining)



The Data Transfer page includes the following fields.

Field	Description
MU Usage	The amount of mobile user data usage. This data includes mobile user traffic for each type of mobile user deployment (Mobile Users—GlobalProtect and Mobile Users—Explicit Proxy), and includes both internal and internet traffic.
Net Usage	The amount of remote network data usage. If you have a <a href="#">Clean Pipe</a> deployment, data usage is displayed here. This data includes both internal and internet traffic.
Internet Traffic	Traffic sent and received from Prisma Access to the internet, including all internet and public SaaS applications. Any traffic sent from Mobile Users—GlobalProtect, Mobile Users—Explicit Proxy, and Remote Networks to the internet, and all Explicit Proxy traffic, displays in the Internet Traffic area.
Internal Traffic	Traffic that matches the following conditions: <ul style="list-style-type: none"> <li>• Traffic from a remote network site to another remote network site using remote network connections.</li> <li>• Traffic from a remote network site to a data center or headquarters location using a remote network connection (for the remote network site) and a service connection (for the data center or headquarters location).</li> <li>• Traffic from a mobile user to a remote network site using a GlobalProtect VPN tunnel and a remote network connection.</li> <li>• Traffic from a mobile user to a data center or headquarters location using a GlobalProtect VPN tunnel and a service connection.</li> </ul>

Prisma Access tracks your data transfer for mobile users, remote networks, and Clean Pipe per *unit*, and tracks the data starting on the date of your license activation. Units are based on the type of Prisma Access license you have; for mobile users, a unit is one mobile user and for remote networks, a unit is 1 Mbps.

Prisma Access allocates 250 GB of data for each unit per year, starting on the date of your license activation. If you have a license with multiple types of Prisma Access deployments, Prisma Access combines the units for all licenses you have to determine the maximum amount of data you can transfer during a

---

1 year period. The following table provides examples of the data transfer limit by license type and units purchased.

If you have a [multi-tenant deployment](#), data transfer across all tenants must add up to the total data transfer limit based on the allocated units in your license.

Quantity Purchased in Units	Data Transfer Limit
1,000 Mobile Users and Remote Networks	250 Terabytes/Year (250 GB * 1,000 units)
1,000 Mobile Users only	250 Terabytes/Year (250 GB * 1,000 units)
1,000 Remote Networks only	250 Terabytes/Year (250 GB * 1,000 units)
1,000 Mobile Users and Remote Networks 1,000 Mobile Users only	500 Terabytes/Year (250 GB * 2,000 units)
1,000 Mobile Users and Remote Networks 1,000 Remote Networks only	500 Terabytes/Year (250 GB * 2,000 units)

# Retrieve the IP Addresses for Prisma Access

If you are manually adding IP addresses of your Prisma Access infrastructure to an allow list in your network, or if you are using an automation script to enforce IP-based restrictions to limit inbound access to enterprise applications, you should understand what these addresses do and why you need to allow them, as well as the tasks you perform to retrieve them.

While you do not perform these tasks until after you complete your Prisma Access configuration, it is useful to understand these concepts in advance, so you understand what to do after your deployment is complete.



To learn about events that cause Prisma Access IP addresses to change and to plan for those changes, see [Plan for IP Address Changes for Mobile Users, Remote Networks, and Service Connections](#).

- [Prisma Access Infrastructure IP Addresses](#)
- [Run the API Script Used to Retrieve IP Addresses](#)
- [API Command Examples](#)
- [Pre-Allocate IP Addresses for Mobile User Locations](#)
- [Be Notified of Changes to IP Addresses](#)
- [Legacy Scripts Used to Retrieve IP and Loopback Addresses](#)

## Prisma Access Infrastructure IP Addresses

The following table provides you with a list of the IP address that Prisma Access uses for each deployment type, along with the keyword you use when you [run the API script](#) to retrieve the IP addresses, and whether or not you need to add them to an allow list.

For mobile users, during initial deployment, Prisma Access assigns two sets of IP addresses for each location you deploy: one set that is assigned to Prisma Access locations and portals that are currently active, and another set to reserve in case of a scaling event, infrastructure upgrade, or other event that causes Prisma Access to add locations, portals, or both. The API script allows you to retrieve the reserved set of IP addresses before they are used, preventing any issues with mobile users being able to access SaaS or public applications during a scaling event.

Deployment Type	IP Address Type	Description
<b>Mobile Users— GlobalProtect</b>	Prisma Access gateway ( <b>gp_gateway</b> )	Retrieves the gateway IP addresses. You must add both gateway and portal IP addresses to allow lists for your mobile user deployments.  Mobile users connect to a Prisma Access gateway to access internal or internet resources, such as SaaS or public applications, for which you have provided access.
	Prisma Access portal ( <b>gp_portal</b> )	Retrieves the portal IP addresses. You must add both gateway and portal

Deployment Type	IP Address Type	Description
		<p>IP addresses to allow lists for your mobile user deployments.</p> <p>As with gateways, you can retrieve both the active IP addresses and ones that are reserved for a scaling event. See <a href="#">Run the API Script Used to Retrieve IP Addresses</a> for examples.</p> <p>Mobile users log in to the Prisma Access portal to receive their initial configuration and gateway location.</p>
	Loopback IP addresses	<p>This address is the source IP address used by Prisma Access for requests made to an internal source, and is assigned from the <a href="#">infrastructure subnet</a>. Add the loopback IP address to an allow list in your network to give Prisma Access access to internal resources such as RADIUS or Active Directory authentication servers.</p> <p>Palo Alto Networks recommends that you allow all the IP addresses of the entire infrastructure subnet in your network, because <a href="#">loopback addresses for mobile users</a> can change. To find the infrastructure subnet, select <b>Panorama &gt; Cloud Services &gt; Status &gt; Network Details &gt; Service Infrastructure</b>. The subnet displays in the <b>Infrastructure Subnet</b> area.</p> <p>To retrieve loopback IP addresses, <a href="#">use the legacy API command</a>.</p>
<b>Mobile Users—Explicit Proxy</b>	Authentication Cache Service (ACS)	This the address for the Prisma Access service that stores the authentication state of the explicit proxy users.
	Network Load Balancer	This is the address that Prisma Access uses for the explicit proxy network load balancer.
<b>Remote Network</b>	Remote Network IP addresses ( <b>remote_network</b> )	Includes <b>Service IP Addresses</b> that Prisma Access assigns for the Prisma Access remote network connection, and <a href="#">egress IP addresses</a> that Prisma Access uses to make sure that remote

Deployment Type	IP Address Type	Description
		network users get the correct default language for their region. Add these addresses to allow lists in your network to give Prisma Access access to internet resources.
	Loopback IP addresses	This is the source IP address used by Prisma Access for requests made to an internal source, and is assigned from the <a href="#">infrastructure subnet</a> . Add the loopback IP address to an allow list to give Prisma Access access to internal resources such as RADIUS or Active Directory authentication servers. To retrieve loopback IP addresses, <a href="#">use the legacy API command</a> .
Clean Pipe	Clean Pipe IP Addresses ( <code>clean_pipe</code> )	If you have a Clean Pipe deployment, add these IP addresses to an allow list to give the Clean Pipe service access to internet resources.
	Loopback IP addresses	This is the source IP address used by Prisma Access for requests made to an internal source, and is assigned from the <a href="#">infrastructure subnet</a> . Add the loopback IP address to an allow list to give Prisma Access access to internal resources such as RADIUS or Active Directory authentication servers. To retrieve loopback IP addresses, <a href="#">use the legacy API command</a> .

## Run the API Script Used to Retrieve IP Addresses

Use the following steps to retrieve the IP addresses that Prisma Access uses in its infrastructure.

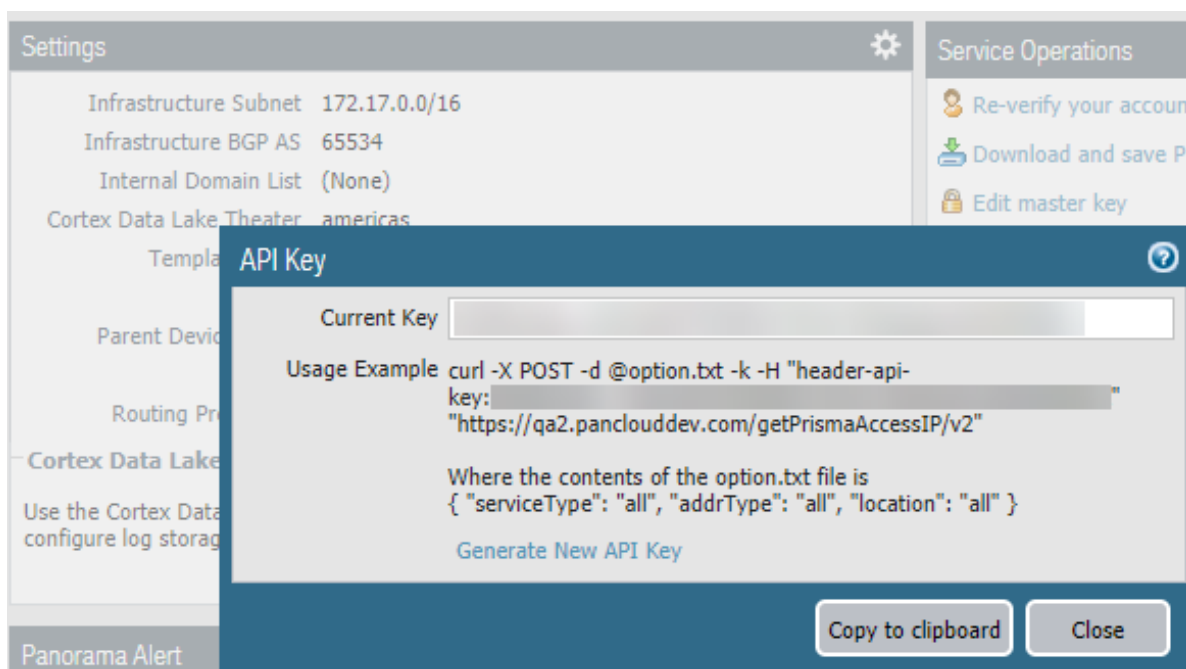


*This command does not retrieve loopback addresses; to retrieve loopback IP addresses, [use the legacy API command](#).*

### STEP 1 | Get the API key.

You need this key to authenticate to Prisma Access and retrieve the list of IP addresses using the API command. Only a Panorama administrator or Superuser can generate or access this API key.

1. Select **Panorama > Cloud Services > Configuration > Service Setup**.
2. Select **Generate API Key**.



If you have already generated an API key, the **Current Key** displays. If you haven't yet generated a key or want to replace the existing key to meet audit or compliance check for key rotation, click **Generate New API Key** for a new key.

**STEP 2 |** Create a .txt file and put the API command options in the file.

Using the API the command to use is a two-step process. First, you create a .txt file, specifying the parameters for the IP addresses to retrieve, and save the file in a folder that is reachable from the location where you run the command. Then, you run the API and specify the name and location of the .txt file you created in the command.

Specify the following keywords and arguments in the .txt file. See [API Command Examples](#) for examples. The examples in this document use a file name of **options.txt** but you can specify any file name, as long as you reference it in the command.

Argument	Possible choices (keywords)	Comments
<b>serviceType</b>	<b>all</b> <b>remote_network</b> <b>gp_gateway</b> <b>gp_portal</b> <b>clean_pipe</b> <b>swg_proxy</b>	<b>all</b> —Retrieves IP addresses you need to add to an allow list for all service types (Remote Networks, Mobile Users (both gateways and portals), and Clean Pipe, as applicable to your deployment). <b>remote_network</b> —Retrieves IP addresses you need to add to an allow list for remote network deployments. <b>gp_gateway</b> —Retrieves the Mobile Users—GlobalProtect gateway IP addresses you need to add to an allow list for mobile user deployments.

Argument	Possible choices (keywords)	Comments
		<p><b>gp_portal</b>—Retrieves the Mobile Users—GlobalProtect portal IP addresses you need to add to an allow list for mobile user deployments.</p> <p><b>clean_pipe</b>—Retrieves the IP addresses you need to add to an allow list for clean pipe deployments.</p> <p><b>swg_proxy</b>—Retrieves the Explicit Proxy IP addresses for the authentication cache service (ACS) and the network load balancers that you need to add to an allow list for explicit proxy deployments.</p> <p>The ACS addresses are common to the ACS service and are not dedicated per tenant. In addition to adding the ACS addresses to your allow lists, your identity provider (IdP) must accept authentication requests from these IP addresses.</p>
<b>addrType</b>	<p><b>all</b></p> <p><b>active</b></p> <p><b>reserved</b></p>	<p><b>all</b>—Retrieves all the IP addresses you need to add to an allow list.</p> <p><b>active</b>—Retrieves the active IP addresses. This keyword is applicable to mobile user deployments only.</p> <p><b>reserved</b>—Retrieves the reserved IP addresses. This keyword is applicable to mobile user deployments only.</p> <p>This API does not retrieve loopback IP addresses. To retrieve loopback IP addresses, <a href="#">use the legacy API command</a>.</p> <p><b>auth_cache_service</b>—Retrieves the IP address for the explicit proxy ACS (explicit proxy deployments only).</p> <p><b>network_load_balancer</b>—Retrieves the IP address for the explicit proxy network load balancer (explicit proxy deployments only).</p>
<b>actionType</b>	<b>pre_allocate</b>	<p><b>Mobile User deployments only</b>—An <b>actionType</b> of <b>pre_allocate</b> allows you to retrieve IP addresses or subnets for Prisma Access gateways and portals for mobile user deployments. Use this with a <b>serviceType</b> of <b>gp_gateway</b> to</p>

Argument	Possible choices (keywords)	Comments
		<p>retrieve pre-allocated gateway IP addresses and a <b>serviceType</b> of <b>gp_portal</b> to retrieve pre-allocated gateway IP addresses.</p> <p>Retrieving the pre-allocated IP addresses lets you add the gateway and portal IP addresses to your organization's allow lists before you onboard mobile user locations, which in turn gives mobile users access to external SaaS apps immediately after you onboard the locations. See <a href="#">Pre-Allocate IP Addresses for Mobile User Locations</a> for details.</p>
<b>location</b>	<b>all</b> <b>deployed</b>	<p><b>all</b>—Retrieves the IP addresses from all locations. For mobile user deployments, this keyword retrieves the IP addresses for both locations you added during onboarding, and locations you did not add.</p> <p><b>deployed</b>—Retrieves IP addresses in all locations that you added during mobile user onboarding.</p> <p>This keyword is applicable to mobile user deployments only. Prisma Access associates IP addresses for every mobile user location during provisioning, even if you didn't select that location <a href="#">during mobile user onboarding</a>. If you specify <b>all</b>, the API command retrieves the IP addresses for all mobile user locations, including ones you didn't select for the deployment. If you specify <b>deployed</b>, the API command retrieves only the IP addresses for the locations you selected during onboarding.</p>

Specify the options in the .txt file in the following format:

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

**STEP 3** | Enter the following command to retrieve the IP addresses:



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

Where *option.txt* is the .txt file you created in Step 2 and *Current-API-Key* is the Prisma Access API key.

For example, given a .txt file name of **option.txt** and an API key of **12345abcde**, use the following API command to retrieve the public IP address for all locations:

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



*The API command can return a large amount of information. To make the output more readable, if you have Python installed, you can add `| python -m json.tool` at the end of the CURL command.*

The API command returns the addresses in the following format:

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

Where:

- **address\_details** shows the details of the address for each location.
  - **serviceType** shows the type of IP address (either remote network (**remote\_network**), Prisma Access gateway (**gp\_gateway**), Prisma Access portal (**gp\_portal**), or Clean Pipe (**clean\_pipe**)).
  - **addressType** specifies the type of address specified with the `addrType` keyword (either **active**, **reserved**, or **pre-allocated** if you are [pre-allocating IP addresses for mobile user locations](#)).
  - **address** shows the IP address you need to add to your allow lists.

If the API returns multiple IP addresses (for example, if you have IP addresses for an active and a reserved Prisma Access gateway), Prisma Access summarizes the IP addresses in the **addresses** field.

- **addresses** lists all the IP addresses for the location that you need to add to your allow lists.
- **zone** is the Prisma Access location associated with the IP addresses.
- **zone\_subnet** is the subnet for mobile user gateways and portals. Prisma Access also provides this subnet if you [pre-allocate mobile user IP addresses](#).

If there are any problems with the options in the .txt file, the API returns an error similar to the following:

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

**STEP 4 |** Update the allow lists on your on-premises servers or SaaS application policy rules with the IP addresses you retrieved.

## API Command Examples

Use the following examples when entering keywords and arguments in the .txt file for the API command. To change the output of the command, change the options in the .txt file; the command itself does not change.

Retrieve These IP Addresses	Specify These Parameters in the .txt File	Comments
<b>Mobile User IP Addresses</b>		
All active and reserved mobile user IP Addresses	<pre>{   "serviceType":     "gp_gateway",   "addrType": "all",   "location": "all" }</pre>	<p>An <i>addrType</i> of <i>all</i> means that Prisma Access retrieves both active and reserved IP addresses for the locations you selected <a href="#">during mobile user onboarding</a>.</p> <p>A <i>location</i> of <i>all</i> means that Prisma Access retrieves IP addresses for all available locations, including ones that you have not onboarded. Prisma Access reserves non-onboarded location IP addresses so that you can add these IP addresses to your allow lists before you onboard them.</p>
Active and reserved IP addresses for onboarded mobile user locations	<pre>{   "serviceType":     "gp_gateway",   "addrType": "all",   "location": "deployed" }</pre>	<p>A <i>location</i> type of <i>deployed</i> means that Prisma Access retrieves only the IP addresses for the locations that you selected <a href="#">during mobile user onboarding</a>.</p>
All active IP Addresses for onboarded mobile user locations	<pre>{   "serviceType":     "gp_gateway",   "addrType": "active",   "location": "deployed" }</pre>	<p>An <i>addrType</i> of <i>active</i> means that Prisma Access retrieves only the active IP addresses, and does not retrieve reserved IP addresses, for the locations you onboarded.</p>
All reserved IP Addresses for onboarded mobile user locations	<pre>{   "serviceType":     "gp_gateway",</pre>	<p>An <i>addrType</i> of <i>reserved</i> means that Prisma Access retrieves only</p>

Retrieve These IP Addresses	Specify These Parameters in the .txt File	Comments
	<pre>"addrType": "reserved", "location": "deployed" }</pre>	<p>the reserved IP addresses for the locations you onboarded.</p> <p>Do not use an <i>addrType</i> of <i>reserved</i> with a <i>location</i> of <i>all</i>; Prisma Access does not allocate active and reserved IP addresses to locations that you have not onboarded.</p>
<b>Remote Network IP Addresses</b>		
Retrieve all remote network IP addresses	<pre>{ "serviceType": "remote_network", "addrType": "all", "location": "all" }</pre>	<p>This command retrieves the public and egress IP addresses of remote networks you have onboarded. Do not use a <i>location</i> of <i>deployed</i> or an <i>addrType</i> of <i>reserved</i>. You can use an <i>addrType</i> of <i>active</i> but it retrieves the same addresses as if you specified an <i>addrType</i> of <i>all</i>.</p>
<b>Clean Pipe IP Addresses</b>		
Retrieve all clean pipe IP addresses	<pre>{ "serviceType": "clean_pipe", "addrType": "all", "location": "all" }</pre>	<p>This command retrieves the public and egress IP addresses of clean pipes you have onboarded. Do not use a <i>location</i> of <i>deployed</i> or an <i>addrType</i> of <i>reserved</i>. You can use an <i>addrType</i> of <i>active</i> but it retrieves the same addresses as if you specified an <i>addrType</i> of <i>all</i>.</p>
<b>Explicit Proxy IP Addresses</b>		
Retrieve the ACS IP addresses for deployed locations	<pre>{ "serviceType": "swg_proxy", "location": "deployed", "addrType": "auth_cache_service" }</pre>	<p>This command retrieves the ACS IP address for your explicit proxy deployment. Entering an <i>addrType</i> of <i>all</i> retrieves all address types (the ACS and the network load balancer IP addresses).</p>

## Pre-Allocate IP Addresses for Mobile User Locations


Prisma Access uses gateway and portal IP addresses for Mobile Users—GlobalProtect deployments, and authentication cache service (ACS) and network load balancer IP addresses for Mobile Users—Explicit Proxy deployments. Mobile Users—GlobalProtect IP addresses are known as *egress IP addresses*. If you need to pre-allocate mobile user IP addresses before you onboard the location (for example, if your organization

---

needs to add the IP addresses for Mobile Users—GlobalProtect deployments to allow lists to give mobile users access to external SaaS applications), you can [run an API script](#) to have Prisma Access pre-allocate these IP addresses for a location ahead of time, before you onboard it. You can then add the location's egress IP addresses to your organization's allow lists before onboarding the location.

The API response also includes the public IP pool subnets for the egress IP addresses for the requested location. The egress IP addresses of any locations you add are a part of this subnet. Adding the subnets to your allow lists provides for future location additions without further allow list modification.

Prisma Access does not pre-allocate your IP addresses and subnets unless you request them using the API script. After you run the pre-allocation script, they have a validity period of 90 days. The IP addresses that Palo Alto Networks provides you are unique, not shared, and dedicated to your Prisma Access deployment during the validity period. You must onboard your locations before the validity period ends or you lose the addresses; to find the validity period at any time, run the API script.

 *Palo Alto Networks recommends that you only pre-allocate IP addresses for locations that you want to onboard later.*

To pre-allocate IP addresses, complete the following task.

**STEP 1** | Retrieve the Prisma Access [API key](#).

**STEP 2** | Pre-allocate the mobile user egress IP addresses by creating a .txt file and specifying the following options in the .txt file you create.

Enter the following text in the .txt file:

- **Mobile Users—GlobalProtect Deployments:**

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

- **Mobile Users—Explicit Proxy Deployments:**

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

Where *location* is the Prisma Access [location](#) or locations where you want to pre-allocate the IP addresses. If you enter multiple locations, use brackets around the set of locations and separate each location entry with quotes, a comma, and a space (for example, ["**location1**", "**location2**", "**location3**"], and so on).

Enter a maximum of 12 locations. Entering more than 12 locations might cause timeout errors when Prisma Access retrieves the pre-allocated IP addresses.

**STEP 3** | Enter the CURL command as shown in Step 3 in [Run the API Script Used to Retrieve IP Addresses](#).

**STEP 4** | Retrieve the IP addresses and subnets you requested, including their validity period, by re-opening the .txt file, removing the existing information, and editing it.

- **Mobile Users—GlobalProtect Deployments:**
  - To request Prisma Access to retrieve all pre-allocated IP addresses, enter the following text in the .txt file.

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

- To request Prisma Access to retrieve all pre-allocated IP addresses for Prisma Access gateways for a given location, enter the same information in the .txt file but substitute `all` with `gp_gateway` in the .txt file.
- To request Prisma Access to retrieve all pre-allocated IP addresses for Prisma Access portals for a given location, enter the same information in the .txt file but substitute `all` with `gp_portal` in the .txt file.
- **Mobile Users—Explicit Proxy Deployments:**

To request that Prisma Access pre-allocate all IP addresses you need to add to allow lists for an explicit proxy deployment, enter the following text in the .txt file.

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

Palo Alto Networks recommends that you enter `all` so you can retrieve all required pre-allocated egress IP addresses to add to your allow lists.



*For Mobile Users—GlobalProtect deployments, while Prisma Access returns up to four addresses for each location (one active and one reserved gateway IP address and, if required, one active and one reserved portal IP address), the API command can return a large amount of information. To make the output more readable, if you have Python installed, you can add | `python -m json.tool` at the end of the CURL command.*

#### STEP 5 | Re-enter the CURL command as shown in Step 3 in [Run the API Script Used to Retrieve IP Addresses](#) to retrieve the pre-allocated addresses.

Prisma Access returns the information in the following format:

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

Where the variables represent the following API command output:

Variable	Explanation
<i>prisma-access-zone1</i>	The Prisma Access location for which pre-allocated IP addresses were retrieved.
<i>ip-address1</i> and <i>ip-address2</i>	The egress IP addresses that Prisma Access has pre-allocated for the specified location.  Prisma Access retrieves <a href="#">two IP addresses for each location</a> ; you must add both of these IP addresses to your allow lists.
<i>subnet-and-mask1</i> and <i>subnet-and-mask2</i>	The subnets that Prisma Access has pre-allocated and reserved for the egress IP addresses in your deployment.
<i>service-type</i>	The type of the pre-allocated egress IP address (either <code>gp_portal</code> for a Prisma Access portal or <code>gp_gateway</code> for a Prisma Access gateway).
<i>validity-period</i>	The remaining time, in days, for which the pre-allocated IP address is valid.  You must onboard your mobile user location before the IP addresses' validity period ends. If the pre-allocated IP addresses expire, you can rerun the API script to retrieve another set of pre-allocated IP addresses.

You could receive an error if you attempt to pre-allocate IP addresses for locations that meet one of the following criteria:

- You have already onboarded the location.
- You onboarded, then deleted the location.

In this case, enter the following text in the .txt file to retrieve the Mobile Users—GlobalProtect IP addresses for the location:

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

- You have reached the maximum number of mobile user locations allowed by your license and cannot add any more locations.
- You entered the location name incorrectly.
- You entered a **serviceType** other than `gp_gateway`.
- you entered an **actionType** other than `pre_allocate`.
- You previously requested egress IP addresses for a location that is also a [compute location](#) and have not yet onboarded it.

---

## Be Notified of Changes to IP Addresses

To be notified of public IP address changes for remote networks and loopback IP address changes for service connections, remote network connections, and mobile users, you can specify a URL at which you can be alerted of a change. Prisma Access uses an HTTP POST request to send the notification. This POST request includes the following notification data in JSON format:

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

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

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

When you receive a notification, you must follow a two-step process. First, you must manually or programmatically [retrieve the IP](#) or [loopback](#) addresses. Then, you must update the IP addresses in your organization's appropriate allow list to ensure that users do not experience any disruption in service.



*Prisma Access sends this notification a few seconds before the new IP address becomes active. We recommend that you use automation scripts to both retrieve and add the new IP addresses to an allow list in your network.*

To add an IP notification URL, complete the following task.

**STEP 1** | Select **Panorama > Cloud Services > Configuration > Service Setup**.

**STEP 2** | Add an **IP Change Event Notification URL** where you can be notified of IP address changes in your Prisma Access infrastructure.



You can specify an IP address or an FQDN to an HTTP or HTTPS web service that is listening for change notifications. Prisma Access sends these notifications from the internet using a public IP address.

You do not need to commit your changes for the notification URL to take effect.

## Legacy Scripts Used to Retrieve IP and Loopback Addresses



*The commands described in this section are superseded as of Prisma Access 1.5; however, they are still supported for when you need to obtain the loopback address, or for deployments that use them in scripts or other automated tools.*

The following table shows the keywords and parameters that are available in the legacy API scripts used with Prisma Access, and provides information and recommendations about which API to use for the type of deployment you have.

These legacy commands retrieve two types of IP addresses, *public IP* and *egress IP* addresses. We provide you with two different legacy API commands so that you can retrieve all the IP addresses you need to add to an allow list.

- A *public IP address* is the source IP address that Prisma Access uses for requests made to an internet-based source. Add the public IP address to an allow list in your network to give Prisma Access access to internet resources such as SaaS applications or publicly accessible partner applications.

Mobile user, remote network, and clean pipe deployments use public IP addresses.

- An *egress IP address* is an IP address that Prisma Access uses for egress traffic to the internet, and you must also add these addresses to an allow list to give Prisma Access access to internet resources.

Among other purposes, Prisma Access uses egress IP addresses so that users receive web pages in the [language they expect](#) from a Prisma Access location. All locations have public IP addresses; however, not all locations have egress IP addresses. The following locations do not use egress IP addresses:

- Any locations that you added before the release of Prisma Access 1.4.
- Bahrain
- Belgium
- France North
- France South
- Hong Kong
- Ireland
- South Korea
- Taiwan
- United Kingdom

Mobile user, remote network, and clean pipe deployments use egress IP addresses.

Commands Used in Mobile User Deployments	
Command Name	Comments
<p><b>get_egress_ip_all=yes</b> command</p> <pre>curl -k -H header-api-key:"Current-API-Key" https://api.gpcloudservice.com/getAddrList/latest?get_egress_ip_all=yes</pre>	<p>This command retrieves all the IP addresses that you add to an allow list to give Prisma Access access to internet resources such as SaaS applications or publicly accessible partner applications. This command has the following constraints:</p> <ul style="list-style-type: none"> <li>• This command can retrieve a large number of addresses (more than 200). If your enterprise cannot add this number of IP addresses to an allow list, you can use the <i>gpcs_gp_gw</i> and <i>gpcs_gp_portal</i> keywords to retrieve only the IP addresses you are currently using; however you will have to rerun these commands every time you add a location. In addition, if a <a href="#">scaling event</a> occurs, you will need to the new IP addresses to an allow list.</li> <li>• Prisma Access does not list the locations that are associated with these IP addresses; therefore, we recommend that you all the IP addresses that are returned with this command to an allow list.</li> </ul>



Commands Used in Mobile User Deployments	
Command Name	Comments
	<ul style="list-style-type: none"> <li>This command does not give you loopback addresses.</li> </ul>
<p><b>gpcs_gp_gw</b> and <b>gpcs_gp_portal</b> keywords</p> <pre>curl -k -H header-api-key: <i>Current-API-Key</i> https://api.gpcloudservice.com/getAddrList/latest?fwType=gpcs_gp_gw   gpcs_gp_portal&amp;addrType=public_ip   egress_ip_list   loopback_ip"</pre>	<p>Use this command if your deployment limits the amount of IP addresses you can add to an allow list. You must add all IP addresses returned with this command to an allow list in your network. You can also retrieve the loopback IP addresses with this command.</p> <p>This command has the following limitations:</p> <ul style="list-style-type: none"> <li>It doesn't list any of the reserved IP addresses used for scaling events.</li> <li>It doesn't list any of the reserved IP addresses used for locations that you haven't yet added.</li> </ul>

Commands Used In Remote Network Deployments	
Command Name	Comments
<p><b>gpcs_remote_network</b> keyword</p> <pre>curl -k -H header-api-key: <i>Current-API-Key</i> https://api.gpcloudservice.com/getAddrList/latest?fwType=gpcs_remote_network &amp;addrType=public_ip   egress_ip_list   loopback_ip"</pre>	<p>Use this command to find the IP addresses that you need to add to an allow list for remote network deployments.</p> <p>You can also use this command to find the egress IP addresses for remote network deployments; the egress and IP addresses can be different <a href="#">in some situations</a>.</p>

Commands Used in Clean Pipe Deployments	
Command Name	Comments
<p><b>gpcs_clean_pipe</b> keyword</p> <pre>curl -k -H header-api-key: <i>Current-API-Key</i> https://api.gpcloudservice.com/getAddrList/latest?fwType=gpcs_clean_pipe&amp;addrType=public_ip   egress_ip_list   loopback_ip"</pre>	<p>Use this command to find the IP addresses that you need to add to an allow list for clean pipe deployments.</p>

## Retrieve Public and Egress IP Addresses for Mobile User Deployments

If you are adding public IP addresses to allow lists to give mobile users access to SaaS or public applications, Prisma Access provides two sets of public IP and egress IP addresses so that it can automatically add locations during a scaling or other event (for example, when a large number of mobile users join a single gateway):

- One set that is assigned to Prisma Access locations and portals that are currently active.
- Another set to reserve in case of a scaling event, infrastructure upgrade, or other event that causes Prisma Access to add locations, portals, or both.

You can then add this reserved set of IP addresses to an allow list before they are used, preventing any issues with mobile users being able to access SaaS or public applications during a scaling event. See [IP Address Allocation For Mobile Users](#) for more information about the IP allocation process.

Retrieve these new addresses by completing the following task:

**STEP 1 |** Get the API key by selecting **Panorama > Cloud Services > Configuration > Service Setup**; then, selecting **Generate API Key**.

You need this key to authenticate to Prisma Access and retrieve the list of IP addresses using the curl command listed below. Only a Panorama administrator or Superuser can generate or access this API key.

**STEP 2 |** Enter the following command to retrieve the mobile user public IP addresses:

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

Where *Current-API-Key* is the Prisma Access API key.

For example, given an API key of **12345abcde**, use the following API command to retrieve the public IP address for all locations:

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

Every time Prisma Access uses the reserved set of public IP addresses, [it allocates another set of reserved IP addresses](#). If you think that Prisma Access has used the reserved set of public IP addresses (for example, if a large number of mobile users have accessed a single location), you can run this API command again to find the new set of reserved public IP addresses. All IP addresses persist after an upgrade.

## Retrieve Public, Loopback, and Egress IP Addresses

To retrieve public, loopback, and egress IP addresses, complete the following steps.

**STEP 1 |** Get the API key and add an **IP Change Event Notification URL** where you can be notified of IP address changes in your Prisma Access infrastructure.

See [Be Notified of Changes to IP Addresses](#) for details.

**STEP 2 |** Retrieve the public IP addresses, loopback IP addresses, or both for Prisma Access.

Use the API key and the API endpoint URL either manually or in an automation script:

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

where you need to replace *Current API Key* with your API key and use one or both of the following keywords and arguments:

Keyword	Description
<b>fwType</b> keyword	
<b>gpcs_gp_gw</b>	Retrieves Prisma Access gateway IP addresses (for mobile user deployments).
<b>gpcs_gp_portal</b>	Retrieves Prisma Access portal IP addresses (for mobile user deployments).
<b>gpcs_remote_network</b>	Retrieves Prisma Access remote network IP addresses (for remote network deployments).
<b>gpcs_clean_pipe</b>	Retrieves Prisma Access Clean Pipe IP addresses.
<b>addrType</b> keyword	
<b>public_ip</b>	Retrieves the source IP addresses that Prisma Access uses for requests made to an internet-based source.  For mobile user locations, Prisma Access lists the IP addresses by location. For remote networks, Prisma Access lists the IP addresses by remote network name.
<b>egress_ip_list</b>	Retrieves the IP addresses that Prisma Access uses with public IP addresses for additional egress traffic to the internet.  For mobile user locations, Prisma Access lists the IP addresses by location. For remote networks, Prisma Access lists the IP addresses by remote network name.
<b>loopback_ip</b>	Retrieves the source IP addresses used by Prisma Access for requests made to an internal source (for example, a RADIUS or Active Directory server), and is assigned from the <a href="#">infrastructure subnet</a> .

If you don't specify a keyword, Prisma Access retrieves all IP addresses.

For example, you can try the following Curl command to manually retrieve the list of public IP addresses for all remote networks:

```
curl -k -H header-api-key:1234y9ydx__0UmxetVTbC8XTyFMaoT4RBZBKBjfx419YVufeFG7
"https://api.gpcloudservice.com/getAddrList/latest?fwType=gpcs_remote_network&addrType=public_ip"
```

or use a simple python script to retrieve the list of all IP addresses, for example:

```
#!/usr/bin/python
import subprocess
import json
api_key = '1234y9ydx__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 3** | Update the allow lists on your on-premises servers or SaaS application policy rules with the IP addresses you retrieved.

---

# Plan for IP Address Changes for Mobile Users, Remote Networks, and Service Connections

After you set up your Prisma Access deployment, it is useful to know when IP addresses change so that you can pro-actively plan your infrastructure and add required IP addresses to allow lists accordingly. The IP address changes can be the result of changes you made (for example, adding another mobile users location) or changes that Prisma Access performs automatically (for example, a large number of mobile users accesses a single Prisma Access gateway).

The following sections describe how IP addresses can change:

- [IP Address Allocation For Mobile Users](#)
- [IP Address Changes For Remote Network Connections](#)
- [Mobile User and Remote Network IP Allocation Changes After a Compute Location Change](#)
- [Loopback IP Address Allocation for Mobile Users](#)

## IP Address Allocation For Mobile Users

After you deploy Prisma Access for users for the first time, Prisma Access adds two sets of [public and \(if applicable\) egress IP addresses](#) for each portal and gateway: one set that is in active use and another set that is reserved for future use. These IP addresses are unique, not shared, and dedicated to your Prisma Access deployment. If you have a multi-tenant setup, Prisma Access adds dedicated IP addresses for each tenant.

Since the public IP address is the source IP address used by Prisma Access for requests made to an internet-based source, you need to know what the public IP address are and add them to an allow list in your network to provide your users access to resources such as SaaS applications or publicly-accessible partner applications.

The public IP addresses can change, and Prisma Access can put the reserved public IP address sets into active use, if the following events occur:

- A large number of mobile users access a location in the same location.

When a scaling event occurs, Prisma Access adds one or more gateways to accommodate the increased number of users, [assigns one or more](#) of the reserved public IP addresses to the new gateways and makes them active, and adds a new set of reserved IP addresses to the mobile user locations to replace the ones that were used.

- You add one or more locations to your deployment.

When you add more locations, Prisma Access adds another gateway and a new set of active and reserved IP addresses for each new location you add.

- Prisma Access upgrades its infrastructure, usually in conjunction with a new software release and an upgrade to the Cloud Services plugin.

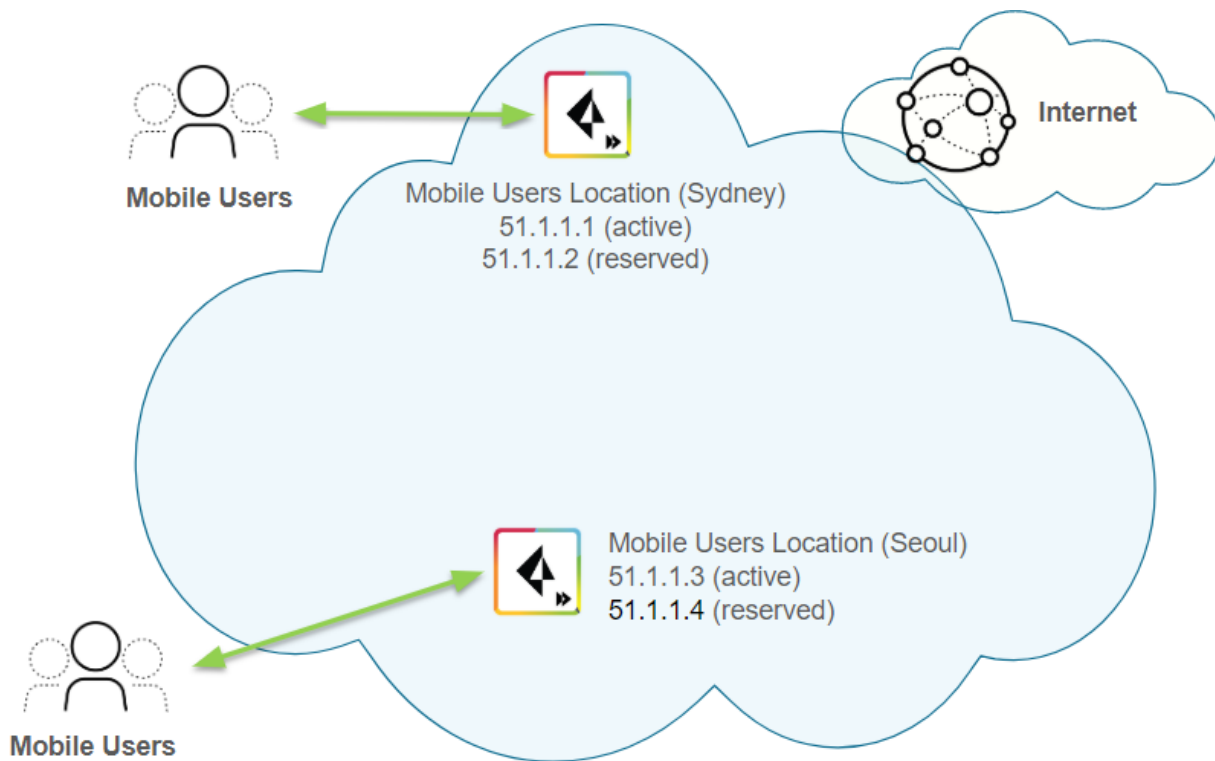
Prisma Access makes the reserved public IP addresses active, and makes the active public IP addresses reserved.

Because Prisma Access adds more public IP addresses when you add a gateway, and can add more public IP addresses after a scaling event, you should [add an IP Change Event Notification URL](#), or use the API to retrieve mobile user addresses, to be notified of IP address changes in your Prisma Access infrastructure. You can then add any added or changed addresses to an allow list.

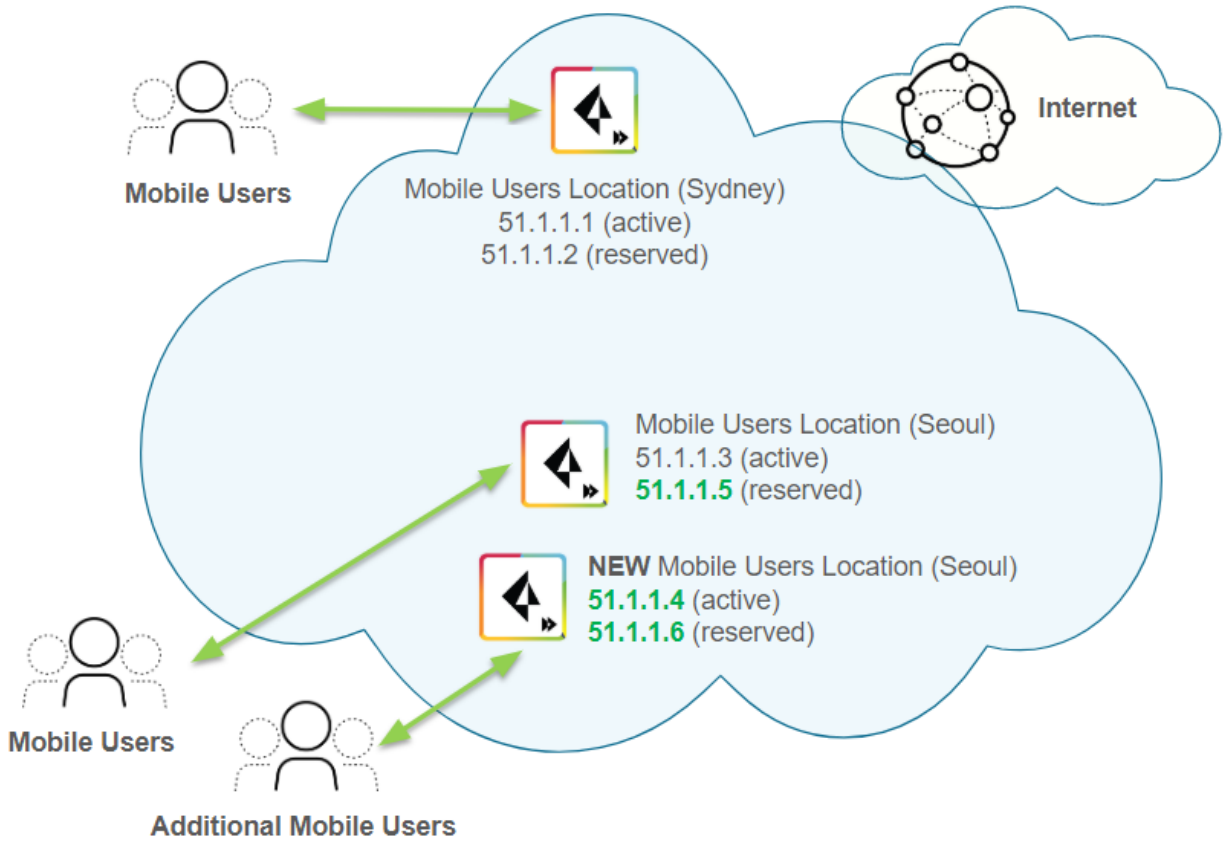
## Public IP Address Scaling Examples for Mobile Users

The following examples illustrate the mobile user public IP address allocation process that Prisma Access uses during a scaling event or when you add a new location.

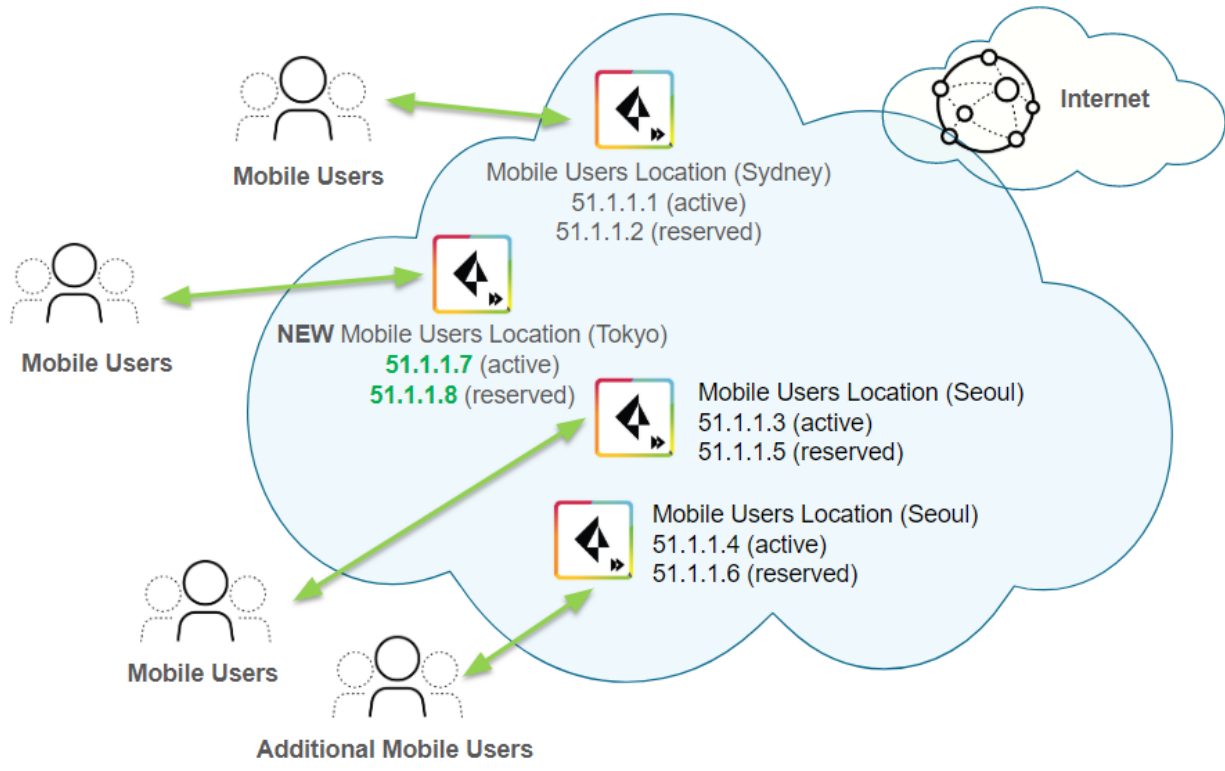
In the following example, you specified two locations in the Asia Pacific region for a new mobile user deployment: Sydney and Seoul. Each location has an active and reserved set of public IP addresses. Prisma Access reserves four sets of IP addresses for the gateways: two active and two reserved.



Then a large number of users log in to the Seoul location. To accommodate these extra users, Prisma Access adds a second gateway for the Seoul location and takes the reserved address from the first Seoul gateway (51.1.1.4) and makes this the active IP address for the second Seoul gateway. It then adds two additional IP addresses (51.1.1.5 and 51.1.1.6 in this example) to use as reserved IP addresses for the two Seoul gateways.




Then you add another location, Tokyo, in the Asia Pacific region. Prisma Access creates two new IP addresses for the new gateway (51.1.1.7 and 51.1.1.8).



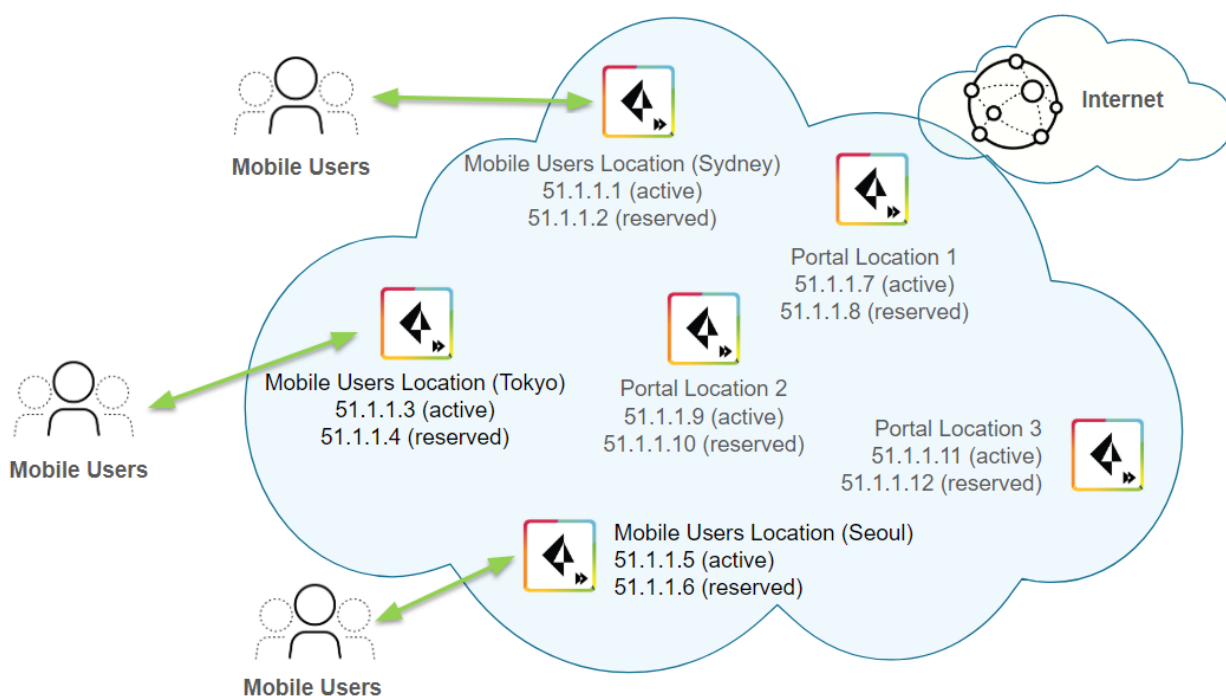
Each time you add a location or have a scaling event, you should [Retrieve Public and Egress IP Addresses for Mobile User Deployments](#) that Prisma Access assigned and add them to an allow list in your network. Prisma Access keeps two sets of IP addresses at all times for all active gateways in each location.

### Mobile User Public IP Address Reassignment Example After an Infrastructure Upgrade

When Prisma Access upgrades its infrastructure, usually to prepare for a software upgrade for the Cloud Services plugin, it changes the public IP addresses from active to reserved and vice versa. The following example illustrates the process.

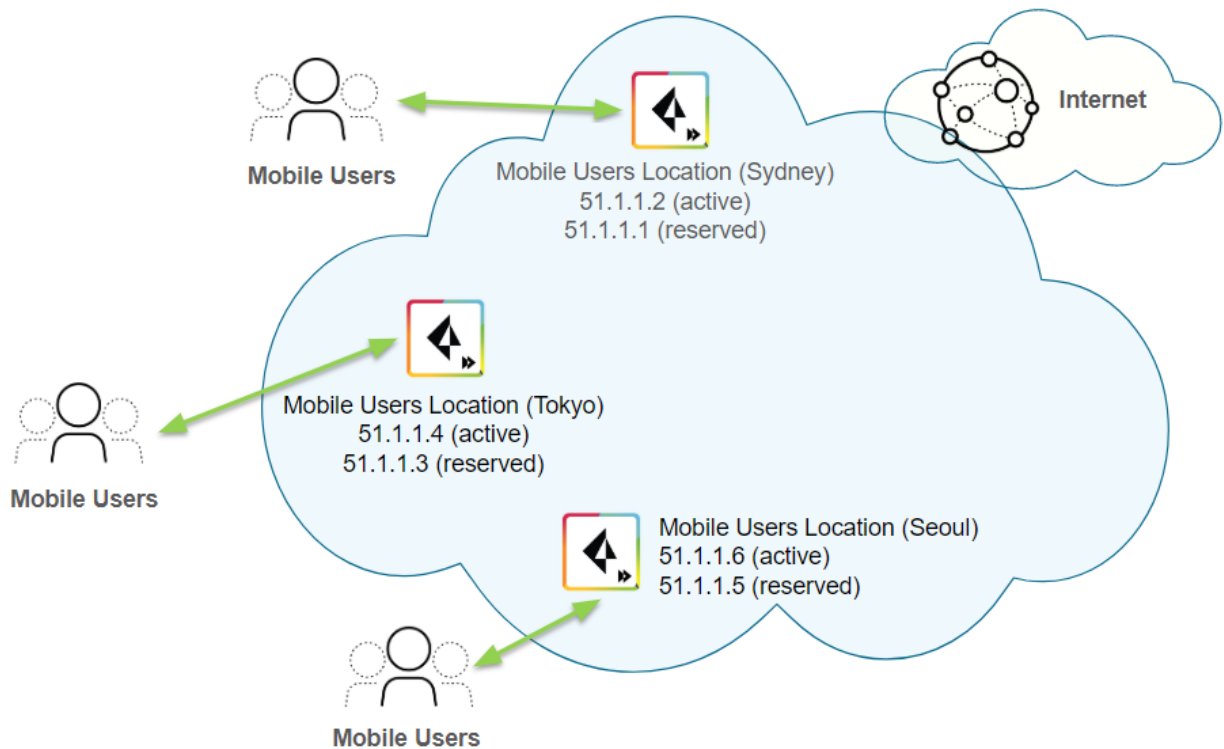
 *Subscribe to text or email notices for upcoming scheduled infrastructure upgrades at [status.paloaltonetworks.com](https://status.paloaltonetworks.com).*

The following graphic shows a sample deployment with three Prisma Access portals, three locations (Sydney, Tokyo, and Seoul), and an active and reserved public IP address for each portal and location.




After an infrastructure upgrade, Prisma Access reverses the public IP addresses for each portal and location. In this example, the Sydney location's active public IP address changes from 51.1.1.1 to 51.1.1.2 and its reserved public IP address changes from 51.1.1.2 to 51.1.1.1. Adding both the active and reserved public IP addresses to allow lists ensures that users can still access the Prisma Access portals and gateways after an infrastructure upgrade.






### IP Address Changes For Remote Network Connections

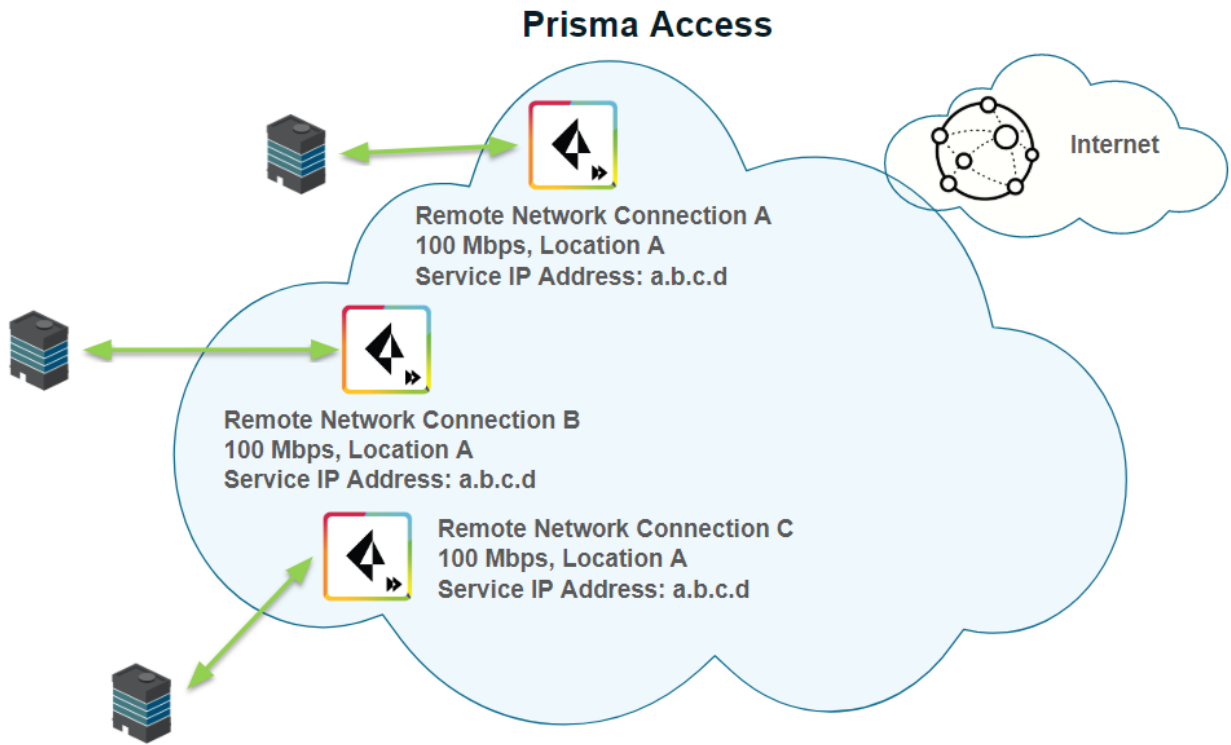
IP addresses for remote network connections are unique, not shared, and dedicated to your Prisma Access deployment. These IP addresses do not change after Prisma Access creates them as part of remote network onboarding, and the IP addresses persist after an upgrade. However, take care when increasing the bandwidth of an existing connection, because the IP address of a remote network can change if that increase causes the bandwidth in a location to exceed 300 Mbps.

 *In addition, egress IP addresses can change if Prisma Access creates a new [compute location](#) and you decide to use this new compute location with locations you have already onboarded. See [Mobile User and Remote Network IP Allocation Changes After a Compute Location Change](#) for details.*

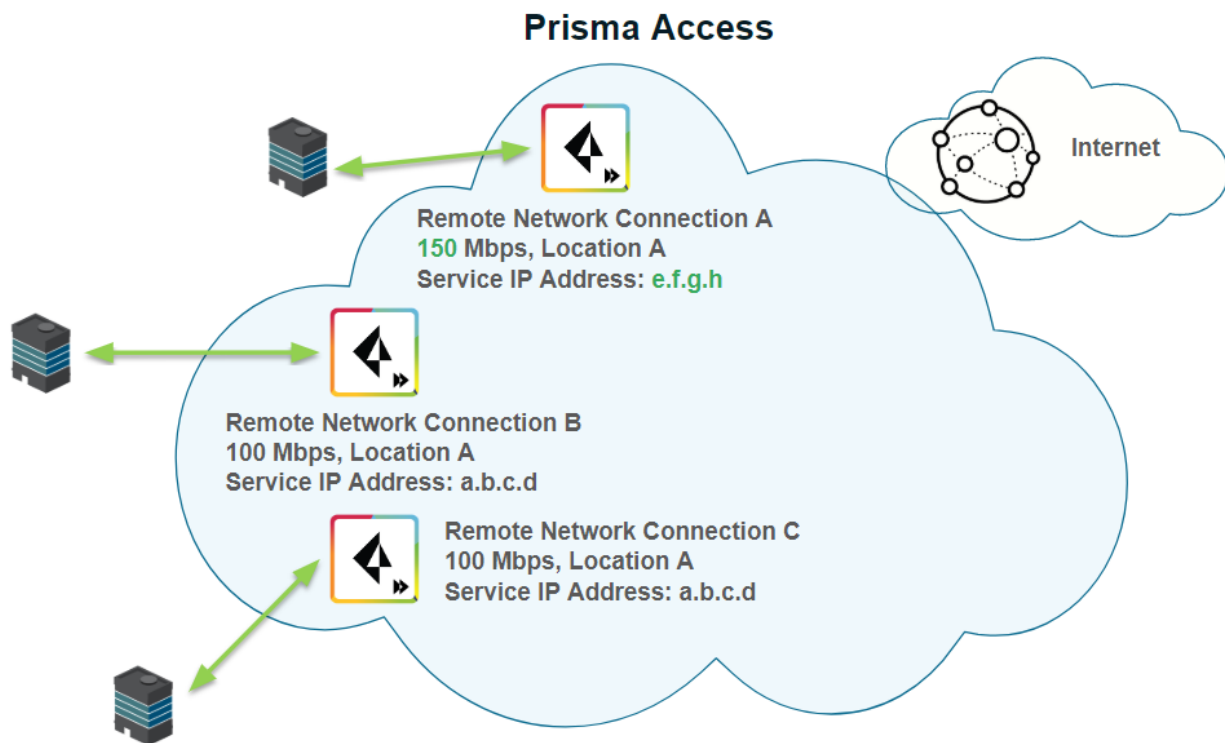
These bandwidth guidelines apply only when you upgrade an existing connection. A single remote network connection, even a 1000 Mbps (Preview) connection, always receives a single **Service IP Address**, regardless of its size.

 *The 1000 Mbps bandwidth option is in preview mode. The throughput during preview is delivered on a best-effort basis and the actual performance will vary depending upon the traffic mix.*


The following example shows three remote network connections in the same location, each with a bandwidth of 100 Mbps. Since the total bandwidth is 300 Mbps, Prisma Access assigns a single IP address for all connections in the location.



The following example shows the bandwidth of remote network connection A being increased from 100 Mbps to 150 Mbps. Since the total bandwidth of all connections is now more than 300 Mbps, Prisma Access assigns a new service IP address for the connection with the additional bandwidth. The other service IP addresses remain unchanged.



Conversely, given five remote networks with a bandwidth of 50 Mbps, if you increase the bandwidth of one of the remote networks to 100 Mbps, the Service IP address of that remote network does not change because the total bandwidth is now 300 Mbps.


 *If you reduce the bandwidth of a remote network connection, the Service IP address does not change.*

To find the service IP addresses in Panorama, select **Panorama > Cloud Services > Status > Network Details** tab and click the **Remote Networks** radio button to display the **Service IP Address** for the remote networks, or [use the API script](#).

### Mobile User and Remote Network IP Allocation Changes After a Compute Location Change

To optimize performance and improve latency, Prisma Access can introduce new [compute locations](#) for existing remote network locations as part of a plugin upgrade. When you upgrade the plugin, you can choose to take advantage of the new compute location. If you change the compute region, Prisma Access changes the gateway and portal IP addresses (for mobile users) and egress IP addresses (for remote networks) for the location or locations to which the new compute location is associated. If you use allow lists in your network to provide users access to internet resources such as SaaS applications or publicly accessible partner applications, you need to add these new IP addresses to your allow lists.

To upgrade to a new compute location after it becomes available, complete the following task.

 *To reduce down time for mobile user deployments, you can use the [API](#) to pre-allocate the new gateway and portal IP addresses before you perform these steps.*


1. Delete the location associated with the new compute location.

2. Commit and push your changes.
3. Re-add the locations you just deleted.
4. Commit and push your changes.
5. Retrieve the new gateway and portal IP addresses (for mobile users) or the new egress IP addresses (for remote networks) [using the API script](#).
6. Make a note of the new IP addresses and add them to your allow lists.

Since you need to allow time to delete and add the existing location and change your allow lists, Palo Alto Networks recommends that you schedule a compute location change during a maintenance window or during off-peak hours.

### Loopback IP Address Allocation for Mobile Users

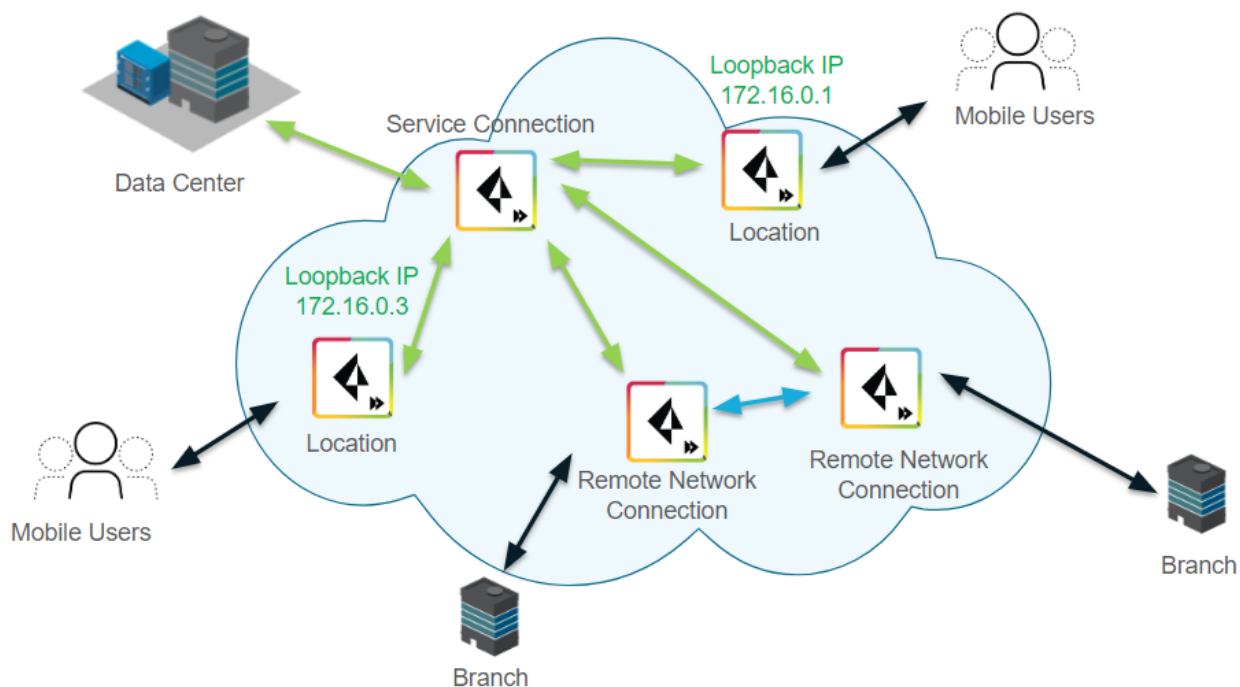
Loopback IP addresses can change during for mobile users during an infrastructure upgrade.

 *Loopback IP addresses do not change for service connections or remote network connections during an infrastructure upgrade; only mobile user loopback IP addresses can change.*

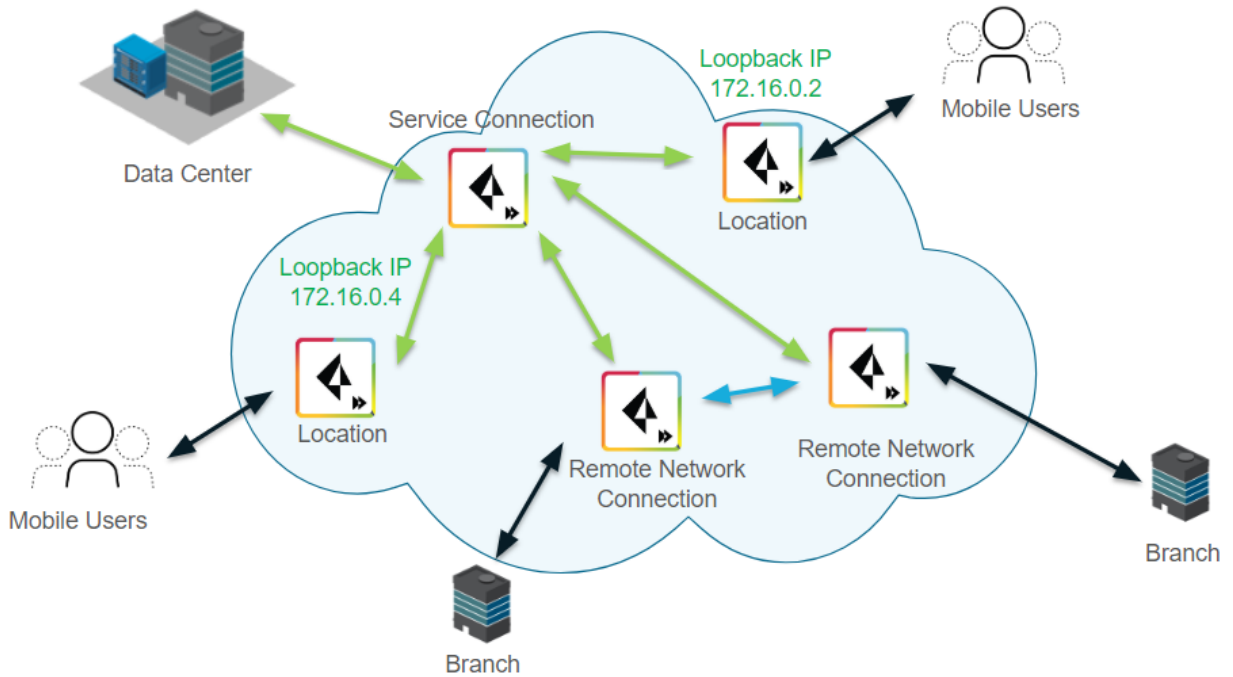
Prisma Access allocates the loopback IP addresses from the infrastructure subnet that you specify when you [enable the Prisma Access infrastructure](#). You can add the entire infrastructure subnet to an allow list and avoid planning for mobile user loopback IP changes during an infrastructure upgrade. To find the infrastructure subnet, select **Panorama > Cloud Services > Status > Network Details > Service Infrastructure** and view the **Infrastructure Subnet**.

Retrieve these addresses using the [Retrieve Public, Loopback, and Egress IP Addresses](#) used to retrieve public IP and loopback IP addresses.

The following example shows a Prisma Access deployment that has an infrastructure subnet of 172.16.0.0/16. Prisma Access has assigned loopback IP addresses 172.16.0.1 and 172.16.0.3 for mobile users from the infrastructure subnet.



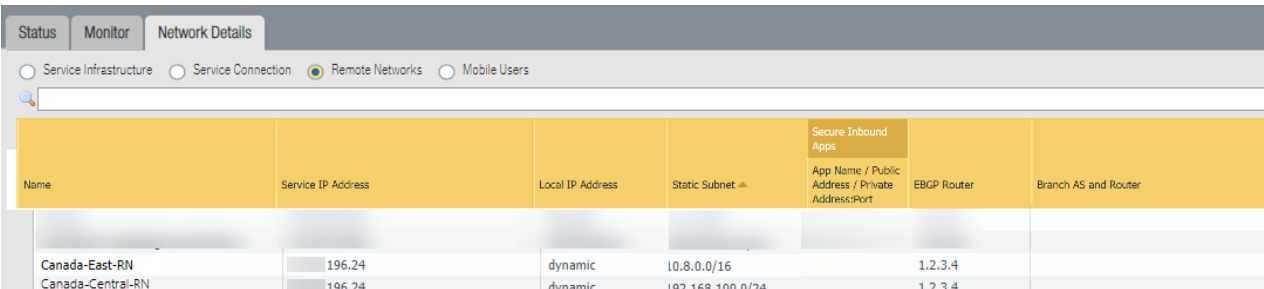
After in infrastructure upgrade (for example, to prepare for a new release of the Cloud Services plugin), Prisma Access assigns two different IP addresses for mobile users from the infrastructure subnet (172.16.0.1 is changed to 172.16.0.2 and 172.16.0.3 is changed to 172.16.0.4).



# Service IP and Egress IP Address Allocation for Remote Networks

Prisma Access has [more than 100 locations](#) available to accommodate worldwide deployments and provide a localized experience. Two locations might map to the same **Service IP address**, which you use as the peer IP address when you set up the IPSec tunnel for the remote network connection. However, the locations might use different egress IP addresses to make sure that the user gets the correct default language for the region.

The following example shows a customer deployment with two remote network locations deployed in Canada: Central Canada and Eastern Canada. Prisma Access assigned the same **Service IP Address** to both locations. When you configure the remote network tunnel, use this IP address as the peer IP address when you create the IPSec tunnel for the remote network connection.




The screenshot shows the 'Network Details' tab in the Prisma Access interface. It features a search bar and a table with columns for Name, Service IP Address, Local IP Address, Static Subnet, Secure Inbound Apps (App Name / Public Address / Private Address:Port), EBG Router, and Branch AS and Router. Two rows are visible: 'Canada-East-RN' and 'Canada-Central-RN'. Both have a Service IP Address of 196.24. The Local IP Address for Canada-East-RN is 'dynamic' and for Canada-Central-RN is 'dynamic'. The Static Subnet for Canada-East-RN is '10.8.0.0/16' and for Canada-Central-RN is '192.168.100.0/24'. Both have an EBG Router of '1.2.3.4'.

Name	Service IP Address	Local IP Address	Static Subnet	Secure Inbound Apps App Name / Public Address / Private Address:Port	EBGP Router	Branch AS and Router
Canada-East-RN	196.24	dynamic	10.8.0.0/16		1.2.3.4	
Canada-Central-RN	196.24	dynamic	192.168.100.0/24		1.2.3.4	

However, Eastern Canada uses a different default language (French) than Central Canada (English). For this reason, Prisma Access assigns them different egress IP addresses. If you run the API script for egress IP addresses, you will receive two different IP addresses for these two locations.

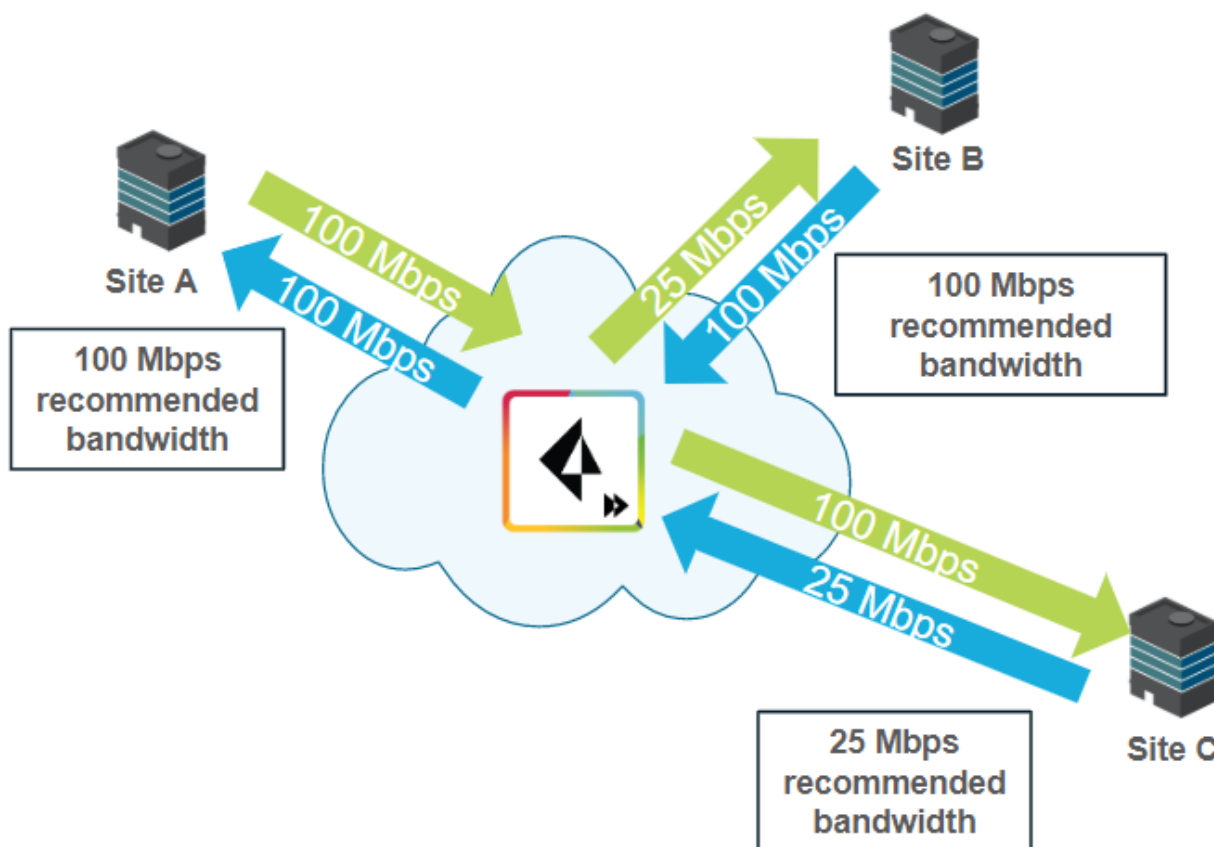
# How to Calculate Remote Network Bandwidth

 This section applies only to deployments where you allocate bandwidth by remote network location. To plan your bandwidth if you allocate bandwidth by compute location, or for upgrade considerations when migrating to allocating bandwidth by compute location, see [Plan to Deploy Remote Networks](#).

When you onboard a remote network, it is important to specify the correct remote network connection bandwidth that meets the needs of your organization.

The number you specify for the bandwidth applies to both the egress and ingress traffic for the remote network connection. If you specify a bandwidth of 50 Mbps, Prisma Access provides you with a remote network connection with 50 Mbps of bandwidth on ingress and 50 Mbps on egress. Your bandwidth speeds can go up to 10% over the specified amount without traffic being dropped; for a 50 Mbps connection, the maximum bandwidth allocation is 55 Mbps on ingress and 55 Mbps on egress (50 Mbps plus 10% overage allocation).

If you have an asymmetric internet connection, you should consider your organization's requirements to determine the bandwidth to specify. Use the following graphic and examples to size your remote network connection.



- Site A has a 100 Mbps connection both upstream and downstream. For this site, specify a remote network connection of 100 Mbps.

- 
- Site B has an asymmetric connection, with 100 Mbps upstream and 25 Mbps downstream, and you want to make sure that the remote network connection does not throttle the upstream traffic. In this case, specify a remote network connection of 100 Mbps.
  - Site C has an asymmetric connection, with 25 Mbps upstream and 100 Mbps downstream. For this site, you want to make sure that the remote network connection does not throttle the upstream traffic, but throttling the downstream traffic is acceptable. In this case, you can specify a remote network connection of 25 Mbps, which ensures that Prisma Access delivers 25 Mbps reliably in both directions.

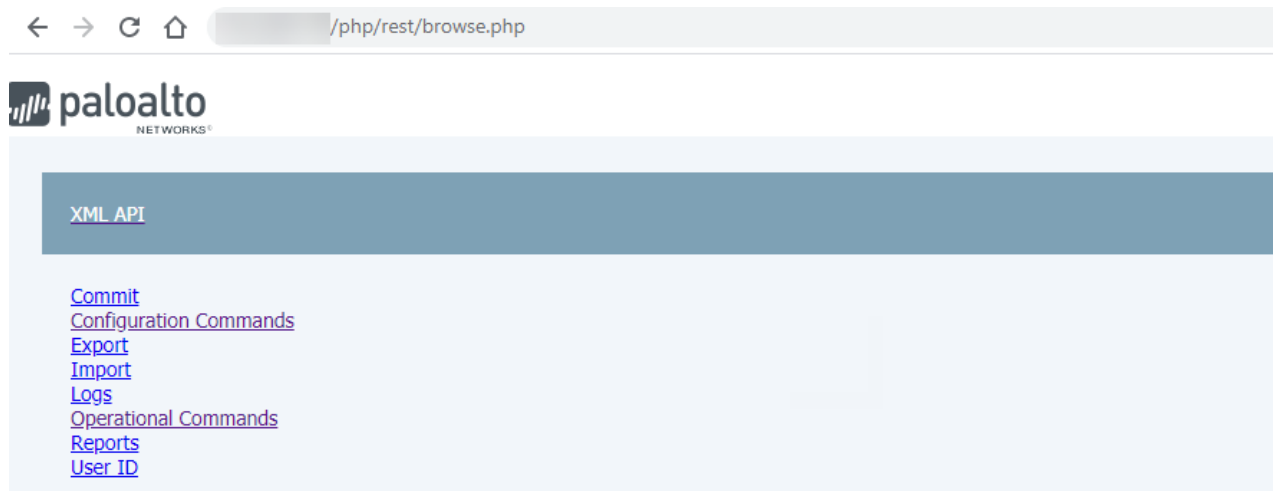


---

# Prisma Access APIs

In addition to the XML APIs that are available for configuration and management in [Panorama](#), there are XML APIs for the Cloud Services plugin that you can use to perform tasks specific to Prisma Access. Use these APIs through a third-party service, application, or script to automate configuration and reporting tasks for Prisma Access.

To access the API using the browser, log in to the Panorama that manages Prisma Access with administrator privileges, then enter `/api` at the end of the URL.



The Prisma Access APIs are located in the following XML Path Language (XPath) nodes in the XML tree:

- Configuration Commands: **XML API > Configuration Commands > devices > entry[@name='localhost.localdomain'] > plugins > cloud\_services**
- Operational Commands: **XML API > Operational Commands > request > plugins > cloud\_services > prisma-access**

As you navigate in the XML tree, Prisma Access populates the tree in the **XML** area. You can enter required values in the **XML** area and click **Submit** to process an XML request. For example, to request the status of a job, navigate to **XML API > Operational Commands > request > plugins > cloud\_services > prisma-access > job-status > jobid**, enter the Job id in the **jobid** field, enter the Service Type **servicetype** area, and click **Submit** to submit your request.

## XML API › Operational Commands › request › plugins › cloud\_services › prisma-access › job-status › jobid

XML

```
<request><plugins><cloud_services><prisma-access><job-status><jobid>25748</jobid><servicetype>remote-networks</servicetype></job-status></prisma-access></cloud_services></plugins></request>
```

Submit

XML API Uri

```
/api/?type=op&cmd=<request><plugins><cloud_services><prisma-access><job-status><jobid></jobid></job-status></prisma-access></cloud_services></plugins></request>
```

Prisma Access returns the output in XML format.

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

```
<?xml version="1.0" encoding="UTF-8" ?>
<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>
```

You can also use the [web interface](#) to find Prisma Access APIs. See the [PAN-OS and Panorama API Usage Guide](#) for details.

# Activate and Install the Prisma Access Components

After you determine what licenses you need and the bandwidth and mobile user quantity that is required for your deployment, you activate and install the components as shown in the following sections.

- > Activate and Install Prisma Access (Panorama Managed)
- > Transfer or Update Prisma Access Licenses
- > Configure Panorama Appliances in High Availability for Prisma Access



---

# Activate and Install Prisma Access (Panorama Managed)

Use the following workflow to activate your Prisma Access (Panorama Managed) licenses and download and install the Cloud Services plugin. If you are upgrading an existing Prisma Access deployment to a new version, use the workflow in the [Prisma Access Release Notes \(Panorama Managed\)](#) to upgrade the Cloud Services plugin.

- [Installation Prerequisites](#)
- [Hub Roles and Prisma Access Installation](#)
- [Activate and Install Prisma Access](#)



*Prisma Access does not support FIPS-CC mode.*

## Installation Prerequisites

Before you begin your installation and activation, make sure that you have the following information and resources:

- ❑ Be sure that you have the order fulfillment email that contains the activation links that are required to activate Prisma Access.
- ❑ If you will use an existing Panorama to manage Prisma Access, be sure you that the Panorama on which you will install the Cloud Services plugin (which activates Prisma Access) is running the minimum Panorama version.

During product activation, you can select an existing Panorama to manage Prisma Access, if you have [registered Panorama](#), [installed the licenses](#), and [activated the support license](#) on the [Customer Support Portal \(CSP\)](#). If you have added the Panorama serial number to the same CSP account on which you want to deploy Prisma Access, you can select the serial number of this Panorama appliance during installation.

Alternatively, if you have a licensed Panorama that you have not yet installed, you can select that Panorama during product activation; the installation process provides you with links to register and install Panorama. In either case, the activation process allows the Panorama appliance you select to manage Prisma Access, and you must make sure that the Panorama appliance is running the minimum software version.

Prisma Access 2.0 Innovation requires a Panorama appliance running the following minimum versions:

- 9.1.4 or a later PAN-OS version of 9.1.x (PAN-OS 10.0.3 required to activate and use PAN-OS 10.0 features)
- 10.0.3 or a later PAN-OS version of 10.0.x

If you use the [Enterprise DLP plugin](#) or [Explicit Proxy](#) with Prisma Access, a minimum Panorama version of 10.0.5 is required.



*Make a note of the serial number of the Panorama appliance; you use that serial number in a later step.*

---

## Hub Roles and Prisma Access Installation

During Prisma Access installation, Palo Alto Networks provides you the required roles on the [Hub](#) to activate Prisma Access, if those Hub roles are not already present. After you complete installation, you are assigned a [role](#) of Instance Admin. If you need additional roles on the Hub to perform system tasks, log in to the Hub, select **Settings > Access Management**, find the **Account Administrator** for your organization, and contact them to be assigned additional roles.

## Activate and Install Prisma Access

If you purchased Prisma Access (Panorama Managed) on or after November 17, 2020, complete the following steps to activate your Prisma Access licenses and download and install the Cloud Services plugin.

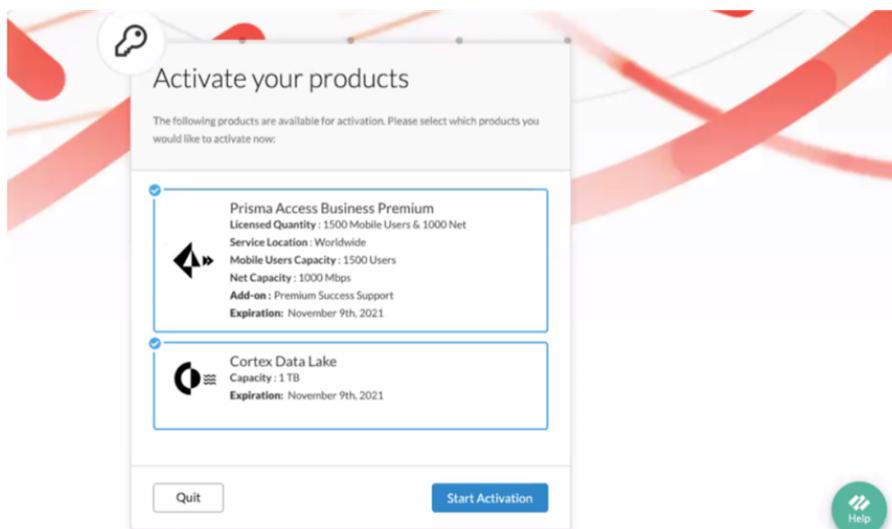
**STEP 1** | When you receive the activation email from Palo Alto Networks, click **Activate** to activate your products.

Select any of the links in the email to activate all of your licensed Prisma Access and Cortex Data Lake products. You will be prompted to sign in to the [Hub](#) if you are not signed in already.

**STEP 2** | Select the products you want to activate; then, click **Start Activation**.

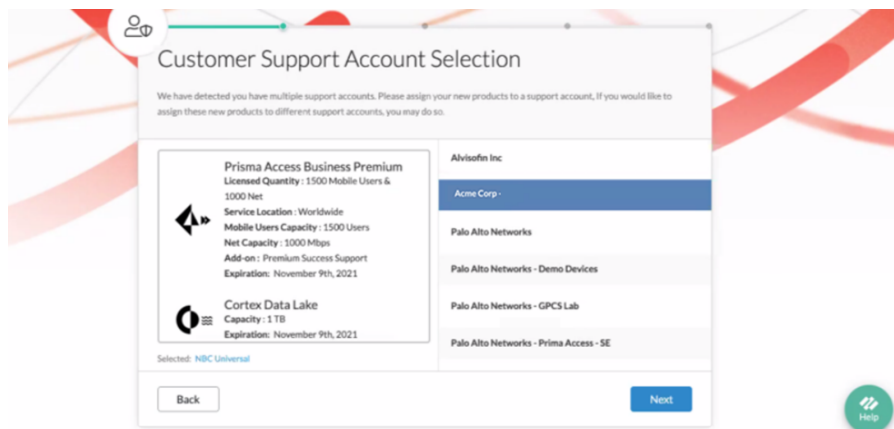
In most cases, activate all products that display; however, if you want to associate Prisma Access with a Cortex Data Lake you have already activated, deselect **Cortex Data Lake**.

If you have purchased the add-ons such as IoT or DLP, these products appear in the **Add-on** area.

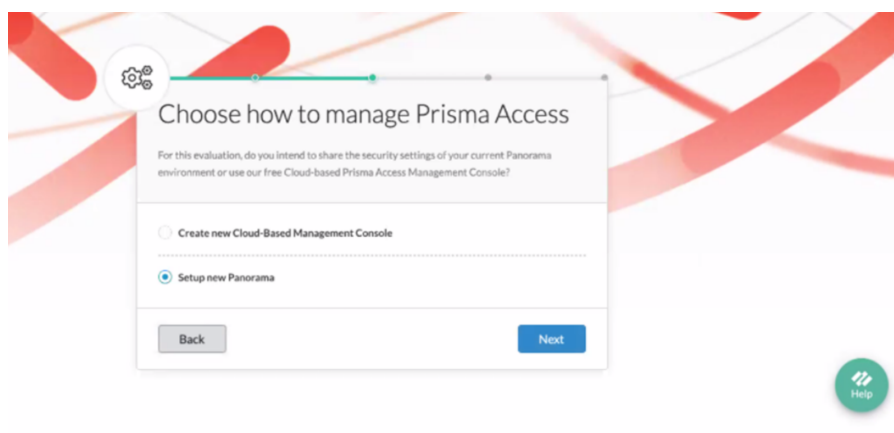


**STEP 3** | Assign the products you selected with a Customer Support Account; then, click **Next**.

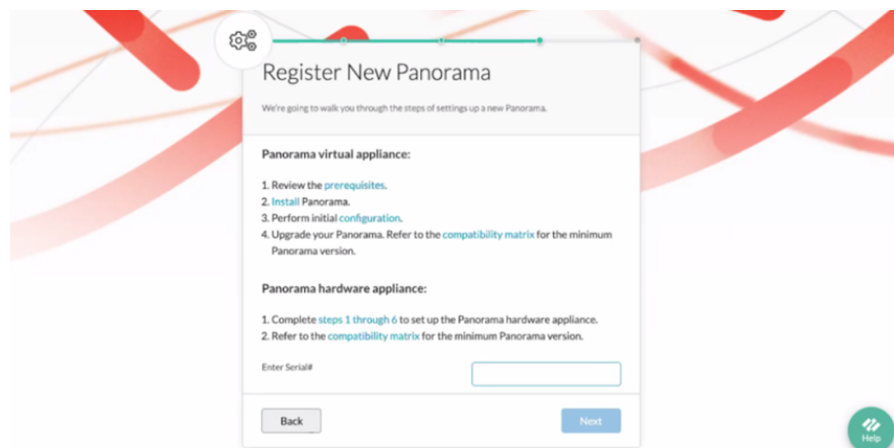
If you have multiple support accounts associated with your email, select the account to which you want to assign the products.



**STEP 4** | Choose the Panorama appliance by selecting **Setup new Panorama**.

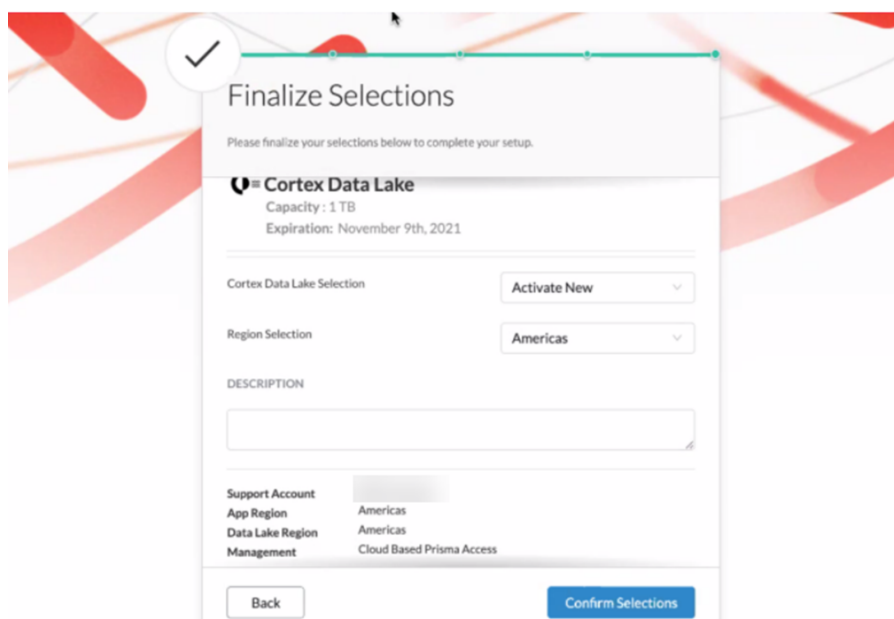


**STEP 5** | Follow the provided steps to register the new Panorama.



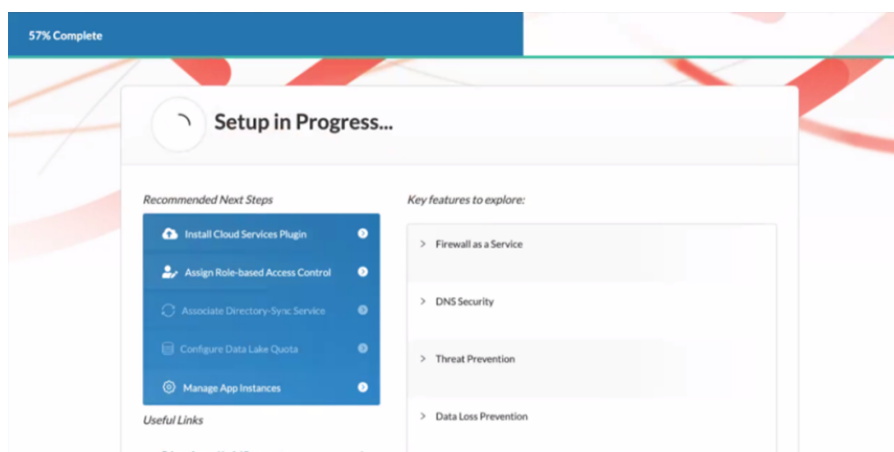
**STEP 6** | Choose the Cortex Data Lake options; then, click **Confirm Selections**.

- In the **Cortex Data Lake Selection** area, choose whether to activate a new Cortex Data Lake instance (**Activate New**), or select an existing Cortex Data Lake instance.
- In the **Region Selection** area, select a region for Cortex Data Lake.



The progress bar can appear to pause during product activation. Wait until the progress bar reaches 100%. The activation process takes approximately 20 minutes.

**STEP 7 |** When setup is complete, copy the one-time password (OTP). You use this when you verify your account on Panorama.



**STEP 8 |** Download and install the Cloud Services plugin.

See the [Palo Alto Networks Compatibility Matrix](#) for the Panorama versions that are supported with the Cloud Services plugin.

You can either download the plugin from the Customer Support Portal, or you can check for plugin updates directly from Panorama.

- To download and install the Cloud Services plugin by downloading it from the Customer Support Portal, complete the following steps.
  1. Log in to the [Customer Support Portal](#) and select **Software Updates > Panorama Integration Plugin**.
  2. Find the Cloud Services plugin in the Panorama Integration Plug In section and download it.





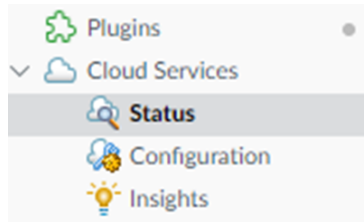
*Do not rename the plugin file or you will not be able to install it on Panorama.*

3. Log in to the Panorama Web Interface of the Panorama you licensed for use with the Prisma Access, select **Panorama > Plugins > Upload** and **Browse** for the plugin **File** that you downloaded from the CSP.
  4. **Install** the plugin.
- To download and install the 2.0 version of the Cloud Services plugin directly from Panorama, complete the following steps:
    1. Select **Panorama > Plugins** and click **Check Now** to display the latest Cloud Services plugin updates.

FILE NAME	VERSION
Name: cloud_services <ul style="list-style-type: none"> <li>cloud_services-</li> </ul>	

2. **Download** the plugin version you want to install.
3. After downloading the plugin, **Install** it.

Installing a newer version of the Cloud Services plugin overwrites the previously installed version. If you are installing the plugin for the first time, after you successfully install, Panorama refreshes and the Cloud Services menu displays on the **Panorama** tab.



### STEP 9 | Retrieve the Prisma Access license(s).

1. Select **Panorama > Licenses** and click **Retrieve license keys from license server**.
2. Verify that you have the licenses for the Prisma Access components you plan to use.

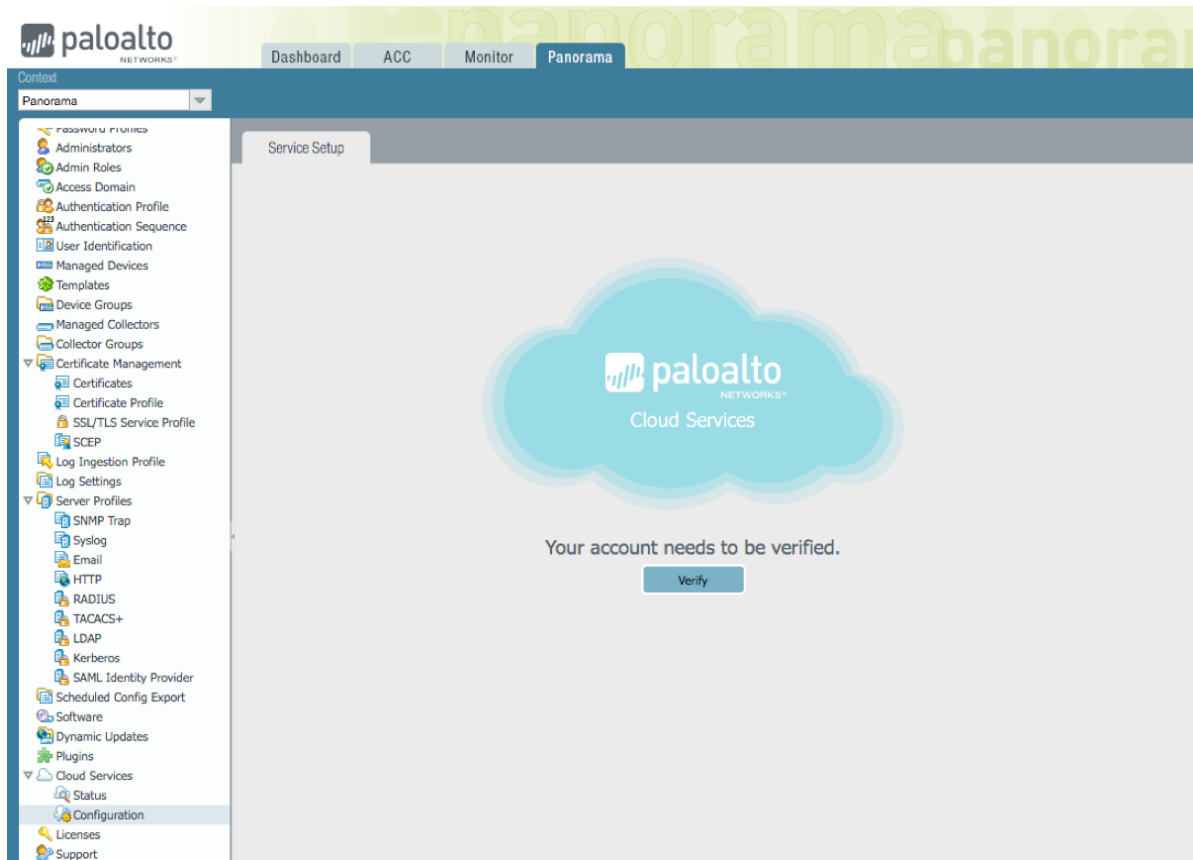
### STEP 10 | Verify your account.

When you try to use the Cloud Services plugin for the first time after installing it, you will be prompted to verify your account. This step ensures that the Panorama serial number is registered to use Prisma Access and enables a secure communication path between the Prisma Access components and Panorama.

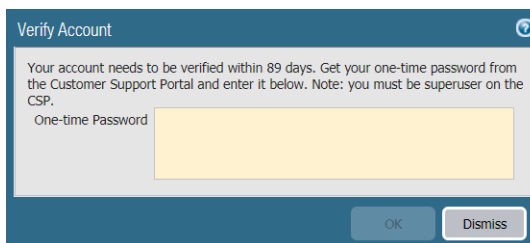


*You also have to re-verify your account every 3 months; complete these steps to re-verify the account.*

1. In Panorama, select **Panorama > Cloud Services > Configuration** and click **Verify**.  
If **Verify** is disabled, check that you have configured a DNS server and NTP server on **Panorama > Setup > Services**.



2. Paste the **One-time Password** you copied and click **OK**.

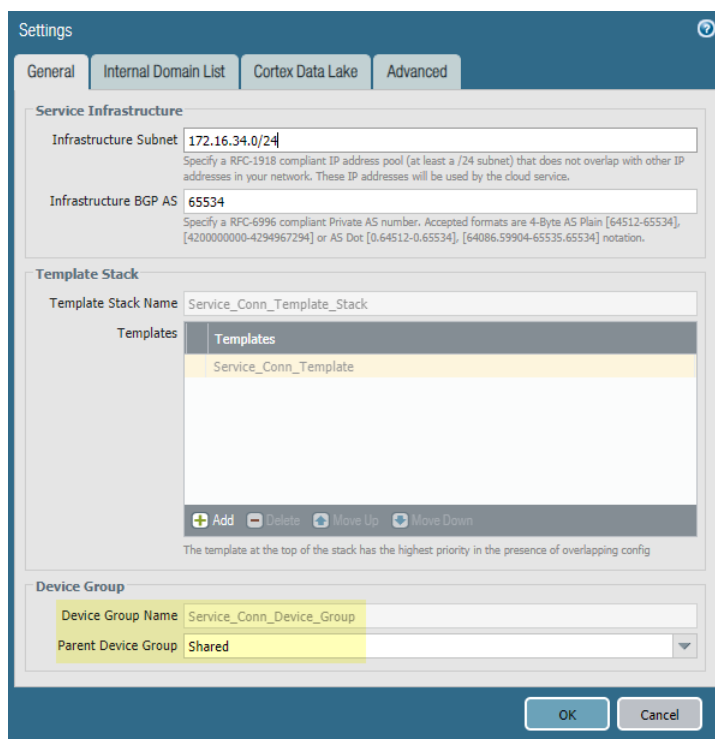


*You have ten minutes to enter the OTP before it expires.*

#### STEP 11 | Apply device group changes in the Prisma Access infrastructure.

Prisma Access moves all device groups under the **Shared** hierarchy. This step applies the device group changes to your configuration.

1. Select **Panorama > Cloud Services > Configuration > Service Setup**.
2. Click the gear icon to edit the **Settings**.
3. Make sure that **Service\_Conn\_Device\_Group** is selected as the **Device Group Name** and **Shared** is selected as the **Parent Device Group**.



4. Click **OK**.

Do not click **Cancel**, even if you did not make any changes to this page.

**STEP 12** | Continue to configure your Prisma Access deployment by [Enabling the Service Infrastructure](#).

---

# Transfer or Update Prisma Access Licenses

If you need to transfer your Prisma Access license from one Panorama appliance to another, or if you have an evaluation Prisma Access license and you purchase a production license, use this workflow to transfer or update your license.



*An evaluation license has the same capabilities as the Prisma Access Local Enterprise edition, including supporting a maximum of 5 locations and 2 service connections, and includes all the supported add-ons. After you purchase your Prisma Access production license, you must determine what is supported with your Prisma Access production license and deactivate the unsupported capabilities before you update your license from evaluation to production.*

*The number of locations and service connections for your production license depends on the license type; check your license details to see the maximum number of locations and service connections that are supported.*

*Evaluation licenses have every Prisma Access capability enabled. After you purchase your Prisma Access production license, you must determine what is supported [with your Prisma Access production license](#) and deactivate the unsupported capabilities before you update your license from evaluation to production.*

If you are upgrading from an evaluation to a paid license, do not proceed with this workflow until the order process is complete, the order has been fulfilled, and the support portal is showing the newly purchased cloud service licenses.

## Supported Update Paths

The procedure you use depends on the type of Prisma Access license you have. If you are upgrading from an evaluation to a paid Prisma Access license, the update path differs depending on the type of license your Panorama appliance has.

- If you are transferring a production (paid) Prisma Access license from one Panorama appliance to another, use the workflow in [Transfer or Update Prisma Access Licenses Between Panorama Appliances](#) to transfer the Prisma Access license.
- If you are upgrading from an evaluation Prisma Access license to a production Prisma Access license, use one of the following workflows to transfer the license:
  - If your Panorama is a production appliance with active, paid licenses, use the workflow in [Reset Your Prisma Access License](#) to update your licenses to the production service. We recommend using this update path because you do not have to migrate your existing configuration.
  - If your Panorama is an evaluation appliance, you need to transfer your Prisma Access license to a production appliance. Use the workflow in [Transfer or Update Prisma Access Licenses Between Panorama Appliances](#) to update your license to the production service.

The following table shows the supported license update methods based on the type of Panorama appliance used with the evaluation.

	Panorama used during evaluation					
	Production Panorama	Production Panorama in HA mode	Evaluation Panorama	Evaluation Panorama in HA mode	Panorama in Public / Private Cloud	Panorama Hardware
Conversion to Paid Service	Supported	Supported	Supported*	Supported*	Supported	Supported

\*Requires a license transfer that is initiated through the Customer Support Portal. All active cloud service licenses registered to your eval Panorama must be transferred at the same time. There is no support for transferring selective licenses.

## Reset Your Prisma Access License

Use this workflow if you need to modify one or more of your licenses; for example, if you update your Prisma Access license from an evaluation to a production version.



*If you are upgrading your Prisma Access license from evaluation to production, make sure that your Panorama appliance has active, paid licenses before starting this procedure. If your Panorama has an evaluation license, you need to [transfer the Prisma Access license to a Panorama with a production license](#).*

**STEP 1** | In the Panorama appliance, select **Panorama > Licenses**.

**STEP 2** | Make a note or take a screenshot of the licenses you have, the quantity of licenses, and the expiration date of each license.

**STEP 3** | Remove the license that you need to modify.

For example, if you are upgrading from an evaluation to a production license, remove the evaluation cloud service licenses you have installed.

1. Open a SSH console session to the Panorama appliance.
2. Enter the **delete license key** command, then press the **Tab** key to view all installed license keys.
3. Delete all Prisma Access license keys, including the license keys for Cortex Data Lake, Prisma Access for Users, Prisma Access for Networks, and Prisma Access for Clean Pipe, as applicable to your deployment.

The following is an example of the process:

```
admin-Panorama> delete license key [then click tab]
GlobalProtect_Cloud_Service_f_2017_11_07.key 2017/11/0712:32:51 0.3K
GlobalProtect_Cloud_Service_for_Mobile_Users_2017_11_07.key 2018/01/10
13:52:18 0.3K
GlobalProtect_Cloud_Service_for_Remote_Networks_2017_11_07.key 2018/01/10
13:52:18 0.3K
Logging_Service_2017_11_07.key 2018/01/10 13:52:18 0.3K

admin-Panorama> delete license key Logging_Service_2017_11_07.key
successfully removed Logging_Service_2017_11_07.key

admin-Panorama> delete license key
GlobalProtect_Cloud_Service_f_2017_11_07.key
```

```
successfully removed GlobalProtect_Cloud_Service_f_2017_11_07.key

admin-Panorama> delete license key
GlobalProtect_Cloud_Service_for_Remote_Networks_2017_11_07.key
successfully removed
GlobalProtect_Cloud_Service_for_Remote_Networks_2017_11_07.key

admin-Panorama> delete license key
GlobalProtect_Cloud_Service_for_Mobile_Users_2017_11_07.key
successfully removed
GlobalProtect_Cloud_Service_for_Mobile_Users_2017_11_07.key
```

**STEP 4** | From the Panorama administration console, select **Panorama > Licenses** and click **Retrieve license keys from license server**.

This step should refresh the licenses you already have, and the new licenses should reflect the new quantity you purchased and the new expiration date.

**STEP 5** | Delete any existing certificates using CLI from Panorama by entering the following command:

```
admin-Panorama> request plugins cloud_services panorama-certificate delete
```

**STEP 6** | Enter the `debug plugins cloud_services reset-endpoint` command to reset the Panorama appliance.

**STEP 7** | Create the new certificate with the new OTP by entering the following command, where **value** is the new OTP:

```
admin-Panorama> request plugins cloud_services panorama-certificate fetch
debug yes otp value
```

**STEP 8** | Complete the [one-time password \(OTP\) verification](#) procedure and verify the Panorama appliance.

**STEP 9** | In Panorama, verify that you can make configuration changes and can successfully [push the configuration to Prisma Access](#).

If the licenses do not update correctly, or if you are not able to make configuration changes after the refresh, contact Palo Alto Networks support.

## Transfer or Update Prisma Access Licenses Between Panorama Appliances

Use the following workflow if you need to transfer Prisma Access licenses from one Panorama appliance to another, for example:

- If you need to transfer production (paid) licenses from one Panorama appliance to another.
- If you are running an evaluation license on a Panorama appliance that also has an evaluation license. In this case, you must transfer the production Prisma Access license from an evaluation to a production Panorama appliance.

Prisma Access automatically preserves all instances and [public and loopback IP addresses](#) during the license transfer.

**STEP 1 | (Optional) Export a snapshot of your Panorama configuration** to a host external to Panorama or to an on-premise firewall.

While Prisma Access saves all its infrastructure settings, including public and loopback IP addresses, you need to transfer any Panorama-specific configuration to the new Panorama appliance. You can export your configuration after the license transfer process is complete, but we recommend exporting it before you transfer the licenses as a best practice.

**STEP 2 | Log in to the Palo Alto Networks Customer Support Portal.**

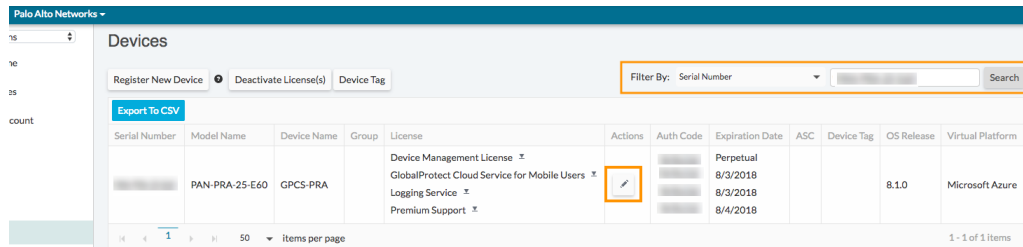
**STEP 3 | Select **Assets > Devices**.**

**STEP 4 | Find the production Panorama appliance to which you will be transferring the production Prisma Access plugin and complete these steps:**

1. Verify that it has an active support license.
2. Make a note of this serial number; you use it in a later step.

**STEP 5 | Search for the current Panorama appliance you are using to run Prisma Access by using the serial number.**

The model name should be in the format PAN-PRA-25-Exx.



**STEP 6 | Click the **Actions** icon for the current Panorama appliance.**

**STEP 7 | Select **Transfer Licenses** and choose the Panorama appliance to which you will be migrating.**

## Device Licenses ✕

### Device Licenses

Serial Number: [REDACTED]

Model: PAN-PRA-25-E60

Device Name: GPCS-PRA

Feature Name	Authorization Code	Expiration Date	Actions
Device Management License	[REDACTED]	Perpetual	⌵
Logging Service	[REDACTED]	08/03/2018	⌵
GlobalProtect Cloud Service for Mobile Users	[REDACTED]	08/03/2018	⌵
Premium Support	[REDACTED]	08/04/2018	⌵

### Activate Licenses

Activate Auth-Code

### Transfer Licenses

Transfer Cloud License

Panorama: - Panorama Select -  
- Panorama Select -

**STEP 8** | Review the EULA and click **Agree**, then click **Submit**.

**STEP 9** | Wait for a confirmation message in the Support Portal for a successful transfer.

**STEP 10** | After the successful transfer of licenses, login to the administration console of your production Panorama appliance.

**STEP 11** | Select **Panorama > Support** and verify that the Panorama appliance has a valid support license.

**STEP 12** | Click **Dashboard** and verify that the Panorama appliance is running the minimum supported software version. See [Prisma Access and Panorama Version Compatibility](#) for details.

**STEP 13** | Verify that the Panorama appliance is configured to use NTP by selecting **Panorama > Setup > Services > NTP** and setting a value, such as pool.ntp.org, for the NTP Server.

**STEP 14** | Install the [Cloud Services plugin](#).

**STEP 15** | Select **Panorama > Licenses** and click **Retrieve license keys from license server**.



---

This should refresh the screen with recently transferred Prisma Access and Cortex Data Lake licenses you purchased. If the cloud service licenses do not appear, contact Palo Alto Networks Support for assistance.

**STEP 16** | Complete the [one-time password \(OTP\) verification](#) procedure and verify the Panorama appliance.

**STEP 17** | Migrate the configuration from the previous Panorama appliance to the current Panorama appliance.

- If the production Panorama appliance is completely new, [export the configuration](#) from the Panorama appliance you used during the evaluation (if you have not done so already) and [import it](#) to this Panorama appliance.
- If this is the Panorama appliance that you have been using to manage your existing VMs and devices, [load a partial configuration](#) to this Panorama appliance.

You can now use this Panorama appliance to configure and manage Prisma Access.

---

# Configure Panorama Appliances in High Availability for Prisma Access

Deploying Panorama appliances in a high availability (HA) configuration provides redundancy in case of a system or network failure and ensures that you have continuous connectivity to Prisma Access. In an HA configuration, one Panorama appliance peer is the active-primary and the other is the passive-secondary. In the event of a failover, the secondary peer becomes active and takes over the role of managing Prisma Access.

- [HA Prerequisites](#)
- [Configure HA](#)

## HA Prerequisites

To simplify the HA set up, configure the Panorama appliances in HA after you purchase Prisma Access and Cortex Data Lake auth codes and components and associate the serial number of the primary Panorama appliance on which you plan to install the Cloud Services plugin with the auth codes, but before you [Activate and Install Prisma Access \(Panorama Managed\)](#). However, you can also use this process to configure existing Panorama appliances that already have the plugin installed.

Whether you are just getting started with a new pair of Panorama appliances, or you have already set up your standalone Panorama appliance and completed the licensing and installation procedures, make sure to check the prerequisites before you enable HA:

- ❑ You must register the Panorama appliance HA peers to the same customer account on the [Customer Support Portal \(CSP\)](#).
- ❑ The Panorama appliance peers must be of the same form factor (hardware appliances of the same model or identical virtual appliances) and same OS version and must have the same set of licenses. The premium support license is required for Prisma Access and Cortex Data Lake.
- ❑ The serial number of the primary Panorama appliance is tied to your Prisma Access and Cortex Data Lake auth codes. If you have installed and set up the plugin on a standalone Panorama appliance, ensure that you use that Panorama appliance as the primary peer. If you need to assign this standalone peer as the secondary Panorama appliance, contact Palo Alto Networks support for assistance with transferring the license to the primary Panorama appliance peer before you continue.

## Configure HA

Set up your Panorama appliances in an HA configuration.

### STEP 1 | Set Up HA on Panorama.

Set the primary Panorama appliance as **Primary** and the secondary Panorama appliance as **Secondary** and be sure that the serial number of your primary Panorama appliance is tied to your Prisma Access and Cortex Data Lake auth codes.

### STEP 2 | Make sure that the primary (active) and secondary (passive) Panorama appliances are synchronized and that the HA link state between them is up.

1. Access the **Dashboard** on the primary Panorama appliance and select **Widgets > System > High Availability** to display the HA widget.
2. **Sync to peer**, click **Yes**, and wait for the **Running Config** to display **Synchronized**.

3. Make sure that the **Local** peer is **active**.
4. Access the **Dashboard** on the passive Panorama appliance and select **Widgets > System > High Availability** to display the HA widget.
5. Verify that the **Running Config** displays **Synchronized**.
6. Make sure that the **Local** peer is **passive**.

**STEP 3 |** Install the Prisma Access components on the primary Panorama appliance.

1. Log in to the primary Panorama appliance and select **Panorama > Licenses**.
2. Click **Retrieve the license keys from license server**.
3. [Activate and Install Prisma Access \(Panorama Managed\)](#), including generating a one-time password (OTP) and verifying your account.

**STEP 4 |** On the primary Panorama appliance, [Access the CLI](#) and enter the following operational command:

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

**STEP 5 |** Check that HA is enabled.

1. Find the following text in the log output, where *X* is the serial number of the primary Panorama appliance and *Y* is the serial number of the secondary Panorama appliance:

```
2017-11-06 15:14:07.790 -0800 INFO: [hainfo] Sending update to CSP for
HA peer serial information to https://updates.paloaltonetworks.com/
licensesvc/licenseservice.asmx/PanoramaHAInfo (https://
updates.paloaltonetworks.com/licensesvc/licenseservice.asmx/
PanoramaHAInfo)

2017-11-06 15:14:07.791 -0800 INFO: [hainfo] Data string is
primarypanoramasn=<varname>X</varname> &secondarypanoramasn=<varname>Y</
varname>

2017-11-06 15:14:17.595 -0800 INFO: [hainfo] HTTP_CODE 200, RESPONSE:
<?xml version="1.0" encoding="utf-8"?> <PanoramaHA xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance (http://www.w3.org/2001/XMLSchema-
instance)" xmlns:xsd="http://www.w3.org/2001/XMLSchema (http://
www.w3.org/2001/XMLSchema)" xmlns="http://www.paloaltonetworks.com/
(http://www.paloaltonetworks.com/)"> <success>true</success>
</PanoramaHA>

2017-11-06 15:14:17.596 -0800 INFO: [hainfo] Cached HA Peer's serial
number <varname>Y</varname>
```

2. Log in to the [Customer Support Portal \(CSP\)](#) and select **Assets > Cloud Services** to verify that both Panorama peers are tied to your Prisma Access and Cortex Data Lake licenses.
3. Check the fields for the primary and secondary Panorama appliance.

The Auth Code, Model Name, License Description, and Expiration Date fields should be the same for the primary and secondary Panorama appliance, because Palo Alto Networks has associated the Prisma Access license automatically to the secondary Panorama appliance.

**STEP 6 |** Log in to the secondary Panorama appliance and [Activate and Install Prisma Access \(Panorama Managed\)](#).

When you log in to the [Customer Support Portal \(CSP\)](#) to generate the OTP, make sure that you specify the serial number for the secondary Panorama appliance.

**STEP 7 |** Commit your changes on the primary and secondary Panorama appliance.

- 
1. **Commit** > **Commit and Push** your changes.
  2. Click **OK** and **Push**.

**STEP 8** | Verify that the primary and secondary Panorama appliances are still in a synchronized state.

# Prepare the Prisma Access Infrastructure and Service Connections

Use the sections in the following chapter to plan and begin configuration of your Prisma Access deployment.

- > Set Up Prisma Access
- > Plan the Service Infrastructure and Service Connections
- > Configure the Service Infrastructure
- > Create a Service Connection to Allow Access to Your Corporate Resources
- > Create a Service Connection to Enable Access between Mobile Users and Remote Networks
- > Deployment Progress and Status
- > Use Traffic Steering to Forward Internet-Bound Traffic to Service Connections
- > How BGP Advertises Mobile User IP Address Pools for Service Connections and Remote Network Connections
- > Routing Preferences for Service Connection Traffic
- > Create a High-Bandwidth Network Using Multiple Service Connections
- > List of Prisma Access Locations



---

# Set Up Prisma Access

The following sections provide you with the summary steps that you take to install and configure Prisma Access and information about proxy server support between Panorama, Prisma Access, and Cortex Data Lake.

- [Prisma Access Onboarding and Configuration Workflow](#)
- [Proxy Support for Prisma Access and Cortex Data Lake](#)

## Prisma Access Onboarding and Configuration Workflow

The following workflow provides you with the summary steps that you take to install and configure Prisma Access



*If you are setting up a deployment that includes multiple instances of Prisma Access on a single Panorama (multi-tenancy), see [Manage Multiple Tenants in Prisma Access](#). Most organizations do not have a need to create and manage multiple tenants.*

**STEP 1 |** Add the following URLs and ports to an allow list on any security appliance that you use with the Panorama appliance that manages Prisma Access.

In addition, if your Panorama appliance uses a [proxy server](#) (**Panorama > Setup > Service > Proxy Server**), or if you use SSL forward proxy with Prisma Access, be sure to add the following URLs and ports to an allow list on the proxy or proxy server.

- [api.gpcloudservice.com](#) (for Prisma Access)
- [api.paloaltonetworks.com](#) (for Prisma Access)
- [apitrusted.paloaltonetworks.com](#) (for Prisma Access)
- The [FQDNs and ports required for Cortex Data Lake](#)

**STEP 2 |** Add the [ports used by Panorama](#) to allow lists in your network.

**STEP 3 |** [Identify your license requirements](#); then [Activate and Install the Prisma Access Components](#).

**STEP 4 |** Import your existing Panorama configuration to Prisma Access, or create new [templates](#) and [device groups](#) to begin configuration of Prisma Access.

In order to push configuration—such as security policy, authentication policy, server profiles, security profiles, address objects, and application groups—to Prisma Access, you must either create new templates and device groups with the configuration settings you want to push to Prisma Access, or leverage your existing device groups and templates by adding them to the template stacks and device group hierarchies that get created when you onboard the service.

Configuration is simplified in Prisma Access because you do not have to configure any of the infrastructure settings, such as interfaces and routing protocols. This configuration is automated and pushed from Panorama in the templates and device groups that the service creates automatically. You can configure any infrastructure settings that are required by the service, such as settings required to create IPsec VPN tunnels to the IPsec-capable devices at your remote network locations, directly from the plugin. Optionally, you can add templates and device group hierarchies to the configuration to simplify the service setup.

To simplify the service setup, create or import the [templates](#) and [device groups](#) you need before you begin the setup tasks for using Prisma Access.

---

When creating templates and device groups for Prisma Access, you do not need to assign managed devices to it. Instead, you will add them to the template stacks and device group hierarchies created by the service. Do not add any of the templates or device groups created by Prisma Access to any other template stacks or device groups.



Also note that some settings that are available in a non-Prisma Access template or device group may not be supported in Prisma Access. See [What Features Does Prisma Access Support?](#) for a list of supported features.

**STEP 5 |** Enable the service infrastructure and service connections that allows communication between Prisma Access elements.

1. [Plan to enable the service infrastructure and service connections.](#)
2. [Enable the service infrastructure.](#)
3. Create a service connection [to allow access to your corporate resources.](#)

If you don't require access to your corporate resources, you should still create a service connection [to enable access between mobile users and remote networks.](#)

**STEP 6 |** [Plan To Deploy Prisma Access for Mobile Users](#) and [Secure Mobile Users With GlobalProtect](#), if required for your deployment.

We recommend using local authentication as a first step to verify that the service is set up and your users have internet access. You can later switch to using your corporate authentication methods.

1. [Secure Mobile Users With GlobalProtect.](#)
2. Configure zones for mobile users.
  1. Create two zones in the Mobile User Template. For example, Mobile-Users and Internet.
  2. [Map the zones.](#) You should map any zone that is not Prisma Access connected users or HQ or branch offices to Untrust.

Under **Panorama > Cloud Services > Configuration > Mobile Users**, map Internet to Untrust; Mobile-Users to Trust.

3. Configure Security policies for the device group.

To create a Security policy to allow traffic to the Internet, select the **Mobile\_User\_Device\_Group Policies > Security > Prerules > Add** a rule. For example: Mobile-Users to Internet.
4. Commit and push your changes to get started with the service.
  1. **Commit** locally on Panorama.
  2. **Commit and Push** to Prisma Access.
  3. Select **Panorama > Cloud Services > Status > Monitor > Mobile Users** to view the **Status** and verify that you can ping the Portal FQDN.
5. Validate that Prisma Access is securing Internet traffic for mobile users.
  1. [Download and install the GlobalProtect app.](#)
  2. Use the app to connect to the portal as a mobile user (local user).
  3. Browse to a few websites on the internet and check the traffic logs on Panorama.

**STEP 7 |** [Plan, create, and configure](#) remote network connections.

1. Add one or more remote networks to Prisma Access.

You can onboard one location and then add additional locations using the bulk import capability.

2. Create a Security policy rule to allow traffic from the remote networks to HQ (For example: Trust to Trust).



3. Validate the connectivity between the service connection, remote network connection, and mobile users.

**STEP 8 |** [Retrieve the IP Addresses for Prisma Access](#) and [Retrieve Public and Egress IP Addresses for Mobile User Deployments](#).

You add these addresses to an allow list on your organization’s network to limit inbound access to your enterprise network and applications.

**STEP 9 |** (Optional) Change the authentication method from local authentication to your organization’s authentication method.

1. Create an authentication profile that meets your organization’s requirements (LDAP, RADIUS, etc).
2. If your organization uses an on-premises authentication server such as RADIUS or Active Directory, add the IP addresses that Prisma Access uses as its source IP address for internal requests ([Prisma Access Infrastructure IP Addresses](#)) to allow lists in your network, or allow the IP addresses of the entire Infrastructure Subnet (Prisma Access takes the loopback IP address from this subnet).
3. Update the Authentication Profile for the Prisma Access portal and gateway to use this new authentication profile.

**STEP 10 |** (Optional) Forward logs from Cortex Data Lake to an external Syslog receiver by [setting up the Log Forwarding app](#).

## Proxy Support for Prisma Access and Cortex Data Lake

If you have deployed a proxy server between Panorama, the Prisma Access infrastructure, and Cortex Data Lake, refer to the following table for details on the expected behavior:

Functionality	Support through a Proxy Server that does not perform SSL Decryption	Support through a Proxy Server that performs SSL Decryption
<b>Initial onboarding to Cortex Data Lake with Certificate Revocation Status checks using OCSP</b>	Supported	Only pass-through proxies are supported; any proxy using SSL decryption is not supported.
<b>Panorama Queries to Cortex Data Lake for Reports and Logs</b>	<p>If the proxy server is the default route on Panorama, you cannot view the data on the ACC and <b>Monitor &gt; Logs</b> pages.</p> <p>You can view data on the ACC and <b>Monitor &gt; Logs</b> pages if Panorama has an alternate route to the Cortex Data Lake and you can bypass the proxy server.</p>	

# Plan the Service Infrastructure and Service Connections

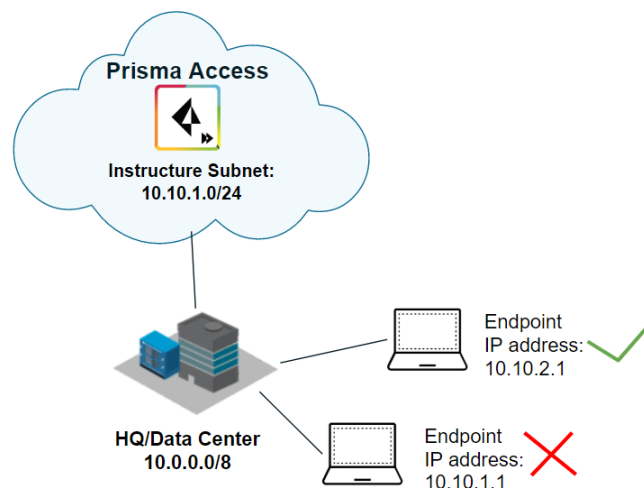
## Plan the Service Infrastructure

To [Enable the Service Infrastructure](#) in the cloud for your remote network locations and mobile users, you must provide a subnet that Prisma Access uses to establish a network infrastructure between your remote network locations, mobile users, and service connections to your headquarters/data center (if applicable). The IP addresses in this subnet also enable Prisma Access to determine the service routes for services such as LDAP, DNS, or SCEP, as well as enable other inter-service communication. Because a large number of IP addresses will be required to set up the infrastructure, you must use a /24 subnet (for example, 172.16.55.0/24) at a minimum. This subnetwork will be an extension to your existing network or with the IP address pools you assign for Prisma Access for users. If you have a large number of mobile users, branch offices, or both, provide a larger infrastructure subnet.

Use the following recommendations and requirements when adding an infrastructure subnet:

- You can assign Prisma Access an infrastructure subnet from an existing supernet in your organization's IP address pool, but do not assign any of the IP addresses from the infrastructure subnet for any other use in your existing network.

The following example shows a Prisma Access infrastructure subnet, 10.10.1.0/24, that you assigned from an existing supernet, 10.0.0.0/8. After you assign 10.10.1.0/24 as the infrastructure subnet, your organization cannot use any IP addresses from that subnet. For example, you can assign 10.10.2.1 to an endpoint, but 10.10.1.1 is not allowed because that IP address is part of the infrastructure subnet.



- If you create a new subnet for the infrastructure subnet, use a subnet that does not overlap with other IP addresses you use internally.
- We recommend using an RFC 1918-compliant subnet. While the use of non-RFC 1918-compliant (public) IP addresses is supported, we do not recommend it, because of possible conflicts with internet public IP address space.
- Do not specify any subnets that overlap with 169.254.169.253, 169.254.169.254, and the 100.64.0.0/10 subnet range because Prisma Access reserves those IP addresses and subnets for its internal use.

- 
- The subnet cannot overlap with the IP address pools you plan to use for the address pools you assign for your mobile users deployment.
  - Because the service infrastructure can be very large, you must designate a /24 subnet at a minimum.

### Service Connection Overview

We recommend always creating a service connection, because it allows Prisma Access to perform the following tasks:

- A service connection allows access to the resources in your HQ or data center.

For example, if your security policy requires user authentication using an on-premises authentication service, such as your Active Directory, you will need to enable Prisma Access to access the corporate location where the service resides (and set up a service account that the service can use to access it). Similarly, if you have corporate resources that your remote networks and mobile users will need to access, you must enable Prisma Access to access the corresponding corporate network.

If you create service connections for this reason, you should [plan for the service connections](#) before implementing them.

- A service connection allows remote networks and mobile users to communicate with each other.

Even if you don't need access to your HQ or data center, you might have a need to allow your mobile users to access your remote network locations. In this case, you can [create a service connection with placeholder values](#). This is required because, while all remote network connections are fully meshed, mobile users connect to remote networks using the service connection in a hub-and-spoke network. For this reason, you might also create a service connection with placeholder values if your existing service connection is not in an ideal geographical location.

The number of service connections you receive depends on your Prisma Access license.

- If you have a ZTNA or Enterprise license, you receive two service connections if you have a Local edition license and five service connections if you have a Worldwide edition license.
- If you [manage multiple tenants](#) and have a ZTNA or Enterprise license, the number of tenants per tenant depends on the number of units you allocate per tenant.
  - If you have a Global license and allocate at least 1,000 units for a tenant, you can allocate a maximum of five service connections for that tenant.
  - If you have a Global license and allocate between 200 and 999 units for a tenant, you can allocate a maximum of two service connections for that tenant (the same as the number of connections for a Local deployment).
  - If you have a Local license, you can allocate a maximum of two service connections per tenant, regardless of the number of units you allocate past the minimum of 200.

See [Multitenancy Configuration Overview](#) for more information about allocating units for tenants and how units correspond to bandwidth (for remote network deployments) or mobile users (for mobile user deployments).



*While each service connection provides approximately 1 Gbps of throughput, the actual throughput is dependent on several factors, including:*

- *Traffic mix (for example, frame size)*
- *Latency and packet loss between the service connection and the headquarters location or data center*
- *Service provider performance limits*
- *Customer termination device performance limits*

- *Other customer data center traffic*

In order for Prisma Access to route users to the resources they need, you must provide the routes to the resources. You can do this in one or more of the following ways:

- Define a static route to each subnetwork or specific resource that you want your users to be able to access.
- Configure BGP between your service connection locations and Prisma Access.
- Use a combination of both methods.

If you configure both static routes and enable BGP, the static routes will take precedence. While it might be convenient to use static routes if you have just a few subnetworks or resources you want to allow access to, in a large data center/HQ environment where you have routes that change dynamically, BGP will enable you to scale easier. Dynamic routing also provides redundancy for your service connections. If one service connection tunnel is down, BGP can dynamically route mobile user and remote network traffic over the operational service connection tunnel.

### Plan the Service Connections

If you use the service connection to access information from your headquarters or data center, gather the following information for each of your HQ/data center sites that you want the cloud service to be able to connect to:



*If you are creating a service connection to allow mobile users access to remote network locations, you do not need this information.*

- IPsec-capable firewall, router, or SD-WAN device connection.
- IPsec settings for terminating the primary VPN tunnel from Prisma Access to the IPsec-capable device on your corporate network.
- IPsec settings for terminating the secondary VPN tunnel from Prisma Access to the IPsec-capable device on your corporate network.



*If you have an existing template that contains [IPsec tunnel](#), [Tunnel Monitoring](#), and [IPsec Crypto Profile](#) configurations, you can add that template to the template stack to simplify the process of creating the IPsec tunnels. Or, you can edit the `Service_Conn_Template` that gets created automatically and create the IPsec configurations required to create the IPsec tunnel back to the corporate site. Prisma Access also provides you with a set of [predefined IPsec templates](#) for some commonly-used network devices, and a generic template for any device that is not included in the predefined templates.*

- List of IP subnetworks at the site.
- List of internal domains that the cloud service will need to be able to resolve.
- IP address of a node at your network's site to which Prisma Access can send ICMP ping requests for IPsec tunnel monitoring.

Make sure that this address is reachable by ICMP from the entire Prisma Access infrastructure subnet.

- Service account for your authentication service, if required for access.
- Network reachability settings for the service infrastructure subnet.

We recommend that you make the entire service infrastructure subnet reachable from the HQ or Data Center site. Prisma Access uses IP addresses for all control plane traffic, including tunnel monitoring, LDAP, User-ID, and so on from this subnet.

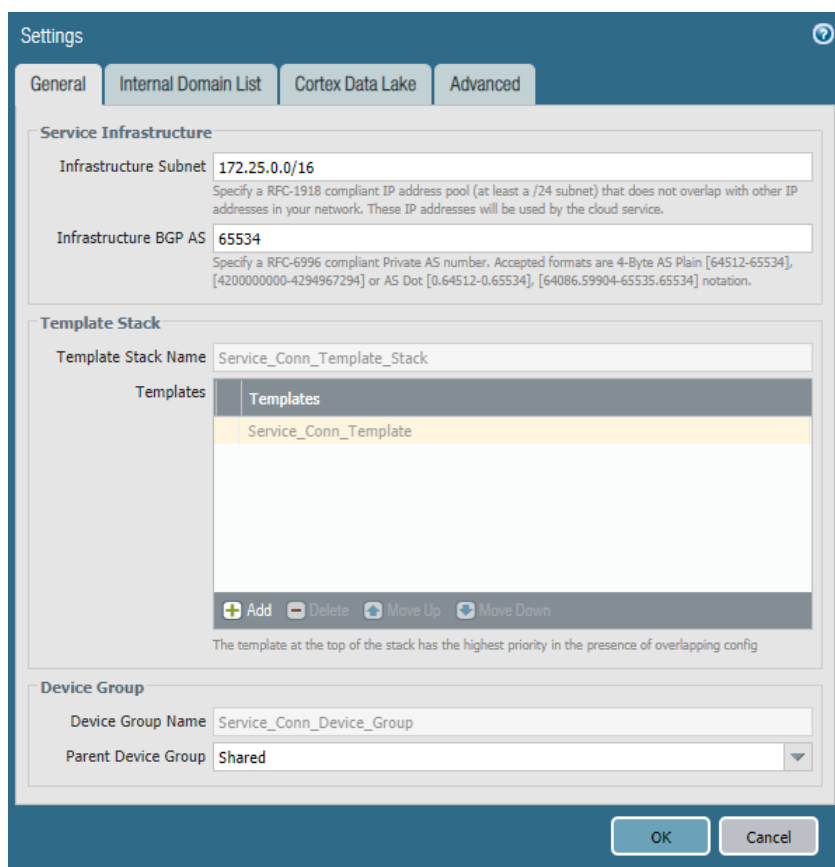
---

Traffic over the service connections does not count towards the remote network bandwidth pool that you purchased.

# Configure the Service Infrastructure

Before you can begin setting up Prisma Access to secure your remote networks and/or mobile users, you must configure an infrastructure subnet, which Prisma Access will use to create the network backbone for communication between your service connections, remote networks, and mobile users, as well as with the corporate networks you plan to connect to Prisma Access over service connections. Because a large number of IP addresses will be required to set up the infrastructure, you must use a /24 subnet (for example, 172.16.55.0/24) at a minimum. See [Plan the Service Infrastructure and Service Connections](#) for the requirements and guidelines to use when assigning an infrastructure subnet.

**STEP 1** | Select **Panorama > Cloud Services > Configuration > Service Setup** and click the gear icon to edit the Settings.



**STEP 2** | On the **General** tab, specify an **Infrastructure Subnet**, for example, 172.16.55.0/24.

See [Plan the Service Infrastructure and Service Connections](#) for the requirements and guidelines to use when assigning an infrastructure subnet.

**STEP 3** | Enter the **Infrastructure BGP AS** you want to use within the Prisma Access infrastructure. If you want to use dynamic routing to enable Prisma Access to dynamically discover routes to resources on your remote networks and HQ/data center locations, specify the autonomous system (AS) number. If you do not supply an AS number, the default AS number 65534 will be used.

**STEP 4 | (Optional) Add one or more [templates](#) to the predefined template stack, *Service\_Conn\_Template\_Stack*.**

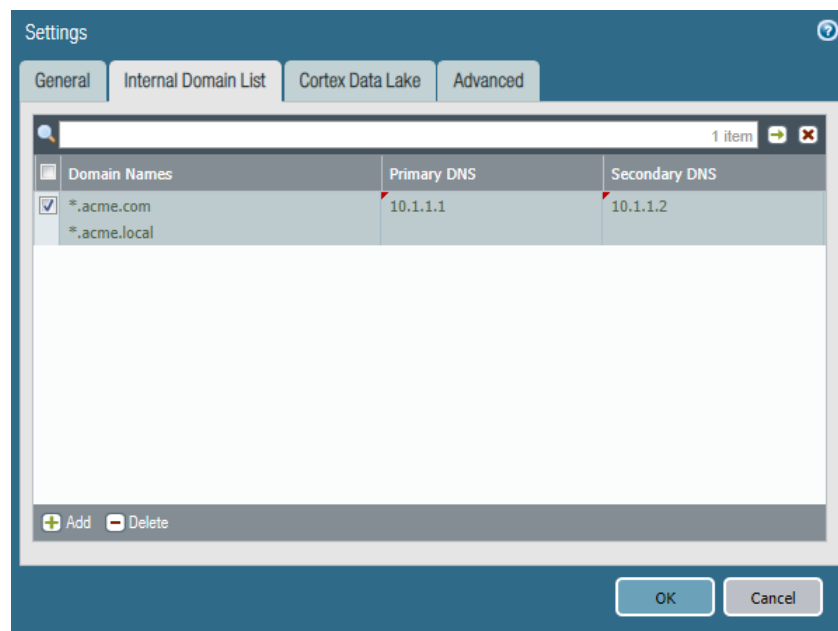
The templates you add here can help simplify the process of adding new service connections. For example, if you add a template containing existing IPsec configuration settings, such as [IPsec tunnel](#), [Tunnel Monitoring](#), and [IPsec Crypto Profile](#) configurations, you can select these configurations when defining the tunnel settings for each service connection rather than having to create the tunnel configuration from scratch. You can optionally edit the predefined *Service\_Conn\_Template* with tunnel settings that you can leverage when creating the tunnels from Prisma Access to your corporate network sites.

**STEP 5 | Enable Prisma Access to resolve your internal domains.**

Use this step if you need Prisma Access to be able to resolve your internal domains to access services, such as LDAP servers, on your corporate network via service connections. For example, if you want a DNS lookup for your corporate domain to go exclusively to the corporate DNS server, specify the corporate domain and the corporate DNS servers here.

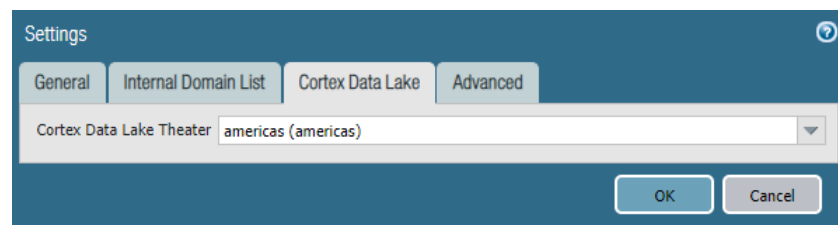
1. Select the **Internal Domain List** tab.
2. **Add the Domain Names, Primary DNS, and Secondary DNS** servers that the cloud service can use to resolve your internal domain names.

You can use a wildcard (\*) in front of the domains in the domain list, for example \*.acme.local or \*.acme.com.



**STEP 6 | Enable Cortex Data Lake.**

1. Select the **Cortex Data Lake** tab.
2. Select a **Cortex Data Lake Theater** and click **OK**.



3. Configure the device groups you are using to push settings to Prisma Access with a [Log Forwarding profile](#) that forwards the desired log types to **Panorama/Cortex Data Lake**.

The Cloud Services plugin automatically adds the following Log Settings (**Device > Log Settings**) after a new installation or when removing non-Prisma Access templates from a Prisma Access template stack:

- Log Settings for System logs (**system-gpcs-default**), User-ID logs (**userid-gpcs-default**), HIP Match logs (**hipmatch-gpcs-default**), and GlobalProtect logs (**gp-prismaaccess-default**) are added to the `Mobile_User_Template`.
- Log Settings for System logs (**system-gpcs-default**), User-ID logs (**userid-gpcs-default**), and GlobalProtect logs (**gp-prismaaccess-default**) are added to the `Remote_Network_Template`.
- Log Settings for System logs (**system-gpcs-default**) and GlobalProtect logs (**gp-prismaaccess-default**) are added to the `Service_Conn_Template`.

These Log Setting configurations automatically forward System, User-ID, HIP Match, and GlobalProtect logs to Cortex Data Lake.

To apply log setting changes, perform the following steps, then commit and push your changes:

- To apply the log setting to the mobile user template, select **Panorama > Cloud Services > Configuration > Mobile Users**, click the gear icon to edit the settings, and click OK.
- To apply the log setting to the remote network template, select **Panorama > Cloud Services > Configuration > Remote Networks**, click the gear icon to edit the settings, and click OK.
- To apply the log setting to the service connection template, select **Panorama > Cloud Services > Configuration > Service Setup**, click the gear icon to edit the settings, and click OK.



See [Add Log Settings to Prisma Access \(Panorama Managed\)](#) for a video that describes the log settings process.

The way you enable log forwarding for other log types depends on the type. For logs that are generated based on a policy match, use a log forwarding profile. See the [Cortex Data Lake Getting Started Guide](#) for more information.

## STEP 7 | (Optional) Change the routing preferences and enable HIP redistribution.

1. Specify the **Routing Preference** to use with service connections.

You can specify network preferences to use either your organization's network, or the Prisma Access network, to process the service connection traffic.

- **Default**—Prisma Access uses default routing in its internal network.
- **Hot potato routing**—Prisma Access hands off service connection traffic to your organization's WAN as quickly as possible.



*Changing the Prisma Access service connection routing method requires a thorough understanding of your organization's topology and routing devices, along with an understanding of how Prisma Access routing works. We recommend that you read the [Routing Preferences for Service Connection Traffic](#) section carefully before changing the routing method from the default setting.*

2. **Enable HIP Redistribution** to have Prisma Access use service connections to redistribute HIP information from mobile users and users at remote networks.

See [Redistribute HIP Information with Prisma Access](#) for more information about enabling HIP redistribution.

## STEP 8 | (Optional) Automatically add a host-specific static route to the static IKE gateway peer for the IPSec tunnel on the Remote Network security processing node (SPN) and Service Connection



corporate access node (CAN) by selecting **Enable automatic IKE peer host routes for Remote Networks and Service Connections**.

After you make this selection, IPSec tunnel packets to the static IKE gateways will be routed over the internet.

**STEP 9 | (Optional) Specify Outbound Routes for the Service (Max 10)** by adding up to 10 prefixes for which Prisma Access adds static routes on all SPNs and CANs. Prisma Access then routes traffic to these prefixes over the internet.

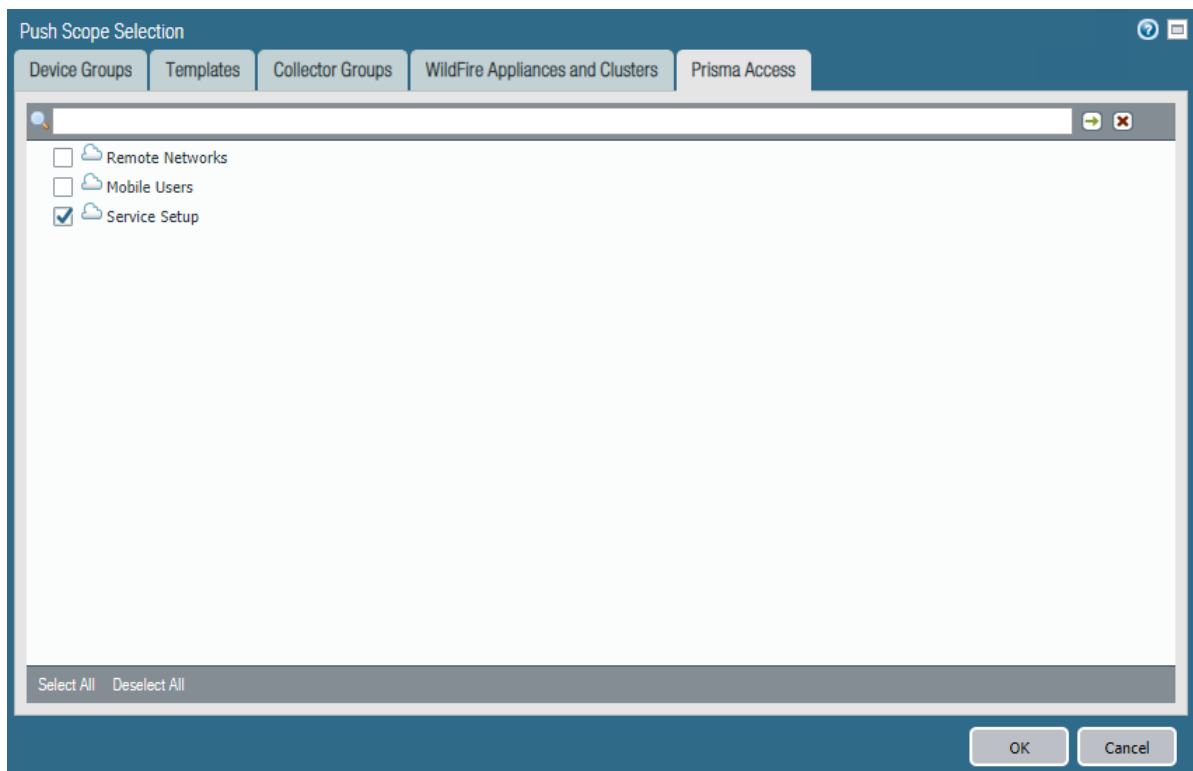
The screenshot shows the 'Settings' dialog box with the 'Advanced' tab selected. The 'Routing' section is expanded, showing a 'Routing Preference' dropdown set to 'Default'. Below it is a checkbox for 'Enable automatic IKE peer host routes for Remote Networks and Service Connections', which is currently unchecked. A search bar above a list area shows '0 items'. The list area is titled 'OUTBOUND ROUTES FOR THE SERVICE(MAX. 10)'. At the bottom of the list area are '+ Add' and '- Delete' buttons. Below the Routing section is the 'HIP Redistribution' section, which has a checkbox for 'Enable HIP Redistribution' that is also unchecked. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

**STEP 10 |** Click **OK** to save the Service Setup settings.

**STEP 11 |** Commit all your changes to Panorama and push the configuration changes to Prisma Access.

1. Click **Commit > Commit to Panorama**.
2. Click **Commit > Push to Devices** and click **Edit Selections**.
3. On the **Prisma Access** tab, make sure **Service setup** is selected and then click **OK**.

Prisma Access should automatically select the components that need to be committed.



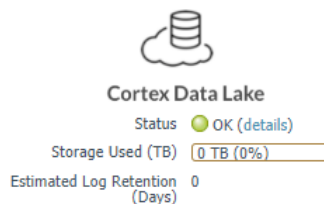
4. Click **Push**.



*If there is a Palo Alto Networks next-generation firewall between the Panorama appliance and the internet, you must add a security policy rule on the firewall to allow the paloalto-logging-service and paloalto-shared-services App-IDs from the Panorama appliance to the internet. These applications allow SSL-secured communication to Prisma Access and to Cortex Data Lake that the Panorama appliance uses to query logs. If the Panorama appliance is behind a legacy Layer 4 firewall, permit ports 443 and 444 outbound from the Panorama to allow this traffic from the Panorama. Note that opening layer 4 ports instead of using Palo Alto Networks App-IDs is less secure and not recommended.*

**STEP 12** | Verify that Prisma Access is successfully connected to Cortex Data Lake.

1. Select **Panorama > Cloud Services > Status > Status > Cortex Data Lake** and verify that the Status is **OK**.



If the status is **Error**, click the details link to view any errors.

**STEP 13** | Continue setting up Prisma Access:

- [Create a Service Connection to Allow Access to Your Corporate Resources](#)
- [Configure Prisma Access for Networks](#)

- 
- [Configure Prisma Access for Users](#)

---

# Create a Service Connection to Allow Access to Your Corporate Resources

To create a service connection to allow access to your corporate resources, complete the following steps.



*If you are creating a service connection to allow communication between mobile users and remote networks, instead of enabling access to your corporate resources, follow the instructions in [Create a Service Connection to Enable Access between Mobile Users and Remote Networks](#).*

**STEP 1** | Select **Panorama > Cloud Services > Configuration > Service Connection**.

**STEP 2** | **Add** a new service connection to one of your corporate network sites.

**STEP 3** | Specify a **Name** for the corporate site.

**STEP 4** | Select the **Location** closest to where the site is located.

See [this section](#) for a list of Prisma Access locations.

**STEP 5** | Select or add a new **IPSec Tunnel** configuration to access the firewall, router, or SD-WAN device at the corporate location:

- If you have added a template to the Service\_Conn\_Template\_Stack (or modified the predefined Service\_Conn\_Template) that includes an IPSec Tunnel configuration, select that **IPSec Tunnel** from the drop-down. Note that the tunnel you are creating for each service connection connects Prisma Access to the IPSec-capable device at each corporate location. The peer addresses in the IKE Gateway configuration must be unique for each tunnel. You can, however, re-use some of the other common configuration elements, such as Crypto profiles.

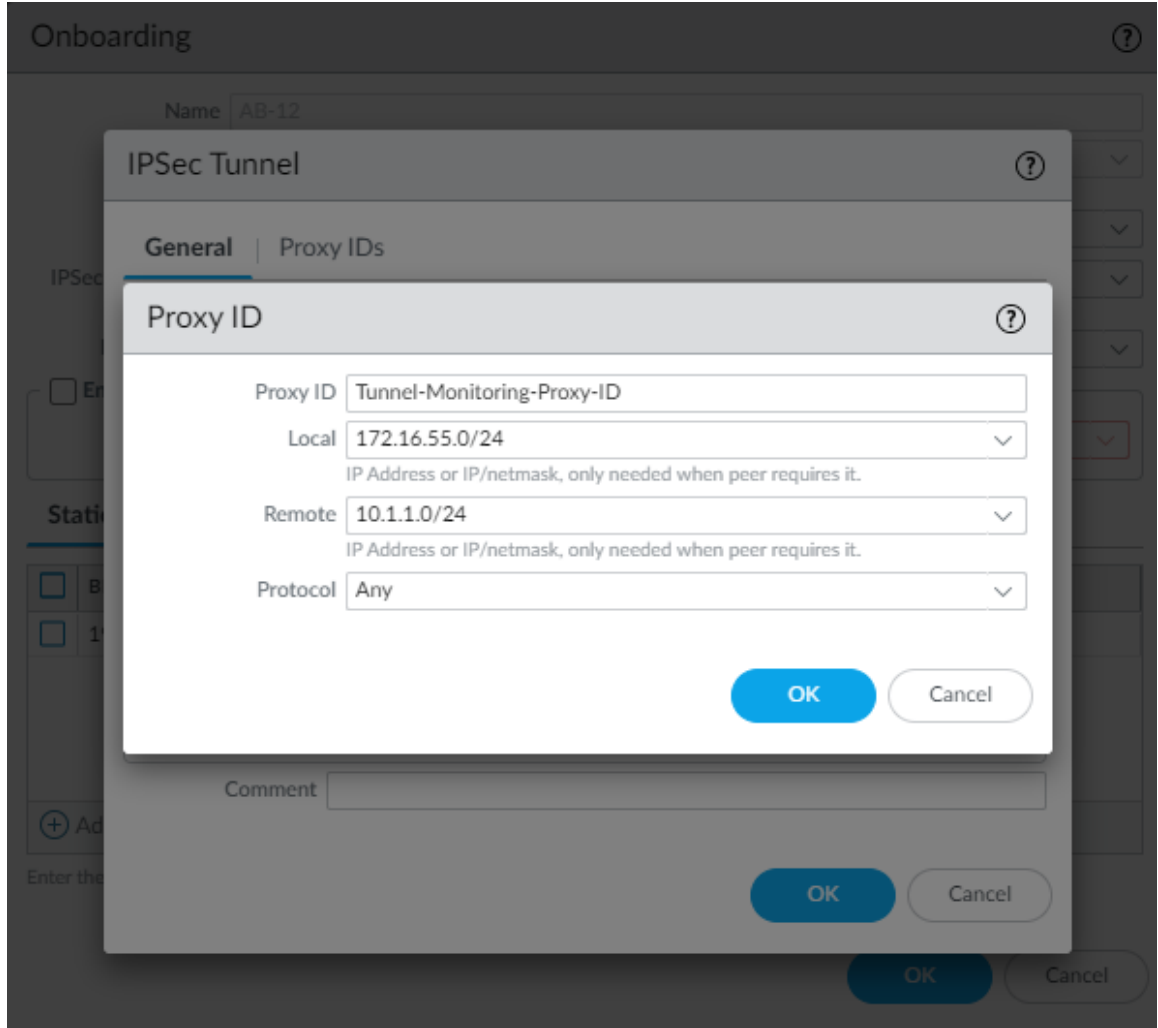


*The IPSec Tunnel you select from a template must use Auto Key exchange and IPv4 only.*


- To [create a new IPSec Tunnel](#) configuration, click **New IPSec Tunnel**, give it a **Name** and configure the **IKE Gateway**, **IPSec Crypto Profile**, and **Tunnel Monitoring** settings.
  - If the IPSec-capable device at your HQ or data center location uses policy-based VPN, on the **Proxy IDs** tab, **Add** a proxy ID that matches the settings configured on your local IPSec device to ensure that Prisma Access can successfully establish an IPSec tunnel with your local device.
  - Leave **Enable Replay Protection** selected to detect and neutralize against replay attacks.
  - Select **Copy TOS Header** to copy the Type of Service (TOS) header from the inner IP header to the outer IP header of the encapsulated packets in order to preserve the original TOS information.
  - To enable tunnel monitoring for the service connection, select **Tunnel Monitor**.
    - Enter a **Destination IP** address.

Specify an IP address at your HQ or data center site to which Prisma Access can send ICMP ping requests for IPSec tunnel monitoring. Make sure that this address is reachable by ICMP from the entire Prisma Access infrastructure subnet.
    - If you use tunnel monitoring with a peer device that uses multiple proxy IDs, specify a **Proxy ID** or add a **New Proxy ID** that allows access from the infrastructure subnet to your HQ or data center site.

The following figure shows a proxy ID with the service infrastructure subnet (172.16.55.0/24 in this example) as the **Local** IP subnet and the HQ or data center's subnet (10.1.1.0/24 in this example) as the **Remote** subnet.



The following figure shows the Proxy ID you created being applied to the tunnel monitor configuration by specifying it in the **Proxy ID** field.

 You must configure a static route on your CPE to the Tunnel Monitor IP Address for tunnel monitoring to function. To find the destination IP address to use for tunnel monitoring from your data center or HQ network to Prisma Access, select *Panorama > Cloud Services > Status > Network Details*, click the *Service Infrastructure* radio button, and find the *Tunnel Monitor IP Address*.

**STEP 6 | BGP and hot potato routing deployments only**—Select a service connection to use as the preferred backup (**Backup SC**).

You can select any service connection that you have already added. Prisma Access uses the **Backup SC** you select as the preferred service connection in the event of a link failure. Selecting a backup service connection can prevent [asymmetric routing issues](#) if you have onboarded more than two service connections. This choice is available in [Hot potato routing](#) mode only.

---

**STEP 7** | If you have a secondary WAN link at this location, select **Enable Secondary WAN** and then select or configure an **IPSec Tunnel** the same way you did to set up the primary IPSec tunnel.

If the primary WAN link goes down, Prisma Access detects the outage and establishes a tunnel to the headquarters or data center location over the secondary WAN link. If the primary WAN link becomes active, the link switches back to the primary link.

If you use static routes, tunnel failover time is less than 15 seconds from the time of detection, depending on your WAN provider.

If you configure BGP routing and have enabled tunnel monitoring, the shortest default hold time to determine that a security parameter index (SPI) is failing is the tunnel monitor, which removes all routes to a peer when it detects a tunnel failure for 15 consecutive seconds. In this way, the tunnel monitor determines the behavior of the BGP routes. If you do not configure tunnel monitoring, the hold timer determines the amount of time that the tunnel is down before removing the route. Prisma Access uses the default BGP HoldTime value of 90 seconds as defined by RFC 4271, which is the maximum wait time before Prisma Access removes a route for an inactive SPI. If the peer BGP device has a shorter configured hold time, the BGP hold timer uses the lower value.

When the secondary tunnel is successfully installed, the secondary route takes precedence until the primary tunnel comes back up. If the primary and secondary are both up, the primary route takes priority.



*If you use a different BGP peer for the secondary (backup) connection, Prisma Access does not honor the Multi-Exit Discriminator (MED) attributes advertised by the CPE. This caveat applies if you use multiple BGP peers on either remote network connections or service connections.*

**STEP 8** | Enable routing to the subnetworks or individual IP addresses at the corporate site that your users will need access to.

Prisma Access uses this information to route requests to the appropriate site. The networks at each site cannot overlap with each other or with IP address pools that you designated for the service infrastructure or for the Prisma Access for users IP pools. You can configure **Static Routes**, **BGP**, or a combination of both.

To configure **Static Routes**:

1. On the **Static Routes** tab, click **Add** and enter the subnetwork address (for example, 172.168.10.0/24) or individual IP address of a resource, such as a DNS server (for example, 10.32.5.1/32) that your remote users will need access to.
2. Repeat for all subnets or IP addresses that Prisma Access will need access to at this location.

### Onboarding

Name

Location

IPSec Tunnel

Backup SC

Enable Secondary WAN

IPSec Tunnel

Static Routes | 
 BGP | 
 QoS

CORPORATE SUBNETS ^


	/24
	/24
	/24

Enter the subnets for your corporate headquarters.

To configure **BGP**:

1. On the **BGP** tab, select **Enable**.

When you enable BGP, Prisma Access sets the time to life (TTL) value for external BGP (eBGP) to 8 to accommodate any extra hops that might occur between the Prisma Access infrastructure and your customer premises equipment (CPE) that terminates the eBGP connection.

 *Prisma Access does not accept BGP default route advertisements for either service connections or remote network connections.*


2. (Optional) Select from the following choices:

- To add a **no-export** community for Corporate Access Nodes (Service Connections) to the outbound prefixes from the eBGP peers at the customer premises equipment (CPE), select **Add no-export community**. This capability is disabled by default.

Do not use this capability in hot potato routing mode.

- To prevent the Prisma Access BGP peer from forwarding routes into your organization's network. **Don't Advertise Prisma Access Routes**.

By default, Prisma Access advertises all BGP routing information, including local routes and all prefixes it receives from other service connections, remote networks, and mobile user subnets. Select this check box to prevent Prisma Access from sending any BGP advertisements, but still use the BGP information it receives to learn routes from other BGP neighbors.

 *Since Prisma Access does not send BGP advertisements if you select this option, you must configure static routes on the on-premises equipment to establish routes back to Prisma Access.*

- To reduce the number of mobile user IP subnet advertisements over BGP to your customer premises equipment (CPE), specify Prisma Access to summarize the subnets before it advertises them by selecting **Summarize Mobile User Routes before advertising**.



By default, Prisma Access advertises the mobile users IP address pools [in blocks of /24 subnets](#); if you summarize them, Prisma Access advertises the pool based on the subnet you specified. For example, Prisma Access advertises a public user mobile IP pool of 10.8.0.0/20 using the /20 subnet, rather than dividing the pool into subnets of 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24, and so on before advertising them. Summarizing these advertisements can reduce the number of routes stored in CPE routing tables. For example, you can use IP pool summarization with cloud VPN gateways (Virtual Private Gateways (VGWs) or Transit Gateways (TGWs)) that can accept a limited number of routes.



*If you have hot potato routing enabled and you enable route summarization, Prisma Access no longer prepends AS-PATHs, which might cause asymmetric routing. Be sure that your return traffic from the data center or headquarters location has guaranteed symmetric return before you enable route summarization with hot potato routing.*

3. Enter the IP address assigned as the Router ID of the eBGP router on the data center/HQ network for which you are configuring this service connection as the **Peer Address**.
4. Enter the **Peer AS**, which is the autonomous system (AS) to which the firewall virtual router or BGP router at your data center/HQ network belongs.
5. (Optional) Enter an address that Prisma Access uses as its Local IP address for BGP.

Specifying a **Local Address** is useful where the device on the other side of the connection (such as an Amazon Web Service (AWS) Virtual Private Gateway) requires a specific local IP address for BGP peering to be successful. Make sure that the address you specify does not conflict or overlap with IP addresses in the Infrastructure Subnet or subnets in the service connection.



*You must configure a static route on your CPE to the BGP Local Address.*

6. (Optional) Enter and confirm a **Secret** passphrase to authenticate BGP peer communications.

The screenshot shows the 'Onboarding' configuration page for a service connection. The 'BGP' tab is selected. Under 'Static Routes', the 'BGP' sub-tab is active. The 'Enable' checkbox is checked. There are options for 'Summarize Mobile User Routes before advertising' (unchecked) and 'Don't Advertise Prisma Access Routes' (unchecked). The 'Add no-export community' is set to 'Enabled Out'. The 'Primary WAN' section has fields for Peer AS (100), Peer Address (192.168.141.2), Local Address (192.168.2.32), Secret, and Confirm Secret. The 'Secondary WAN' section has a 'Same as Primary WAN' checkbox checked, with Peer AS (100) and Peer Address fields visible. 'OK' and 'Cancel' buttons are at the bottom right.

**STEP 9 | (Optional)** If you configured a **Secondary WAN** and you need to change the **Peer Address** or **Local Address** for the secondary (backup) BGP peer, deselect **Same as Primary WAN** and enter a unique Peer and, optionally, Local IP address for the secondary WAN.

In some deployments (for example, when using BGP to peer with an [AWS VPN gateway](#)), the BGP peer for the primary and secondary WAN might be different. In those scenarios, you can choose to set a different BGP peer for the secondary WAN.



For BGP deployments with secondary WANs, Prisma Access sets both the primary and secondary tunnels in an UP state, but follows normal BGP active-backup behavior for network traffic. Prisma Access sets the primary tunnel as active and sends and receives traffic through that tunnel only; if the primary tunnel fails, Prisma Access detects the failure using BGP rules, sets the secondary tunnel as active, and uses only the secondary tunnel to send and receive traffic.

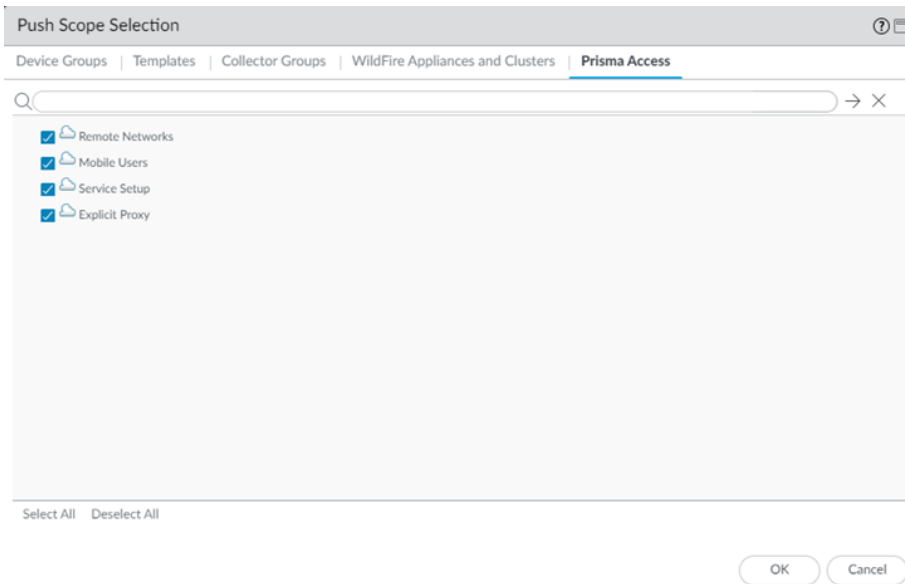
**STEP 10** | If required, enable **Quality of Service** for the service connection and specify a **QoS profile** or add a **New QoS Profile**.

You can create QoS profiles to shape QoS traffic for remote network and service connections and apply those profiles to traffic that you marked with PAN-OS security policies, traffic that you marked with an on-premises device, or both PAN-OS-marked and on-premise-marked traffic. See [Configure Quality of Service in Prisma Access](#) for details.

**STEP 11** | Commit your changes to Panorama and push the configuration changes to Prisma Access.

1. Click **Commit** > **Commit and Push**.

2. **Edit Selections** and, in the **Prisma Access** tab, make sure that **Service Setup** is selected in the **Push Scope**, then click **OK**.



3. Click **Commit and Push**.

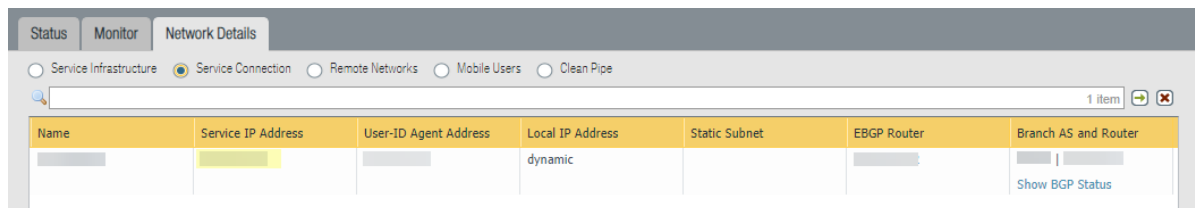
**STEP 12** | Add more service connections by repeating Step 2 through Step 11.

See [Service Connection Overview](#) for the maximum number of service connections you can onboard.

**STEP 13** | Configure the IPsec tunnel or tunnels from your IPsec-capable device on your corporate network back to Prisma Access.

1. To determine the IP address of the tunnel within Prisma Access, select **Panorama > Cloud Services > Status > Network Details**, click the **Service Connection** radio button, and note the **Service IP Address** for the site.

The Service IP Address is the public-facing address that you will need to connect to when you create the tunnel from your IPsec-capable device back to the service connection.



2. On your IPsec-capable device at the corporate location, configure an IPsec tunnel that connects to the Service IP Address within Prisma Access and commit the change on that device so that the tunnel can be established.

## Verify Service Connection Status

To verify that the service connection has been successfully set up, select **Panorama > Cloud Services > Status > Status** and check that the Status is **OK**.

The **Deployment Status** area allows you to view the progress of onboarding and deployment jobs before they complete, as well as see more information about the status of completed jobs. See [Deployment Progress and Status](#) for details.



## Service Connections

Status ● Warning

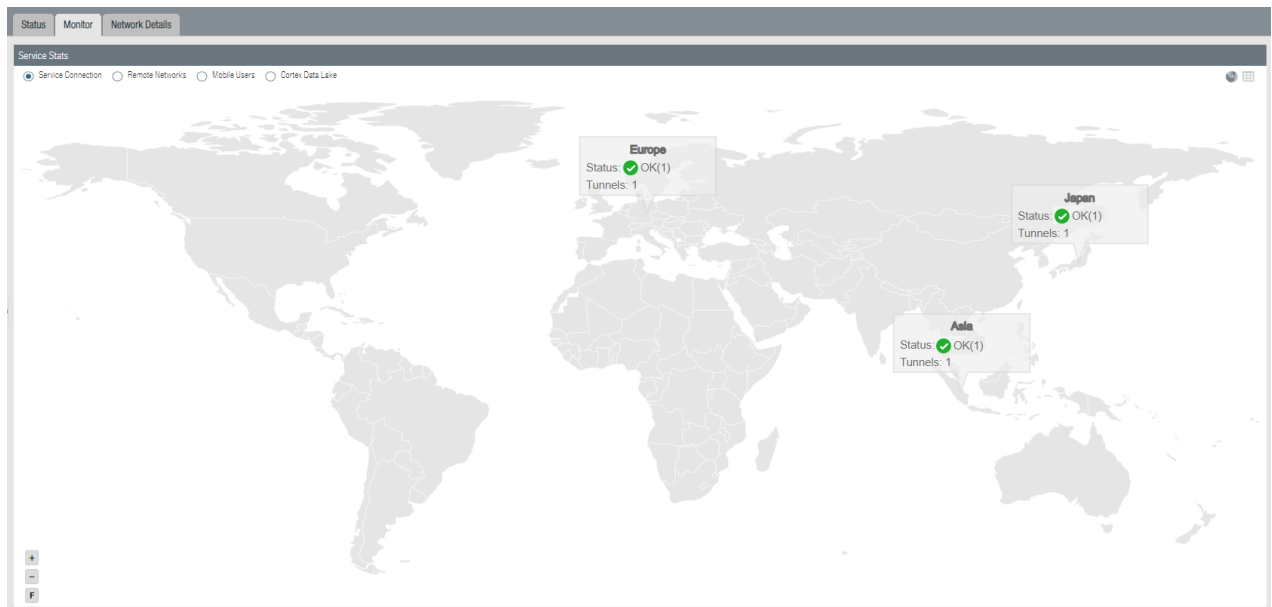
Config Status ● OK

Service Connections 2

Deployment Status ● Success (details)

If the status is not **OK**, hover over the Status icon to view any errors.

To see a graphical representation of the service connection along with status details, select **Service Connection** on the **Monitor** tab.



Select a region to get more detail about that region.

Europe locations

Status: OK(1)  
Tunnels: 1

+  
-  
F

Status Statistics

Location	Remote Peer	Allocated Bandwidth (Mbps)	ECMP	Config Status	BGP Status	Tunnel Status
Ireland	SC1	10	Disabled	In sync	Not Enabled	OK

Click the tabs below the map to see additional information about the service connections.

**Status tab:**

- **Location**—The location where your service connection is deployed.
- **Remote Peer**—The corporate location to which this service infrastructure is setting up an IPsec tunnel.
- **Allocated Bandwidth**—The number of service connections you have allocated multiplied by 300 Mbps.

This number does not reflect the available service connection bandwidth.



*While each service connection provides approximately 1 Gbps of throughput, the actual throughput is dependent on several factors, including:*

- *Traffic mix (for example, frame size)*
- *Latency and packet loss between the service connection and the headquarters location or data center*
- *Service provider performance limits*
- *Customer termination device performance limits*
- *Other customer data center traffic*
- **ECMP**—If you have equal cost multipath (ECMP) configured for this service connection. Since ECMP is not used for service connections, this status is **Disabled**.
- **Config Status**—The status of your last configuration push to the service. If the local configuration and the configuration in the cloud match, the Config Status is **In sync**. If you have made a change locally, and not yet pushed the configuration to the cloud, this may display the status **Out of sync**. Hover over the status indicator for more detailed information. After committing and pushing the configuration to Prisma Access, the Config Status changes to **In sync**.
- **BGP Status**—Displays information about the BGP state between the firewall or router at your corporate/ headquarters location and Prisma Access where the service connection is established. Although you

might temporarily see the status pass through the various BGP states (**Idle**, **Active**, **Open send**, **Open pend**, **Open confirm**, most commonly, the BGP status shows:

- **Connect**—The router at your data center/headquarters is trying to establish the BGP peer relationship with Prisma Access.
- **Established**—The BGP peer relationship has been established.

This field will also show if the BGP connection is in an error state:

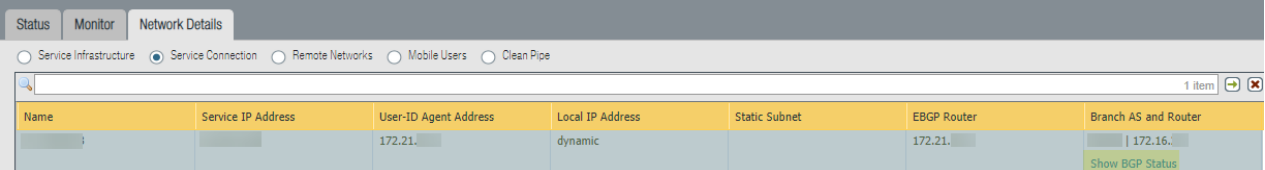
- **Warning**—There has not been a BGP status update in more than eight minutes. This may indicate an outage on the firewall.
- **Error**—The BGP status is unknown.
- **Tunnel Status**—The operational status of the connection between Prisma Access and your service connection.

**Statistics** tab:

- **Location**—The location where your service connection is deployed.
- **Remote Peer**—The corporate location to which the service connection is setting up an IPsec tunnel.
- **Ingress Bandwidth (Mbps)**—The bandwidth from the HQ/data center location to Prisma Access.
- **Ingress Peak Bandwidth (Mbps)**—The peak load from the HQ/data center location into the cloud service.
- **Egress Bandwidth (Mbps)**—The bandwidth from Prisma Access into the HQ/data center location.
- **Egress Peak Bandwidth (Mbps)**—The peak load from Prisma Access into the HQ/data center location.
- **QoS**—Select this button to display a graphic chart that shows a real-time and historical QoS statistics, including the number of dropped packets per class. This chart displays only for service connections or remote network connections that have QoS enabled.

## Verify Service Connection BGP Status

If you configured BGP, you can check its status by selecting **Panorama > Cloud Services > Status > Network Details > Service Connection > Show BGP Status**.



Name	Service IP Address	User-ID Agent Address	Local IP Address	Static Subnet	EBGP Router	Branch AS and Router
		172.21.	dynamic		172.21.	172.16. <a href="#">Show BGP Status</a>

The BGP Status dialog displays. This table provides you with the following information:

- **Peer**—Routing information for the BGP peer, including status, total number of routes, configuration, and runtime statistics and counters. The total number of routes display in the **bgpAfilpv4-unicast Counters** area, in the **Incoming Total** and **Outgoing Total** fields.

**BGP Status** ?

Refresh BGP Status  
Manual

**Peer** | Local RIB | RIB Out

Refresh

35 items → X

NAME	VALUE
Status	
Name	AB-2
Group	
Local IP	172.16.30.1
Peer IP	10.1.1.5
Peer AS	5
Password Set	no
Status	Connect
Status Duration (secs.)	0
Community	
Configuration	

- **Local RIB**—BGP routes that Prisma Access uses locally. Prisma Access selects this information from the BGP RIB-In table, which stores the information sent by neighboring networking devices, applies local BGP import policies and routing decisions, and stores the Local RIB information in the Routing Information Base (RIB).

Note that only the first 256 entries are shown. To view additional entries, enter a subnet or IP address in the Filter field and click Apply Filter to view a subset of the routing entries up to a maximum of 256.

**BGP Status** ?

Refresh BGP Status  
Manual

**Peer** | **Local RIB** | RIB Out

Refresh

0 items → X

PREFIX	FLAG	NEXT HOP	WEIGHT	LOCAL PREFERE...	AS PATH	ORIGIN	MED	FLAP COUNT

- **RIB Out**—Routing information that Prisma Access advertises to its peers through BGP update messages. See [How BGP Advertises Mobile User IP Address Pools](#) for an example of this table.

---

# Create a Service Connection to Enable Access between Mobile Users and Remote Networks

We recommend always creating a service connection, even if you don't need to access resources at your organization's HQ or data center. You must configure a service connection to allow network communication between mobile users and remote network locations and between mobile users in different geographical locations.

We recommend creating this type of service connection for the following environments:

- Your deployment includes both remote networks and mobile users and you do not already have a service connection configured.
- You have mobile users in different geographical areas who need direct access to each other's endpoints.
- You have already configured a service connection, but the existing service connection is not in an ideal location between the remote networks and mobile users.

All remote network locations communicate to each other in a mesh network. Mobile users connect to remote networks using the service connection in a hub-and-spoke network. In some cases, it might improve network efficiency to place another service connection closer to the remote network or networks that the mobile users most frequently access.

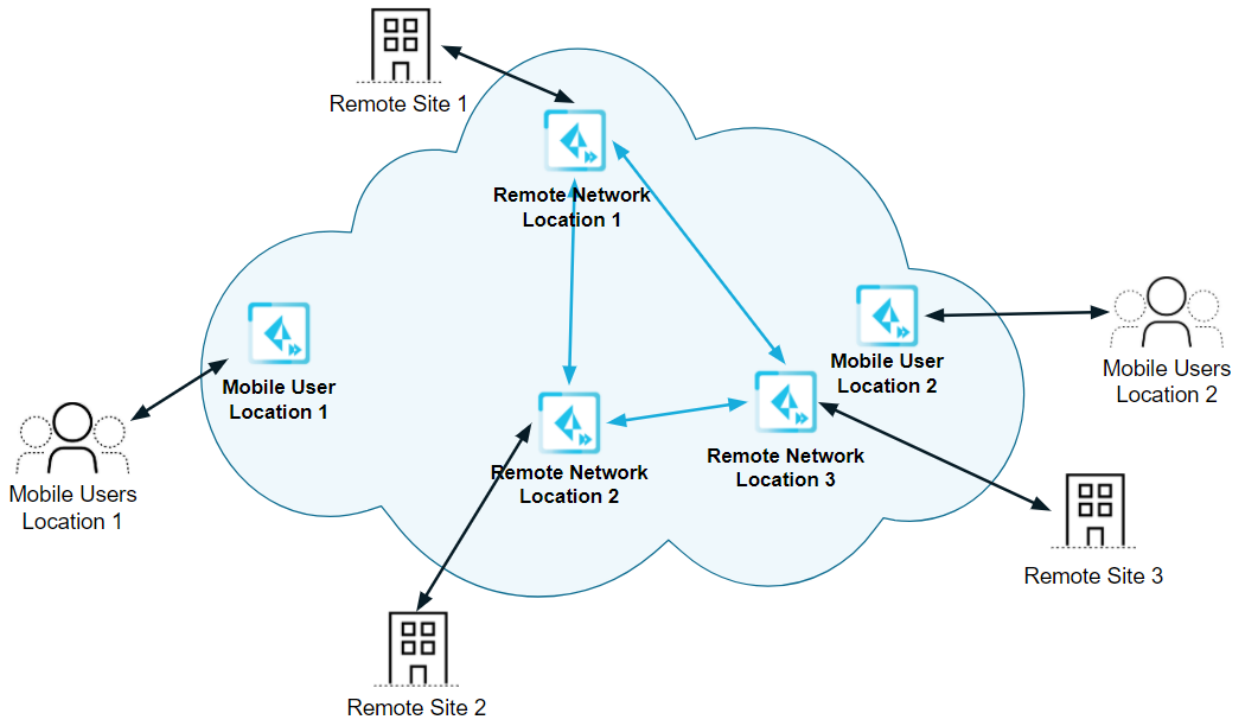
To configure a service connection to connect mobile users and remote networks, **Add** a [service connection](#) using the following values:

- Specify a **Region** that is close to your mobile users.
- **Add** an **IPSec Tunnel** and **IKE Gateway**, using placeholder values.
- Add placeholder **Corporate Subnets**.

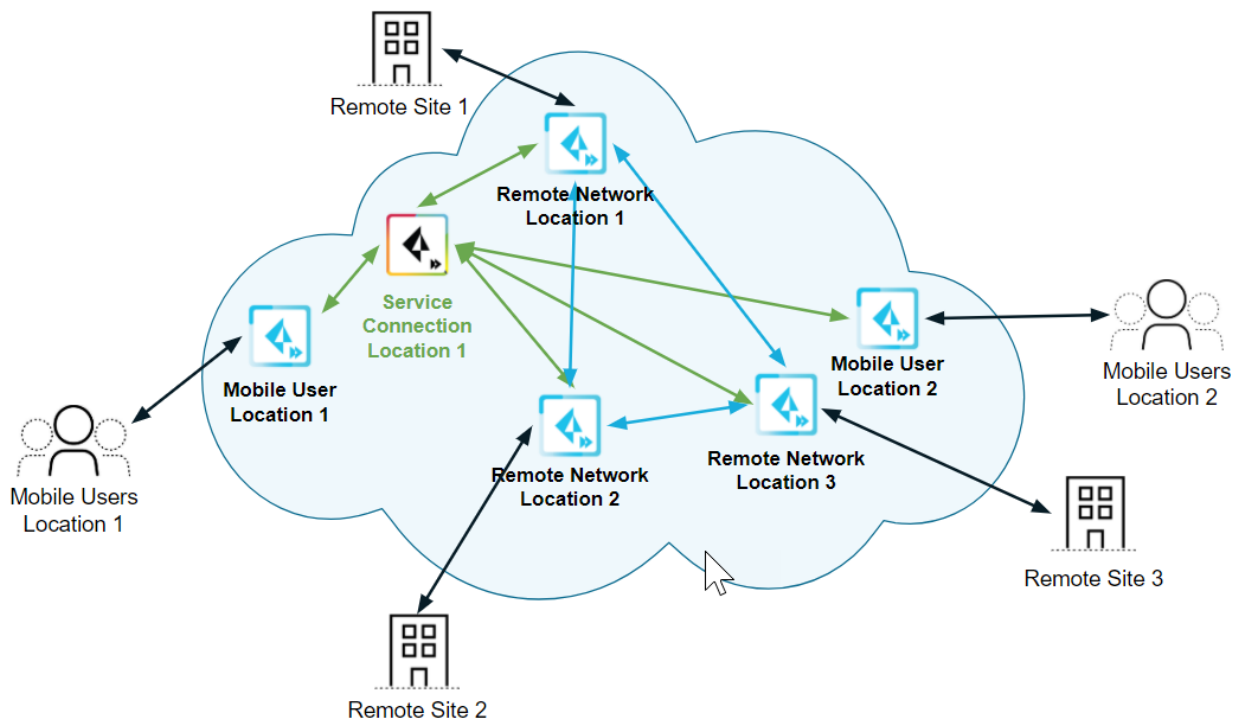
Since Prisma Access doesn't route any traffic through this tunnel, any value that does not conflict or overlap with other configured subnets is valid.

The following example shows a Prisma Access deployment with mobile users in different geographical areas and remote networks. The remote network connections are connected in a mesh network in the Prisma Access infrastructure, but the mobile users cannot connect to the remote networks. In addition, the mobile users in different geographic areas cannot connect to each other without a service connection.

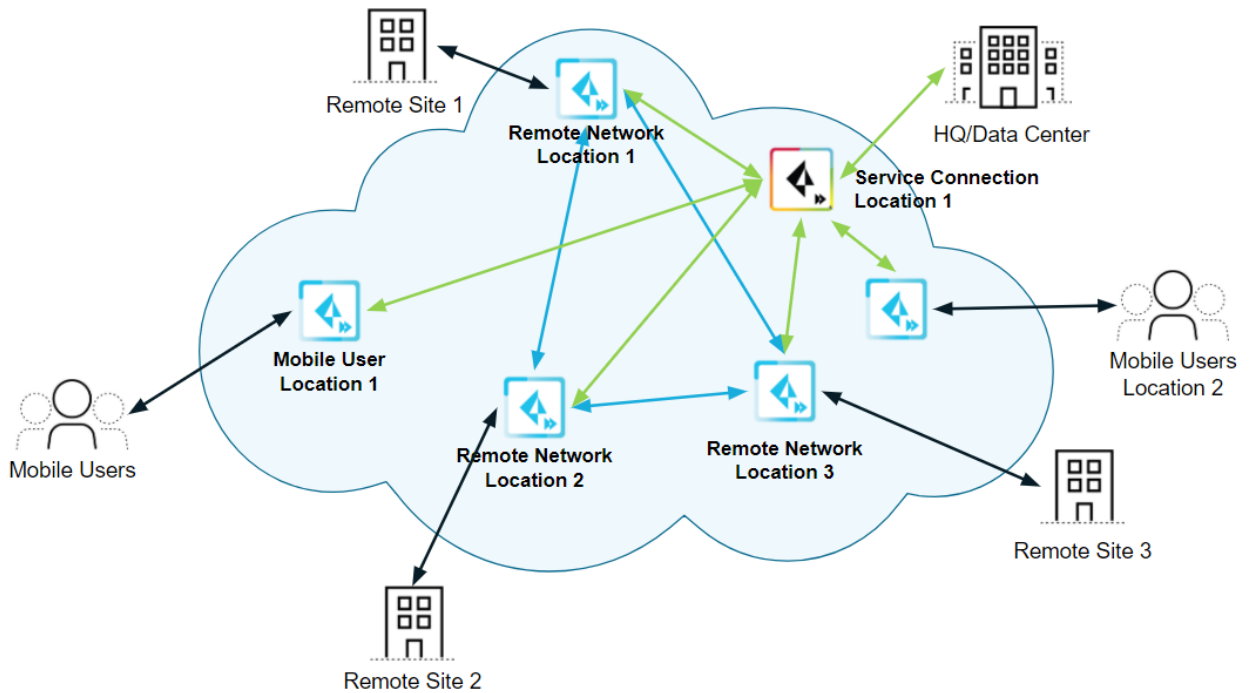




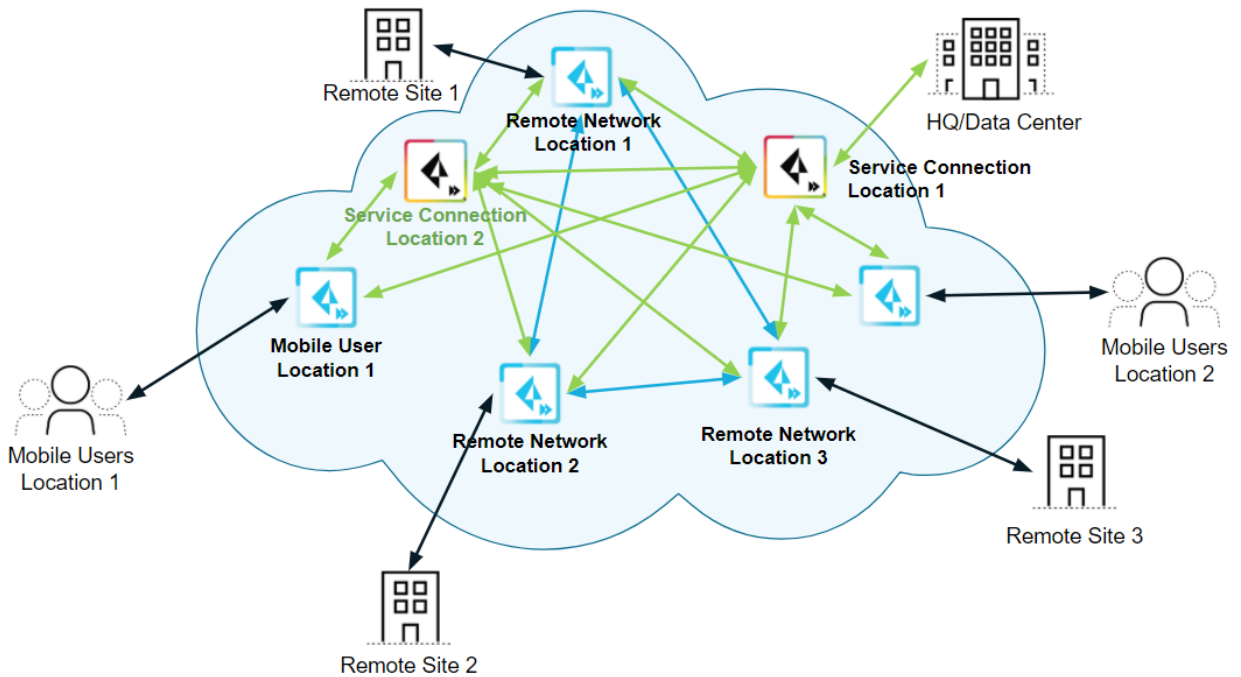
After you add a service connection, the service connection connects the mobile users and the remote networks in a hub-and-spoke network.



Another case where a service connection of this type is useful is when the service connection is far from the mobile users. The following figure shows an example of this network deployment.



Adding a second service connection that is closer to the mobile users creates a more efficient network between the mobile users and remote networks.

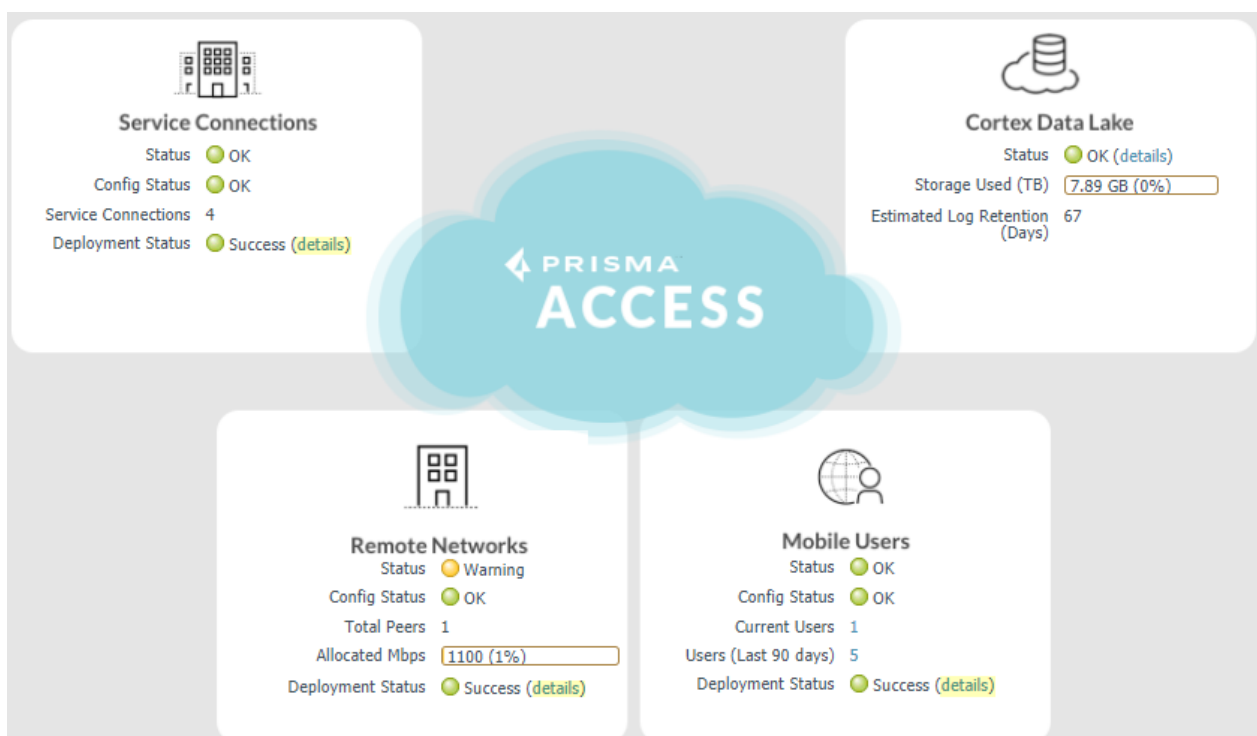


# Deployment Progress and Status

When you configure and commit and push your changes for a [service connection](#), [remote network connection](#), [mobile user deployment](#), or [clean pipe instance](#), Prisma Access begins a series of events to complete the deployment process. To allow you to view the progress of onboarding and deployment jobs before they complete, and to view the status of completed jobs, Prisma Access provides you with deployment status information that is available on the Prisma Access status page.

Checking the progress of a job is useful if, for example, you need the Service IP Address of a service connection or remote network connection to complete the IPsec tunnel connection to your customer premises equipment (CPE). Since Prisma Access does not create the Service IP Address until onboarding is complete, you can view the status of the onboarding job from the deployment status page, instead of refreshing the Network Details page and waiting for the Service IP Address to display.

To view the status of deployment jobs, select **Panorama > Cloud Services > Status > Status**.



The Deployment Status area displays a graphic element (a bubble) showing the status of the deployment, along with the following text:

Deployment Status Text	Description
<b>Started</b>	The deployment job has started.
<b>In-Progress</b>	The deployment job is in progress.
<b>Success</b>	The deployment job succeeded.
<b>Failed</b>	The deployment job failed.
<b>Timeout</b>	The deployment job timed out.

Deployment Status Text	Description
<b>Warning</b>	The deployment job was partially successful; some commit operations succeeded and some commit operations failed.

Click **details** to view the Job ID of the job, its status, and the percentage of its completion. The **Job ID** field is the [Job ID that is associated with the commit operation](#) in Panorama.

Job ID	Overall Status	Percentage Completion
1555	Warning	100%
1540	Success	100%
1526	Failed	100%
1524	Success	100%
1522	Success	100%
1519	Success	100%
1510	Success	100%
1467	Success	100%

To view more details of a specific deployment job, click the left arrow next to **Job ID**. The following screenshot shows the deployment status of a commit that has the Panorama Job ID of 1555. The overall status is **Warning** because two of the nodes failed during the commit stage.

Remote Networks				Last 8 jobs	
Job ID	Overall Status		Percentage Completion		
1555	Warning		100%		
<b>Remote Networks</b> Number of Nodes <b>3</b> Provisioning In Progress <b>0</b> Provisioning Failed <b>2</b> Provisioning Complete <b>1</b>					
Name	Location	Node Status	Action Needed	Error Details	
Remote-Network2	Switzerland	Commit Failed	Commit and push your changes from Panorama again.	IKE gateway Remote-Network2 should use the same IKE crypto profile as CiscoASA-IKE-Gateway-Default (IKEv1: default).(Module: ikemgr). IKEv1 gateway CiscoASA-IKE-Gateway-Default should use the same IKE crypto profile as Remote-Network2 (IKEv1: CiscoASA-IKE-Crypto-Default).(Module: ikemgr).	
Remote-Network3	Switzerland	Commit Failed	Commit and push your changes from Panorama again.	IKE gateway Remote-Network2 should use the same IKE crypto profile as CiscoASA-IKE-Gateway-Default (IKEv1: default).(Module: ikemgr). IKEv1 gateway CiscoASA-IKE-Gateway-Default should use the same IKE crypto profile as Remote-Network2 (IKEv1: CiscoASA-IKE-Crypto-Default).(Module: ikemgr).	
Remote-Network1	Ireland	Commit Succeeded			
1540	Success		100%		
1526	Failed		100%		
1524	Success		100%		
1522	Success		100%		
1518	Success		100%		

The first line of the job status shows the following information:

- The type of deployment job (either **Service Connections**, **Remote Networks**, **Clean Pipe**), or the type of mobile user onboarding operation (**GlobalProtect Gateways**, **GlobalProtect Portals**, or both gateways and portals).
- The **Number of Nodes** that are in the job.

Nodes represent the number of cloud firewalls, gateways, or portals that Prisma Access is configuring for a specific job. The number of nodes do not always correspond to the number of Service Connections, Remote Networks, mobile user locations, or Clean Pipe instances that you deployed; for example, onboarding a location might cause configuration changes to both Prisma Access firewalls and portals.

- The number of nodes that are still being provisioned (**Provisioning in Progress**).
- The number of nodes that failed (**Provisioning Failed**).
- The number of nodes that completed provisioning (**Provisioning Complete**).

The next line in the table provides more granular information about the deployment job. The following screenshot shows three mobile user locations (Australia Southeast, South Africa West, and Brazil East) being successfully onboarded.

Mobile Users			
Job ID	Overall Status	Percentage Completion	
42233	Success	100%	
<b>GlobalProtect Gateways</b> Number of Nodes <b>3</b> Provisioning In Progress <b>0</b> Provisioning Failed <b>0</b> Provisioning Complete <b>3</b>			
Location	Node Status	Action Needed	Error Details
Australia Southeast	Commit Succeeded		
South Africa West	Commit Succeeded		
Brazil East	Commit Succeeded		
<b>GlobalProtect Portals</b> Number of Nodes <b>3</b> Provisioning In Progress <b>0</b> Provisioning Failed <b>0</b> Provisioning Complete <b>3</b>			
Location	Node Status	Action Needed	Error Details
US East	Commit Succeeded		
Singapore	Commit Succeeded		
Ireland	Commit Succeeded		
42229	Success	100%	
42223	Success	100%	
42221	Timeout	100%	

Field	Description
<b>Name</b> (Service Connection, Remote Network, and Clean Pipe deployments only)	The name of the service connection, remote network connection, or clean pipe instance.
<b>Location</b>	The location where the service connection, remote network connection, mobile user, or clean pipe node was onboarded.
<b>Node Status</b>	<p>The status of the deployment operation.</p> <ul style="list-style-type: none"> <li>• <b>Validation Checks In Progress</b>—The deployment job has started, and preliminary checks are in progress.</li> <li>• <b>Validation Checks Succeeded</b>—The deployment job has started, and preliminary checks have succeeded.</li> <li>• <b>Validation Checks Failed</b>—The job failed during validation. More information about the failure is available in the <b>Error Details</b> area.</li> <li>• <b>Commit In Progress</b>—Validation checks have completed, and the commit job is complete.</li> <li>• <b>Commit Succeeded</b>—Validation checks have completed, and the commit job succeeded.</li> <li>• <b>Commit Failed</b>—The job failed during the commit stage. More information about the failure is available in the <b>Error Details</b> area.</li> <li>• <b>Deployment In Progress</b>—Preliminary checks and commit operations have completed for the job, and deployment is in progress.</li> <li>• <b>Deployment Succeeded</b>—The job completed all stages and was successful.</li> <li>• <b>Deployment Failed</b>—Preliminary checks and commit operations completed, but the job failed during the deployment stage. More information about the failure is available in the <b>Error Details</b> area.</li> </ul>

Field	Description
Action Needed	If a job failed, provides additional information about the steps you can perform to fix the issue (either <b>Commit and push your changes from Panorama again</b> or <b>Open a support case</b> ).

Prisma Access does not retain the details of jobs that you onboard and later delete. For example, job 42233 added the Australia Southeast, South Africa West, and Brazil East mobile user locations. If you delete those locations later, clicking the left arrow next to **Job ID** for job 42233 does not provide any additional details about the job.

The screenshot shows the 'Mobile Users' interface with a search bar and a table of jobs. The table has three columns: Job ID, Overall Status, and Percentage Completion. The jobs listed are as follows:

Job ID	Overall Status	Percentage Completion
42238	Success	100%
42233	Success	100%
No deployment changes were required to the Prisma Access infrastructure		
42229	Success	100%
42223	Success	100%
42221	Timeout	100%
42219	Success	100%
42217	Failed	100%
42215	Success	100%
42213	Failed	100%

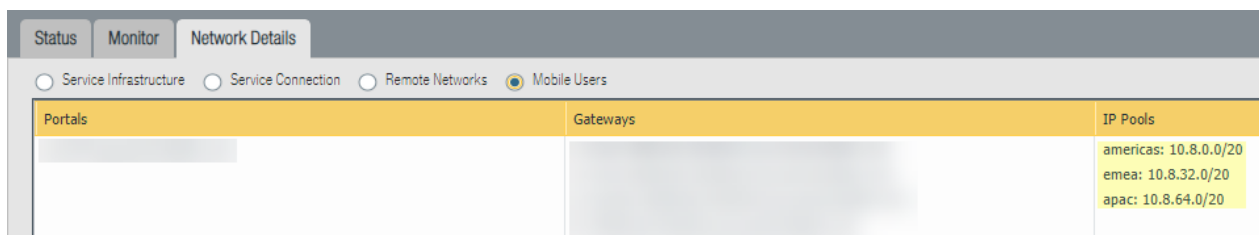
The interface also includes a search bar, a 'Last 10 jobs' label, and a 'Close' button at the bottom right.

---

# How BGP Advertises Mobile User IP Address Pools for Service Connections and Remote Network Connections

If you enable BGP for service connections or remote network connections, after you [Secure Mobile Users With GlobalProtect](#), Prisma Access allocates the mobile user IP address pools you specified using Class C (/24) address blocks. BGP therefore advertises allocated mobile user subnets in blocks of /24, rather than the entire pool(s) associated with that region. When Prisma Access adds a /24 subnet for a Prisma Access gateway, it automatically sends a BGP advertisement. As subnets are added and removed, Prisma Access automatically updates its BGP advertisements. This allocation method provides more flexibility when advertising BGP routes, especially if you configured a **Worldwide** pool instead of allocating pools per region. Dividing the IP address pool into smaller subnets allows the same subnet to be added, removed, or deleted and then reused in different regions when allocated address space is exhausted.

The following screenshot, from **Panorama > Cloud Services > Status > Network Details > Mobile Users**, shows three /20 IP pools for mobile users divided by region.



The **RIB Out** table, from **Panorama > Cloud Services > Status > Network Details > Service Connection > Show BGP Status** (in the **Branch AS and Router** area), shows the mobile users address pool divided into blocks of /24 subnets for BGP route advertisements. Note that the entire /20 subnets are not advertised.



**BGP Status** ?

Refresh BGP Status

Manual ▼

Refresh

Peer Local RIB RIB Out

17 items ➔ ✕

Prefix ▲	Flag	Next Hop	Wei...	Local Pref...	AS Path	Origin	MED	Adv. Status	Aggr. Status
10.8.0.0/24		172....						adve...	no aggr...
10.8.1.0/24		172....						adve...	no aggr...
10.8.2.0/24		172....						adve...	no aggr...
10.8.3.0/24		172....						adve...	no aggr...
10.8.4.0/24		172....						adve...	no aggr...
10.8.5.0/24		172....						adve...	no aggr...
10.8.32.0/24		172....						adve...	no aggr...
10.8.33.0/24		172....						adve...	no aggr...
10.8.34.0/24		172....						adve...	no aggr...
10.8.64.0/24		172....						adve...	no aggr...
10.8.65.0/24		172....						adve...	no aggr...
10.8.66.0/24		172....						adve...	no aggr...
10.8.67.0/24		172....						adve...	no aggr...
10.8.68.0/24		172....						adve...	no aggr...

Close

---

# Use Traffic Steering to Forward Internet-Bound Traffic to Service Connections

Prisma Access allows you to create traffic steering rules to specify targets for internet-bound traffic from mobile users and remote network connections. You can specify the traffic to be redirected to a service connection before sending to the internet, or you can specify the traffic to directly egress to the internet. This functionality is known as *Traffic Steering*.

Alternatively, you can configure Prisma Access to accept a [default route](#) from your CPE to Prisma Access so that Prisma Access forwards internet-bound mobile user traffic to the best service connection in your deployment.

The following sections provide an overview of default routes and traffic steering, as well as the steps you take to configure it.

- [Default Routes](#)
- [Traffic Steering](#)
- [Traffic Steering Requirements](#)
- [Traffic Steering Examples](#)
- [Traffic Steering Rule Guidelines](#)
- [Zone Mapping and Security Policies for Dedicated Connections](#)
- [Configure Traffic Steering](#)

## Default Routes

Use Prisma Access' default route capability to accept default routes being advertised from your CPE to service connections. You can use BGP or static routes to advertise the default route. Prisma Access uses BGP to advertise these routes over multiple service connections, which allows Prisma Access to route mobile user traffic through the best service connection for a given mobile user location. To enable service connections to accept default routes, specify **Accept Default Route over Service Connections** when you [configure global settings for service connections](#).

After you enable default routes, your internet-bound traffic will be steered to service connections instead of egressing from the mobile user locations. This functionality can be useful if you want to redirect internet-bound traffic to the data center; for example, if you have a third-party security stack in your data center and you want the stack to perform additional screening or inspection.

Use the following guidelines when implementing default routes:

- Default routes apply to mobile user deployments only; remote network connections operate normally with no change when you enable default routes.
- You do not need to specify target service connections or traffic steering rules when you allow default routes, although they are supported for use with default routes. See [Traffic Steering Examples](#) for examples of using default routes with traffic steering.
- When you specify the **Accept Default Route over Service Connections** setting, all Prisma Access service connections, with the exception of dedicated service connections, accept default routes and will use the routes in traffic steering decisions.
- Before you enable this setting, make sure that your data centers are sending default routes; otherwise, routing through service connections will fail.

- 
- Palo Alto Networks recommends that all data centers advertise a default route; when Prisma Access receives the routes, it can then select the best service connection to use for the remote network location.
  - When you [create service connections](#), use either static routes only or BGP only for the connections. Palo Alto Networks does not recommend mixing service connections that use BGP and static routes when using default routes.
  - Using default routes is supported with [multi-tenant deployments](#).
  - Prisma Access does not forward Clientless VPN, portal, or gateway SAML authentication traffic to a public identity provider (IdP) using the default route.

For more information and examples of implementing default routes with traffic steering, see [Traffic Steering Examples](#).

## Traffic Steering

In standard Prisma Access deployments, a service connection provides access to internal network resources, such as authentication services and private apps in your headquarters or data center. Service connections process internal traffic, where no internet access is required. In some cases, you might want to redirect internet-bound traffic to the data center. Traffic steering allows you to redirect mobile user or remote network traffic to a service connection before being sent to the internet.

You can use traffic steering with mobile user deployments, remote network deployments, or a combination of both. Use traffic steering to direct internet-bound network traffic based on many criteria including IP addresses, [Custom URL categories](#), service type (HTTP or HTTPS), [User-ID](#), [Dynamic Address Groups \(DAGs\)](#) and IP-based [External Dynamic Lists \(EDLs\)](#).

There are two action types supported with traffic steering:

- **Forward to the target**—Use the criteria in traffic steering rules to forward internet-bound traffic through a target you create that uses one or more service connections.
- **Forward to the internet**—Use the criteria in traffic steering rules to directly forward traffic from its source (mobile user location or remote network connection) to the internet, without being forwarded to a service connection.

If you forward to a target, you can choose to create two types of target groups: dedicated and non-dedicated.

- A service connection that is used only for traffic steering-related traffic is a *dedicated service connection*. To set a service connection to be used as a dedicated service connection, select **Dedicated for Traffic Steering Only** when you [configure traffic steering](#) in Panorama.

You might want to configure a dedicated service connection if you use a third-party security stack that is outside of your organization's internal network to process traffic before it is sent to a public SaaS application or the internet. Because the security stack is not a part of your organization's network, you don't want this service connection to process any internal network traffic.

- A service connection that is used for traffic steering and for standard service connection-related traffic (such as traffic going to an authentication server in the data center) is a *non-dedicated service connection*.

Setting a service connection as a dedicated service connection causes the following changes to your deployment:

- The zone for all service connections associated with this target changes from Trust to Untrust. Check your [zone mapping](#) and [security policies](#) to make sure that your network reflects this change.

- 
- Service connections that are configured as dedicated service connections do not participate in BGP routing, either internally or externally.
  - If your dedicated service connection uses BGP, the BGP status shows as **Not Enabled** when you open the status page (**Panorama > Cloud Service > Status > Monitor > Service Connection**), select a region, then select the Status tab. To check the BGP status of a service connection, check the service connections configuration page (**Panorama > Cloud Services > Configuration > Service Connection**).
  - By default, the service connections apply source NAT to the forwarded traffic. The source IP address is the **EBGP Router** address of the service connection (**Panorama > Cloud Services > Status > Network Details > Service Connection > EBGP Router**), which is taken from the Infrastructure Subnet (**Panorama > Cloud Services > Status > Network Details > Service Infrastructure**).

You can disable source NAT and use your organization's source IP addresses for the dedicated service connection; to do so, select **Disable Source NAT for Dedicated SC** when you **Add** a target in the **Target Service Connections for Traffic Steering** area.

## Traffic Steering Requirements

Before you implement traffic steering in your Prisma Access deployment, make sure that your network environment has the following infrastructure requirements:

- Prisma Access must be able to connect to the IPSec-capable CPE (such as a router or SD-WAN device) that your organization uses to terminate the service connection, and the IP address for the device must be reachable from Prisma Access.

You create a service connection using standard **IPSec** and **IKE** cryptographic profiles between the stack location and Prisma Access. You can use static routes, BGP, or a combination of both when you [create a service connection](#) and use traffic steering. If you use default routes with traffic steering, Palo Alto Networks recommends that you use either BGP only or static routes only. If you use static routing, specify the public IP address used by the organization's CPE as the **Peer Address** when you [create an IKE gateway](#).

- Prisma Access might not match the first few packets of a URL from a URL category in a traffic steering rule, which means that the first few packets of a network session (for example, a TCP handshake) might not match the rule. Palo Alto Networks recommends that, for URLs you use in traffic steering rules, you create a security policy rule to allow them through the Untrust zone so that the handshake can complete when a new session begins.
- If you are using this configuration with a security stack, the stack location must be reachable from the service connection by a standard IPSec tunnel configuration.

Use the following guidelines when configuring traffic steering:

- You can specify up to 1,000 URLs (aggregated) in a traffic steering configuration, including regular and wildcard (\*.example.com) URLs in [custom URL categories](#).
- Prisma Access prepends an asterisk to URLs in custom URL categories, if you use this category in a traffic steering rule. If you use the same URL category policies for both traffic steering and other security policy rules, these changes apply to both the traffic steering rules and other security policy rules.

If you have custom URL categories that are not used in traffic steering rules, Prisma Access does not change the URLs in those categories.

- Use all lower-case URLs when you enter URLs in a custom URL category.
- You can configure a maximum of 100 traffic steering rules.
- If you have primary and backup tunnels configured, traffic steering using traffic steering rules will not work after a failover from the primary (active) to the backup tunnel. [Default routing](#) works in a failover scenario with primary and backup tunnels.

# Traffic Steering Examples

The following sections describes different types of traffic steering deployments.


## Default Route Example

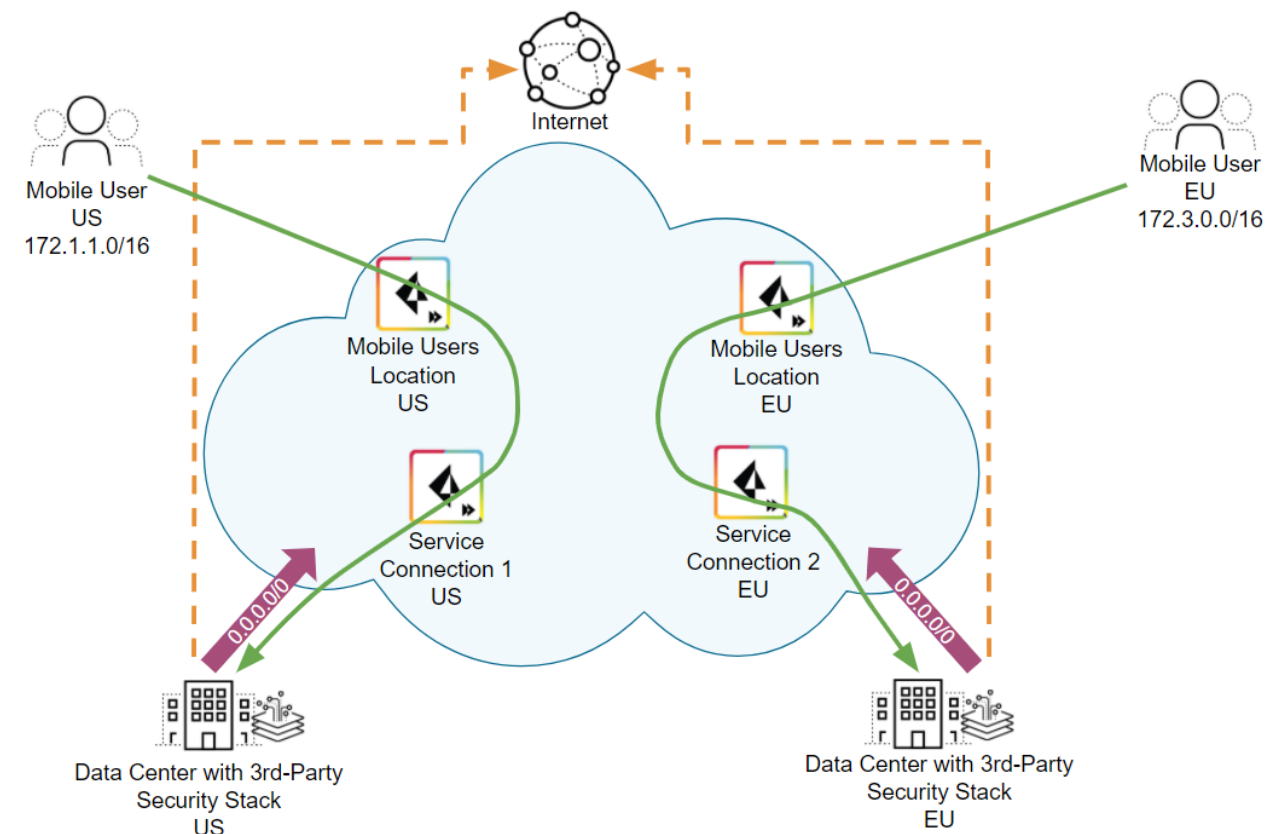
The following example shows a sample Prisma Access deployment the following components:

- Two Prisma Access mobile user locations; one in the United States (US) and one in Europe (EU).
- Two Prisma Access service connections; one in the US and one in the EU, with both data centers sending default routes to the service connections (**Accept Default Route over Service Connections** is enabled).
- Two data centers; one in the US and one in the EU.

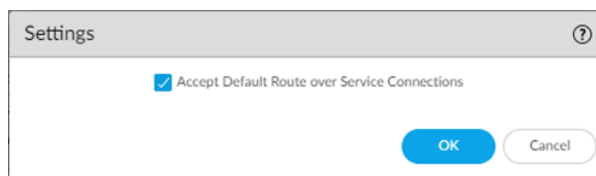
Each data center has a 3rd-party security stack; for this reason, you want all internet-bound traffic to go through the data center before egressing to the internet.

When a mobile user sends data center traffic, Prisma Access checks its routing tables, determines the closest service connection, and forwards the traffic to that service connection. In the following example, Prisma Access sends data center traffic from the mobile users in the US to Service Connection and traffic from the mobile users in the EU to Service Connection 2.

 Use non-dedicated service connections with default routes; dedicated service connections do not participate in BGP routing, so they cannot receive BGP advertisements from the HQ or data center.

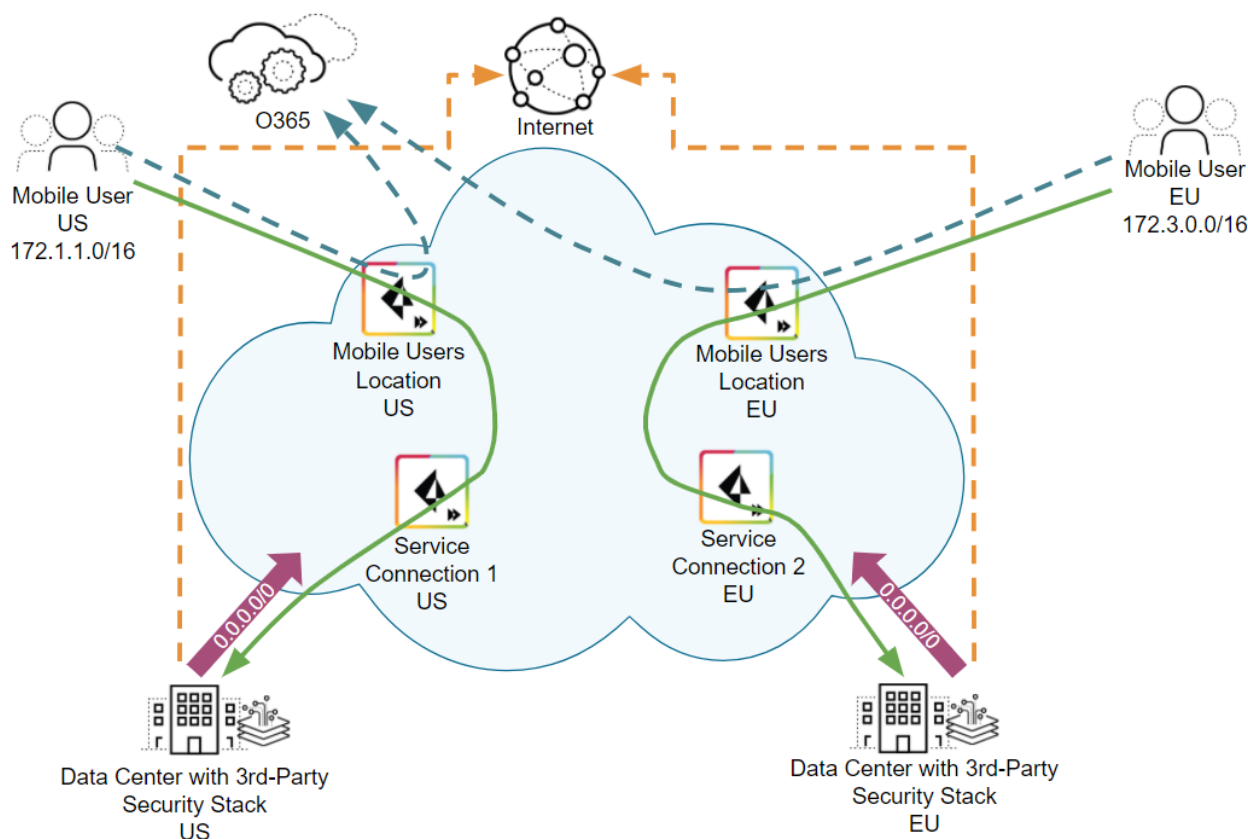


To enable default routes, select **Accept Default Route over Service Connections** when you configure traffic steering settings. After you configure this setting and commit and push your changes, Prisma Access sends internet-bound traffic over the service connections.



## Default Routes with Traffic Steering Direct to Internet Example

The following example shows you using more granular control for external SaaS application-bound traffic. In this case, you want to send Office 365 traffic to egress to the internet directly from the mobile user location, instead of sending it to the data center for further processing. Use traffic steering along with default routes for this configuration.



To allow Prisma Access to route Office 365 traffic directly to the internet, perform the following actions:

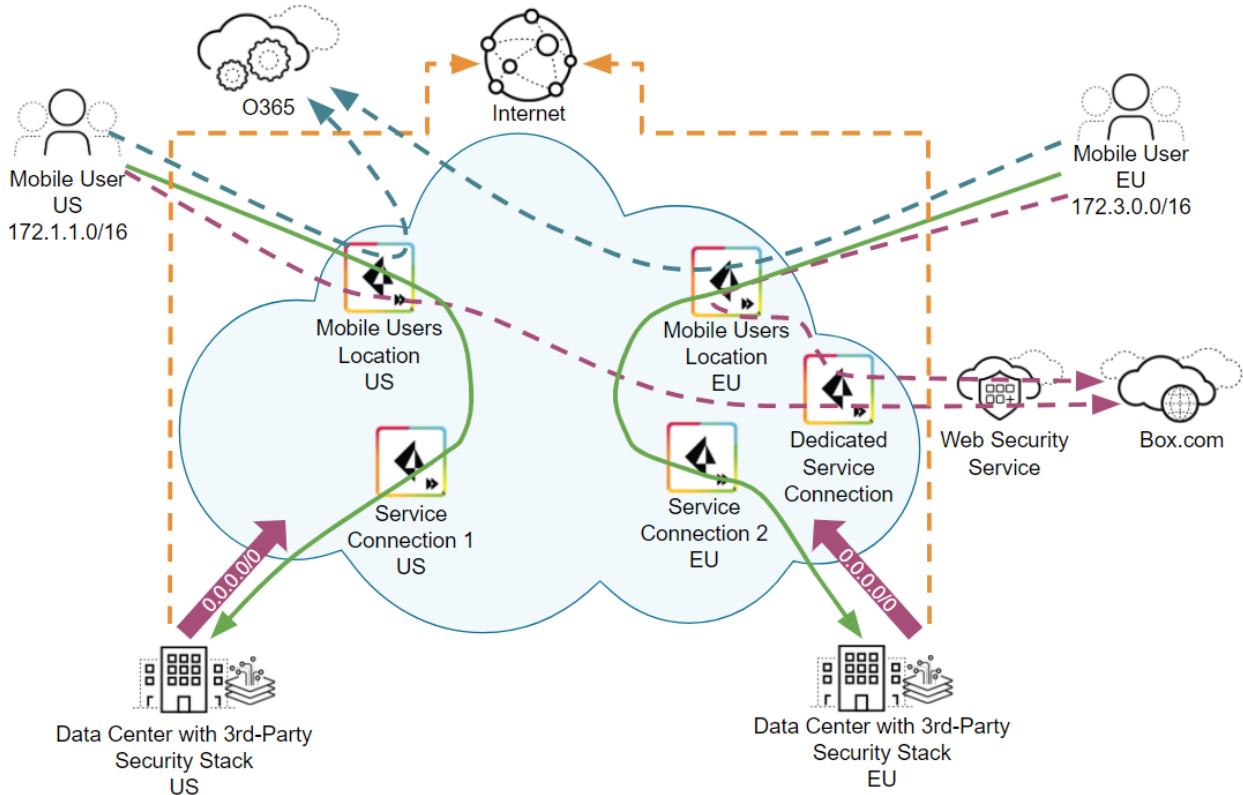
- Create an [EDL \(Object > External Dynamic Lists\)](#) with IP addresses that match the Office 365 addresses.
- Create a [Custom URL category \(Objects > Custom Objects > URL Category\)](#) with URLs that match Office 365 URL.
- create [create traffic forwarding rules](#) and specify the EDL and URL category you created as destination match criteria with an **Action of Forward to the internet**.

This configuration sends Office 365 traffic directly to the internet, while other internet-bound traffic is sent to the data center for further processing before egressing to the internet.

Traffic Steering Rules							
Q direct 2 / 6 → ×							
GENERAL - RULE NAME	Source		Destination		SERVICE	ACTION	
	SOURCE ADDRESS	USER	DESTINATION	URL CATEGORY			
<input type="checkbox"/> Direct-Egress-O365-IP	any	any	o365-ip		any	Forward to the internet	
<input type="checkbox"/> Direct-Egress-O365-URL	any	any	any	category-office	any	Forward to the internet	


## Default Routes with Traffic Steering and Dedicated Service Connection Example

In this example, in addition to the previous configuration, you have a third-party internet security service, and you want to send traffic from box.com to be processed by the security service before egressing to the internet. You do not want to send any other internet-bound traffic to the security service; for this reason, you create a dedicated service connection for the box.com traffic. After your configuration is complete, Prisma Access sends \*.box.com destination traffic to the stack.



To enable this deployment, you perform the following actions in the Traffic Steering tab:

- Create a Target Service Connection group that assigns one or more service connections to the target and select **Dedicated for Traffic Steering Only**, which makes the target service connection or connections dedicated.

 If you create a target with more than one service connection, Prisma Access chooses the best service connection to forward the internet-bound traffic.

---

### Target Service Connection for Traffic Steering ?

Group Name

Target  SERVICE CONNECTION ^

prisma-service\_4

Add  Delete

Dedicated for Traffic Steering Only (Included Service connections will be marked as Untrust Zone for Security Policy)

Disable source NAT for Dedicated SC

- Create a traffic steering rule that forwards traffic to the URL. The following screenshot shows the traffic destination being assigned a custom URL category that contains the URL \*.box.com.



**Traffic Steering Rules** ?

General | Source | **Destination** | Service | Action

<input checked="" type="checkbox"/> Any	<input type="checkbox"/> URL CATEGORY ^
<input type="checkbox"/> DESTINATION ^	<input checked="" type="checkbox"/> box-dot-com

+ Add - Delete      + Add - Delete

Select Any in the URL area to have Prisma Access forward all HTTP and HTTPS traffic.  
Deselect URL and URL category for forward/exclude all traffic

OK Cancel

- Create an **Action** in the traffic steering rule of **Forward to the target** and specify the target group name you created (**dedicated** in this case).

**Traffic Steering Rules** ?

General | Source | Destination | Service | **Action**

Forward to the target     Forward to the internet

Target Group Name: dedicated

OK Cancel

## Traffic Steering Rule Guidelines

Traffic steering can process a wide variety of possible configurations; however, it is important to understand how Prisma Access processes rules, so you can create rules that are easy to maintain and manage. To help you create the rules that work best for your deployment, follow these guidelines:

- Prisma Access evaluates rules in the order that you create them (from top to bottom). Specify more specific rules at the top and more general rules at the bottom.
- Palo Alto Networks recommends that you create multiple rules with fewer matching criteria, instead of creating fewer rules with multiple types of criteria. Creating simpler rules both speeds up rule creation and makes it easier to modify a rule.

- 
- Since you cannot move a rule up or down in a list after you create it, carefully plan your rule order before you create the rules.
  - Rules that specify **Any** source address and User, **Any** source destination and URL Category, and **Any** service are not supported. Use more specific rules; for example, specify a rule with **Any** source or destination traffic and a service of **service-http** and **service-https**.
  - If you are going to specify rules for users in the **Source User** field, make sure that Prisma Access can distinguish between users if the same username is shared between users who authenticate locally and users who authenticate using LDAP by authenticating LDAP users in the format of `domain/username` and authenticating local users in the format of `username` (without the domain name).
  - If you have configured an on-premises next-generation firewall as a **master device**, you can auto-populate user and group information for mobile user device groups in traffic steering and security policy rules by selecting **Panorama > Cloud Services > Configuration > Mobile Users**, clicking the gear icon to edit the Settings, and selecting the **Master Device** in the Device Group area. While this populates the master device in every device group, it only populates the user and group information for mobile users in security policy rules.
  - If an EDL (type IP List) is used in a Traffic Steering Rule, and the EDL source URL of the EDL is updated to a URL that is not accessible, Prisma Access may continue to use the cached IP list from the previous URL.
  - Prisma Access bypasses Traffic Steering for rules with a service type of HTTP or HTTPS if you use an application override policy for TCP ports 80 and 443.

In addition, traffic steering does not work for URLs from URL categories referenced in the traffic steering rule if you have configured an application override policy for TCP ports 80 or 443.

- You can specify destination IP addresses and URL categories in the same rule. If you do, Prisma Access uses a logical OR to process the destination criteria in the rule, but processes the URLs and URL category traffic based on TCP ports 80 and 8080 for HTTP and TCP port 443 for HTTPS.

For a rule with IP addresses and URL categories, traffic matches the rule if either the IP address or the URL category matches, but processes the URL category traffic based on ports 80, 443, and 8080 only. Palo Alto Networks does not recommend creating a rule of this type; instead, create simpler rules.

For example, you want to enforce the following rules for your network traffic:

- You have an internal HTTP server with an IP address of 10.1.1.1 in the data center, and you want to direct internal HTTP and HTTPS traffic to this server. The IP address of the server is 10.1.1.1.  
Traffic to this server should not go to the internet and should be processed internally; therefore, choose a non-dedicated target for this traffic, because this type of target processes both internal and internet-bound traffic.
- You want office365.com traffic to be routed directly to the internet.
- You want traffic from \*.example.com or any traffic defined in a custom URL category of **custom-social-networking** to be routed to a dedicated connection.
- You want any other HTTP and HTTPS traffic to use the same non-dedicated service connection target as that used for the internal HTTP server.

For this example, create the rules from the most specific to the least specific, as shown in the following screenshot. Do not add the rule that allows all HTTP and HTTPS traffic first, or Prisma Access would direct all HTTP and HTTPS traffic to the non-dedicated connection without evaluating any of the other rules.

Traffic Steering Rules							
GENERAL - RULE NAME	Source		Destination		SERVICE	ACTION	
	SOURCE ADDRESS	USER	DESTINATION	URL CATEGORY			
<input type="checkbox"/> Internal-http-https	any	any	10.1.1.1		service-http service-https	Forward to the target	
<input type="checkbox"/> Direct-Egress-O365-IP	any	any	o365-ip		any	Forward to the Intern	
<input type="checkbox"/> Direct-Egress-O365-URL	any	any	any	category-office	any	Forward to the Intern	
<input type="checkbox"/> custom-social-networking	any	any	any	custom-social-networking	any	Forward to the target	
<input type="checkbox"/> any-http-https	any	any	any		service-http service-https	Forward to the target	

## Zone Mapping and Security Policies for Dedicated Connections

If you create a target that uses a dedicated service connection, the zone for the dedicated service connection changes from **Trust** to **Untrust** (non-dedicated service connection targets do not change their zones). Since you cannot create zones or configure zone mapping for service connections, you make [zone mapping](#) and [security policy](#) changes for dedicated service connections to the mobile users and device groups instead. Complete the following steps to configure zone mapping for dedicated connections.



*These steps show a sample configuration; you can tailor this example to suit your deployment.*

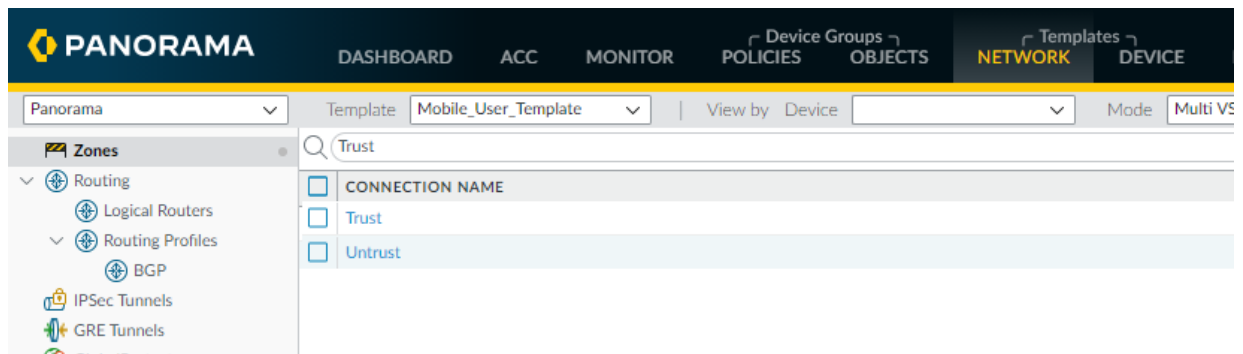
**STEP 1 |** Select **Network > Zones**.

**STEP 2 |** Select the correct **Template** from the drop-down list (either **Mobile\_User\_Template** for mobile users or **Remote\_Network\_Template** for remote networks).

If you have a mobile user and a remote network deployment, you need to perform these steps twice; once in the **Mobile\_User\_Template** and once in the **Remote\_Network\_Template**.

**STEP 3 |** **Add** two zones for your trusted and untrusted zones.

This example creates two zones called **Trust** and **Untrust**.



**STEP 4 |** Create default policies for the zones you created.

1. Select **Policies > Security > Post Rules**.
2. Select the correct **Device Group** from the drop-down list (either **Mobile\_User\_Device\_Group** for remote networks or **Remote\_Network\_Device\_Group** for mobile users).

If you have a mobile user and remote network deployment, you need to perform these steps twice; once in the **Mobile\_User\_Device\_Group** and once in the **Remote\_Network\_Device\_Group**.

3. **Add** a default policy to use for Trust zone-to-Trust zone traffic.

This policy allows **Any** traffic to pass for all **Source, User, Destination, Application, and Service/URL Category** traffic.

### Security Policy Rule

General | Source | Destination | Application | Service/URL Category | Actions | Usage

Name: Trust-Trust

Rule Type: universal (default)

Description:

Tags:

Group Rules By Tag: None

Audit Comment:

[Audit Comment Archive](#)

4. **Add** a default policy to use for Trust zone-to-Untrust zone traffic, using the same parameters you used for the Trust-to-Trust policy.

When complete, you have two security policies, one for Trust-to-Trust traffic and one for Trust-to-Untrust traffic.

	NAME	LOCATION	TAGS	TYPE	ZO
1	Trust-Trust	Mobile_User_De...	none	universal	
2	Trust-UnTrust	Mobile_User_De...	none	universal	

#### STEP 5 | Define **Zone Mapping** for the remote networks, mobile users, or both, as required for your deployment.

1. Set the zone mapping for the remote networks, mobile users, or both.
  - For mobile users, select **Panorama > Cloud Services > Configuration > Mobile Users**.
  - For remote networks, select **Panorama > Cloud Services > Configuration > Remote Networks**.
2. Click the gear icon next to **Zone Mapping** to edit the settings.

Service Setup | **Mobile Users** | Remote Networks | Service Connection | Traffic Steering | Superuser Operations

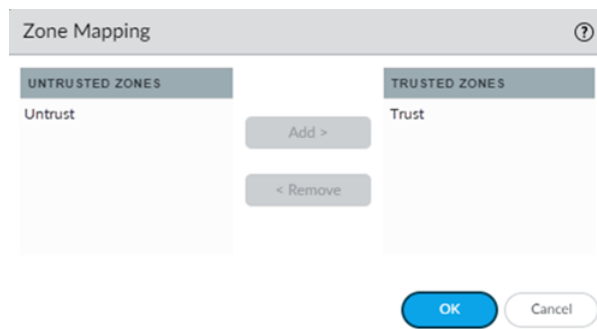
Settings

Template Stack: Mobile\_User\_Template\_Stack  
 Parent Device Group: PAVM1

Zone Mapping

Trusted Zones: Trust  
 Untrusted Zones: Untrust

3. Set the **Zone Mapping** for your deployment, moving the zone for trusted traffic to the **Trusted Zones** and the zone for untrusted traffic to the **Untrusted Zones**; then, click **OK**.



## Configure Traffic Steering

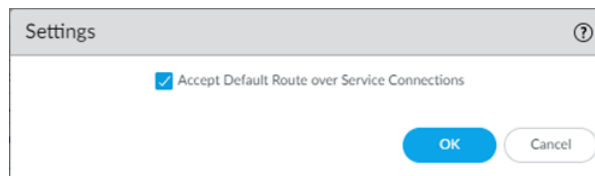
Configure traffic steering for your deployment by completing the following steps.

**STEP 1 |** Onboard your [service connections](#), [mobile users](#) and [remote networks](#), as applicable to your deployment.

**STEP 2 |** Select **Panorama > Cloud Services > Configuration > Traffic Steering**.

**STEP 3 |** (Optional, [mobile user deployments only](#)) Allow Prisma Access to accept and install the default route advertised over one or more service connections from the CPE by clicking the gear icon to open the Settings and selecting **Accept Default Route over Service Connections**.

Default routes have [specific guidelines](#) that you must follow when using them; for example, default routes are supported for mobile user deployments only and have no effect on remote network deployments. Be sure to review these guidelines before implementing default routes with traffic steering.



**STEP 4 |** (Optional) Create a target group and assign a service connection to it.

1. In the **Target Service Connections for Traffic Steering** area, **Add** a group and give it a **Group Name**.
2. **Add** a **Target** for the traffic, specifying the **Service Connection** to use with the target; then, click **OK**.

Palo Alto Networks does not recommend using multiple service connections (whether dedicated or non-dedicated) in a target service connection group that is referenced in a traffic steering rule. In addition, a given service connection can only exist in one target and you cannot add a single service connection to two different targets.

3. Choose whether to make the service connections associated with this target a dedicated service connection.
  - You can use a dedicated service connection to steer traffic to a third-party security stack or cloud that is not on your premises and does not need to participate in routing. To set a service connection to be used as a dedicated service connection, select **Dedicated for Traffic Steering Only**.



*Dedicated service connections change their zones; see [Traffic Steering](#) for details.*

- Deselect **Dedicated for Traffic Steering Only** if you will send both normal service connection-related and traffic steering traffic through the service connection; with this choice, the zone for the service connection remains as Trust.
4. Choose whether to enable or disable source NAT.

To disable source NAT for Dedicated service connections, select **Disable Source NAT for Dedicated SC**. Source NAT is enabled by default (the check box is deselected).

If you disable source NAT, Prisma Access uses your organization's source IP addresses for the dedicated service connection. If you enable source NAT, Prisma Access uses the **EBGP Router** address of the service connection (**Panorama > Cloud Services > Status > Network Details > Service Connection > EBGP Router**) as the source IP address, even after the traffic egresses from the dedicated service connection.

**STEP 5 |** Create rules for the target you created and apply them to the target.

1. In the **Traffic Steering Rules** area, **Add** a traffic steering rule.
2. In the **General** tab, **Name** the traffic steering rule.
3. In the **Source** tab, specify rules for source traffic.
  - In the **Source Address** field, specify one or more of the following objects, or select **Any** to have traffic from any source go to this target:
    - An IP address
    - An [address object](#) that you created in Panorama (**Objects > Addresses**)
    - A [Dynamic Address Group \(DAG\)](#)
    - An [External Dynamic List \(EDL\)](#) using IP addresses or URLs
  - In the **Source User** field, specify rules for source user traffic. You can specify the following user information:
    - Users  
Enter users in either the *domain/user* or the *user@domain* format.
    - User groups

- Use full distinguished names (DNs) when entering user groups.
- Users configured on Panorama (**Device > Local User Database > Users**)
- User groups configured on Panorama (**Device > Local User Database > User Groups**)

If you use address objects, DAGs, EDLs, users, or user groups, specify them as **Shared** to share them with all device groups in Prisma Access. In addition, do not enter 0.0.0.0/0 in address objects, DAGs, or EDLs; instead, enter 0.0.0.0/0 directly in the rule.



*Prisma Access automatically populates users from the mobile users device group only.*

4. In the **Destination** tab, specify the following values:

- In the **Destination** area, specify one of the following criteria, or select **Any** to have traffic processed by the rules in the **URL Category** field:
  - An IP address or prefix
  - An [address object](#) that you created in Panorama (**Objects > Addresses**)
  - A [Dynamic Address Group \(DAG\)](#)
  - An IP address-based [External Dynamic List \(EDL\)](#)



*Do not enter 0.0.0.0/0 in address objects, DAGs, or EDLs; instead, enter 0.0.0.0/0 directly in the rule.*

Leave **Any** selected to pass all traffic to be processed by the rules in the **URL Category** area. If you specify rules in the **Destination**, and **URL Category** areas, Prisma Access processes the rules in the **Destination** category first.

- In the **URL Category** field, enter a custom [URL category](#) (**Objects > Custom Objects > URL Category**) When you create a custom URL category, enter URLs in all lower case. Traffic steering supports custom URL and predefined URL categories.

You can use wildcards with the URLs in URL categories. The following wildcard formats are supported:

- \*.example.com
- \*.fqdn.example.com

The following formats are not supported:

- \*
- \*.\*
- \*example.com
- example.com/*path* (only domain names are supported)
- \*fqdn.example.com
- fqdn.example.\*

URLs in custom URL categories use the same URL pattern matching as that used by next-generation firewalls.

Use the following guidelines when configuring destination options:

- If you specify a URL category, Prisma Access only matches HTTP and HTTPS traffic, even when service is set to Any.
- Do not create a custom URL category with a type of **Category Match**.
- Do not create a custom URL category with the name **Custom\_URL\_Category\_TFR** because, for deployments that are migrated from Prisma Access 1.7 to 2.0, URLs entered in the URL area from 1.7 are moved to a custom URL category named **Custom\_URL\_Category\_TFRnumber**, where *number* is a number appended to the custom URL category.

**Traffic Steering Rules** ⓘ

General | Source | **Destination** | Service | Action

Any

DESTINATION ^

URL CATEGORY ^

test1

test2

+ Add - Delete + Add - Delete

Select Any in the URL area to have Prisma Access forward all HTTP and HTTPS traffic.  
Deselect URL and URL category for forward/exclude all traffic

OK Cancel

5. In the **Service** tab, specify a service type.

Specify **service-http** to forward HTTP traffic and specify **service-https** to specify HTTPS traffic. Select **Any** to forward traffic of any service type.

6. In the **Action** tab, select the **Target Group Name** that you want to apply to the traffic steering rule.

7. Forward traffic to the specified service connection target, or send the traffic directly to the internet without going through the service connection.

- To have Prisma Access forward traffic to a service connection target, select **Forward to the target**; then select the **Target Group Name**.
- To have Prisma Access forward traffic directly to the internet without first sending it to a service connection, select **Forward to the internet**.

**Traffic Steering Rules** ⓘ

General | Source | Destination | Service | **Action**

Forward to the target  Forward to the internet

Target Group Name: Non\_dedicated

OK Cancel

8. Click **OK** to save your changes.



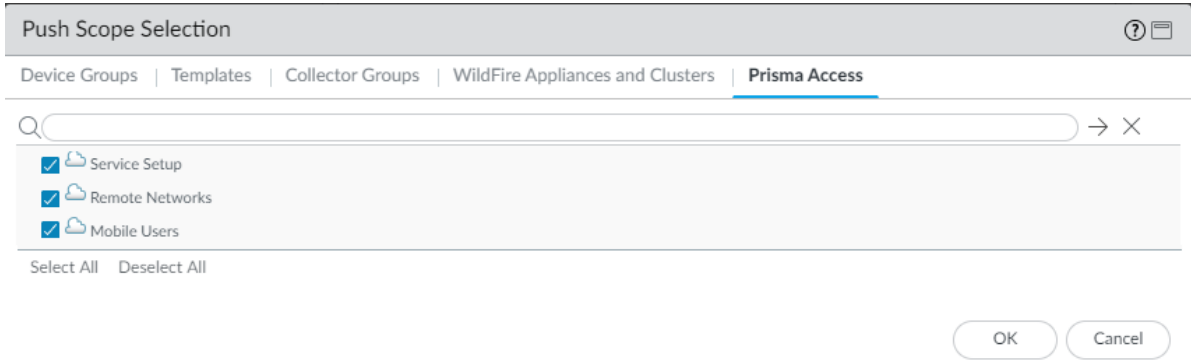
---

**STEP 6 | Optional** Specify additional traffic steering rules.

Prisma Access processes multiple rules in the order that you create them (from top to bottom).

**STEP 7 |** Commit and push your changes to make them active in Prisma Access.

1. Select **Commit > Commit and Push** and **Edit Selections** in the Push Scope.
2. Select **Prisma Access**, then select **Service Setup, Remote Networks,** and **Mobile Users.**



3. Click **OK** to save your changes to the Push Scope.
4. **Commit** and **Push** your changes.

---

# Routing Preferences for Service Connection Traffic

Prisma Access uses BGP for dynamic routing, and uses BGP path selection to install routes in the route table. When Prisma Access routes traffic to your headquarters or data center using service connections, it uses routing methods that direct that traffic effectively. Prisma Access uses a default routing model that was designed to fit the majority of network deployments; however, not all organization's networks are the same. To fit a wider range of deployments, Prisma Access allows you choose another mode for service connection routing. The following sections describe the BGP routing methods that Prisma Access uses, along with the factors you need to consider in your organization's network before changing Prisma Access' default method of service connection routing.



*Changing the Prisma Access service connection routing method requires a thorough understanding of your organization's topology and routing devices, along with an understanding of how Prisma Access routing works as described in this section. We recommend that you read this section carefully before changing the routing method from the default setting.*

Prisma Access supports static routing and dynamic routing using BGP for service and remote network connections; this section assumes that you use BGP routing for your Prisma Access deployments. When you select BGP routing, your organization's network learns BGP information from Prisma Access.

- [Routing Modes for Service Connections](#)
- [Mobile User and Remote Network Routing to Service Connections Overview](#)
- [Prisma Access Default Routing](#)
- [Hot Potato Routing](#)
- [Configure Routing Preferences](#)

## Routing Modes for Service Connections

You can choose from the following routing modes with Prisma Access:

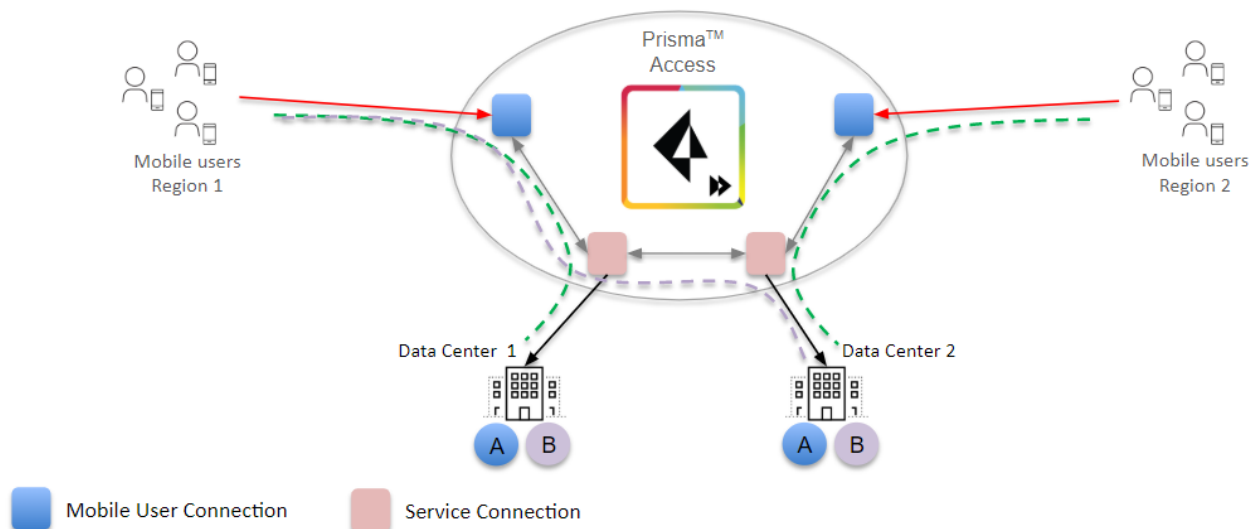
- **Default routing**—This is the current routing model that Prisma Access uses.  
Use this routing mode if you want Prisma Access to use BGP best path-selection mechanisms without adjusting any of the BGP attributes. In this mode, Prisma Access will honor any attribute advertised by the customer premises equipment (CPE).
- **Hot Potato Routing**—Prisma Access hands off the traffic as quickly as it can to your organization's network.  
Use this routing method if you want your organization's network to perform the majority of routing decisions.


## Mobile User and Remote Network Routing to Service Connections Overview

It is useful to understand how Prisma Access routes traffic between mobile users, remote networks, and service connections, because the routing used by mobile user traffic and remote network traffic between service connections is different.

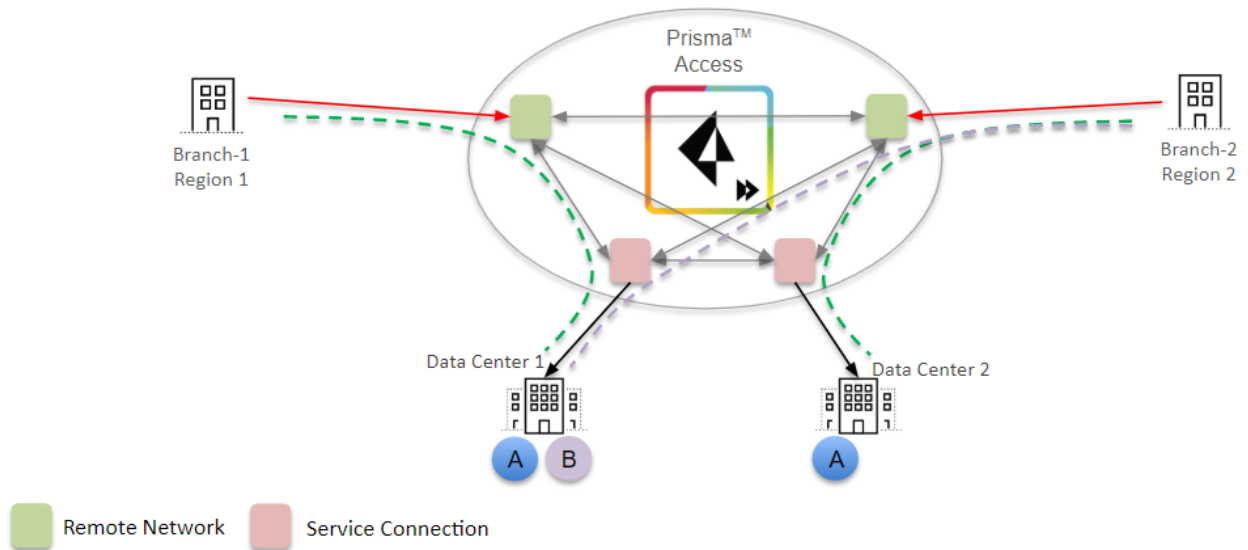
**Mobile User-service connection routing**—The mobile user connection forms an IPSec tunnel with the nearest service connection. Prisma Access uses iBGP for internal routing and eBGP to peer with the

customer premises equipment at the data center. The following diagram shows mobile users in Regions 1 and 2 being routed to the respective service connections in that region. Mobile users in Region 1 are accessing applications **A** and **B** located at Data Center 1. If your organization's network uses BGP routing for their service connections and a service connection experiences an ISP failure at Data Center 1, Prisma Access detects the failure and routes the traffic for applications **A** and **B** to Data Center 2 after BGP convergence, providing redundancy to your network's data centers.



 *Prisma Access uses the following timing with BGP when it detects a failure: If you configure BGP routing and have enabled tunnel monitoring, the shortest default hold time to determine that a security parameter index (SPI) is failing is the tunnel monitor, which removes all routes to a peer when it detects a tunnel failure for 15 consecutive seconds. In this way, the tunnel monitor determines the behavior of the BGP routes. If you do not configure tunnel monitoring, the hold timer determines the amount of time that the tunnel is down before removing the route. Prisma Access uses the default BGP HoldTime value of 90 seconds as defined by RFC 4271, which is the maximum wait time before Prisma Access removes a route for an inactive SPI. If the peer BGP device has a shorter configured hold time, the BGP hold timer uses the lower value. When the secondary tunnel is successfully installed, the secondary route takes precedence until the primary tunnel comes back up. If the primary and secondary are both up, the primary route takes priority.*

**Remote Network-service connection routing**—Prisma Access creates a full mesh network with other remote networks and service connections. As with mobile users, Prisma Access uses iBGP for its internal routing and eBGP to peer with customer premises equipment to exchange routes. If a user in Branch 1 is accessing application **A** from Data Center 1 in your organization's data center and the link between Branch 1 and Data Center 1 goes down, Prisma Access routes the traffic for application **A** to Data Center 2 after BGP convergence.



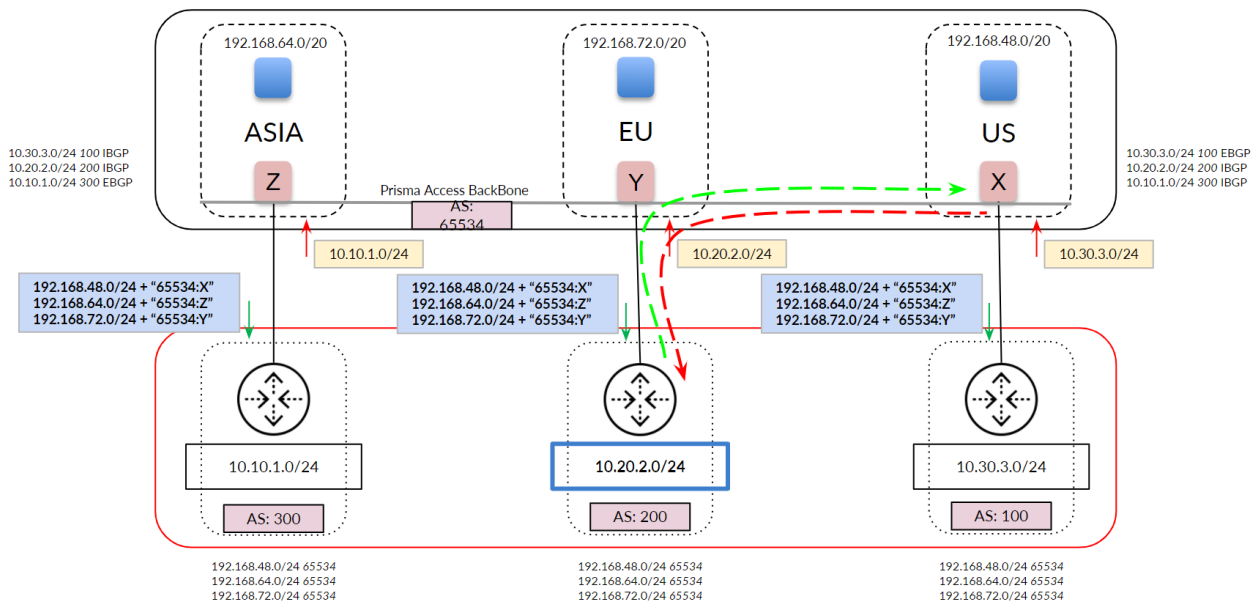
## Prisma Access Default Routing

The following figure shows an example of Prisma Access routing service connection traffic in default routing mode. The organization's network has three separate networks in three data centers and does not have a backbone connecting the networks. In default routing mode, mobile user pools are advertised equally on the three networks, as shown at the bottom of the figure.

Note that, when Prisma Access advertises mobile user routes, it [divides the subnets into Class C /24 address blocks](#) before advertising them; thus, it advertises the /20 mobile user subnets in chunks of /24 as prefixes are consumed by the gateways.

Make a note of how Prisma Access uses BGP route advertisements:

- Prisma Access does not adjust the default BGP attributes for mobile user advertised routes (Prisma Access adds its AS number to the route advertisements).
- Prisma Access advertises mobile user routes in [blocks of /24 subnets](#) and adds BGP community values in the routes it advertises through the service connection. The following figure shows a mobile user deployment with three service connections and three different IP address blocks specified for the [mobile user IP address pool](#): 192.168.64.0/20 for the **Asia, Australia & Japan** region, 192.168.72.0/20 for the **Africa, Europe & Middle East** region, and 192.168.48.0/20 for the **North America & South America** region. Prisma Access divides these routes into block of /24 and advertises them with an Prisma Access' AS number of **65534**, but also appends the BGP community values to the advertisements (**Z** for Asia, **Y** for EU, and **X** for US). Those routes are shown in the middle of the figure. In this way, you can differentiate service connections in your network, even though Prisma Access assigns the same AS number to them.



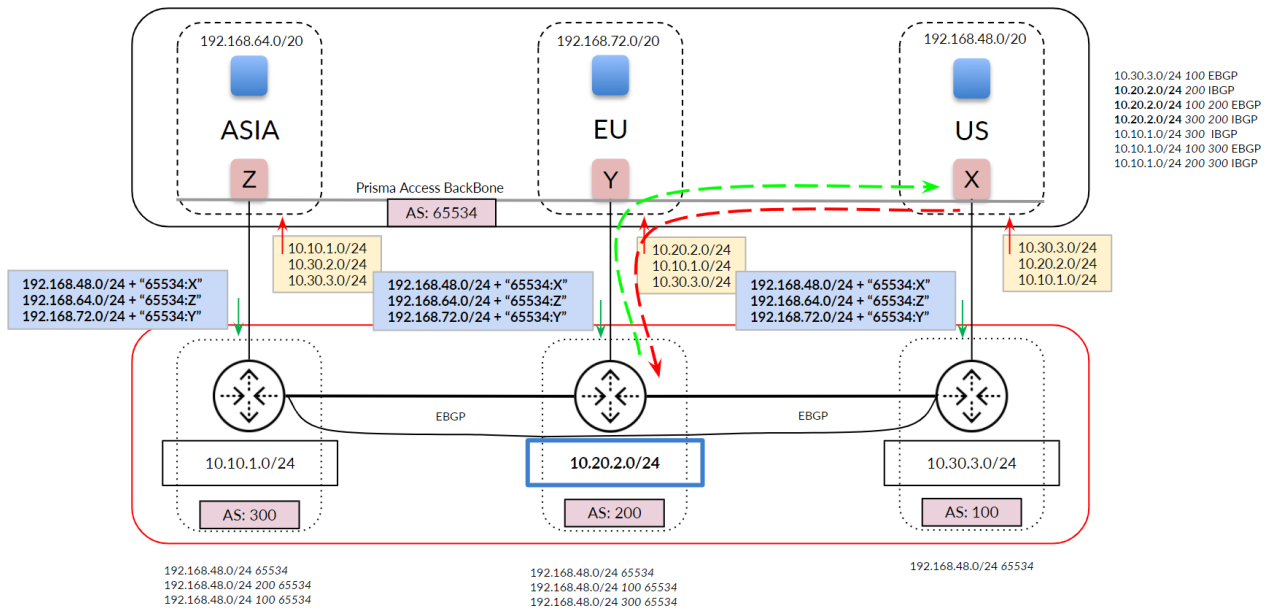
You can view the community string by selecting **Panorama > Cloud Services > Status > Network Details > Service Connection > Show BGP Status** and find the **Community** field in the **Peer** tab.

The screenshot shows the BGP Status interface in Panorama. The Peer tab is selected, showing details for a peer with IP 192.168.2.2 and AS 200. The Community field is highlighted with the value 65534:63033. The interface also shows incoming and outgoing counters and capabilities.

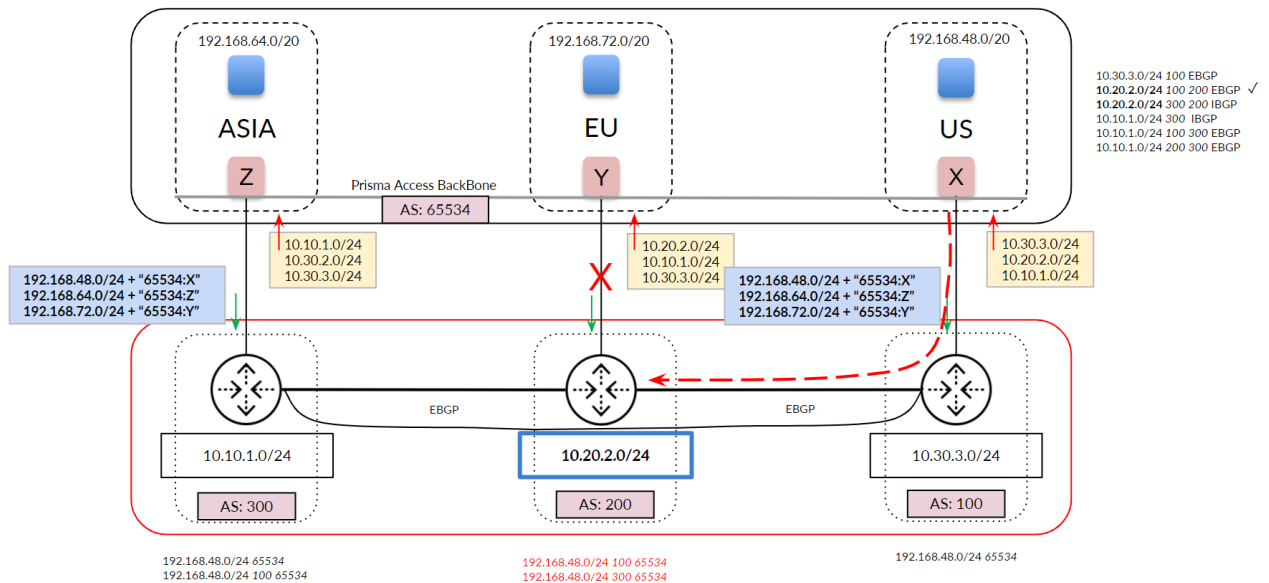
Name	Value
Peer IP	192.168.2.2
Peer AS	200
Password Set	no
Status	Established
Status Duration (secs.)	19647
Community	65534:63033
<b>bgpAfiiPv4-unicast Counters</b>	
Incoming Total	3
Incoming Accepted	3
Incoming Rejected	0
Outgoing total	14
Outgoing Advertised	14
<b>Capability</b>	
Multiprotocol Extensions(1)	IPv4 Unicast

The following figure shows a more common network with a full-mesh eBGP backbone. The figure shows the routes that Prisma Access has learned from your organization's network on the top right. Note the extra routes that Prisma Access has learned through the Prisma Access backbone (iBGP) and your organization's backbone (eBGP).

For traffic between mobile users in the **North America & South America** region (US in the diagram) and the data center in your organization's **Africa, Europe & Middle East** region (EU in the diagram), Prisma Access chooses the path through the EU service connection because it prefers routes with a shorter AS-PATH.



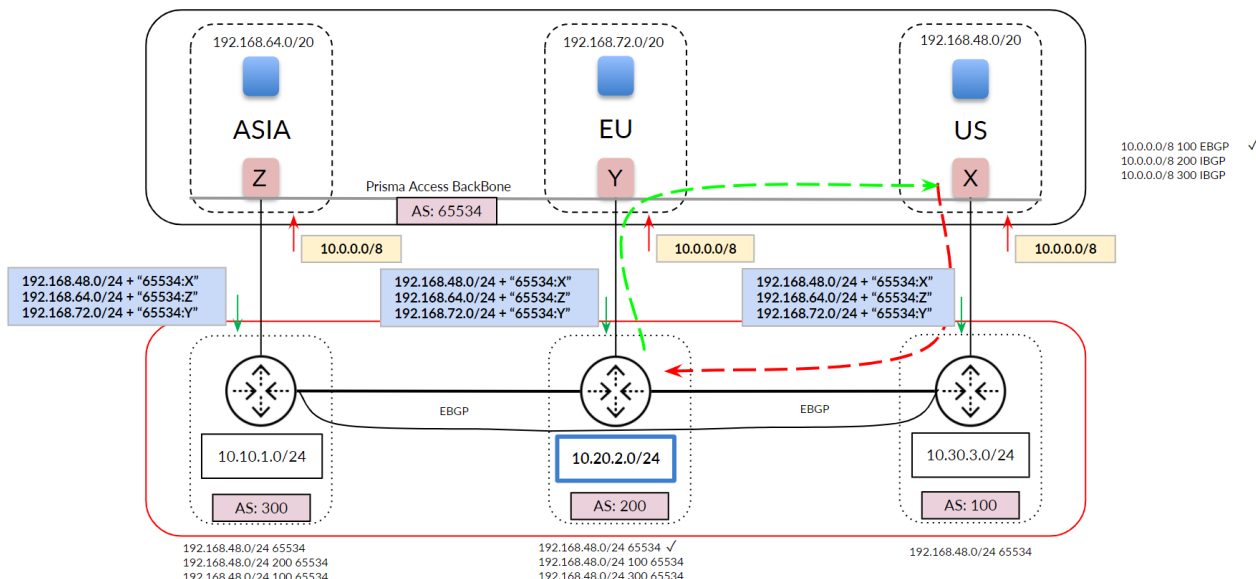
In deployments with a full-mesh eBGP backbone, asymmetry can arise when Prisma Access cannot reach a particular data center due to an ISP/CPE failure at the customer's data center. The following figure shows what could happen when the link to the EU service connection goes down. Your network detects the link failure and builds a new route table for AS 200. Traffic from the US service connection to AS 200 uses the path through AS 100 because the eBGP route for your backbone between AS 200 and AS 100 is preferred to the iBGP route between service connections EU and US. However, return traffic is not guaranteed through the same path because the on-premises CPE can choose either path (shown in red) to return the traffic.



The previous examples show a network whose routes have not been aggregated (that is, you have not performed route summarization before you send the BGP route advertisements to Prisma Access). The following example shows a network that summarizes its routes to 10.0.0.0/8 before sending to Prisma Access. If you select default routing, this configuration can lead to asymmetric routing issues, because Prisma Access cannot determine the correct return path from the summarized routes.



If your Prisma Access deployment has Remote Networks, Palo Alto Networks does not recommend the use of route summarization on Service Connections. Route summarization on service connections is for Mobile Users deployments only.



If you use route aggregation for mobile users, we strongly recommend that you enable [hot potato routing](#) instead of default routing, where Prisma Access hands off the traffic as quickly as possible to your organization’s network; in addition, we recommend that you select a **Backup SC** as described in the following section for each service connection to have a deterministic routing behavior.

## Hot Potato Routing

When you select **Hot Potato Routing**, Prisma Access egresses the traffic bound to service connections/data centers from its internal network as quickly as possible.

With hot potato routing, Prisma Access prepends the AS path (AS-PATH) to the BGP prefix advertisements sent from gateways. This prepending is performed when the prefixes are advertised out of the service connection to your organization’s on-premises CPE. Prisma Access prepends the AS-PATHs so that your CPE gives the correct preference to the primary and secondary tunnels, so that if the primary tunnel goes down, your CPE chooses the secondary tunnel as the backup.

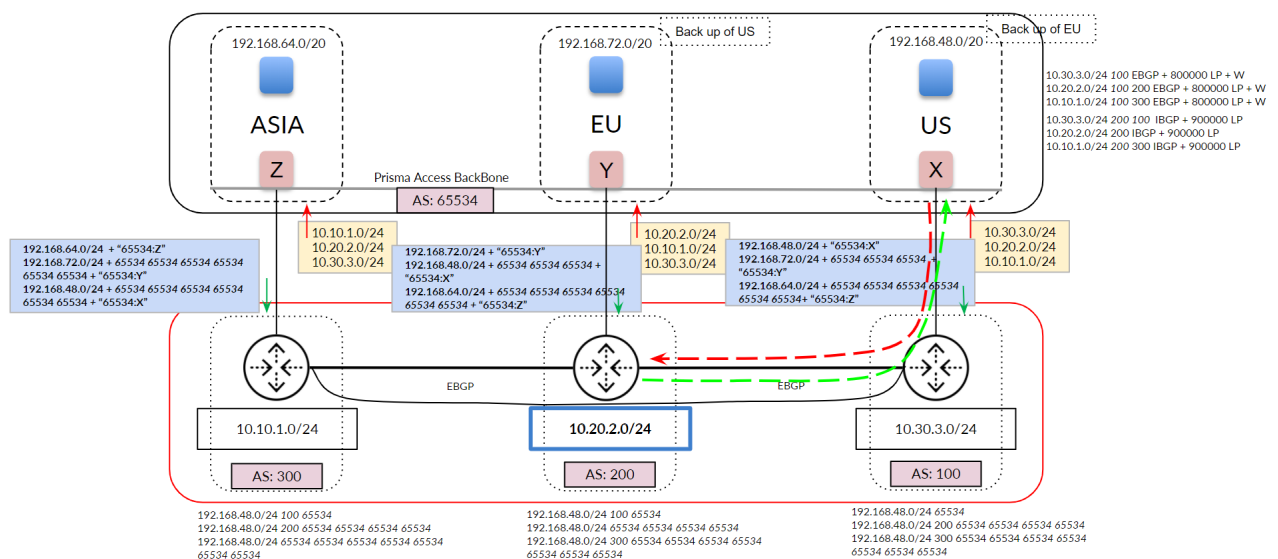
If you specified a different IP address for the secondary (backup) BGP peer, Prisma Access adds more prepends based on the tunnel type, as shown in the following table.

Prefix Type	Service Connection Tunnel Type	Number of As-Path Prepends	Total AS-PATHs Seen on the CPE
Gateway prefixes from primary service connection	Primary or Secondary tunnel with the same BGP peer IP address	0	1
Gateway prefixes from backup service connection	Primary or Secondary tunnel with the same BGP peer IP address	3	4
Gateway prefixes from all other service connections	Primary or Secondary tunnel with the same BGP peer IP address	6	7

Prefix Type	Service Connection Tunnel Type	Number of As-Path Prepends	Total AS-PATHs Seen on the CPE
Gateway prefixes from primary service connection	Secondary tunnel with a different BGP peer IP address	1	2
Gateway prefixes from backup service connection	Secondary tunnel with a different BGP peer IP address	4	5
Gateway prefixes from all other service connections	Secondary tunnel with a different BGP peer IP address	7	8

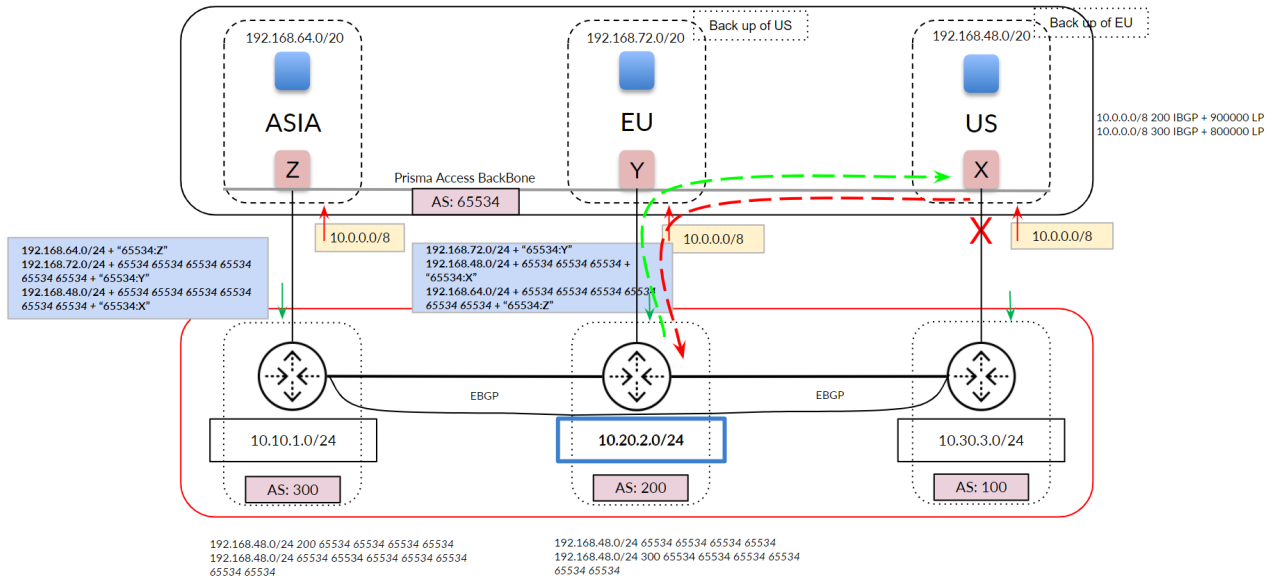
In hot potato routing mode, Prisma Access allows you to specify a backup service connection (**Backup SC**) during onboarding. Specifying a **Backup SC** informs Prisma Access to use that service connection as the backup when a service connection link fails.

The following figure shows a hot potato routing configuration for traffic between the US service connection and AS 200, with the EU service connection configured as the **Backup SC** of the US connection. Using hot potato routing, Prisma Access sends the traffic from its closest exit path through the US service connection. The return traffic takes the same path through AS100 because this path has a shorter AS-PATH to the mobile user pool in the US location. Prisma Access prepends the AS-PATH to its prefix advertisements depending on whether the tunnel is a primary tunnel, a backup tunnel, or not used for either primary or backup.

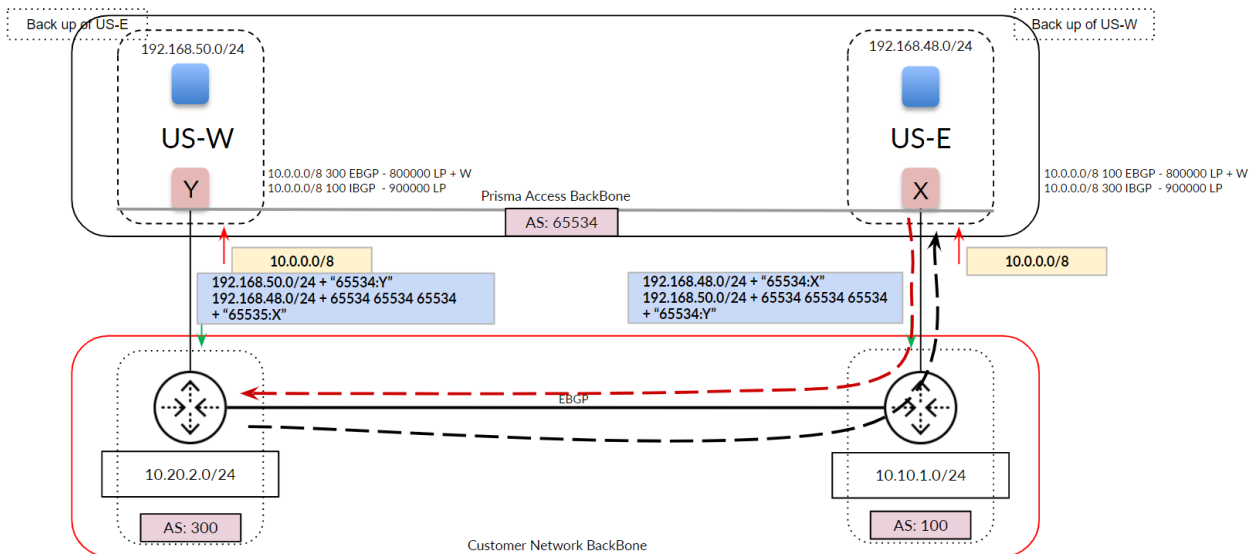


Because you have set up a backup service connection, if the link to the US service connection goes down, hot potato routing sends the traffic out using its shortest route through the EU service connection. This routing scenario also applies to networks that use route aggregation.





You can also use backup service connections for multiple service connections in a single region. The following figure shows a Prisma Access deployment with two service connections in the North America region. In this case, you specify a **Backup SC** of US-E for the US-W service connection, and vice versa, to ensure symmetric routing.



## Configure Routing Preferences

To enable routing preferences, complete the following steps.

- To change the routing defaults, choose between **Default** and **Hot Potato Routing** when you [configure the Service Setup](#) for service connections.
- To specify a preferred service connection to use if a link fails, configure a **Backup SC** when you [create a service connection](#).

---

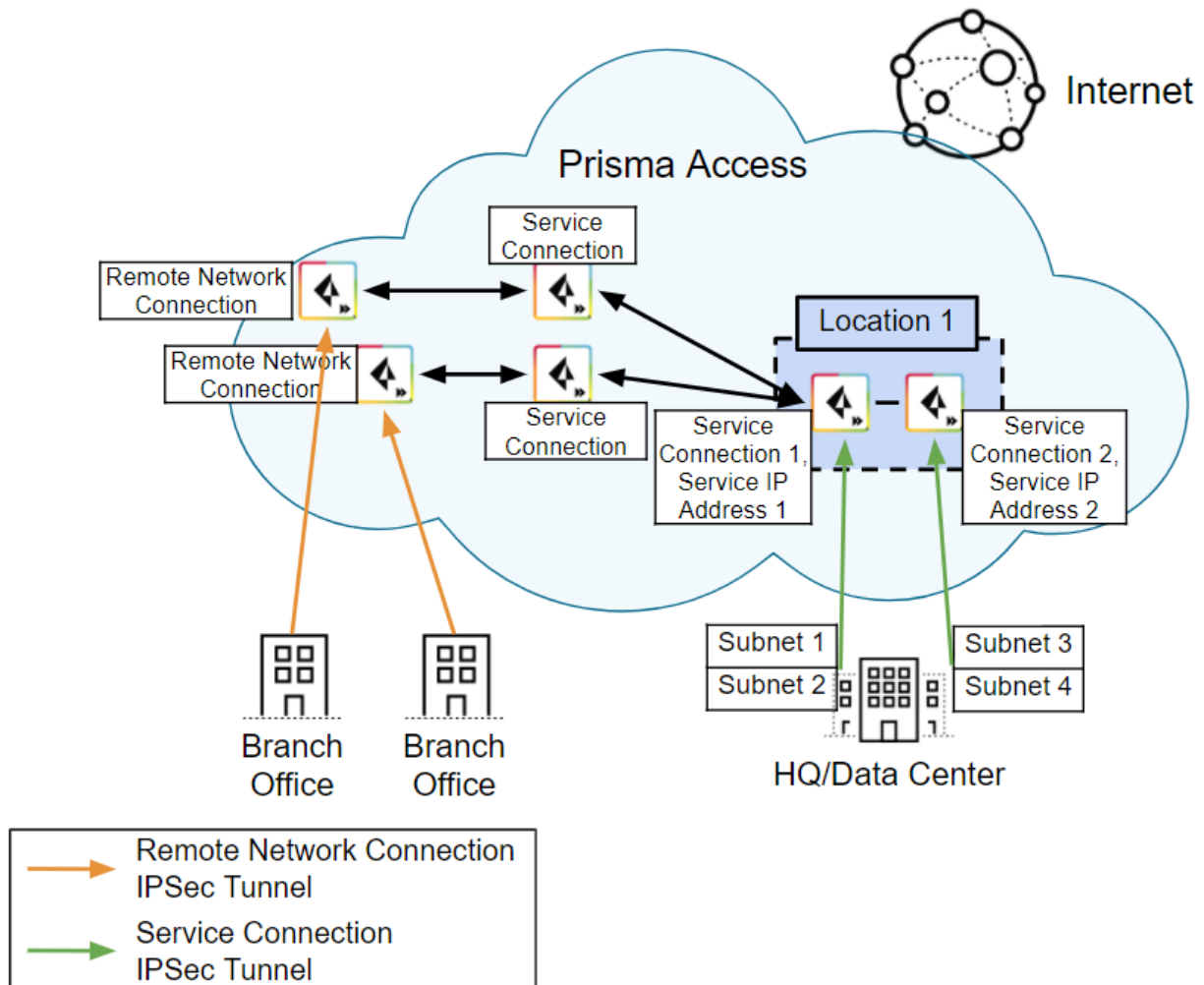
# Create a High-Bandwidth Network Using Multiple Service Connections

If you have a headquarters or data center location that requires additional service connection bandwidth, you can configure multiple service connections to that location by completing the following workflow.


Each Prisma Access service connection is not bandwidth capped, but Palo Alto Networks expects that each service connection can provide approximately 1 Gbps of throughput. While this bandwidth is usually sufficient to access internal resources in a headquarters or data center location, you might have a deployment that requires additional bandwidth; for example, if you are hosting an internal or private SaaS application in a data center.

To create a high-bandwidth service connection to a headquarters or data center site, you onboard the site using multiple service connections to the same Prisma Access location. The following diagram shows a Prisma Access remote network deployment with a headquarters or data center site that has two service connections from the same Prisma Access location, effectively providing 2 Gbps of bandwidth between the site and the Prisma Access location.

In addition to the service connections being deployed for high-bandwidth access, the diagram shows another set of service connections. These service connections provide normal routing functions for Prisma Access (in this diagram, they provide internal routing access between the remote network connections and the high-bandwidth service connections). Palo Alto Networks recommends that, when you deploy a high-bandwidth connection, you reserve service connections to provide access to the resource in the headquarters or data center location only, and deploy additional service connections to use for internal routing between remote networks, mobile users, and the resources in the data center.



Each service connection is active and has its own **Service IP Address**; you use that address to terminate the IPsec tunnel for each service connection. Prisma Access does not limit the maximum number of service connections you can onboard to a single headquarters or data center remote network location.

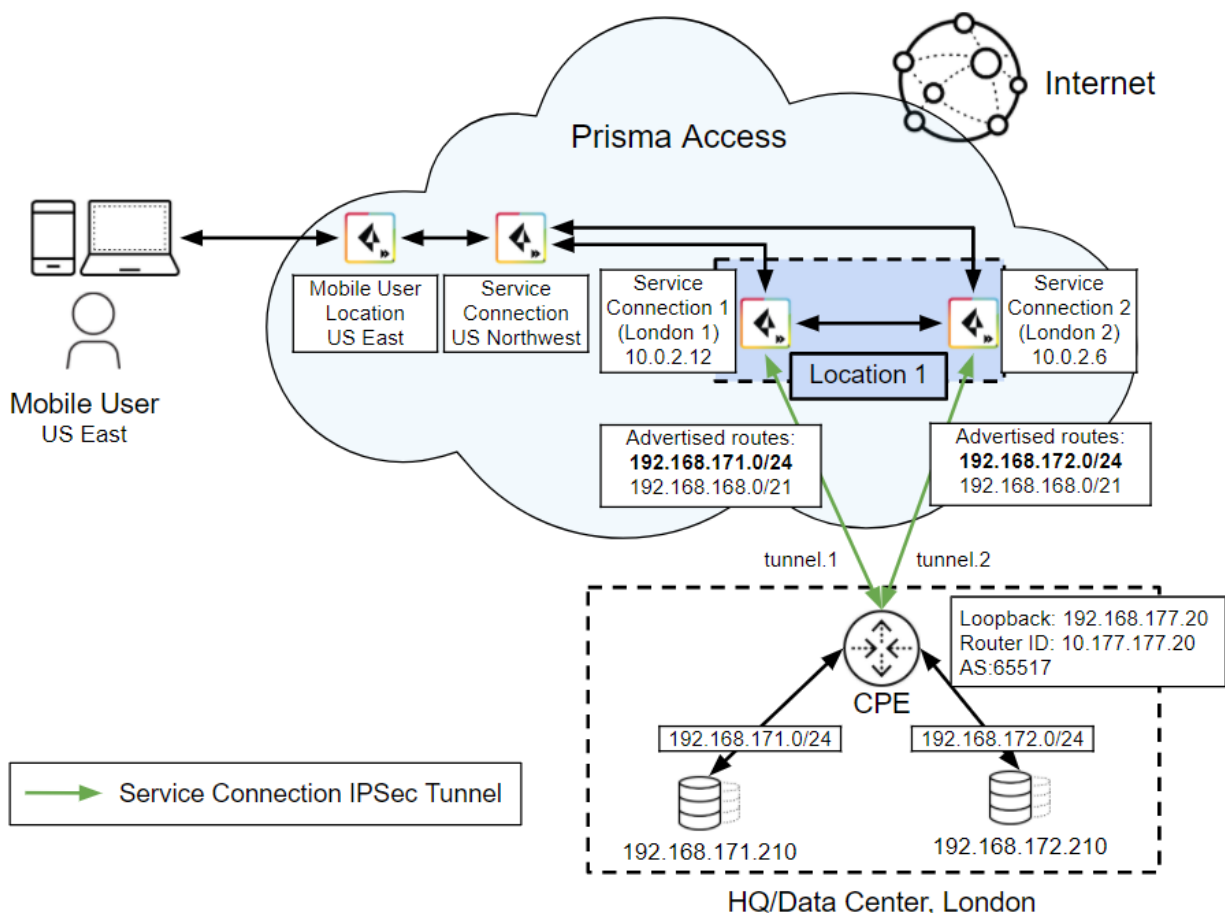
 While each service connection provides approximately 1 Gbps of throughput, the actual throughput is dependent on several factors, including:

- Traffic mix (for example, frame size)
- Latency and packet loss between the service connection and the headquarters location or data center
- Service provider performance limits
- Customer termination device performance limits
- Other customer data center traffic


## Create a High-Bandwidth Connection to a Headquarters or Data Center Location

To configure multiple service connections to a single headquarters or data center location, complete the following steps.

The steps in this section use a deployment example as shown in the following diagram. In this example, the London headquarters location connects to two different service connections (London 1 and London 2) using two different IPsec tunnels that are terminated on two different customer premises equipment (CPE) interfaces (tunnel.1 and tunnel.2).



This example, and the steps in this section, use a next-generation firewall to terminate the service connections on the CPE; however, you can use any CPE that supports symmetric routing and PBF or policy-based routing as the CPE.

 Use these steps for guidance; each use case could require additional design and planning that are beyond the scope of this document.

**STEP 1 |** Before you deploy multiple service connections from a single Prisma Access location to a single site, make sure that your network has the following prerequisites:

- You must divide the subnets in the headquarters or data center location and advertise a unique subnet on each service connection.
- Your customer premises equipment (CPE) must support, and you must be able to configure, the following networking features:
  - **Policy-based forwarding (PBF)** or policy-based routing—Your CPE must be able to selectively pick a specific path for a specific local source IP address and subnet.
  - **Symmetric return**—You must be able to configure your CPE to ensure symmetric traffic flows to and from a specific IP address and subnet, and configure symmetric return for failover tunnels if one of the tunnels goes down.

**STEP 2 |** Create the service connections and establish connectivity for the IPsec tunnels used for the service connections.

1. On the Panorama that manages Prisma Access, [Create a service connection](#), including creating a new [IPsec Tunnel](#) configuration, [IKE Gateway](#), [IPsec Crypto Profile](#), and [Tunnel Monitoring](#) settings.



*Prisma Access offers predefined IPsec templates that you can use to simplify the IPsec tunnel creation process.*

2. Find the IP address to use as the remote side of the IPsec tunnel from your CPE to Prisma Access by selecting **Panorama > Cloud Services > Status > Network Details**, clicking the **Service Connection** radio button, and noting the **Service IP Address** for the site.

Name	Service IP Address	User-ID Agent Address	Local IP Address	Static Subnet	EBGP Router	Branch AS and Router
			dynamic			

3. On your CPE, create an IPsec tunnel to the service connections
  1. Verify that the IKE and IPsec tunnels use the same cryptographic profiles for authentication and encryption between the peers.
  2. Use the **Service IP Address** as the peer address for the tunnel.

If you use a next-generation firewall as the CPE, select **Network > IPsec Tunnels** and create two tunnels for the service connections (**tunnel.1** and **tunnel.2** in the following screenshot).

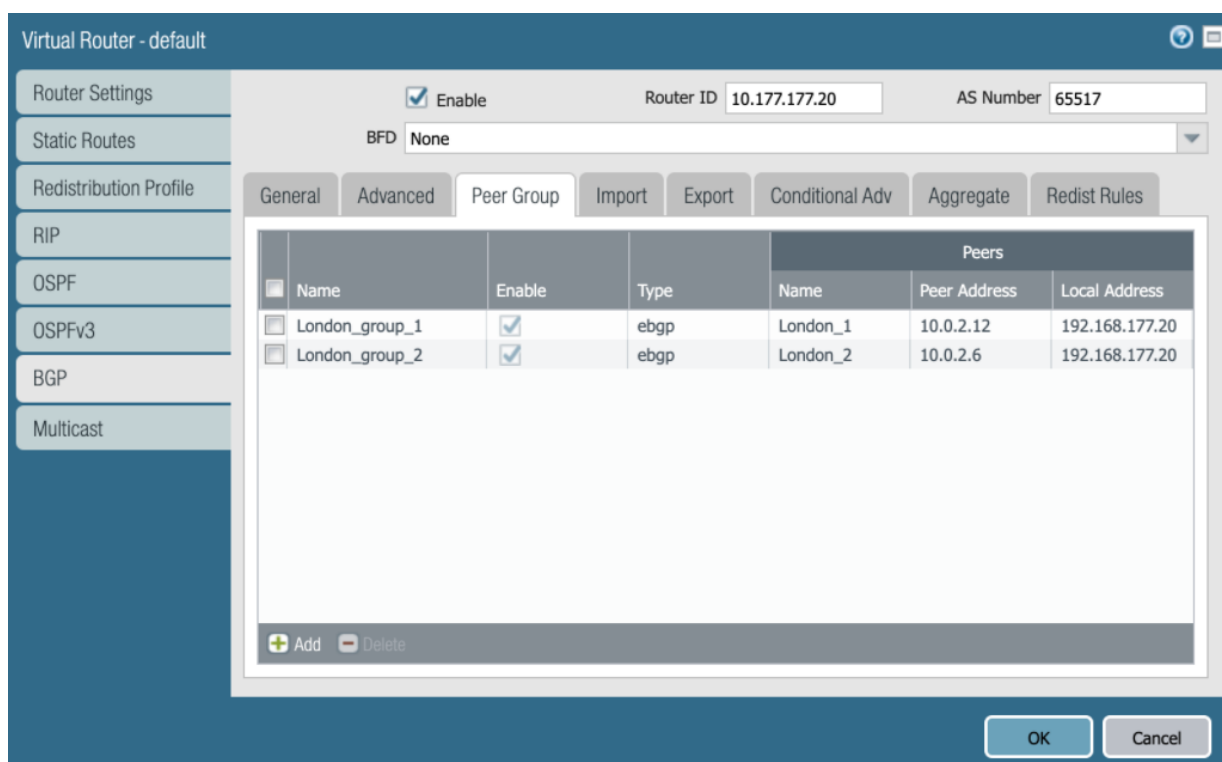
Name	Status	Type	IKE Gateway/Satellite				Tunnel Interface				
			Interface	Local IP	Peer Address	Status	Interface	Virtual Router	Virtual System	Security Zone	Status
London_1	●	Auto Key	ethernet1/1			● IKE Info	tunnel.1	default (Show Routes)	vsys1	Private	●
London_2	●	Auto Key	ethernet1/1			● IKE Info	tunnel.2	default (Show Routes)	vsys1	Private	●

**STEP 3 |** Create virtual router settings for the CPE.

You create BGP routing instances that advertise one subnet on one tunnel and the other subnet on another tunnel, which ensures load balancing on the two active tunnels.

If you are using a next-generation firewall as the CPE, select **Network > Virtual Routers**, **Add** virtual router settings, then **Add a BGP Peer Group** for each tunnel, specifying the following settings:

- Specify a **Router ID** and **AS Number** of the CPE router (10.177.177.20 and 65517, respectively, in this example).
- Specify the **EBGP Router** address of the service connections (**Panorama > Cloud Services > Status > Network Details > Service Connection > EBGP Router**) as the **Peer Address** for the service connections (10.0.2.12 for Service Connection 1 and 10.0.2.6 for Service Connection 2 in this example).
- For the **Local Address**, you can specify the loopback address of the CPE (192.168.177.20 in this example).



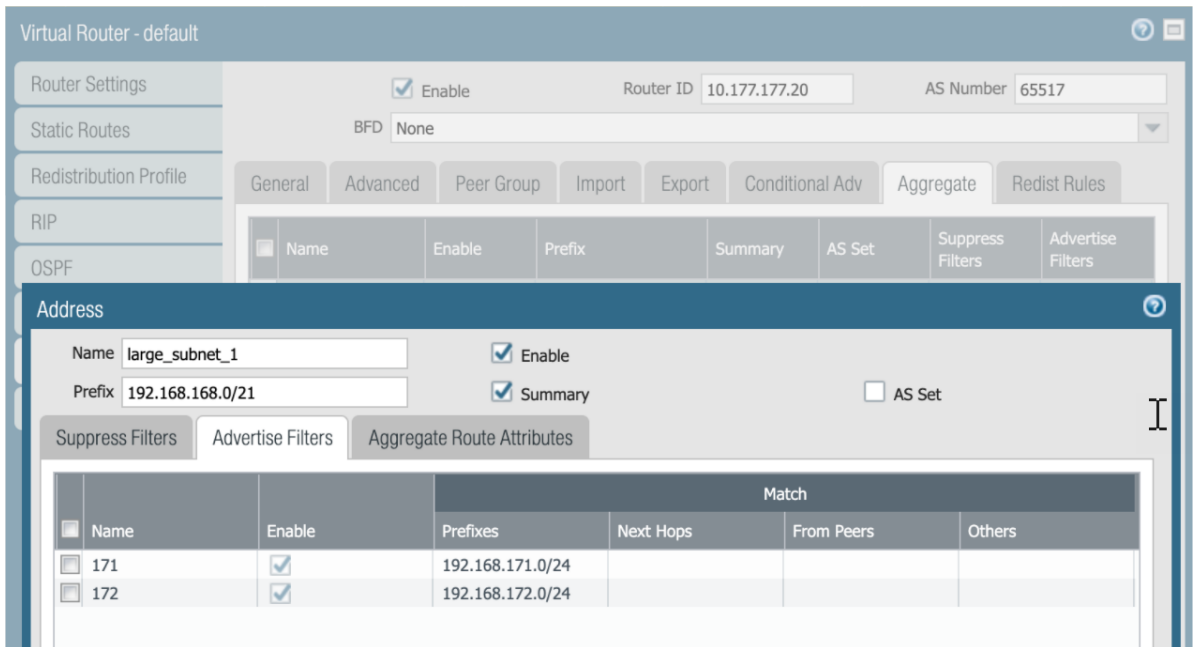
#### STEP 4 | Create a summarized subnet for the IP addresses used for both tunnels.

Providing a summarized subnet guarantees redundancy. When both tunnels are up, the traffic uses the most specific routes to reach their destination; for example, 192.168.171.0/24 uses tunnel.1 to reach its destination. Adding a summarized subnet that covers all advertised subnets (192.168.168.0/21 in this example) ensures that traffic from 192.168.171.0/24 is reachable from tunnel.2 if tunnel.1 goes down and traffic from 192.168.172.0/24 is reachable from tunnel.1 if tunnel.2 goes down.

If you are using a next-generation firewall as the CPE, complete the following steps.

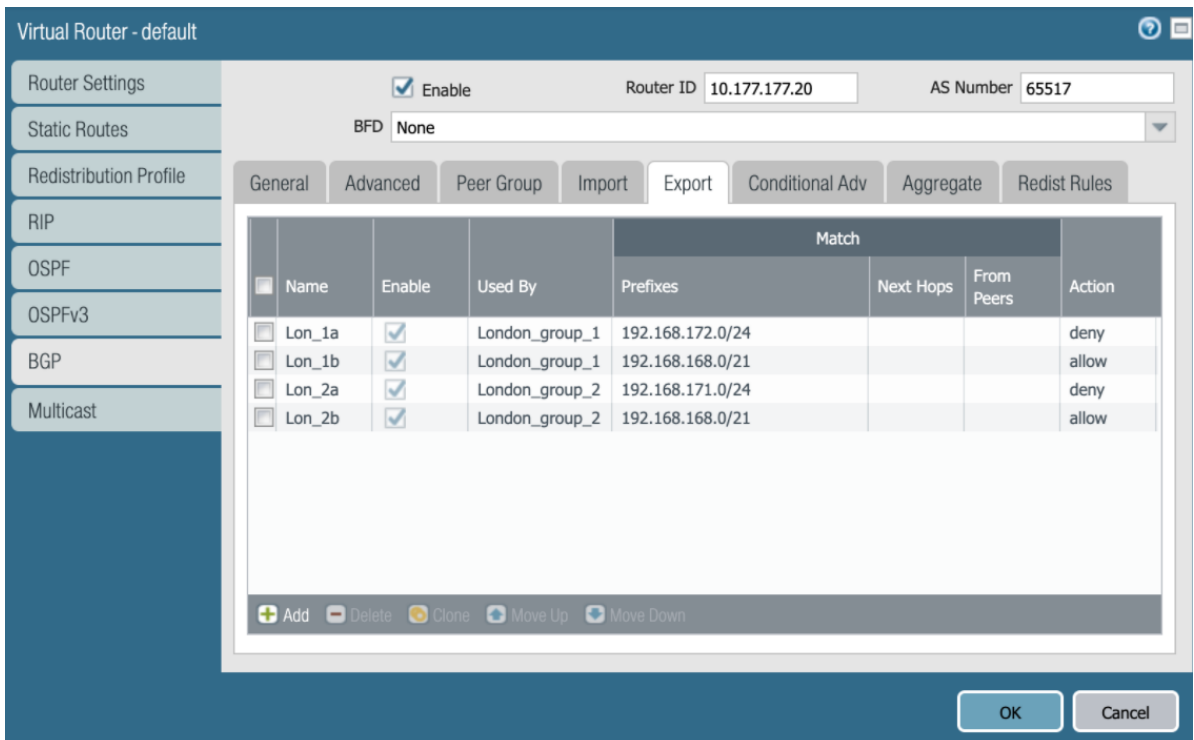
1. Continue to modify the virtual router profile and **Add** route aggregation parameters (**Network > Virtual Routers > BGP > Aggregate**).
2. Enter summary subnets for the subnets you are advertising for the service connections.

In this example, enter a **Prefix** of **192.168.168.0/21**, which summarizes the two data center subnets.



3. Enter **Export** settings to ensure that the tunnels advertise the correct subnets.

In this example, you specify an **Action** of **deny** and **allow** for the subnets so that the first subnet (192.168.171.0/24) is reachable from tunnel.1 and the second subnet (192.168.172.0/24) is reachable from tunnel.2.

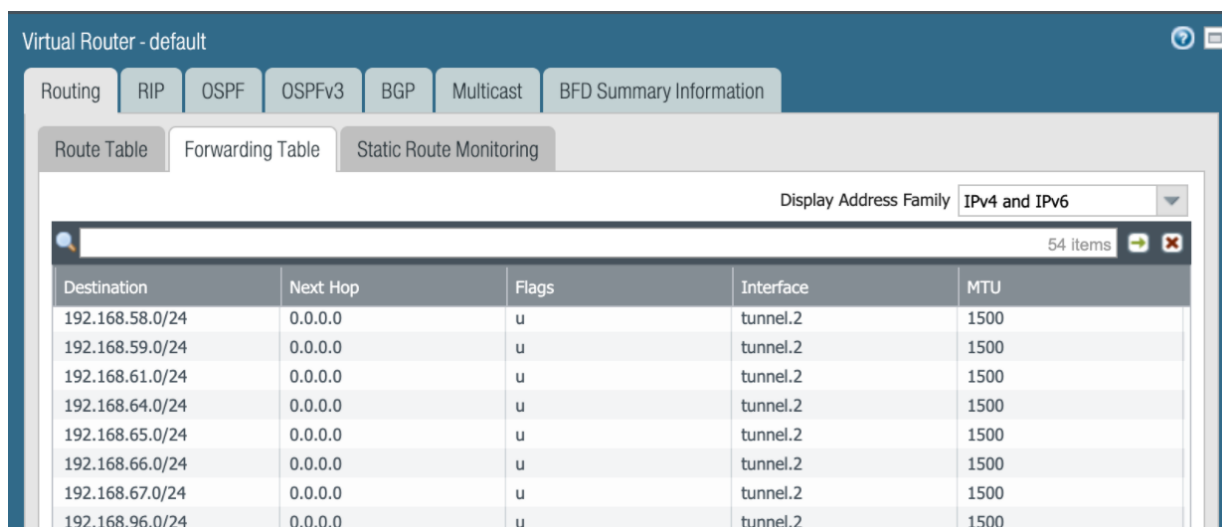


**STEP 5 | (Deployments with more than two service connections only)** If you require more than two service connections to connect the users to private resources for more than 2 Gbps bandwidth, add AS-PATH prepends for the exported routes so that the service connections use symmetric

routing to and from the data center in the event of a failover. See [Configure More than Two Service Connections to a Headquarters or Data Center Location](#) for details.

**STEP 6 |** To ensure symmetric return (to make sure that traffic from 192.168.171.0/24 always uses tunnel.1 and traffic from 192.168.172.0 always uses tunnel.2), enter PBF or policy-based routing rules.

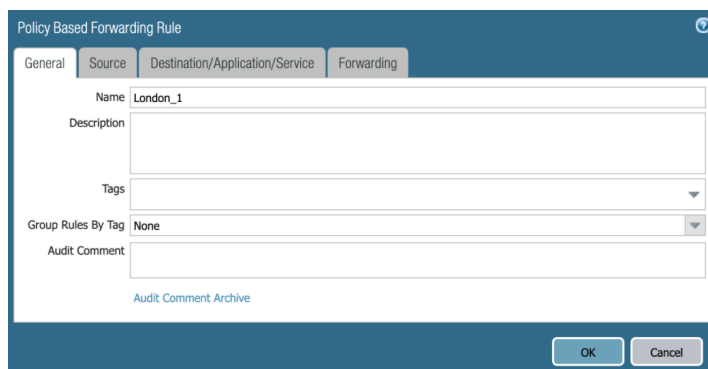
By default, BGP installs routes in the routing table for all different destinations regardless of the preferred tunnel. The following screenshot shows that BGP advertises all destinations from the 192.168.168.0/21 subnet for tunnel.2, which might cause asymmetric routing for traffic from 192.168.171.0/24.



Destination	Next Hop	Flags	Interface	MTU
192.168.58.0/24	0.0.0.0	u	tunnel.2	1500
192.168.59.0/24	0.0.0.0	u	tunnel.2	1500
192.168.61.0/24	0.0.0.0	u	tunnel.2	1500
192.168.64.0/24	0.0.0.0	u	tunnel.2	1500
192.168.65.0/24	0.0.0.0	u	tunnel.2	1500
192.168.66.0/24	0.0.0.0	u	tunnel.2	1500
192.168.67.0/24	0.0.0.0	u	tunnel.2	1500
192.168.96.0/24	0.0.0.0	u	tunnel.2	1500

To ensure symmetric routing, configure a set of **PBF** or route-based forwarding rules. If you are using a next-generation firewall as the CPE, complete the following steps.

1. Select **Policies > Policy Based Forwarding** and **Add** a PBF policy rule.



Policy Based Forwarding Rule

General | Source | Destination/Application/Service | Forwarding

Name: London\_1

Description:

Tags:

Group Rules By Tag: None

Audit Comment:

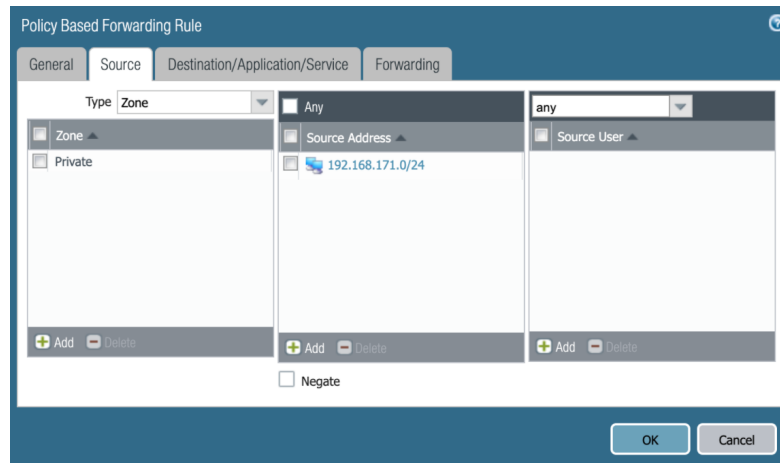
Audit Comment Archive

OK Cancel

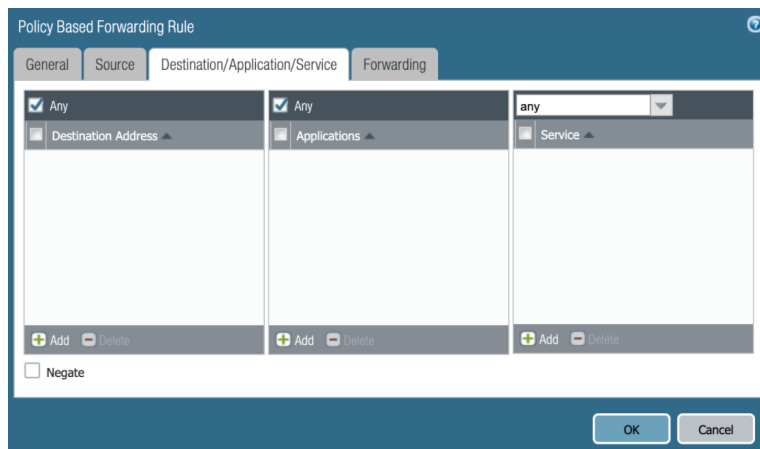
2. Select **Source** and **Add** a **Source Address** to use for the PBF.

In this case, you want to create a PBF for tunnel.1, so you enter the 192.168.171.0/24 subnet.





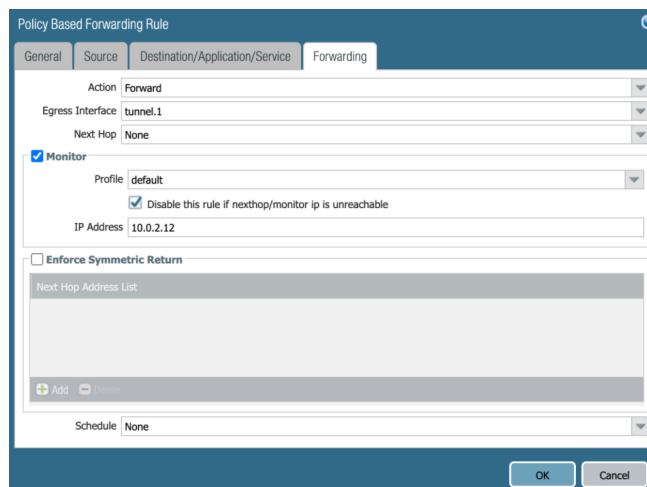
3. Select **Destination/Application/Service** and select **Any** Destination Address and **Any** application.



4. Select **Forwarding** and specify the following parameters; then, click **OK**:

- Select an **Action** of **Forward**.
- Select an **Egress Interface** of the tunnel to which you want to forward the IP subnet (**tunnel.1** in this case).
- Select **Monitor** and select the following monitoring profiles:
  - Select a **Profile** of **default**.
  - Select **Disable this rule if nexthop/monitor ip is unreachable**.
  - Specify an **IP Address** of the service connection's **EBGP Router** address (**Panorama > Cloud Services > Status > Network Details > Service Connection > EBGP Router**).

Enabling monitoring and selecting the EBGP router address of the service connection ensures that, if tunnel.1 goes down, the firewall disables the PBF policy and routes the traffic on the tunnel that is still up (tunnel.2).



- Repeat Step 6, substituting the **EBGP Router** address of Service Connection 1 with the **EBGP Router** address of Service Connection 2 and the subnet of tunnel.1 with the subnet of tunnel.2.

When complete, you have two PBF policies, one for tunnel.1 and one for tunnel.2.

Name	Tags	Zone/Interface	Source Address	User	Destination Address	Application	Service	Action	Egress I/F
1 London_1	none	Private	192.168.171.0/24	any	any	any	any	forward	tunnel.1
2 London_2	none	Private	192.168.172.0/24	any	any	any	any	forward	tunnel.2

**STEP 7 |** Select **Network > Virtual Routers > Static Routes** and assign the **EBGP Router** address of Service Connection 1 to the **Interface** of **tunnel.1**; then, assign the **EBGP Router** address of Service Connection 2 to the **Interface** of **tunnel.2**

Entering specific static routes for each of the router BGP addresses ensures that tunnel monitoring functions correctly, because the EBGP Router IP address of Service Connection 1 is reachable only by tunnel.1 and the EBGP Router IP address of Service Connection 2 is reachable only by tunnel.2.

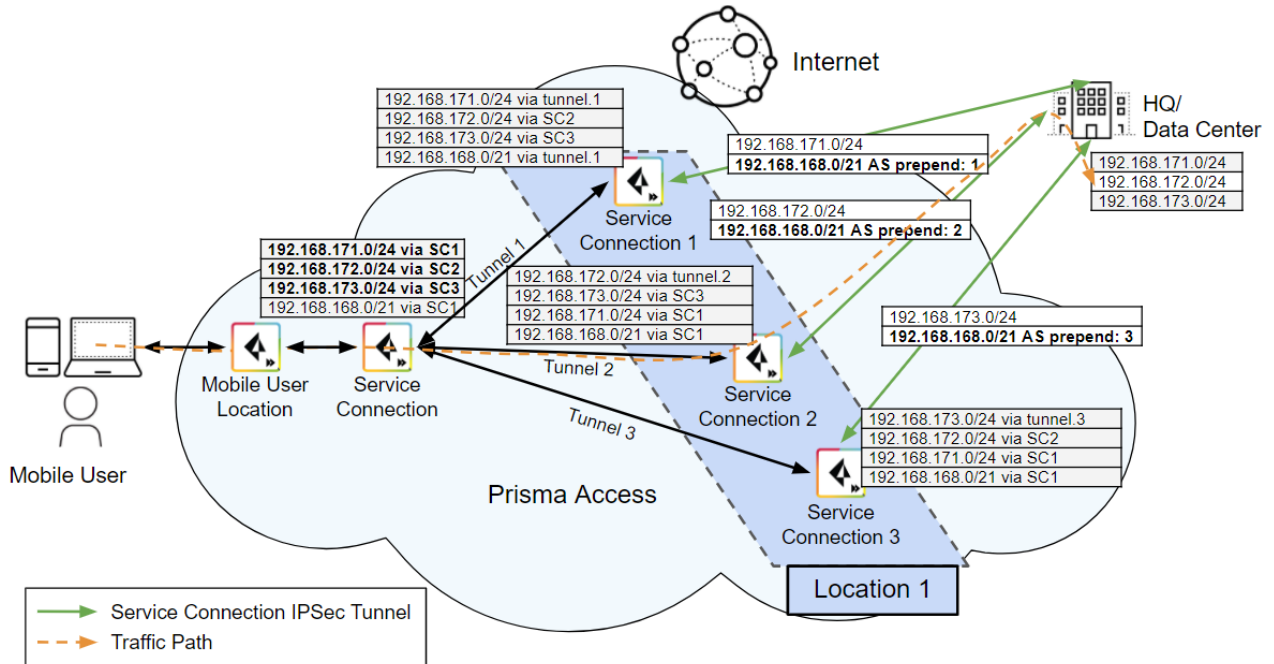
Name	Destination	Interface	Type	Value
ipsec_1		ethernet1/1	ip-address	192.168.173.1
ipsec_2		ethernet1/1	ip-address	192.168.173.1
bgp_1	10.0.2.12/32	tunnel.1		
bgp_2	10.0.2.6/32	tunnel.2		

## Configure More than Two Service Connections to a Headquarters or Data Center Location

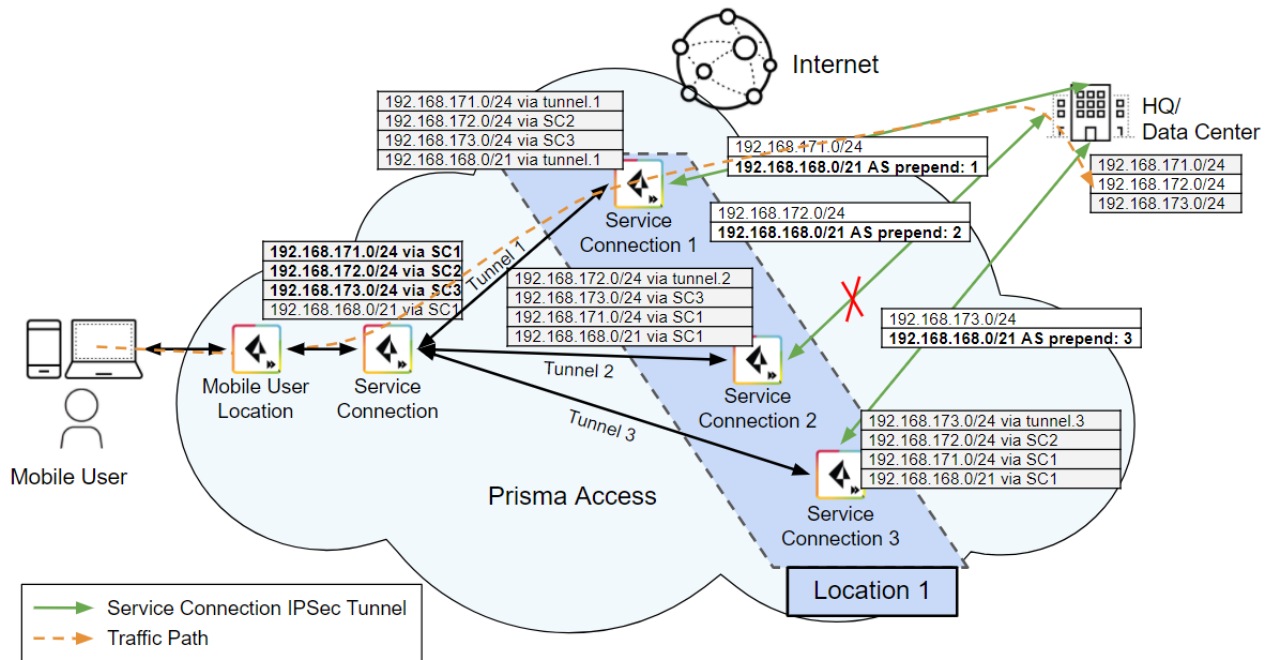
When you use two tunnels for a high-bandwidth service connection, there is only one traffic path left available in case of a tunnel failure, which simplifies the configuration of a failover path. If you use more than two connections for a high-bandwidth connection, you need to perform additional configuration to ensure a consistent behavior for tunnel failovers.

Because you use a summarized subnet for tunnel failover, you need to explicitly state the service connection tunnel to use if a failover occurs. Since BGP routing chooses the shortest number of AS-PATHS for a route, you can prepend AS-PATHS to routes to have BGP prefer a tunnel in the case of a failover.

The following example shows routing tables for a high-bandwidth service connection using three service connections. If all three tunnels are up, Prisma Access uses the more specific routes to reach the subnets in the headquarters or data center location. Since the user is accessing a resource in the 192.168.172.0/24 subnet, the service connection closest to the mobile user checks its routing table and selects Tunnel 2 as the path to the data center resource.



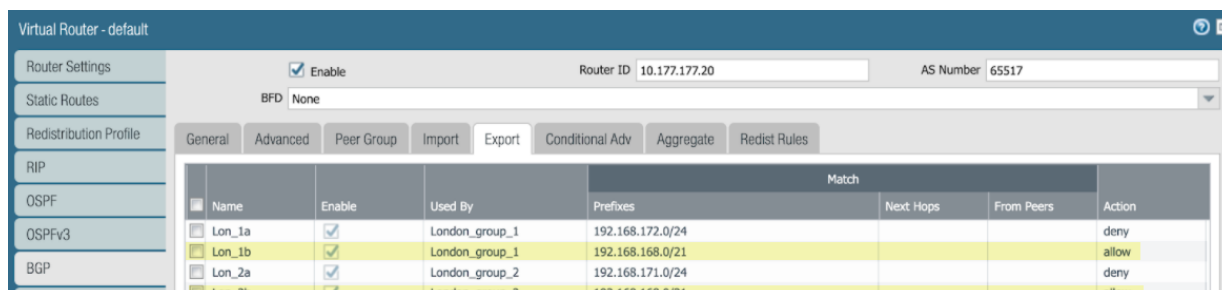
If Tunnel 2 goes down, the more specific route to the resource in the 192.168.172.0/24 subnet is not available, so the service connection closest to the user uses the summarized 192.168.168.0/21 subnet. You have configured only one AS-PATH prepend for Service Connection 1; therefore, Prisma Access chooses Tunnel 1 as the failover path because it has fewer AS-PATH prepends.



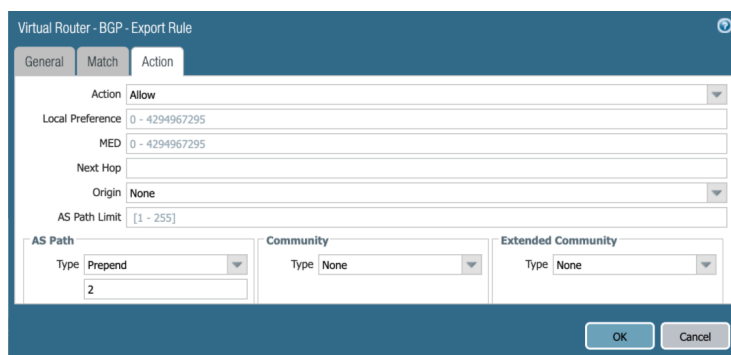
To add preponds to routes if you are using a next-generation firewall as the CPE, complete the following task.

**STEP 1** | Select the virtual router BGP export profiles (**Network > Virtual Routers > BGP > Export**).

**STEP 2** | Modify the export rule you created when you [configured the service connections](#) that has an **Action of Allow**.



**STEP 3** | In the AS Path area, add a **Prepend**, then enter the number of AS-PATH preponds to add (**2** in this example).



**STEP 4** | Repeat Steps 2 and 3 for each export rule that has an **Action of Allow**, adding AS-PATH preponds to match the failover scenarios you have planned for your deployment.

In the examples used in this section, you add an AS-PATH prepend of 1 for the tunnel to the data center location for Service Connection 1 (tunnel.1), an AS-PATH prepend of 2 for the tunnel used for Service Connection 2 (tunnel.2), and an AS-PATH prepend of 3 for the tunnel used for Service Connection 3 (tunnel.3).

When complete, this example uses the following tunnels in the event of a failover:

- If tunnel.2 or tunnel.3 goes down, the traffic for the corresponding subnet fails over to tunnel.1, which has the shortest advertised AS-PATH.
- If tunnel.1 goes down, the traffic for its subnet (192.168.171.0/24) fails over to tunnel.2, which has the shortest advertised AS-PATH.

**STEP 5** | Add backup PBF or policy-based routing policies to ensure symmetric return traffic in the event of a tunnel failure.

While the AS-PATH preponds ensure that the traffic from Prisma Access to the data center uses a specific tunnel in the event of a failover, you must also ensure a symmetric return path for the traffic from the data center to Prisma Access. To ensure symmetric return, use PBF or policy-based routing policies that mirror the failover scenarios you created for traffic from Prisma Access to the data center.

In this example, for tunnel.1 traffic that has a source IP of 192.168.171.0/24, you create a backup PBF Policy that forces return traffic to use tunnel.2 in the event of a failover. The first PBF rule becomes

disabled if the tunnel monitor IP address is not reachable; when this failover occurs, the CPE (a next-generation firewall in this example) evaluates the next rule in the list.

		Source			Destination					
	Name	Tags	Zone/Interface	Address	User	Address	Application	Service	Action	Egress I/F
1	London_1	none	Private	192.168.171.0/24	any	any	any	any	forward	tunnel.1
2	London_1_backup	none	Private	192.168.171.0/24	any	any	any	any	forward	tunnel.2

You then add more PBF rules to match the failover scenarios you created for traffic from Prisma Access to the data center.

		Source			Destination					
	Name	Tags	Zone/Interface	Address	User	Address	Application	Service	Action	Egress I/F
1	London_1	none	Private	192.168.171.0/24	any	any	any	any	forward	tunnel.1
2	London_1_backup	none	Private	192.168.171.0/24	any	any	any	any	forward	tunnel.2
3	London_2	none	Private	192.168.172.0/24	any	any	any	any	forward	tunnel.2
4	London_2_backup	none	Private	192.168.172.0/24	any	any	any	any	forward	tunnel.1
5	London_3	none	Private	192.168.173.0/24	any	any	any	any	forward	tunnel.3
6	London_3_backup	none	Private	192.168.173.0/24	any	any	any	any	forward	tunnel.1

---

# List of Prisma Access Locations

The following table lists the available locations for Prisma Access.

The locations are sorted by an alphabetical list, by compute locations, and by regions as listed in the Cloud Service plugin in Panorama. When you onboard [service connections](#) or [remote network connections](#), the locations appear alphabetically in the drop-down. When you onboard [mobile users](#), the locations are sorted by region. If you are in North America, we provide a [map](#) you can use as a reference.

- [List of Locations by Compute Location](#)
- [List of Locations by Region](#)
- [Map of North America Locations](#)

## List of Locations by Compute Location

The following table shows the locations and their corresponding compute location.

Compute Location	Prisma Access Location
Asia Northeast	Japan Central
Japan South	Japan South
Asia South	Bangladesh India North India South India West Pakistan South Pakistan West
Asia Southeast	Cambodia Indonesia Malaysia Myanmar Philippines Singapore Thailand Vietnam
Australia Southeast	Australia East Australia Southeast Australia South New Zealand Papua New Guinea

Compute Location	Prisma Access Location
Bahrain	Bahrain
Belgium	Belgium
Canada Central	Canada Central Canada East
Europe Central	Andorra Austria Bulgaria Croatia Czech Republic Egypt Germany Central Germany North Germany South Greece Hungary Israel Italy Jordan Kenya Kuwait Liechtenstein Luxembourg Moldova Monaco Nigeria Poland Portugal Romania Saudi Arabia Slovakia Slovenia South Africa Central Spain Central Spain East

Compute Location	Prisma Access Location
	Turkey Ukraine United Arab Emirates Uzbekistan
Europe North	Belarus Finland Lithuania Norway Russia Central Russia Northwest Sweden
Europe Northwest	France South United Kingdom
Europe West	Denmark Netherlands Central Netherlands South
France North	France North
Hong Kong	Hong Kong
Ireland	Ireland
South Africa West	South Africa West
South America East	Argentina Bolivia Brazil Central Brazil East Brazil South Chile Ecuador Paraguay Peru Venezuela
South Korea	South Korea



Compute Location	Prisma Access Location
Switzerland	Switzerland
Taiwan	Taiwan
US Central	US Central US South
US East	US East US Northeast
US Northwest	Canada West US Northwest
US Southeast	Colombia Costa Rica Mexico Central Panama US Southeast
US Southwest	Mexico West US Southwest US West

## List of Locations by Region

The following table provides you with a list of locations separated by region.

Locations
<b>Africa Region</b>
Kenya
Nigeria
South Africa Central
South Africa West
<b>Asia Region</b>
Bangladesh
Cambodia
Hong Kong

---

## Locations

India North

India South

India West

Indonesia

Malaysia

Myanmar

Pakistan South

Pakistan West

Papua New Guinea

Philippines

Singapore

South Korea

Taiwan

Thailand

Vietnam

### **ANZ Region**

Australia East

Australia South

Australia Southeast

New Zealand

### **Europe Region**

Andorra

Austria

Belarus

Belgium

Bulgaria

---

---

## Locations

Croatia

Czech Republic

Denmark

Finland

France North

France South

Germany Central

Germany North

Germany South

Greece

Hungary

Ireland

Italy

Liechtenstein

Lithuania

Luxembourg

Moldova

Monaco

Netherlands Central

Netherlands South

Norway

Poland

Portugal

Romania

Russia Central

Russia Northwest

---

---

## Locations

Slovakia

Slovenia

Spain Central

Spain East

Sweden

Switzerland

UK

Ukraine

Uzbekistan

### **Japan Region**

Japan Central

Japan South

### **Middle East Region**

Bahrain

Egypt

Israel

Jordan

Kuwait

Saudi Arabia

Turkey

United Arab Emirates

### **North America Region**

Canada Central

Canada East

Canada West

Costa Rica

---

---

## Locations

Mexico Central

Mexico West

Panama

US Central

US East

US Northeast

US Northwest

US South

US Southeast

US Southwest

US West

### **South America Region**

Argentina

Bolivia

Brazil Central

Brazil East

Brazil South

Chile

Colombia

Ecuador

Paraguay

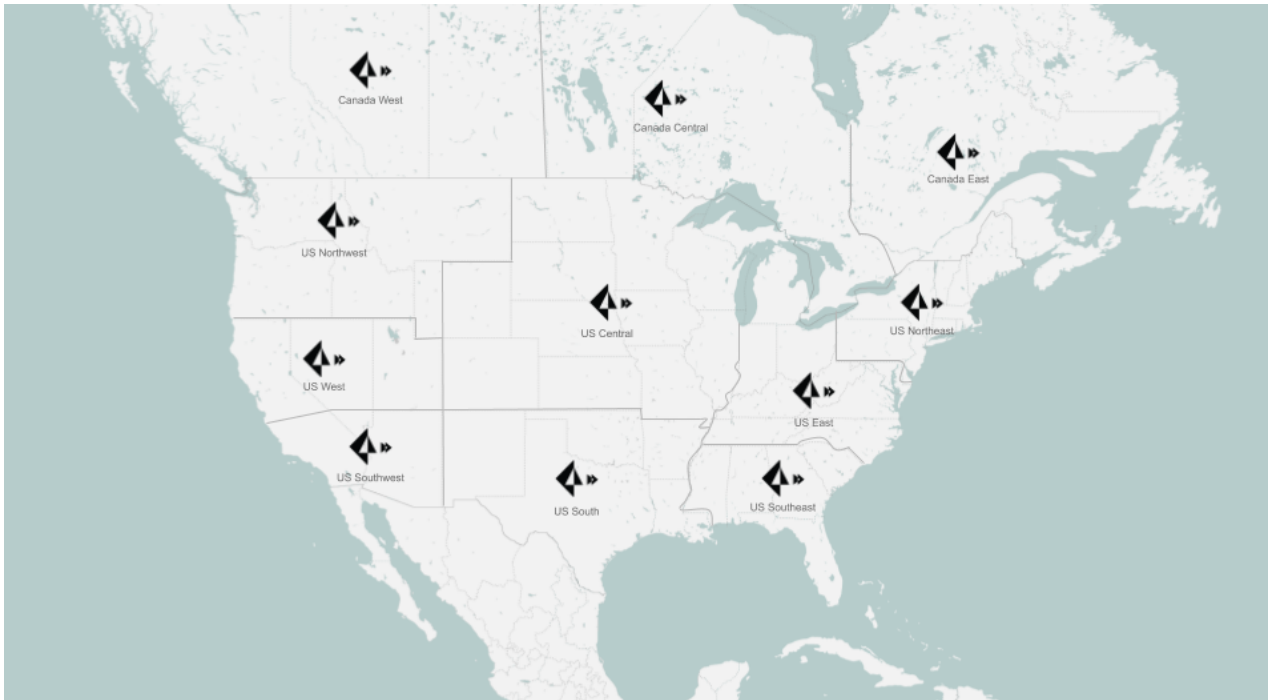
Peru

Venezuela

---

## Map of North America Locations

To assist you with onboarding service connections, remote networks, and mobile user locations in North America, use the following map as a reference.



# Secure Mobile Users with Prisma Access

Securing mobile users from threats and risky applications is often a complex mix of procuring and setting up the security and IT infrastructure and then ensuring bandwidth and uptime requirements in multiple locations around the globe while staying within your budget. Prisma Access allow you to secure mobile users using either GlobalProtect or an explicit proxy.

- > Plan To Deploy Prisma Access for Mobile Users
- > Secure Mobile Users With GlobalProtect
- > Secure Mobile Users with an Explicit Proxy
- > Zone Mapping
- > Specify IP Address Pools for Mobile Users
- > How the GlobalProtect App Selects a Prisma Access Location for Mobile Users
- > View Logged In User Information and Log Out Current Users
- > Quick Configs for Mobile User Deployments
- > Report Website Access Issues





---

# Plan To Deploy Prisma Access for Mobile Users

Prisma Access offers two connection methods to secure mobile users; you can [secure them using GlobalProtect](#) or [secure them using an explicit proxy](#). The following sections help you to choose which method works best for your deployment and provides you with a checklist to make sure that you have everything ready to deploy Prisma Access for mobile users.

- [Plan to Secure Mobile Users](#)
- [Secure Mobile Users with GlobalProtect](#)
- [Secure Mobile Users With an Explicit Proxy](#)
- [Supported Explicit Proxy Locations](#)

## Plan to Secure Mobile Users

This section provides the benefits of each connection method provided by Prisma Access for Users, as well as which connection method fits better in your deployment. If you determine that your deployment would benefit by having some users connect using GlobalProtect and some users connect using an explicit proxy, Prisma Access allows you to distribute the users in your GlobalProtect for Users license between Mobile Users—GlobalProtect and Mobile Users—Explicit Proxy. However, you cannot connect using GlobalProtect and an explicit proxy on the same endpoint.

- **Secure Mobile Users with GlobalProtect**—If your goal is to secure mobile users' access to all applications, ports, and protocols, and to get consistent security whether the user is inside or outside your network, use Mobile Users—GlobalProtect. The GlobalProtect infrastructure is deployed for you and scales based on the number of active users and their locations. After you complete the configuration, users then connect to the closest Prisma Access gateway (location) you have onboarded for policy enforcement. This enables you to enforce consistent security for your users even in locations where you do not have a network infrastructure and IT presence.

The GlobalProtect app installed on the users' endpoint secures users traffic to internet, SaaS applications, your internal and public cloud resources.

- **Secure Mobile Users with an Explicit Proxy**—If your organization has designed its network around an explicit proxy design, the explicit proxy connect method will help you quickly replace the existing method and move to the Prisma Access Secure Access Service Edge (SASE) solution. You can then send internet and external SaaS application traffic to the Prisma Access infrastructure and enforce security in the cloud.

With an explicit proxy, you configure a proxy URL and a Proxy Auto-Configuration (PAC) file. The GlobalProtect app is not required to be installed on the users' endpoints.

## Secure Mobile Users with GlobalProtect

If you use GlobalProtect to [GlobalProtect to secure mobile users](#), use the following checklist to ensure that you will be able to successfully enable the service and enforce consistent policy for your mobile users (protecting users with the GlobalProtect app installed on their endpoints and allowing users to securely access applications using [Clientless VPN](#)).

### ❑ Pre-Installation checklist:

- **IP address pool**—To configure Prisma Access for users, you need to provide an IP address pool that does not overlap with other IP addresses you use internally or with the IP address pool you designated for the [Infrastructure Subnet](#).



*We recommend using an RFC 1918-compliant IP address pool. While the use of non-RFC 1918-compliant (public) IP addresses is supported, we do not recommend it because of possible conflicts with internet public IP address space. In addition, do not specify any subnets that overlap with 169.254.169.253, 169.254.169.254, and the 100.64.0.0/10 subnet range because Prisma Access reserves those IP addresses and subnets for its internal use.*

Prisma Access uses this IP address pool to assign IP addresses to the virtual network adapters of endpoints when they connect to Prisma Access using the GlobalProtect app. Each device that connects to a Prisma Access mobile user gateway requires its own IP address. You specify the [IP address pools](#) that Prisma Access uses for the IP address allocation during the mobile user onboarding process. We recommend that the number of IP addresses in the pool is 2 times the number of mobile user devices that will connect to Prisma Access. If your organization has a bring your own device (BYOD) policy, or if a single user has multiple user accounts, make sure that you take those extra devices and accounts into consideration when you allocate your IP pools. If the IP address pool reaches its limit, additional mobile user devices will not be able to connect.

When mobile user devices connect to a gateway, Prisma Access takes IP addresses from the pools you specified and allocates them to the gateway in /24 blocks. When a /24 block reaches its limit as more user devices log in, Prisma Access allocates more /24 blocks from the pool to the gateway. Prisma Access [advertises these /24 subnets](#) into its backbone as they are allocated based on their gateway assignments.

- **Template**—The Prisma Access GlobalProtect deployment automatically creates a template stack and a top-level template. If you are already running GlobalProtect on premise and you want to leverage your existing configuration, you can add additional templates to the stack to push existing [GlobalProtect portal](#), [GlobalProtect gateway](#), [User-ID](#), [server profile](#) (for example, for connecting to your authentication service), [certificate](#), and [SSL/TLS service profile](#) configurations to Prisma Access for users. If you do not have templates with existing configuration settings, you can manually enter the required configuration settings when you [Secure Mobile Users With GlobalProtect](#). Additionally, any template(s) you add to the stack must contain the zone configuration for the zones you use to enforce Security policy for your mobile users.
- **Parent Device Group**—When you configure Prisma Access for users, you must specify a parent device group to use when you push your address groups and [Security policy](#), [Security profiles](#), other policy objects (such as application groups and objects), [HIP objects and profiles](#), and [authentication policy](#) that the service requires to enforce consistent policy for your remote users.
- **Locations to Onboard**—Prisma Access provides you with worldwide locations where you can [Secure Mobile Users With GlobalProtect](#). Before you onboard your locations, view [this list](#) to determine which locations you should onboard for your mobile users deployment.

Choose locations that are closest to your users or in the same country as your users. If a location is not available in the country where your mobile users reside, you can pick a location that uses the same language as your mobile users.

You can also divide the locations by geographical region. Keeping all locations in a single region allows you to [specify an IP address pool](#) for that region only, which can be useful if you have a limited number of IP addresses that you can allocate to the pool. A single regional IP address pool also provides more granular control over deployed regions and allows you to exclude regions as required by your policy or industry regulations.

If you have a Local license for Prisma Access for Users and you have a GlobalProtect deployment as well as an Explicit Proxy deployment, you can deploy a maximum of five locations for both deployments combined. You need to allocate the five locations between both deployments (for example, two locations for Mobile Users—GlobalProtect and three locations for Mobile Users—Explicit Proxy). If you have a Worldwide license, there are no restrictions for the maximum number of locations.

- **Portal Hostname**—Prisma Access for users enables you to quickly and easily set up the portal hostname using a default domain name (.gpccloudservice.com). In this case, the cloud service automatically publishes the hostname to public DNS servers and handles all certificate generation. However, you can opt to use your own company domain name in the portal hostname. If you plan to use your company domain name, you must [obtain your own certificates](#) for the portal and configure an [SSL/TLS service profile](#) to point to the certificate before you configure the service. Additionally, if you use your own domain name in the portal hostname, you also need to configure your DNS servers to point to the portal DNS CNAME, which is provided during the configuration process.
- **Service Connection**—You must [create and configure a service connection](#) if you want to enable your mobile users to access resources, such as authentication servers, on your internal network (for example, an authentication server in your data center or HQ location) or enable your mobile users to access your remote network locations.

Even if you don't plan to use the connection to provide access to your internal resources, you must [configure at least one service connection with placeholder values](#) if you want your mobile users to be able to connect to your remote network locations or if you have mobile users in different geographical areas who need direct access to each other's endpoints.

- **IPv6 Usage in Your Network**—Determine whether you want to perform any mitigation for IPv6 traffic in your network to reduce the attack surface. In a dual stack endpoint that can process both IPv4 and IPv6 traffic, mobile user IPv6 traffic is not sent to Prisma Access by default and is sent to the local network adapter on the endpoint instead. For this reason, Palo Alto Networks recommends that you configure Prisma Access to [sinkhole IPv6 traffic](#).
- **Set up Logging for GlobalProtect Endpoints**—You have two options to collect logs from mobile users who use the GlobalProtect app:
  - **Manual Log Collection from GlobalProtect Endpoints**—Have the mobile users collect the logs from the GlobalProtect app for [Windows](#), [macOS](#), and [Linux](#) devices. This option requires no additional configuration.
  - **GlobalProtect App Log Collection for Troubleshooting**—Allow the GlobalProtect app to perform end-to-end diagnostic tests to resolve connection, performance, and access issues, and generate troubleshooting and diagnostic logs to be sent to Cortex Data Lake for further analysis. You need to generate a certificate so that the GlobalProtect app can authenticate with Cortex Data Lake to collect the troubleshooting logs. This functionality is under **Panorama > Cloud Services > Configuration > Service Setup > Generate Certificate for GlobalProtect App Log Collection**. See [GlobalProtect App Log Collection for Troubleshooting](#) for configuration details.

#### □ Post-Installation checklist:

- **Add the Public IP Addresses to an allow list in Your Network**—After you onboard your locations, you need to [Retrieve Public and Egress IP Addresses for Mobile User Deployments](#) used by each location and add these locations' IP addresses to an allow list in your network to allow mobile users access to SaaS or public applications. If you add more locations, you will also need to retrieve the new IP addresses that Prisma Access allocates for the newly-added location or locations.

## Secure Mobile Users With an Explicit Proxy

If you want to [secure mobile users using an explicit proxy](#), use the configuration guidelines shown in [Explicit Proxy System Guidelines and Requirements](#).

### *Supported Explicit Proxy Locations*

Prisma Access supports the following locations for explicit proxy. Explicit Proxy uses GeoDNS to resolve and connect the mobile user to the closest Prisma Access deployed location.

Explicit proxy supports the following locations:

- **Africa, Europe & Middle East:**

- 
- South Africa West
  - Belgium
  - Finland
  - France North
  - Germany Central
  - Ireland
  - Netherlands Central
  - Switzerland
  - UK
  - Bahrain
  - **Asia, Australia & Japan:**
    - Hong Kong
    - India West
    - Singapore
    - South Korea
    - Taiwan
    - Australia Southeast
    - Japan Central
    - Japan South
  - **North America & South America:**
    - Canada East
    - US Central
    - US East
    - US Northwest
    - US Southeast
    - US Southwest
    - Brazil South

# Secure Mobile Users With GlobalProtect

When you secure mobile users using GlobalProtect, you will need to define the settings to configure the portal and gateways in the cloud. For example, you will define a portal hostname, set up the IP address pool for your mobile users, and configure DNS settings for your internal domains. You may be able to leverage using existing configurations for some of the required settings, such as what authentication profile to use to authenticate mobile users. If you already have a template with your authentication profiles, certificates, certificate profiles, and server profiles, you can add that template to the predefined template stack during onboarding to simplify the setup process.

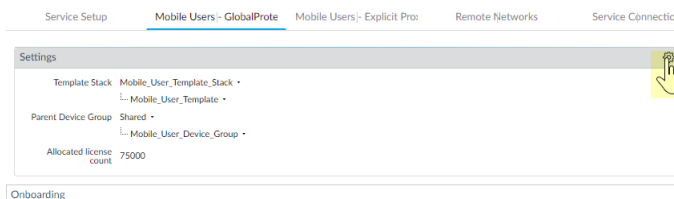
While it is not necessary to push your Security policy settings and objects to the cloud during the onboarding process, if you already have device groups and templates with the configuration objects you need (for example, Security policy, zones, User-ID configuration, and other policy objects) go ahead and add them when you onboard. This way you can to complete the [zone mapping](#) that is required to enable Prisma Access to map the zones in your policy to the appropriate interfaces and zones within the cloud. However, if you don't have your policy set yet, you can go back later and push it to Prisma Access for users.

In addition, if you want your mobile users to be able to connect to your remote network locations, or if you have mobile users in different geographical areas who need direct access to each other's endpoints, you must configure at least one [service connection with placeholder values](#), even if you don't plan to use the connection to provide access to your data center or HQ locations. The reason this is required is because, while all remote network locations are fully meshed, Prisma Access gateways (also known as *locations*) connect to the service connection in a hub-and-spoke architecture to provide access to the internal networks in your Prisma Access infrastructure.

**STEP 1 |** Select **Panorama > Cloud Services > Configuration > Mobile Users—GlobalProtect**.

**STEP 2 |** Configure the template stack and device group hierarchy that the cloud service will push to the portal and gateway.

1. Edit the **Settings**.



2. In the Templates section of the **Settings** tab, **Add** the template that contains the configuration you want to push to Prisma Access for users.

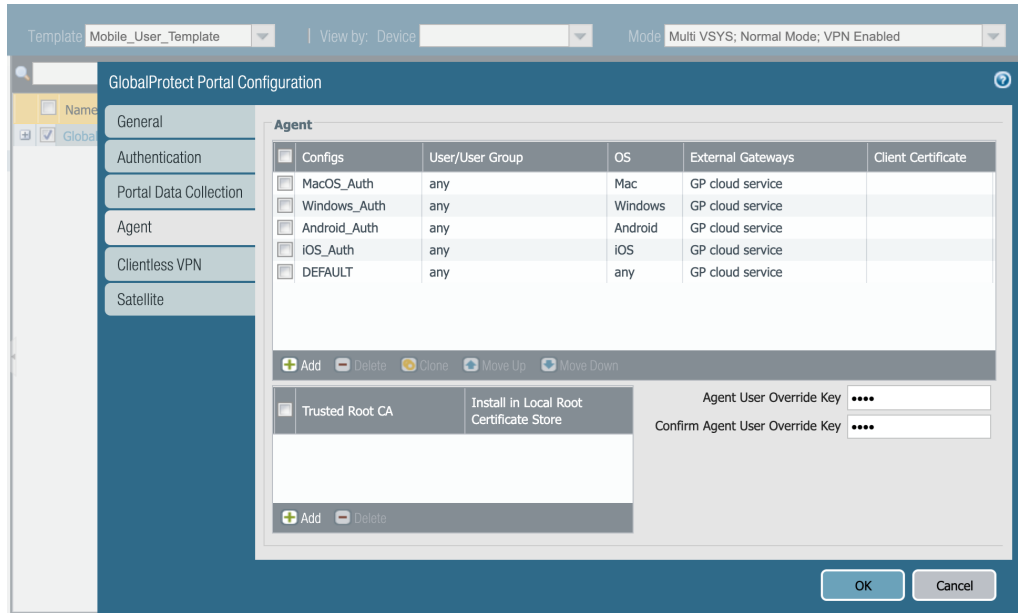


*Although you can add existing templates to the stack from the plugin, you cannot create a new template from the plugin. Instead, use the workflow to [add a new template](#).*

You can **Add** more than one existing template to the stack and then order them appropriately using **Move Up** and **Move Down**. This is important because Panorama evaluates the templates in the stack from top to bottom and settings in templates that are higher in the stack take priority over the same settings specified in templates that are lower in the stack. You cannot move the default `Mobile_User_Template` from the top of the stack; this prevents you from overriding any settings that Prisma Access requires to create the network infrastructure in the cloud.



If you want to customize the agent configuration that the Prisma Access for users pushes to clients from the portal, you must edit the GlobalProtect Portal configuration in the Mobile\_User\_Template to add a new agent configuration. After configuring the Agent configuration, move it above the DEFAULT agent configuration that is predefined in the template to ensure that your settings take precedence over the default settings. When editing this template, do not remove or change the External Gateway entry.



3. In the Device Group section, select the **Parent Device Group** that contains the configuration settings you want to push to Prisma Access for users, or leave the parent device group as **Shared** to use the Prisma Access device group shared hierarchy.

You will push all of the configuration—including the address groups, [Security policy](#), [Security profiles](#), and other policy objects (such as application groups and objects), [HIP objects and profiles](#) and [authentication policy](#)—that Prisma Access for users needs to enforce consistent policy to your mobile users using the [device group hierarchy](#) you specify here. In addition, you must make sure that you have configured a [Log Forwarding profile](#) that forwards the desired log types to **Panorama/Cortex Data Lake** in a device group that gets pushed to Prisma Access for users; this is the only way that the cloud service knows which logs to forward to Cortex Data Lake.

Settings
?

Settings | Group Mapping Settings

Template Stack

Template Stack Name:

Templates	TEMPLATES
	Mobile_User_Template
<input type="checkbox"/>	test

+ Add
 - Delete
↑ Move Up
↓ Move Down

The template at the top of the stack has the highest priority in the presence of overlapping config

Device Group

Device Group Name:

Parent Device Group:

Master Device:

OK
Cancel

4. (Optional) If you have configured an on-premises next-generation firewall as a **master device**, select the **Master Device** you configured.

When you select the **Master Device**, Prisma Access auto-populates user and group information in the security policy rules in Panorama for mobile user and remote network device groups.

**STEP 3 | (Optional)** Configure Prisma Access to use Directory Sync to retrieve user and group information.

You must [configure Directory Sync](#) to retrieve user and group information from your Active Directory (AD) before you enable and configure Directory Sync integration in Prisma Access using the settings in the **Group Mapping Settings** tab. See [Get User and Group Information Using Directory Sync](#) for details.

**STEP 4 |** Click **OK** to save the mobile user settings.

**STEP 5 |** Map the zones configured within the selected template stack as trusted or untrusted.

On a Palo Alto Networks next-generation firewall, Security policy is enforced between zones, which map to physical or virtual interfaces on the firewall. However, with Prisma Access for users, the networking infrastructure is automatically set up for you, which means you no longer need to configure interfaces and associate them with zones. However, to enable consistent security policy enforcement, you must map the zones you use within your organization as trust or untrust so that Prisma Access for users can translate the policy rules you push to the cloud service to the internal zones within the networking infrastructure.

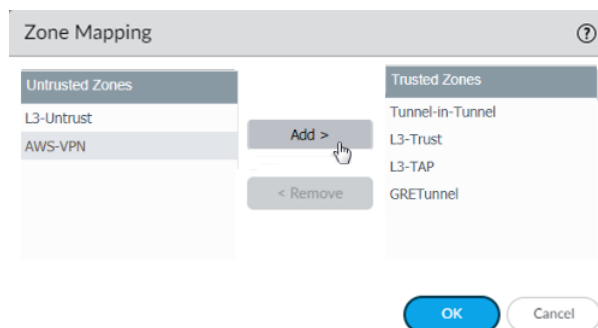
PRISMA ACCESS ADMINISTRATOR'S GUIDE (PANORAMA MANAGED) | Secure Mobile Users with Prisma Access **175**

© 2021 Palo Alto Networks, Inc.

1. Edit the [Zone Mapping](#) settings.

By default, all of the zones in the `Mobile_User_Template_Stack` are classified as Untrusted Zones.

2. For each zone you want to designate as trusted, select it and click **Add** to move it to the list of **Trusted Zones**.

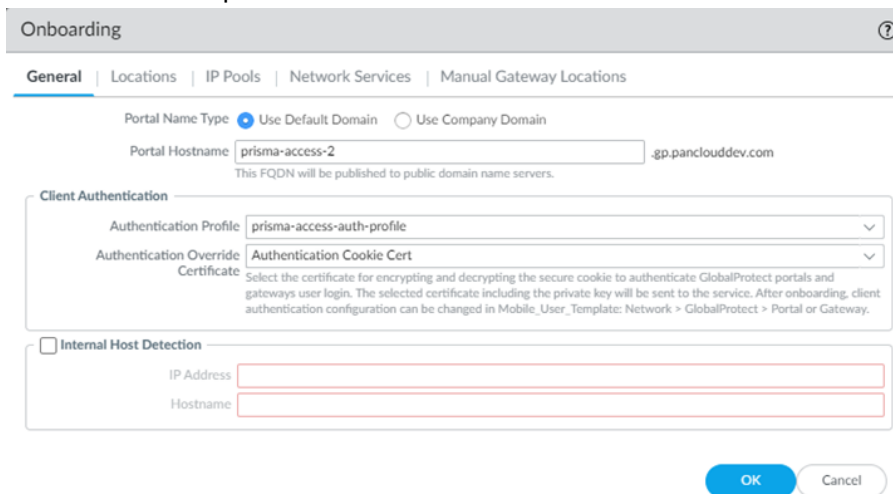


3. Click **OK** to save your changes.

## STEP 6 | Configure the GlobalProtect portal and external gateway settings.

You can configure Prisma Access gateways as external gateways only—not as internal gateways.

1. In the Onboarding section, click **Configure**.
2. On the **General** tab, specify the **Portal Name Type**:
  - **Use Default Domain**—If you select this option, your portal hostname uses the default domain name: `.gpcloudservice.com`. In this case, simply enter a **Portal Hostname** to append to the default domain name. Prisma Access for users will automatically create the necessary certificates and publish the hostname to public DNS servers.



*If you already have a GlobalProtect deployment with an existing portal name and you want to continue to use that portal name, add a CNAME entry that maps Prisma Access portal name to your existing portal name. For example, if you have an existing portal named `portal.acme.com` and you want to map the new Prisma Access portal to this same name, you would add a CNAME of `gpcs2.gpcloudservice.com` to the DNS entry for your existing portal.*

- **Use Company Domain**—Select this option if you want the domain in the portal hostname to match your company domain name (for example, `myportal.mydomain.com`). If you want to use this option, you must first [obtain your own certificate](#) and configure an [SSL/TLS service profile](#) that points to it. Then you can configure the portal name by selecting the **SSL/TLS Service Profile** and



entering the **Portal Hostname**. If you use this option, you must point your internal DNS servers to the **Portal DNS CNAME**, which is the hostname of the portal with the `.gpcloudservice.com` domain. For example, if you specified a DNS hostname of `acme-portal.acme.com`, you would need to create a DNS CNAME entry that maps that hostname to `acme-portal.gpcloudservice.com` on your internal DNS servers.

3. Select an **Authentication Profile** that specifies how Prisma Access should authenticate mobile users or create a new one.


If you added a parent device group that contains an authentication profile configuration, you should see it on the list of available profiles. If you did not push the profile in the device group, you can [create an authentication profile](#) now.

4. Select an **Authentication Override Certificate** to encrypt the secure cookies that mobile users authenticate to the portal and gateway.

If you added a parent device group that contains the certificate you want to use to encrypt authentication cookies, you should see it on the list of available certificates. If you did not push a certificate in the device group, you can [import](#) or [generate one](#) now.

5. (Optional) If you do not require GlobalProtect endpoints to have tunnel connections when on the internal network, enable **Internal Host Detection**.

1. Select the **Internal Host Detection** check box.
2. Enter the **IP Address** of a host that users can reach only from the internal network.
3. Enter the DNS **Hostname** for the IP address you entered. Clients that try to connect perform a reverse DNS lookup on the specified address. If the lookup fails, the client determines that it needs a tunnel connection to Prisma Access for users.


 *Prisma Access copies the internal host detection settings you specify here to the settings in your [GlobalProtect portal configuration](#) (`Network > GlobalProtect > Portals > <portal-config> > Agent > <agent-config> > Internal`). If you change your portal configuration settings through `Network > GlobalProtect > Portals` at a later time, those changes are not reflected in the settings you specify here. For this reason, Palo Alto Networks recommends that you either enter the internal host detection settings here or configure the same settings in both places.*

**STEP 7 |** Select the **Locations** and the regions associated with those locations where you want to deploy your mobile users.

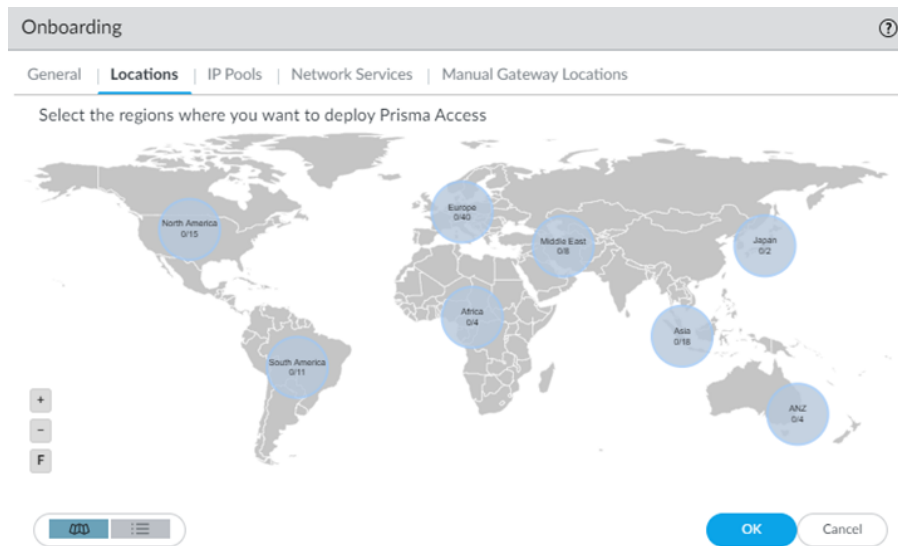
The **Locations** tab displays a map. Highlighting the map shows the global regions (Americas, Europe, and Asia Pacific) and the locations available inside each region. Select a region, then select the locations you want to deploy in each region. Limiting your deployment to a single region provides more granular

control over deployed regions and allows you to exclude regions as required by your policy or industry regulations. See [List of Prisma Access Locations](#) for the list of regions and locations. You can select a location in a region that is closest to your mobile users, or select a location as required by your policy or industry regulations.

Specify a single region to reduce the minimum IP address pool that you need in Step 8. See [Specify IP Address Pools for Mobile Users](#) for more information.

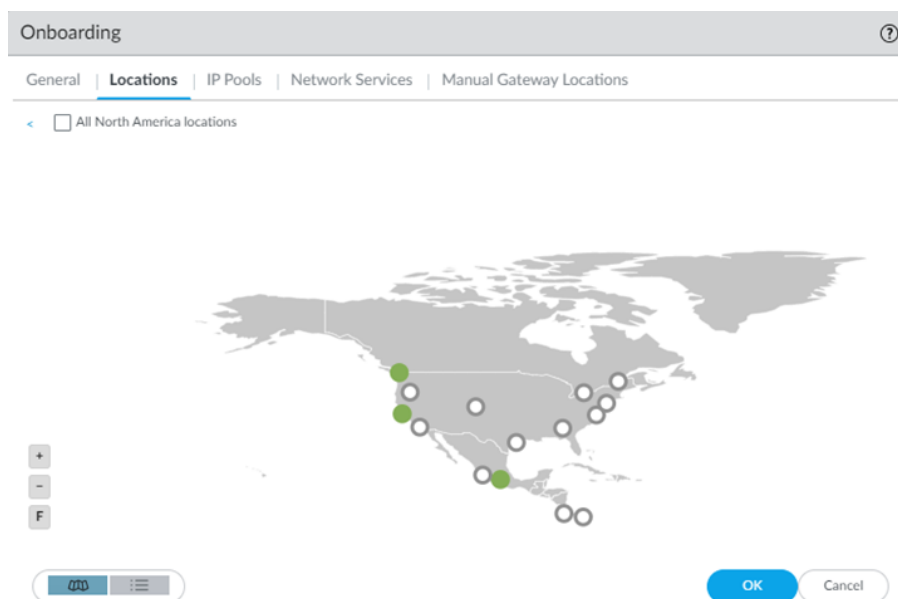
 *Prisma Access uses the Hong Kong, Netherlands Central, and US Northwest locations as fallback mobile user locations if other locations are not available. For this reason, Palo Alto Networks strongly recommends that you enable at least one of these locations during mobile user onboarding.*

1. Click the **Locations** tab and select a region.

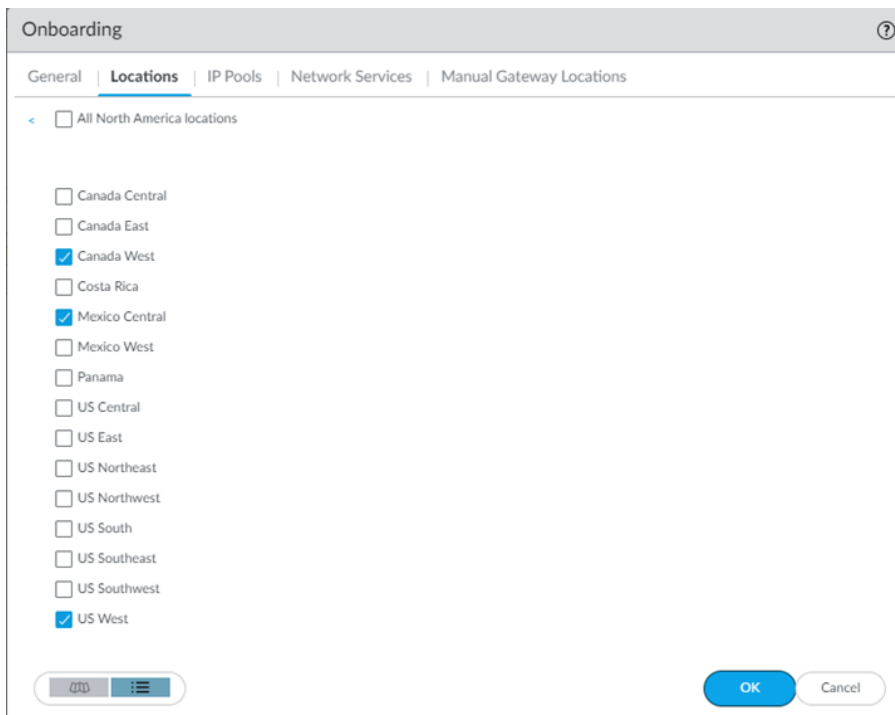


2. Select one or more Prisma Access gateways within your selected region using the map.

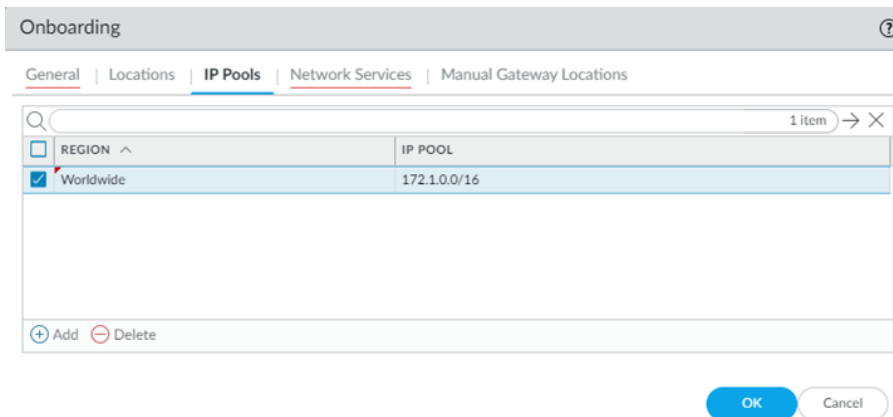
Hovering your cursor over a location highlights it. White circles indicate an available location; green circles indicate that you have selected that location.



In addition to the map view, you can view a list of regions and locations. Choose between the map and list view from the lower left corner. In the list view, the list displays regions sorted by columns, with all locations sorted by region. You can select **All** sites within a region (top of the dialog).



**STEP 8** | Set up the IP address pools that Prisma Access for users uses to assign IP addresses to GlobalProtect endpoints by selecting the **IP Pools** tab and **Add** and IP address pool.



- **Region**—Select **Worldwide** to use a single IP address pool for all GlobalProtect clients using the cloud service or select an available region.

You can use a single IP address pool for all GlobalProtect endpoints **Worldwide**, you can set separate pools for each region where you have mobile users, or you can specify both **Worldwide** and region-specific IP pools. For example, you can add an pool for a specific region and then add a **Worldwide** pool to use for all other regions. Prisma Access then uses the **Worldwide** IP addresses to scale as you onboard additional gateways in other regions to accommodate more mobile users. If you specify a pool for a region, and you exhaust the available IP addresses in that pool, Prisma Access will take IP addresses from the **Worldwide** pool to use in that region.

- 
- **IP Pool**—Enter an IP address pool to assign to the endpoints in the selected region. The addresses in this pool must not overlap with other networks you use internally or with the pools you assigned when you [Enable the Service Infrastructure](#).

If you deploy locations in a single region, the minimum required subnet is /23 (512 IP addresses) per location. Additional locations require a minimum /23 subnet. If you specify a Worldwide subnet, the minimum required subnet is /23 but we recommend providing enough subnets to allocate a number of IP addresses that is equal to or greater than the number of licensed mobile users so that they can log in at the same time. Do not specify any subnets that overlap with 169.254.169.253, 169.254.169.254, and the 100.64.0.0/10 subnet range because Prisma Access reserves those IP addresses and subnets for its internal use. See how to [Specify IP Address Pools for Mobile Users](#) for more information.



*We recommend using an RFC 1918-compliant IP address pool. While we support the use of non-RFC 1918-compliant (public) IP addresses for mobile users, we do not recommend using these non-compliant IP addresses due to possible conflicts with internet public IP address space.*

**STEP 9 |** To specify the [DNS resolution settings](#) for your internal and external (public) domains, select **Network Services** tab and then click **Add**.

GlobalProtect endpoints with an active tunnel connection use their virtual network adapters rather than their physical network adapters and therefore require separate DNS resolution settings.

Configure network settings in the **Network Services** window.

- Select a **Region** from the drop-down at the top of the window.

Select a specific region, or select **Worldwide** to apply the DNS settings globally. If you specify multiple proxy settings with a mix of regional and Worldwide regions, Prisma Access uses the regional settings for the Locations in the region or regions you specify and uses the worldwide settings elsewhere. Prisma Access evaluates the rules from top to bottom in the list.

- **Add** one or more rules to configure the DNS settings for **Internal Domains**.
  - Enter a unique **Rule Name** for the rule.
  - you want your internal DNS server to only resolve the domains you specify, enter the domains to resolve in the **Domain List**. Specify an asterisk in front of the domain; for example, \*.acme.com. You can specify a maximum of 1,024 domain entries.
  - If you have a **Custom DNS server** that can access your internal domains, specify the **Primary DNS** and **Secondary DNS** server IP addresses, or select **Use Cloud Default** to use the default Prisma Access DNS server.
- Specify the DNS settings for **Public Domains**.
  - **Use Cloud Default**—Use the default Prisma Access DNS server.
  - **Same as Internal Domains**—Use the same server that you use to resolve internal domains. When you select this option, the DNS Server used to resolve public domains is same as the server configured for the first rule in the **Internal Domains** section.
  - **Custom DNS server**—If you have a DNS server that can access your public (external) domains, enter the Primary DNS server address in that field.

(Optional) You can **Add** a **DNS Suffix** to specify the suffix that the client should use locally when an unqualified hostname is entered that it cannot resolve, for example, acme.local. Do not enter a wildcard (\*) character in front of the domain suffix (for example, acme.com). You can add multiple suffixes.

- If you want Prisma Access to proxy DNS requests, configure Configure values for the use for UDP queries (the **Interval** to retry the query in seconds and the number of retry **Attempts** to perform).

If you want Prisma Access to [proxy DNS requests](#) for your GlobalProtect users, You must update your endpoints to use the **Remote Network DNS Proxy IP Address** as the primary DNS server (**Panorama > Cloud Services > Status > Network Details > Service Infrastructure**).

Network Services

Region: Worldwide

Internal Domains (1 item)

RULE NAME	DOMAIN LIST	PRIMARY DNS	SECONDARY DNS
Local	*.acme.local	10.1.1.3	10.1.1.4

Public Domains

Primary DNS:  Use Cloud Default  Same as Internal Domains  Custom DNS Server

Secondary DNS:  Use Cloud Default  Same as Internal Domains  Custom DNS Server

Client DNS Suffix Search List (0 items)

Buttons: Add, Delete, Import, OK, Cancel

**STEP 10 | (Optional)** If your deployment uses Windows Internet Name Service (WINS) based, you can specify WINS servers to resolve NetBIOS name-to-IP address mapping by selecting **WINS Configuration**; selecting a region for the WINS server or selecting **Worldwide** to apply the WINS configuration worldwide, then specifying a **Primary WINS** and, optionally, **Secondary WINS** server address.

After you enable WINS, Prisma Access can push WINS configuration to mobile users' endpoints over GlobalProtect.

Onboarding ?

General | Locations | IP Pools | **Network Services** | Manual Gateway Locations

2 items → ×

	REGION	Internal Domains				Public Domains	
		RULE NAME	PRIMARY DNS	SECONDARY DNS	DOMAIN LIST	PRIMARY DNS	SECONDARY DNS
<input type="checkbox"/>	Worldwide	Local	10.1.1.3	10.1.1.4	*.acme.local	Same as Internal	Same as Internal
<input type="checkbox"/>	North America & South America	NA rule	Use Cloud Default	Use Cloud Default		Use Cloud Default	Use Cloud Default

+ Add - Delete

For a domain entry in the Internal Domains list, enter as \*-domain>. For example \*.acme.com.  
For a domain entry in the DNS Suffix Search list, enter as <domain>. For example, acme.com

**UDP Queries Retries**

Interval (Sec)

Attempts

**WINS Configuration**

1 item → ×

REGION	PRIMARY WINS	SECONDARY WINS
<input checked="" type="checkbox"/> Worldwide	10.1.1.1	10.2.2.2

+ Add - Delete

Select this to provide a region-specific Primary and Secondary WINS server configuration.

**STEP 11 | (Optional)** If you allow your mobile users to manually select gateways from the GlobalProtect app, select the **Manual Gateway Locations** that the users can view from their GlobalProtect app.

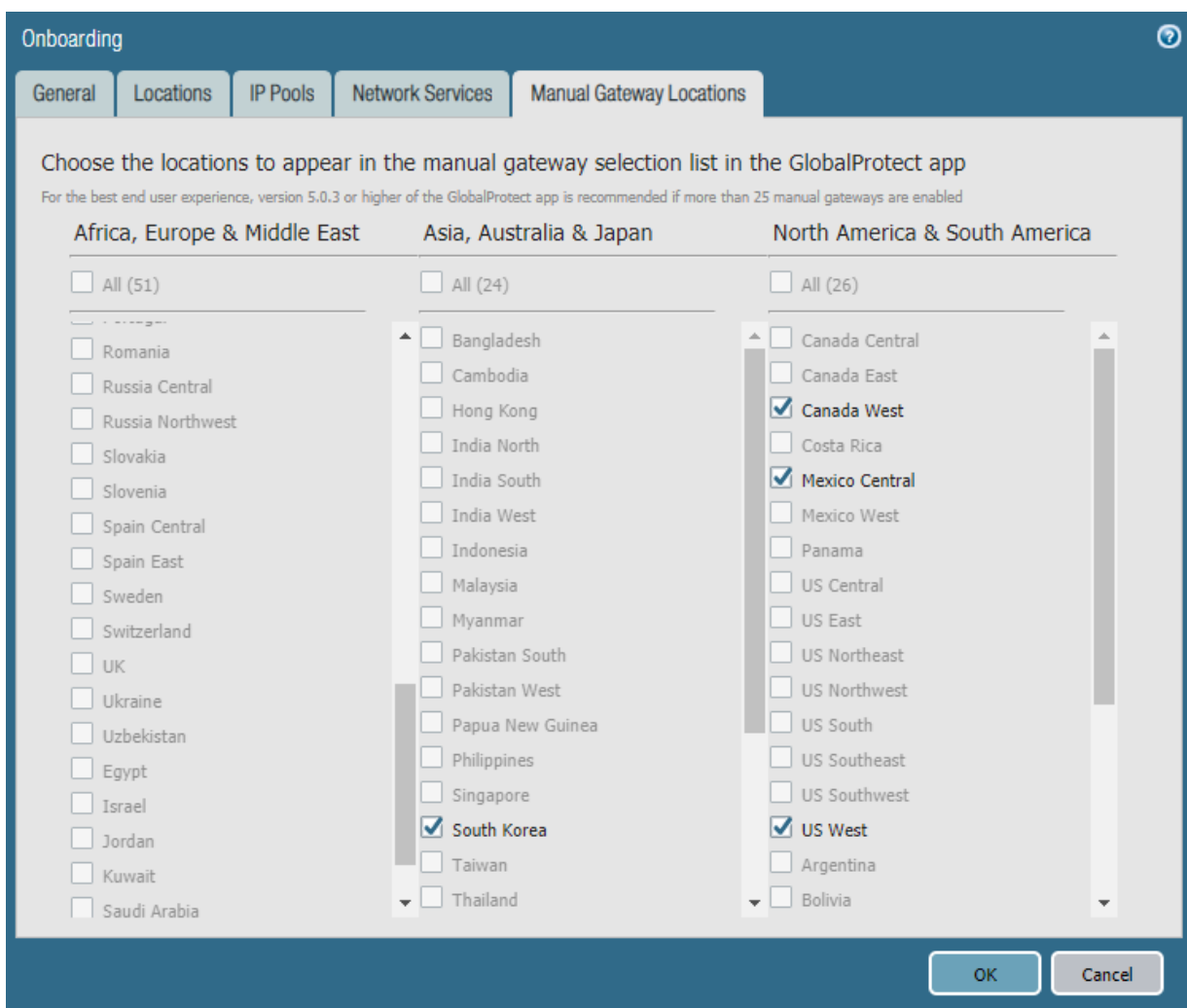
Choosing a subset of onboarded locations reduces the number of available gateways that mobile users can view in their GlobalProtect app for manual gateway selection.


If you do not select manual gateways in this tab, Prisma Access selects the following list of gateways by default.

- Australia Southeast
- Belgium
- Brazil South
- Canada East
- Finland
- France North
- Germany Central
- Hong Kong
- India West
- Ireland
- Israel
- Japan Central
- Netherlands Central
- Saudi Arabia

- Singapore
- South Africa Central
- South Korea
- Taiwan
- UK
- US East
- US West

Prisma Access lets you select only gateways that you have onboarded. For example, if you don't choose **UK** when you select locations, you cannot select **UK** as a manual gateway (the location is grayed out).



 *If you allow users to manually choose more than 25 gateways, we recommend using version 5.0.3 or later of the GlobalProtect app for the best end user experience.*

**STEP 12** | Click **OK** to save the Onboarding settings.

**STEP 13** | To secure traffic for your mobile users, you must create security policy rules.

1. Select the **Device Group** in which to add policy rules. You can select the `Mobile_User_Device_Group` or the parent device group that you selected when setting up Prisma Access for mobile users.

2. **Create security policy rules.** Make sure that you do not define security policy rules to allow traffic from any zone to any zone. In the security policy rules, use the zones that you defined in the template stack you are pushing to the cloud service.

#### STEP 14 | Configure logs to forward to Cortex Data Lake.

The Cloud Services plugin automatically adds the following Log Settings (**Device > Log Settings**) after a new installation or when removing non-Prisma Access templates from a Prisma Access template stack:

- Log Settings for System logs (**system-gpcs-default**), User-ID logs (**userid-gpcs-default**), HIP Match logs (**hipmatch-gpcs-default**), and GlobalProtect logs (**gp-prismaaccess-default**) are added to the Mobile\_User\_Template.
- Log Settings for System logs (**system-gpcs-default**), User-ID logs (**userid-gpcs-default**), and GlobalProtect logs (**gp-prismaaccess-default**) are added to the Remote\_Network\_Template.
- Log Settings for System logs (**system-gpcs-default**) and GlobalProtect logs (**gp-prismaaccess-default**) are added to the Service\_Conn\_Template.

These Log Setting configurations automatically forward System, User-ID, and HIP Match logs to Cortex Data Lake.

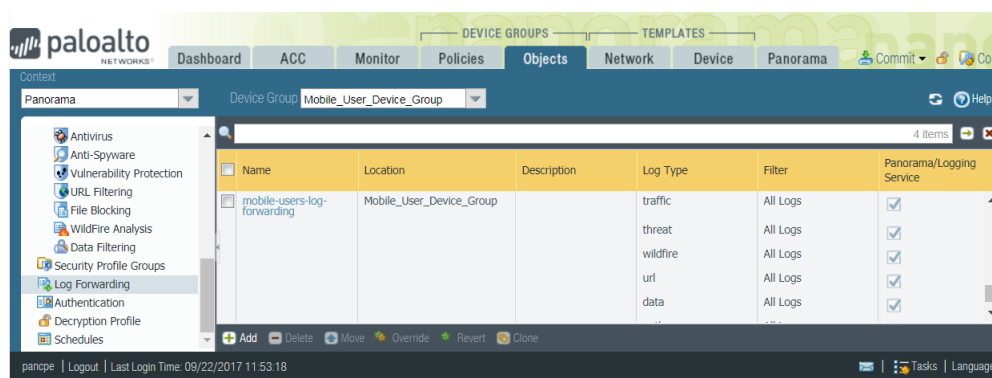
#### STEP 15 | (Optional) Forward logs for other log types to Cortex Data Lake.

To do this, you must create and attach a log forwarding profile to each policy rule for which you want to forward logs. See the [Cortex Data Lake Getting Started Guide](#) for more information.

1. Select the **Device Group** in which you added the policy rules.
2. Select **Objects > Log Forwarding** and **Add** a profile. In the Log Forwarding Profile Match List, **Add** each log type that you want to forward.

The following example enables forwarding of Traffic, Threat Prevention, WildFire Submission, URL Filtering, Data Filtering, and Authentication logs.

3. Select **Panorama/Cortex Data Lake** as the Forward Method. When you select Panorama, the logs are forwarded to Cortex Data Lake. You will be able to monitor the logs and generate reports from Panorama. Cortex Data Lake provides a seamless integration to store logs without backhauling them to your Panorama at the corporate headquarters, and Panorama can query Cortex Data Lake as needed.

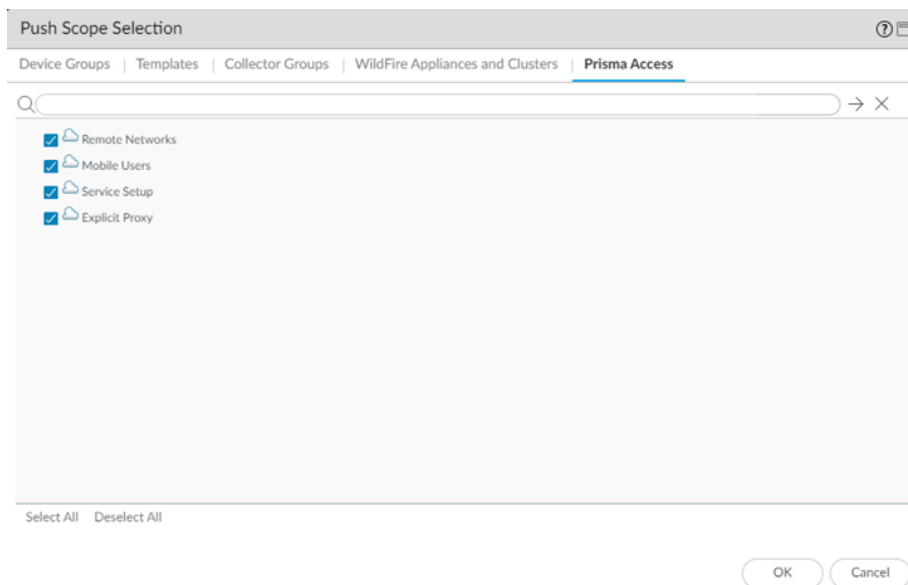


4. Select **Policies > Security** and edit the policy rule. In **Actions**, select the Log Forwarding profile you created.

#### STEP 16 | Commit all your changes to Panorama and push the configuration changes to Prisma Access.

1. Click **Commit > Commit and Push**.
2. **Edit Selections** and, in the **Prisma Access** tab, make sure that **Mobile Users** is selected in the **Push Scope**, then click **OK**.



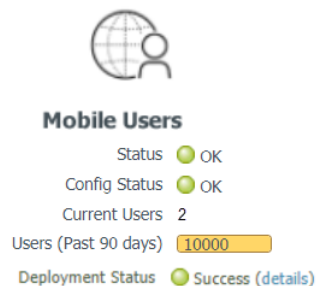


3. Click **Commit and Push**.

**STEP 17** | To verify that Prisma Access for users is deployed and active, select **Panorama > Cloud Services > Status > Status**.

After the provisioning completes, the mobile users **Status** and **Config Status** should show **OK**.

The **Deployment Status** area allows you to view the progress of onboarding and deployment jobs before they complete, as well as see more information about the status of completed jobs. See [Deployment Progress and Status](#) for details.



To view the number of unique users who are currently logged in, or to log out a logged in user, click the hyperlinked number next to **Current Users**. See [View Logged In User Information and Log Out Current Users](#) for details.

Domain	Client OS	Private IP	Computer	User	Public IP	Login At	Logout
	Browser			test1		2019-07-18 15:44:28 PDT	⊗
	Apple Mac OS X 10.13.6	10.19.19.2	-MacBook-Pro	test		2019-07-18 15:44:21 PDT	⊗

Export to CSV

Close

To view historical information of previously-logged in users for a 90-day time period, click the number next to **Users (Last 90 days)**.

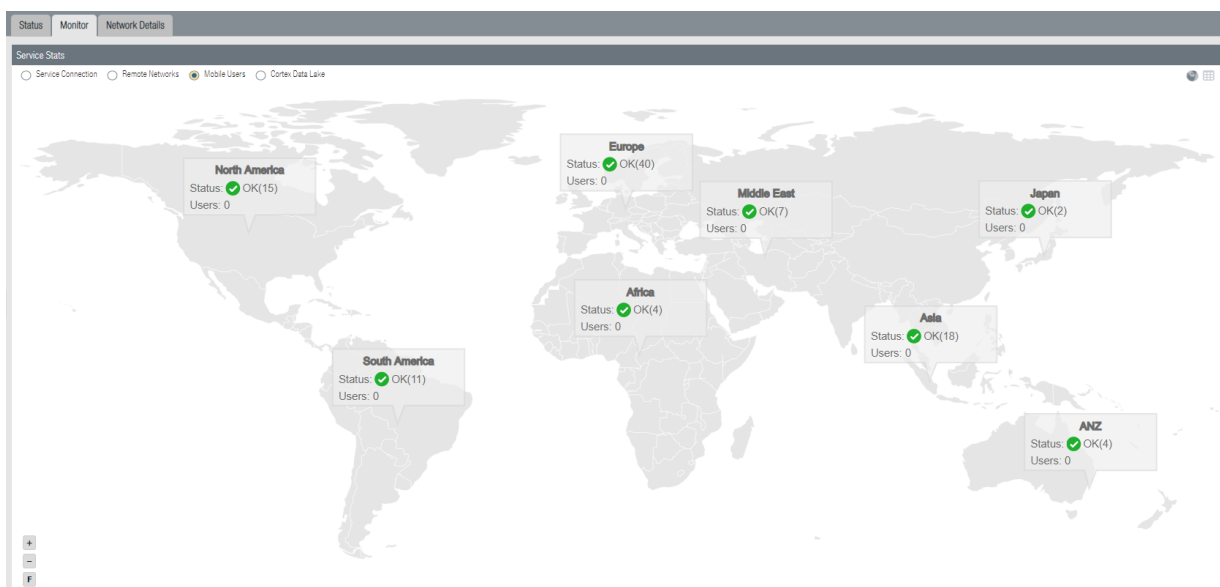
To export the list of users to a csv file, select **Export to CSV**. Note that a maximum of 45,000 users can be exported to a CSV file.

Client OS	User	Login At	Public IP
Apple Mac OS X 10.13.6		2018-12-05 15:18:05 PST	
Android 8.1.0		2019-01-07 13:30:21 PST	
Microsoft Windows 7 Enterprise Edition Service Pack 1, 32-bit		2019-01-04 17:35:51 PST	
Apple iOS 12.0.1		2019-01-02 10:40:54 PST	
Android 7.0		2019-02-19 15:50:12 PST	

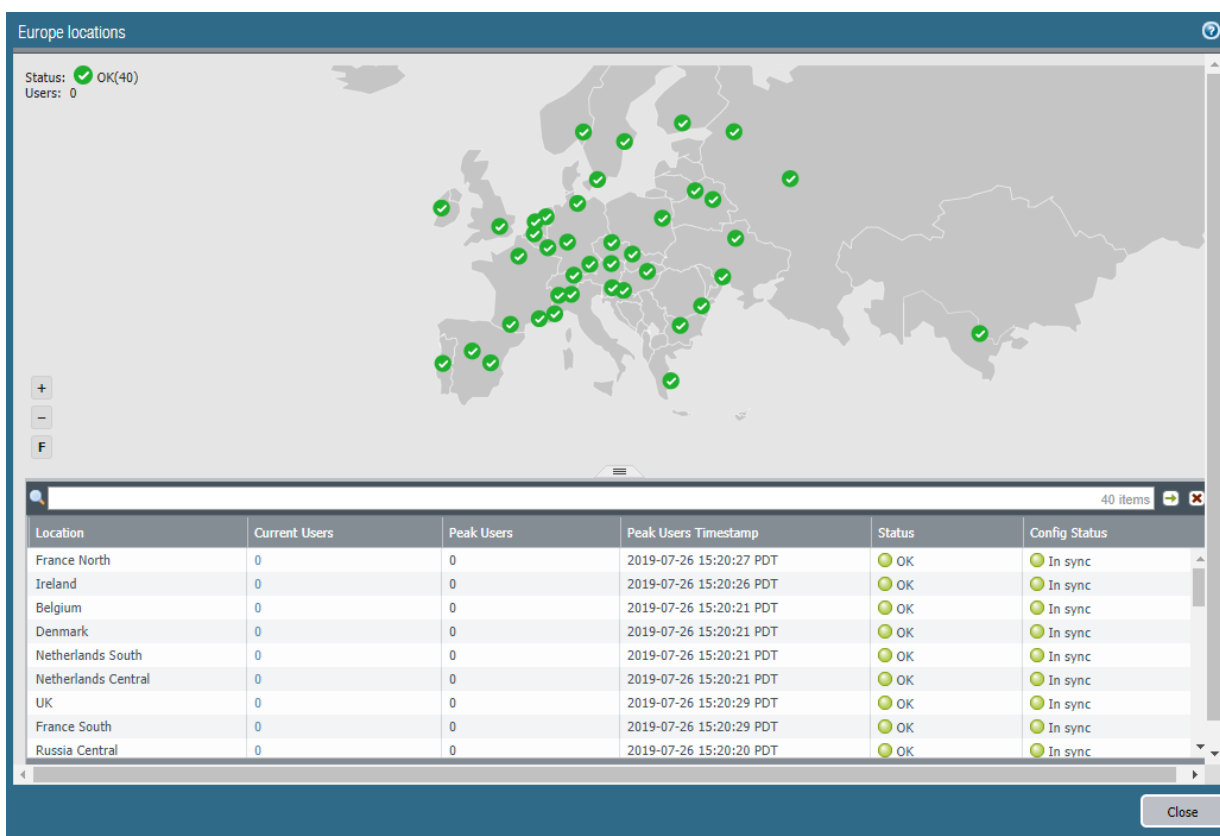
Export to CSV

Close

To display a map that shows the locations of Prisma Access portals and gateways running in the regions you have selected, select **Monitor**; then, select **Mobile Users**.



Select a region to get more detail about that region.



**STEP 18** | If you chose to **Use Company Domain** for your portal hostname, you must add a DNS entry on your internal DNS servers to map the portal hostname you defined to the Portal DNS CNAME displayed on the **Cloud Services > Configuration > Mobile Users > Onboarding > General** tab (for example, `<portal_hostname>.gpcloudservice.com`).

**STEP 19** | Deploy the **GlobalProtect app** software to your end users.

---

For Mac OS or Windows users, you can direct users to the Prisma Access portal address, where they can download the GlobalProtect app from the portal.



*Prisma Access manages the version of the GlobalProtect app on the portal and you can select the active version from the versions that Prisma Access hosts, as well as control the ability of users to download it.*

Alternatively, you can [host GlobalProtect app software on a web server](#) for your Mac OS and Windows users. Prisma Access is compatible with any GlobalProtect app versions that are not listed as [end of life](#).

Mobile app users can [download and install the GlobalProtect mobile app](#) from the appropriate app store for their operating systems.

# Secure Mobile Users with an Explicit Proxy

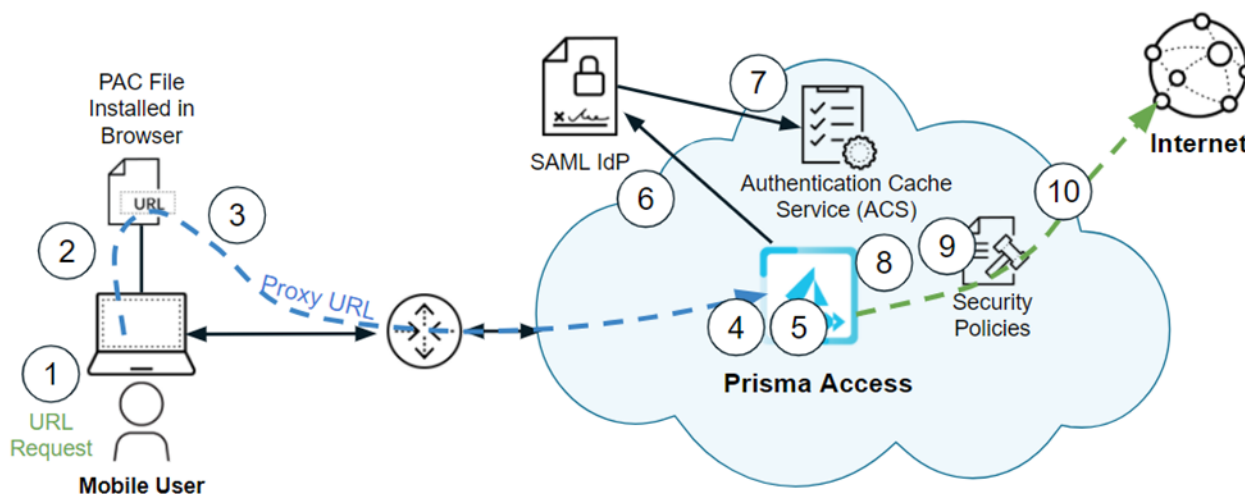
In addition to [securing mobile users with GlobalProtect](#), you can configure an explicit proxy using Prisma Access. Consider using an explicit proxy if your existing network already uses proxies, if you use PAC files on your end users' endpoints, or if you need to use a proxy for auditing or compliance purposes.

- [Explicit Proxy Workflow](#)
- [Explicit Proxy System Guidelines and Requirements](#)
- [Set Up an Explicit Proxy to Secure Mobile Users](#)
- [PAC File Guidelines and Requirements](#)
- [Security Policy Guidelines and Requirements](#)
- [Verify and Monitor the Explicit Proxy Deployment](#)

## Explicit Proxy Workflow

The following section shows the workflow when mobile users are secured by Prisma Access using an explicit proxy as the connection method. Before you start, you need to have [configured Mobile Users—Explicit Proxy](#).

The traffic takes the following path. Callouts in the figure show the process.



**STEP 1 |** The mobile user browses the Internet or accesses the SaaS application by entering the URL or IP address using a web browser.

**STEP 2 |** The browser on the mobile users' endpoint checks for the PAC file.

This PAC file specifies that the URL or SaaS request should be forwarded to Prisma Access explicit proxy.

**STEP 3 |** The HTTPS client (the browser on the mobile user's endpoint) forwards the URL request to the proxy URL.

**STEP 4 |** The traffic is redirected to the explicit proxy, and the proxy decrypts the traffic.

---

**STEP 5 |** The proxy inspects the traffic and checks for the authentication cookie set up by the Prisma Access explicit proxy.

The cookie contains information that identifies the mobile user, and uses the cookie to authenticate the user.

**STEP 6 |** If, upon inspection of the cookie, Prisma Access determines that the user has not been authenticated, it redirects the user for authentication.

**STEP 7 |** After the IdP authenticates the user, Prisma Access stores the authentication state of the user in the Authentication Cache Service (ACS). The validity period of the authentication is based on the **Cookie Lifetime** value you specify during explicit proxy configuration.

**STEP 8 |** The explicit proxy checks for the presence and validity of our cookie. If the cookie is not present or is invalid, the user is redirected to ACS. After ACS confirms the authentication of the user, the user is redirected back to the explicit proxy with a token. The proxy then validates that token and sets the cookie for that domain for that user.

**STEP 9 |** Prisma Access applies security enforcement based on the security policy rules that the administrator has configured.

**STEP 10 |** If the URL is not blocked by security policy rules, Prisma Access sends the URL request to the internet.

## Explicit Proxy System Guidelines and Requirements

Before you secure mobile users with an explicit proxy, make sure that you complete all the software and network requirements described in [Secure Mobile Users With an Explicit Proxy](#).

**Licensing and Onboarding Guidelines**—Use the following guidelines when you license and onboard your explicit proxy deployment:

- Explicit proxy supports a subset of Prisma Access locations. See [Supported Explicit Proxy Locations](#) for the list of locations.

If you have a Local or Evaluation license for Prisma Access for Users and you have a Mobile Users—GlobalProtect deployment as well as a Mobile Users—Explicit Proxy deployment, you can deploy a maximum of five locations for both deployments combined. You need to allocate the five locations between both deployments (for example, two locations for Mobile Users—GlobalProtect and three locations for Mobile Users—Explicit Proxy). If you have a Worldwide license, there are no restrictions for the maximum number of locations.

- Specify a minimum of 200 units from your Mobile Users license for your Explicit Proxy deployment.

If you have a Mobile Users—GlobalProtect deployment and enter a number that exceeds the number of available users, Prisma Access takes those users from your Mobile Users for GlobalProtect deployment and allocates them to your Mobile Users—Explicit Proxy deployment. As shown in the following table, if you have 1000 users licensed and have 750 users licensed for Mobile Users - GlobalProtect, and you then enter 500 licensed users in the Mobile Users - Explicit Proxy, Prisma Access takes 250 licensed users from the pool for Mobile Users - GlobalProtect and assigns it to Mobile Users - Explicit Proxy, so that each mobile users component is licensed for 500 users.

Total Licensed Mobile User Allocation	Existing Licensed Mobile Users—GlobalProtect Allocation	New Licensed Mobile Users—Explicit Proxy Allocation	New Licensed Mobile Users—GlobalProtect Allocation
1000 Users	750 Users	250 Users	750 Users (no change)
1000 Users	750 Users	500 Users	500 Users Prisma Access takes 250 users from the 750 Mobile Users—GlobalProtect license to allocate the 500 users you specified for the Mobile Users—Explicit Proxy license.

**System and Network Requirements**—When configuring explicit proxy, make sure that you have configured the following system and network requirements:

- You must configure an [SSL decryption](#) policy for all explicit proxy traffic. Decryption is required for Prisma Access to read the authentication state cookie set up by Prisma Access on the mobile user's browser.
- If mobile users are connecting from remote sites or headquarters/data center locations using an explicit proxy, the mobile user endpoint must be able reach and route to the IdP, ACS FQDN, Explicit Proxy URL, and URL of the PAC file hosted by Prisma Access. To find the ACS FQDN and the Explicit Proxy URL, select **Panorama > Cloud Services > Status > Network Details > Mobile Users—Explicit Proxy**.
- The maximum supported TLS version is 1.2. When creating a decryption profile, specify a **Max Version of TLS v1.2**.

**Decryption Profile**
?

Name:

Shared

Disable override

**Decryption Mirroring**

Interface:

Forwarded Only

**SSL Decryption** | No Decryption | SSH Proxy

---

SSL Forward Proxy | SSL Inbound Inspection | **SSL Protocol Settings**

**Protocol Versions**

Min Version:

Max Version:

**Key Exchange Algorithms**

RSA       DHE       ECDHE

**Encryption Algorithms**

3DES       AES128-CBC       AES128-GCM       CHACHA20-POLY1305

RC4       AES256-CBC       AES256-GCM

**Authentication Algorithms**

MD5       SHA1       SHA256       SHA384

Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted. Check boxes to block those sessions instead.

- You must strip out ALPN headers from HTTP/2 traffic. See [Security Policy Guidelines and Requirements](#) for details.

**Panorama and Content Version Requirements**—Make sure that your deployment has the following minimum Panorama and Antivirus Content version requirements:

- Explicit proxy requires a minimum Panorama version of 10.0.5.
- Explicit Proxy requires a minimum antivirus Content Version of 3590 to be installed on the Panorama to support the predefined security policies. Install the required Content Version before committing the **Mobile Users—Explicit Proxy** configuration.

**Palo Alto Networks Subscription Support**—Explicit proxy supports Threat Prevention, URL Filtering, and WildFire subscriptions. DNS Security and DLP Security subscriptions are not supported.

**Mobile User App Support and Browser Guidelines**—Explicit Proxy supports the following apps and has the following browser guidelines and requirements:

- Explicit proxy secures internet and SaaS applications accessed over the mobile users' browser using HTTP and HTTPS traffic only. Non-web ports and protocols are not supported.
- Explicit proxy does not support the full client-based version of Microsoft 365 (Office 365), which uses non-web ports. However, it is designed to support web-based M365, including Office Online ([office.com](https://office.com)).
- Explicit proxy does not provide access to private applications.
- Mobile users will be unidentified in the traffic logs for sites that are not decrypted and on the HTTP requests where browsers do not send cookies such as cross-origin resource sharing (CORS) requests.
- Make a note of the following browser requirements:
  - If you use Explicit Proxy, do not disable cookies in your browser; if you do, you cannot browse any web pages.



- If you are using explicit proxy with Microsoft Edge, be sure that **Settings > Privacy, Search, and Services > Tracking prevention** is set to **Basic**.
- If you use Safari with explicit proxy, you might experience issues when accessing websites. Instead of Safari, use Microsoft Edge, Firefox, Chrome, or Internet Explorer as your browser.
- When using Firefox with an explicit proxy, go to `about:config` and set `security.csp.enable` to `false`. In addition, some add-ons, such as ones that perform ad blocking or tracking protection, might interfere with tracking protection.
- You might have issues when accessing the following desktop applications when using explicit proxy: Office 365, Slack, Zoom, or Webex.

**PAC File Requirements and Guidelines**—Explicit proxy has certain requirements for its PAC files; see [PAC File Guidelines and Requirements](#) for details.

## Set Up an Explicit Proxy to Secure Mobile Users

To secure mobile users with an explicit proxy, complete the following steps.

**STEP 1 | Configure SAML authentication**, including configuring a **SAML Identity Provider** and an **Authentication Profile**, for Prisma Access. You specify the authentication profile you create in a later step.

Use the following guidelines when configuring authentication for the IdP and in Panorama:

- **Panorama Guidelines:**
  - Be sure that you configure the authentication profile under the **Explicit\_Proxy\_Template**.
  - Use **mail** as the user attribute in the IdP server profile and in the **Authentication Profile** on Panorama.
  - Explicit proxy does not support **Sign SAML Message to IdP** in the SAML Identity Provider Server Profile.
  - If you configure a [Master Device](#) or Directory Sync, use **mail** or **userPrincipalName** as the **SamAccountName** in Group Mapping.
  - When using Panorama to manage Prisma Access, Directory Sync does not auto-populate user and group information to security policy rules. To populate user and group information from Directory Sync and simplify rule creation, you can optionally configure a next-generation firewall as a [Master Device](#) using an on-premises or VM-series next generation firewall and associate it to Prisma Access.
- **IdP Guidelines:**
  - SAML is the only supported authentication protocol. Prisma Access supports PingOne, Azure AD, and Okta as SAML authentication providers, but you should be able to use any vendor that supports SAML 2.0 as a SAML identity provider (IdP).
  - Use the following URLs when configuring SAML:
 

**SAML Assertion Consumer Service URL:** `https://global.acs.prismaaccess.com/saml/acs`

**Entity ID URL:** `https://global.acs.prismaaccess.com/`

For more details about configuring SAML authentication with Prisma Access, including examples for Okta and Active Directory Federation Services (ADFS) 4.0, see [Authenticate Mobile Users](#) in the [Prisma Access Integration Guide \(Panorama Managed\)](#).
  - If you use Okta as the IdP, use **mail** as the login username in the Okta profile.
  - Enter a single sign on URL of `global.acs.prismaaccess.com`.
  - Single Logout (SLO) is not supported.

- 
- To troubleshoot IdP authentication issues, use the IdP's monitoring and troubleshooting capabilities. The ACS does not log IdP authentication failures.

## STEP 2 | Configure explicit proxy settings.

1. Select **Panorama > Cloud Services > Configuration > Mobile Users - Explicit Proxy** and click the gear icon to edit the explicit proxy **Settings**.
2. In the **Settings** tab, edit the following settings:

- (Optional) In the Templates section, **Add** the template or templates that contains the configuration you want to push for explicit proxy.

By default, Prisma Access creates a new template stack **Explicit\_Proxy\_Template\_Stack** and a new template **Explicit\_Proxy\_Template**. If you have existing settings you want to import, import them now. If you are starting with a new explicit proxy configuration, make sure that you are using this template when you create and edit your **Network** and **Device** settings in Panorama.

You can **Add** more than one existing template to the stack and then order them appropriately using **Move Up** and **Move Down**. Panorama evaluates the templates in the stack from top to bottom, and settings in templates that are higher in the stack take priority over the same settings specified in templates that are lower in the stack. You cannot move the default **Explicit\_Proxy\_Template** from the top of the stack; this prevents you from overriding any required explicit proxy settings.

- In the Device Group section, select the **Parent Device Group** that contains the configuration settings you want to push for the explicit proxy, or leave the parent device group as **Shared** to use the Prisma Access device group shared hierarchy. The **Device Group Name** cannot be changed.
- (Optional) in the Master Device section, specify a **Master Device**.

Explicit Proxy uses Directory Sync to retrieve user and group information. Directory Sync does not auto-populate user and group information to security policy rules and to Panorama. To simplify rule creation based on user and group information, you can associate an on-premises or VM-series next generation firewall [as a Master Device](#).

- In the License Allocation section, specify the number of mobile users to allocate for explicit proxy.

Settings
?

Settings | Group Mapping Settings

**Template Stack**

Template Stack Name:

Templates	TEMPLATES
	Explicit_Proxy_Template

+ Add - Delete ↑ Move Up ↓ Move Down

The template at the top of the stack has the highest priority in the presence of overlapping config

**Device Group**

Device Group Name:

Parent Device Group:

Master Device:

**License Allocation**

Mobile Users License: 80000 (GlobalProtect: 75000, Explicit Proxy: 5000)

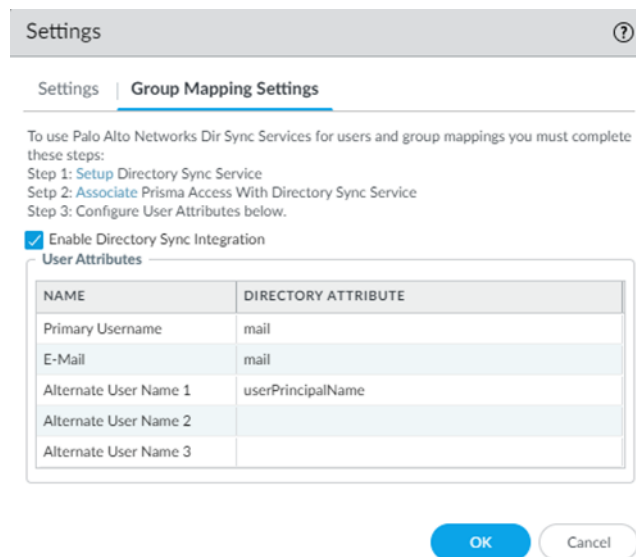
Allocated license count for Explicit Proxy:

OK
Cancel

- In the **Group Mapping Settings** tab, configure Prisma Access to use [Directory Sync for mobile users](#) to retrieve user and group information.

You use [Directory Sync](#) to populate user and group information for an explicit proxy deployment. To configure Directory Sync, you [set up Directory Sync on your AD](#) and associate the Panorama that manages Prisma Access with Directory Sync in the hub; then, set up [Directory Sync](#) in Prisma Access.

Enter **mail** for the Directory Attribute in the **Primary Username** field and **mail** for the **E-Mail** field.



4. Click **OK** when finished.

### STEP 3 | Click **Configure** to configure the explicit proxy setup.

1. Specify an **Explicit Proxy URL**.

By default, the name is *proxyname.proxy.prismaaccess.com*, where *proxyname* is the subdomain you specify, and uses port 8080. If you want to use your organization's domain name in the Explicit Proxy URL (for example, *thisproxy.proxy.mycompany.com*), enter a CNAME record your organization's domain.

For example, to map a proxy URL named *thisproxy.prismaaccess.com* to a proxy named *thisproxy.proxy.mycompany.com*, you would add a CNAME of *thisproxy.proxy.prismaaccess.com* to the CNAME record in your organization's domain.

2. Specify an **Authentication Profile** and **Cookie Lifetime**.

- Specify the SAML **Authentication Profile** you used in Step 1, or add a **New** authentication profile to use with Prisma Access.

You must [configure SAML authentication](#), including configuring a **SAML Identity Provider (IdP)** and an **Authentication Profile**, to use an explicit proxy.

- (**Optional**) Specify a **Cookie Lifetime** for the cookie that stores the users' authentication credentials.

Prisma Access caches the user's credentials and stores them in the form of a cookie. To change the value, specify the length of time to use in Seconds, Minutes, Hours, or Days.

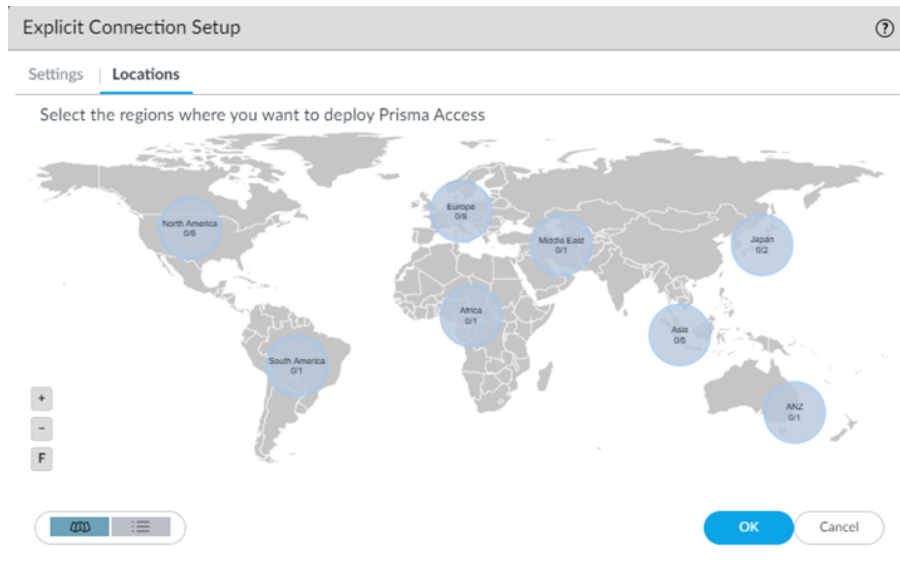
### STEP 4 | Select the **Locations** and the regions associated with those locations where you want to deploy your explicit proxy for mobile users. Prisma Access adds a proxy node into each location you select.

Explicit proxy supports a subset of all Prisma Access locations. See [Supported Explicit Proxy Locations](#) for the list of locations.

The **Locations** tab displays a map. Highlighting the map shows the global regions (Americas, Europe, and Asia Pacific) and the locations available inside each region. Select a region, then select the locations you want to deploy in each region. Limiting your deployment to a single region provides more granular control over deployed regions and allows you to exclude regions as required by your policy or industry regulations. See [List of Prisma Access Locations](#) for the list of regions and locations. You can select a

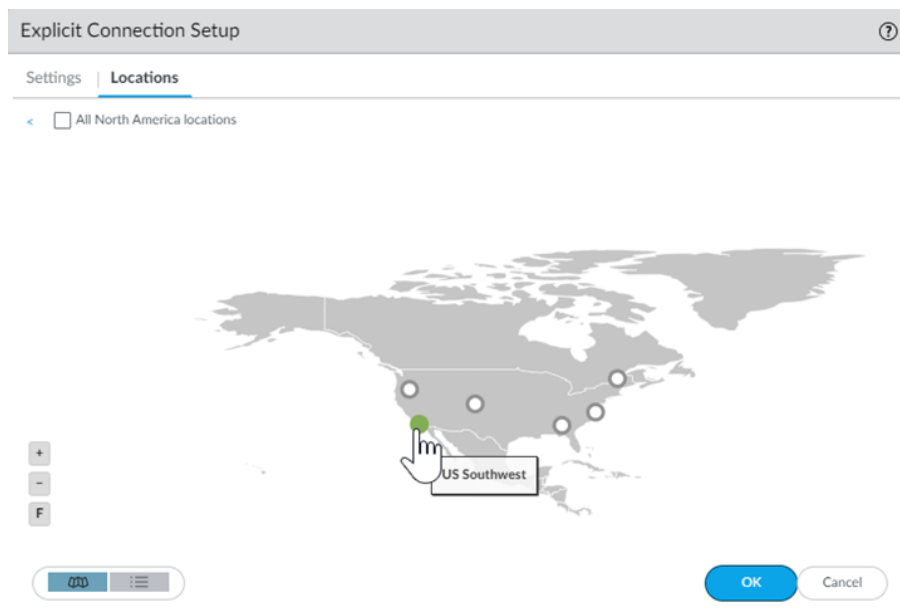
location in a region that is closest to your mobile users, or select a location as required by your policy or industry regulations.

1. Click the **Locations** tab and select a region.

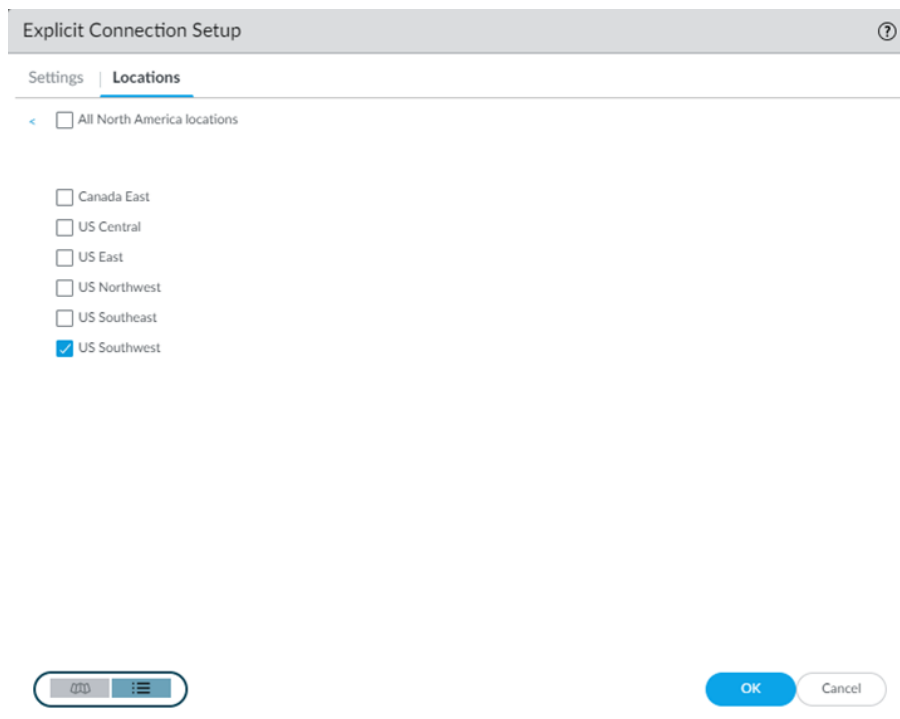


2. Select one or more explicit proxy locations within your selected region using the map.

Hovering your cursor over a location highlights it. White circles indicate an available location; green circles indicate that you have selected that location.



In addition to the map view, you can view a list of regions and locations. Choose between the map and list view from the lower left corner. In the list view, the list displays regions sorted by columns, with all locations sorted by region. You can select **All** sites within a region (top of the dialog).



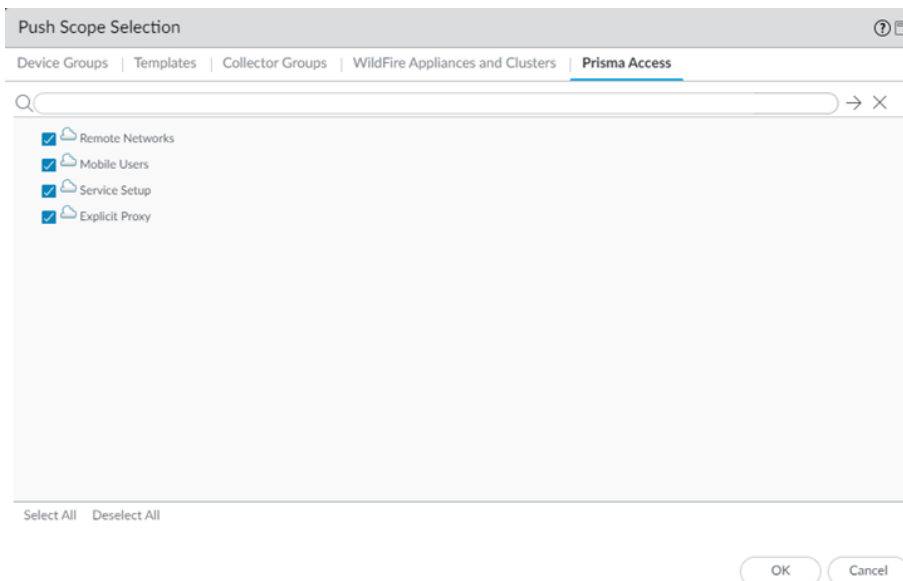
3. Click **OK** to add the locations.

**STEP 5 |** Configure security policy rules to enforce your organization’s security policies.

Explicit proxy has rules and recommendations for configuring security policy rules, and you must configure a decryption policy to strip out ALPN headers. See [Security Policy Guidelines and Requirements](#) for details.

**STEP 6 |** Commit your changes to Panorama and push the configuration changes to Prisma Access.

1. Click **Commit > Commit and Push**.
2. **Edit Selections** and, in the **Prisma Access** tab, make sure that **Explicit Proxy** is selected in the **Push Scope**, then click **OK**.



3. Click **Commit and Push**.

**STEP 7 |** Select the PAC file to use with the explicit proxy.

1. Select **Panorama > Cloud Services > Configuration > Mobile Users > Explicit Proxy**.

Be sure that you enter a port of 8080 in the PAC file.

2. Select the **Connection Name** for the explicit proxy setup you just configured.
3. Enter the **PAC (Proxy Auto-Configuration) File** to use for the explicit proxy.



*Be sure that you understand how PAC files work and how to modify them before you upload them to Prisma Access.*

Proxy Auto Configuration

Download sample PAC file

PAC (Proxy Auto-Configuration) File  Browse...

**Browse** and upload the file.

Prisma Access provides you with a sample PAC file; you can **Download sample PAC file**, change the values, and upload that file. See [PAC File Guidelines and Requirements](#) for PAC file requirements and guidelines as well as a description of the contents of the sample PAC file.

## PAC File Guidelines and Requirements

Use the following guidelines and requirements when configuring the PAC file to use with explicit proxy:

- Only ASCII text format is supported for PAC files. Palo Alto Networks recommends that you create and save the PAC file in a text editor such as VI or Vim.
- Upload the PAC file after you create your explicit proxy configuration and commit and push your changes. After you upload your PAC file, a commit and push operation is not required.
- You must have at least one Prisma Access tenant Explicit Proxy URL in the `return "PROXY foo.proxy.prismaaccess.com:8080"` ; statement beginning for traffic ingressing to Prisma Access. Either use a configured domain used when you push your changes or use a valid IPv4 address or **DIRECT** keyword such as `PROXY paloaltonetworks-245139.proxy.prismaaccess.com:8080` or `PROXY 1.2.3.4:8080`, and so on.
- If the proxy is not being bypassed, then you must provide a **PROXY** keyword. A valid proxy statement is required if no **DIRECT** keyword is configured for the proxy bypass.
- If a valid **PROXY** statement is found before an invalid **PROXY** statement, explicit proxy skips the validity check all on all **PROXY** statements after the first. For example, a PAC file with the valid statement `PROXY paloaltonetworks-245139.proxy.prismaaccess.com:8080` followed by the invalid statement `PROXY foo.proxy.prismaaccess.com:8080` would be considered valid since explicit proxy skips the validity check for `foo.proxy.prismaaccess.com:8080`.
- If you are using a **PROXY** statement to have ACS traffic bypass the Prisma Access proxy, the **PROXY** statement should not use the Explicit Proxy URL. In this configuration, the explicit proxy provides an error message, but allows you to upload the PAC file. You can direct the ACS traffic to other proxies using a valid FQDN or IPv4 address, or directly to the internet, using the **DIRECT** keyword.
- Only IPv4 addresses are supported in **PROXY** statements. Do not use IPv6 addresses in **PROXY** statements.
- The maximum file size for a PAC file is 256 KB.
- You must specify IdP and ACS URLs to be bypassed.
- You cannot delete a PAC file after you're uploaded it. You can, however, upload a new PAC file to overwrite the existing one.

- Explicit proxy supports only one hosted PAC file.
- If you change the Explicit Proxy URL in Prisma Access but do not change the PAC file to reflect the changed URL, the change won't be applied.
- If you change the Explicit Proxy URL in Prisma Access but do not change the PAC file to reflect the change, the change won't be applied. You must upload a new PAC file specifying the new Explicit Proxy URL.

Explicit proxy provides you with a sample PAC file that you can modify and use as the PAC file for your explicit proxy deployment. The sample PAC file that Prisma Access provides contains the following data:

```
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";
}
```

If you want to use the default PAC file that Prisma Access provides, you can optionally modify the fields in the PAC file as described in the following table.

Text	Description
<pre>var resolved_ip =   dnsResolve(host); ... return "DIRECT";</pre>	<p>Enter any hostnames or IP addresses that should not be sent to the explicit proxy between the JavaScript functions <code>var resolved_ip =</code> and <code>return "DIRECT";</code>.</p> <p>If you do not modify the data in this file, the following hostnames and IP addresses bypass the explicit proxy:</p> <ul style="list-style-type: none"> <li>• <code>if (isPlainHostName(host)</code>—Bypasses the explicit proxy for hostnames that contain no dots (for example, <code>http://intranet</code>).</li> <li>• <code>shExpMatch(host, "*.local")   </code>—Bypasses the proxy for any hostnames that are hosted in the internal network (localhost).</li> <li>• <code>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,</code></li> </ul>



Text	Description
	<pre>"192.168.0.0", "255.255.0.0")    isInNet(resolved_ip, "127.0.0.0", "255.255.255.0"))—Bypasses the explicit proxy for any IP addresses that are in the private or loopback IP address range.</pre>
<pre>if (url.substring(0,4) == "ftp:") return "DIRECT";</pre>	<p>Bypasses the explicit proxy for FTP sessions.</p>
<pre>if (shExpMatch(host, "*.okta.com")    shExpMatch(host, "*.oktacdn.com")) return "DIRECT";</pre>	<p>Bypasses the explicit proxy for the SAML IdP. Be sure to add the following FQDNs in this section:</p> <ul style="list-style-type: none"> <li>• Add the <b>ACS FQDN</b>. Find this FQDN under <b>Panorama &gt; Cloud Services &gt; Status &gt; Network Details &gt; Mobile Users—Explicit Proxy &gt; ACS FQDN</b>.</li> <li>• All FQDNs used by the IdP.</li> </ul> <p>If you use Okta as the IdP used for SAML authentication, enter <b>*.okta.com</b> and <b>*.oktacdn.com</b>.</p>
<pre>if (shExpMatch(host, "*.acs.prismaaccess.com")) return "DIRECT";</pre>	<p>Bypasses the explicit proxy for the Prisma Access Authentication Cache Service (ACS).</p>
<pre>return "PROXY foo.proxy.prismaaccess.com:8080"</pre>	<p>Bypasses the explicit proxy for the Explicit Proxy URL.</p> <p>You must have at least one Prisma Access tenant Explicit Proxy URL in the <code>return "PROXY foo.proxy.prismaaccess.com:8080";</code> statement for traffic ingressing to Prisma Access. Either use a configured domain used when you push your changes, or use a valid IPv4 address or DIRECT keyword such as <code>PROXY paloaltonetworks-245139.proxy.prismaaccess.com:8080</code> or <code>PROXY 1.2.3.4:8080</code>.</p>

## Security Policy Guidelines and Requirements

To make required configuration changes and to control the URLs that mobile users can access from the explicit proxy, use security policies. Use the following guidelines and requirements when configuring your security policies:

- Based on your business goals, create security policies for sanctioned internet and SaaS apps using App-ID and user groups that need access to those applications.

- Create a security policy rule at the bottom of the list with web browsing and SSL App-IDs for any user to allow access to internet sites for cases such as CORS requests or undecrypted HTTPs where users cannot be identified.
- Attach security profiles to all security policy rules so that you can prevent both known and unknown threats following the [security profile best practices](#).
- Ensure that your security policy rules do not allow traffic for non-HTTP/HTTPS protocols and non-standard web ports.
- Create a decryption profile and a decryption policy rule to remove ALPN headers from uploaded files. Explicit proxy does not support native HTTP/2 support, so you must remove the ALPN headers.

1. Select **Objects > Decryption > Decryption Profile**.

Choose any device group in the Device Group drop-down at the top of the page; decryption profiles are shared across device groups.

2. **Add** a new profile and give it a **Name**.

3. Select **SSL Forward Proxy**, then select **Strip ALPN** in the **Client Extension** area.

The screenshot shows the 'Decryption Profile' configuration page. The 'Name' field contains 'remove-ALPN'. There are checkboxes for 'Shared' and 'Disable override'. Under 'Decryption Mirroring', the 'Interface' dropdown is set to 'None', and there is a checkbox for 'Forwarded Only'. The 'SSL Decryption' tab is selected, with sub-tabs for 'SSL Forward Proxy', 'SSL Inbound Inspection', and 'SSL Protocol Settings'. The 'SSL Forward Proxy' sub-tab is active, showing 'Server Certificate Verification' (with several unchecked checkboxes and a 'Details' link), 'Unsupported Mode Checks' (with three unchecked checkboxes), 'Failure Checks' (with three unchecked checkboxes), and 'Client Extension' (with the 'Strip ALPN' checkbox checked). At the bottom right, there are 'OK' and 'Cancel' buttons. A note at the bottom states: 'Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted. Check boxes to block those sessions instead.'

4. Select **Policies > Decryption**.

5. **Add** a decryption policy and give it a **Name**.

6. In the **Options** area, select an **Action** of **Decrypt** and the **Decryption Profile** you created.

## Verify and Monitor the Explicit Proxy Deployment

After you have configured the explicit proxy for mobile users, monitor the status and troubleshoot any issues by checking the following Prisma Access components.

- Check the status of your explicit proxy deployment.
  - Select **Panorama > Cloud Services > Status > Status** to see the explicit proxy status.

**Mobile Users - Explicit Proxy**

Status ● OK

---

Config Status ● OK

---

Current Users **1**

---

Users (Last 90 days) **12**

---

Deployment Status ● Success (details)

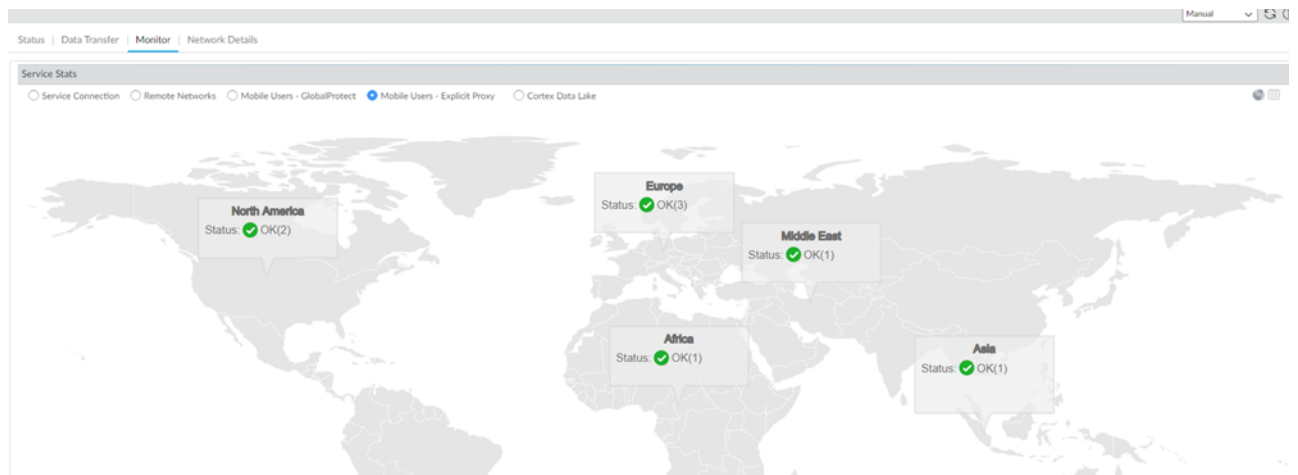
The mobile users **Status** and **Config Status** fields indicate whether the connection between Prisma Access and your mobile users is **OK**, unable to fetch the status on the tunnel (**Warning**), or that the mobile users cannot connect to the explicit proxy (**Error**).

Click the hyperlink next to **Current Users** and **Users (Last 90 days)** to get more information about mobile users.

- **Current Users**—The current number of authenticated users who have browsed traffic in the last five minutes.
- **Users (Last 90 days)**—The number of unique authenticated explicit proxy users for the last 90 days.

Users (Last 90 days)				
IP ADDRESS	REGION	USER AGENT	USER	LOGIN AT
	us-west-2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.190 Safari/537.36		2021-02-25 11:39:53 PS
	us-west-2	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0		2021-02-25 07:57:44 PS
	us-central1	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.193 Safari/537.36		2021-02-11 13:01:14 PS
	us-central1	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.96 Safari/537.36		2021-02-10 17:17:32 PS
	us-west-2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36		2021-02-19 12:33:23 PS
	us-central1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.104 Safari/537.36		2021-02-03 21:57:43 PS
	us-central1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.104 Safari/537.36		2021-02-03 22:35:46 PS
	us-west-2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36		2021-02-25 05:03:05 PS
	us-west-2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36		2021-02-23 22:29:16 PS
	us-west-2	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.3 Safari/605.1.15		2021-02-23 00:06:43 PS
	us-west-2	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36		2021-02-24 06:13:47 PS
	us-central1	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:85.0) Gecko/20100101 Firefox/85.0		2021-02-09 18:21:55 PS

- Select **Panorama > Cloud Services > Status > Monitor > Mobile Users—Explicit Proxy** to display a map showing the deployed explicit proxy locations.



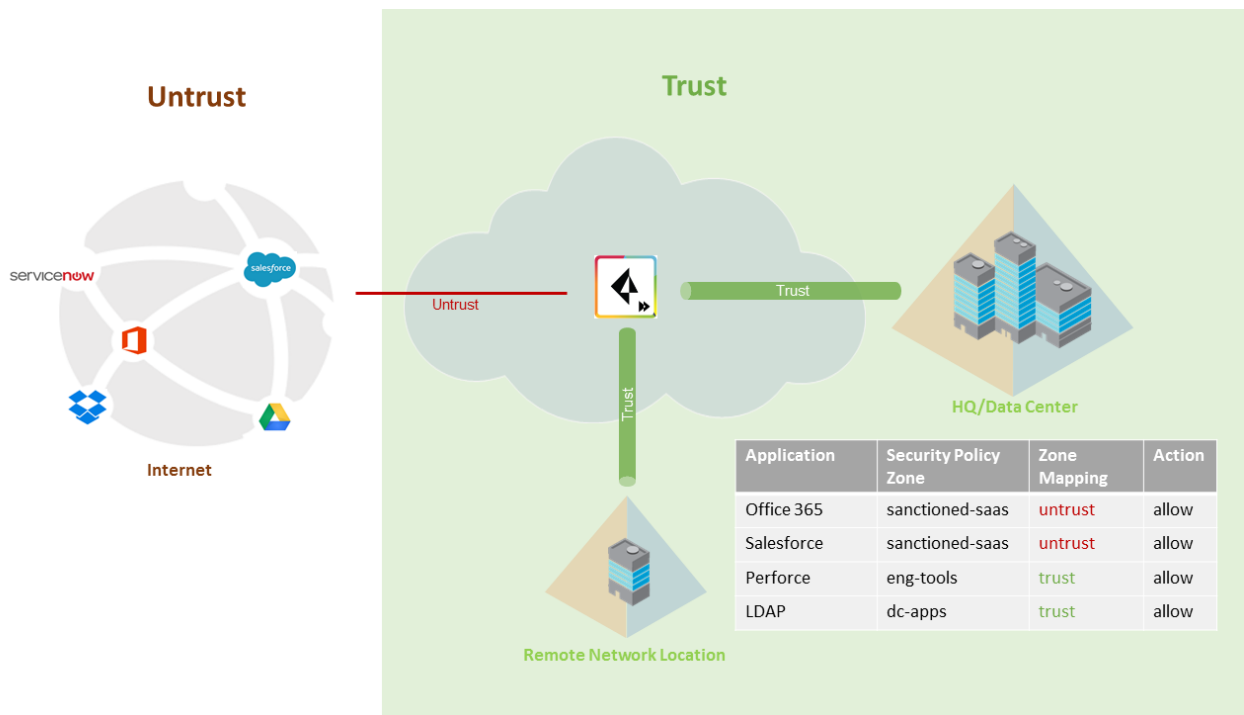
- Select **Panorama > Cloud Services > Status > Network Details > Mobile Users—Explicit Proxy** to view the following details:

EXPLICIT PROXY URL	ACS FQDN	SAML META DATA
panwppcproxy.proxy.panclouddev.com:8080	global-qa.acs.panclouddev.com	<a href="#">Export SAML Metadata</a>

- **Explicit Proxy URL**—The URL used to the explicit proxy.
- **ACS FQDN**—The FQDN of the ACS.
- **SAML Meta Data**—The authentication profile metadata used by SAML. You can **Export SAML Metadata** to save the metadata file.

# Zone Mapping

On a firewall, zones are associated with interfaces. But within Prisma Access, the networking infrastructure is automatically set up for you. This means that you no longer need to worry about configuring interfaces and associating them with the zones you create. However, to enable consistent security policy enforcement, you must create zone mappings so that Prisma Access will know whether to associate a zone with an internal (trust) interface or an external (untrust) interface. This will ensure that your security policy rules are enforced properly. By default, all of the zones you push to Prisma Access are set to untrust. You should leave any zones associated with internet-bound traffic, including your sanctioned SaaS applications, set to untrust. However, for all zones that enable access to applications on your internal network or in your data center, you must map them to trust. Notice in the example below, all sanctioned SaaS applications—Office 365 and Salesforce in this case—are segmented into the sanctioned-saas zone to enable visibility and policy enforcement over the use of these applications. To enable Prisma Access to associate the sanctioned-saas zone with an external-facing interface, you must map this zone to untrust. Similarly, the eng-tools and dc-apps zones provide access to applications in the corporate office and you must therefore designate them as trusted zones.



When creating zones, do not use any of the following names for the zones, because these are names used for internal zones:

- trust
- untrust
- inter-fw
- Any name you use for the remote networks (remote network names are used as the source zone in Cortex Data Lake logs)

---

# Specify IP Address Pools for Mobile Users

You need to make sure that you have specified an IP address pool that allows enough coverage for the mobile users in your organization. It is important to remember that each unique user can use multiple devices to connect to Prisma Access at the same time, and each connected device requires a unique IP address from the pool. The addresses in this pool must not overlap with other address pools you use internally or with the IP subnet you assign when you [Enable the Service Infrastructure](#).

We recommend that the number of IP addresses in the pool is 2 times the number of mobile user devices that will connect to Prisma Access. If your organization has a bring your own device (BYOD) policy, or if a single user has multiple user accounts, make sure that you take those extra devices and accounts into consideration when you allocate your IP pools. If your pool space is limited, you can specify a smaller address pool; however, if your IP address pool reaches its limit, additional mobile user devices will not be able to connect.

In Panorama, the UI validates that you enter valid IP subnets (for example, if you enter a pool with a subnet of less than /23, it will prompt you to change it). However, it does not check to ensure that you have allocated sufficient IP addresses for your deployment.



*This validation is not available if you configure locations using CLI. If you deploy all locations using CLI, we recommend that you add a /18 address in the Worldwide pool for mobile users.*

Prisma Access checks your configuration to make sure that you have specified the following minimum IP address pool:

- A minimum of /23 (512 IP addresses) is required for either a Worldwide or regional address pool.
- If you do not onboard any Prisma Access gateways in a region, an IP address pool for that region is not required. For example, if you specify gateways in the US East, US Northwest, and US Northeast locations, you need to only specify an IP address pool for the North America & South America region. Conversely, if you enable mobile user locations in Europe without specifying either a Worldwide address pool or an IP address pool in Africa, Europe, & Middle East, your deployment will fail.
- If you specify a mix of Worldwide and regional pools, Prisma Access uses the IP pools in the region first. If regional pools are exhausted, Prisma Access will take IP address blocks from the Worldwide pool, which allows you to configure extra IP addresses in the Worldwide IP address pool to function as a fallback pool.

If you specify more than one block of IP address pools, Prisma Access uses the pools in the order that you entered them during [mobile user setup](#).

---

# How the GlobalProtect App Selects a Prisma Access Location for Mobile Users

When a mobile user connects to a Prisma Access location, the app uses the following selection process to determine to which location it connects.



*You enable the mobile user locations where you want Prisma Access to be present during mobile user onboarding. If you do not select the location during onboarding, Prisma Access does not use it in your deployment.*

- If the mobile user connects in a country that has a Prisma Access location, the user connects to the location in that country.
- If the mobile user cannot connect to an in-country location for any reason, Prisma Access selects from one or more of the following mobile user locations to connect the user based on region:
  - **Asia, Australia & Japan:** India West, Japan Central, Singapore, Taiwan
  - **Africa, Europe & Middle East:** Finland, Germany Central, Netherlands Central, UK
  - **North America & South America:** Brazil South, Canada East, US Central, US Northeast

Palo Alto Networks recommends that you add these locations in their respective regions during mobile user onboarding to provide redundancy.

- Prisma Access has designated the following locations as alternative (fallback) locations. If mobile users cannot access in-country or in-region locations, Prisma Access connects mobile users to one of the following locations:
  - Hong Kong
  - Netherlands Central
  - US Northwest

Palo Alto Networks strongly recommends that you enable at least one of these locations during mobile user onboarding.
- If you use on-premises gateways with Prisma Access locations, you can specify priorities in Prisma Access to let mobile users connect to either a specific on-premises GlobalProtect gateway or a Prisma Access location. See [Manage Priorities for Prisma Access and On-Premises Gateways](#) for details.
- When mobile users connect, the GlobalProtect app does not use the following Prisma Access locations in the automatic gateway selection process, even if you selected the Prisma Access locations in the plugin during onboarding. However, mobile users can still manually select one of these locations and set it as a [preferred location \(gateway\)](#) as long as you allow them to [manually select those locations](#) during mobile user onboarding:
  - Australia: Australia East and Australia South
  - Brazil: Brazil East and Brazil Central
  - Canada: Canada Central
  - France: France South
  - Germany: Germany North and Germany South
  - India: India North and India South
  - Mexico: Mexico West
  - Netherlands: Netherlands South
  - Pakistan: Pakistan West
  - Russia: Russia Northwest
  - Spain: Spain East

---

# View Logged In User Information and Log Out Current Users

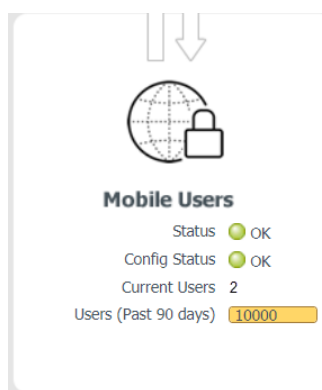
There are several locations in Panorama where you can view the list of logged-in users. You can view unique users, the location in which the users are logged in, and tables that provide additional information. It is also important to understand how Prisma Access counts the number of users in each location.

You can get a detailed view of users from several locations:


- To see an [overall view of users](#) and to open a table that allows you to view and log out logged-in users, select **Panorama > Cloud Services > Status > Status**.
- To see a [graphic view of users](#) in a map view, and to view users by region and location, select **Panorama > Cloud Services > Status > Service Stats > Mobile Users**.
- To learn how Prisma Access counts users in each of these areas, see [How Prisma Access Counts Users](#).

## View Mobile Users from the Status Tab

To view the total number of unique users who are currently logged in across all locations, select **Panorama > Cloud Services > Status > Status**.



To view more details about the users who are currently logged in, click the hyperlinked number next to **Current Users** to display the **Current Users** table.

 *The total number of users that display in the Status page, and the number that displays in the pop-up table, might be different; the number that displays in the table might be larger. See [How Prisma Access Counts Users](#) for details.*

You can log out active users from the **Current Users** table; to do so, select the user and click **Logout**. Note that you might have to close and then re-open the screen to have Prisma Access remove the logged-out user from the **Current Users** page.

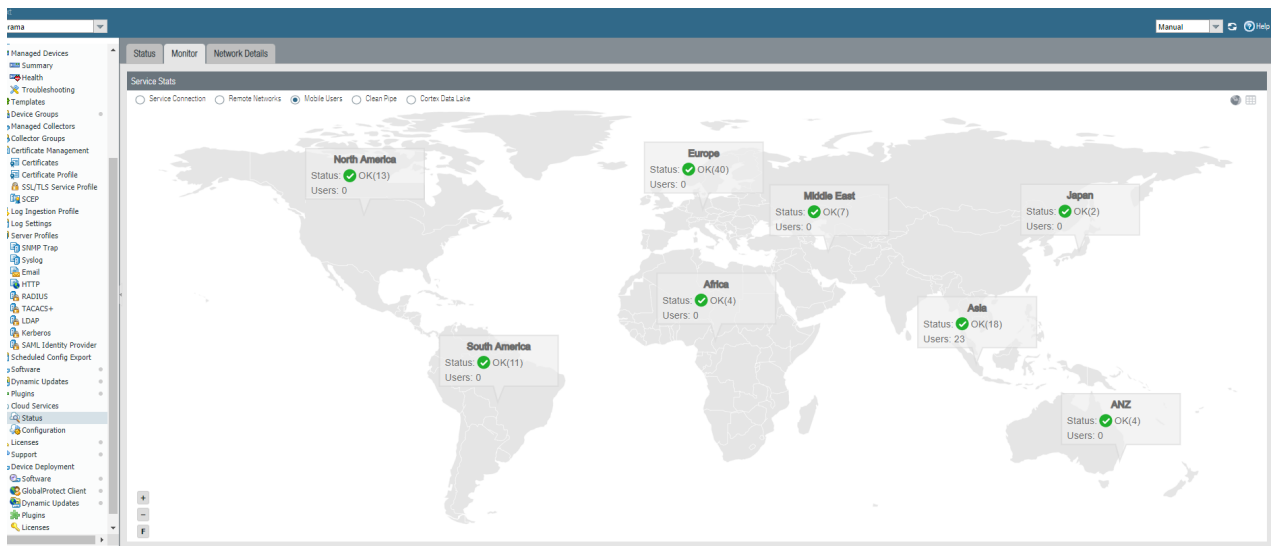
The following screen shows users who logged in with the GlobalProtect app and with Clientless VPN. The screen shows the users' username, public IP, and last login time. If the user is logged in with the GlobalProtect app, it also shows their client OS, private IP address, and computer name.



Domain	Client OS	Private IP	Computer	User	Public IP	Login At	Logout
	Browser			test1		2019-07-18 15:44:28 PDT	
	Apple Mac OS X 10.13.6	10.19.19.2	-MacBook-Pro	test		2019-07-18 15:44:21 PDT	

## View Mobile Users from the Monitor Tab

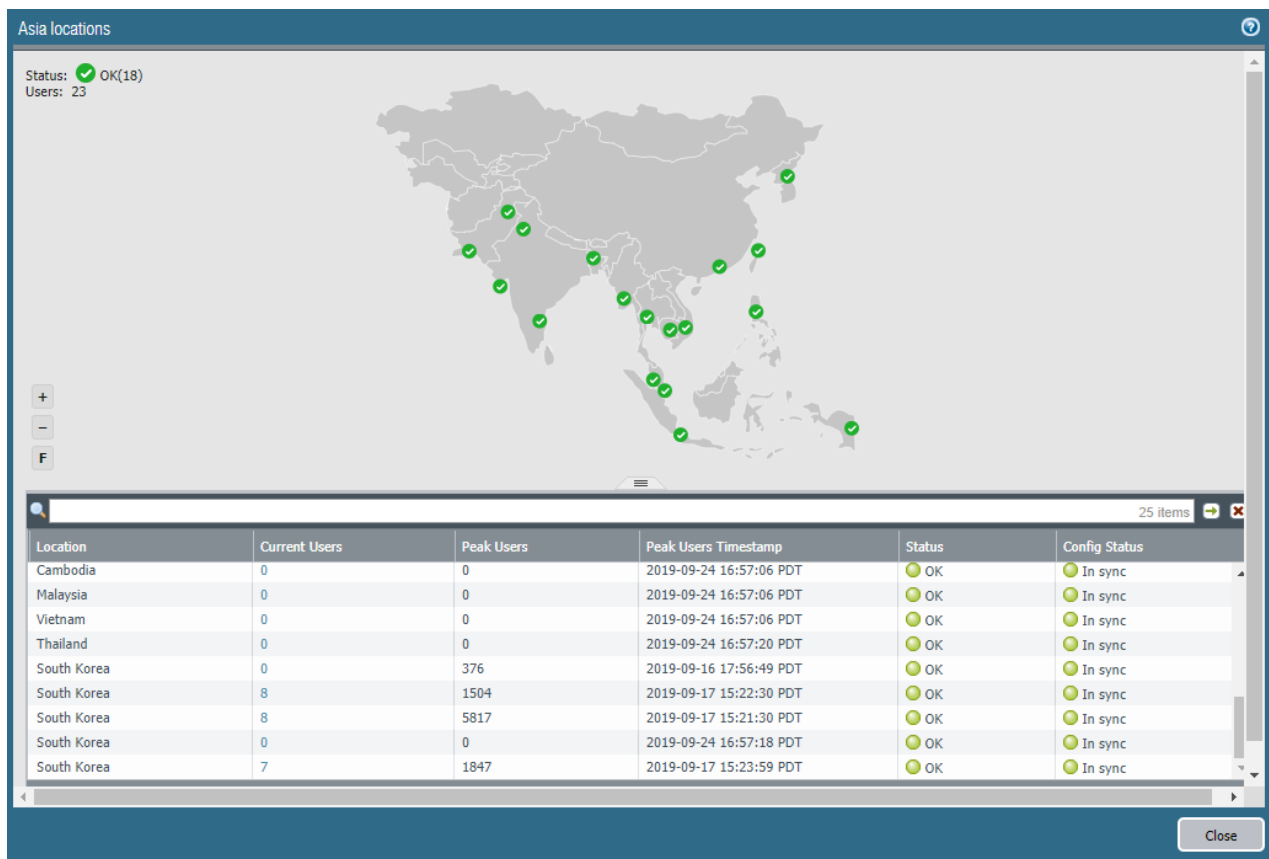
To view the number of unique users that are logged in per region, select **Panorama > Cloud Services > Status > Service Stats > Mobile Users**.



To view details about locations in a region, click the region.



*The number of users that displays in the global map view page and the number that displays in the table per region might be different; the number that displays in the table might be larger. See [How Prisma Access Counts Users](#) for details.*



## How Prisma Access Counts Users

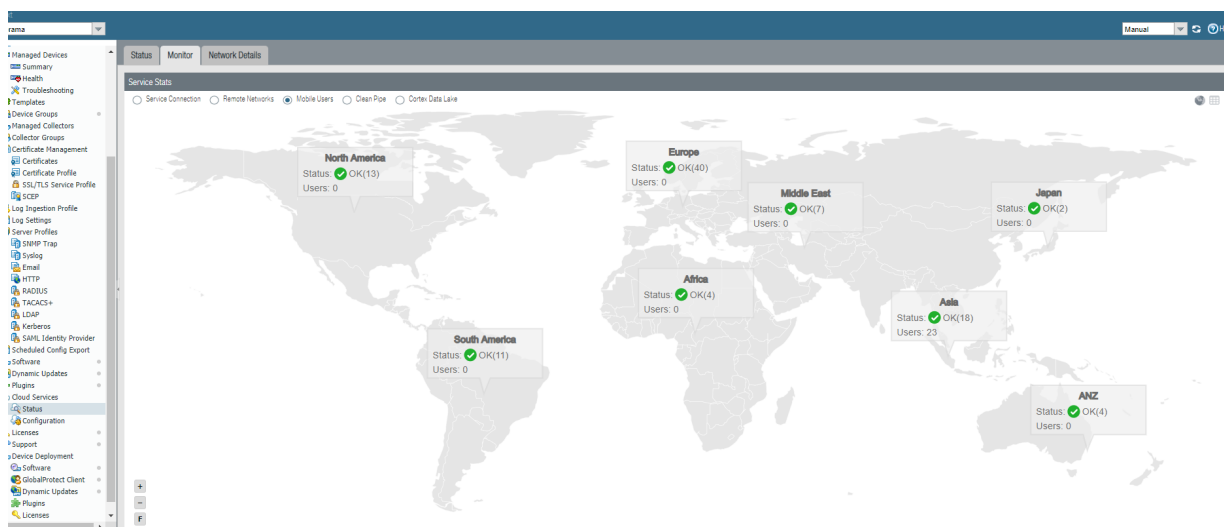
The number of total users that display in the status areas might be different than the number that displays in the associated tables. The following section describes the differences.

- Status tab (Panorama > Cloud Services > Status > Status)**—The number of users that displays in the main page, in the **Mobile Users** area, might be different than the number that displays in the table when you click the **Current Users** hyperlink. The number that displays in the **Mobile Users** area counts the number of unique users; the list of users in the **Current Users** table counts all users per login or connection. If a single user is logged in to more than one gateway or is connected with multiple devices, the number in the table might be larger.

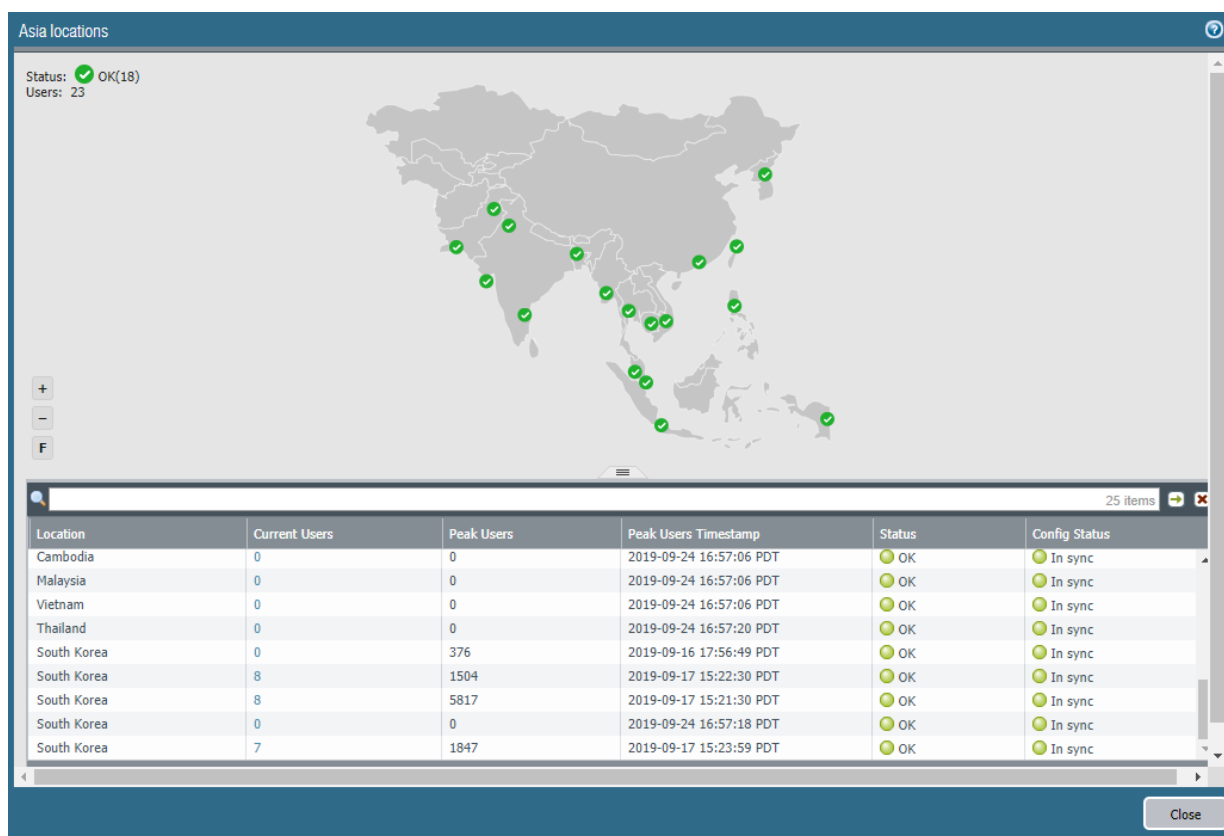
For example, a user **user1** is logged into two gateways in the **United Kingdom** location; this condition might have occurred because Prisma Access automatically added gateways when a large number of users logged in to the same location. In this case, Prisma Access counts **user1** once in the **Mobile Users** area, but twice in the **Current Users** table.

- Monitor tab (Panorama > Cloud Services > Status > Service Stats > Mobile Users)**—The number of **Users** you see in the global map might be different than the number that displays in the table when you select a region. A user that is logged in to more than one gateway or is connected with multiple devices might show up multiple times in the table.

The following screenshots provide an example. There are 23 unique users logged into the **Asia** region, as shown in the global map.



If you select the **Asia** region, Prisma Access gives the number of unique users (23) on the top left of the region page. However, two users are connected via multiple devices in the **South Korea** location (for example, a smart phone and a computer). Because the users have two separate connections, Prisma Access counts them twice in the table, giving a total number count in the table of 25.



---

# Quick Configs for Mobile User Deployments

The following topics show some common Prisma Access deployment scenarios for remote networks and provide instructions for how to configure them.

For information about integrating Prisma Access with third-party authentication providers, refer to the [Prisma Access Integration Guide](#).

- [Prisma Access with On-Premises Gateways](#)
- [Manage Priorities for Prisma Access and On-Premises Gateways](#)
- [DNS Resolution for Mobile Users and Remote Networks](#)
- [Sinkhole IPv6 Traffic From Mobile Users](#)
- [Identification and Quarantine of Compromised Devices With Prisma Access](#)
- [Collect User and Group Information Using the Directory Sync Service](#)
- [Configure Quality of Service in Prisma Access](#)

## Prisma Access with On-Premises Gateways

Prisma Access enables you to extend the Palo Alto Networks security platform out to your remote network locations and your mobile users without having to build out your own global security infrastructure and expand your operational capacity. In cases where you have already deployed GlobalProtect gateways in regions where you already have the infrastructure to manage it, you can leverage this investment by configuring Prisma Access to direct mobile users to your existing external gateways when appropriate.

You can [Manage Priorities for Prisma Access and On-Premises Gateways](#), which allow you to specify priorities for on-premises and Prisma Access gateways. Administrators cannot specify mobile users to connect to a specific Prisma Access gateway; however administrators can [Allow Mobile Users to Manually Select Specific Prisma Access Gateways](#) using the GlobalProtect app.



*You cannot use your own portal with Prisma Access. You can only use the portal that is deployed when your Prisma Access for mobile users is provisioned.*

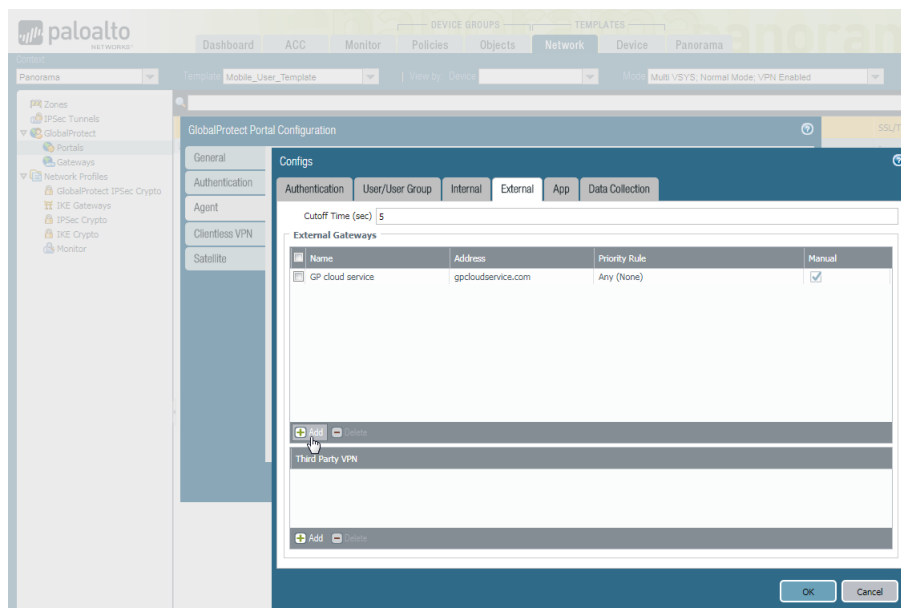
To configure one of these hybrid Prisma Access deployments, you must edit the GlobalProtect\_Portal configuration within the Mobile\_User\_Template to add your on-premises gateways to the appropriate regions:


### STEP 1 | Edit the Prisma Access portal configuration.

1. To add an existing gateway to the list of available gateways, select **Network > GlobalProtect > Portals**.
2. Select **Mobile\_User\_Template** from the **Template** drop-down.
3. Select **GlobalProtect\_Portal** to edit the Prisma Access portal configuration.

### STEP 2 | Add your on-premises gateway to the list of gateways in the agent configuration.

1. Select the **Agent** tab and select the **DEFAULT** agent configuration or **Add** a new one.
2. Select the **External** tab and **Add** your on-premises gateway.



 If you add a new agent configuration and you want to add the Prisma Access gateways to the list of external gateways in that configuration, you must set the Name to GP cloud service and the Address to gpcloudservice.com. You must enter these values exactly as shown, and you cannot use either of these values for non-Prisma Access gateways.

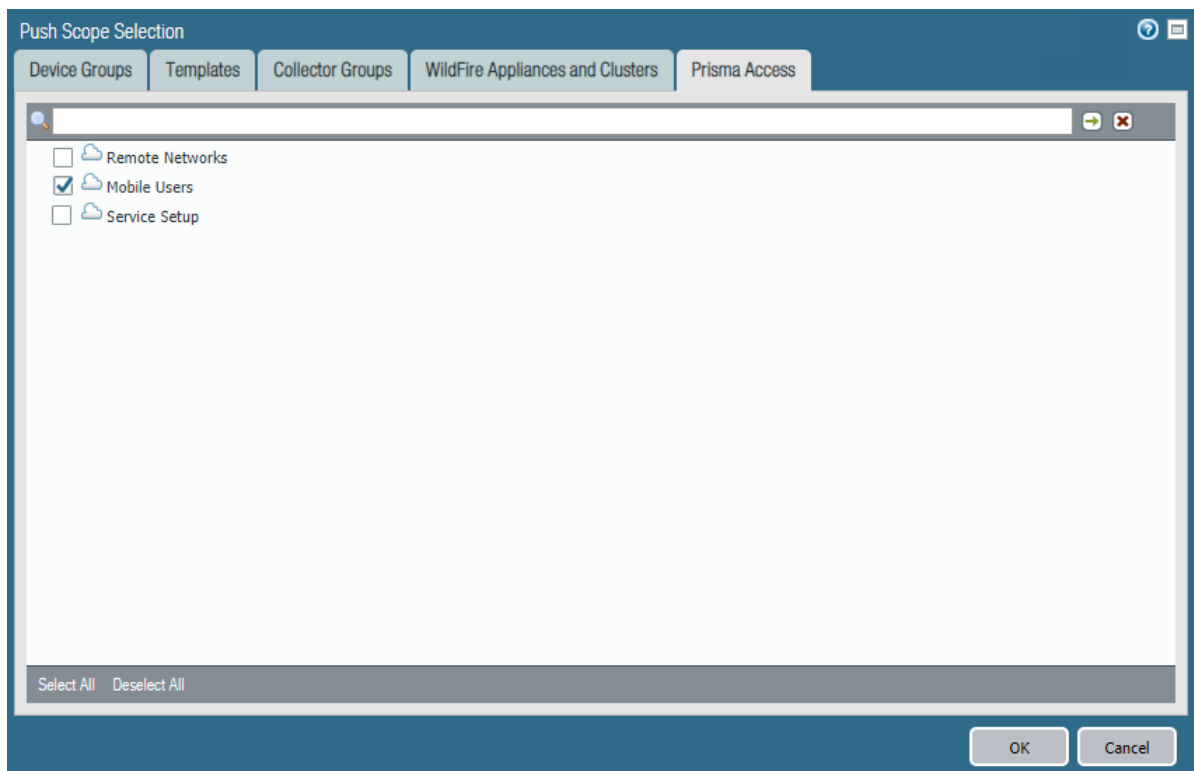
3. Enter the **Name** of the gateway and specify either the **FQDN** or **IP** address of the gateway in the **Address** field; this value must exactly match the common name (CN) in the gateway certificate.
4. (Optional) If you want mobile users to only connect to the gateway when they are in the corresponding region, **Add** the **Source Region** to restrict the gateway to. For example, if you have a gateway in France, you would select FR (France). If you have a gateway in Sweden, you would select (SE) Sweden.

One benefit of this is that users will then be able to access a gateway that enables access to internet resources in their own language.

5. Configure other [agent settings](#) as necessary to complete the agent configuration.
6. Click **OK** to save the portal configuration.

### STEP 3 | Commit all your changes to Panorama and push the configuration changes to Prisma Access.

1. Click **Commit** > **Commit to Panorama**.
2. Click **Commit** > **Push to Devices** and click **Edit Selections**.
3. On the **Prisma Access** tab, make sure **Prisma Access for users** is selected and then click **OK**.




4. Click **Push**.

## Manage Priorities for Prisma Access and On-Premises Gateways

Prisma Access enables you to extend the Palo Alto Networks security platform out to your mobile users. In a hybrid deployment where your enterprise uses [Prisma Access with On-Premises Gateways](#), you can set priorities in Prisma Access to let mobile users connect to either a specific on-premises GlobalProtect gateway or a Prisma Access gateway.

You can select an on-premises gateway that is physically closest to your mobile users and allow users to connect to a different gateway (either on-premises or cloud) to ensure secure access for mobile users if they change locations. You can also specify priority for gateways that are in the same country or same linguistic area as your mobile users.

 *If you add on-premises gateways to your Prisma Access deployment, check to see if the priority for the Prisma Access gateways is set to None and, if it is, change the priority. If the priority is set to None, the service will not select a gateway. See [Configure Priorities for Prisma Access and On-Premises Gateways](#) to change the priority of your Prisma Access gateways.*

If you require users to connect to a specific Prisma Access gateway, you can [Allow Mobile Users to Manually Select Specific Prisma Access Gateways](#). Mobile users choose one of the Prisma Access gateways using the GlobalProtect app that is installed on their endpoint.

Complete the following workflow to configure gateway priorities in Prisma Access.

- [Set Equal Gateway Priorities for On-Premises and Prisma Access Gateways](#)
- [Set a Higher Gateway Priority for an On-Premises Gateway](#)
- [Set Higher Priorities for Multiple On-Premises Gateways](#)

- [Configure Priorities for Prisma Access and On-Premises Gateways](#)
- [Allow Mobile Users to Manually Select Specific Prisma Access Gateways](#)

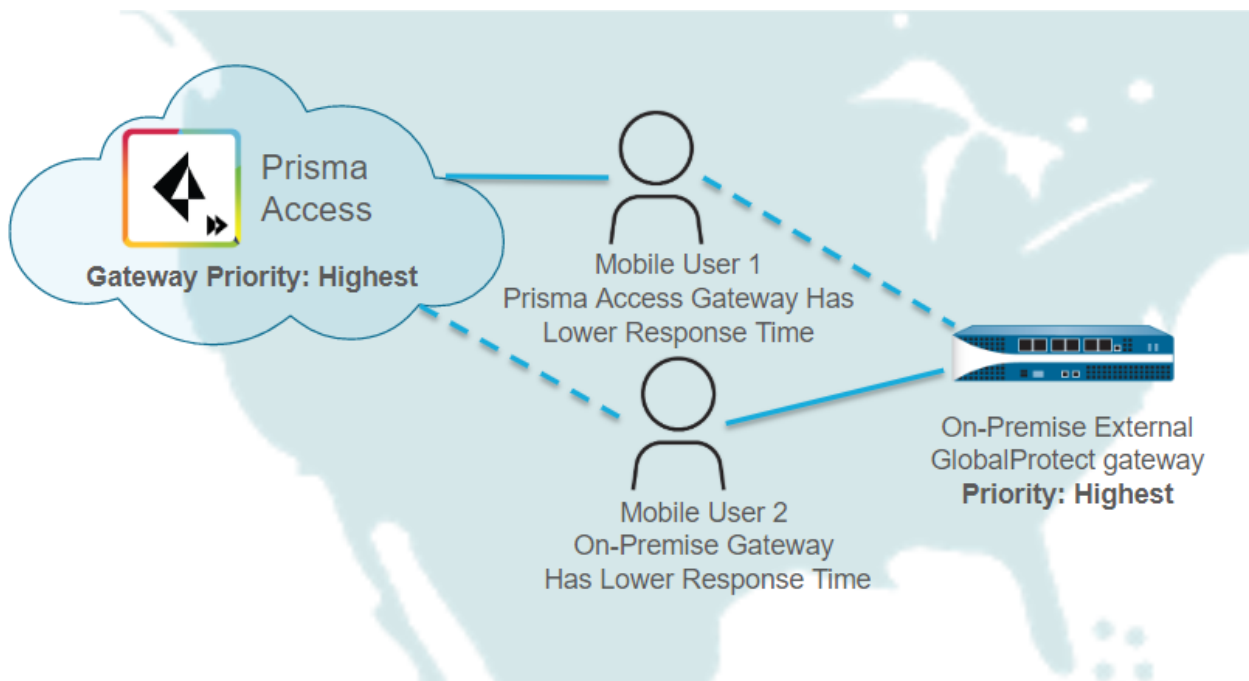
## Set Equal Gateway Priorities for On-Premises and Prisma Access Gateways

To enable secure access for your mobile workforce no matter where they are located, you can set equal priorities for the on-premises GlobalProtect gateways and the Prisma Access gateways. The GlobalProtect app uses [Gateway Priority in a Multiple Gateway Configuration](#) to determine the preferred gateway.

You can use this configuration if your mobile users are most often closer to an on-premises gateway. When users change locations, the GlobalProtect app chooses another gateway (either on-premises or Prisma Access gateway) based on the highest priority and lowest response time.

The following figure shows a sample configuration with two mobile users in North America. You set the gateway priority to **Highest** for both the Prisma Access gateways and the on-premises gateways.

In this example, User 1's GlobalProtect app determines that the Prisma Access gateway has a lower response time than the on-premises gateway, and user 2's GlobalProtect app determines that the on-premises gateway has a lower response time. Since all gateways have the same priority, User 1 connects to the Prisma Access gateway and User 2 connects to the on-premises gateway, based on the lower response time.



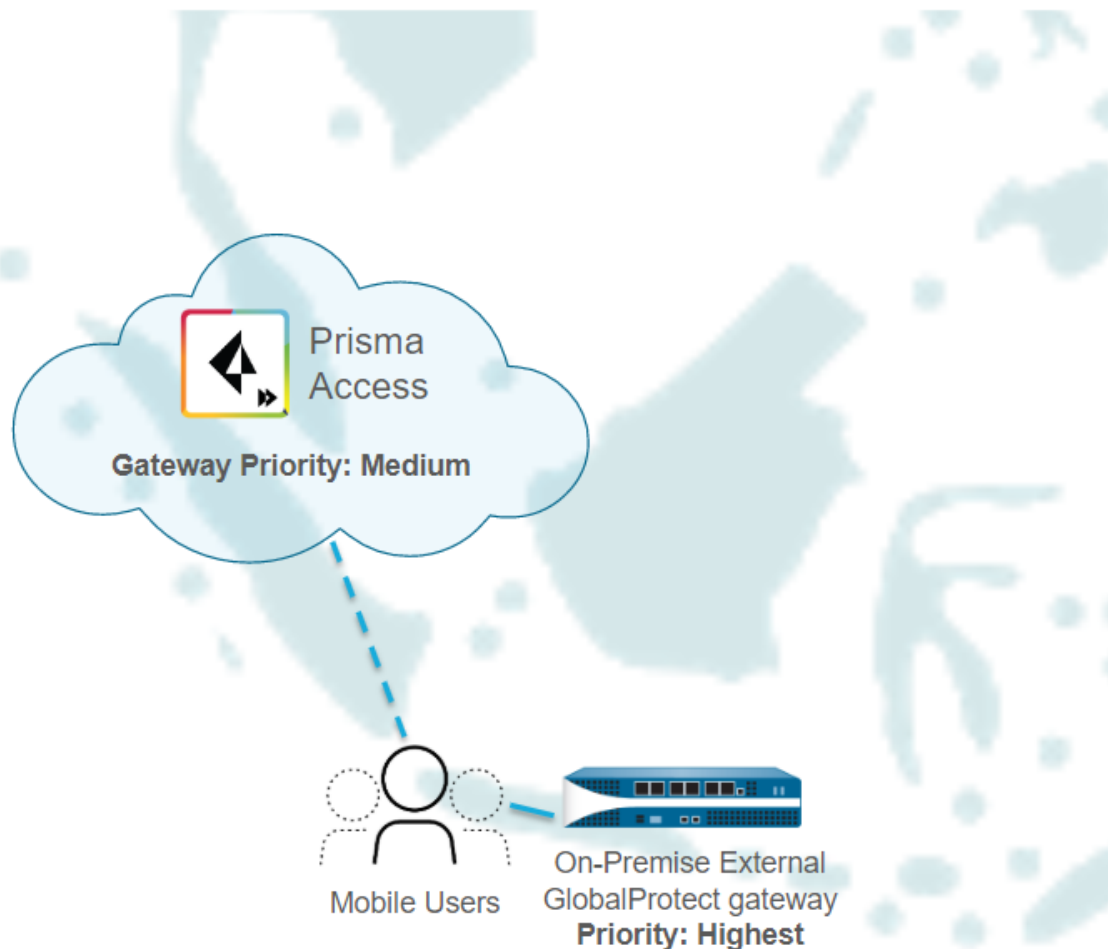
## Set a Higher Gateway Priority for an On-Premises Gateway

In situations where you want to direct mobile users to use an on-premises gateway instead of the Prisma Access gateways, specify the on-premises gateways with a source region and a higher priority than the Prisma Access gateway.

The following figure shows a sample configuration for mobile users in Indonesia. To avoid the possibility of mobile users being connected to the nearest Prisma Access gateway in Singapore, you set the gateway priority to **Highest** for the on-premises gateway in Indonesia and set the priority to **Medium** for the Prisma Access gateways.

This example also specifies a source region of Indonesia for the on-premises gateway. We recommend specifying a source region for the following reasons:

- Specifying a source region for an on-premises gateway allows users in a region to access that gateway and prevents users outside of that region from connecting to that gateway. In this example, only mobile users in Indonesia can connect to the on-premises gateway with the source region of Indonesia, and the higher priority means that the on-premise gateway has priority over the Prisma Access gateways.
- If you set a source region of **Any** for the on-premises gateway in Indonesia, every mobile user in your organization would prefer the on-premises gateway in Indonesia, because of its higher priority and worldwide accessibility. This configuration means that mobile users might never connect to the Prisma Access gateways.



## Set Higher Priorities for Multiple On-Premises Gateways

To ensure that traffic to the internet stays in language-specific regions, you can configure multiple gateways in multiple source regions, setting the priority of the on-premise gateways to **Highest** and the priority of the Prisma Access gateways to **Medium**.

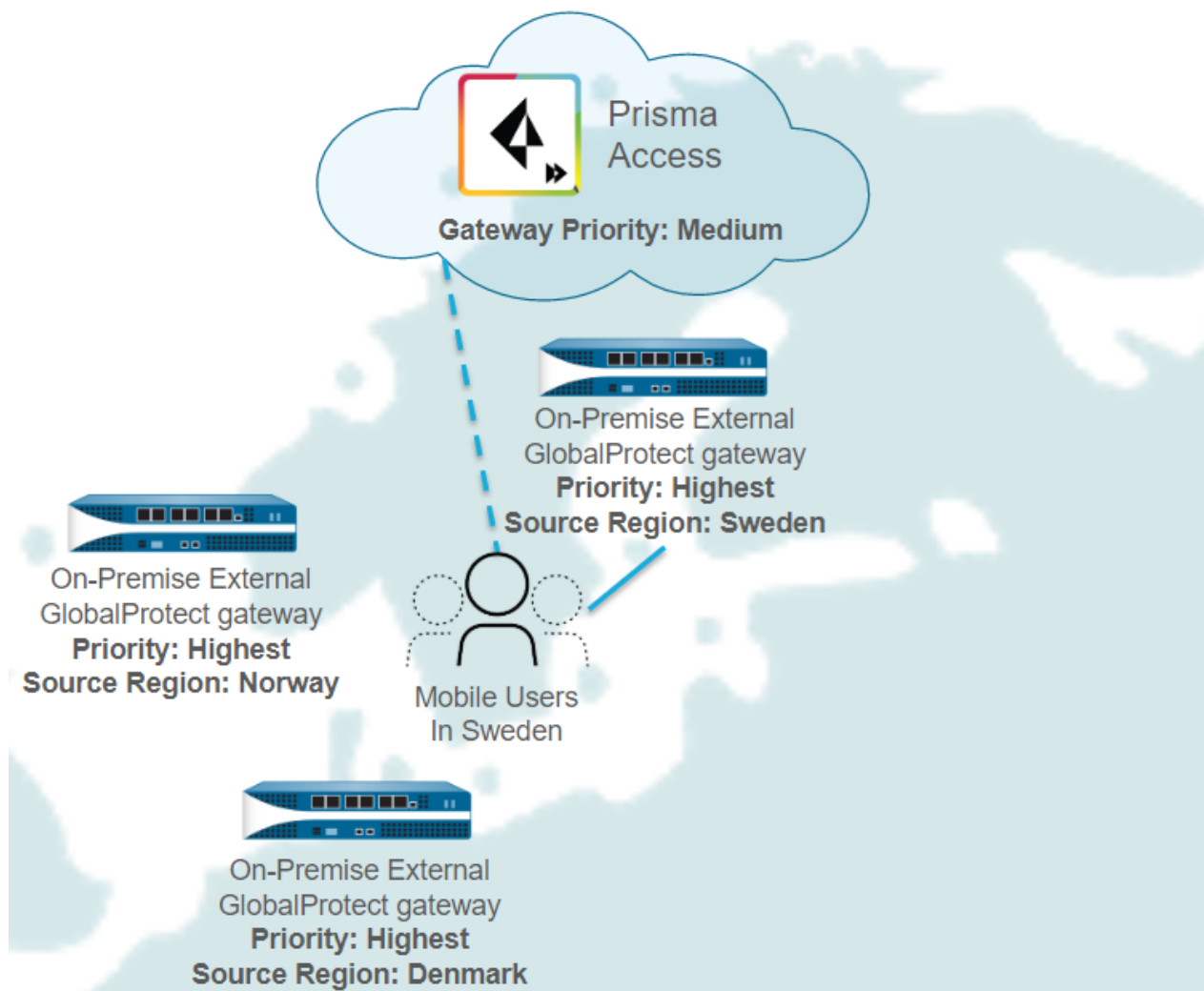
The following figure shows a sample configuration for mobile users in Scandinavia. Using this configuration, when the mobile users access internet websites, the websites use the character encoding set that is specific to their languages.

In this example, you configure on-premises gateways with source regions in Denmark, Norway, and Sweden. You set the priority of those gateways to **Highest** and set the priority of the Prisma Access



gateways to **Medium**. Specifying a source region for the on-premises gateways allows users in those regions to access those gateways, and prevents users outside of those regions from connecting to those gateways.

In this example, the GlobalProtect app for mobile users in Sweden selects the on-premises gateway in Sweden because of the source region and higher gateway priority.



## Configure Priorities for Prisma Access and On-Premises Gateways

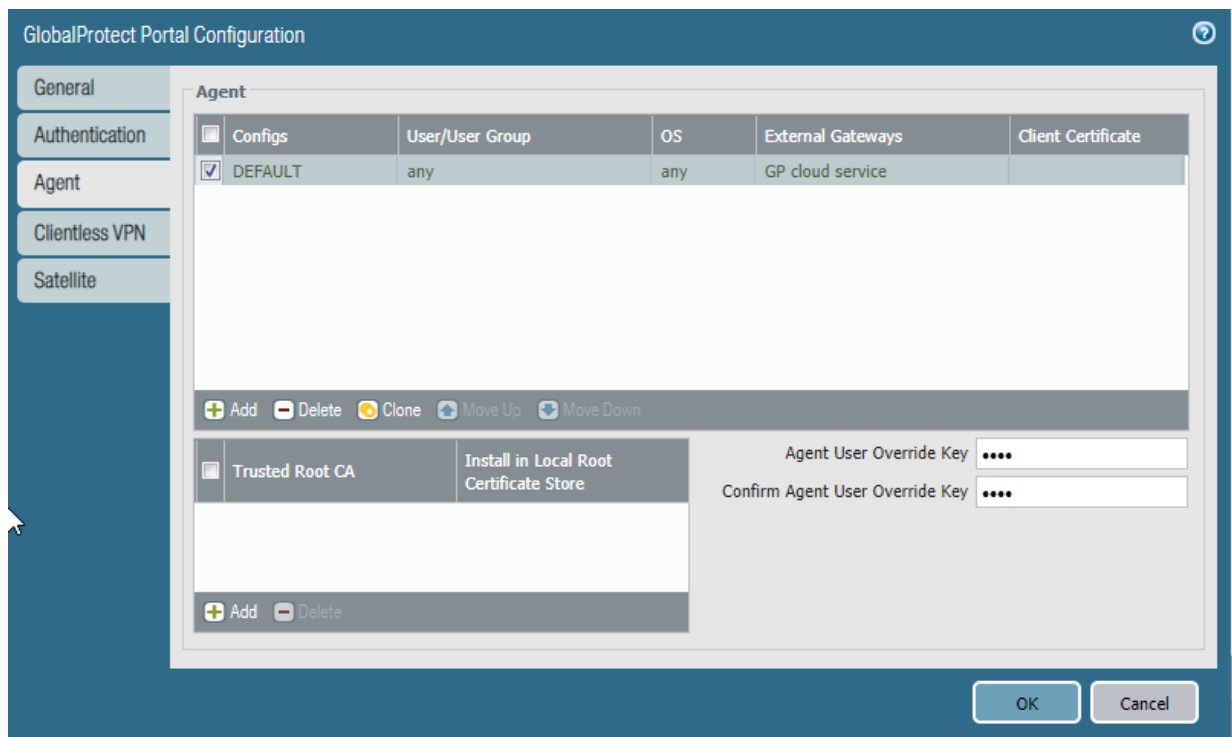
Use this workflow to configure priorities for a deployment that uses on-premises gateways with Prisma Access.

**STEP 1** | Log in to Prisma Access.

**STEP 2** | Select **Network > GlobalProtect > Portals** in the **Mobile\_User\_Template** template.

**STEP 3** | Click the portal name in the **Name** field.

**STEP 4** | Click the **Agent** tab.



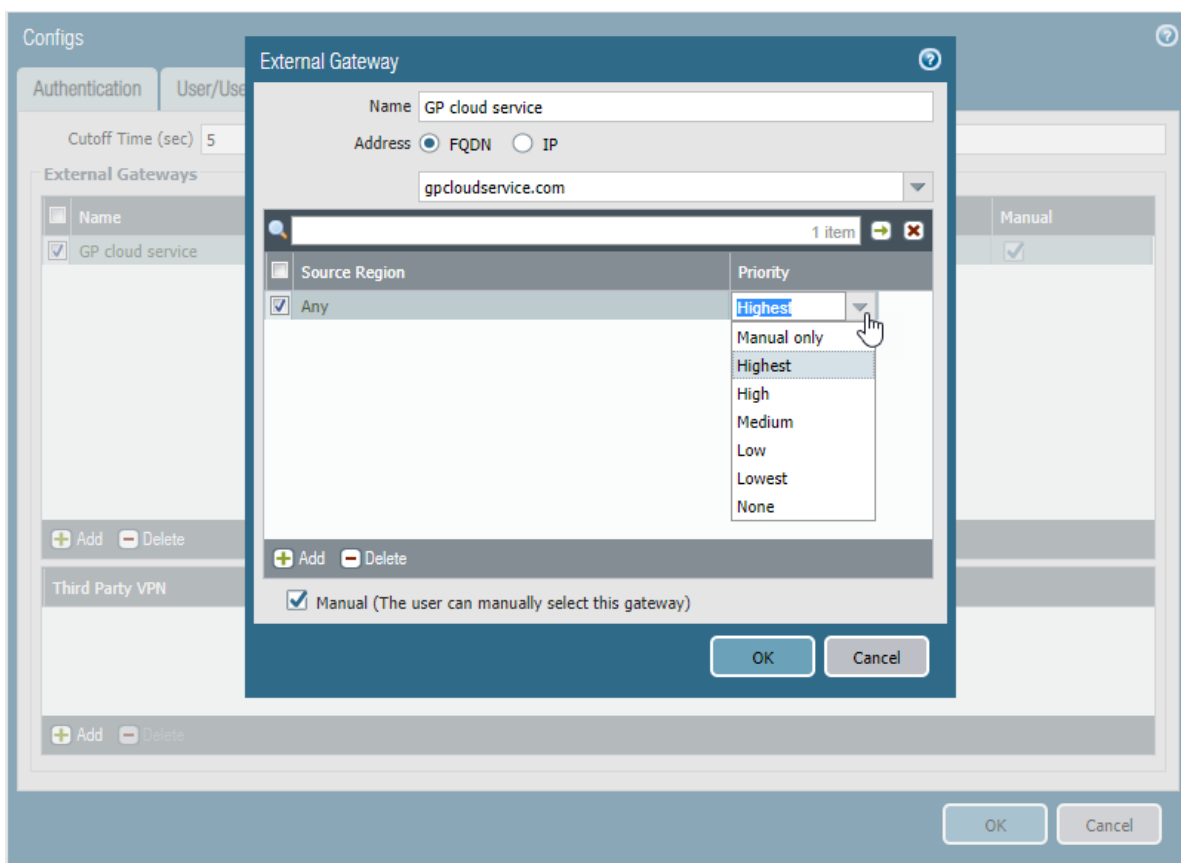
**STEP 5** | Click the name of the agent to configure.

The default agent is named **DEFAULT**.

**STEP 6** | Click the **External** tab.


**STEP 7** | Set the priority of the Prisma Access gateways.

1. Click **GP cloud service**.
2. Set the priority for your preferred configuration.
  - To [Set Equal Gateway Priorities for On-Premises and Prisma Access Gateways](#), change the priority from **None** to **Highest**.
  - To [Set a Higher Gateway Priority for an On-Premises Gateway](#) or [Set Higher Priorities for Multiple On-Premises Gateways](#), change the priority from **None** to **Medium**.



3. Be sure that the **Manual** check box is selected.

Checking the **Manual** check box ensures that mobile users can select a specific Prisma Access gateway if it is required.

 *Do not add a source region for the Prisma Access gateways; any region you specify is not applied to the configuration.*

4. Click **OK**.

#### STEP 8 | Add one or more on-premises external gateways to your configuration.


1. Enter a descriptive **Name** for the gateway.

The name you enter should match the name you defined when you configured the gateway, and it should be descriptive enough for users to know the location of the gateway to which they connect.

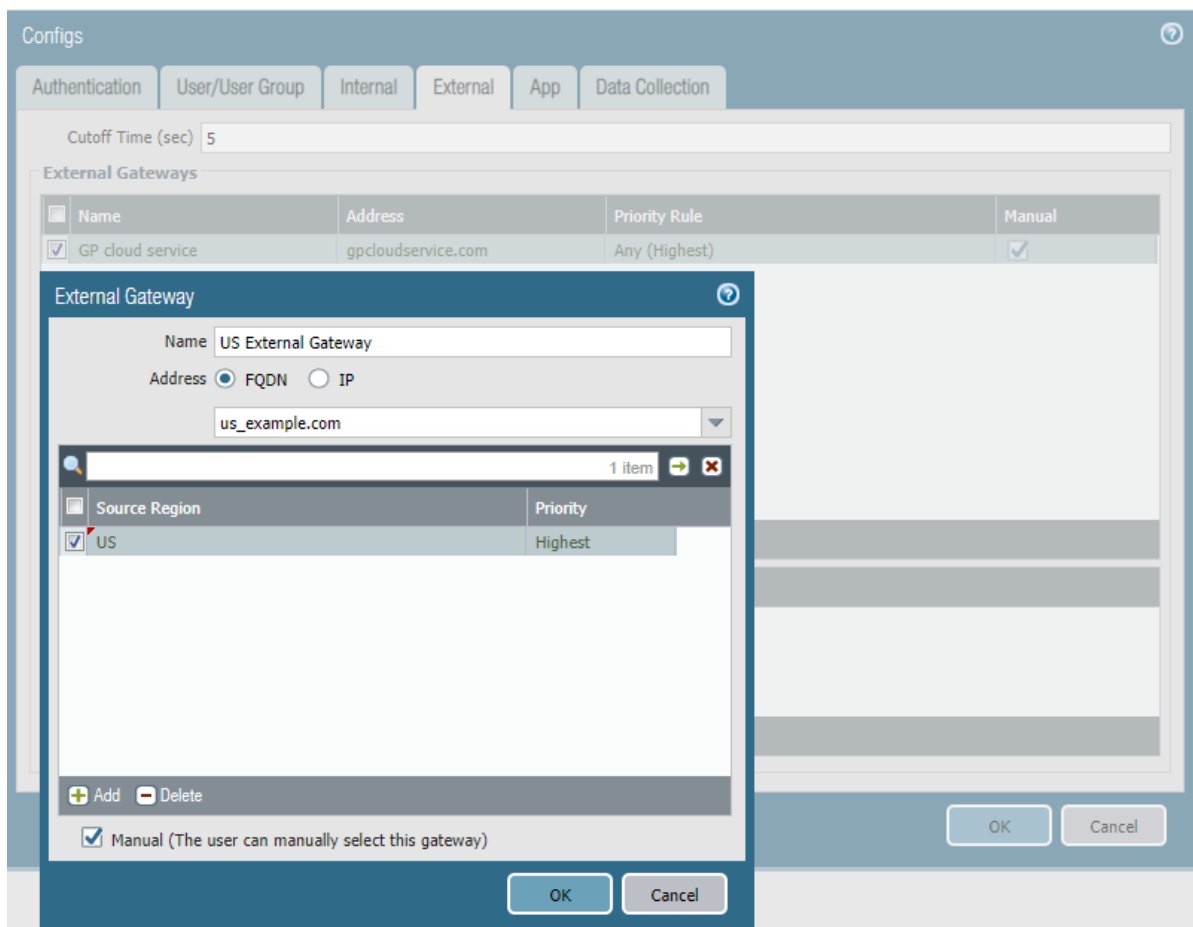
2. Enter the FQDN or IP address of the interface where the gateway is configured in the Address field.

You can configure an IPv4 address. The address you specify must exactly match the Common Name (CN) in the gateway server certificate.

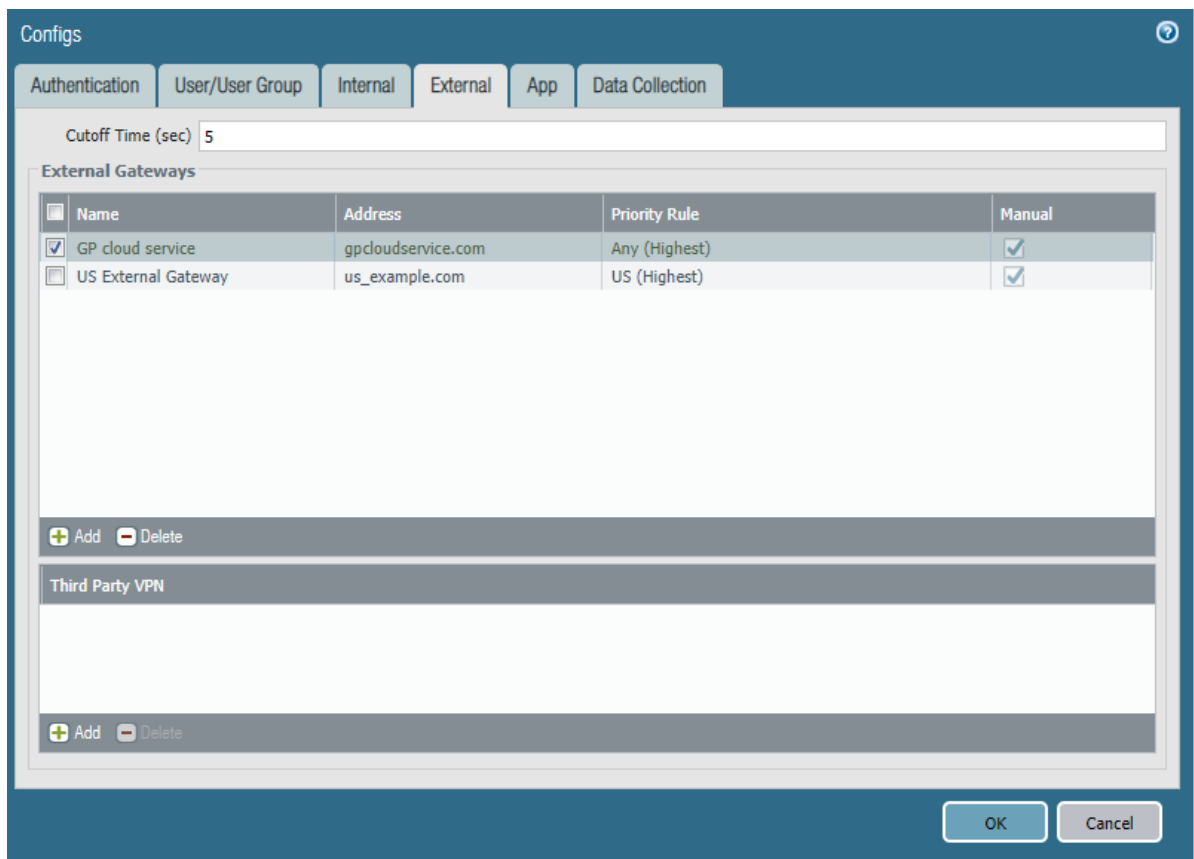
3. Add one or more **Source Regions** for the on-premises gateway, or select **Any** to make the gateway available to all regions.

 *If you set the priority of on-premises external gateways higher than Prisma Access gateways, we recommend that you specify source regions for the external gateways. If you specify Any for the region, the GlobalProtect app might never select Prisma Access gateways over on-premises gateways because of the higher priority for the on-premises gateways.*


4. Select the **Manual** check box to allow users to manually switch to the gateway.
5. Set the **Priority** of the on-premises gateway to **Highest** (the default).



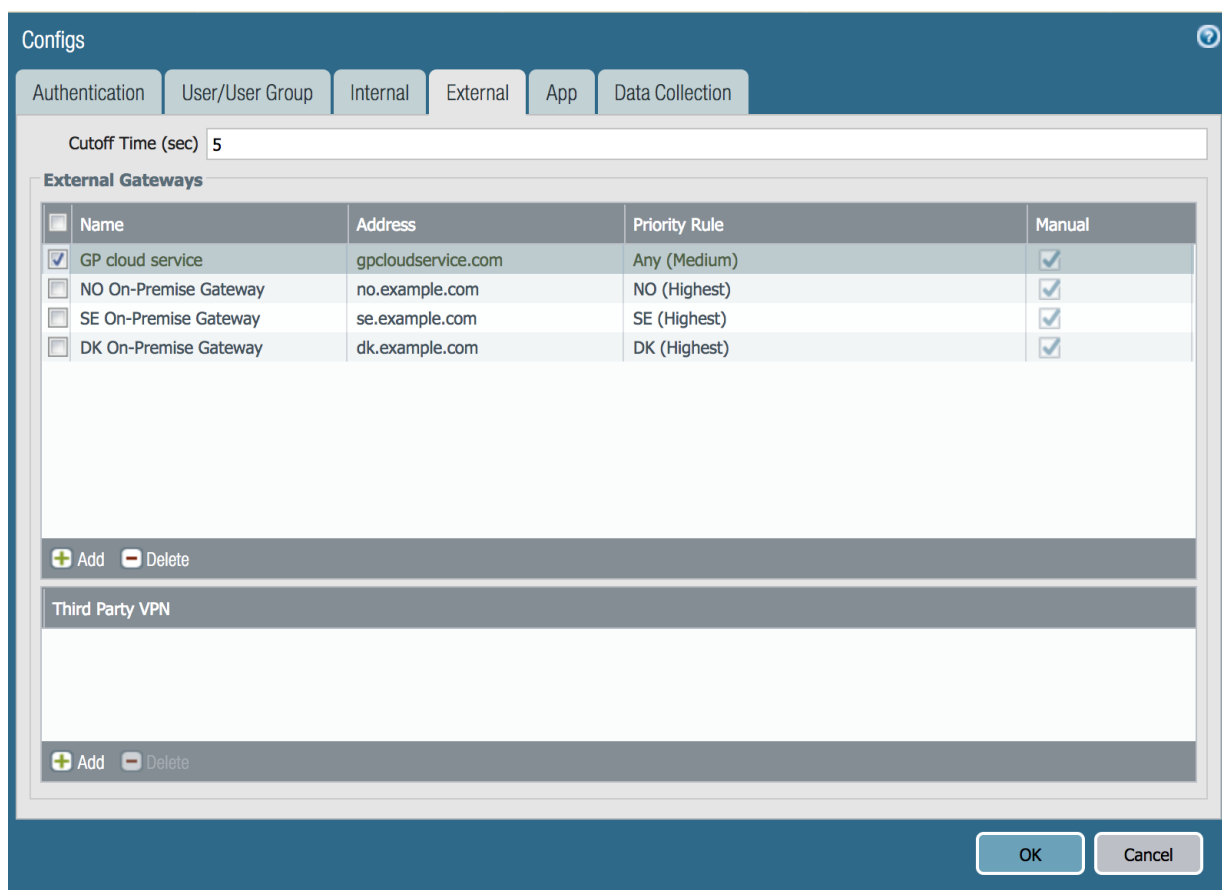
6. Click **OK**.



**STEP 9 | (Optional)** Set the priority for additional gateways by repeating Step 8.


 *Be sure to specify the correct source regions.*

The following figure shows a sample configuration with multiple gateways that have source regions in Norway, Sweden, and Denmark. Note that the **Manual** check box is selected, which indicates that a mobile user can manually select any of these gateways.



## Allow Mobile Users to Manually Select Specific Prisma Access Gateways

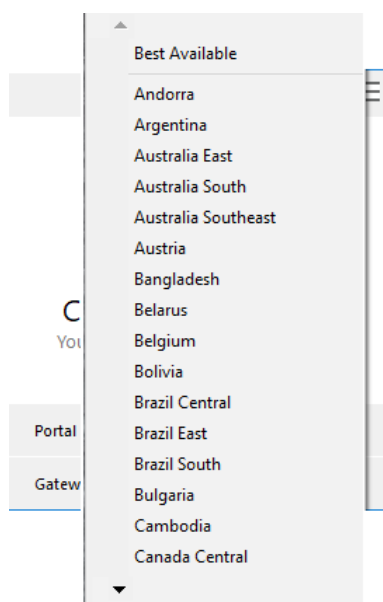
When system administrators specify priorities for gateways in Panorama, they can only specify priorities for all Prisma Access gateways as a whole.

 *When configuring the Prisma Access gateways, do not specify a source region. Any region you specify is not applied to the configuration.*

To choose a specific Prisma Access gateway, mobile users can select the gateway on their endpoint from the drop-down list in their GlobalProtect app.

 *This configuration requires that you configure Manual selection of the gateway when you [Configure Priorities for Prisma Access and On-Premises Gateways](#).*

The following figure shows a user choosing a list of Prisma Access gateways from the endpoint's GlobalProtect app.



The tasks you perform to connect to a specific gateway are based on the operating system of your endpoint. For details, see the [GlobalProtect App User Guide](#).

## DNS Resolution for Mobile Users and Remote Networks

Prisma Access provides you with different ways to resolve DNS queries for mobile users and remote networks. The following sections describe the different types of DNS resolution that Prisma Access supports for mobile users and remote networks, along with the steps you use to configure it.

- [DNS Resolution for Prisma Access](#)
- [DNS Resolution for Mobile Users](#)
- [DNS Resolution for Remote Networks](#)

### *DNS Resolution for Prisma Access*

Prisma Access allows you to specify DNS servers to resolve both domains that are internal to your organization and external domains. Prisma Access proxies the DNS request based on the configuration of your DNS servers. The following table shows the supported DNS resolution methods for internal and external domains and indicates when Prisma Access proxies the DNS requests.

Internal DNS Resolution Method	External DNS Resolution Method	Prisma Access Proxies the DNS Request (Yes/No)
Single rule, DNS server configured for Internal Domains	Cloud Default	Yes
Single rule, DNS server configured for Internal Domains	Same as Internal Domains	No
Single rule, DNS server configured for Internal Domains	Custom DNS server	Yes

Internal DNS Resolution Method	External DNS Resolution Method	Prisma Access Proxies the DNS Request (Yes/No)
Single rule, Cloud Default set for a domain	Cloud Default	Yes
Single rule, Cloud Default set for a domain	Same as Internal Domains	Yes
Single rule, Cloud Default set for domain	Custom DNS server	Yes
Multiple rules, DNS server configured for Internal Domains	Cloud Default	Yes
Multiple rules, DNS server configured for Internal Domains	Same as Internal Domains	Yes
Multiple rules, DNS server configured for Internal Domains	Custom DNS server	Yes
No configuration	Cloud Default	No
No configuration	Custom DNS Server	No
No configuration	No configuration	No
No DNS resolution specified (default configuration is present, which uses Cloud Default)	No DNS resolution specified	No

The source IP address of the DNS request depends on whether or not Prisma Access proxies the DNS request.

- When Prisma Access does not proxy the DNS requests, the source IP address of the DNS request changes to the IP address of the device that requested the DNS lookup. This source IP address allows you to enforce source IP address-based DNS policies or identify endpoints that communicate with malicious domains. This behavior applies for both mobile users and remote network deployments.
- When Prisma Access proxies the DNS requests, the source IP address of the DNS request changes to the following addresses:
  - **Mobile User deployments**—The source IP address of the DNS request is an IP address taken from the [mobile user IP address pool](#) for internal requests and the [mobile user location's gateway IP address](#) for external requests.
  - **Remote Network deployments**—The source IP address of the DNS request is the **EBGP Router Address** for internal requests and the [Service IP Address](#) of the remote network connection for external requests.

The following guidelines and restrictions apply to using DNS resolution with Prisma Access:

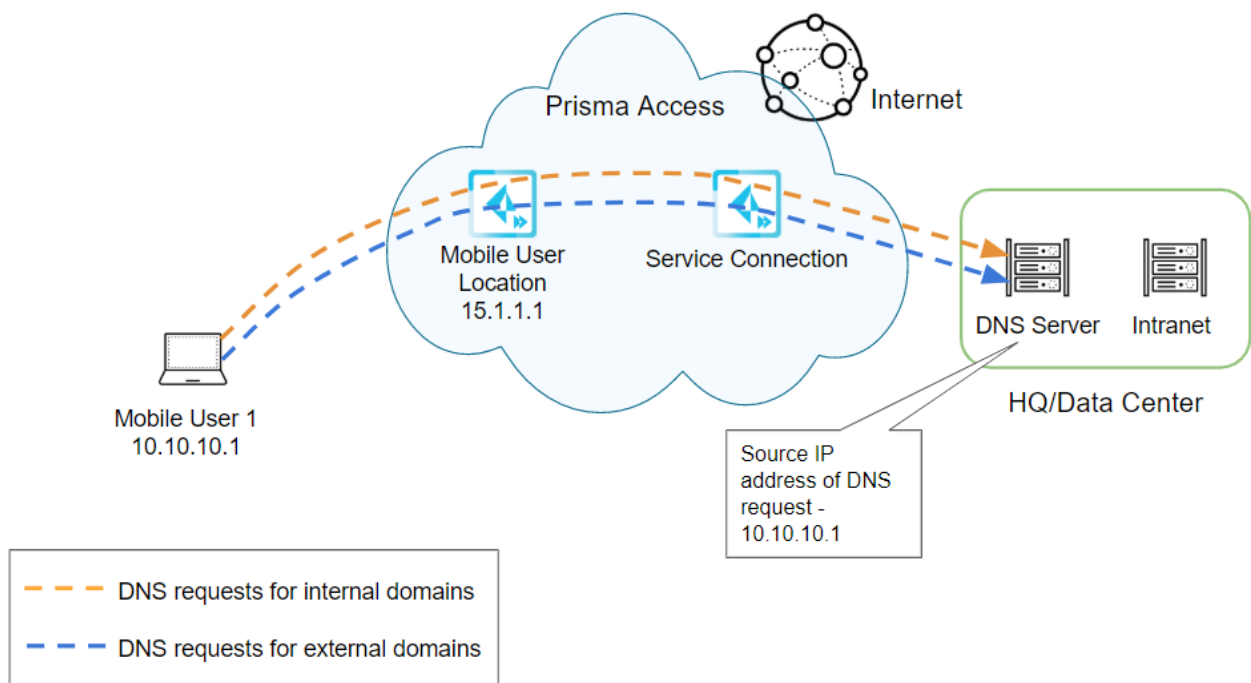


- The maximum number of concurrent pending TCP DNS requests (**Max Pending Requests**) that Prisma Access supports is 64.
- For UDP queries, the DNS proxy sends another request if it hasn't received a response in 2 seconds, and retries a maximum of 5 times before trying the next DNS server.
- Prisma Access caches the DNS entries with a time-to-live (TTL) value of 300 seconds. EDNS responses are also cached.

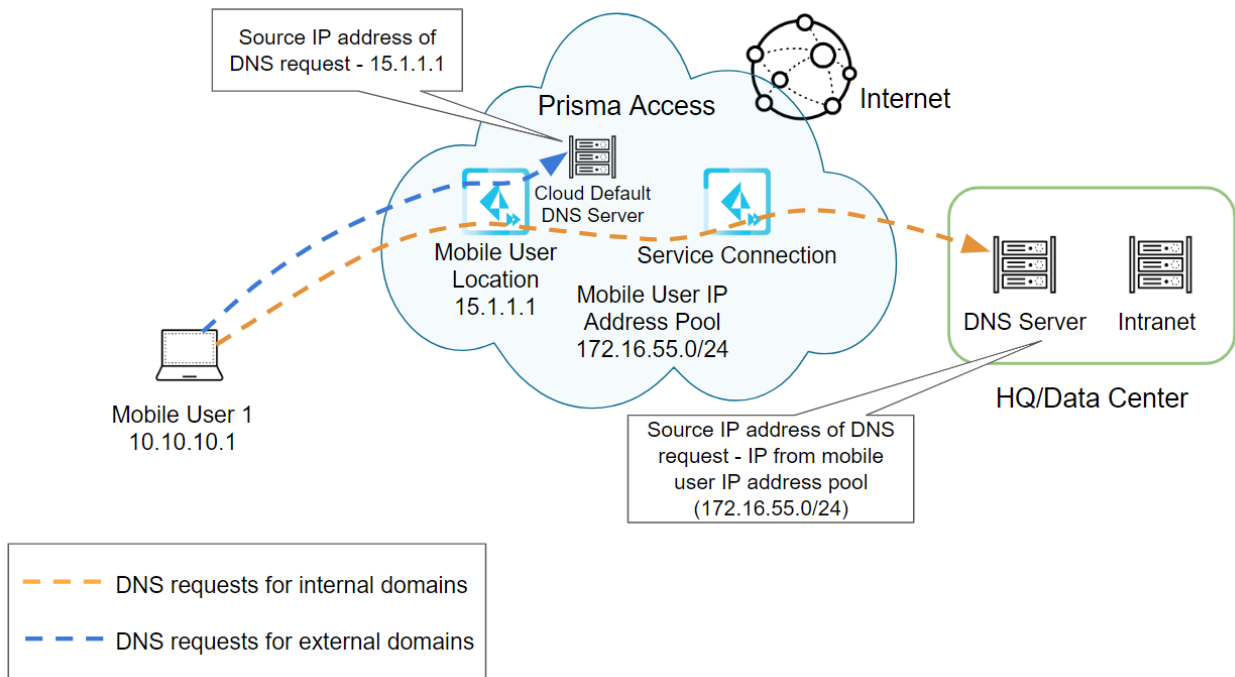
## DNS Resolution for Mobile Users

The following section provides examples of how Prisma Access processes the source IP address of the DNS requests after you configure DNS resolution [for mobile users](#) and [for remote networks](#).

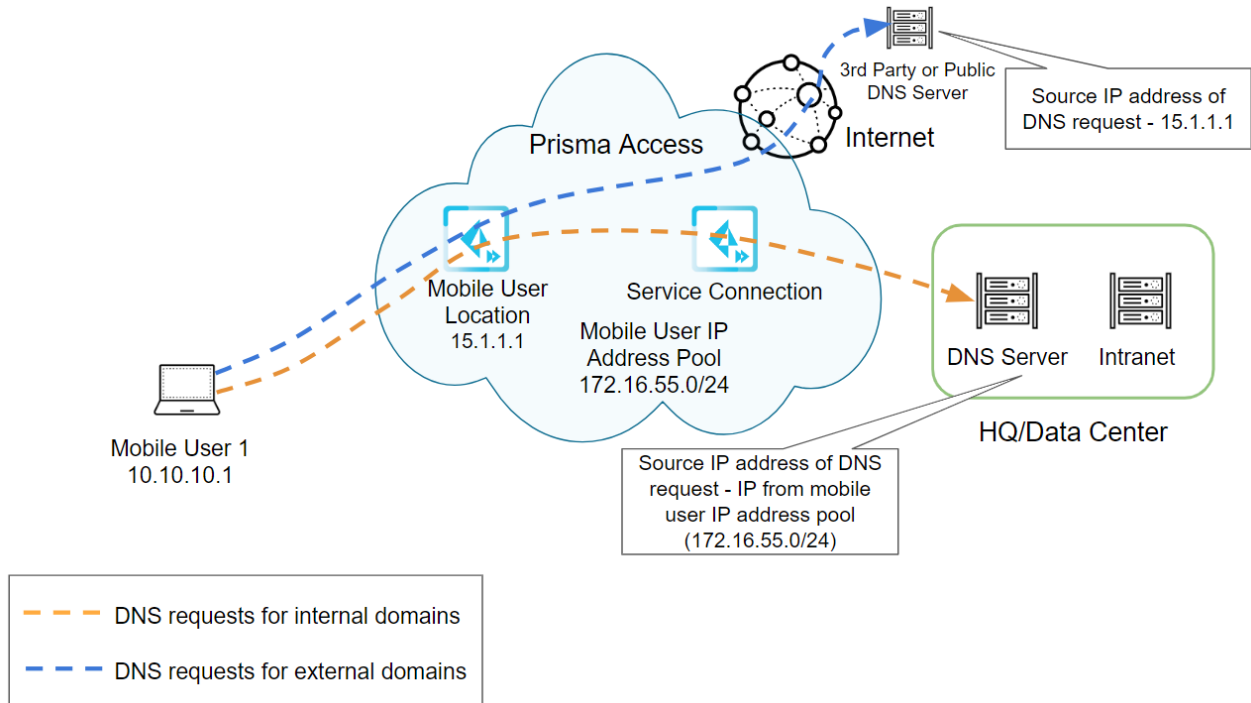
The following figure show a deployment where you have assigned an internal DNS server to resolve both internal and external domains. In this case, Prisma Access does not proxy the DNS requests, and the DNS server sees the request coming from 10.10.10.1 (the IP address of Mobile User 1's device).



The following figure shows the DNS requests for internal domains being resolved by the DNS server in the headquarters or data center location, while requests for external domains are resolved by Prisma Access' Cloud Default DNS server. In this case, Prisma Access proxies the requests, and the source IP address of the DNS request changes to an IP address from the [mobile user IP address pool](#) (172.16.55.0/24) for internal requests and to the [mobile user location's gateway IP address](#) (15.1.1.1 in this example) for external requests.



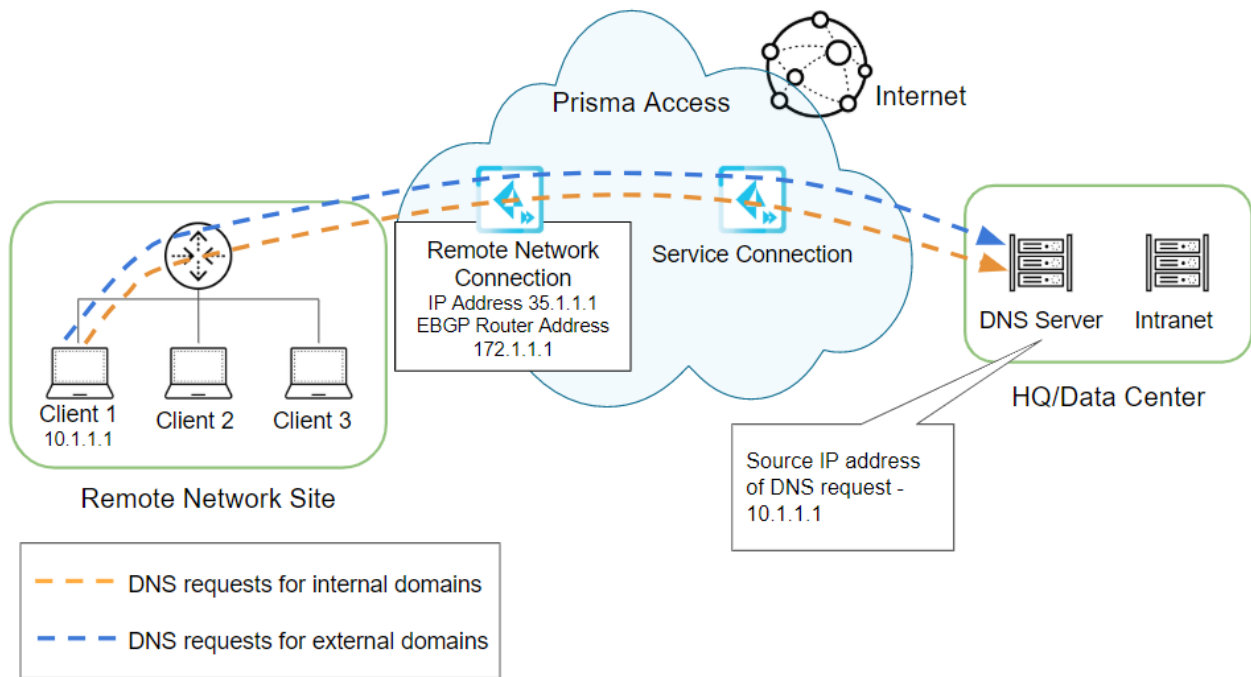
The following figure shows the organization using a third-party or public DNS server accessible through the internet for requests to external domains. Prisma Access proxies these requests as well, and the source IP address changes to an IP address from the mobile user IP address pool (172.16.55.0/24) for internal requests and to 15.1.1.1 for external requests.




## DNS Resolution for Remote Networks

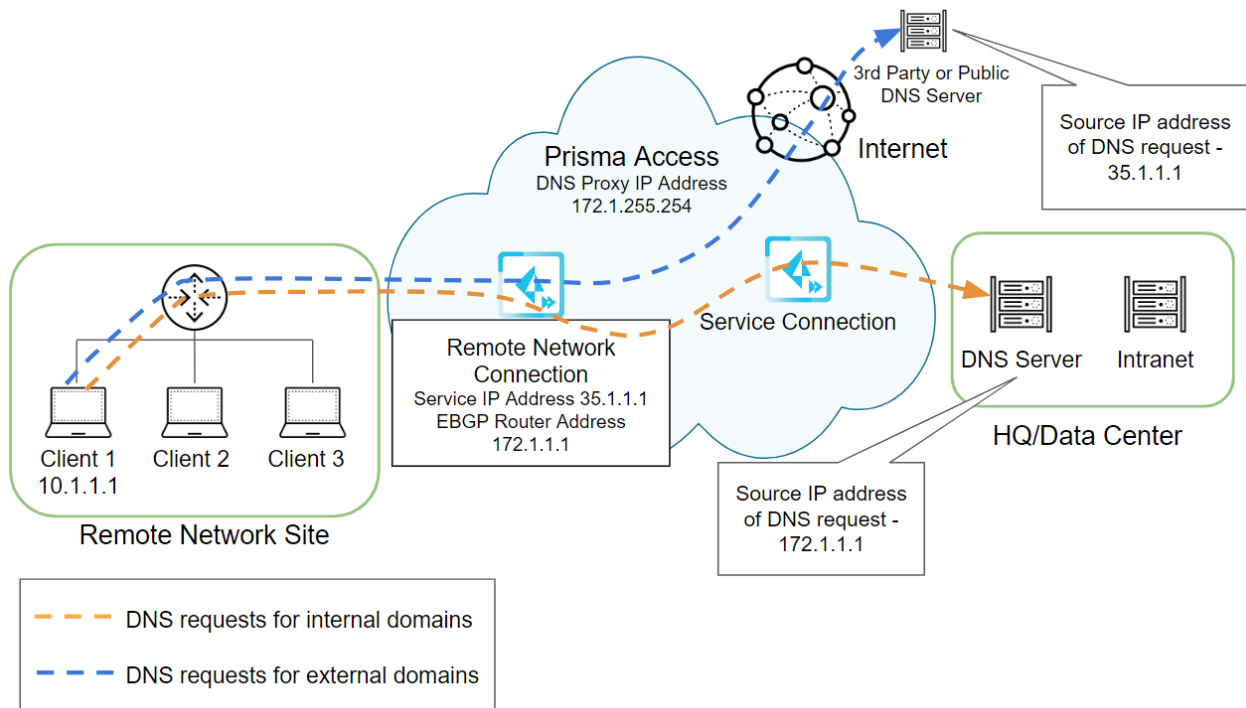
If you have an existing remote network deployment, you can continue to use the DNS resolution methods that you already have in place, or you can use Prisma Access to proxy the DNS request. Proxying the DNS requests allows you to send DNS requests for public domains to one server and send DNS request for internal domains to another server.

The following figure shows a DNS request to a deployment where an internal DNS server is used to process requests for both internal and external domains. The **remote network IP address** is 35.1.1.1 and the **EBGP Router IP address** is 172.1.1.1. In this case, Prisma Access does not proxy the requests and, if the internal DNS server does not use NAT, the source IP of the DNS request is 10.1.1.1 (the IP address of Client 1's device in the remote network site).



If Prisma Access proxies the DNS request, the source IP addresses of the proxied DNS requests changes to the **EBGP Router Address** for internal requests and the **Service IP Address** of the remote network connection for external requests, as shown in the following figure.

 *When you configure the DNS address in your network to use for Prisma Access proxied external requests, specify the Remote Network DNS Proxy IP Address (Panorama > Cloud Services > Status > Service Infrastructure > Remote Network DNS Proxy IP Address). In the following example, you would specify 172.1.255.254 in your network for the DNS server.*



## Sinkhole IPv6 Traffic From Mobile Users

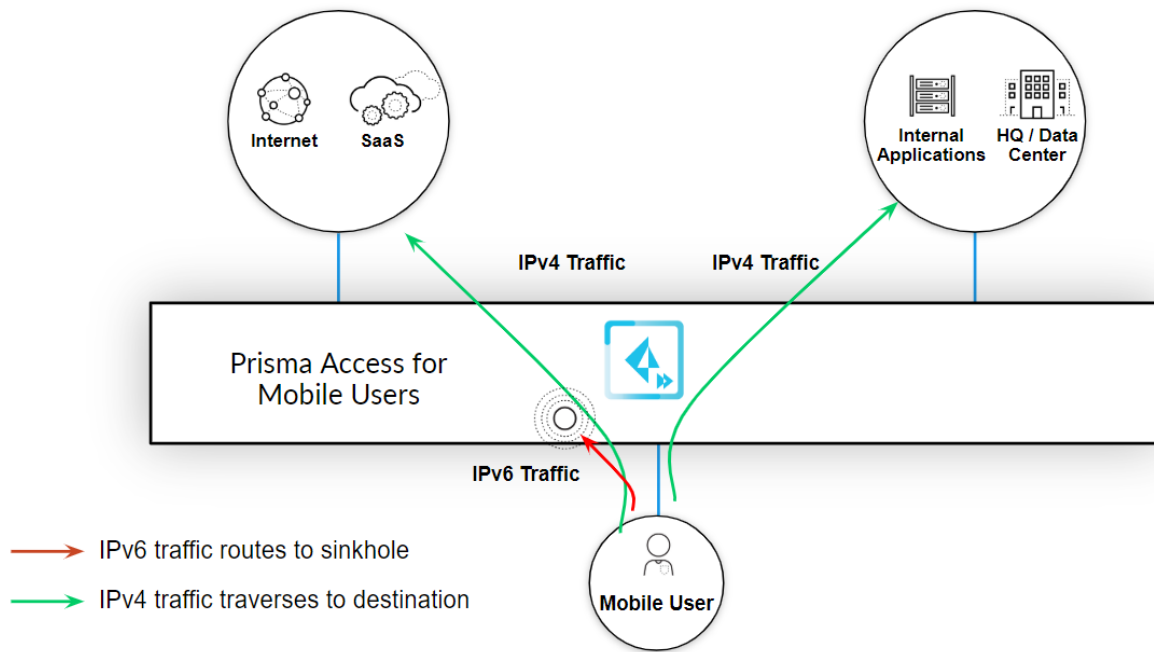
In a dual stack endpoint that can process both IPv4 and IPv6 traffic, the GlobalProtect app sends mobile user IPv4 traffic to be protected through the GlobalProtect VPN tunnel to Prisma Access. However, mobile user IPv6 traffic is not sent to Prisma Access by default and is sent to the local network adapter on the endpoint instead. To reduce the attack surface for IPv6-based threats, Palo Alto Networks recommends that you configure Prisma Access to sinkhole IPv6 traffic. Because endpoints can automatically fall back to an IPv4 address, you can enable a secure and uninterrupted user experience for mobile user traffic to the internet.

In addition, Palo Alto Networks recommends that you configure GlobalProtect to completely [disable network traffic on the local network adapter](#). If you have a hybrid Prisma Access deployment with on-premises next-generation firewalls configured as GlobalProtect gateways, you can configure IPv6 sinkhole functionality [on the on-premises GlobalProtect gateway](#).

- [Configure Prisma Access to Sinkhole IPv6 Traffic](#)
- [Configure GlobalProtect to Disable Direct Access to the Local Network](#)
- [Set Up an IPv6 Sinkhole On the On-Premises Gateway](#)

## Configure Prisma Access to Sinkhole IPv6 Traffic

You can configure Prisma Access so that it sinkholes all mobile user IPv6 traffic. When you enable this functionality, Prisma Access assigns an IPv6 address to the connecting endpoint in addition to an IPv4 address; then, it routes the IPv6 traffic to Prisma Access and discards it using a built-in security policy, as shown in the following figure.




To configure Prisma Access so that it sinkholes all mobile user IPv6 traffic, complete the following steps.

- STEP 1** | Open a secure CLI session with admin-level privileges, using the same IP address that you use to log in to the Panorama that manages Prisma Access.
- STEP 2** | Enter `configure` to enter configuration mode.
- STEP 3** | Enter the `set plugins cloud_services mobile-users ipv6 yes` command.  
If you need to disable this command in the future, enter `set plugins cloud_services mobile-users ipv6 no`.
- STEP 4** | Enter `commit` to save your changes locally.
- STEP 5** | Enter `exit` to exit configuration mode.
- STEP 6** | Enter `commit-all shared-policy include-template yes device-group Mobile_User_Device_Group` to commit and push your changes and make them active in Prisma Access.

## Configure GlobalProtect to Disable Direct Access to the Local Network

To make sure that all mobile user traffic is sent to Prisma Access, you can completely disable outgoing connections, including local subnet traffic, from being sent to the local adapter. You can deactivate all outgoing connections to the local adapter by [making configuration changes to the GlobalProtect gateway](#).

You can perform these steps on Panorama or on an on-premises firewall that has been configured as a GlobalProtect gateway.

 *Disabling local network access causes all traffic, including IPv4 and IPv6 traffic, from being sent to the local adapter. In addition, you won't be able to access resources on your local subnet, such as printers.*

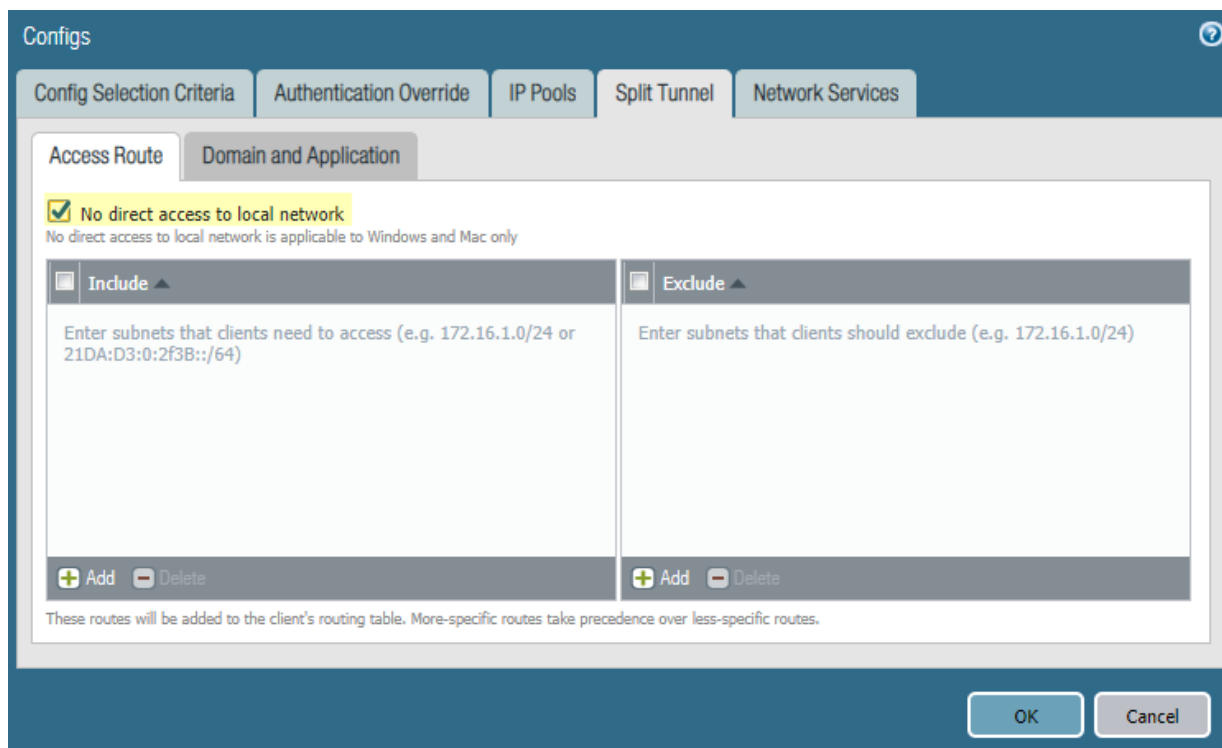
**STEP 1** | Select **Network > GlobalProtect > Gateways**.

**STEP 2** | Select an existing GlobalProtect gateway or **Add** a new one.

**STEP 3** | Select **Agent > Client Settings**.

**STEP 4** | Select the **DEFAULT** configuration or **Add** a new one.

**STEP 5** | Select **Split Tunnel**; then, select **No direct access to local network**.



**STEP 6** | (Panorama and Prisma Access deployments only) Commit your changes locally to make them active in Panorama.

1. Select **Commit > Commit to Panorama**.
2. Make sure that your change is part of the **Commit Scope**.
3. Click **OK** to save your changes to the push scope.
4. **Commit** your changes.

**STEP 7** | **Commit** and **Push** your changes to make them active in Prisma Access.

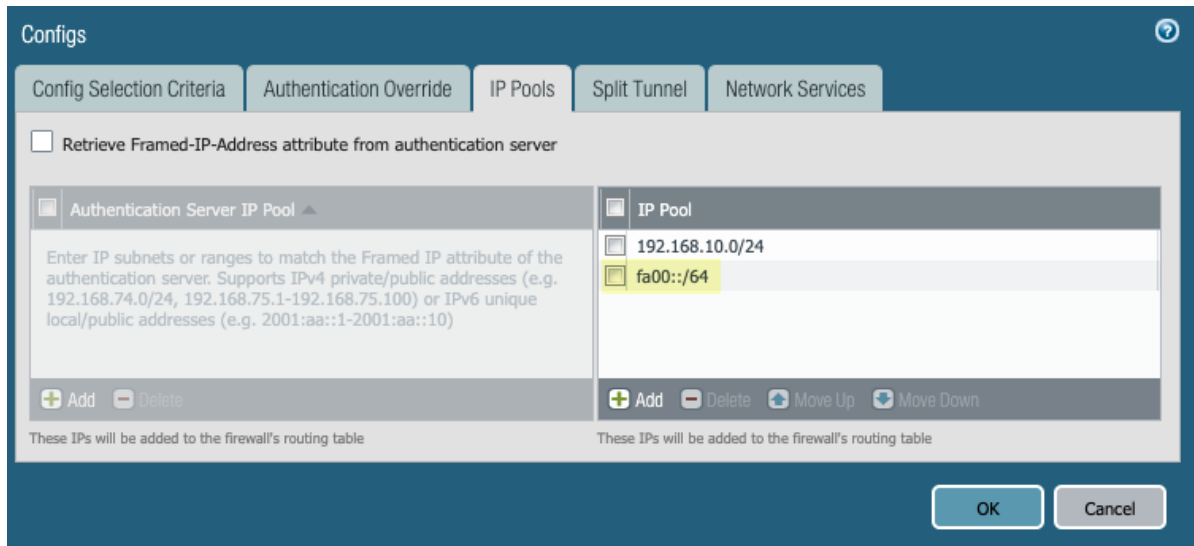
## Set Up an IPv6 Sinkhole On the On-Premises Gateway

If you have a hybrid deployment that uses next-generation firewalls configured as gateways with Prisma Access, perform the following task on the on-premises gateway to drop the IPv6 traffic.

**STEP 1** | Add IPv6 IP pools to your GlobalProtect agent configuration.

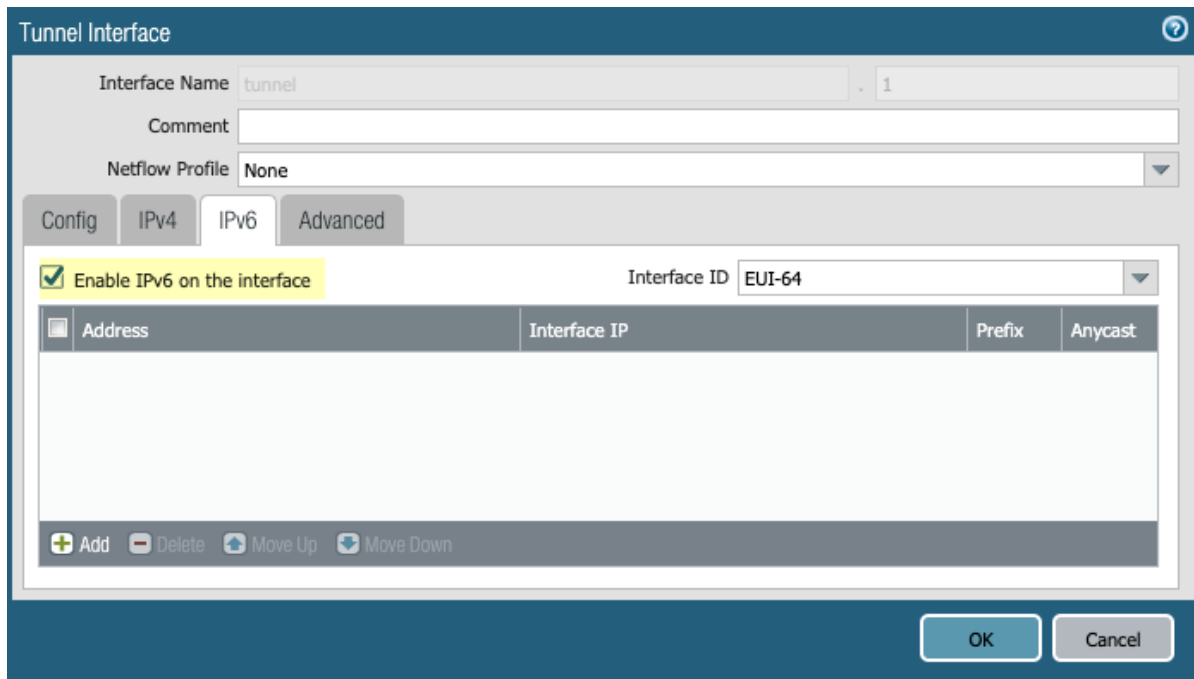
1. Select **Network > GlobalProtect > Gateways**.
2. Select an existing GlobalProtect gateway or **Add** a new one.
3. Select **Agent > Client Settings**.
4. Select the agent configuration to modify or **Add** a new one.

5. Select **IP Pools**; then, **Add** an IPv6 pool to assign to the virtual network adapter on the endpoints that connect to the GlobalProtect gateway uses for mobile network traffic and click **OK**.



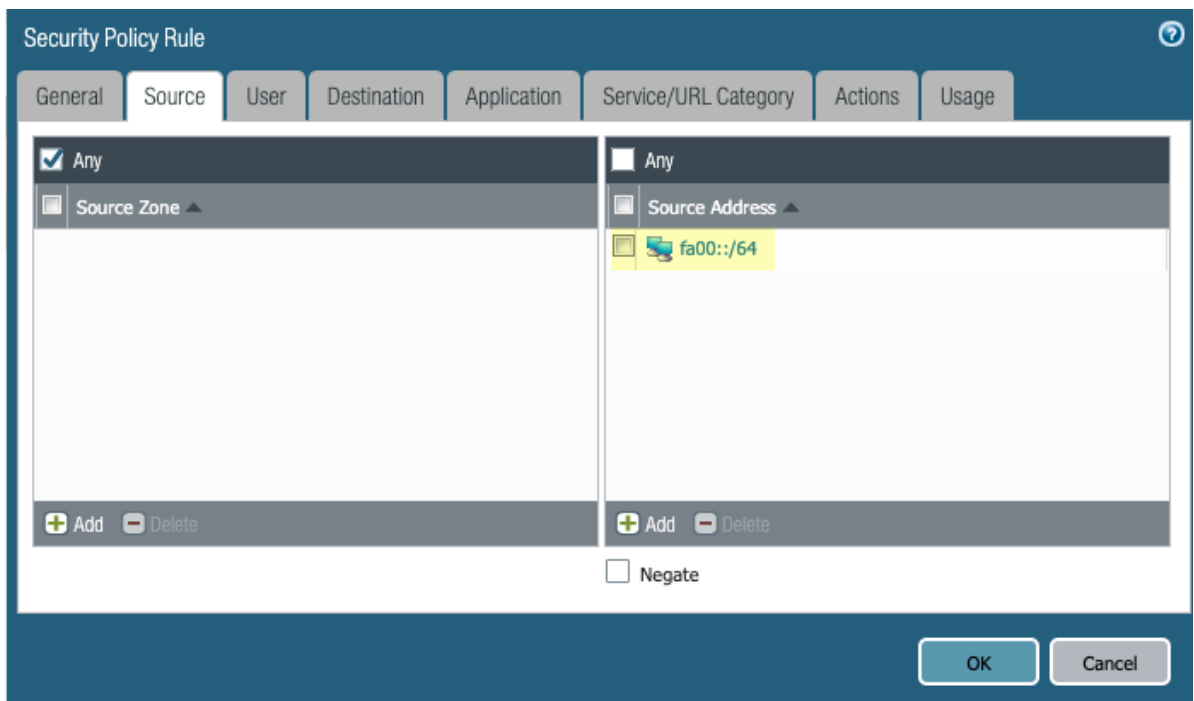
**STEP 2 |** Enable IPv6 on the interface.

1. Select **Device > Interface > Tunnel** and select the tunnel **Interface** that you use for the mobile user's traffic.
2. Select **IPv6**; then, select **Enable IPv6 on the interface**.

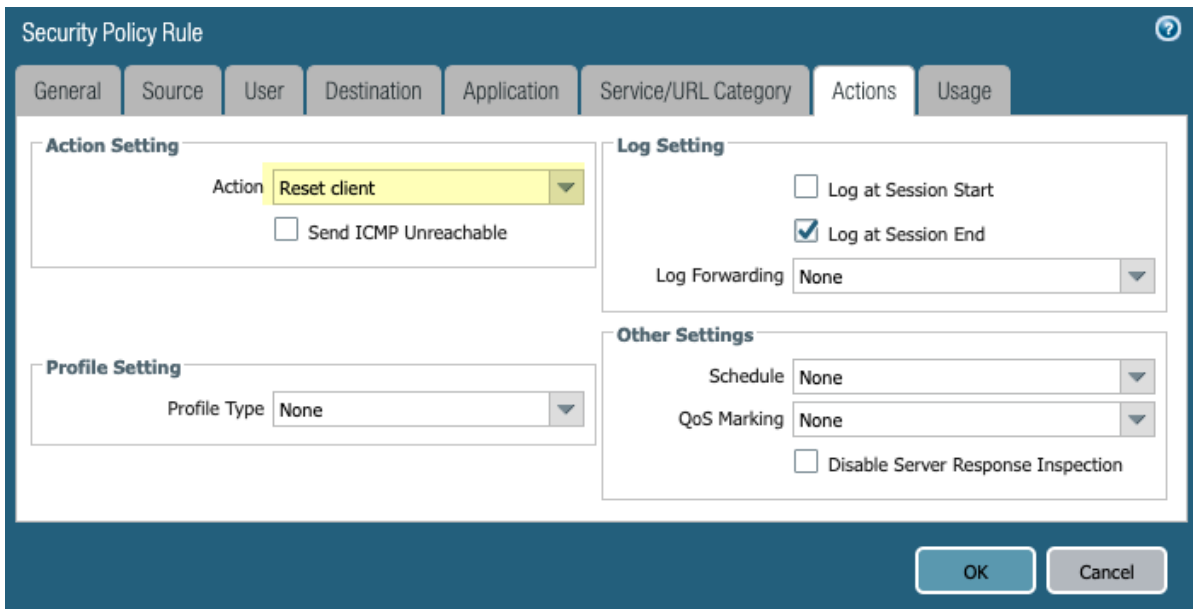


**STEP 3 |** Add a security policy to set a TCP reset action that will terminate sessions with IPv6 source traffic that matches the IP pools you configured in Step 1.

1. Select **Policies > Security** and **Add** a new security policy.
2. Set the **Source Address** in the rule to match the IP pools you configured in Step 1.



3. Select **Actions**; then, select an **Action Setting** of **Reset Client** and click **OK**.



**STEP 4 | Commit** your changes.

**STEP 5 | (Optional)** Perform this task on all the gateway firewalls in your deployment.

## Identification and Quarantine of Compromised Devices With Prisma Access

Prisma Access allows you to [identify and quarantine compromised devices](#) that are connected with the GlobalProtect app. You do this by either [manually](#) or [automatically](#) adding devices to a quarantine list. After



you quarantine the device, you can [block the quarantined device](#) from accessing the network to ensure consistent policy.

- [Quarantine List Redistribution Overview](#)
- [Use Cases for Quarantine List Redistribution](#)
- [Configure Quarantine List Redistribution in Prisma Access](#)

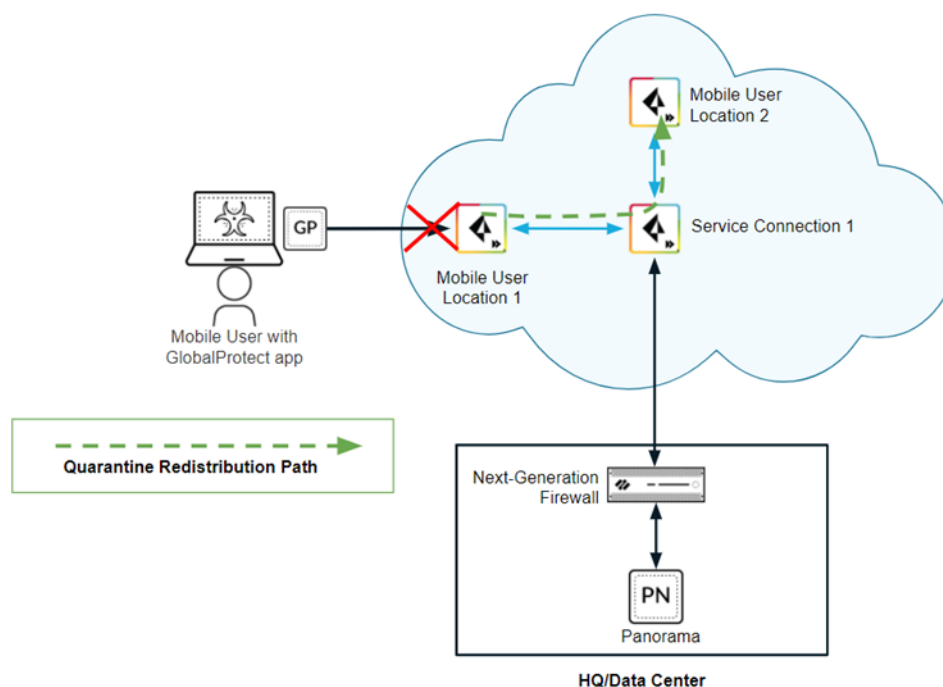
## Quarantine List Redistribution Overview

Each Prisma Access mobile user location ends and receives its quarantine information between the Panorama that manages Prisma Access and its nearest service connection. If you have next-generation firewalls or gateways, you should have the service connection redistribute the quarantine list information to and from Panorama and the on-premise firewalls or gateways. You should also redistribute the quarantine list information from Panorama to the service connection to ensure consistent policy enforcement for all mobile user locations (gateways) in Prisma Access.

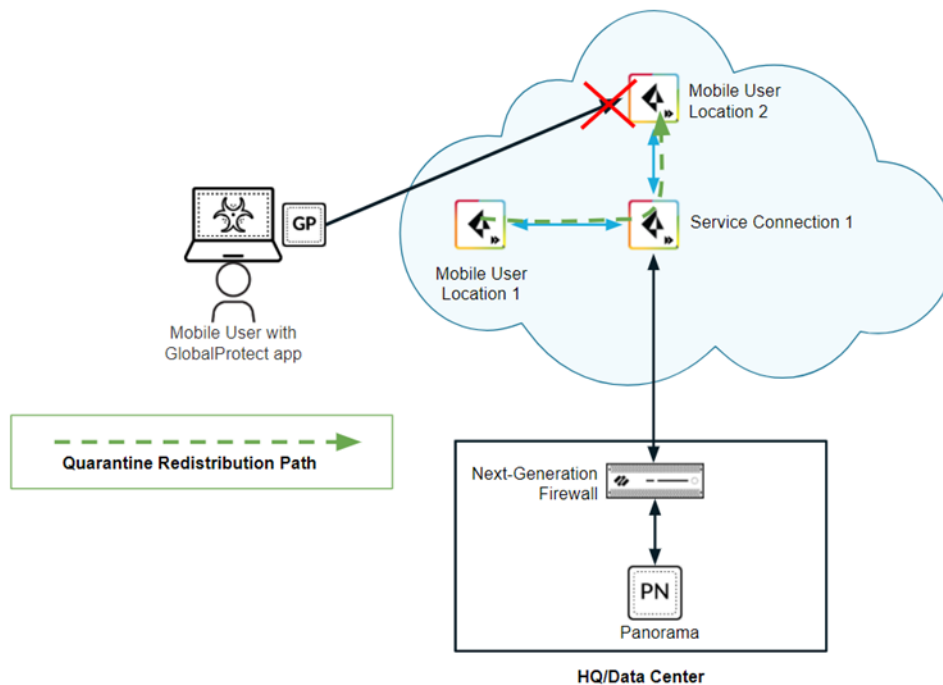
## Use Cases for Quarantine List Redistribution

The following section describes some common Prisma Access deployments where quarantine list redistribution is useful for consistent policy enforcement for compromised devices.

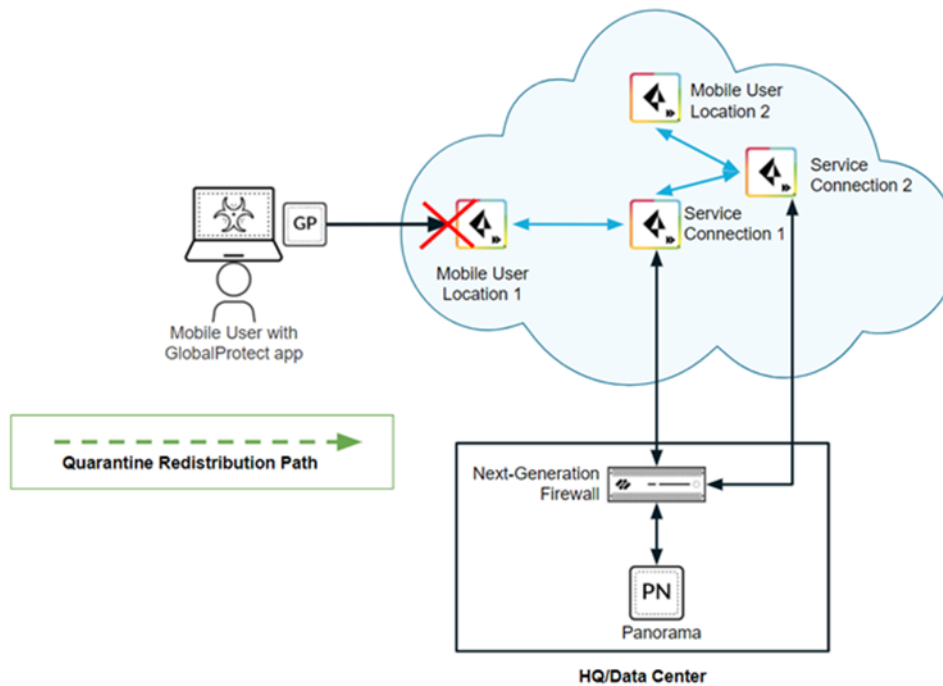
- **Quarantine List Redistribution between Mobile User Locations Connected to Same Service Connection**—In the following example, a GlobalProtect Mobile User who is connected to Mobile User Location 1 becomes compromised and is [auto-quarantined](#). Prisma Access blocks or restricts the quarantined device per policy.



A service connection (Service Connection 1 in this example) redistributes the quarantine list information between all mobile user locations to which it is connected. Since Mobile User Location 2 receives the redistributed quarantine list information by way of Service Connection 1, the GlobalProtect mobile user attempt to connect to Mobile User Location 2 is also blocked.




- Quarantine List Redistribution between Mobile User Locations Connected to Different Service Connections**—In the following example, there are two mobile user locations, but they connect to two different service connections. A GlobalProtect user attempted to connect to Mobile User Location 1. Mobile User Location 1 detects the GlobalProtect user endpoint as compromised and quarantines it.

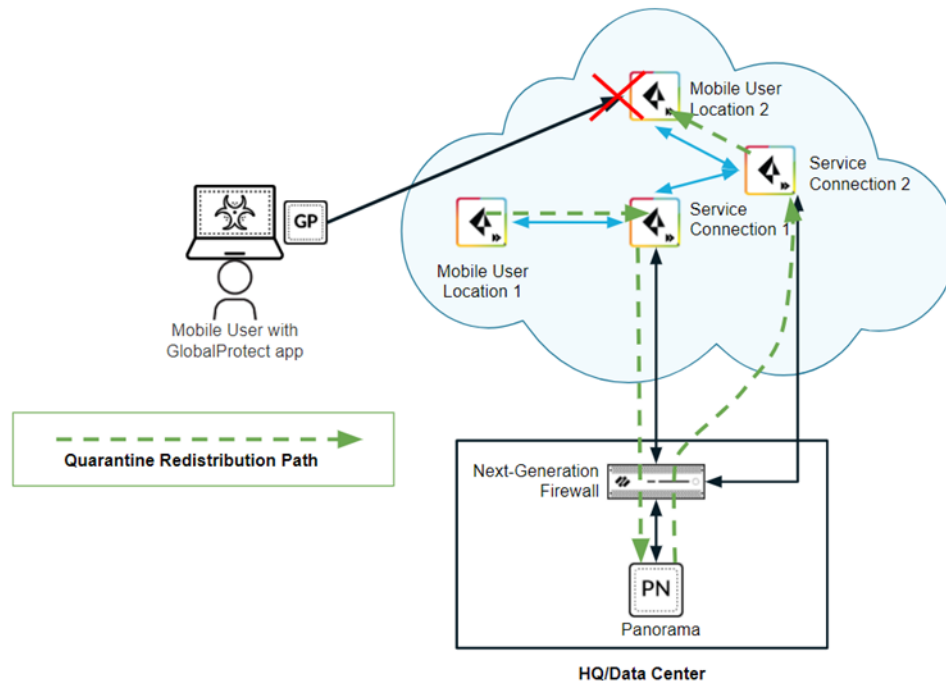


To redistribute the quarantine list information from Mobile User Location 1 to Mobile User Location 2, perform the following actions:

- Redistribute the quarantine list information from Service Connection 1 to Panorama.
- Redistribute the quarantine list information from Panorama to Service Connection 2.

With this configuration, when the GlobalProtect user connects to Mobile User Location 1 and is quarantined, then the quarantine list information redistributes from Mobile User Location 1 to Mobile User Location 2 and any connection attempts to Mobile User Location 2 are blocked.

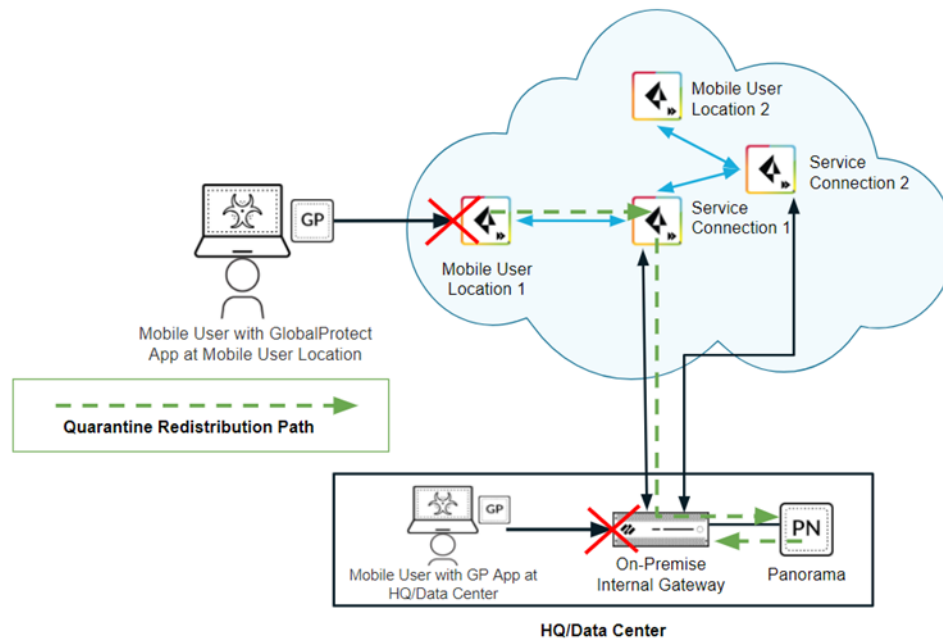
 This configuration is also valid if the GlobalProtect user connects to Mobile User Location 2 and is quarantined; the quarantine list information redistributes from Mobile User Location 2 to Mobile User Location 1.



- Quarantine List Redistribution Between Prisma Access and a Next-Generation Firewall or Gateway—**  
 In the following example, A GlobalProtect user attempted to connect to Mobile User Location 1. Mobile User Location 1 detects the GlobalProtect user endpoint as compromised and quarantines it. The mobile user then goes to the company's headquarters and attempts to log in again. The headquarters is protected with a next-generation firewall configured as a GlobalProtect gateway using Internal Host Detection.

Mobile User Location 1 redistributes the quarantine list information to Panorama through Service Connection 1, and Panorama redistributes the quarantine list information to the on-premise internal gateway. When the user attempts to log in from the headquarters location, GlobalProtect detects that the on-premises gateway is configured as an internal gateway and connects to the gateway without a tunnel.

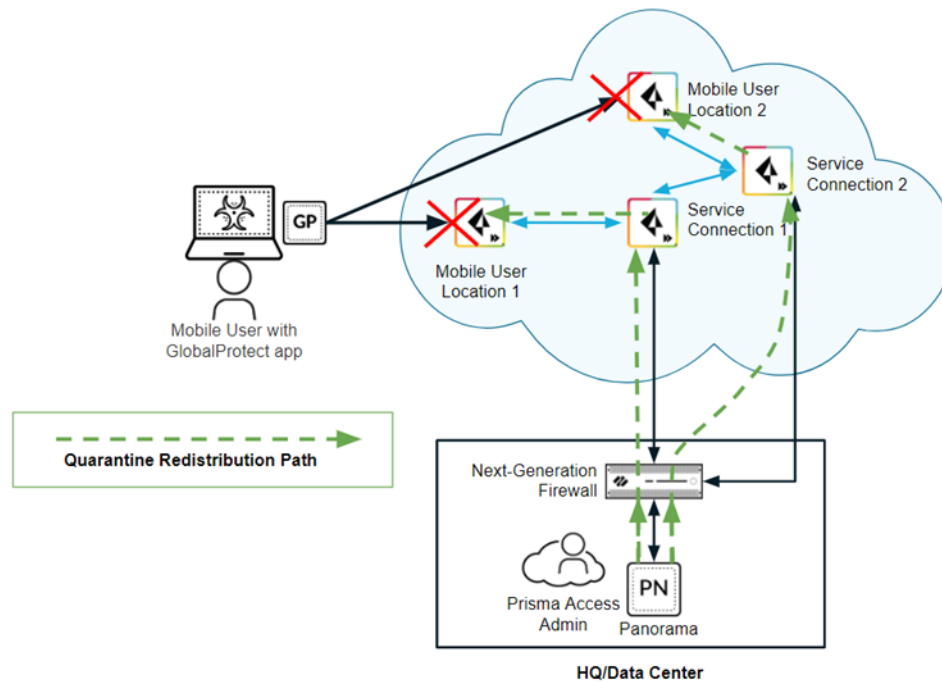
Since the quarantine list information has been redistributed to the on-premises gateway, the user is blocked at the gateway based on the configured user policies.



If you use a next-generation firewall or gateway with Prisma Access, you should configure Panorama to redistribute quarantine list information to the firewall or gateway, all service connections, and Panorama.

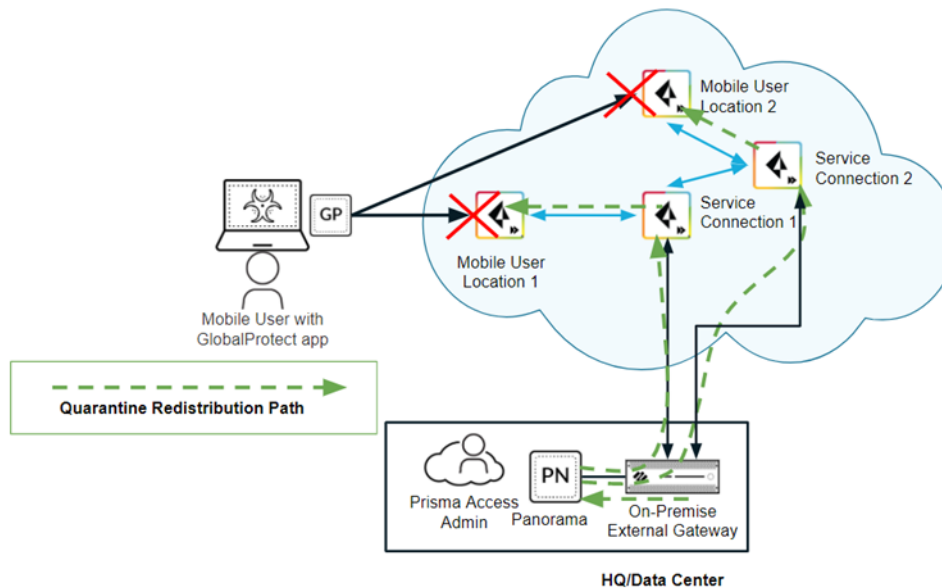
- Administrator Manually Quarantines Mobile User at Panorama**—In this example, the Prisma Access administrator has manually added a mobile user to the quarantine list at the Panorama appliance that manages Prisma Access. The administrator has set up redistribution between Panorama, the next-generation firewall, and the service connections. Panorama redistributes the updated quarantine list information to the firewall and the service connections. The service connections then redistribute the quarantine list information to the mobile user locations.

The mobile user was connected to Mobile User Location 1. After Mobile User Location 1 receives the updated quarantine list information, the user is disconnected. If the user attempts to connect to Mobile User Location 2, the connection is blocked and the mobile user receives a quarantine notification.



- Mobile User is Auto or Manually Quarantined at the On-Premises Gateway**—In this example, there is a next-generation firewall that has been configured as an external gateway at the headquarters or data center location. The administrator has manually quarantined a mobile user at the external gateway. The external gateway redistributes the quarantine list information from the external gateway to Panorama.

After Panorama has received the updated quarantine list information from the external gateway, it redistributes that information to Service Connections 1 and 2, which then redistributes it to Mobile User Locations 1 and 2. If a mobile user attempts to connect to either Mobile User Location 1 or 2, Prisma Access blocks the connection and the user receives a quarantine notification.



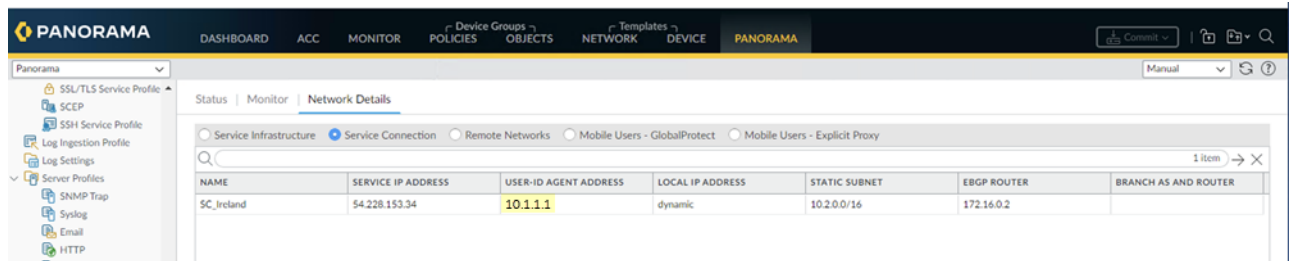
## Configure Quarantine List Redistribution in Prisma Access

To redistribute quarantine information to and from service connections, the Panorama that manages Prisma Access, and next-generation firewalls, complete the following steps.

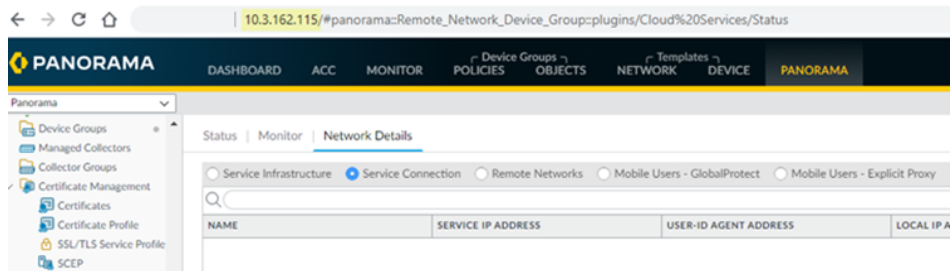
**STEP 1** | Make sure that the Panorama management IP address is able to communicate with the User-ID agent address for all service connections to which you want to redistribute quarantine list information.

Communication between the User-ID Agent address of the service connection and the management IP address of Panorama is required for Prisma Access to send and receive quarantine list information between Panorama and the service connections.

- To find the **User-ID Agent Address**, select **Panorama > Cloud Services > Status > Network Details > Service Connection > User-ID Agent Address**.



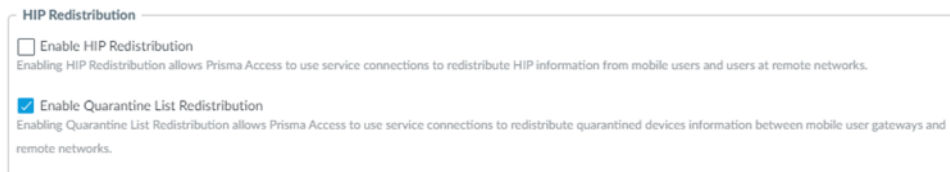
- To find the management IP address of the Panorama that manages Prisma Access, note the IP address that displays in the web browser when you access Panorama.



**STEP 2** | Allow Prisma Access to redistribute quarantine list information.

1. In Panorama, select **Panorama > Cloud Services > Configuration > Service Setup**.
2. Click the gear icon to edit the settings.
3. In the **Advanced** tab, select **Enable Quarantine List Redistribution**.

Enabling quarantine list redistribution allows Prisma Access to redistribute the quarantine list information received from one or more mobile user locations (gateways) to service connections.



**STEP 3** | **Commit** and **Push** your changes.

**STEP 4** | Configure Panorama to receive quarantine list information from Prisma Access by configuring management interface settings.

1. In the Panorama that manages Prisma Access, select **Panorama > Setup > Interfaces**.
2. Select the **Management** interface.
3. Select **User-ID**.

Management Interface Settings

Public IP Address

IP Address

Netmask

Default Gateway

IPv6 Address/Prefix Length

Default IPv6 Gateway

Device Management Services

- Device Management and Device Log Collection
- Collector Group Communication
- Syslog Forwarding

Administrative Management Services

- HTTP
- HTTPS
- Telnet
- SSH

Network Services

- Ping
- SNMP
- User-ID

PERMITTED IP ADDRESSES	DESCRIPTION

+ Add - Delete

OK Cancel

**STEP 5** | Configure a data redistribution agent that redistributes quarantine list information from the service connections to Panorama.

1. From the Panorama that manages Prisma Access, select **Panorama > Cloud Services > Status > Network Details > Service Connection**.
2. Make a note of the **User-ID Agent Address** (**Panorama > Cloud Services > Status > Network Details > Service Connection > User-ID Agent Address**) for each service connection.
3. Select **Panorama > Data Redistribution > Agents**.
4. **Add** a Data Redistribution agent, give it a **Name** and select **Enabled**.
5. Enter the **User-ID Agent Address** of the service connection as the **Host** and 5007 as the **Port**.



*Make sure that your network does not block access to this port between Panorama and Prisma Access.*

6. (**Optional**) If you have configured this service connection as a Collector (**Device > Data Redistribution > Collector Settings**), enter the **Collector Name** and **Collector Pre-Shared Key**.
7. Select **Quarantine List**; then, click **OK**.

Add a Data Redistribution Agent
?

Name

Enabled

Add an Agent Using  Serial Number  Host and Port

Host  ▼

LDAP Proxy

Port

Collector Name

Collector Pre-Shared Key

Confirm Collector Pre-Shared Key

Data type  IP User Mappings  HIP

IP Tags  Quarantine List

User Tags

OK
Cancel

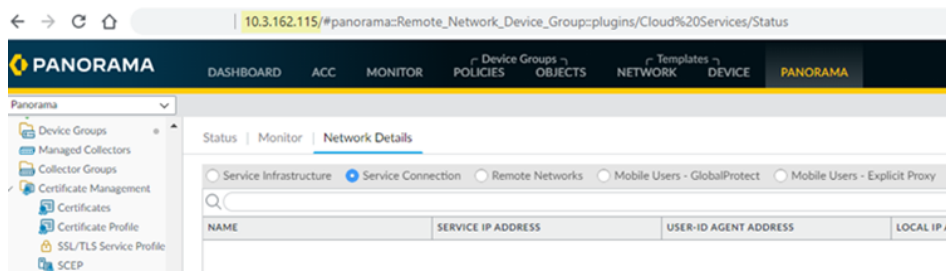
8. Repeat Step 5 for all the service connections in your Prisma Access deployment.

**STEP 6 |** Select **Commit > Commit to Panorama** to save your changes locally on the Panorama that manages Prisma Access.

**STEP 7 |** Configure a data redistribution agent that redistributes quarantine list information from Panorama to the service connections.

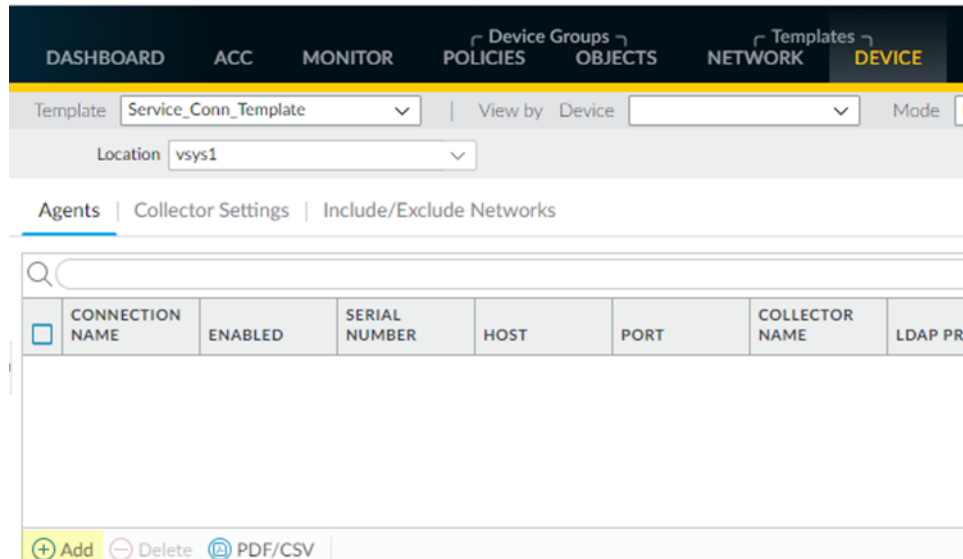
1. Find the management IP address of the Panorama that manages Prisma Access.

This address displays by in the web browser address bar when you access Panorama.



2. Make sure that you are in the **Service\_Conn\_Template** template, then select **Device > Data Redistribution > Agents**.





3. **Add** a Data Redistribution agent, give it a **Name** and select **Enabled**.
4. Enter the management IP address of the Panorama appliance. as the **Host** and 5007 as the **Port**.

### Add a Data Redistribution Agent ?

Name

Enabled

Add an Agent Using  Serial Number  Host and Port

Host

LDAP Proxy

Port

Collector Name

Collector Pre-Shared Key

Confirm Collector Pre-Shared Key

Data type  IP User Mappings  HIP

IP Tags  Quarantine List

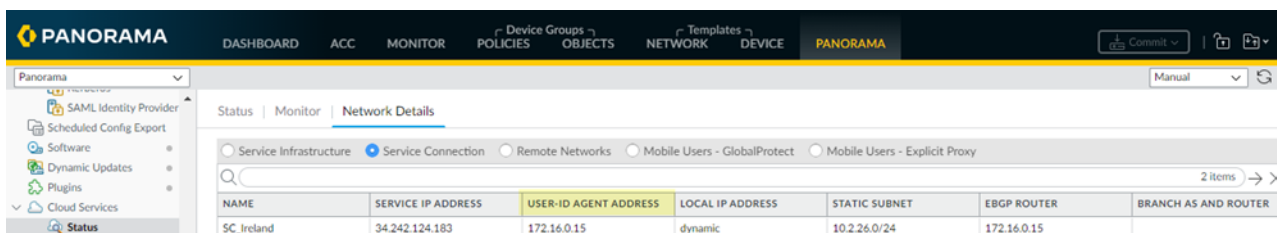
User Tags

5. Select **Quarantine List**; then, click **OK**.


**STEP 8 |** Configure a data redistribution agent that redistributes quarantine list information from the service connections to mobile user gateways.

1. From the Panorama that manages Prisma Access, select **Panorama > Cloud Services > Status > Network Details > Service Connection**.
2. Make a note of the **User-ID Agent Address** of the service connection from which you want to redistribute quarantine list information.

Since all service connections have the same redistributed quarantine list information, choose any service connection. You can also configure more than one service connection.



3. Make sure that you are in the **Mobile\_User\_Template**, then select **Device > Data Redistribution > Agents**.
4. **Add** a Data Redistribution agent, give it a **Name**, and select **Enabled**.
5. Enter the **User-ID Agent Address** of the service connection as the Host and **5007** as the Port.

 *Make sure that your network does not block access to this port between Panorama and Prisma Access.*

6. (Optional) If you have configured this service connection as a Collector (**Device > Data Redistribution > Collector Settings**), enter the **Collector Name** and **Collector Pre-Shared Key**.
7. Select **Quarantine List**; then, click **OK**.

**Add a Data Redistribution Agent** ?

Name:

Enabled

Add an Agent Using:  Serial Number  Host and Port

Host:

LDAP Proxy

Port:

Collector Name:

Collector Pre-Shared Key:

Confirm Collector Pre-Shared Key:

Data type:  IP User Mappings  HIP  
 IP Tags  Quarantine List  
 User Tags

8. **Commit and Push** your changes.

**STEP 9 |** View your quarantine list information by selecting **Panorama > Device Quarantine**.

See [View Quarantined Device Information](#) in the [GlobalProtect Administrator's Guide](#) for details.

---

# Report Website Access Issues

Some websites such as stubhub.com, ticketmaster.com, or dollartree.com, block traffic from the cloud IP address range. When users who are secured by Prisma Access attempt to access these websites, they can be denied access with the following message on the web browser:

## Access Denied.

**You don't have permission to access "http://www.dollartree.com/" on this server.** Reference #18.7f955b8.1509600370.44eb7c8

To report this problem, enter <https://reportasite.gpcloudservice.com/> from a web browser and provide the URL of the website that is inaccessible. After 24-48 hours, return to <https://reportasite.gpcloudservice.com/> and enter the same URL to see its status.



*Palo Alto Networks reviews all reported sites. If an access issue is found, Palo Alto Networks categorizes the site and adds an egress policy which changes the IP address of the site. When users access a site using a different IP address, their first attempt might be unsuccessful because the client is expected to receive a TCP RST packet, which causes modern browsers to auto-retry the connection and successfully load the site.*

If, after 48 hours, the website continues to be blocked even after a retry operation, verify that you have configured security policy to allow the user to access the specific website/web category. After confirming that your acceptable use policy allows the requested web content, open a [Support Case](#) with Palo Alto Networks Technical Support for assistance with the impacted traffic flow, specifying the steps taken to isolate the issue.



# Use Remote Networks to Secure Branches

As you business scales and your office locations become geographically distributed, Prisma Access for networks allows you to speedily onboard your remote network locations and deliver best-in-breed security for your users. It offers a convenient option that removes the complexity in configuring and managing devices at every remote location. The service provides an efficient way to easily add new remote network locations and minimize the operational challenges with ensuring that users at these locations are always connected and secure, and it allows you to manage policy centrally from Panorama for consistent and streamlined security for your remote network locations.

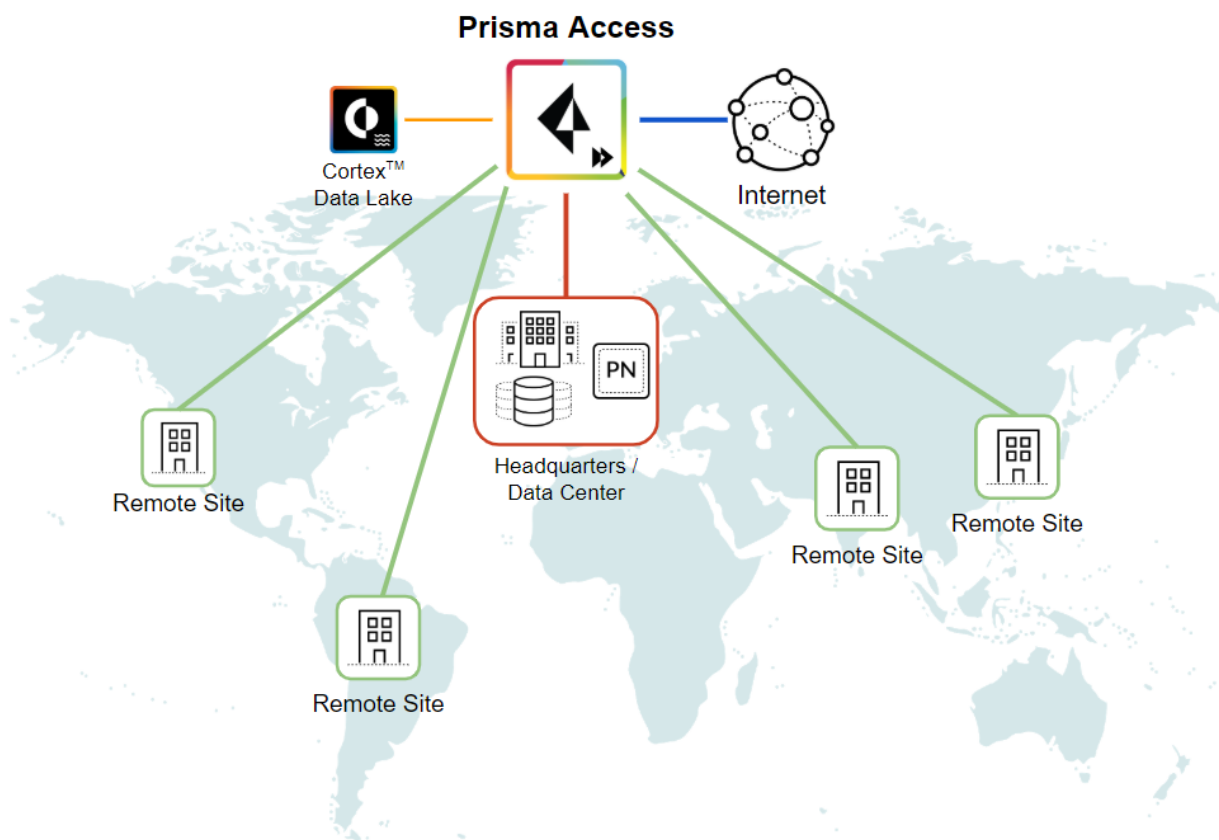
To connect your remote network locations to Prisma Access, you can use the Palo Alto Networks next-generation firewall or a third-party, IPSec-compliant device including SD-WAN, that can establish an IPSec tunnel to the service.

- > Plan to Deploy Remote Networks
- > Onboard and Configure Remote Networks
- > Quick Configs for Remote Network Deployments



# Plan to Deploy Remote Networks

Prisma Access for networks allows you to pick the geographic locations where you want to deploy Prisma Access to secure your remote network locations.



Use the following sections to plan for your remote network deployment or for planning considerations you need to when upgrading from a previous version of Prisma Access.

- [Remote Network Planning Prerequisites](#)
- [Aggregate Bandwidth Upgrade Considerations](#)

## Remote Network Planning Prerequisites

Before you begin to [onboard remote networks](#), make sure you have the following configuration items ready to ensure that you will be able to successfully enable the service and enforce policy for users in your remote network locations:

- ❑ **Bandwidth Allocation per Compute Location**—Plan your bandwidth for your remote networks locations at an aggregate level per [compute location](#). Each location you onboard has a corresponding compute location for which bandwidth is allocated. You allocate bandwidth per compute location instead of per location.

The aggregate bandwidth model is available for new and existing deployments; however, in some cases, you should not upgrade to the new model and continue to allocate bandwidth by location. See [Aggregate Bandwidth Upgrade Considerations](#) for details.

All locations you onboard share the allocated bandwidth for that compute location. For example, you need to onboard four branch offices using remote networks in the Singapore, Thailand, and Vietnam

---

locations. All these locations map to the Asia Southeast compute location. If you allocate 200 Mbps bandwidth to the Asia Southeast compute location, Prisma Access divides the 200 Mbps of bandwidth between the four branch offices you onboarded in that location. If you also add a location in Hong Kong, you note that Hong Kong maps to the Hong Kong compute location, and you would need to add bandwidth to that compute location. Specify a minimum bandwidth of 50 Mbps per compute location.

Prisma Access dynamically allocates the bandwidth based on load or demand per location. Using the previous example where the four sites collectively use up to 200 Mbps, if one or more sites are not using as much bandwidth as the other sites, Prisma Access provides more bandwidth for the locations that are more in demand, giving you a more efficient use of allocated bandwidth. In addition, if one of the sites goes down, Prisma Access reallocates the bandwidth between the other sites that are still up in that compute location.



*For more details about the bandwidth allocation process and the steps you perform to configure it, see [this video](#).*

- ❑ **Service Connection**—If your remote network locations require access to infrastructure in your corporate headquarters to authenticate users or to enable access to critical network assets, you must [create a service connection](#) so that headquarters and the remote network locations are connected. If the remote network location is autonomous and does not need to access to infrastructure at other locations, you do not need to set up the service connection (unless your mobile users need access).
- ❑ **Template**—Prisma Access automatically creates a template stack (Remote\_Network\_Template\_Stack) and a top-level template (Remote\_Network\_Template) for Prisma Access for networks. To [Onboard and Configure Remote Networks](#), you will either need to configure the top-level template from scratch or leverage your existing configuration, if you are already running a Palo Alto networks firewall on premise. The template requires the settings to establish the IPSec tunnel and Internet Key Exchange (IKE) configuration for protocol negotiation between your remote network location and Prisma Access for networks, zones that you can reference in security policy, and a log forwarding profile so that you can forward logs from the Prisma Access for remote networks to Cortex Data Lake.
- ❑ **Parent Device Group**—Prisma Access for networks requires you to specify a parent device group that will include your [security policy](#), [security profiles](#), and other policy objects (such as application groups and objects, and address groups), as well as [authentication policy](#) so that Prisma Access for networks can consistently enforce policy for traffic that is routed through the IPSec tunnel to Prisma Access for networks. You will need to either define policy rules and objects on Panorama or use an existing device group to secure users in the remote network location.



*If you use an existing device group that references zones, make sure to add the corresponding template that defines the zones to the Remote\_Network\_Template\_Stack. Doing so will allow you to complete the zone mapping when you [Onboard and Configure Remote Networks](#).*

- ❑ **IP Subnets**—In order for Prisma Access to route traffic to your remote networks, you must provide routing information for the subnetworks that you want to secure using Prisma Access. You can do this in several ways. You can either define a static route to each subnetwork at the remote network location, or configure BGP between your service connection locations and Prisma Access, or use a combination of both methods. If you configure both static routes and enable BGP, the static routes take precedence. While it might be convenient to use static routes if you have just a few subnetworks at your remote network locations, in a large deployment with many remote networks [with overlapping subnets](#), BGP will enable you to scale more easily.
- ❑ **IPSec Termination Nodes**—IPSec termination nodes allow you to associate remote networks with compute locations. When you [onboard a remote network](#), select an IPSec termination node for the remote network that correlates to the compute location.

You can specify a maximum of 250 remote networks per IPSec termination node. After you use 250 remote networks on an IPSec termination node in a compute location, you cannot onboard additional remote networks in that IPSec termination node. You can have a maximum of 200 IPSec termination nodes in a compute location.



# Aggregate Bandwidth Upgrade Considerations

If you have an existing Prisma Access deployment and have already onboarded remote networks, you can choose to either migrate your deployment to the aggregate bandwidth model or continue to allocate bandwidth by location after the upgrade.

Multi-tenant deployments can upgrade to the aggregate bandwidth model, and you can mix tenants in a multi-tenant deployment that use either the aggregate bandwidth model or allocate bandwidth by location.

Continue to allocate bandwidth by location if you have any of the following Prisma Access capabilities enabled:

- [Quality of Service for remote networks](#)
- [Secure inbound access for remote networks](#)
- Any remote network connections that have a bandwidth of 1000 Mbps
- If you have deployed [Prisma Access for Networks \(formerly CloudGenix\) Cloud Blade 2.0](#) (Cloud Blade 2.1 is supported)

A minimum bandwidth allotment of 300 Mbps is required to migrate to the bandwidth allocation model. In some cases, Prisma Access might consume additional bandwidth when allocating bandwidth based on compute locations, and your licensed bandwidth might not be sufficient to migrate. Palo Alto Networks recommends that you map your existing remote networks to their respective compute locations and perform a calculation of the bandwidth you require before you migrate to the bandwidth allocation model. In multi-tenant deployments, you might need to redistribute the bandwidth between tenants before you upgrade.

For example, you have the following remote network connections in the following locations with the following bandwidth.

Location	Bandwidth
US Northwest	150 Mbps
South Africa West	2 Mbps
Ireland	20 Mbps
South Korea	2 Mbps
<b>Total Bandwidth: 174 Mbps</b>	

When you migrate to the bandwidth allocation model, you allocate bandwidth at the [compute location](#) level. The minimum bandwidth you can allocate to a compute location is 50 Mbps, which changes the effective bandwidth consumption of the South Africa West, Ireland, and South Korea locations.

Location	Compute Location	Allocated Bandwidth per Compute Location
US Northwest	US Northwest	150 Mbps
South Africa West	South Africa West	50 Mbps
Ireland	Ireland	50 Mbps
South Korea	South Korea	50 Mbps

---

Location	Compute Location	Allocated Bandwidth per Compute Location
----------	------------------	------------------------------------------

**Total Bandwidth: 300 Mbps**

---

---

# Onboard and Configure Remote Networks

For each remote network that you want to secure using Prisma Access for networks, you must use the following workflow to push the required policy configuration to Prisma Access and onboard each remote network so that you can start sending traffic from the remote site through the IPsec tunnel to Prisma Access.

Use one of the following workflows to onboard your remote networks:

- If you have a new deployment, or if you have an existing deployment that wants to migrate to allocating bandwidth by compute location, use the workflow to [allocate bandwidth by compute location](#), also known as the *bandwidth allocation model*.

Not all existing deployments can upgrade to the bandwidth allocation model. See [Aggregate Bandwidth Upgrade Considerations](#) for details.

- If you have an existing deployment with onboarded remote networks and you want to continue to allocate bandwidth per remote network location, or if you have a deployment that cannot migrate to the bandwidth allocation model, use the procedure to [allocate bandwidth by remote network location](#).

Before you begin onboarding your remote networks, be sure you go through the steps to [Plan to Deploy Remote Networks](#).

## Configure Prisma Access for Networks—Configure Bandwidth by Compute Location

If you need to onboard many remote network locations, onboard a remote network using this workflow and then [import the remote network configuration](#).

**STEP 1** | Select **Panorama > Cloud Services > Configuration > Remote Networks** and edit the settings by clicking the gear icon in the **Settings** area.

1. In the Templates section, **Add** any templates that contain configuration you want to push to Prisma Access for networks. For example, if you have existing templates that contain your zone configurations, or IPsec tunnel, IKE Gateway, or crypto profile settings, you can add them to the predefined Remote\_Network\_Template\_Stack to simplify the onboarding process.

You can **Add** more than one template to the stack and then order them appropriately using **Move Up** and **Move Down**. This is important because Panorama evaluates in the stack from top to bottom, with settings in templates higher in the stack taking priority over the same settings specified in templates lower in the stack. Note that you cannot move the default template from the top of the stack.



*Although you can add existing templates to the stack from the plugin, you cannot create a new template from the plugin. Instead, use the workflow to [add a new template](#).*

2. Select the **Parent Device Group** for Prisma Access for remote networks. You can select an existing device group or use **Shared**.

You will push all of the configuration—including the [security policy](#), [security profiles](#), and other policy objects (such as application groups and objects, and address groups), [HIP objects and profiles](#) and [authentication policy](#)—that Prisma Access for networks needs to enforce consistent policy to your remote network users using the [device group hierarchy](#) you specify here.



You don't need to define all of the policy that you will push to the remote network yet. Instead, configure the settings to onboard the remote site. You can then go back and add the templates and device groups with the complete configurations to push consistent policy out to your remote networks.

3. If you will be configuring remote networks that have overlapping subnets, select the **Overlapped Subnets** check box to enable outbound internet access for those locations.

While configuring [Remote Network Locations with Overlapping Subnets](#) introduces some limitations, it is acceptable in some cases (for example, if you want to add a guest network at a retail store location).

Settings

Settings | DNS Proxy | Group Mapping Settings

Template Stack

Template Stack Name: Remote\_Network\_Template\_Stack

Templates

TEMPLATES
Remote_Network_Template
<input type="checkbox"/> test

+ Add - Delete ↑ Move Up ↓ Move Down

The template at the top of the stack has the highest priority in the presence of overlapping config

Device Group

Device Group Name: Remote\_Network\_Device\_Group

Parent Device Group: Shared

Master Device:

Overlapped Subnets

Overlapped Subnets

Enabling Overlapped Subnets allows outbound internet to be supported for remote networks with overlapping subnets that are configured in the same region.

OK Cancel

## STEP 2 | (Optional) Configure DNS Proxy settings for your remote network.

Prisma Access allows you to [specify DNS servers](#) to resolve both domains that are internal to your organization and external domains. If you do not specify any settings, Prisma Access does not proxy DNS requests for remote networks.

1. In the **Remote\_Network\_Device\_Group** device group, select **Policies > Security** and **Add** a security policy rule with an **Application** of **DNS** and an **Action** of **Allow** to allow DNS traffic.

Without a security policy rule to allow DNS traffic, DNS resolution does not occur.

	NAME	LOCATION	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	P
1	dns-traffic-rule	Remote_Network...	none	universal	Trust	any	any	any	any	any	any	dns	any	Allow	n

2. If you configure Prisma Access to [proxy the DNS requests](#) from your remote networks, update the DNS settings on all the endpoints in that network to use the Prisma Access **Remote Network DNS Proxy IP Address** as the primary DNS server and use your DNS server as secondary DNS server. You can get this DNS proxy IP from **Panorama > Cloud Services > Status > Network Details > Service Infrastructure**.

<input checked="" type="radio"/> Service Infrastructure <input type="radio"/> Service Connection <input type="radio"/> Remote Networks <input type="radio"/> Mobile Users <input type="radio"/> Clean Pipe					
INFRASTRUCTURE SUBNET	INFRASTRUCTURE BGP AS	CAPTIVE PORTAL REDIRECT IP ADDRESS	TUNNEL MONITOR IP ADDRESS	LOOPBACK IPS	REMOTE NETWORK DNS PROXY IP ADDRESS
172.16.30.0/24	65534	172.16.30.254	172.16.30.254	172.16.30.4 172.16.30.5	172.16.30.254

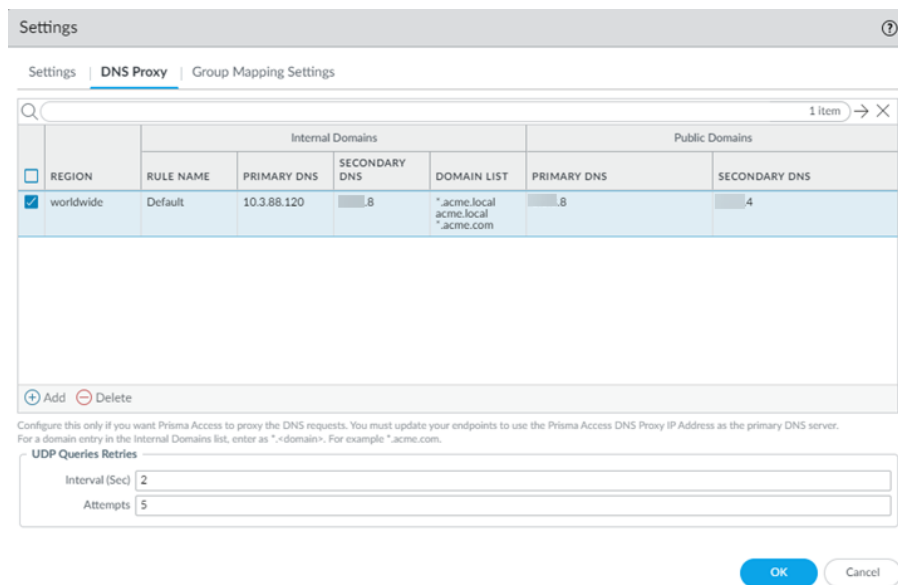
### 3. Add one or more **DNS Proxy** settings, entering the following values:

- Select a **Region** from the drop-down at the top of the window.
 

Select a specific region, or select **Worldwide** to apply the DNS settings globally. If you specify multiple proxy settings with a mix of regional and Worldwide regions, Prisma Access uses the regional settings for the Locations in the region or regions you specify and uses the worldwide settings elsewhere. Prisma Access evaluates the rules from top to bottom in the list.
- **Add** one or more rules to configure the DNS settings for **Internal Domains**.
  - Enter a unique **Rule Name** for the rule.
  - you want your internal DNS server to only resolve the domains you specify, enter the domains to resolve in the **Domain List**. Specify an asterisk in front of the domain; for example, \*.acme.com. You can specify a maximum of 1,024 domain entries.
  - If you have a **Custom DNS server** that can access your internal domains, specify the **Primary DNS** and **Secondary DNS** server IP addresses, or select **Use Cloud Default** to use the default Prisma Access DNS server.
- Specify the DNS settings for **Public Domains**.
  - **Use Cloud Default**—Use the default Prisma Access DNS server.
  - **Same as Internal Domains**—Use the same server that you use to resolve internal domains. When you select this option, the DNS Server used to resolve public domains is same as the server configured for the first rule in the **Internal Domains** section.
  - **Custom DNS server**—If you have a DNS server that can access your public (external) domains, enter the Primary DNS server address in that field.

(Optional) You can **Add** a **DNS Suffix** to specify the suffix that the client should use locally when an unqualified hostname is entered that it cannot resolve, for example, acme.local. Do not enter a wildcard (\*) character in front of the domain suffix (for example, acme.com). You can add multiple suffixes.
- If you want Prisma Access to proxy DNS requests, configure Configure values for the use for UDP queries (the **Interval** to retry the query in seconds and the number of retry **Attempts** to perform).

If you want Prisma Access to [proxy DNS requests](#) for your GlobalProtect users, You must update your endpoints to use the **Remote Network DNS Proxy IP Address** as the primary DNS server (**Panorama > Cloud Services > Status > Network Details > Service Infrastructure**).



**STEP 3 | (Optional)** Configure Prisma Access to use the Directory Sync service to retrieve user and group information.

You must [configure Directory Sync](#) to retrieve user and group information from your Active Directory (AD) before you enable and configure Directory Sync integration in Prisma Access using the settings in the **Group Mapping Settings** tab. See [Get User and Group Information Using Directory Sync](#) for details.

**STEP 4 |** Create new zones in the one of the templates in the stack (**Network > Zones > Add**) or [map the zones](#) referenced in existing templates you added to the stack as trusted or untrusted. On Panorama, policy rules are defined in device groups, and zones are defined in templates. Therefore, you need to make sure that you add the templates that reference the zones included in your policy rules to the template stack.

On a Palo Alto Networks® next-generation firewall, security policy is enforced between zones, which map to physical or virtual interfaces on the firewall. But as Prisma Access for networks has only two zones, trust and untrust, you need to map any zone with traffic bound to the Internet (including your sanctioned SaaS applications) as untrust and all internal zones as trust.

1. (Optional) Edit the [zone mapping](#) settings.

By default, all of the zones in Prisma Access for networks template stack are classified as Untrusted Zones. If you have not yet defined zones or if the templates in the Remote\_Network\_Template\_Stack do not have zone configurations, you can come back and add them when you push policy to Prisma Access for networks.

2. For each zone you want to designate as trusted, select it and click **Add** to move it to the list of **Trusted Zones**.
3. Click **OK** to save the mappings.

**STEP 5 |** Allocate bandwidth for the locations that you want to onboard by clicking the gear icon in the **Bandwidth Allocation** area.

You allocate bandwidth at an aggregate level per [compute location](#). See [Plan to Deploy Remote Networks](#) for details.

Service Setup   Mobile Users   Clear Pipe   **Remote Networks**   Service Connection   Traffic Steering

---

Settings	Zone Mapping	Bandwidth Allocation
Template Stack Remote_Network_Template_Stack... └ Remote_Network_Template · Parent Device Group Shared · └ Remote_Network_Device_Group · Overlapped Subnets <input type="checkbox"/>	Trusted Zones (Not Configured) Untrusted Zones (Not Configured)	Allocated Bandwidth 1139/1200 Mbps

If you have an existing remote networks deployment that currently onboards remote networks by location, a pop-up window displays, asking if you want to migrate to the bandwidth allocation model. Click **Migrate** to continue, or **Cancel** to cancel the migration.



*You must Commit and Push your changes after you migrate to the bandwidth allocation model.*

**Aggregate Bandwidth Settings** ⓘ ?

You are currently allocating bandwidth for remote networks on a per site basis. You now have the flexibility to allocate bandwidth at a compute location level, so that all remote network sites in that compute location share the bandwidth you allocate. When any site in that compute location does not consume the bandwidth it becomes available for other sites in that compute location.

Click **Migrate** to migrate to the Aggregate bandwidth allocation model; you cannot revert to allocating bandwidth per site after you migrate. Click **Cancel** to cancel the migration and continue to allocate bandwidth by site.

Migrate
Cancel

**STEP 6 |** Enter the **Bandwidth Allocation** you want for each **Compute Location** that is associated with the **Prisma Access Locations** you want to onboard; then, click **OK**.

To verify the bandwidth amount you entered, select the check mark next to the bandwidth amount; to cancel the amount, select **x**.

Specify a minimum bandwidth of 50 Mbps and a maximum bandwidth of the maximum remaining licensed bandwidth.

**Bandwidth Allocation** ?


**Allocated Total : 1139 / 1200 Mbps**  
Click each bandwidth allocation to edit bandwidth allocated to compute location

Search:  25 items

Bandwidth Allocation (Mbps)	Compute Location	Prisma Access Locations
0	Canada Central	Canada Central, Canada East
0	US Northwest	Canada West, US Northwest
0	US Southeast	Costa Rica, Mexico Central, Panama, US Southeast, Colombia
0	US Southwest	Mexico West, US Southwest, US West
0	US Central	US Central, US South
100	US East	US East, US Northeast
0	South America East	Argentina, Bolivia, Brazil Central, Brazil East, Brazil South, Chile, Ecuador, Paraguay, Peru, Venezuela
0	Europe Central	Andorra, Austria, Bulgaria, Croatia, Czech Republic, Germany Central, Germany North, Germany South, Greece, Hungary, Italy, Liechtenstein, Luxembourg, Moldova, Monaco, Poland, Portugal, Romania, Slovakia, Slovenia, Spain Central, Spain East, Ukraine, Uzbekistan, Egypt, Israel, Jordan, Kuwait, Saudi Arabia, Turkey, United Arab Emirates, Kenya, Nigeria, South Africa Central
0	Europe North	Belarus, Finland, Lithuania, Norway, Russia Central, Russia Northwest, Sweden
0	Belgium	Belgium
0	Europe West	Denmark, Netherlands Central, Netherlands South

**OK**

**STEP 7 |** Click **Add** in the Onboarding settings, and specify a **Name** to identify the infrastructure that will secure the remote network location you are onboarding.

 *You cannot change the name of the remote network location after you enter it. Make sure you know your naming scheme for your remote networks before you begin onboarding.*

**STEP 8 |** (BGP deployments only) Create a configuration so that your remote network connection can use up to four IPsec tunnels for its traffic (**ECMP Load Balancing**).

QoS is not supported with ECMP load balancing, and static routes are not supported (BGP is required). If your deployment uses one IPsec tunnel for its remote network connection or uses static routes, select **None** for **ECMP Load Balancing** and continue to Step 11.

1. Select one of the choices to enable or disable ECMP load balancing.

- **None**—Do not use ECMP load balancing (use a single remote network tunnel for this remote network connection). This is the only choice you can make for static routes; BGP is required for ECMP load balancing.
- **Enabled with Symmetric Return**—Specify up to four IPsec tunnels for this remote network connection and force Prisma Access to use the same link for the return traffic as it used to send the traffic.

Select this option if you use one or more tunnels as a backup tunnel to be used only if one of the primary tunnels go down. If a link fails, Prisma Access uses one of the other tunnels to send and receive traffic symmetrically.



Onboarding
?

Name

ECMP Load Balancing

Location

IPSec Termination Node


<input type="checkbox"/> IPSEC TUNNEL	BGP

+ Add
- Delete

2. **Add** an IPsec tunnel for the remote network connection and specify the following values:


- **Enable**—Enables BGP for the IPsec tunnel.  
This selection is not configurable; you must enable BGP to configure ECMP.
- **Summarize Mobile User Routes before advertising**—Reduces the number of mobile user IP subnet advertisements over BGP to your customer premises equipment (CPE) by summarizing them.

By default, Prisma Access advertises the mobile users IP address pools **in blocks of /24 subnets**; if you summarize them, Prisma Access advertises the pool based on the subnet you specified. For example, Prisma Access advertises a public user mobile IP pool of 10.8.0.0/20 using the /20 subnet, rather than dividing the pool into subnets of 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24, and so on before advertising them. Summarizing these advertisements can reduce the number of routes stored in CPE routing tables. For example, you can use IP pool summarization with cloud VPN gateways (Virtual Private Gateways (VGWs) or Transit Gateways (TGWs) that can accept a limited number of routes.

 *If you enable route summarization for a location that uses ECMP, you must enable route summarization on all links to that location, or you will receive an error during commit.*

Prisma Access sets the community string for aggregated mobile user routes to 0xFFFFE:0xFFF0.

- **Advertise Default Route**—Allows Prisma Access to advertise a default route for the remote network using eBGP.

 *You must publish your default routes before you make this selection to advertise them. In addition, be sure that your network does not have another default route being advertised by BGP, or you could introduce routing issues in your network.*

- **Don't Advertise Prisma Access Routes**—Prevents the Prisma Access BGP peer from forwarding routes into your organization's network.

By default, Prisma Access advertises all BGP routing information, including local routes and all prefixes it receives from other service connections, remote networks, and mobile user subnets. Select this check box to prevent Prisma Access from sending any BGP advertisements, but still use the BGP information it receives to learn routes from other BGP neighbors.

Since Prisma Access does not send BGP advertisements if you select this option, you must configure static routes on the on-premises equipment to establish routes back to Prisma Access.

## Link ?

IPSec Tunnel

### BGP

- Enable
- Advertise Default Route
- Summarize Mobile User Routes before advertising
- Don't Advertise Prisma Access Routes

Peer As

Peer IP Address

Local IP Address

Secret

Confirm Secret

- **Peer AS**—Specify the autonomous system (AS) to which the firewall, virtual router, or BGP router at your remote network belongs.
- **Peer IP Address**—Enter the IP address assigned as the Router ID of the eBGP router on the remote network for which you are configuring this connection.
- **Local IP Address (Optional)**—Enter an address that Prisma Access uses as its Local IP address for BGP. Specify the IP address to use on the Prisma Access side of the tunnel.

Specifying a **Local Address** is useful where the device on the other side of the connection (such as an Amazon Web Service (AWS) Virtual Private Gateway) requires a specific local IP address for BGP peering to be successful. Make sure that the address you specify does not conflict or overlap with IP addresses in the Infrastructure Subnet or subnets in the remote network.

- **Secret and Confirm Secret (Optional)**—Enter and confirm a passphrase to authenticate BGP peer communications.
3. Repeat the previous step to add up to four tunnels to use with the remote network connection.

**Onboarding** ?

Name

ECMP Load Balancing

Location

IPSec Termination Node

	IPSEC TUNNEL	BGP
<input type="checkbox"/>	ECMP-IRE-1	yes
<input type="checkbox"/>	ECMP-IRE-2	yes
<input type="checkbox"/>	ECMP-IRE3	yes
<input type="checkbox"/>	ECMP-IRE4	yes

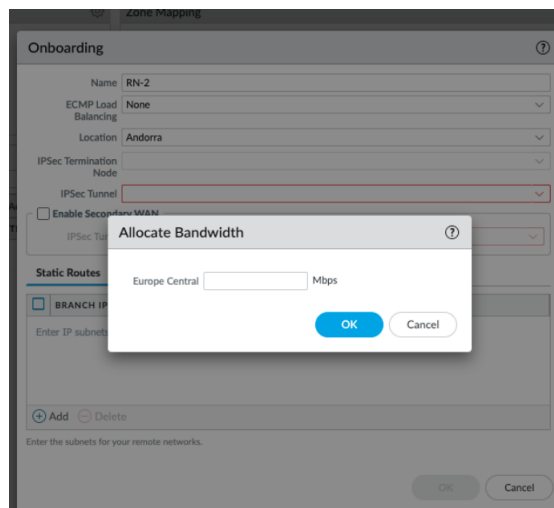
+ Add - Delete

OK
Cancel

**STEP 9** | Select the **Location** in which Prisma Access will deploy the infrastructure required to secure your remote network location. This region should be geographically located close to your remote network location.

See [this table](#) for a list of Prisma Access locations.

If you have not yet allocated bandwidth for the [compute location](#) to which the location maps, Prisma Access prompts you to enter bandwidth for that compute location.



**STEP 10** | Select the **IPSec Termination Node** that you want to use for this remote network. Prisma Access uses this node to associate remote network locations with compute locations.

---

**STEP 11** | (Static routing or single-tunnel deployments only) Select or add a new **IPSec Tunnel** configuration to access the firewall, router, or SD-WAN device at the corporate location:

- If you have added a template to the Remote\_Network\_Template\_Stack (or modified the predefined Remote\_Network\_Template) that includes an IPSec Tunnel configuration, select that **IPSec Tunnel** from the drop-down. Note that the tunnel you are creating for each remote network connection connects Prisma Access to the IPSec-capable device at each branch location.

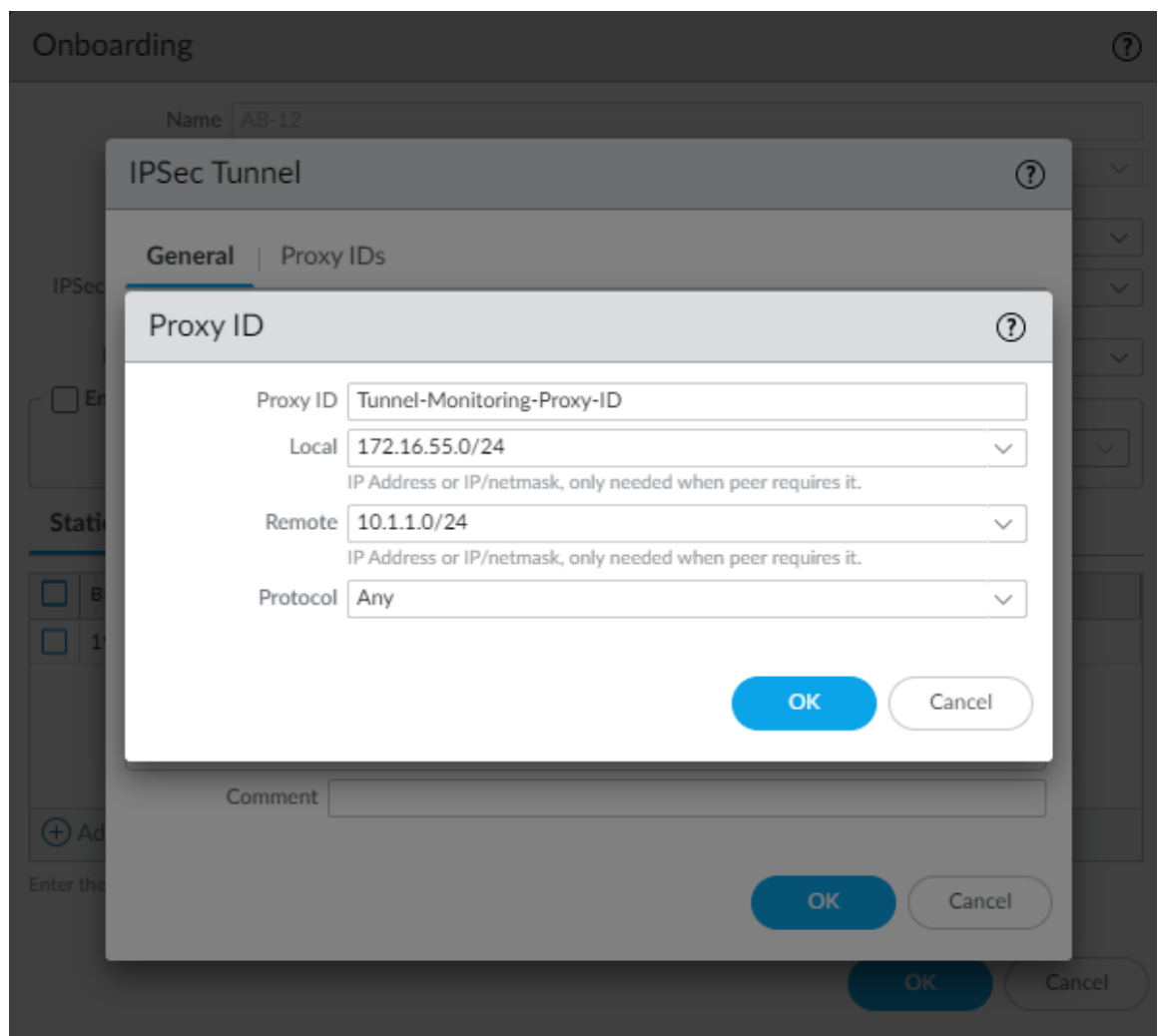
User the following guidelines when configuring an IPSec tunnel:

- The peer addresses in the IKE Gateway configuration must be unique for each tunnel. You can, however, re-use some of the other common configuration elements, such as crypto profiles.
- The IPSec Tunnel you select from a template must use Auto Key exchange and IPv4 only.
- If you onboard multiple remote networks to the same location with dynamic IKE peers, you must use the same IKE crypto profile for all remote network configurations.
- To [create a new IPSec Tunnel](#) configuration, click **New IPSec Tunnel**, give it a **Name** and configure the [IKE Gateway](#), [IPSec Crypto Profile](#), and [Tunnel Monitoring](#) settings.
  - If the IPSec-capable device at your branch location uses policy-based VPN, on the **Proxy IDs** tab, **Add** a proxy ID that matches the settings configured on your local IPSec device to ensure that Prisma Access can successfully establish an IPSec tunnel with your local device.
- Leave **Enable Replay Protection** selected to detect and neutralize against replay attacks.
- Select **Copy TOS Header** to copy the Type of Service (TOS) header from the inner IP header to the outer IP header of the encapsulated packets in order to preserve the original TOS information.
- To enable tunnel monitoring for the service connection, select **Tunnel Monitor**.
  - Enter a **Destination IP** address.

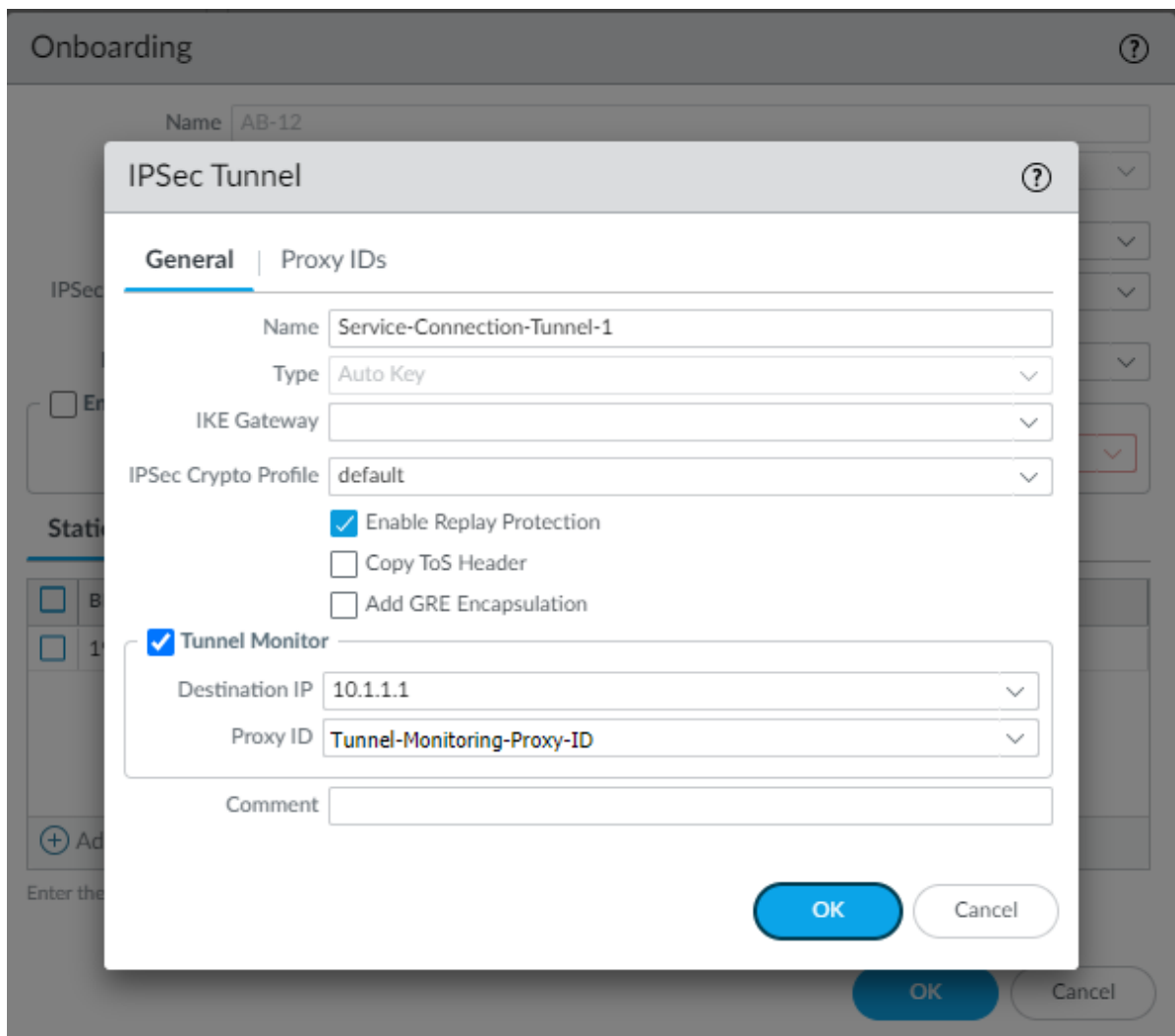
Specify an IP address at your branch location to which Prisma Access can send ICMP ping requests for IPSec tunnel monitoring. Make sure that this address is reachable by ICMP from the entire Prisma Access infrastructure subnet.


- If you use tunnel monitoring with a peer device that uses multiple proxy IDs, specify a **Proxy ID** or add a **New Proxy ID** that allows access from the infrastructure subnet to your branch location.

The following figure shows a proxy ID with the service infrastructure subnet (172.16.55.0/24 in this example) as the **Local** IP subnet and the branch location's subnet (10.1.1.0/24 in this example) as the **Remote** subnet.




The following figure shows the Proxy ID you created being applied to the tunnel monitor configuration by specifying it in the **Proxy ID** field.



 You must configure a static route on your CPE to the Tunnel Monitor IP Address for tunnel monitoring to function. To find the destination IP address to use for tunnel monitoring from your branch location to Prisma Access, select Panorama > Cloud Services > Status > Network Details, click the Service Infrastructure radio button, and find the Tunnel Monitor IP Address.

**STEP 12** | If you have a secondary WAN link at this location, select **Enable Secondary WAN**.

 Be sure to create a unique IPsec tunnel for each remote network's secondary WAN; Prisma Access does not support reusing the same IPsec tunnel for secondary WANs in multiple remote networks.

If you use static routes, tunnel failover time is less than 15 seconds from the time of detection, depending on your WAN provider.

If you configure BGP routing and have enabled tunnel monitoring, the shortest default hold time to determine that a security parameter index (SPI) is failing is the tunnel monitor, which removes all routes to a peer when it detects a tunnel failure for 15 consecutive seconds. In this way, the tunnel monitor determines the behavior of the BGP routes. If you do not configure tunnel monitoring, the hold timer determines the amount of time that the tunnel is down before removing the route. Prisma Access uses the default BGP HoldTime value of 90 seconds as defined by RFC 4271, which is the maximum wait

---

time before Prisma Access removes a route for an inactive SPI. If the peer BGP device has a shorter configured hold time, the BGP hold timer uses the lower value.

When the secondary tunnel is successfully installed, the secondary route takes precedence until the primary tunnel comes back up. If the primary and secondary are both up, the primary route takes priority.



*If you use a different BGP peer for the secondary (backup) connection, Prisma Access does not honor the Multi-Exit Discriminator (MED) attributes advertised by the CPE. This caveat applies if you use multiple BGP peers on either remote network connections or service connections.*

### STEP 13 | Enable routing to the subnetworks or individual IP addresses at the remote network site that your users will need access to.

Prisma Access uses this information to route requests to the appropriate site. The networks at each site cannot overlap with each other or with IP address pools that you designated for the service infrastructure or for the Prisma Access for users IP pools. You can configure **Static Routes**, **BGP**, or a combination of both.

- To configure **Static Routes**:
  1. On the **Static Routes** tab, click **Add** and enter the subnetwork address (for example, 172.168.10.0/24) or individual IP address of a resource, such as a DNS server (for example, 10.32.5.1/32) that your remote users will need access to.
  2. Repeat for all subnets or IP addresses that Prisma Access will need access to at this location.

Onboarding
?

Name

ECMP Load Balancing

Location

IPSec Termination Node

IPSec Tunnel

Enable Secondary WAN

IPSec Tunnel

**Static Routes** | BGP

BRANCH IP SUBNETS ^

<input checked="" type="checkbox"/>	

Enter the subnets for your remote networks.

- To configure **BGP**:
  1. Select the **BGP** tab.
  2. Select the **ECMP Load Balancing** choices. See Step 8.
  3. If you select **None** for **ECMP Load Balancing**, enter the BGP choices.



Onboarding
?

Name

ECMP Load Balancing

Location

IPSec Termination Node

IPSec Tunnel

Enable Secondary WAN

IPSec Tunnel

Static Routes | **BGP**

Enable

Summarize Mobile User Routes before advertising

Advertise Default Route

Don't Advertise Prisma Access Routes

**Primary WAN**

Peer AS

Peer Address

Local Address

Secret

Confirm Secret

**Secondary WAN**

Same as Primary WAN

Peer AS

Peer Address

Local Address

Secret

Confirm Secret

4. To enable BGP for the remote network connection, select **Enable**.

When you enable BGP, Prisma Access sets the time to life (TTL) value for external BGP (eBGP) to 8 to accommodate any extra hops that might occur between the Prisma Access infrastructure and your customer premises equipment (CPE) that terminates the eBGP connection.

5. To reduce the number of mobile user IP subnet advertisements over BGP to your customer premises equipment (CPE) by summarizing them, select **Summarize Mobile User Routes before advertising**.


By default, Prisma Access advertises the mobile users IP address pools [in blocks of /24 subnets](#); if you summarize them, Prisma Access advertises the pool based on the subnet you specified. For example, Prisma Access advertises a public user mobile IP pool of 10.8.0.0/20 using the /20 subnet, rather than dividing the pool into subnets of 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24, and so on before advertising them. Summarizing these advertisements can reduce the number of routes stored in CPE routing tables. For example, you can use IP pool summarization with cloud VPN gateways (Virtual Private Gateways (VGWs) or Transit Gateways (TGWs)) that can accept a limited number of routes.

---

Prisma Access sets the community string for aggregated mobile user routes to 0xFFFFE:0xFFF0.

6. To allow Prisma Access to advertise a default route for the remote network using eBGP, select **Advertise Default Route**.

If you select **Advertise Default Route**, be sure that your network does not have another default route being advertised by BGP, or you could introduce routing issues in your network.

 *You must publish your default routes before you make this selection to advertise them. In addition, be sure that your network does not have another default route being advertised by BGP, or you could introduce routing issues in your network.*


7. To prevent the BGP peer on the Prisma Access firewall from forwarding routes into your organization's network, select **Don't Advertise Prisma Access Routes**.

By default, Prisma Access advertises all BGP routing information, including local routes and all prefixes it receives from other service connections, remote networks, and mobile user subnets. Select this check box to prevent Prisma Access from sending any BGP advertisements, but still use the BGP information it receives to learn routes from other BGP neighbors.

Since Prisma Access does not send BGP advertisements if you select this option, you must configure static routes on the on-premises equipment to establish routes back to Prisma Access.


8. Enter the **Peer AS**, which is the autonomous system (AS) to which the firewall, virtual router, or BGP router at your remote network belongs.
9. Enter the IP address assigned as the Router ID of the eBGP router on the remote network for which you are configuring this connection as the **Peer Address**.
10. (Optional) Enter an address that Prisma Access uses as its Local IP address for BGP.

Specifying a **Local Address** is useful where the device on the other side of the connection (such as an Amazon Web Service (AWS) Virtual Private Gateway) requires a specific local IP address for BGP peering to be successful. Make sure that the address you specify does not conflict or overlap with IP addresses in the Infrastructure Subnet or subnets in the remote network.

 *You must configure a static route on your CPE to the BGP Local Address.*

11. (Optional) Enter and confirm a passphrase to authenticate BGP peer communications.
12. (Optional) If you configured a **Secondary WAN** and you need to change the **Peer Address** or **Local Address** for the secondary (backup) BGP peer, deselect **Same as Primary WAN** and enter a unique Peer and, optionally, Local IP address for the secondary WAN.

In some deployments (for example, when using BGP to peer with an [AWS VPN gateway](#)), the BGP peer for the primary and secondary WAN might be different. In those scenarios, you can choose to set a different BGP peer for the secondary WAN.

 *For BGP deployments with secondary WANs, Prisma Access sets both the primary and secondary tunnels in an UP state, but follows normal BGP active-backup behavior for network traffic. Prisma Access sets the primary tunnel as active and sends and receives traffic through that tunnel only; if the primary tunnel fails, Prisma Access detects the failure using BGP rules, sets the secondary tunnel as active, and uses only the secondary tunnel to send and receive traffic.*

Onboarding
?

Name

ECMP Load Balancing

Location

IPSec Termination Node

IPSec Tunnel

Enable Secondary WAN

IPSec Tunnel

---

Static Routes

BGP

Enable

Summarize Mobile User Routes before advertising

Advertise Default Route

Don't Advertise Prisma Access Routes

**Primary WAN**

Peer AS

Peer Address

Local Address

Secret

Confirm Secret

**Secondary WAN**

Same as Primary WAN

Peer AS

Peer Address

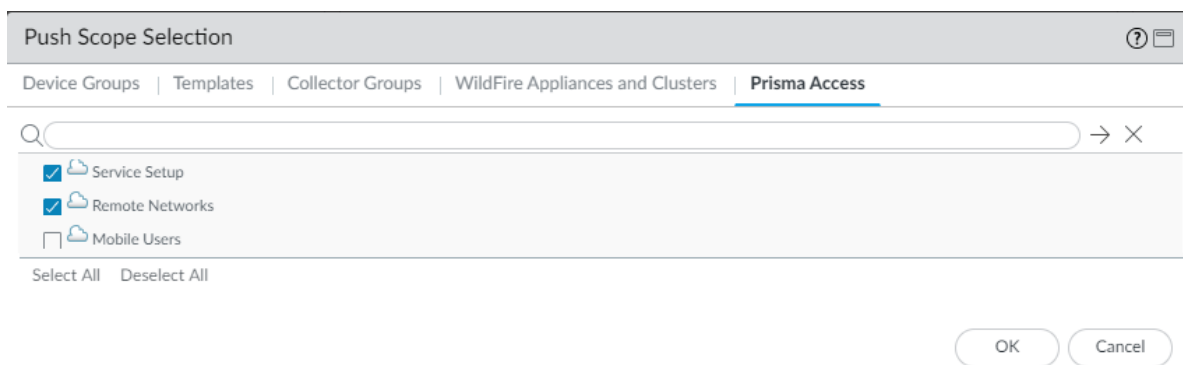
Local Address

Secret

Confirm Secret

**STEP 14** | Commit the configuration changes to Panorama and push the configuration out to Prisma Access for networks.

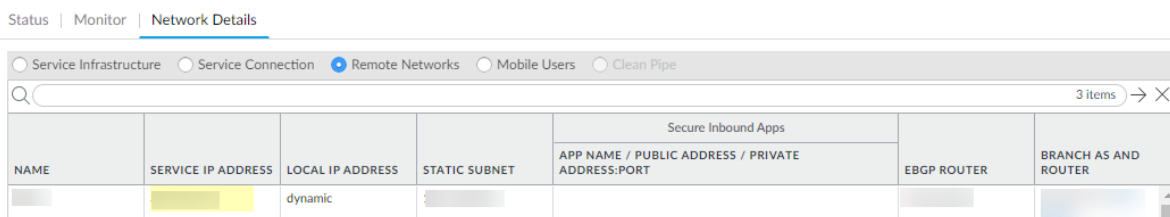
1. Click **Commit** > **Commit to Panorama**.
2. Click **Commit** > **Commit and Push**. Click **Edit Selections** > **Prisma Access**, and select both Prisma Access for networks and Prisma Access for service setup to push the configuration out to the service.



3. Click **OK** and **Push**.

**STEP 15** | Configure the IPsec-capable device at the remote network location to set up an IPsec connection with Prisma Access for networks.

1. Find the **Service IP Address** for this remote network connection by selecting **Panorama > Cloud Services > Status > Network Details**, clicking the **Remote Networks** radio button, and viewing the **Service IP Address** field. Prisma Access for networks infrastructure has assigned this IP address for the Prisma Access remote network connection, and you must configure this as the peer IP address to set up the IPsec tunnel between the remote network location and Prisma Access for networks.



2. Check the **Local IP address** for the device at the remote network location on the **Panorama > Cloud Services > Status > Network Details > Remote Networks** page. If you are performing NAT at the remote network location, the **Local IP address** displays the IP address of the device after NAT.

**STEP 16** | To secure traffic at the remote network location you must create security policy rules.

1. Select **Policies**.
2. Select the **Device Group** in which to add policy rules. You can select the **Remote\_Network\_Device\_Group** or the parent device group that you selected for defining policies to secure the remote network location.
3. **Create security policy rules**. Make sure that you do not define security policy rules to allow traffic from any zone to any zone. In the security policy rules, use the zones that you defined in your template.

If a user on your network is denied access to a website, [report website access issues](#) before you open a ticket with Palo Alto Networks.

**STEP 17** | Enable logging to Cortex Data Lake. You must create and attach a log forwarding profile to each policy rule for which you want to forward logs.

1. Select **Objects > Log Forwarding**.
2. Select the **Device Group** in which you added the policy rules, for example, **Remote\_Network\_Device\_Group**.
3. **Add** a Log Forwarding profile. In the log forwarding profile match list, **Add** each **Log Type** that you want to forward.
4. Select **Panorama/Cortex Data Lake** as the Forward Method to enable Prisma Access to forward the logs to Cortex Data Lake. You will be able to monitor the logs and generate reports from Panorama.

Cortex Data Lake provides a seamless integration to store logs without backhauling them to your Panorama at the corporate headquarters, and Panorama can query Cortex Data Lake as needed.

The following example enables forwarding of Traffic, Threat Prevention, WildFire Submission, URL Filtering, Data Filtering, and Authentication logs to Cortex Data Lake.

The screenshot shows the Panorama web interface with the 'OBJECTS' tab selected. A table lists log forwarding configurations for a policy rule named 'remote-network-log-forwarding'. The table has columns for 'CONNECTION NAME', 'LOCATION', 'ENABLE ENHANCED LOGGING', 'DESCRIPTION', 'LOG TYPE', 'FILTER', 'PANORAMA/CORTEX DATA LAKE', and 'QUARANTINE'. The 'remote-network-log-forwarding' rule is selected, and its log types (traffic, threat, wildfire, url, traffic, auth) are all configured to forward logs to Cortex Data Lake.

CONNECTION NAME	LOCATION	ENABLE ENHANCED LOGGING	DESCRIPTION	LOG TYPE	FILTER	PANORAMA/CORTEX DATA LAKE	QUARANTINE
<input checked="" type="checkbox"/>	remote-network-log-forwarding	Remote_Network_Device...		traffic	All Logs	<input checked="" type="checkbox"/>	<input type="checkbox"/>
				threat	All Logs	<input checked="" type="checkbox"/>	<input type="checkbox"/>
				wildfire	All Logs	<input checked="" type="checkbox"/>	<input type="checkbox"/>
				url	All Logs	<input checked="" type="checkbox"/>	<input type="checkbox"/>
				traffic	All Logs	<input checked="" type="checkbox"/>	<input type="checkbox"/>
				auth	All Logs	<input checked="" type="checkbox"/>	<input type="checkbox"/>

5. Select **Policies > Security** and edit the policy rule. In **Actions**, select the Log Forwarding profile you created.

**STEP 18 |** Commit all your changes to Panorama and push the configuration changes to Prisma Access.

1. Click **Commit > Commit to Panorama**.
2. Click **Commit > Push to Devices** and click **Edit Selections**.
3. On the **Prisma Access** tab, make sure **Prisma Access for networks** is selected and then click **OK**.
4. Click **Push**.

## Configure Prisma Access for Networks Allocating Bandwidth by Location

If you have deployed remote networks using the Cloud Services plugin 1.7 or earlier, you can continue to allocate bandwidth by location by completing the following steps.

Before you begin onboarding your remote networks, be sure you go through the steps to [Plan to Deploy Remote Networks](#).

If you need to onboard many remote network locations, onboard a remote network using this workflow and then [import the remote network configuration](#).

**STEP 1 |** Select **Panorama > Cloud Services > Configuration > Remote Networks** and edit the settings by clicking the gear icon in the **Settings** area.

1. In the Templates section, **Add** any templates that contain configuration you want to push to Prisma Access for networks. For example, if you have existing templates that contain your zone configurations, or IPSec tunnel, IKE Gateway, or crypto profile settings, you can add them to the predefined Remote\_Network\_Template\_Stack to simplify the onboarding process.

You can **Add** more than one template to the stack and then order them appropriately using **Move Up** and **Move Down**. This is important because Panorama evaluates in the stack from top to bottom, with settings in templates higher in the stack taking priority over the same settings specified in templates lower in the stack. Note that you cannot move the default template from the top of the stack.



*Although you can add existing templates to the stack from the plugin, you cannot create a new template from the plugin. Instead, use the workflow to [add a new template](#).*

2. Select the **Parent Device Group** for Prisma Access for remote networks. You can select an existing device group or use **Shared**.

You will push all of the configuration—including the [security policy](#), [security profiles](#), and other policy objects (such as application groups and objects, and address groups), [HIP objects and profiles](#) and [authentication policy](#)—that Prisma Access for networks needs to enforce consistent policy to your remote network users using the [device group hierarchy](#) you specify here.



*You don't need to define all of the policy that you will push to the remote network yet. Instead, configure the settings to onboard the remote site. You can then go back and add the templates and device groups with the complete configurations to push consistent policy out to your remote networks.*

3. (Optional) If you have configured an on-premises next-generation firewall as a [master device](#), select the **Master Device** you configured.

When you select the **Master Device**, Prisma Access auto-populates user and group information in the security policy rules in Panorama for mobile user and remote network device groups.

4. If you will be configuring remote networks that have overlapping subnets, select the **Overlapped Subnets** check box to enable outbound internet access for those locations.

While configuring [Remote Network Locations with Overlapping Subnets](#) introduces some limitations, it is acceptable in some cases (for example, if you want to add a guest network at a retail store location).

The screenshot shows the 'Settings' window with the 'Group Mapping Settings' tab selected. Under 'Template Stack', the 'Template Stack Name' is 'Remote\_Network\_Template\_Stack'. Below it, a table lists templates, with 'Remote\_Network\_Template' selected. At the bottom of the table are buttons for 'Add', 'Delete', 'Move Up', and 'Move Down'. A note states: 'The template at the top of the stack has the highest priority in the presence of overlapping config'. In the 'Device Group' section, 'Device Group Name' is 'Remote\_Network\_Device\_Group' and 'Parent Device Group' is 'Shared'. In the 'Overlapped Subnets' section, the 'Overlapped Subnets' checkbox is unchecked. A note below it reads: 'Enabling Overlapped Subnets allows outbound internet to be supported for remote networks with overlapping subnets that are configured in the same region.' At the bottom right are 'OK' and 'Cancel' buttons.

## STEP 2 | (Optional) Configure **DNS Proxy** settings for your remote network.

Prisma Access allows you to [specify DNS servers](#) to resolve both domains that are internal to your organization and external domains. If you do not specify any settings, Prisma Access does not proxy DNS requests for remote networks.

1. In the **Remote\_Network\_Device\_Group** device group, select **Policies > Security** and **Add** a security policy rule with an **Application** of **DNS** and an **Action** of **Allow** to allow DNS traffic.

Without a security policy rule to allow DNS traffic, DNS resolution does not occur.

	NAME	LOCATION	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION
					ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE			
1	dns-traffic-rule	Remote_Networ...	none	universal	Trust	any	any	any	any	any	any	dns	any	Allow

- If you configure Prisma Access to **proxy the DNS requests** from your remote networks, update the DNS settings on all the endpoints in that network to use the Prisma Access **Remote Network DNS Proxy IP Address** as the primary DNS server and use your DNS server as secondary DNS server. You can get this DNS proxy IP from **Panorama > Cloud Services > Status > Network Details > Service Infrastructure**.

Infrastructure Subnet	Infrastructure BGP AS	Captive Portal Redirect IP Address	Tunnel Monitor IP Address	Loopback IPs	Remote Network DNS Proxy IP Address
172.3.0.0/16	65534	172.3.255.254	172.3.255.254	172.3.0.11 172.3.0.18 172.3.0.11 172.3.0.18 172.3.0.11 172.3.0.18	172.3.255.254

- Add one or more DNS proxy settings, entering the following values:

- For **Internal Domains**:

- Select a **Region (North America & South America, Africa, Europe & Middle East, or Asia, Australia & Japan)**, or specify **Worldwide** to apply the DNS settings globally.

You can add multiple region-specific DNS proxy settings, or specify a DNS proxy for one or more regions and specify another worldwide DNS proxy for the rest of the world. If you specify only a regional setting and onboard remote networks in that region only, Prisma Access does not proxy the DNS requests, and the source IP address of the DNS request is the remote network's **EBGP Router IP address**. If you specify multiple proxy settings with a mix of regional and worldwide regions, Prisma Access uses the regional settings for the Locations in the region you specify; otherwise, Prisma Access uses the worldwide settings.

- Specify the IP addresses of the **Primary DNS** and **Secondary DNS** servers that your remote network should use to resolve internal domains.
- (Optional) If you want your internal DNS server to only resolve the domains you specify, enter the domains to resolve in the **Domain List**.

You can use a wildcard (\*) in front of the domains in the domain list, for example \*.acme.local or .acme.com. You can specify a maximum of 1,024 domain entries.

- For **External Domains**:

- Enter a **Primary DNS** choice.

To use the default Prisma Access DNS server, select **Use Cloud Default**. To use the same server that you use to resolve internal domains, select **Same as Internal Domains**. To use third-party or public DNS server, select **Custom DNS Server**, then specify the IP address of the DNS server.

- Enter a **Secondary DNS** choice, choosing from the same options you chose for the **Prisma DNS**.

Settings
?

Settings | DNS Proxy | Group Mapping Settings

1 item → ×

REGION	Internal Domains				Public Domains		
	RULE NAME	PRIMARY DNS	SECONDARY DNS	DOMAIN LIST	PRIMARY DNS	SECONDARY DNS	
<input checked="" type="checkbox"/>	worldwide	Default	10.3.88.120	.8	*.acme.local acme.local *.acme.com	.8	.4

+ Add
⊖ Delete

Configure this only if you want Prisma Access to proxy the DNS requests. You must update your endpoints to use the Prisma Access DNS Proxy IP Address as the primary DNS server. For a domain entry in the Internal Domains list, enter as \*.<domain>. For example \*.acme.com.

**UDP Queries Retries**

Interval (Sec)

Attempts

OK
Cancel

**STEP 3 |** (Optional) Configure Prisma Access to use the Directory Sync service to retrieve user and group information.

You must [configure Directory Sync](#) to retrieve user and group information from your Active Directory (AD) before you enable and configure Directory Sync integration in Prisma Access using the settings in the **Group Mapping Settings** tab. See [Get User and Group Information Using Directory Sync](#) for details.

**STEP 4 |** Create new zones in the one of the templates in the stack (**Network > Zones > Add**) or [map the zones](#) referenced in existing templates you added to the stack as trusted or untrusted. On Panorama, policy rules are defined in device groups, and zones are defined in templates. Therefore, you need to make sure that you add the templates that reference the zones included in your policy rules to the template stack.

On a Palo Alto Networks® next-generation firewall, security policy is enforced between zones, which map to physical or virtual interfaces on the firewall. But as Prisma Access for networks has only two zones, trust and untrust, you need to map any zone with traffic bound to the Internet (including your sanctioned SaaS applications) as untrust and all internal zones as trust.


1. (Optional) Edit the [zone mapping](#) settings.

By default, all of the zones in Prisma Access for networks template stack a are classified as Untrusted Zones. If you have not yet defined zones or if the templates in the Remote\_Network\_Template\_Stack do not have zone configurations, you can come back and add them when you push policy to Prisma Access for networks.

2. For each zone you want to designate as trusted, select it and click **Add** to move it to the list of **Trusted Zones**.

3. Click **OK** to save the mappings.

**STEP 5 |** Click **Add** in the Onboarding settings, and specify a **Name** to identify the infrastructure that will secure the remote network location you are onboarding.

 *You cannot change the name of the remote network location after you enter it. Make sure you know your naming scheme for your remote networks before you begin onboarding.*



**STEP 6 | (BGP deployments only)** Create a configuration so that your remote network connection can use up to four IPsec tunnels for its traffic (**ECMP Load Balancing**).

QoS is not supported with ECMP load balancing, and static routes are not supported (BGP is required). If your deployment uses one IPsec tunnel for its remote network connection or uses static routes, select **None** for **ECMP Load Balancing** and continue to Step 9.

Specify a minimum **Bandwidth** of **50 Mbps**.

Prisma Access divides the bandwidth you select by the number of tunnels; for example, if you specify 300 Mbps and add four tunnels, each tunnel carries 75 Mbps. If one of the tunnels goes down, your network connection will now carry 225 Mbps instead of 300 Mbps.

1. Select one of the choices to enable or disable ECMP load balancing.

- **None**—Do not use ECMP load balancing (use a single remote network tunnel for this remote network connection). This is the only choice you can make for static routes; BGP is required for ECMP load balancing.
- **Enabled with Symmetric Return**—Specify up to four IPsec tunnels for this remote network connection and force Prisma Access to use the same link for the return traffic as it used to send the traffic.


Select this option if you use one or more tunnels as a backup tunnel to be used only if one of the primary tunnels go down. If a link fails, Prisma Access uses one of the other tunnels to send and receive traffic symmetrically.

The screenshot shows the 'Onboarding' configuration window. The 'Name' field is 'ECMP-IRE-RN'. The 'ECMP Load Balancing' dropdown is set to 'Enabled with Symmetric Return'. The 'Location' dropdown is set to 'Ireland'. The 'Bandwidth' dropdown is set to '50 Mbps'. Below these fields is a table with two columns: 'IPSec Tunnel' and 'BGP'. The table is currently empty. At the bottom left of the table area are '+ Add' and '- Delete' buttons. At the bottom right of the window are 'OK' and 'Cancel' buttons.

2. **Add** an IPsec tunnel for the remote network connection and specify the following values:


- **Enable**—Enables BGP for the IPsec tunnel.  
This selection is not configurable; you must enable BGP to configure ECMP.
- **Summarize Mobile User Routes before advertising**—Reduces the number of mobile user IP subnet advertisements over BGP to your customer premises equipment (CPE) by summarizing them.

By default, Prisma Access advertises the mobile users IP address pools [in blocks of /24 subnets](#); if you summarize them, Prisma Access advertises the pool based on the subnet you specified. For example, Prisma Access advertises a public user mobile IP pool of 10.8.0.0/20 using the /20 subnet, rather than dividing the pool into subnets of 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24, and so on before advertising them. Summarizing these advertisements can reduce the number of routes stored in CPE routing tables. For example, you can use IP pool summarization with cloud VPN gateways (Virtual Private Gateways (VGWs) or Transit Gateways (TGWs)) that can accept a limited number of routes.

 *If you enable route summarization for a location that uses ECMP, you must enable route summarization on all links to that location, or you will receive an error during commit.*

Prisma Access sets the community string for aggregated mobile user routes to 0xFFFFE:0xFFF0.

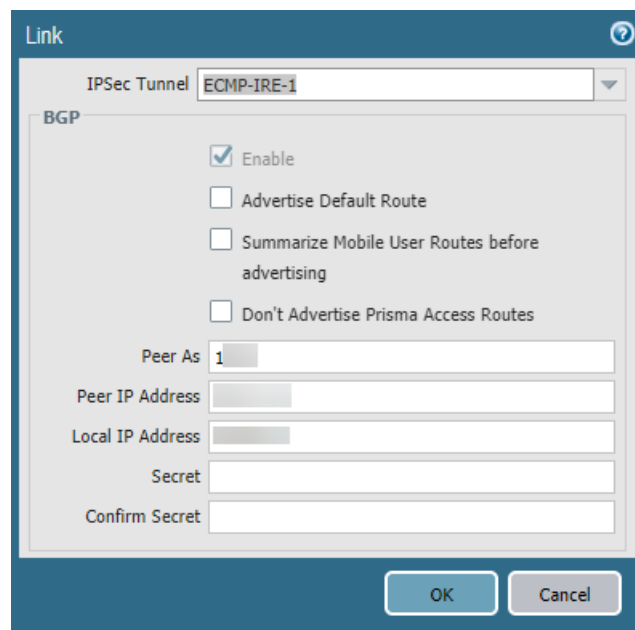
- **Advertise Default Route**—Allows Prisma Access to advertise a default route for the remote network using eBGP.

 *You must publish your default routes before you make this selection to advertise them. In addition, be sure that your network does not have another default route being advertised by BGP, or you could introduce routing issues in your network.*

- **Don't Advertise Prisma Access Routes**—Prevents the Prisma Access BGP peer from forwarding routes into your organization's network.

By default, Prisma Access advertises all BGP routing information, including local routes and all prefixes it receives from other service connections, remote networks, and mobile user subnets. Select this check box to prevent Prisma Access from sending any BGP advertisements, but still use the BGP information it receives to learn routes from other BGP neighbors.

Since Prisma Access does not send BGP advertisements if you select this option, you must configure static routes on the on-premises equipment to establish routes back to Prisma Access.



- **Peer AS**—Specify the autonomous system (AS) to which the firewall, virtual router, or BGP router at your remote network belongs.
- **Peer IP Address**—Enter the IP address assigned as the Router ID of the eBGP router on the remote network for which you are configuring this connection.

- **Local IP Address (Optional)**—Enter an address that Prisma Access uses as its Local IP address for BGP. Specify the IP address to use on the Prisma Access side of the tunnel.

Specifying a **Local Address** is useful where the device on the other side of the connection (such as an Amazon Web Service (AWS) Virtual Private Gateway) requires a specific local IP address for BGP peering to be successful. Make sure that the address you specify does not conflict or overlap with IP addresses in the Infrastructure Subnet or subnets in the remote network.

- **Secret and Confirm Secret (Optional)**—Enter and confirm a passphrase to authenticate BGP peer communications.
3. Repeat the previous step to add up to four tunnels to use with the remote network connection.

IPSec Tunnel	BGP
<input type="checkbox"/> ECMP-IRE-1	yes
<input type="checkbox"/> ECMP-IRE-2	yes
<input type="checkbox"/> ECMP-IRE3	yes
<input type="checkbox"/> ECMP-IRE4	yes

**STEP 7 |** Select the **Location** in which Prisma Access will deploy the infrastructure required to secure your remote network location. This region should be geographically located close to your remote network location.

See [this table](#) for a list of Prisma Access locations.

**STEP 8 |** Select the **Bandwidth** you want to allocate to this remote network location. The bandwidth you select cannot exceed the total amount of bandwidth you have licensed. Use this setting to define the amount of the total licensed bandwidth you want to allocate to this location.

To help you determine how much bandwidth a specific site needs, consider the bandwidth available from your ISP at each location. See [How to Calculate Remote Network Bandwidth](#) for more details and suggestions. If you enable **ECMP Load Balancing**, you must specify a minimum of 50 Mbps.



*You can change the bandwidth of a remote network connection after you onboard it, with the exception of the 500 Mbps (w/o SSL Decryption) or 1000 Mbps (Preview) bandwidth choices. If you select either of these preview choices and then need to change the bandwidth, you must first add an identical network with the only change being the lower, non-Preview bandwidth choice, commit your changes, make a note of the Service IP address and reconfigure your IPsec tunnel to use that address, then delete the existing remote network with the preview bandwidth choice.*

**STEP 9 |** (**Static routing or single-tunnel deployments only**) Select or add a new **IPSec Tunnel** configuration to access the firewall, router, or SD-WAN device at the corporate location:

- 
- If you have added a template to the Remote\_Network\_Template\_Stack (or modified the predefined Remote\_Network\_Template) that includes an IPSec Tunnel configuration, select that **IPSec Tunnel** from the drop-down. Note that the tunnel you are creating for each remote network connection connects Prisma Access to the IPSec-capable device at each branch location.

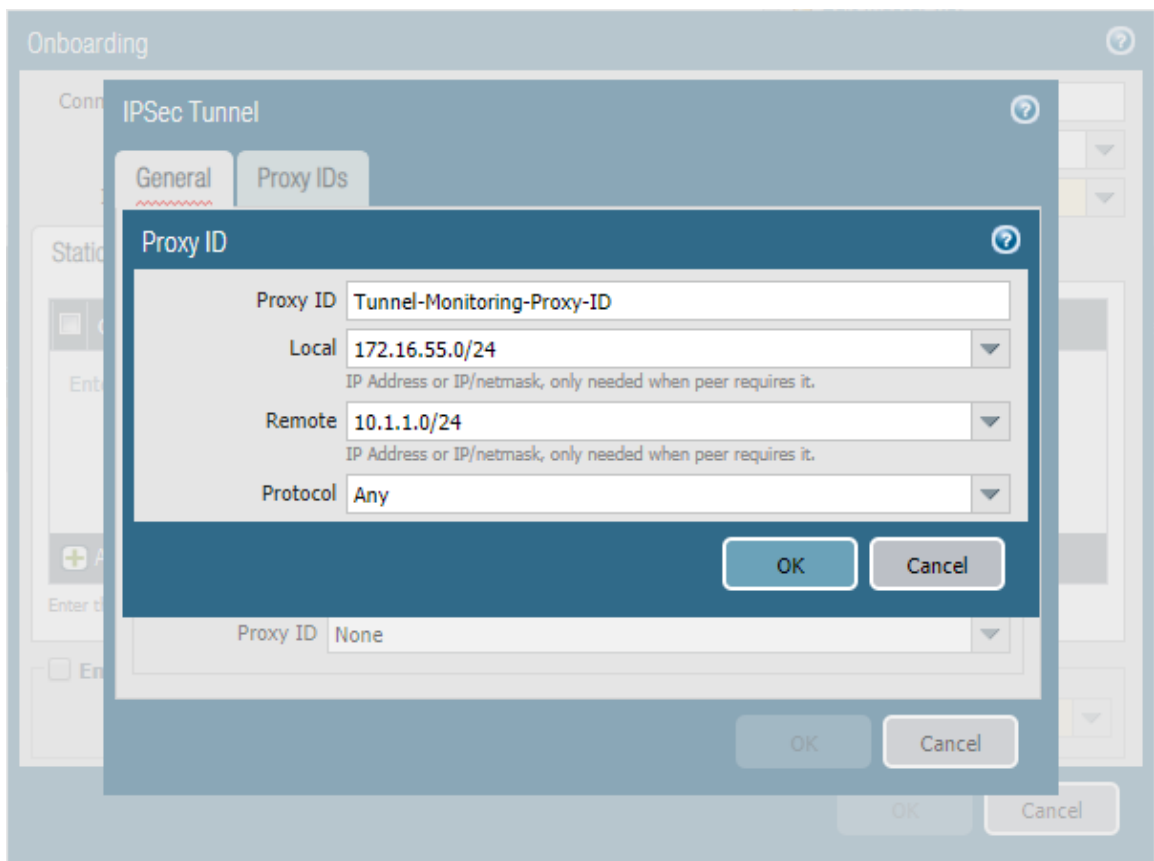
User the following guidelines when configuring an IPSec tunnel:

- The peer addresses in the IKE Gateway configuration must be unique for each tunnel. You can, however, re-use some of the other common configuration elements, such as crypto profiles.
- The IPSec Tunnel you select from a template must use Auto Key exchange and IPv4 only.
- If you onboard multiple remote networks to the same location with dynamic IKE peers, you must use the same IKE crypto profile for all remote network configurations.
- To [create a new IPSec Tunnel](#) configuration, click **New IPSec Tunnel**, give it a **Name** and configure the [IKE Gateway](#), [IPSec Crypto Profile](#), and [Tunnel Monitoring](#) settings.
  - If the IPSec-capable device at your branch location uses policy-based VPN, on the **Proxy IDs** tab, **Add** a proxy ID that matches the settings configured on your local IPSec device to ensure that Prisma Access can successfully establish an IPSec tunnel with your local device.
  - Leave **Enable Replay Protection** selected to detect and neutralize against replay attacks.
  - Select **Copy TOS Header** to copy the Type of Service (TOS) header from the inner IP header to the outer IP header of the encapsulated packets in order to preserve the original TOS information.
  - To enable tunnel monitoring for the service connection, select **Tunnel Monitor**.
    - Enter a **Destination IP** address.

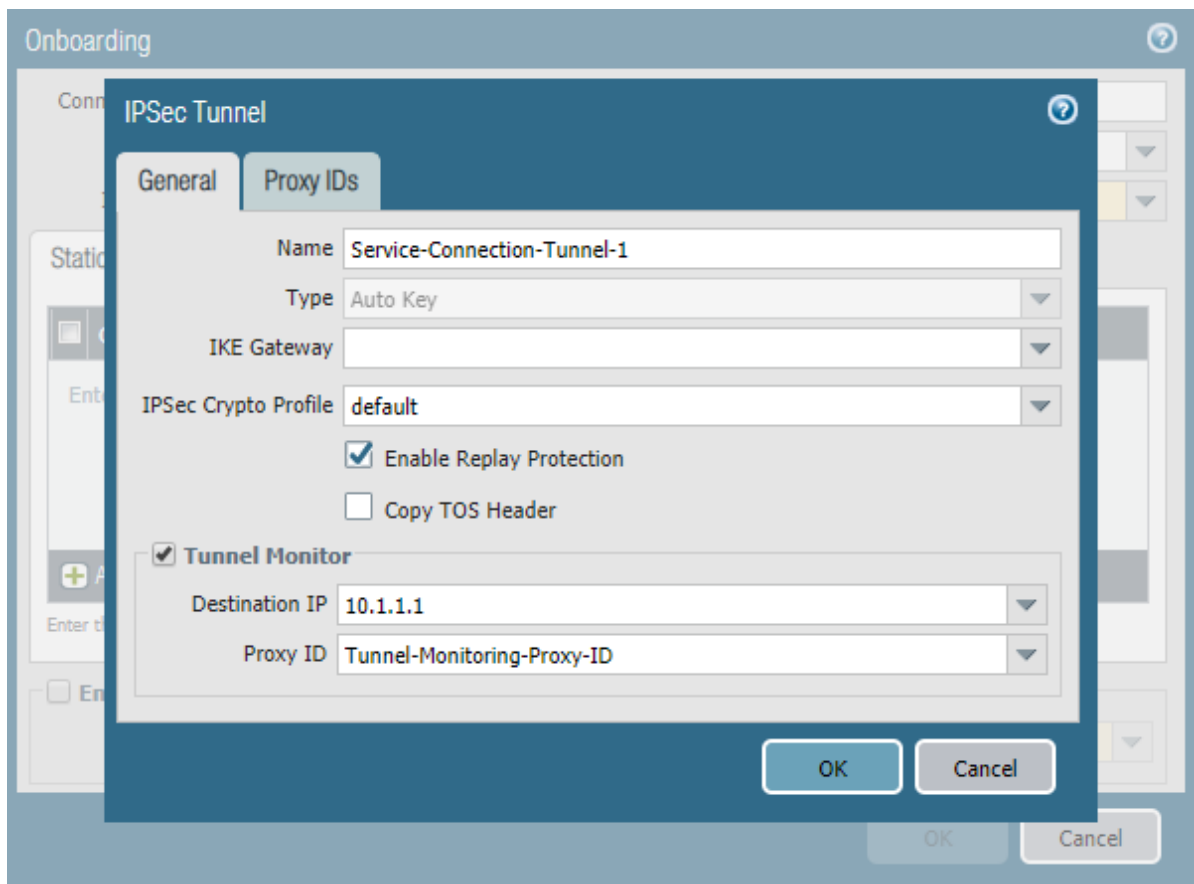
Specify an IP address at your branch location to which Prisma Access can send ICMP ping requests for IPSec tunnel monitoring. Make sure that this address is reachable by ICMP from the entire Prisma Access infrastructure subnet.


- If you use tunnel monitoring with a peer device that uses multiple proxy IDs, specify a **Proxy ID** or add a **New Proxy ID** that allows access from the infrastructure subnet to your branch location.

The following figure shows a proxy ID with the service infrastructure subnet (172.16.55.0/24 in this example) as the **Local** IP subnet and the branch location's subnet (10.1.1.0/24 in this example) as the **Remote** subnet.




The following figure shows the Proxy ID you created being applied to the tunnel monitor configuration by specifying it in the **Proxy ID** field.



 You must configure a static route on your CPE to the Tunnel Monitor IP Address for tunnel monitoring to function. To find the destination IP address to use for tunnel monitoring from your branch location to Prisma Access, select **Panorama > Cloud Services > Status > Network Details**, click the **Service Infrastructure** radio button, and find the **Tunnel Monitor IP Address**.

**STEP 10** | If you have a secondary WAN link at this location, select **Enable Secondary WAN**.

 Be sure to create a unique IPsec tunnel for each remote network's secondary WAN; Prisma Access does not support reusing the same IPsec tunnel for secondary WANs in multiple remote networks.

If you use static routes, tunnel failover time is less than 15 seconds from the time of detection, depending on your WAN provider.

If you configure BGP routing and have enabled tunnel monitoring, the shortest default hold time to determine that a security parameter index (SPI) is failing is the tunnel monitor, which removes all routes to a peer when it detects a tunnel failure for 15 consecutive seconds. In this way, the tunnel monitor determines the behavior of the BGP routes. If you do not configure tunnel monitoring, the hold timer determines the amount of time that the tunnel is down before removing the route. Prisma Access uses the default BGP HoldTime value of 90 seconds as defined by RFC 4271, which is the maximum wait time before Prisma Access removes a route for an inactive SPI. If the peer BGP device has a shorter configured hold time, the BGP hold timer uses the lower value.

When the secondary tunnel is successfully installed, the secondary route takes precedence until the primary tunnel comes back up. If the primary and secondary are both up, the primary route takes priority.



If you use a different BGP peer for the secondary (backup) connection, Prisma Access does not honor the Multi-Exit Discriminator (MED) attributes advertised by the CPE. This caveat applies if you use multiple BGP peers on either remote network connections or service connections.

**STEP 11** | Enable routing to the subnetworks or individual IP addresses at the remote network site that your users will need access to.

Prisma Access uses this information to route requests to the appropriate site. The networks at each site cannot overlap with each other or with IP address pools that you designated for the service infrastructure or for the Prisma Access for users IP pools. You can configure **Static Routes**, **BGP**, or a combination of both.

- To configure **Static Routes**:
  1. On the **Static Routes** tab, click **Add** and enter the subnetwork address (for example, 172.168.10.0/24) or individual IP address of a resource, such as a DNS server (for example, 10.32.5.1/32) that your remote users will need access to.
  2. Repeat for all subnets or IP addresses that Prisma Access will need access to at this location.

The screenshot shows the 'Onboarding' configuration window for a remote network site. The 'Name' field is set to 'HQ1-US-West'. Other fields include 'ECMP Load Balancing' (None), 'Location' (US West), 'Bandwidth' (25 Mbps), and 'IPSec Tunnel' (HQ1-US-West-IPsec-Tunnel). There is an unchecked checkbox for 'Enable Secondary WAN' with an empty 'IPSec Tunnel' dropdown below it. The 'Static Routes' tab is selected, showing a table with one row checked. Below the table are 'Add' and 'Delete' buttons. A note at the bottom says 'Enter the subnets for your remote networks.' 'OK' and 'Cancel' buttons are at the bottom right.

- To configure **BGP**:
  1. Select the **BGP** tab.
  2. Select the **ECMP Load Balancing** choices. See Step 6.

3. If you select **None** for **ECMP Load Balancing**, enter the BGP choices.

The screenshot shows the 'Onboarding' configuration window for BGP. The 'Name' field is 'HQ1-US-West-BGP'. 'ECMP Load Balancing' is set to 'None'. 'Location' is 'US West', 'Bandwidth' is '25 Mbps', and 'IPsec Tunnel' is 'Generic-IPsec-Tunnel-Default'. The 'Enable Secondary WAN' checkbox is checked, and its 'IPsec Tunnel' is 'CloudGenix-IPsec-Tunnel-Default'. The 'BGP' tab is selected, showing the 'Enable' checkbox checked. Below it are three unchecked checkboxes: 'Summarize Mobile User Routes before advertising', 'Advertise Default Route', and 'Don't Advertise Prisma Access Routes'. The 'Primary WAN' section has 'Peer AS' set to '65524' and empty fields for 'Peer Address', 'Local Address', 'Secret', and 'Confirm Secret'. The 'Secondary WAN' section has 'Same as Primary WAN' checked and 'Peer AS' set to '65524', with empty fields for 'Peer Address', 'Local Address', 'Secret', and 'Confirm Secret'. 'OK' and 'Cancel' buttons are at the bottom right.

4. To enable BGP for the remote network connection, select **Enable**.

When you enable BGP, Prisma Access sets the time to life (TTL) value for external BGP (eBGP) to 8 to accommodate any extra hops that might occur between the Prisma Access infrastructure and your customer premises equipment (CPE) that terminates the eBGP connection.

5. To reduce the number of mobile user IP subnet advertisements over BGP to your customer premises equipment (CPE) by summarizing them, select **Summarize Mobile User Routes before advertising**.

By default, Prisma Access advertises the mobile users IP address pools [in blocks of /24 subnets](#); if you summarize them, Prisma Access advertises the pool based on the subnet you specified. For example, Prisma Access advertises a public user mobile IP pool of 10.8.0.0/20 using the /20 subnet, rather than dividing the pool into subnets of 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24, and so on before advertising them. Summarizing these advertisements can reduce the number of routes stored in CPE routing tables. For example, you can use IP pool summarization with cloud VPN gateways (Virtual Private Gateways (VGWs) or Transit Gateways (TGWs)) that can accept a limited number of routes.

Prisma Access sets the community string for aggregated mobile user routes to 0xFFFFE:0xFFFF0.

6. To allow Prisma Access to advertise a default route for the remote network using eBGP, select **Advertise Default Route**.

If you select **Advertise Default Route**, be sure that your network does not have another default route being advertised by BGP, or you could introduce routing issues in your network.





*You must publish your default routes before you make this selection to advertise them. In addition, be sure that your network does not have another default route being advertised by BGP, or you could introduce routing issues in your network.*

7. To prevent the BGP peer on the Prisma Access firewall from forwarding routes into your organization's network, select **Don't Advertise Prisma Access Routes**.

By default, Prisma Access advertises all BGP routing information, including local routes and all prefixes it receives from other service connections, remote networks, and mobile user subnets. Select this check box to prevent Prisma Access from sending any BGP advertisements, but still use the BGP information it receives to learn routes from other BGP neighbors.

Since Prisma Access does not send BGP advertisements if you select this option, you must configure static routes on the on-premises equipment to establish routes back to Prisma Access.

8. Enter the **Peer AS**, which is the autonomous system (AS) to which the firewall, virtual router, or BGP router at your remote network belongs.
9. Enter the IP address assigned as the Router ID of the eBGP router on the remote network for which you are configuring this connection as the **Peer Address**.
10. (Optional) Enter an address that Prisma Access uses as its Local IP address for BGP.

Specifying a **Local Address** is useful where the device on the other side of the connection (such as an Amazon Web Service (AWS) Virtual Private Gateway) requires a specific local IP address for BGP peering to be successful. Make sure that the address you specify does not conflict or overlap with IP addresses in the Infrastructure Subnet or subnets in the remote network.



*You must configure a static route on your CPE to the BGP Local Address.*

11. (Optional) Enter and confirm a passphrase to authenticate BGP peer communications.
12. (Optional) If you configured a **Secondary WAN** and you need to change the **Peer Address** or **Local Address** for the secondary (backup) BGP peer, deselect **Same as Primary WAN** and enter a unique Peer and, optionally, Local IP address for the secondary WAN.

In some deployments (for example, when using BGP to peer with an [AWS VPN gateway](#)), the BGP peer for the primary and secondary WAN might be different. In those scenarios, you can choose to set a different BGP peer for the secondary WAN.



*For BGP deployments with secondary WANs, Prisma Access sets both the primary and secondary tunnels in an UP state, but follows normal BGP active-backup behavior for network traffic. Prisma Access sets the primary tunnel as active and sends and receives traffic through that tunnel only; if the primary tunnel fails, Prisma Access detects the failure using BGP rules, sets the secondary tunnel as active, and uses only the secondary tunnel to send and receive traffic.*

**STEP 12** | If required, enable **Quality of Service** for the remote network connection and specify a [QoS profile](#) or add a **New QoS Profile**.

You can create QoS profiles to shape QoS traffic for remote network and service connections and apply those profiles to traffic that you marked with PAN-OS security policies, traffic that you marked with an on-premises device, or both PAN-OS-marked and on-premise-marked traffic. See [Configure Quality of Service in Prisma Access](#) for details.

**STEP 13** | Commit the configuration changes to Panorama and push the configuration out to Prisma Access for networks.

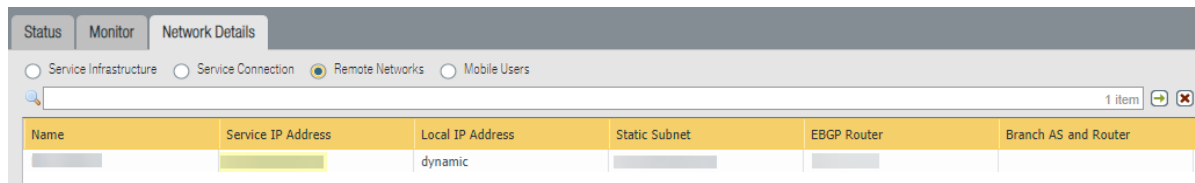
1. Click **Commit** > **Commit to Panorama**.
2. Click **Commit** > **Commit and Push**. Click **Edit Selections** > **Prisma Access**, and select both Prisma Access for networks and Prisma Access for service setup to push the configuration out to the service.

3. Click **OK** and **Push**.

**STEP 14** | Configure the IPSec-capable device at the remote network location to set up an IPSec connection with Prisma Access for networks.

1. Find the **Service IP Address** for this remote network connection by selecting **Panorama** > **Cloud Services** > **Status** > **Network Details**, clicking the **Remote Networks** radio button, and viewing the

**Service IP Address** field. Prisma Access for networks infrastructure has assigned this IP address for the Prisma Access remote network connection, and you must configure this as the peer IP address to set up the IPSec tunnel between the remote network location and Prisma Access for networks.



2. Check the **Local IP address** for the device at the remote network location on the **Panorama > Cloud Services > Status > Network Details > Remote Networks** page. If you are performing NAT at the remote network location, the **Local IP address** displays the IP address of the device after NAT.

**STEP 15** | To secure traffic at the remote network location you must create security policy rules.

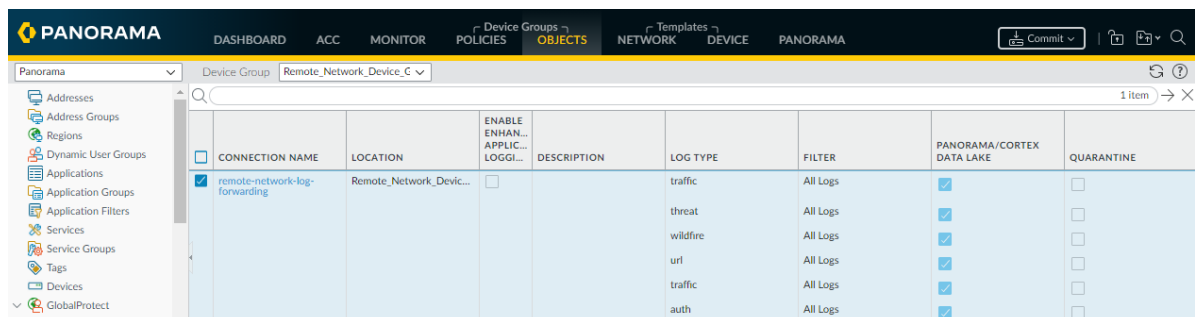
1. Select **Policies**.
2. Select the **Device Group** in which to add policy rules. You can select the Remote\_Network\_Device\_Group or the parent device group that you selected for defining policies to secure the remote network location.
3. **Create security policy rules**. Make sure that you do not define security policy rules to allow traffic from any zone to any zone. In the security policy rules, use the zones that you defined in your template.

If a user on your network is denied access to a website, [report website access issues](#) before you open a ticket with Palo Alto Networks.

**STEP 16** | Enable logging to Cortex Data Lake. You must create and attach a log forwarding profile to each policy rule for which you want to forward logs.

1. Select **Objects > Log Forwarding**.
2. Select the **Device Group** in which you added the policy rules, for example, Remote\_Network\_Device\_Group.
3. **Add** a Log Forwarding profile. In the log forwarding profile match list, **Add each Log Type** that you want to forward.
4. Select **Panorama/Cortex Data Lake** as the Forward Method to enable Prisma Access to forward the logs to Cortex Data Lake. You will be able to monitor the logs and generate reports from Panorama. Cortex Data Lake provides a seamless integration to store logs without backhauling them to your Panorama at the corporate headquarters, and Panorama can query Cortex Data Lake as needed.

The following example enables forwarding of Traffic, Threat Prevention, WildFire Submission, URL Filtering, Data Filtering, and Authentication logs to Cortex Data Lake.



5. Select **Policies > Security** and edit the policy rule. In **Actions**, select the Log Forwarding profile you created.

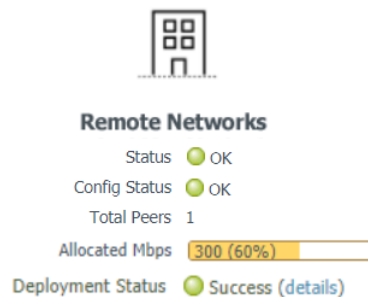
**STEP 17** | Commit all your changes to Panorama and push the configuration changes to Prisma Access.

1. Click **Commit > Commit to Panorama**.
2. Click **Commit > Push to Devices** and click **Edit Selections**.
3. On the **Prisma Access** tab, make sure **Prisma Access for networks** is selected and then click **OK**.
4. Click **Push**.

## Verify Remote Network Connection Status

Select **Panorama > Cloud Services > Status > Status** to verify that the remote network connections have been successfully deployed.

The **Deployment Status** area allows you to view the progress of onboarding and deployment jobs before they complete, as well as see more information about the status of completed jobs. See [Deployment Progress and Status](#) for details.



To display a map that shows the locations of the remote networks in the regions you have selected, select **Panorama > Cloud Services > Status > Monitor** and click the **Remote Networks** tab.

Select a region to get more detail about that region.

Click the tabs below the map to see additional remote network statistics.

**Status** tab:

Asia locations

Site | Bandwidth Usage

Status: ● OK(257)  
Remote Networks: 257

Location	Remote Peer	IPSec Termination Node	ECMP	Config Status	BGP Status	Tunnel Status
Hong Kong	AB-708	hong-kong-clover	Disabled	<span style="color: green;">●</span> In sync	<span style="color: green;">●</span> Not Enabled	<span style="color: green;">●</span> OK
Hong Kong	AB-693	hong-kong-clover	Disabled	<span style="color: green;">●</span> In sync	<span style="color: green;">●</span> Not Enabled	<span style="color: green;">●</span> OK
Hong Kong	AB-697	hong-kong-clover	Disabled	<span style="color: green;">●</span> In sync	<span style="color: green;">●</span> Not Enabled	<span style="color: green;">●</span> OK
Hong Kong	AB-696	hong-kong-clover	Disabled	<span style="color: green;">●</span> In sync	<span style="color: green;">●</span> Not Enabled	<span style="color: green;">●</span> OK
Hong Kong	AB-567	hong-kong-clover	Disabled	<span style="color: green;">●</span> In sync	<span style="color: green;">●</span> Not Enabled	<span style="color: green;">●</span> OK
Hong Kong	AB-566	hong-kong-clover	Disabled	<span style="color: green;">●</span> In sync	<span style="color: green;">●</span> Not Enabled	<span style="color: green;">●</span> OK
Hong Kong	AB-565	hong-kong-clover	Disabled	<span style="color: green;">●</span> In sync	<span style="color: green;">●</span> Not Enabled	<span style="color: green;">●</span> OK

257 items

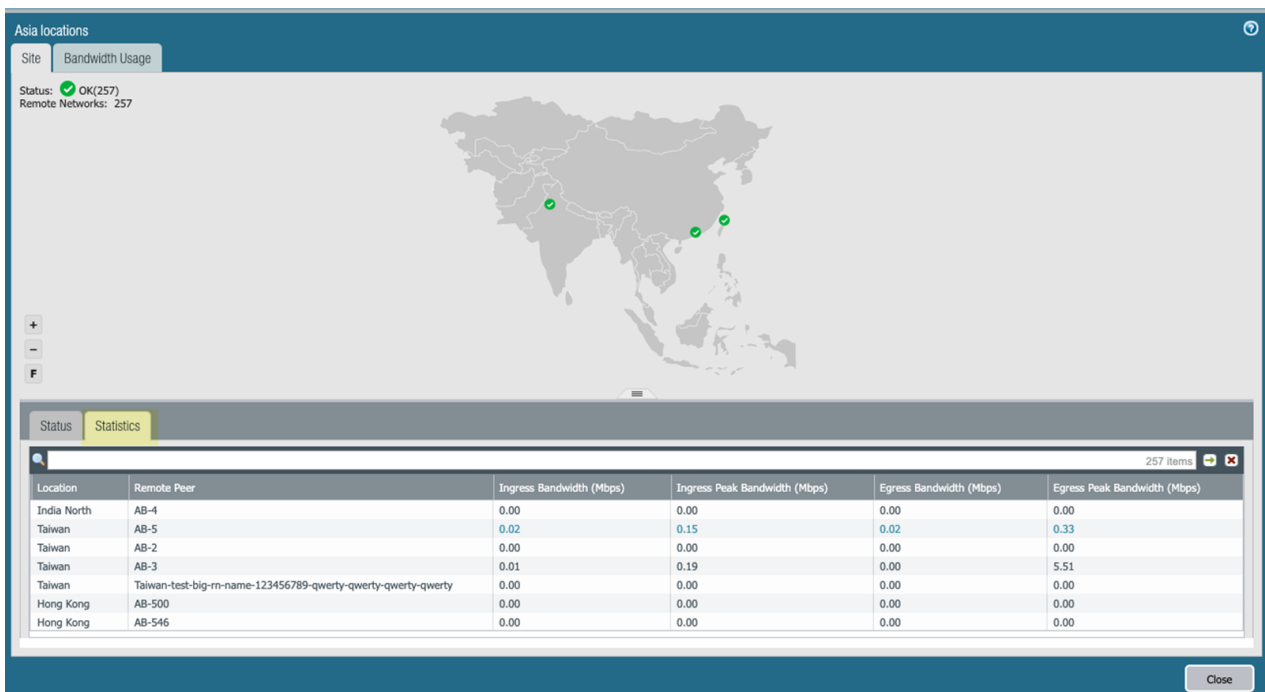
Close

- **Location**—The location where your remote network is deployed.
- **Remote Peer**—The peer to which the remote network has an IPsec tunnel connection.
- **IPsec Termination Node**—The IPsec termination node associated with the remote network.
- **ECMP**—Whether you have enabled **ECMP Load Balancing** on this remote network connection.
- **Config Status**—The status of your last configuration push to the service. If you have made a change locally, and not yet pushed the configuration to the cloud, the status shows **Out of sync**. Hover over the status indicator for more detailed information. After committing and pushing the configuration to Prisma Access, the Config Status changes to **In sync**.
- **BGP Status**—Displays information about the BGP state between the firewall or router at the remote network location and Prisma Access. Although you might temporarily see the status pass through the various BGP states (**idle**, **active**, **open send**, **open pend**, **open confirm**, most commonly, the BGP status shows:
  - **Connect**—The router at the remote network location is trying to establish the BGP peer relationship with Prisma Access.
  - **Established**—The BGP peer relationship has been established.

This field will also show if the BGP connection is in an error state:

  - **Warning**—There has not been a BGP status update in more than eight minutes. This may indicate an outage on the firewall.
  - **Error**—The BGP status is unknown.
- **Tunnel Status**—The operational status of the connection between Prisma Access and the remote network.

#### Statistics tab:



- **Location**—The location where your remote network is deployed.
- **Remote Peer**—The corporate location to which this remote network is setting up an IPsec tunnel.
- **Ingress Bandwidth (Mbps)**—The bandwidth from the remote network location to Prisma Access.



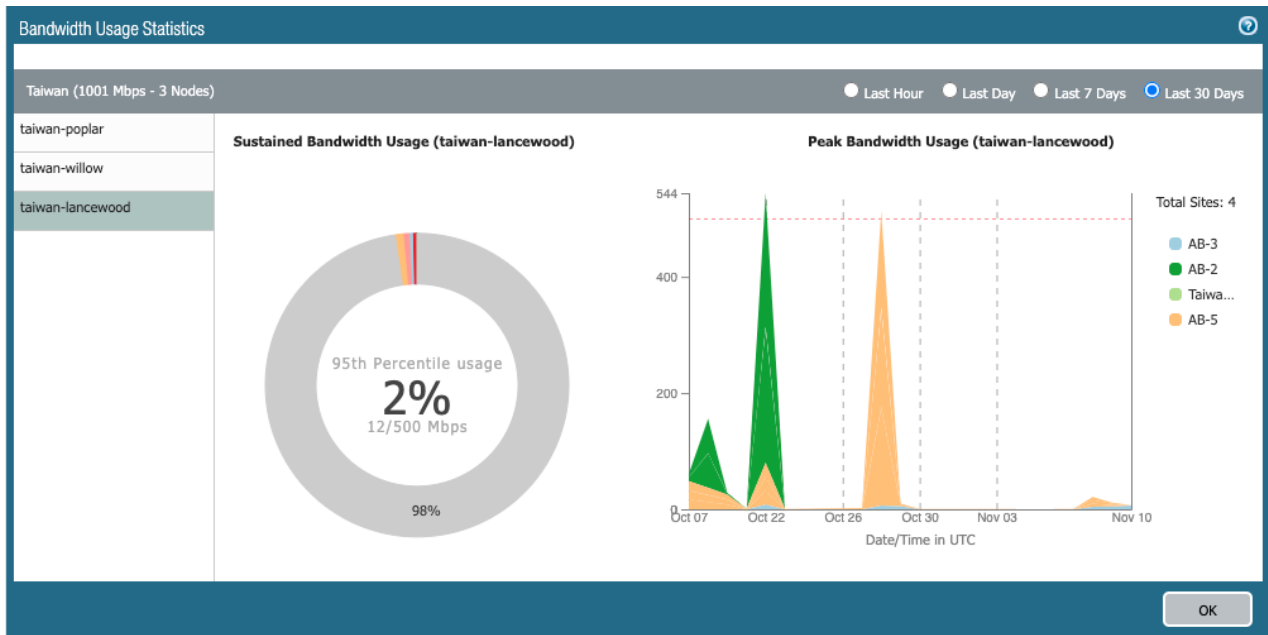
For the *Ingress Bandwidth*, *Ingress Peak Bandwidth*, *Egress Bandwidth*, and *Egress Peak Bandwidth* fields, when the bandwidth consumption on a remote network goes beyond 80% of the allocated bandwidth, the numbers display in a red color.

- **Ingress Peak Bandwidth (Mbps)**—The peak load from the remote network location into the cloud service.
- **Egress Bandwidth (Mbps)**—The bandwidth from Prisma Access into the remote network location.
- **Egress Peak Bandwidth (Mbps)**—The peak load from Prisma Access into the remote network location.

To find statistics about locations in the region, select **Bandwidth Usage**.



Select the check mark for a location to see detailed bandwidth usage. If there is more than one site in a region, select or deselect the region to view statistics for that region only (**Peak Bandwidth Usage** only).



## Verify Remote Connection BGP Status

If you configured BGP, you can check its status by selecting **Panorama > Cloud Services > Status > Network Details > Remote Networks > BGP Status**.

Status | Monitor | Network Details

Service Infrastructure 
  Service Connection 
  Remote Networks 
  Mobile Users 
  Clean Pipe

Q 3 items → ×

NAME	SERVICE IP ADDRESS	LOCAL IP ADDRESS	STATIC SUBNET	Secure Inbound Apps		EBGP ROUTER	BRANCH AS AND ROUTER
				APP NAME / PUBLIC ADDRESS / PRIVATE ADDRESS:PORT			
		dynamic					5   10.1.1.5   <a href="#">BGP Status</a>

The BGP Status dialog displays. This table provides you with the following information:

- **Peer**—Routing information for the BGP peer, including status, total number of routes, configuration, and runtime statistics and counters. The total number of routes display in the **bgpAfilpv4-unicast Counters** area, in the **Incoming Total** and **Outgoing Total** fields.



**BGP Status** ?

Refresh BGP Status  
Manual ▼

Refresh

**Peer** | Local RIB | RIB Out

Q 35 items → X

NAME	VALUE
▼ Status	
Name	AB-2
Group	
Local IP	172.16.30.1
Peer IP	10.1.1.5
Peer AS	5
Password Set	no
Status	Connect
Status Duration (secs.)	0
Community	
▼ Configuration	

- **Local RIB**—Routing information that has been received from different peers and is stored in the Routing Information Base (RIB).

**BGP Status** ?

Refresh BGP Status  
Manual ▼

Refresh

**Peer** | **Local RIB** | RIB Out

Q 0 items → X

PREFIX	FLAG	NEXT HOP	WEIGHT	LOCAL PREFERE...	AS PATH	ORIGIN	MED	FLAP COUNT

- **RIB Out**—Routing information that Prisma Access advertises to its peers through BGP update messages. See [How BGP Advertises Mobile User IP Address Pools for Service Connections and Remote Network Connections](#) for an example of this table and for information about how BGP utilizes the IP address pool you create for mobile users.

---

# Quick Configs for Remote Network Deployments

The following topics show some common Prisma Access deployment scenarios for remote network deployments and provide instructions for how to configure them:

- [Remote Network Locations with Overlapping Subnets](#)
- [Remote Network Locations with WAN Link](#)
- [Use Predefined IPSec Templates to Onboard Service and Remote Network Connections](#)
- [Onboard Remote Networks with Configuration Import](#)
- [Configure Quality of Service in Prisma Access](#)
- [Create a High-Bandwidth Network for a Remote Site](#)
- [Provide Secure Inbound Access to Remote Network Locations](#)
- [Configure User-ID and User-Based Policies with Prisma Access](#)
- [DNS Resolution for Mobile Users and Remote Networks](#)
- [Collect User and Group Information Using the Directory Sync Service](#)

## Remote Network Locations with Overlapping Subnets

As a general rule, you cannot have any overlapping subnets within a Prisma Access deployment. That is, the subnets for all remote network locations, your service connections, and your Prisma Access for mobile users IP address pool cannot overlap. However, in some circumstances you cannot avoid having overlapping subnets; for example:

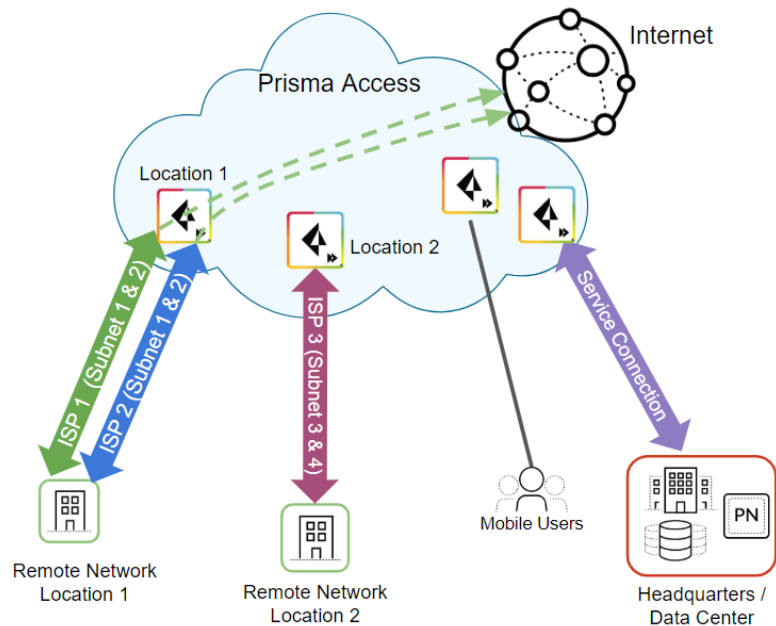
- Your organization has two WAN links that you want to combine for a higher bandwidth throughput in a single remote network location (an active/active WAN deployment).
- You want to configure an overlapping subnet deployment by design (for example, your organization uses the same network topology and IP assignments across multiple retail locations).
- Your organization has one fast WAN link and a slower WAN link, and you want to add both of them to a remote network and designate the WAN link for traffic based on the subnet or application. For example, you might want to route all guest Wi-Fi traffic over one WAN and all other traffic over the other WAN, or you might want to send all web traffic over one WAN and all other traffic over the other WAN.
- You acquired a company that uses subnets that overlap with your existing subnets you have in use.

Prisma Access allows you to onboard remote network locations with overlapping subnets, as long as you select **Overlapped Subnets** check box in the remote network settings when you [Onboard and Configure Remote Networks](#).



*Remote network connections with overlapped subnets support outbound internet only. Refer to the table in the following figure for more details. You can bypass these limitations by configuring source NAT on the on-premise Palo Alto Networks next-generation firewall (if present) or networking device (router, switch, or SD-WAN device) that connects to the IPSec tunnel used for the remote network connection with overlapped subnets.*

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



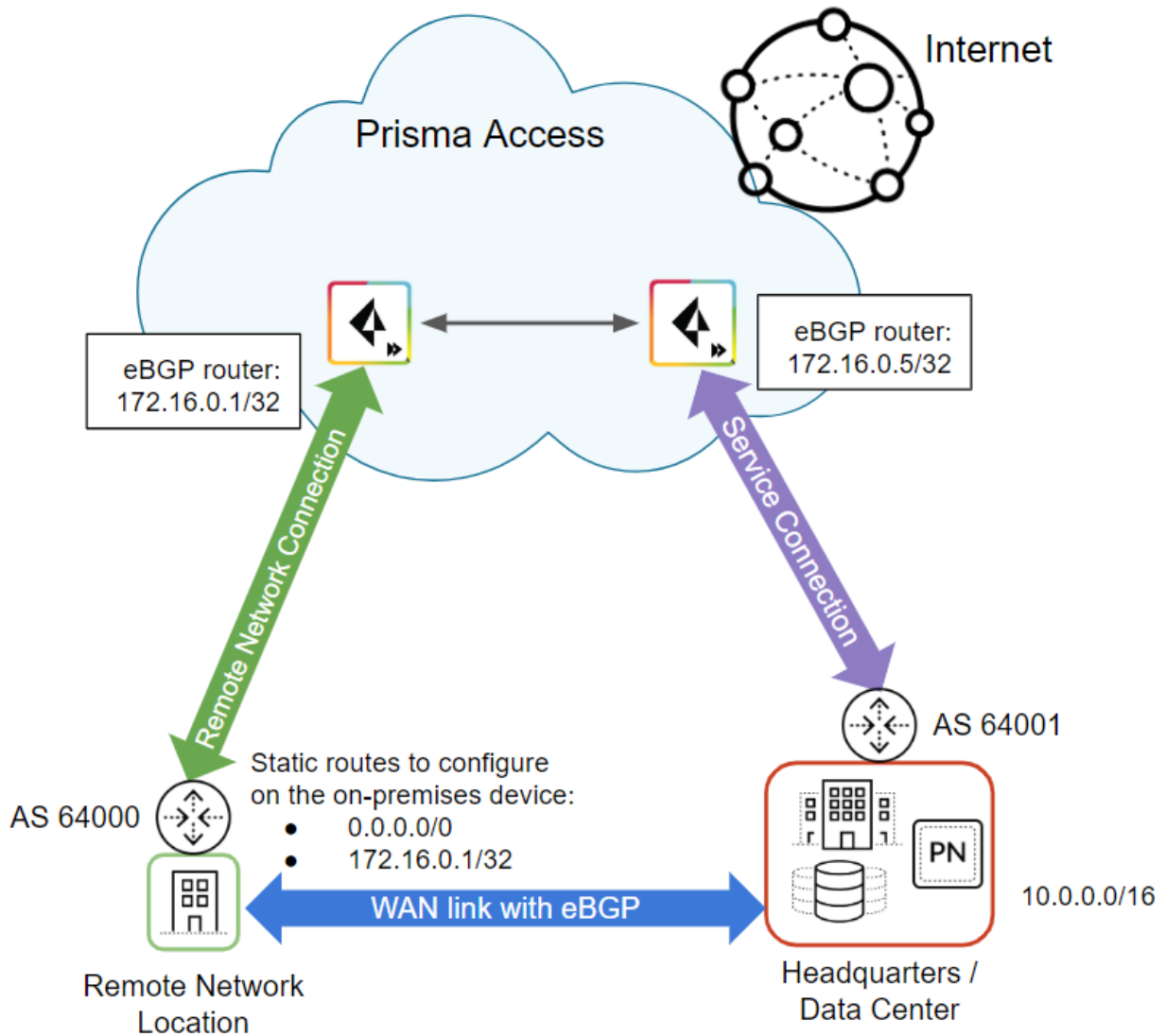
If you add a location with overlapping subnets, it has no effect on locations that don't use overlapping subnets; those sites retain their existing functionality.

## Remote Network Locations with WAN Link

If you have a deployment where the HQ and remote network location(s) are directly connected over a WAN link and each of these locations is secured by Prisma Access, to ensure optimal routing (with eBGP) you must:

- Add a static route to the eBGP router address. In addition to the default route that sends all traffic to Prisma Access, you must add a static route locally on the IPsec-capable device or router at the remote network(s).
- Filter the routes that are advertised from the IPsec capable device or router at HQ to the eBGP peers at other directly connected locations. As a best practice, configure the BGP router at HQ to only advertise routes that you want to allow across the WAN link; you ensure that the eBGP router at HQ does not advertise the routes it learns from Prisma Access to other remote network location(s) secured by Prisma Access. In this example, the eBGP router at HQ only advertises routes that employees from the branch office will need to connect to the servers (subnets) at HQ.

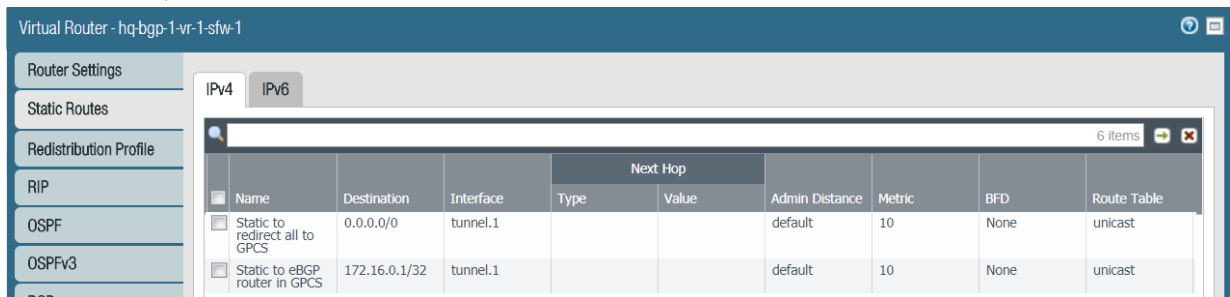
The following illustration shows a retail business with two paths to the servers at the HQ location. One path is a WAN link that provides direct connectivity for employees accessing servers at HQ, and the other path secures traffic generated by other users at this location. For example, traffic generated by customers accessing the retailer's website over Wifi or using the kiosk at the branch office to check inventory. This traffic is sent through the tunnel to the remote network and on to HQ.



To set up this configuration, [create a remote network connection](#) and [create a service connection](#) to onboard the remote network and HQ locations. The details below show how to set up the router configuration at each location to ensure optimal routing:

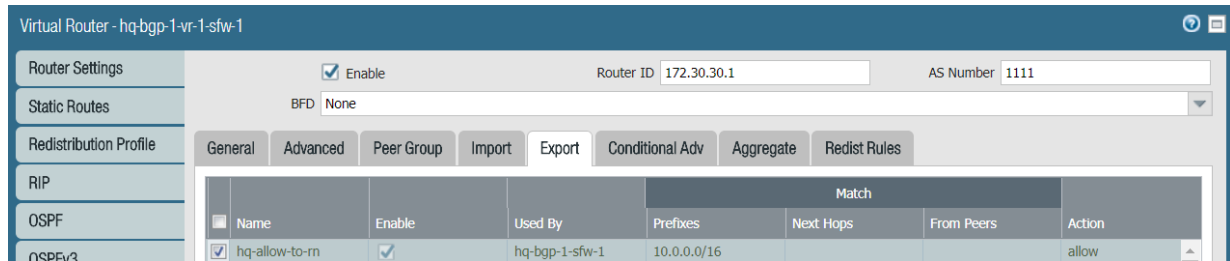
**STEP 1 |** Add the static routes on your router or on-premises IPsec capable device at the remote network location.

If you have a Palo Alto Networks firewall at the edge of the WAN link, on **Network > Virtual Routers > Static Routes**, Add the [static routes](#):



**STEP 2** | Configure the routes that you want to advertise to another directly connected location over the WAN link.

In this example, you need to configure this on the at HQ location. If you have an on-premises Palo Alto Networks firewall at the edge of the WAN link, you can set up [route redistribution](#) and configure which BGP routes to export on **Network > Virtual Routers > BGP**.



## Use Predefined IPsec Templates to Onboard Service and Remote Network Connections

Prisma Access includes predefined IPsec templates for common third-party IPsec and SD-WAN devices. These profiles expedite and simplify the onboarding of service connections and remote network connections that use one of these devices to terminate the connection.

Sharing a common template also allows you to [Onboard Multiple Remote Network Connections of the Same Type](#) with commonly-shared cryptos, pre-shared keys, and Peer identifiers.

- [Template Names and Types](#)
- [Onboard a Service Connection or Remote Network Connection Using Predefined Templates](#)
- [Onboard Multiple Remote Network Connections of the Same Type](#)
- [Supported IKE and IPsec Cryptographic Profiles for Common SD-WAN Devices](#)

### Template Names and Types

Prisma Access provides you with the following predefined templates that you can use to set up IPsec tunnels between your on-premises device and Prisma Access:

- [IPsec Tunnels](#) (**Network > IPsec Tunnels**) under Remote\_Network\_Template and Service\_Conn\_Template.
- [IKE Gateways](#) (**Network > Network Profiles > IKE Gateways**) under Remote\_Network\_Template and Service\_Conn\_Template.
- [IPsec Crypto Profiles](#) (**Network > Network Profiles > IPsec Crypto**) under Remote\_Network\_Template and Service\_Conn\_Template.
- [IKE Crypto Profiles](#) (**Network > Network Profiles > IKE Crypto**) under Remote\_Network\_Template and Service\_Conn\_Template.

Currently, templates for the following vendors are available:



*In addition to the following templates, we provide a Generic template that you can use with any on-premises device that is not listed here.*

- Cisco appliances:
  - Cisco Integrated Services Routers (ISRs)
  - Cisco Adaptive Security Appliances (ASAs)

- 
- Citrix
  - Prisma SD-WAN (formerly CloudGenix)
  - Riverbed
  - Silver Peak

Use the following workflows to onboard service connections or remote network connections using the predefined IPSec templates.

## Onboard a Service Connection or Remote Network Connection Using Predefined Templates

To onboard a service connection or remote network connection using the templates provided by Prisma Access, complete the following task.

**STEP 1 |** In Panorama, perform configuration so that the templates display in Panorama.

When you upgrade the Cloud Services plugin, the new templates do not automatically display. Complete this step once after upgrading to have the templates permanently display. New installations perform this initial configuration as part of their first-time setup and this extra step is not required.



*You can also complete this step if you delete these templates and need to retrieve them.*

- For service connections, select **Panorama > Cloud Services > Configuration > Service Setup**, click the gear icon in the **Settings** area to open the **Settings**, then click **OK**.
- For remote network connections, select **Panorama > Cloud Services > Configuration > Remote Networks**, click the gear icon in the **Settings** area to open the **Settings**, then click **OK**.

**STEP 2 |** Select **Network**, then select the correct **Template** (either **Remote\_Network\_Template** if you are [creating a remote network connection](#) or **Service\_Conn\_Template** if you are [creating a service connection](#)).

**STEP 3 |** Determine the type of device that is used to terminate the service connection or remote network connection, and find a template to use with that device.



*If your SD-WAN or IPSec device is not on the list, use the generic profiles.*

**STEP 4 |** Select **Network > Network Profiles > IKE Gateways** and make the following changes to the IKE gateway profile for your device:

You can use the IPSec crypto and IKE crypto profiles with no changes; however, you must make specific changes to the IKE gateway profile to match the network settings.

- (Optional) If you know the public IP address of the on-premises device that will be used to set up the IPSec tunnel with Prisma Access, set a static IP address by specifying a **Peer IP Address Type of IP** and enter the **Peer Address** for the IPSec tunnel.
- If using a pre-shared key for the IPSec tunnel, specify a **Pre-shared Key**.
- Specify a **Peer Identification** of either **IP Address** or **User FQDN**.

Be sure that you match the settings you specify here when you configure the device used to terminate the other side of the IPSec tunnel.

**IKE Gateway**

**Advanced Options**

Name: Generic-IKE-Gateway-Default

Version: IKEv1 only mode

Peer IP Address Type:  IP  Dynamic

Authentication:  Pre-Shared Key  Certificate

Pre-shared Key: .....

Confirm Pre-shared Key: .....

Local Identification: None

Peer Identification: User FQDN (email address) | generic\_sc@generic.com

OK Cancel

**STEP 5 |** Onboard the [service connection](#) or [remote network connection](#), specifying the **IPSec tunnel** configuration that matches the device on the other side of the IPSec tunnel.

**STEP 6 | (Optional)** If you need to add a backup tunnel (Secondary WAN) for a service connection or remote connection, perform the following additional configuration steps.

1. Create a new **IKE Gateway** for the backup tunnel, copying the settings from the predefined template you want to duplicate.

The following example creates a backup tunnel configuration for generic networking devices.

**IKE Gateway**

**Advanced Options**

Name: Generic-IKE-Gateway-Backup

Version: IKEv1 only mode

Peer IP Address Type:  IP  Dynamic

Authentication:  Pre-Shared Key  Certificate

Pre-shared Key: .....

Confirm Pre-shared Key: .....

Local Identification: None

Peer Identification: User FQDN (email address) | generic\_rn@generic.com

OK Cancel

2. Under **Advanced Options**, specify the **IKE Crypto Profile** for the predefined template you want to use.



*Palo Alto Networks recommends that you use GCM ciphers instead of CBC ciphers for IPsec tunnels.*

The screenshot shows the 'IKE Gateway' configuration window with the 'Advanced Options' tab selected. Under 'Common Options', there are two unchecked checkboxes: 'Enable Passive Mode' and 'Enable NAT Traversal'. The 'IKEv1' section has a dropdown for 'Exchange Mode' set to 'auto', and another dropdown for 'IKE Crypto Profile' set to 'Generic-IKE-Crypto-Default'. Below this is an unchecked checkbox for 'Enable Fragmentation'. The 'Dead Peer Detection' section is checked, with 'Interval' and 'Retry' both set to '5'. At the bottom right are 'OK' and 'Cancel' buttons.

3. Create a new **IPsec Tunnel**, specifying the new IKE gateway you created, but copying all the other settings from the default template.



The screenshot shows the 'IPsec Tunnel' configuration window. The 'General' tab is selected. The configuration includes the following fields and options:

- Name:** Generic-IPsec-Tunnel-Backup
- Type:** Auto Key
- IKE Gateway:** Generic-IKE-Gateway-Backup
- IPsec Crypto Profile:** Generic-IPsec-Crypto-Default
- Enable Replay Protection
- Copy TOS Header
- Tunnel Monitor
  - Destination IP:** None
  - Proxy ID:** None

Buttons: OK, Cancel

4. When you onboard the service connection or remote network connection, **Enable Secondary WAN** and specify the tunnel you created for the backup WAN.

**STEP 7 |** Complete the configuration of the service connection or remote network connection by matching the cryptos, pre-shared key, and Peer identifiers on the device that is used to terminate the other side of the IPSec tunnel.

**STEP 8 |** (Optional) If you need to onboard multiple remote network connections that use the same types of networking devices, **Export** the configuration of the remote network, edit the settings, then **Import** that configuration.

See [Onboard Multiple Remote Network Connections of the Same Type](#) for details.

## Onboard Multiple Remote Network Connections of the Same Type

To streamline the process to [Onboard and Configure Remote Networks](#), you can onboard a single remote network connection that uses a networking device that is common to your network deployment, then **Export** those settings to a Comma Separated Value (CSV) text file. The CSV file includes the values of IPSec tunnel and IKE gateway settings for the network you selected for export. After you export the common configuration settings, you can edit these settings and make them unique for each new remote network you want to onboard, retain the settings that are common to each device, then **Import** that configuration.

---

For more information, including a description of all editable fields in the CSV table, see [Onboard Remote Networks with Configuration Import](#).

## Supported IKE and IPsec Cryptographic Profiles for Common SD-WAN Devices

This section provides you with the supported cryptographic profiles for many common SD-WAN devices. If you are configuring an SD-WAN device, use these profiles as a guideline as to what you can configure for the remote network in Prisma Access.

- [Aruba SD-WAN supported IKE and IPsec crypto profiles](#)
- [Aryaka SD-WAN supported IKE and IPsec crypto profiles](#)
- [Citrix SD-WAN supported IKE and IPsec crypto profiles](#)
- [CloudGenix SD-WAN device supported IKE and IPsec crypto profiles](#)
- [Nuage Networks SD-WAN supported IKE and IPsec crypto profiles](#)
- [Riverbed SteelConnect SD-WAN supported IKE and IPsec crypto profiles](#)
- [Silver Peak SD-WAN supported IKE and IPsec crypto profiles](#)
- [Viptela SD-WAN supported IKE and IPsec crypto profiles](#)

## Onboard Remote Networks with Configuration Import

To streamline the process to [Onboard and Configure Remote Networks](#), you have the option to onboard at least one remote network and then export those settings to a Comma Separated Value (CSV) text file. The CSV file includes the values of IPsec tunnel and IKE gateway settings for the network you selected for export, and you can then edit these settings and make them unique for each new network you may want to onboard. You can modify the CSV file to include 1000 new remote networks and then import the CSV file back to speed up the process of onboarding new remote network locations.

The CSV file does not include keys or passwords, such as the BGP shared secret, the IKE preshared key, Proxy ID, IKE crypto profile, IPsec crypto profile. Therefore, any keys and passwords required for the IPsec tunnel and IKE gateway settings are inherited from the network you select when you initiate the CSV file import.

When using this bulk import process, you must wait for Prisma Access to deploy the infrastructure for securing these locations.

**STEP 1 |** Select **Panorama > Cloud Services > Configuration > Remote Networks** (in the Onboarding section).

**STEP 2 |** Select a region, then **Export** the configuration of a remote network that you have previously onboarded.

You must select a remote network and click **Export**. A CSV file that includes the settings is downloaded to your computer.

**STEP 3 |** Modify the CSV file to add configuration for remote networks.

See [Fields in the Remote Networks Table](#) for a description of the fields and the possible values in this file.

You must rename the network(s) listed in the exported file. If the file has duplicate names the import will fail.

**STEP 4 |** **Import** the CSV file.


The configuration from the file are displayed on screen. The remote network you selected to import the file will serve as a model configuration, and the remote networks listed in the file will inherit the keys and any missing values that do not have to be unique from there.


#### STEP 5 | Commit and push your changes.

1. **Commit > Commit and Push** your changes.
2. Click **OK** and **Push**.

### Fields in the Remote Networks Table

The following table provides a description of the fields in the remote networks table. Fields marked as **Y** in the **Required** row are required fields and fields marked as **N** are optional.

Field	Description	Required? (Y/N)
name	The name of the remote network.	Y
bandwidth	<p>The allocated bandwidth of the remote network. Acceptable values are:</p> <ul style="list-style-type: none"> <li>• 2 Mbps</li> <li>• 5 Mbps</li> <li>• 10 Mbps</li> <li>• 20 Mbps</li> <li>• 25 Mbps</li> <li>• 50 Mbps</li> <li>• 100 Mbps</li> <li>• 150 Mbps</li> <li>• 300 Mbps</li> <li>• 500 Mbps</li> <li>• 1000 Mbps</li> </ul> <p> <i>The 1000 Mbps bandwidth option is in preview mode. The throughput during preview is delivered on a best-effort basis and the actual performance will vary depending upon the traffic mix.</i></p>	Y
region	<p>The remote network's region. See the <a href="#">list of Prisma Access locations</a> for the values to enter.</p> <p>Enter the locations exactly as they are in this document (for example, <b>US West</b>, or <b>Japan South</b>).</p>	Y
subnets	Statically routed subnets on the LAN side of the remote network. Separate multiple subnets with commas.	N
bgp_peer_as	The BGP Autonomous System Number (ASN) of the remote network peer device.	N
bgp_peer_address	The BGP peer address of the remote network peer device.	N

Field	Description	Required? (Y/N)
tunnel_name	The name of the IPSec tunnel configuration. A unique value is required.	Y
gateway_name	The name of the IKE Gateway configuration. A unique value is required.	Y
peer_ip_address	The IP address of the Prisma Access peer device.	N
local_id_type	The type of IKE ID that Prisma Access presents to the peer device. If you use certificates in the remote network to which you import this file, all imported types specified will refer to the Configured Certificate values.	N
local_id_value	The value of the IKE ID that Prisma Access presents to the peer device. If you use certificates in the remote network to which you import this file, all imported types specified will refer to the Configured Certificate values.	N
peer_id_type	The value of the IKE ID that the peer presents to Prisma Access. If you use certificates in the remote network to which you import this file, all imported types specified will refer to the Peer Certificate values.	N
peer_id_value	The value of the IKE ID that Prisma Access presents to the peer device. If you use certificates in the remote network to which you import this file, all imported types specified will refer to the Peer Certificate values.	N
monitor_ip	The tunnel monitoring IP address the cloud will use to determine that the IPSec tunnel is up and the peer network is reachable.   <i>You cannot export a proxy-ID value for the tunnel monitor.</i>	N
proxy_ids	The proxy IDs that are configured for the peer. For route-based VPNs, leave this field blank. Specify the Proxy ID in the following CSV configuration format:  <pre>[{"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}}}]</pre>	N
sec_wan_enabled	Specifies whether or not you enable a secondary IPSec tunnel. Acceptable values are <i>yes</i> and <i>no</i> .	N
sec_tunnel_name	The name of the secondary IPSec tunnel configuration. A unique value is required if you specify a secondary tunnel.	N

Field	Description	Required? (Y/N)
sec_gateway_name	The name of the secondary IKE Gateway configuration. A unique value is required if you specify a secondary tunnel.	N
sec_peer_ip_address	The IP address of the Prisma Access peer device for the secondary IPSec tunnel.	N
sec_local_id_type	The type of IKE ID that Prisma Access presents to the peer device for the secondary IPSec tunnel. If you use certificates in the remote network to which you import this file, all imported types specified will refer to the Configured Certificate values.	N
sec_local_id_value	The value of the IKE ID that Prisma Access presents to the peer device for the secondary IPSec tunnel. If you use certificates in the remote network to which you import this file, all imported types specified will refer to the Configured Certificate values.	N
sec_peer_id_type	The value of the IKE ID that the peer presents to Prisma Access for the secondary IPSec tunnel. If you use certificates in the remote network to which you import this file, all imported types specified will refer to the Peer Certificate values.	N
sec_peer_id_value	The value of the IKE ID that Prisma Access presents to the peer device for the secondary IPSec tunnel. If you use certificates in the remote network to which you import this file, all imported types specified will refer to the Peer Certificate values.	N
sec_monitor_ip	The tunnel monitoring IP address the cloud will use for the secondary IPSec tunnel to determine that the IPSec tunnel is up and the peer network is reachable.   <i>You cannot export a proxy-ID value for the tunnel monitor.</i>	N
sec_proxy_ids	The proxy IDs that are configured for the peer for the secondary IPSec tunnel. For route-based VPNs, leave this field blank. Specify the Proxy ID in the following CSV configuration format:  <pre>[{"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}}}]</pre>	N

---

# Configure Quality of Service in Prisma Access



*This capability is not supported for remote networks if you use [bandwidth allocation per compute location](#) for remote networks.*

Quality of Service (QoS) is a set of technologies that work on a network to guarantee its ability to dependably run high-priority applications and traffic under limited network capacity. You can configure QoS in Prisma Access to prioritize business-critical traffic or traffic that requires low latency, such as VoIP or videoconferencing. You can also reserve a minimum amount of bandwidth for business-critical applications.

Prisma Access uses the same [QoS profiles](#) and supports the same Differentiated Services Code Point (DSCP) markings as next-generation Palo Alto Networks firewalls. However, the configuration process is different than configuring QoS on next-generation firewalls.

Prisma Access can either mark ingress traffic using a [security policy](#) or it can honor DSCP markings set by your organization's on-premises device.

Prisma Access for Clean Pipe also supports QoS; see [Configure Quality of Service for Clean Pipe](#) for details.

- [QoS Configuration Overview](#)
- [QoS Examples](#)
- [Configure QoS in Prisma Access](#)
- [Configure Quality of Service for Clean Pipe](#)

## QoS Configuration Overview

Use the following workflow to configure QoS in Prisma Access. See [Configure QoS in Prisma Access](#) for the detailed steps.

1. Mark the ingress traffic using a security policy or using marking from an on-premises device.

You can create PAN-OS [security policies](#) to mark traffic destined to Prisma Access for mobile users and for remote network connections. For service connections, Prisma Access will honor traffic marking from your organization's on-premises devices. Optionally, you can also use on-premises devices to mark traffic for remote networks.



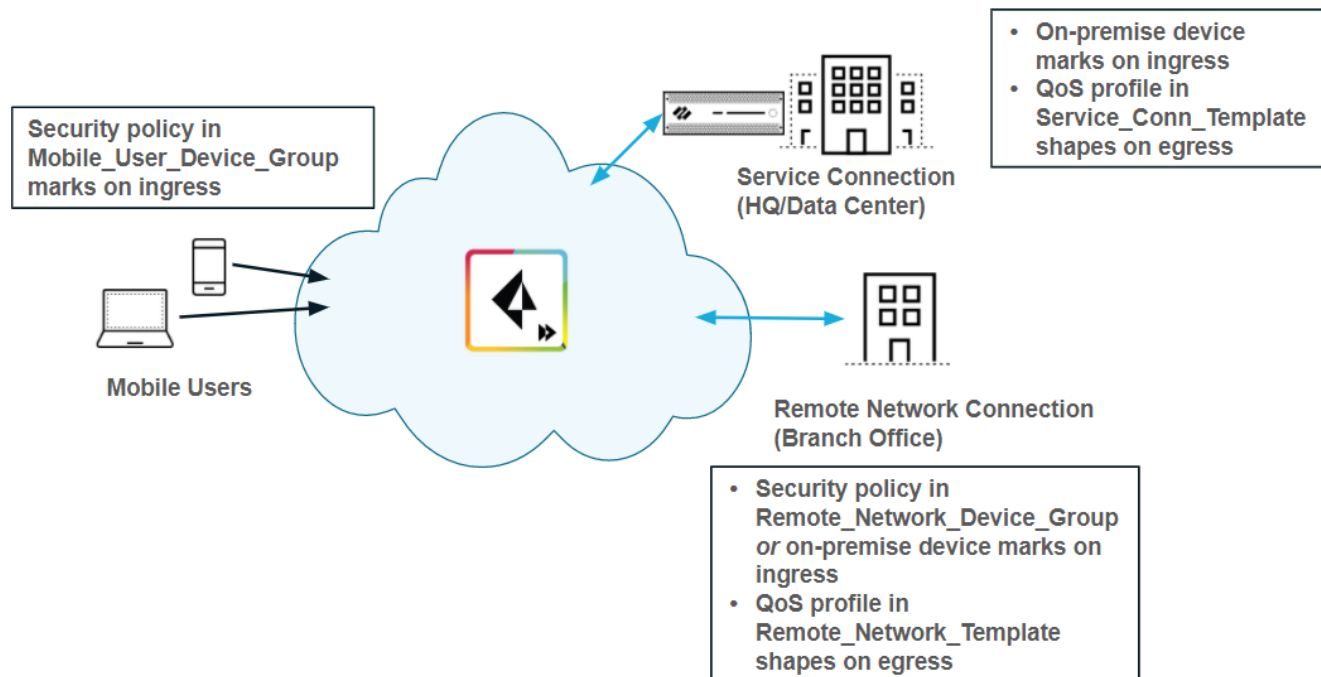
*To ensure predictable results, we recommend marking traffic using either security policies in Prisma Access or your on-premises device, but not both. If there are differences between the security policies in Prisma Access and the on-premises device, the security policy in Prisma Access overrides the policy in the on-premises device.*

2. Map the traffic to classes using a [QoS policy](#) rule.
3. Shape the traffic using a [QoS profile](#).

You can create QoS profiles to shape QoS traffic for service connections and for remote network connections and apply those profiles to traffic that you marked with PAN-OS security policies, traffic that you marked with an on-premises device, or both PAN-OS-marked and on-premise-marked traffic.

4. Enable QoS on the service connection or remote network connection and bind the QoS profile to the connection.

The following figure shows the available QoS deployments in Prisma Access.




## QoS Examples

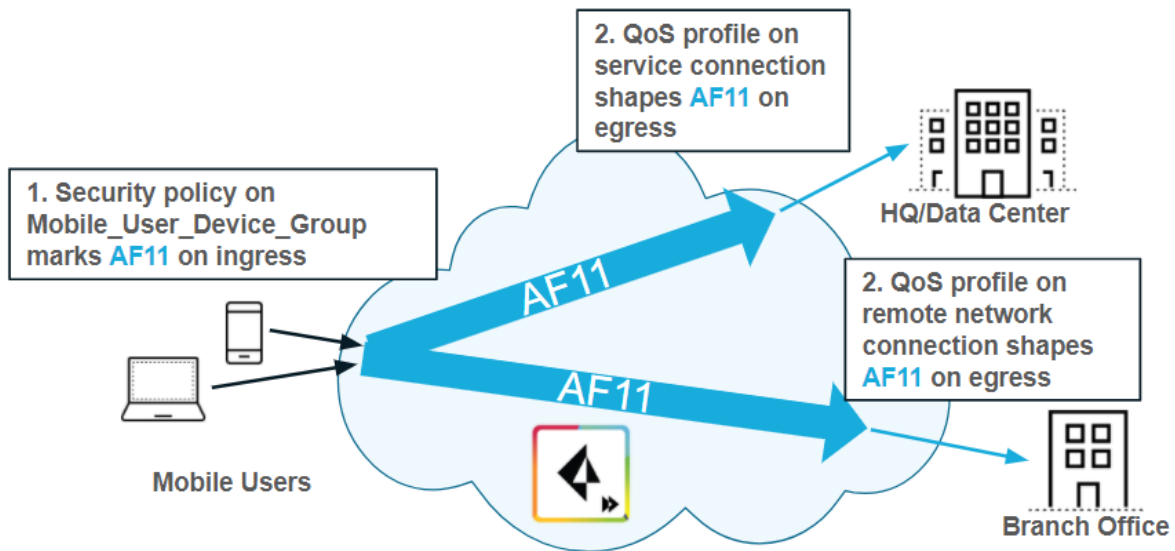
The following examples show how Prisma Access marks and shapes traffic.

In the following example, the administrator created a security policy on the Mobile\_User\_Device\_Group to mark incoming mobile user traffic. These policies assign traffic an IP precedence value of AF11.

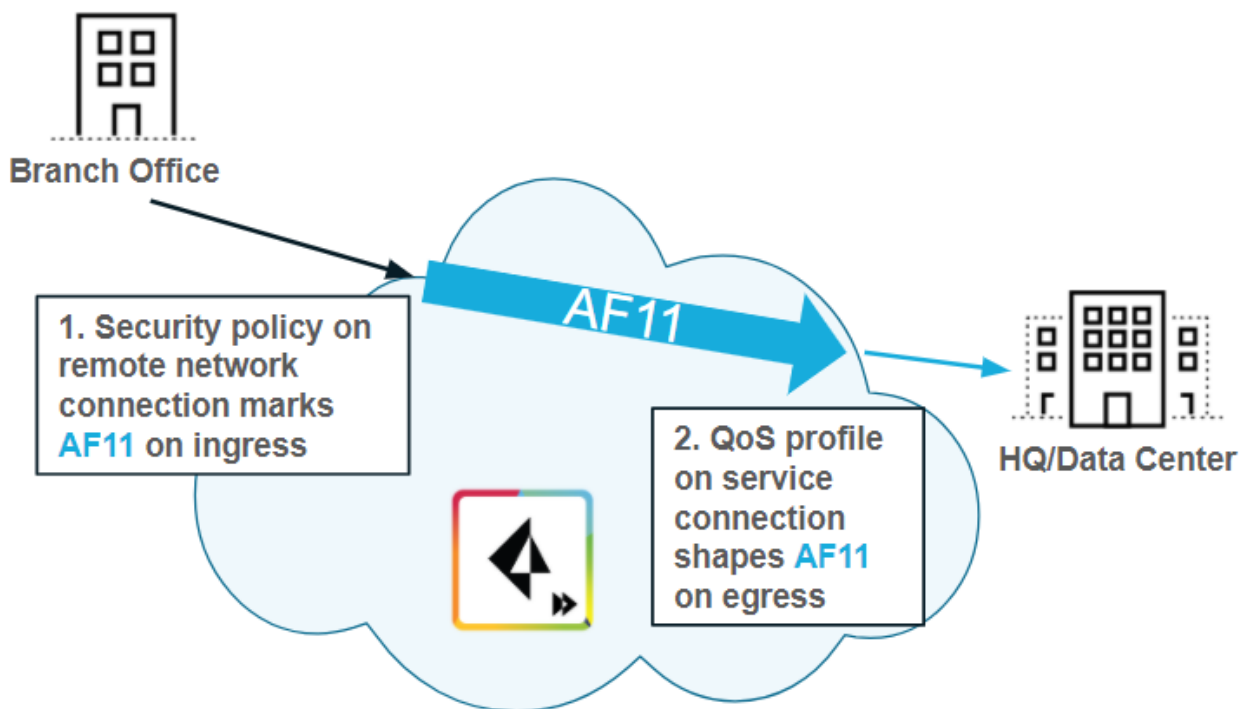
The administrator also created QoS profiles with [QoS policy](#) rules, enabled QoS on the service connection and remote network connection, and applied the profiles to those connections to shape the traffic at the traffic's egress point based on the QoS markings.

 *Prisma Access marks traffic at its ingress point based on security policies or honors marking set by your on-premises devices, and shapes the traffic on egress to your service connections or remote network connections using QoS profiles.*





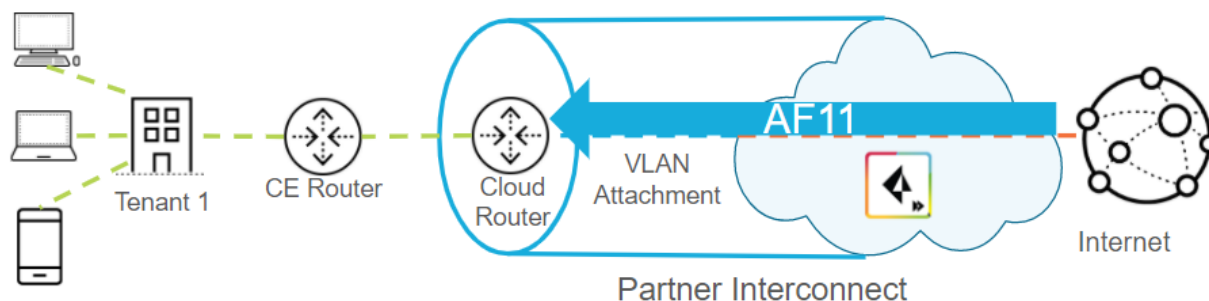
The following example shows the QoS traffic flow from a branch office to an HQ/data center. The administrator creates a [security policy](#) on the **Remote\_Network\_Device\_Group** to mark the incoming traffic from the remote network connection and enabled QoS and applied a QoS profile on the service connection to shape the outgoing traffic.



The following example shows a hybrid deployment with an on-premises firewall at a branch that is connected by Prisma Access with a remote network connection, and the on-premises firewall marks the traffic. This deployment honors the marking set on the on-premises firewall. You must enable QoS and apply a QoS profile on the service connection, so that Prisma Access can shape the traffic at egress.

Prisma Access honors all DSCP marking from the on-premises device as long as that traffic does not match an overriding security policy on Prisma Access.

The following example shows a [Clean Pipe](#) configuration that shapes on ingress (from the internet to Clean Pipe side). See [Configure Quality of Service for Clean Pipe](#) for configuration details.



## Configure QoS in Prisma Access


Configure Quality of Service in Prisma Access by completing the following task.

**STEP 1 |** Add one or more [security policy](#) rules for remote networks and mobile users to mark the ingress traffic for QoS.

You use these policies to match a traffic flow and assign it a selected DSCP value.

1. Select **Policies > Security > Pre Rules**.

Alternatively, select **Policies > Security > Post Rules** to add a rule at the bottom of the rule order that is evaluated after a pre-rule.

 *Be sure that you select the correct Device Group. To create a security rule for a remote network, select the device group for the remote network (for example, `Remote_Network_Device_Group`); for mobile users, select the device group for the mobile users (for example, `Mobile_User_Device_Group`).*

2. **Add** a security policy rule.
3. Enter a **Name** for the rule.
4. Define the matching criteria for the source or destination fields in the packet.

See [Create a Security Policy Rule](#) for details.

5. Click **Actions**, then select a **QoS Marking** of either **IP DSCP** or **IP Precedence**.
6. Enter the QoS value in binary form, or select the value from the drop-down.

The following screenshot shows a security policy rule that matches traffic marked with an **IP DSCP** value of **af11**.

## STEP 2 | Add one or more QoS policy rules.

You use QoS policies to bind DSCP marking to one of eight available classes. You use these classes later when you create one or more QoS profiles.

1. Select **Policies > QoS > Pre Rules**.

Alternatively, select **Policies > QoS > Post Rules** to add a rule at the bottom of the rule order that is evaluated after a pre-rule.

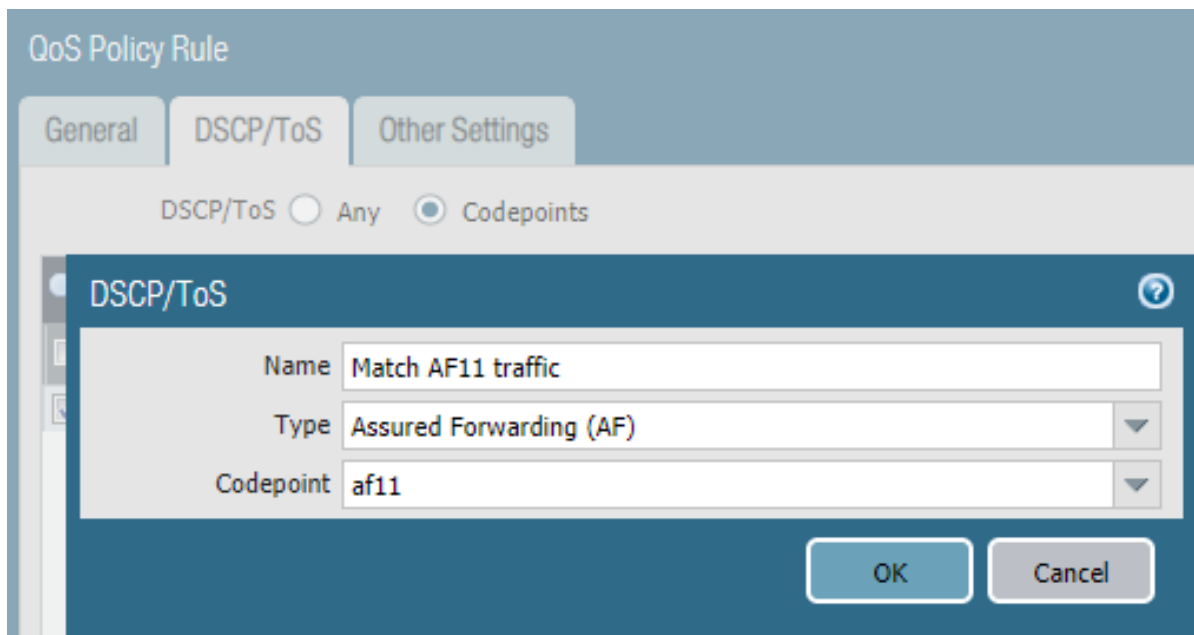


*Be sure that you select the correct Device Group for the service connection (for example, `Service_Conn_Device_Group`) or remote network connection (for example, `Remote_Network_Device_Group`). If a rule in a Shared device group has defined values other than the values in the General, DSCP/ToS, and Other settings areas, Prisma Access does not apply the rule on the remote network and service connection.*

2. **Add** a QoS policy rule.
3. Click **General** and enter a name for the policy rule.
4. Click the **DSCP/ToS** tab, then click **Codepoints** and **Add** one or more new codepoints.

For Clean Pipe deployments, you can specify additional QoS settings in policy, such as source, destination, or application.

5. Specify a **Name** for the DSCP/ToS rule, then select a **Type** and **Codepoint**.

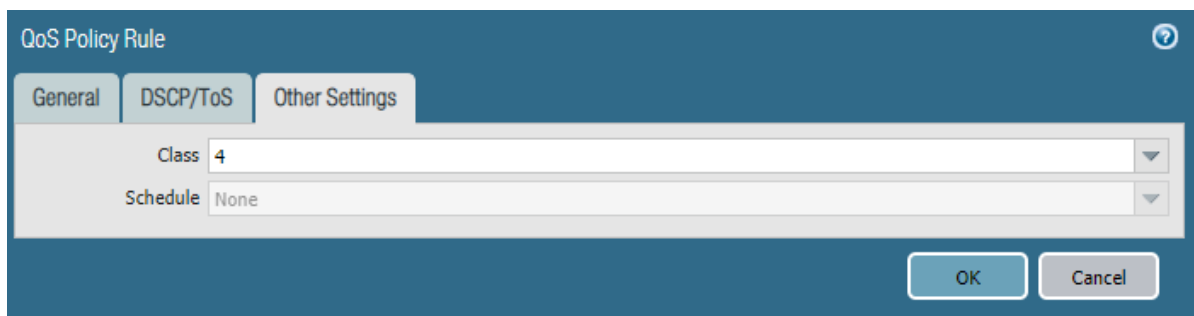


Alternatively, keep the default value (**Any**) to allow the policy to match to traffic regardless of the Differentiated Services Code Point (DSCP) value or the IP Precedence/Type of Service (ToS) defined for the traffic.

6. Click the **Other Settings** tab, then Choose the QoS **Class** to assign to the rule.

You define class characteristics in the QoS profile.

7. Click **OK**.



### STEP 3 | Create one or more [QoS profiles](#) to shape QoS traffic on egress for service connections and remote network connections.

You use profiles to shape the traffic at egress point by defining QoS classes and assigning a bandwidth to them. You must select either an existing QoS profile or create a new QoS profile when you enable QoS for Prisma Access.

1. Select the correct template the profile you want to create (**Remote\_Network\_Template** or **Service\_Conn\_Template**); then, select **Network > Network Profiles > QoS Profile** and
2. **Add** a profile.
3. Enter a profile **Name**.
4. Set the overall bandwidth limits for the QoS profile rule.
  - Enter an **Egress Max** that represents the maximum throughput (in Mbps) for traffic leaving the service connection or remote network connection.
    - For service connections, specify a number of up to 1 Gpbs (1,000 Mbps).



Do not enter a number greater than 1 Gbps; Prisma Access calculates service connection bandwidth per service connection IPsec tunnel and not cumulatively across multiple tunnels.

- For remote network connections, specify a number up to the maximum licensed bandwidth of your remote network connection.
- Enter an **Egress Guaranteed** bandwidth that is the guaranteed bandwidth for this profile (in Mbps).

Any traffic that exceeds the Egress Guaranteed value is best effort and not guaranteed. Bandwidth that is guaranteed but is unused continues to remain available for all traffic.

5. In the Classes section, **Add** one or more classes and specify how to mark up to eight individual QoS classes.

- Select the **Priority** for the class (either **real-time**, **high**, **medium**, or **low**).
- Enter the **Egress Max** for traffic assigned to each QoS class you create.

The **Egress Max** for a QoS class must be less than or equal to the Egress Max for the QoS profile.

- Enter the **Egress Guaranteed** bandwidth in Mbps for each QoS class.

Guaranteed bandwidth assigned to a class is not reserved for that class—bandwidth that is unused continues to remain available to all traffic. When a class of traffic exceeds the egress guaranteed bandwidth, Prisma Access passes that traffic on a best-effort basis.

<input type="checkbox"/>	Class	Priority	Egress Max	Egress Guaranteed
<input type="checkbox"/>	class1	real-time	20	3
<input type="checkbox"/>	class2	high	10	1
<input type="checkbox"/>	class3	low	5	0

class 4 is the default class

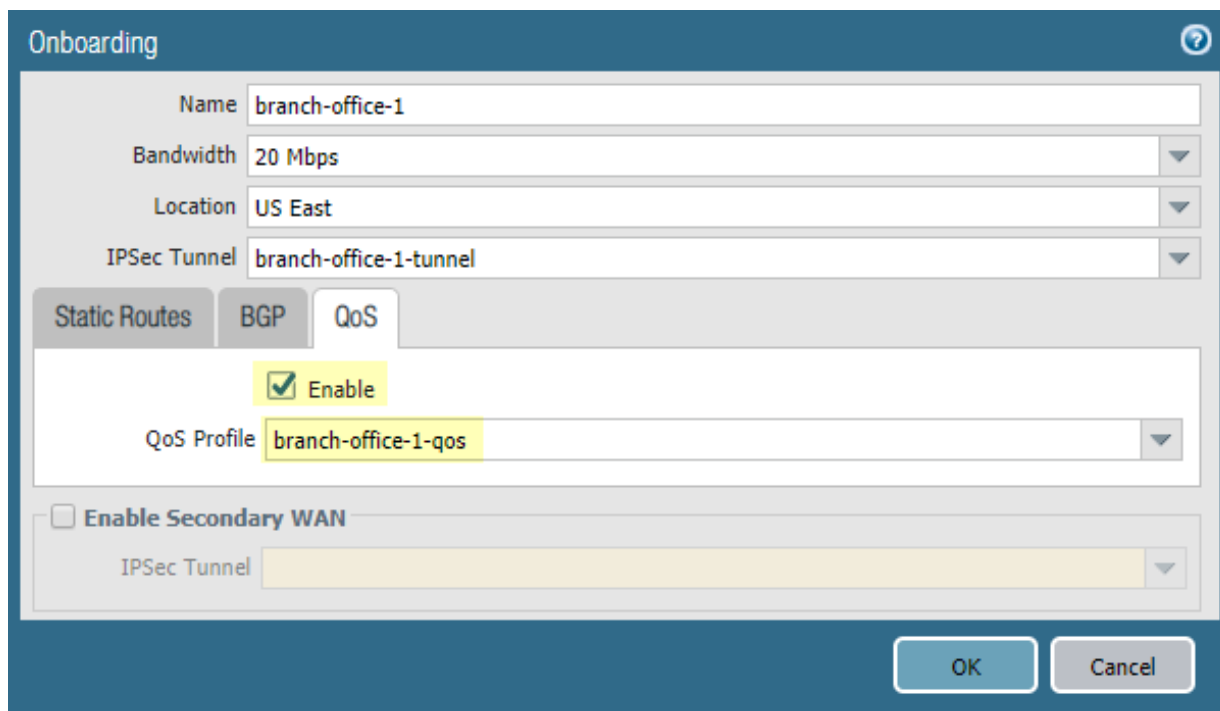
6. Click **OK**.

**STEP 4** | Enable QoS for the service connection, remote network connection, or both, and apply the QoS profile to the connection.

1. Enable QoS.

- For service connections, select **Panorama > Cloud Services > Configuration > Service Setup**, select a **Connection Name**, click the **QoS** tab, and **Enable QoS**.
- For remote network connections, select **Panorama > Cloud Services > Configuration > Remote Networks**, select the hypertext for a remote network connection **Name**, click the **QoS** tab, and **Enable QoS**.
- For Clean Pipe deployments, select **QoS** during Clean Pipe onboarding, then select the **QoS Profile** to use with the clean pipe.

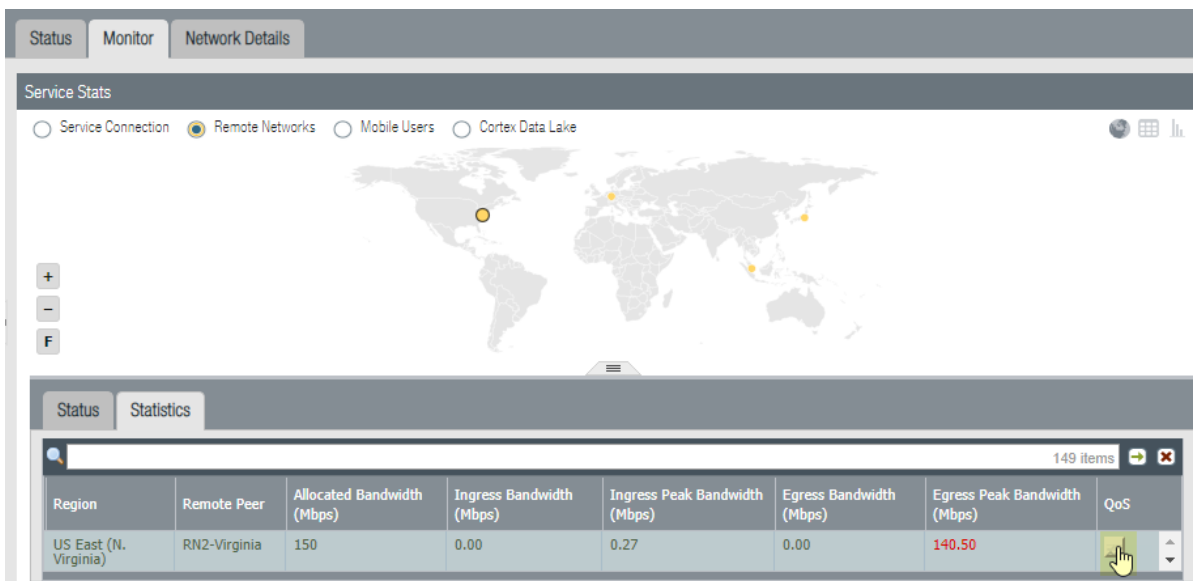
2. Select the QoS profile you created in Step 3 and click **OK**.



The screenshot shows the 'Onboarding' configuration window for QoS. The window has a dark blue header with the title 'Onboarding' and a help icon. Below the header, there are several input fields: 'Name' (branch-office-1), 'Bandwidth' (20 Mbps), 'Location' (US East), and 'IPSec Tunnel' (branch-office-1-tunnel). Below these fields are three tabs: 'Static Routes', 'BGP', and 'QoS'. The 'QoS' tab is selected. Under the 'QoS' tab, there is a checkbox labeled 'Enable' which is checked. Below the checkbox is a dropdown menu for 'QoS Profile' with the value 'branch-office-1-qos'. Below the 'QoS' section is a checkbox labeled 'Enable Secondary WAN' which is unchecked. Below this checkbox is another dropdown menu for 'IPSec Tunnel'. At the bottom right of the window are two buttons: 'OK' and 'Cancel'.

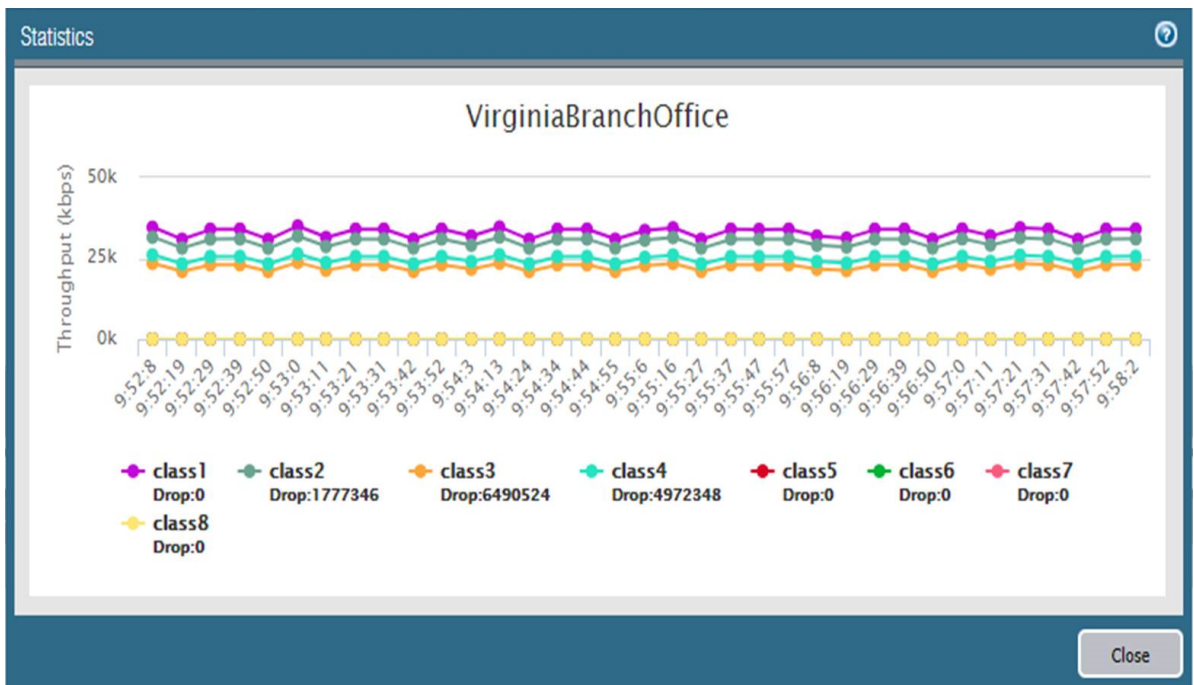
**STEP 5** | Check the QoS status.

1. Select **Panorama > Cloud Services > Status > Monitor > Service Connection** or **Panorama > Cloud Services > Status > Monitor > Remote Networks**, then **Monitor** the **Statistics**.
2. Click **QoS** to view a page with QoS statistics.



This page displays a chart with real-time and historical QoS statistics, including the number of dropped packets per class. This chart displays only for service connections or remote network connections that have QoS enabled, shows the last five minutes of the connection's network activity, and refreshes every 10 seconds.

The following figure shows traffic being passed for classes 1,2,3, and 4. The data below the figure shows the number of packets dropped based on the QoS configuration for classes 2, 3, and 4.



### Configure Quality of Service for Clean Pipe


For Clean Pipe deployments, you can create [QoS policies](#) to define the traffic that receives QoS treatment and [QoS profiles](#) to define the classes of service, including priority, that the traffic can receive. You can define QoS based on DSCP values or zones (Trust or Untrust). To implement QoS with Clean Pipe, select the [QoS Profile](#) when you onboard the Clean Pipe. See [Configure Prisma Access for Clean Pipe](#) for details.

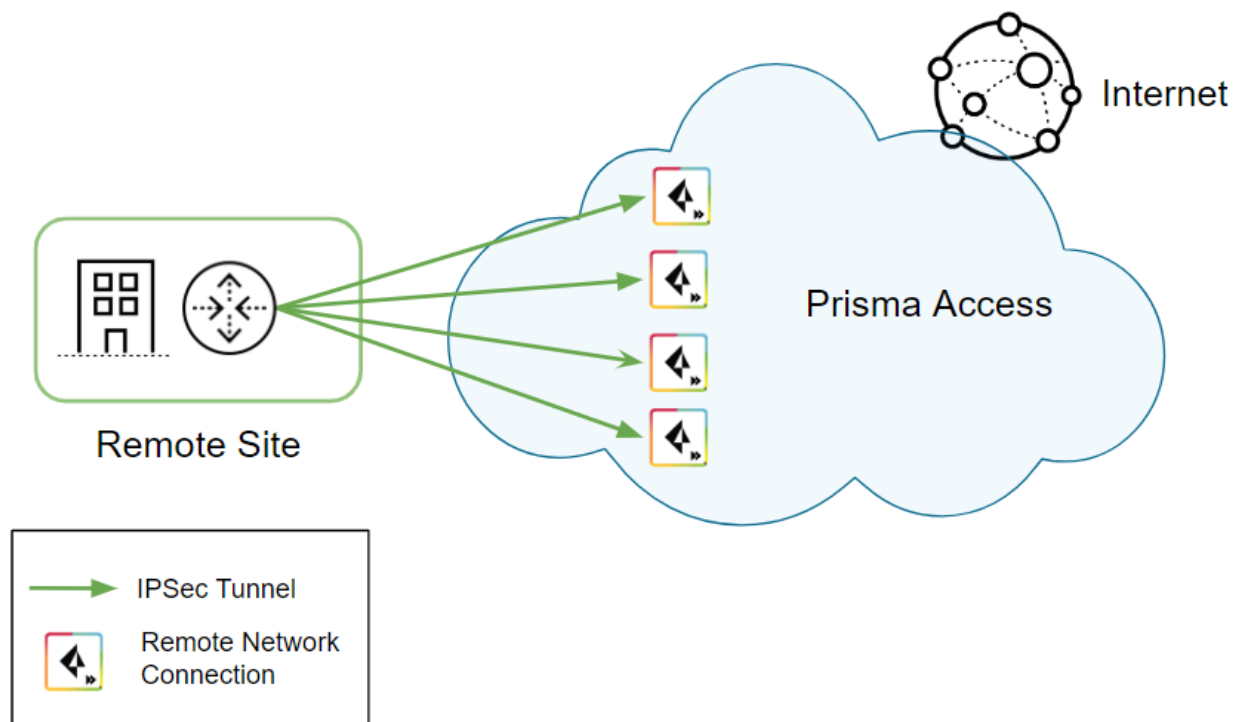
## Create a High-Bandwidth Network for a Remote Site

If you want to secure your branch office or site for outbound internet access with a high-bandwidth connection to Prisma Access, you can load balance traffic from your branch office or site using multiple IPSec tunnels by completing the steps in this chapter.

### Topology for High-Bandwidth Remote Network

The following diagram shows a sample topology for a branch location using multiple IPSec remote network tunnels between the site and Prisma Access. In this diagram, we use four 300 Mbps remote network tunnels to create a 1.2 Gbps throughput to traffic egressing to the internet. The CPE devices can be Palo Alto Networks next-generation firewalls or other devices that are capable of creating multiple IPSec tunnels and performing load balancing between these tunnels. One of the methods to achieve this is by enabling ECMP with session stickiness. The CPE must maintain session affinity per tunnel while applying ECMP over multiple tunnels.

 This example shows four tunnels. The maximum number of tunnels you can use for a high-bandwidth connection in Prisma Access is based on the maximum number of IPSec tunnels your CPE devices support with the load balancing protocol you use (ECMP in this example).



Consider the following restrictions and recommendations before you deploy this configuration:

- Use BGP routing for the IPSec tunnels; static routing is not supported.
- Use this configuration for outbound internet access only.
- Do not use tunnel monitoring on either Prisma Access or the CPE devices. Availability of the IPSec tunnel is determined by BGP peering between the CPE and Prisma Access' remote network. If an IPSec tunnel goes down and BGP connection is interrupted, the routes learned over BGP on that tunnel are automatically removed from ECMP.



- 
- Because you use BGP to determine when a tunnel goes down, consider the HoldTime value you have configured on your CPE devices. The hold timer determines the amount of time that the tunnel is down before removing the route. Prisma Access uses the default BGP HoldTime value of 90 seconds as defined by RFC 4271. If you configure a lower hold time for the BGP CPE devices in the remote network site, BGP uses the lower hold time value. Palo Alto Networks recommends a KeepAlive value of 10 seconds and a HoldTime value of 30 seconds for your CPE devices with this deployment.

## Create a High-Bandwidth Remote Network Connection

To create a high-bandwidth remote network connection, complete the following task.

**STEP 1 |** in Panorama, configure the Prisma Access remote network tunnels.

1. (Optional) if you haven't already, set up [IKE gateways](#), [IKE crypto](#) and [IPSec crypto](#) profiles, and [IPSec tunnels](#) for the remote network connections you create.

Make a note of the IKE and IPSec cryptographic profiles; you specify the same settings on the CPE you use to terminate the remote network connection in the remote network location.

2. Select **Panorama > Cloud Services > Configuration > Remote Networks** and create four [remote network connections](#), specifying the following settings:

- Select a **Bandwidth** of **300 Mbps**.
- Select the same **Location** for each connection.
- **Enable BGP** and **Advertise Default Route**.
- Specify the same **Peer AS** for all remote network connections.

This example shows a **Peer AS** of 2000; in this example, you select a **Peer AS** of 2000 for all four connections.

- (Optional) if you want to create a backup remote network, create one by selecting **Enable Secondary WAN**; then, select the **IPSec Tunnel** you created for the backup tunnel.

**Onboarding**

Name: Korea-RN1

ECMP Load Balancing: None

Location: South Korea

Bandwidth: 300 Mbps

IPSec Tunnel: RN1-US1

Enable Secondary WAN

IPSec Tunnel: RN2-US1

Static Routes | **BGP** | QoS | Inbound Access

Enable

Advertise Default Route

Don't Advertise Prisma Access Routes

**Primary WAN**

Peer AS: 2000

Peer Address: 192.168.6.2

Local Address: 192.168.6.100

Secret: [ ]

Confirm Secret: [ ]

**Secondary WAN**

Same as Primary WAN

Peer AS: 2000

Peer Address: [ ]

Local Address: [ ]

Secret: [ ]

Confirm Secret: [ ]

OK Cancel

When complete, you have four 300 Mbps remote network connections for the same location. If you configured backup tunnels, you also have four secondary tunnels to be used for failover purposes.

Settings

Template Stack: Remote\_Network\_Template\_Stack

Parent Device Group: Shared

Overlapped Subnets:

Zone Mapping

Trusted Zones: trust

Untrusted Zones: untrust

Onboarding


Connection Name	Location	Prisma Access			Links		Remote Networks	
		Bandwidth	ECMP	IPSec Tunnel	Peer IP Address	BGP	Subnets	
<input checked="" type="checkbox"/> Korea-RN1	South Korea	300 Mbps	Disabled	RN1-US1 (Primary)	dynamic	Enabled		
<input type="checkbox"/> Korea-RN2	South Korea	300 Mbps	Disabled	RN2-US1 (Secondary)	dynamic	Enabled		
<input type="checkbox"/> Korea-RN3	South Korea	300 Mbps	Disabled	Korea-RN2-BK (Secondary)	dynamic	Enabled		
<input type="checkbox"/> Korea-RN4	South Korea	300 Mbps	Disabled	Korea-RN3 (Primary)	dynamic	Enabled		
				Korea-RN3-BK (Secondary)	dynamic			
				Korea-RN4 (Primary)	dynamic	Enabled		
				Korea-RN4-BK (Secondary)	dynamic			

3. Select **Panorama > Cloud Services > Status > Network Details > Remote Networks** and make a note of the **Service IP Address** and **EBGP Router** addresses.

You use the **Service IP Address** as the peer IP address when you configure the IPsec tunnel on the CPE devices in the remote network site, and you use these addresses and the **EBGP Router** addresses when you create static routes on the CPE devices.

Name	Service IP Address	Local IP Address	Static Subnet	EBGP Router	Branch AS and Router
Korea-RN1		dynamic		192.168.6.100	2000   192.168.6.2   BGP Status
Korea-RN2		dynamic		192.168.6.102	2000   192.168.6.4   BGP Status
Korea-RN3		dynamic		192.168.6.103	2000   192.168.6.6   BGP Status
Korea-RN4		dynamic		192.168.6.104	2000   192.168.6.8   BGP Status









**STEP 2 |** On the CPE devices in the remote network site, configure the remote network tunnels.

 *The configuration in these steps use Palo Alto Networks next-generation firewalls; you can use any CPE device that supports IPsec tunnels and ECMP for this deployment.*

1. Create four active tunnels from the active CPE to each of the four network connections. For the **Peer IP** address, enter the **Service IP Address** of the remote network you received from Prisma Access in Step 1.c.

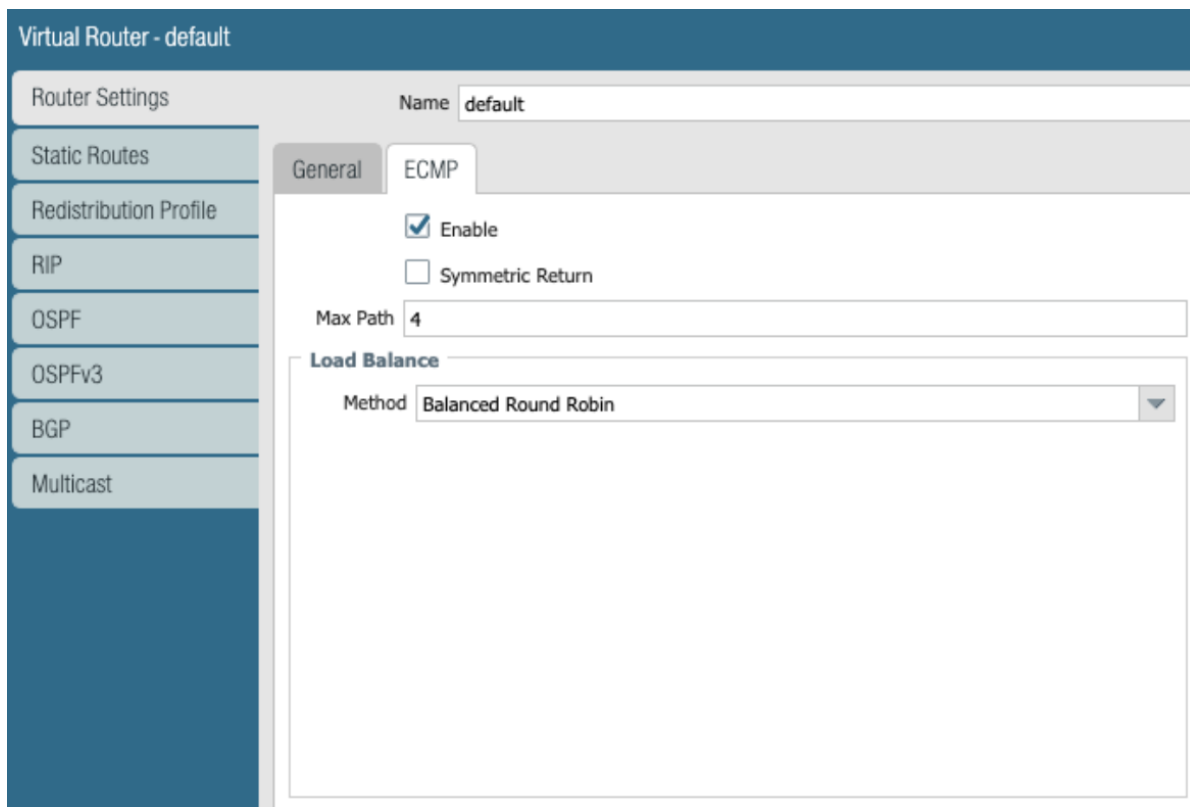
Name	Status	Type	Interface	IKE Gateway/Satellite			Interface
				Local IP	Peer IP	Status	
SK-RN1-ISP1	 Tunnel Info	Auto Key	ethernet1/1			 IKE Info	tunnel.2
SK-RN2-ISP1	 Tunnel Info	Auto Key	ethernet1/1			 IKE Info	tunnel.3
SK-RN3-ISP1	 Tunnel Info	Auto Key	ethernet1/1			 IKE Info	tunnel.4
SK-RN4-ISP1	 Tunnel Info	Auto Key	ethernet1/1			 IKE Info	tunnel.5

2. (Optional) If you create backup tunnels, create them from the active CPE to each of the four network connections. For the **Peer IP** address, enter the **Service IP Address** of the remote network you received from Prisma Access in Step 1.c.

Name	Status	Type	Interface	IKE Gateway/Satellite			Interface
				Local IP	Peer IP	Status	
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 |** Configure ECMP on the CPE devices in the remote network site.

1. Select **Network > Virtual Routers**.
2. Select the **default** virtual router, or **Add** a new virtual router.
3. Select **Router Settings > Enable > ECMP**, then **Enable ECMP** with a **Max Path** of **4** and a load balance **Method** of **Balanced Round Robin**.

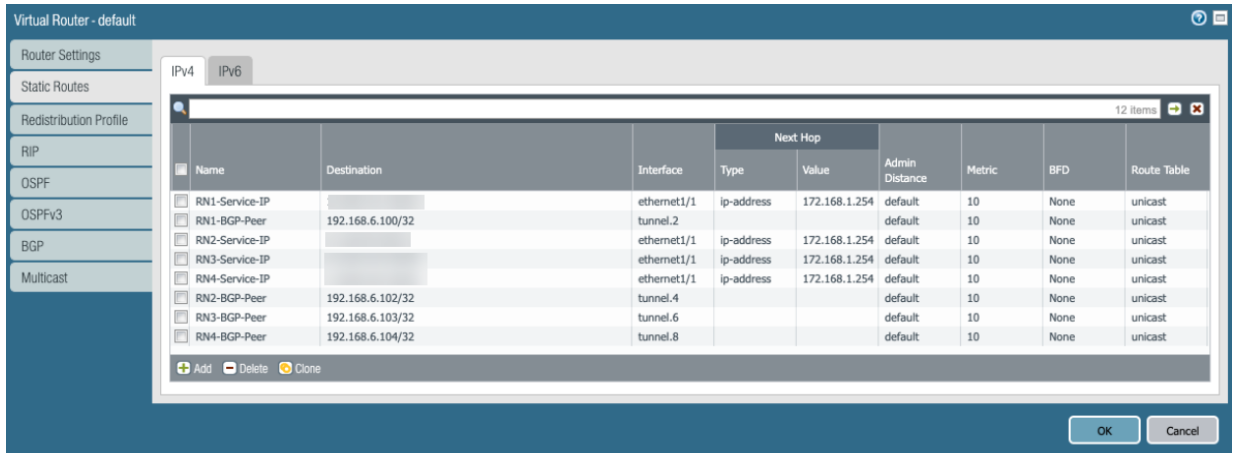


**STEP 4 |** On the CPE devices in the remote network site, create static routes to the Prisma Access **Service IP Address** and **eBGP Router IP** addresses you retrieved in Step 1.c.

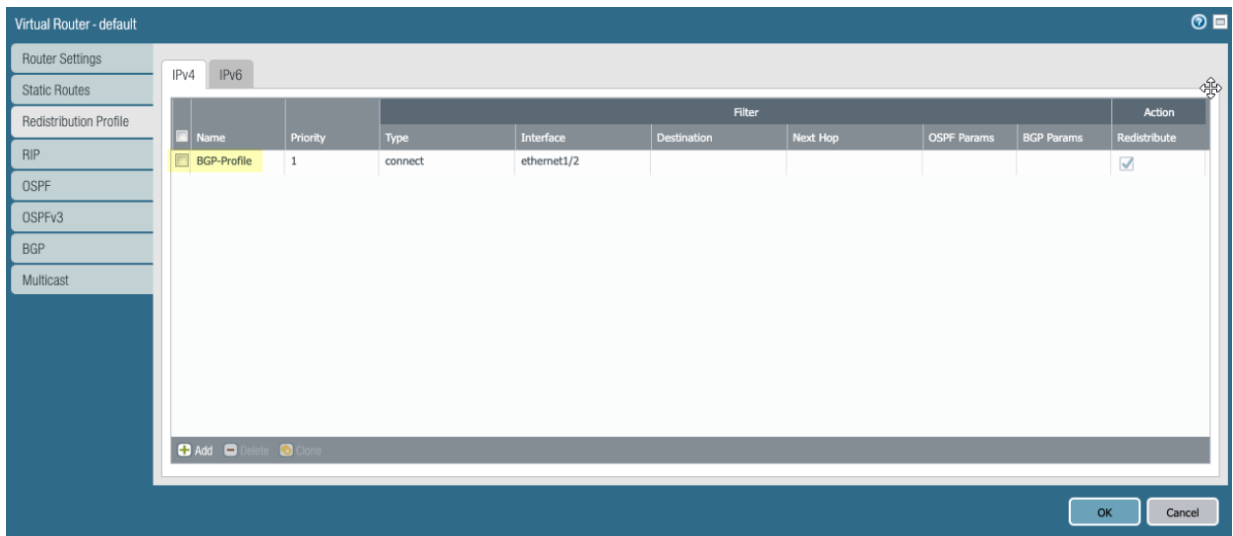
As previously stated, dynamic routing with BGP is required for this configuration. To facilitate BGP connection between the CPE and Prisma Access' eBGP router, you need to add a static route for the eBGP router IP address on the CPE, and the next-hop must be the tunnel interface on the CPE. You must repeat this step for all other Remote Network eBGP router IP addresses on remaining tunnels.

The following example shows the route on the active CPE. If you created backup tunnels on a standby CPE, create the same routing on the standby CPE.

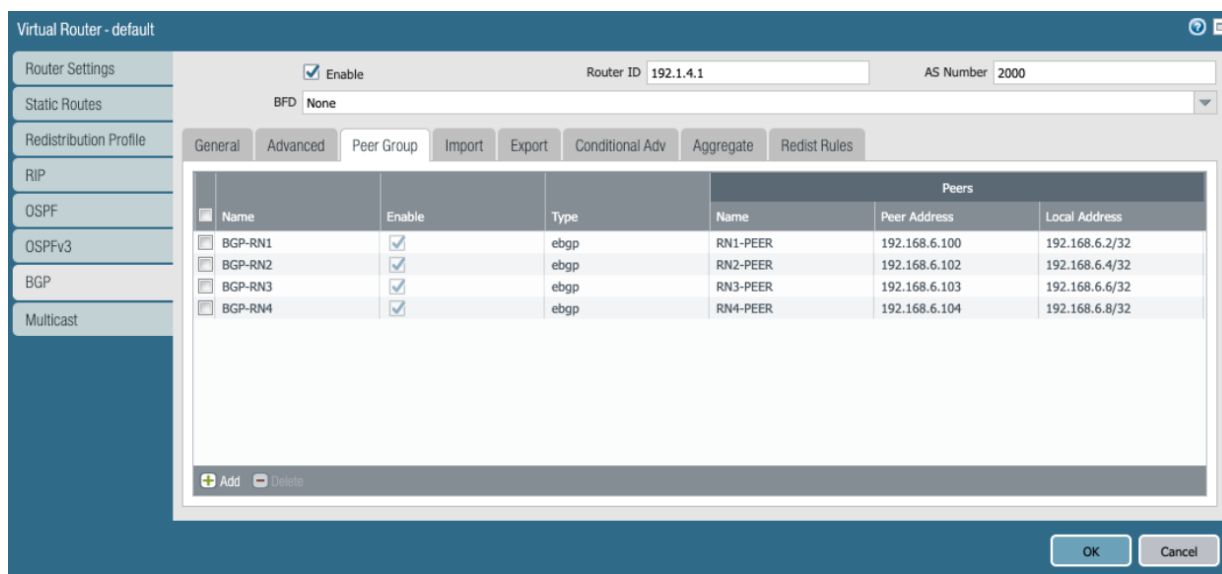
If you are configuring a Palo Alto Networks next-generation firewall, select **Static Routes > IPv4** to add the static routes.



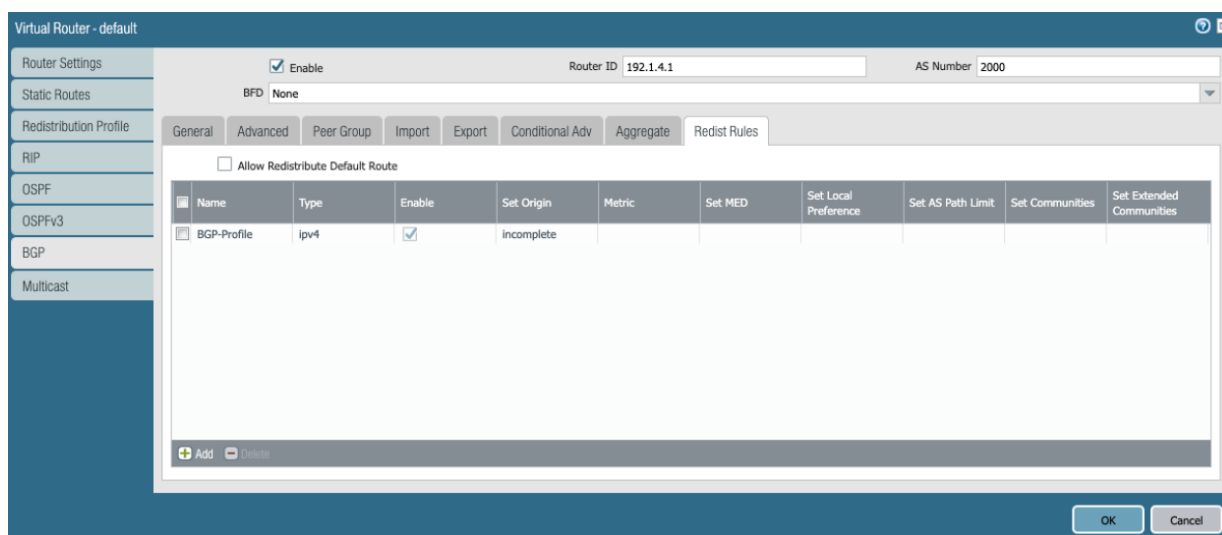
**STEP 5** | Enable [route redistribution](#) on the CPE devices by selecting **Redistribution Profile > IPv4**, then **Add** an IPv4 route redistribution profile.



**STEP 6** | Select **BGP > Peer Group**, **Enable BGP** on the virtual router instance, then **Add Remote Network BGP peers**.



**STEP 7 |** Select **BGP > Redist Rules**, then attach the route redistribution profile you created in Step 5.



**STEP 8 |** Validate that the CPE is passing traffic on all four of its tunnels.

**STEP 9 |** Check the status of the ECMP-enabled connections from Prisma Access.

- Select **Panorama > Cloud Services > Monitor > Remote Networks**, select the region where you deployed the ECMP connections, then select **Status**.



*In this area, ECMP displays as No. This is expected because you are not configuring the Prisma Access [ECMP load balancing](#) feature.*

Location	Remote Peer	Allocated Bandwidth (Mbps)	ECMP	Config Status	BGP Status	Tunnel Status
South Korea	Korea-RN1	300	Disabled	Commit in progress	Established	OK
South Korea	Korea-RN2	300	Disabled	In sync	Established	OK
South Korea	Korea-RN3	300	Disabled	In sync	Established	OK
South Korea	Korea-RN4	300	Disabled	Commit in progress	Established	OK

- Select **Statistics** to see that traffic is passing through each remote network tunnel.

Location	Remote Peer	Allocated Bandwidth (Mbps)	Ingress Bandwidth (Mbps)	Ingress Peak Bandwidth (Mbps)	Egress Bandwidth (Mbps)	Egress Peak Bandwidth (Mbps)	QoS
South Korea	Korea-RN2	300	21.16	278.13	18.15	21.14	
South Korea	Korea-RN3	300	125.12	259.45	79.14	179.12	
South Korea	Korea-RN4	300	245.18	286.12	12.17	94.07	
South Korea	Korea-RN1	300	35.17	56.17	32.16	178.16	

When you have completed this workflow, you have created a high-bandwidth configuration for the remote network. Keep in mind that this solution is supported for outbound traffic only.

## Provide Secure Inbound Access to Remote Network Locations



*This capability is not supported if you [bandwidth allocation per compute location for remote networks](#).*

If your organization hosts internet-accessible applications at a remote network site, providing access to those applications exposes your network to all the threats posed by an open internet. This section describes how Prisma Access provides a way to provide secure access to those applications, when you should implement it, and how to configure it.


- [Secure Inbound Access for Remote Network Sites](#)
- [Secure Inbound Access Examples](#)
- [Guidelines for Using Secure Inbound Access](#)
- [Configure Secure Inbound Access for Remote Network Sites](#)

### Secure Inbound Access for Remote Network Sites

Prisma Access for remote networks allows outbound access to internet-connected applications. In some cases, your organization might have a requirement to provide inbound access to an application or website at a remote site, and provide secure access to that application for any internet-connected user—not just users who are protected by Prisma Access. For example:


- You host a public-facing custom application or portal at a remote network site.
- You have a lab or staging environment for which you want to provide secure access.
- You have a need to provide access to an application or website to users who are not members or an organizational domain.
- You have IoT devices that require access to an internal asset management, tracking, or status application.

To do this, create a remote network that allows secure inbound access. If you require outbound access as well as inbound access for a remote network site, create [two remote network sites in the same location](#)—one for inbound access and one for outbound access.

 *While this solution can provide access for up to 50,000 concurrent inbound sessions per remote network, Palo Alto Networks does not recommend using this solution to provide access to a high-volume application or website.*

To make internet-accessible applications available from a remote network site, you first make a list of the applications to which you want to provide access, and assign a private IP, port number, and protocol combination for each application. If you use the same IP address for multiple applications, the port/protocol combination must be unique for each application; if you use the same port/protocol combination for multiple applications, each IP address must be unique.

To begin configuration, you choose how many public IP addresses you want to associate for the applications. You can specify either 5 or 10 public IP addresses per remote network site. Each public IP allocation takes bandwidth from your Remote Networks license, in addition to the license cost for the remote network. 5 IP addresses take 150 MB from your remote network license allocation, and 10 IP addresses take 300 MB. The following table provides examples of bandwidth cost.

 *Use the following examples as a guide; you can use any remote network bandwidth to implement secure inbound access.*

Number of IP Addresses	Remote Network Bandwidth	Bandwidth Allocation from Remote Network Bandwidth Pool
5 IP addresses (Cost 150 MB from Remote Network bandwidth pool)	150 MB	300 MB (150 MB for 5 inbound access IP addresses + 150 MB remote network bandwidth)
10 IP addresses (Cost 300 MB from Remote Network bandwidth pool)	150 MB	450 MB (300 MB for 10 inbound access IP addresses + 150 MB remote network bandwidth)
5 IP addresses (Cost 150 MB from Remote Network bandwidth pool)	300 MB	450 MB (150 MB for 5 inbound access IP addresses + 300 MB remote network bandwidth)
10 IP addresses (Cost 300 MB from Remote Network bandwidth pool)	300 MB	600 MB (300 MB for 10 inbound access IP addresses + 300 MB remote network bandwidth)

After you choose the number of public IP addresses, you then enter the application, along with its associated private IP/port number/protocol combination, for which you want secure inbound access.

You can decide how you want to map your application to the public IP addresses. By default, Prisma Access assigns the public IP addresses to the applications you specify, and multiple applications can be assigned to a single IP address. If you need to map a single application to a single public IP address, you can select **Dedicated IP** during system configuration. You can configure up to 100 inbound applications for each group of provisioned public IP addresses (either 5 or 10).



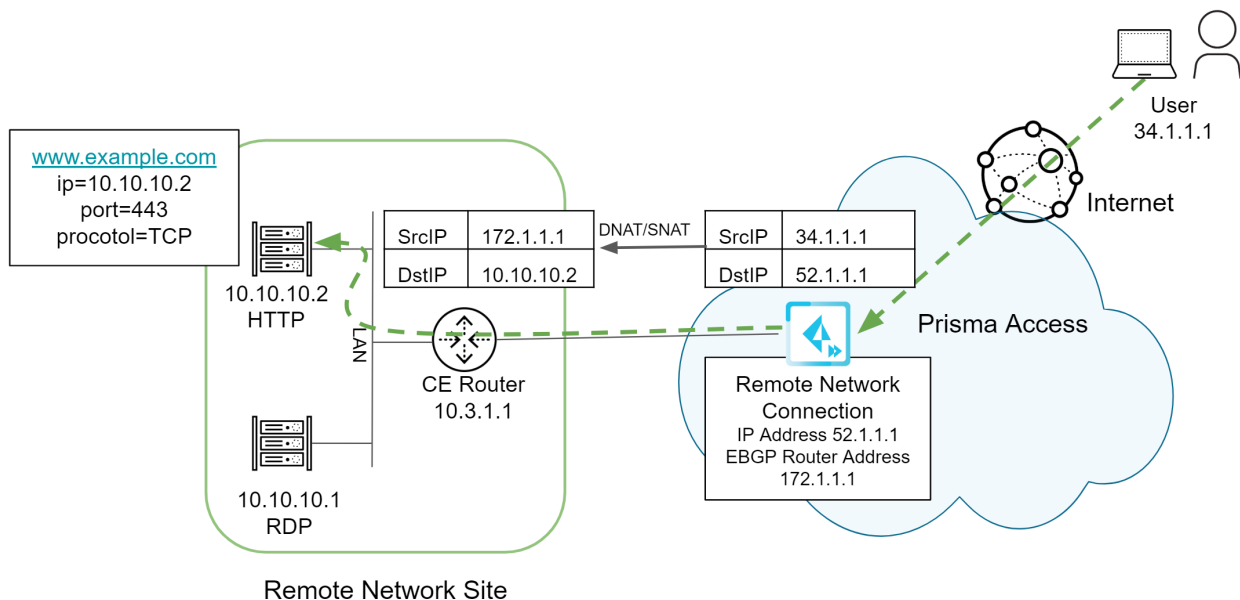
## Secure Inbound Access Examples

This section provides inbound access examples, along with the IP addresses that Prisma Access assigns in various deployments.

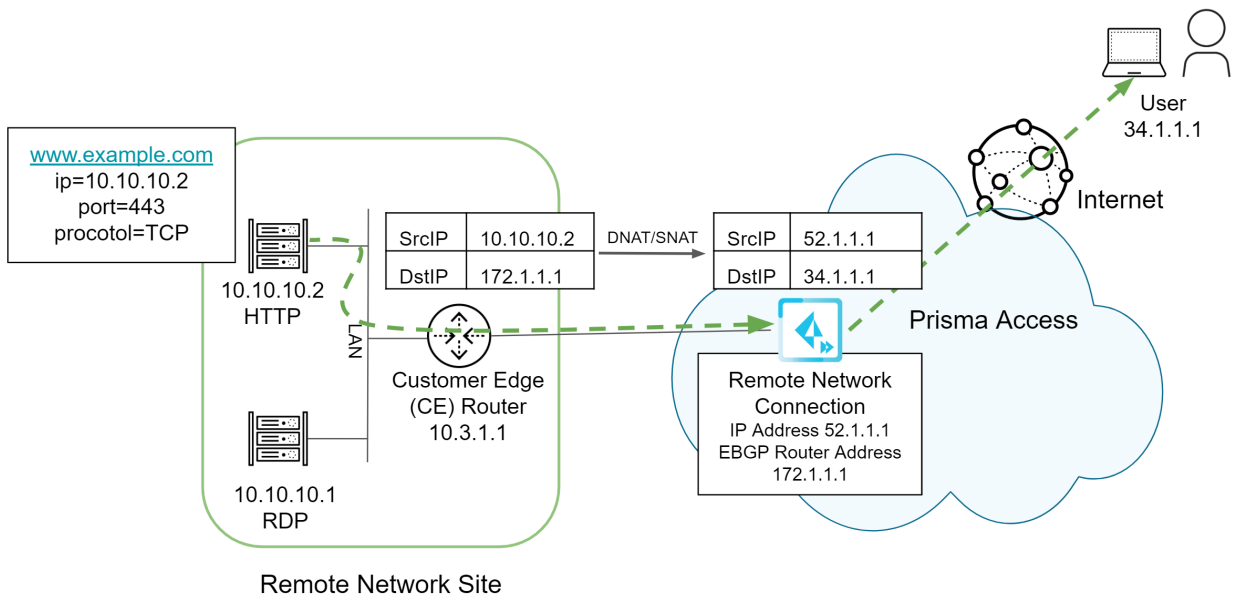
The following example shows a sample configuration to enable inbound access for an application ([www.example.com](http://www.example.com)) at a remote network site. You assign an IP address of 10.10.10.2, a port of 443, and a protocol of TCP to the application. You then enter these values in Prisma Access when you configure inbound access. After you save and commit your changes, Prisma Access assigns a public IP address to the application you defined, in this case 52.1.1.1.

Prisma Access performs source network address translation (source NAT) on the packets by default. If the IPSec-capable device at your remote network site is capable of performing [symmetric return](#) (such as a Palo Alto Networks next-generation firewall), you can disable source NAT.

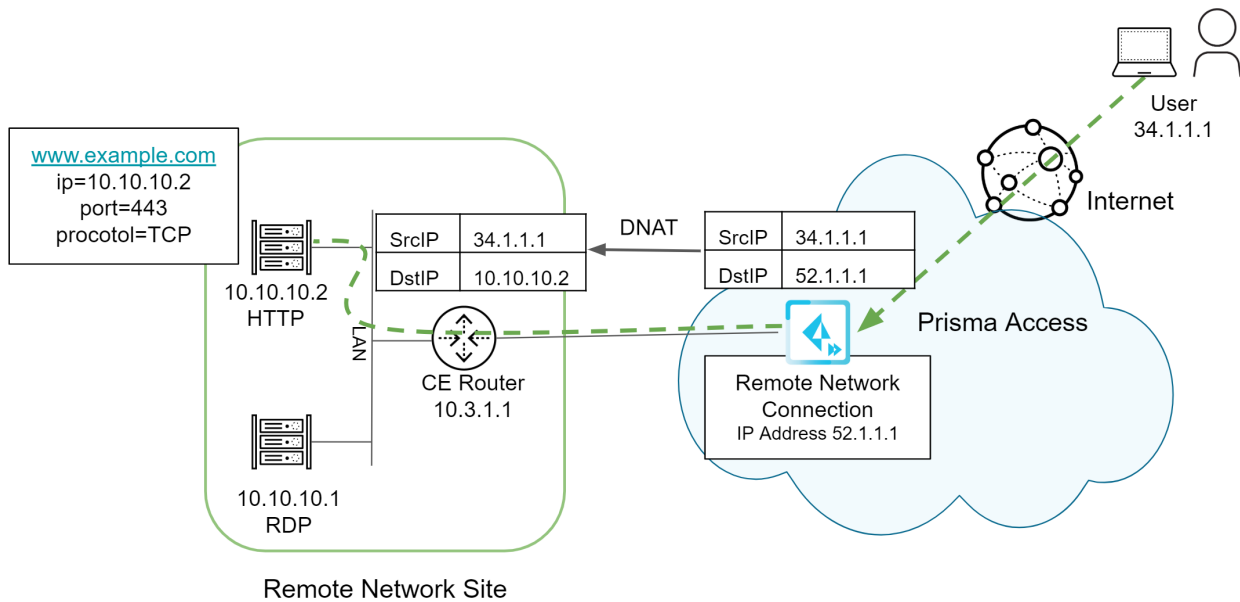
The following figure shows the traffic flow from users to applications. Since source NAT is enabled, the source IP address in the routing table changes from the IP of the user's device (34.1.1.1) to the remote network's **EBGP Router** address (**Panorama > Cloud Services > Status > Network Details > Remote Networks > EBGP Router**). (172.1.1.1).



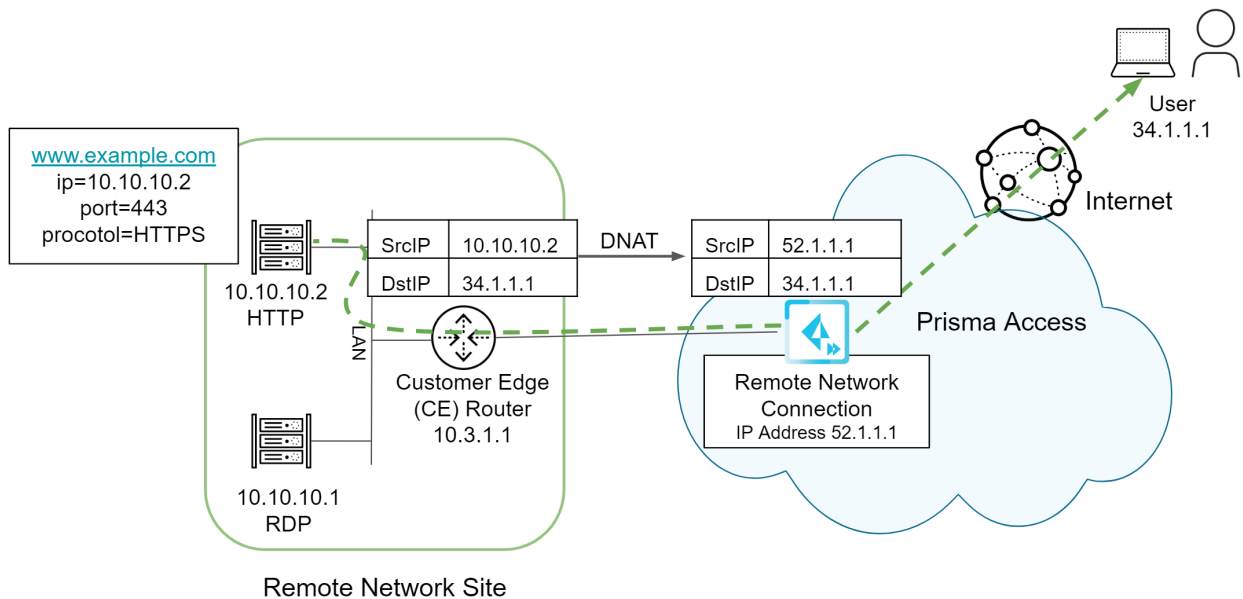
The following figure shows the return path of traffic with source NAT enabled.



If you disable source NAT, Prisma Access still performs destination NAT, but the source IP address of the request is unchanged.



For return traffic, SNAT is disabled, and the destination address for all routing tables is user's IP address (34.1.1.1).



## Guidelines for Using Secure Inbound Access

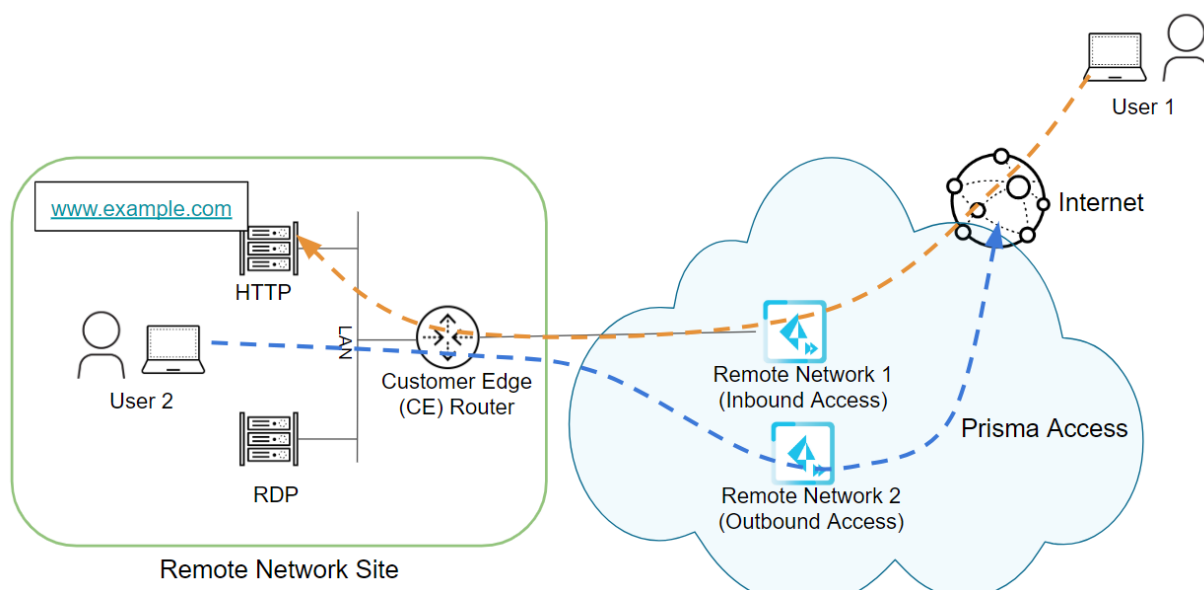
Use the following guidelines and restrictions when you configure a remote network to use secure inbound access:

- The following locations are supported:
  - Australia Southeast
  - Belgium
  - Brazil South
  - Canada East
  - Finland
  - Germany Central
  - Hong Kong
  - India West
  - Japan Central
  - Netherlands Central
  - Singapore
  - Switzerland
  - Taiwan
  - UK
  - US Central
  - US East
  - US Northwest
  - US Southeast
  - US Southwest
- You cannot modify an existing remote network to provide secure inbound access; instead, create a new remote network.
- The inbound access feature is not available on remote networks that use [ECMP load balancing](#).
- Application port translation is not supported.

- The [bulk import](#) feature to onboard remote networks does not support inbound access. Use Panorama to onboard new inbound access remote networks.
- Do not use remote network inbound access with [traffic forwarding rules with service connections](#).
- Outbound traffic originating at the branch is not allowed on the inbound remote network.
- User-ID and application authentication are not supported.
- Prisma Access enforces the following rate limiting thresholds to provide flood protection, and measures the rate in connections per second (CPS):

Flood Protection Type	Alarm Rate in CPS	Activate Rate in CPS
<a href="#">SYN Flood</a>	10000	15000
<a href="#">ICMP Flood</a>	20	20

- Remote networks that are configured for secure inbound access can only be used for that purpose. If you require outbound access as well as inbound access for a remote network site, create two remote network sites in the same location—one for inbound access and one for outbound access—as shown in the following figure. In this example, User 1 uses Remote Network 1 for inbound access to [www.example.com](#), while User 2 uses Remote Network 2 for outbound internet access from the remote network location.



- If you have a custom Prisma Access deployment where one of the cloud providers is excluded, inbound access might not be supported because you cannot choose the locations during remote network onboarding.
- Secure inbound access is not supported with evaluation licenses.

## Configure Secure Inbound Access for Remote Network Sites

To create a remote network sites that allows secure inbound access, complete the following steps.

**STEP 1** | Select **Panorama > Cloud Services > Configuration > Remote Networks** and **Add** a connection.

Any bandwidth is supported for secure inbound access.

**STEP 2 | Select Inbound Access and Enable secure inbound access.**

The screenshot shows the 'Onboarding' wizard in Palo Alto Networks Panorama. The 'Inbound Access' tab is selected. The configuration includes:


- Name: Secure-Inbound-Access-RN
- ECMP Load Balancing: None
- Location: Canada East
- Bandwidth: 300 Mbps
- IPSec Tunnel: Generic-IPSec-Tunnel-Default
- Enable Secondary WAN
- IPSec Tunnel: (empty dropdown)

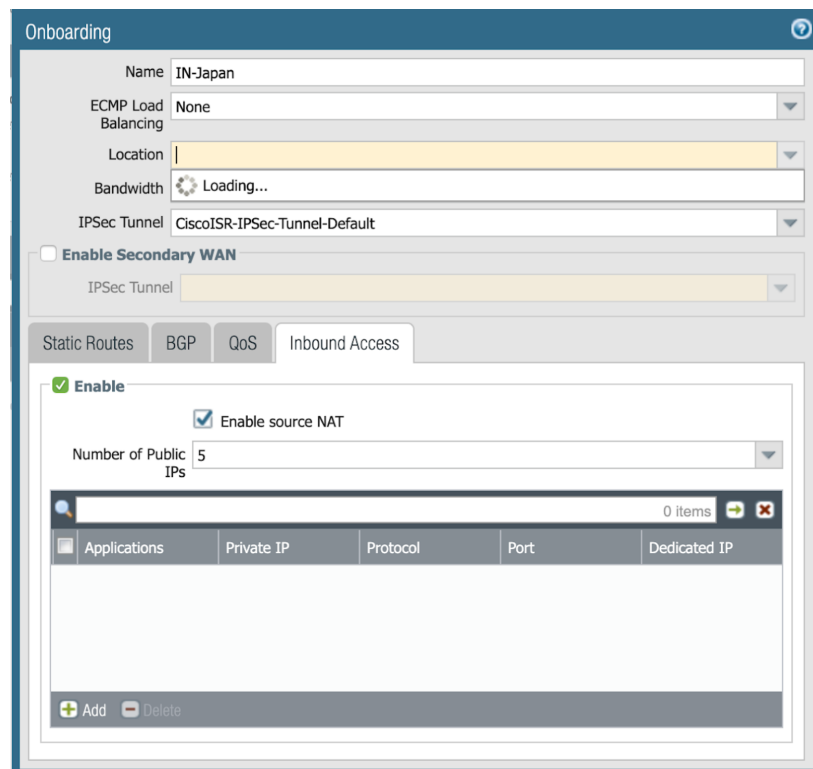
The 'Inbound Access' section is expanded, showing:

- Enable
- Enable source NAT
- Number of Public IPs: 5

Below this is a table with columns: Applications, Private IP, Protocol, Port, and Dedicated IP. The table is currently empty, with '0 items' displayed. There are 'Add' and 'Delete' buttons at the bottom of the table.

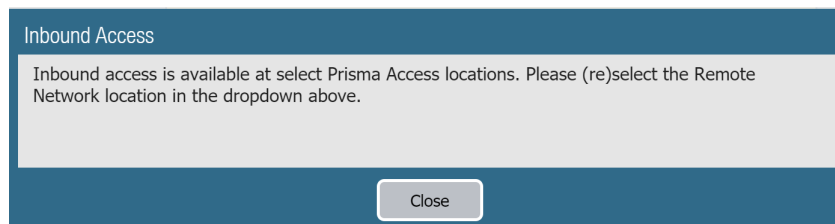
At the bottom of the wizard are 'OK' and 'Cancel' buttons.

 *If Palo Alto Networks has created a custom Prisma Access deployment for your organization where one of the cloud providers is excluded, inbound access features may not be configurable due to non-availability of the supported locations; in this case, no locations display in the Location area, as shown in the following screenshot.*



**STEP 3** | When prompted, click **Close** and select or re-select, a supported location.

Prisma Access prompts you with a verification window when you enable secure inbound access, to make sure that you select a supported location.



**STEP 4** | (Optional) To disable source NAT, deselect **Enable Source NAT**.

By default, source NAT is enabled. If the IPsec-capable device at your remote network site is capable of performing [symmetric return](#) (such as a Palo Alto Networks next-generation firewall), deselect **Enable source NAT**.

**STEP 5** | Select the **Number of Public IPs** that you want to allocate for secure inbound access (**5** or **10**).

The IP addresses you use for inbound secure access take bandwidth from your remote network license. 5 public IP addresses use 150 MB from your remote networks license; 10 public IP addresses use 300 MB from your remote network license.

**STEP 6** | **Add** the applications to provide secure inbound access.

You can configure up to 100 inbound applications for each group of provisioned public IP addresses (either 5 or 10). Enter a unique **Private IP** address, **Protocol**, and **Port** combination for each application. It is acceptable to use duplicate private IP addresses and ports for two applications, as long as you select **TCP** for one application and **UDP** for another application.

Provide the following values:

- Specify the name of the **Application**.
- Specify the **Private IP** address to use with this application.
- Specify the **Protocol** to use with the application (**TCP** or **UDP**).
- Specify the **Port** to use with the application.
- Choose whether you want to dedicate a single public IP address to a single application; to do so, select **Dedicated IP**.

Onboarding

Name: Secure-Inbound-Access-RN

ECMP Load Balancing: None

Location: Canada East

Bandwidth: 300 Mbps

IPsec Tunnel: Generic-IPsec-Tunnel-Default

Enable Secondary WAN

IPsec Tunnel: [Dropdown]

Static Routes | BGP | QoS | Inbound Access

Enable

Enable source NAT

Number of Public IPs: 5

Applications	Private IP	Protocol	Port	Dedicated IP
<input checked="" type="checkbox"/> www.example.com	10.10.10.2	TCP	443	<input type="checkbox"/>

+ Add - Delete

OK Cancel

**STEP 7** | Click **OK** to save your changes.

**STEP 8** | (Optional) If you selected an unsupported location, a window prompts you to a supported location. If required, select a supported location, then click **OK**.

**STEP 9** | **Save** and **Commit** your changes.

**STEP 10** | Wait approximately 30 minutes for Prisma Access to generate the public IP addresses; then select **Panorama > Cloud Services > Status > Network Details > Remote Networks** and make a note of the **Public Address** that is associated with the **App Name** for application you created.

If you selected **Dedicated IP**, find the single application that is associated with the **Public Address**.

Name	Service IP Address	Local IP Address	Static Subnet	Secure Inbound Apps	EBGP Router	Branch AS and Router
Secure-Inbound-Access-RN		dynamic	192.168.1.0/24	second / / 19.0.0.1:9090 www.example.com / 3 / / 192.168.1.10:22	10.100.101.2	
IN-RN-LA		dynamic	192.168.68.0/24	app15 / / 192.168.68.80:8010 app70 / / 10.10.10.56:8066 app79 / / 10.10.10.65:8075 app29 / / 10.10.10.14:8025 app32 / / 10.10.10.17:8028 app56 / / 10.10.10.42:8052 app6 / / 192.168.68.71:8001 more...	10.100.101.4	

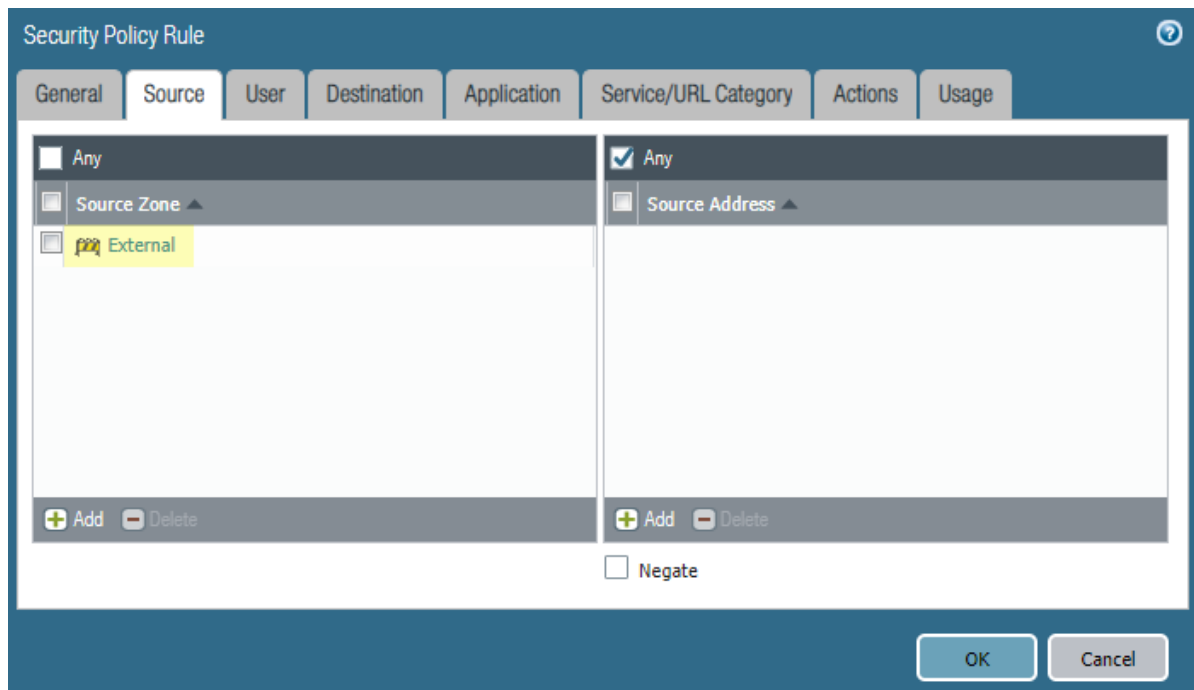
### STEP 11 | Create security policies to allow traffic from the inbound internet users.

Because Prisma Access' default security policy only allows untrust-to-untrust traffic, you need to configure security policies to allow untrust-to-trust (**external-to-internal**) traffic for your inbound access applications. Palo Alto Networks recommends that you limit the type of access you permit to inbound applications. The following examples provide access to SSH servers, web portals, and RDP servers.

1. Select **Policies > Security** and **Add** a policy.

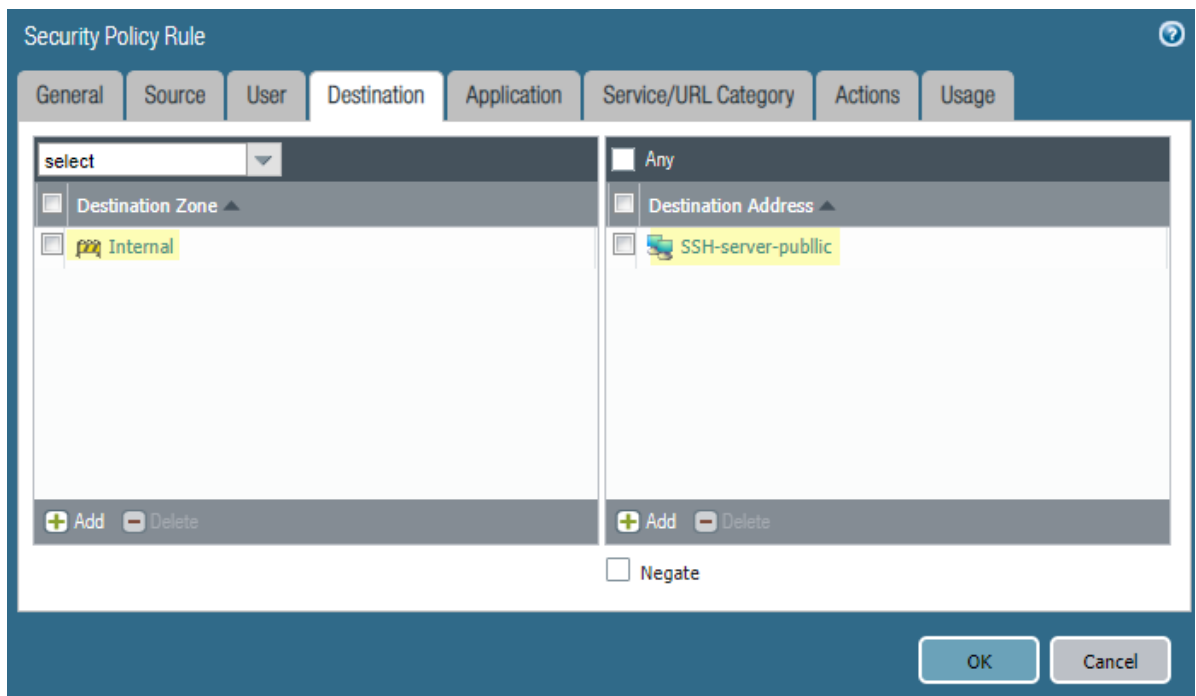
Be sure to create this policy under the **Remote\_Network\_Device\_Group** device group.

2. Select the **Source** traffic as **external**.

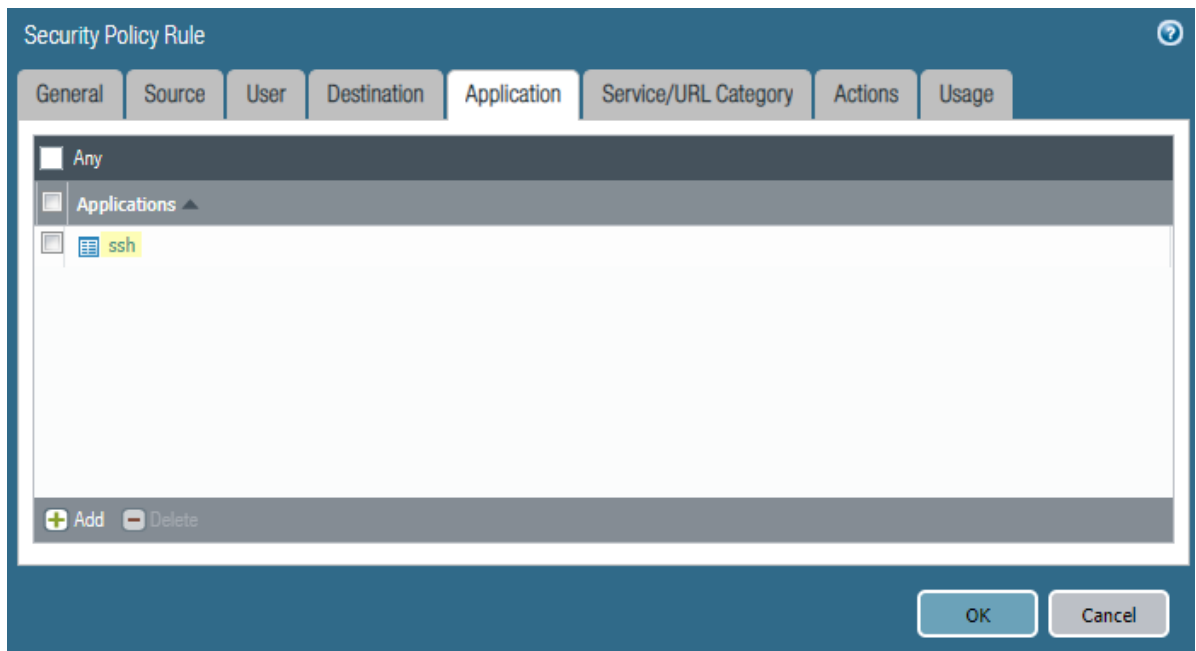


3. Create a policy to allow SSH server traffic by selecting the **Destination Zone** for destination traffic as **Internal** and specifying a **Destination Address** of **SSH-server-public**.

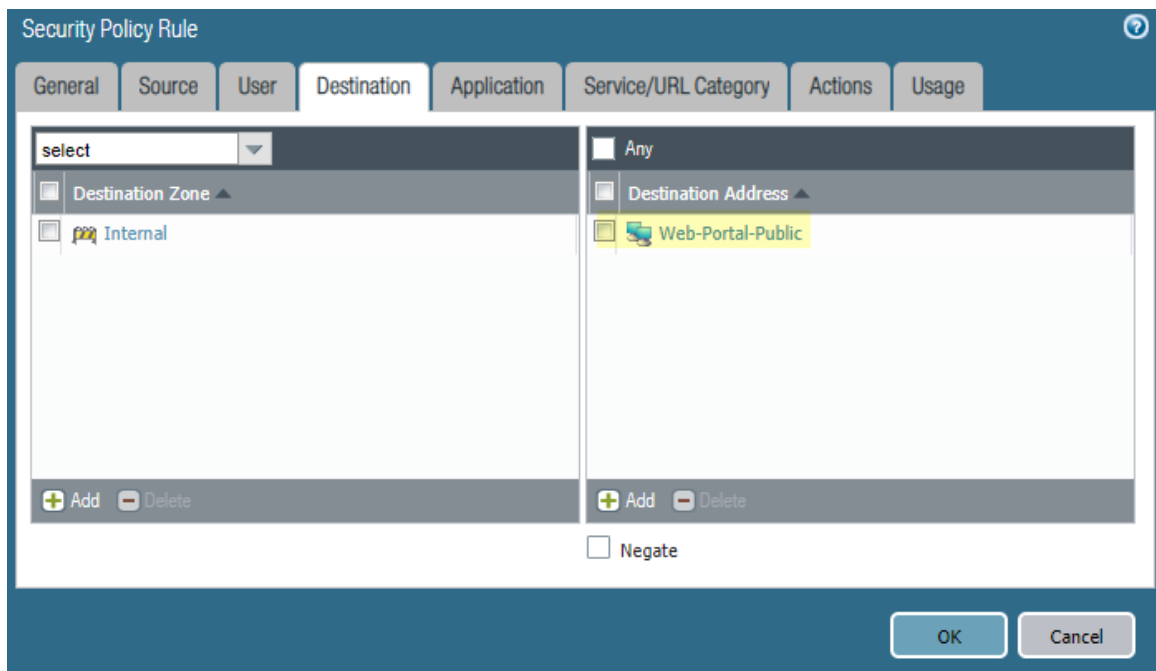




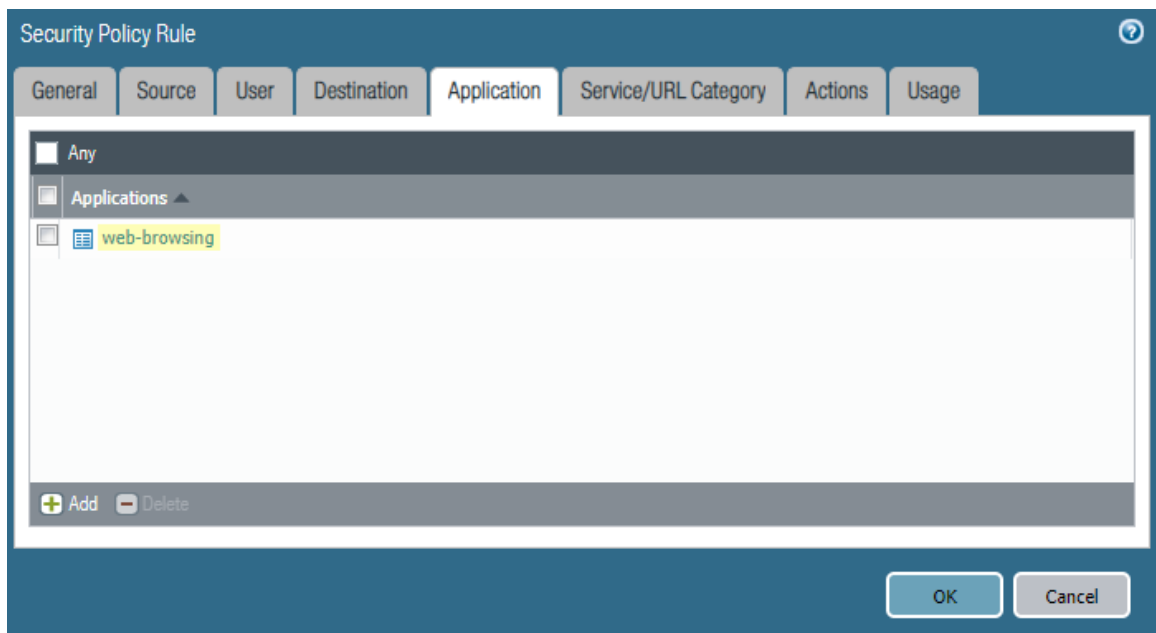
4. Select an **Application** of **ssh**.



5. Select a **Service/URL Category** of **application-default** to allow or deny applications based only their default ports as defined by Palo Alto Networks.
6. In **Actions**, select **Allow**.
7. Click **OK** to save the policy.
8. Create a policy to allow web portal access by creating a policy in the previous steps but substituting the following settings in the **Destination** and **Application** tabs:
  - Select a **Destination Address** of **Web-Portal-Public**.



- Select an **Application** of **web-browsing**.



9. Create a security policy for RDP server access, using the same settings as you did for the other policies but substituting **RDP-Server-Public** as the **Destination Address** and **webrdp** as the **Application**.

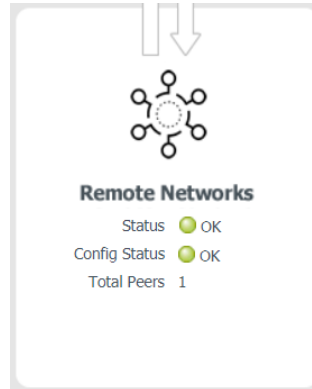
When complete, you have three different policies to allow SSH server access, web portal access, and RDP server access.

Name	Location	Tags	Type	Source				Destination		Application	Service	Action	Profile	Options	Target
				Zone	Address	User	HP Profile	Zone	Address						
1. genericpolicy	Remote_Network...	none	universal	pp	External	any	any	any	pp	Internal	any	any	allow		any
2. SSH Server Access	Remote_Network...	none	universal	pp	External	any	any	any	pp	Internal	SSH-Server-Public	ssh	application-default	allow	any
3. Web Portal Access	Remote_Network...	none	universal	pp	External	any	any	any	pp	Internal	Web-Portal-Public	web-browsing	application-default	allow	any
4. RDP Server Access	Remote_Network...	none	universal	pp	External	any	any	any	pp	Internal	RDP-Server-Public	webrdp	application-default	allow	any

**STEP 12** | Save and Commit your changes.

**STEP 13** | Check that the remote network connection is operational and correctly processing inbound traffic.

1. Select **Panorama > Cloud Services > Status > > Status > Remote Networks** and hover over the **Status** and **Config Status** areas to see the tunnel's status.



2. If you find issues, select **Panorama > Cloud Services > Status > > Monitor > Remote Networks**, select the location of the remote network tunnel in the map, and hover over the **Tunnel Status** area to determine the cause of the error.

A screenshot of the Palo Alto Networks Panorama interface showing the 'Remote Networks' monitoring page. The page title is 'Asia locations'. It shows a map of Asia with a green checkmark over India and a yellow warning icon over Hong Kong. Below the map is a table with columns: Location, Remote Peer, Allocated Bandwidth (Mbps), ECMP, Config Status, BGP Status, Tunnel Status, and Inbound Access. A tooltip is visible over the 'Warning' icon in the Tunnel Status column for the Hong Kong entry.

Location	Remote Peer	Allocated Bandwidth (Mbps)	ECMP	Config Status	BGP Status	Tunnel Status	Inbound Access
India West	IN-RN-MUMBAI	5	Disabled	In sync	Not Enabled	OK	Enabled
Hong Kong	RN-HONGKONG	100	Disabled	In sync	Not Enabled	Warning	Disabled

**Tunnel Status/Monitoring State**  
ipsec-hongkong Down/off



# Configure User-ID and User-Based Policies with Prisma Access

Prisma Access requires that you configure IP address-to-username mapping to consistently enforce user-based policy for mobile users and users at remote network locations. In addition, you need to configure username to user-group mapping if you want to enforce policy based on group membership.

You can then configure your deployment to allow Panorama to get the list of user groups retrieved from the group mapping, which allows you to easily select these groups from a drop-down list when you create and configure policies in Panorama.

The following sections provide an overview and the steps you perform to configure and implement User-ID in Prisma Access.

- > [Configure User-ID in Prisma Access](#)
- > [Configure User-ID for Remote Network Deployments](#)
- > [Configure Your Prisma Access Deployment to Retrieve Group Mapping](#)
- > [Redistribute User-ID Information Between Prisma Access and On-Premises Firewalls](#)
- > [Collect User and Group Information Using the Directory Sync Service](#)



---

# Configure User-ID in Prisma Access

This section provides the steps you perform to configure User-ID for Prisma Access.

**STEP 1** | Configure IP address-to-username mapping for your mobile users and users at remote network locations.

- For mobile users, the GlobalProtect agent in Prisma Access automatically performs User-ID mapping.
- For users at remote networks, [configure User-ID for your remote network locations](#) to map IP addresses to User IDs.

**STEP 2** | Configure username to user-group mapping for your mobile users and users at remote network locations.

To configure username-to-user group mapping for all users, enable group mapping [for mobile users](#) and [for users at remote networks](#) using an LDAP server profile.



*We recommend using a [Group Include List](#) in the LDAP server profile, so that you can specify which groups you want to retrieve, instead of retrieving all group information.*

**STEP 3** | Allow Panorama to use group mappings in security policies by configuring one or more next-generation on-premises or VM-series firewalls as a [Master Device](#).

If you don't configure a **Master Device** with a Prisma Access User-ID deployment, use [long-form distributed name \(DN\) entries](#) instead.

**STEP 4** | [Redistribute HIP information to Panorama](#).

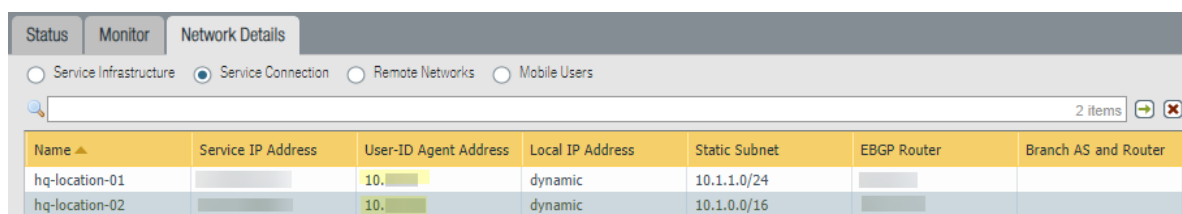
# Configure User-ID for Remote Network Deployments

The process for retrieving User-ID information for Prisma Access is similar to configuring User-ID for on-premise Palo Alto Networks next-generation firewalls. To configure User ID-to-IP address mapping for Prisma Access, use the following workflow.

## STEP 1 | Map IP addresses to users in Prisma Access.

- To use a Windows-based User-ID Agent for IP address-to-username mapping, create a dedicated service account [for the User-ID agent](#), then configure user mapping [using the Windows User-ID agent](#).
- To use the PAN-OS integrated User-ID Agent for IP address-to-username mapping, Create a dedicated service account [for the User-ID Agent](#), then configure User-ID using [the PAN-OS integrated User-ID agent](#).

If you use either a Windows or PAN-OS User-ID Agent, use the **User-ID Agent Address (Panorama > Cloud Services > Status > Network Details > Service Connection)** from Prisma Access in your User-ID agent configuration to configure your on-premise firewalls to retrieve User-ID mappings from the Prisma Access infrastructure. For more information about User-ID redistribution from Prisma Access to an on-premises firewall, see [Redistribute User-ID Information From Prisma Access to an On-Premise Firewall](#).



Name	Service IP Address	User-ID Agent Address	Local IP Address	Static Subnet	EBGP Router	Branch AS and Router
hq-location-01		10.	dynamic	10.1.1.0/24		
hq-location-02		10.	dynamic	10.1.0.0/16		

By default, the User-ID agent uses port 5007 to listen for User-ID information requests. Make sure that you implement security policies that allow User-ID traffic from this port between Prisma Access and the Active Directory server or User-ID Agent.



*You can also use the `paloalto-userid-agent App ID` to retrieve the information from the Windows domain controller; however, if you do this, you must decrypt the SSL traffic for User-ID.*

- To enable IP address-to-username mapping for users with client systems that aren't logged in to your domain servers—for example, users running Linux clients that don't log in to the domain—you can Map IP Addresses to Usernames [Using Authentication Portal](#) (formerly Captive Portal).

To authenticate users using MFA, SAML, or Authentication Portal, we recommend mapping a hostname to the **Captive Portal Redirect IP Address** in Prisma Access and associating it with your internal DNS servers. If you choose to use Kerberos single sign-on (SSO) with the authentication portal, the hostname is required. Alternatively, you can use the **Captive Portal Redirect IP Address** by itself to redirect users.

To find the **Captive Portal Redirect IP Address**, select **Panorama > Cloud Services > Status > Network Details > Service Infrastructure**. Prisma Access assigns this IP address from the infrastructure subnet IP address pool.



Infrastructure Subnet	Infrastructure BGP AS	Captive Portal Redirect IP Address	Tunnel Monitor IP Address	Loopback IPs
10.0.2.0/24		10.	10.	10.0.2.44 10.0.2.40 10.0.2.34 10.0.2.45 10.0.2.35 10.0.2.37 10.0.2.31 more...

- To enable IP address-to-username mapping using syslog listening, [Configure User-ID to Monitor Syslog Senders for User Mapping](#).
- To enable IP address-to-username mapping for users on Windows-based terminal servers, [Configure User Mapping for Terminal Server Users](#).
- To enable IP address-to-username mapping using an XML API, [Send User Mappings to User-ID Using the XML API](#).
- To enable IP address-to-username mapping without using an agent, [Configure User-ID for Prisma Access Using the PAN-OS Integrated User-ID Agent](#).

## STEP 2 | Allow Panorama to use group mappings in security policies.

- To [allow Panorama to retrieve group mapping information](#), add one or more next-generation firewalls to your deployment and then [configure the firewall as a Master Device](#).

We recommend using a Master Device in Prisma Access User-ID deployments, because it allows you to select groups from drop-down lists in policies that you create and configure in Panorama, which simplifies group-based policy configuration.

- If you don't use a master device, you can configure group-based policy by [specifying the full distinguished name \(DN\)](#) of the group.

## Configure User-ID for Prisma Access Using the PAN-OS Integrated User-ID Agent

The following procedure shows how to configure the PAN-OS integrated User-ID agent on the firewall for IP address-to-username mapping. The integrated User-ID agent performs the same tasks as the Windows-based agent with the exception of NetBIOS client probing. While we support WMI probing, we do not recommend it.

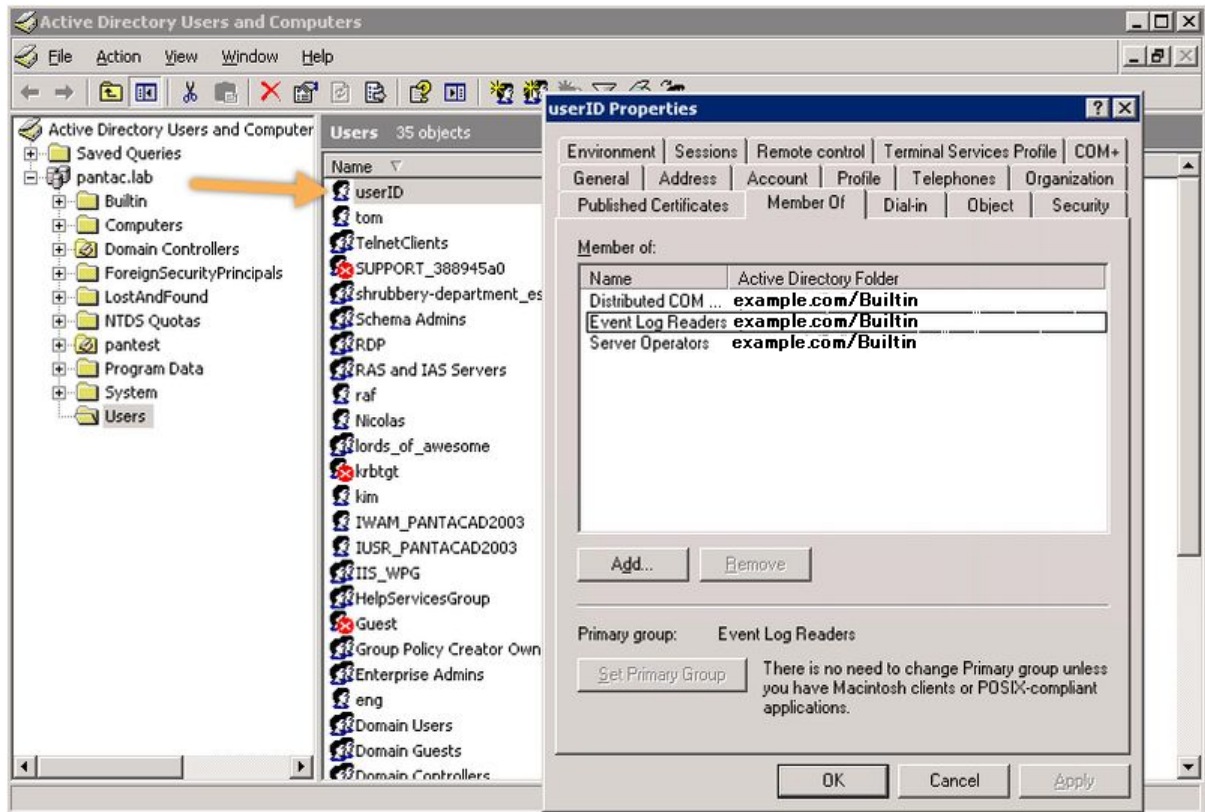
### STEP 1 | Create the User-ID service account in the Windows Active Directory (AD) server that is being used by the authentication server.


Be sure that the user you create is part of the following groups:

- Distributed COM Users
- Event Log Readers
- Server Operators



*Server Operator membership is only required if you enable monitoring of user sessions (Enable Session) when you configure server monitoring in Panorama in Step 5.b.*



 We recommend only making these group associations. You do not have to configure Domain Admin or Enterprise Admin privileges for the User-ID service account to work correctly. Giving privileges to the account that aren't required can give your network a larger attack surface.

## STEP 2 | Configure Windows Management Instrumentation (WMI) on the AD server.

The device uses WMI Authentication and you must modify the CIMV2 security properties on the AD server that connects to the device.

1. Open a command prompt window and run the `wmicmgmt.msc` command.
2. In the **WMI Control** pane, right-click **WMI Control**, choose **Properties**, and select the **Security** tab.

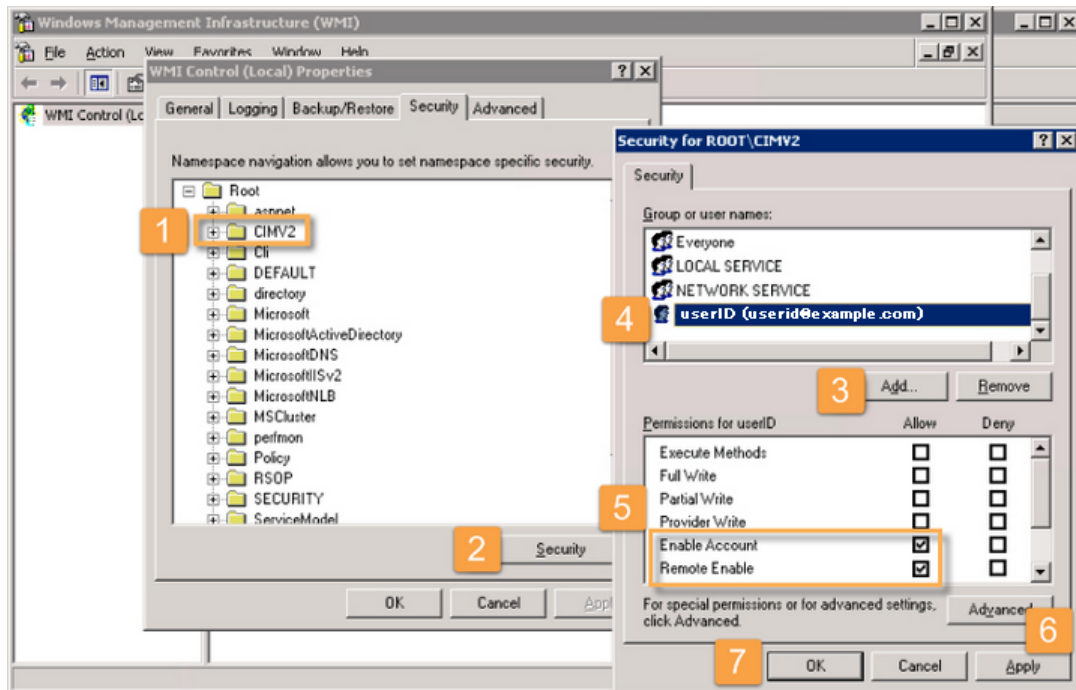


## STEP 3 | Make the following changes in the CIMV2 folder:

1. Select the **CIMV2** folder.
2. Click **Security**.
3. Click **Add**
4. Select the service account you created in Step 1.

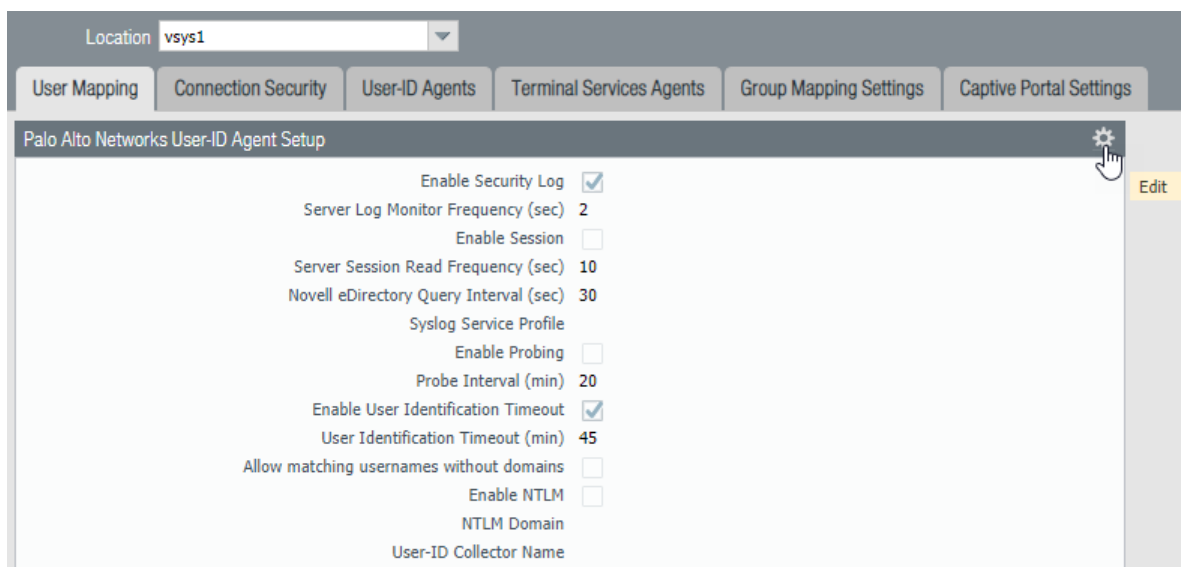
This example uses the **UserID** user with the email of **userid@example.com**.

5. Check **Allow** for the **Enable Account** and **Remote Enable** for the account you created.
6. Click **Apply**.
7. Click **OK**.



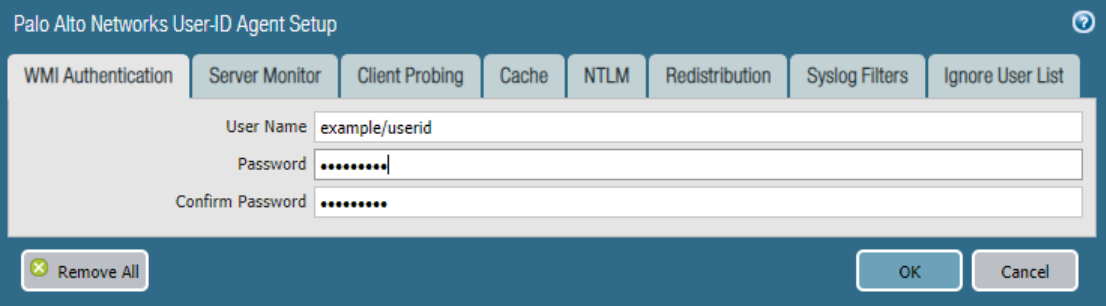
**STEP 4 |** In Panorama, select **Device > User Identification > User Mapping** and click the gear icon to edit the settings.

Be sure that you have selected the **Remote\_Network\_Template** at the top of the page.



**STEP 5** | Make the following changes to the Palo Alto Networks User-ID Agent Setup settings:

1. Select **WMI Authentication** and enter the domain and username (in the format *domain/username*) for the User-ID service account, along with a valid password.



The screenshot shows the 'Palo Alto Networks User-ID Agent Setup' dialog box with the 'WMI Authentication' tab selected. The 'User Name' field contains 'example/userid', the 'Password' field contains a masked password, and the 'Confirm Password' field also contains a masked password. At the bottom, there are buttons for 'Remove All', 'OK', and 'Cancel'.

2. (Optional) Select **Server Monitor** and change the default settings, if required.
  - To disable security log monitoring on Windows servers, deselect **Enable Security Log**.
  - To enable monitoring of user sessions on the monitored servers, select **Enable Session**.
3. (Optional) Select **Client Probing** and select **Enable Probing** to enable WMI probing.
4. Click **OK** to exit from the **Palo Alto Networks User-ID Agent Setup**.

**STEP 6** | If you have not done so already, click **Add** in the **Server Monitoring** area and add a **Name**, **Description**, **Type**, and **Network Address** for the server you need to monitor.

---

# Configure Your Prisma Access Deployment to Retrieve Group Mapping

After you configure User-ID mapping in Prisma Access, you need to be able to retrieve the current IP address-to-username and username-to-user group information for mobile users and users at remote networks. To allow the Panorama that manages your deployment to [retrieve group mapping information](#), you must add one or more next-generation firewalls to your deployment and then [designate the firewall as a Master Device](#). You then create policies in Panorama and enforce the policies using the list of user groups that Panorama retrieved from the Master Device.


Panorama cannot retrieve group mapping information in Prisma Access deployments without next-generation firewalls, because Prisma Access does not have any devices in its device groups that you can specify as a **Master Device**. If you have a standalone Prisma Access deployment, you can still [implement User-ID mapping in policies](#) by using long-form Distinguished Name (DN) entries.

- [Retrieve Group Mappings Using a Master Device](#)
- [Configure an on-premises or VM-Series Firewall as a Master Device](#)
- [Implement User-ID in Security Policies For a Standalone Prisma Access Deployment](#)

## Retrieve Group Mappings Using a Master Device

To allow Panorama to collect group mappings, you need to [add a device group](#), then designate one or more next-generation firewalls as a **Master Device**. You can configure either an on-premises firewall or a VM-series firewall as a master device.

- To allow Panorama to collect group mapping information from mobile users, create a device group that specifies the on-premises or VM-series firewall as the **Master Device** and specify this device group as a **Parent Device Group** of the **Mobile\_User\_Device\_Group** device group.
- To allow Panorama to collect group mapping information from users connected to remote networks, create a device group that specifies the on-premises or VM-series firewall as the **Master Device** and specify this device group as a **Parent Device Group** of the **Remote\_Network\_Device\_Group** device group.
- To allow Panorama to collect group mapping information from users or resources available through a service connection, create a device group that specifies the on-premises or VM-series firewall as the **Master Device** and specify this device group as a **Parent Device Group** of the **Service\_Conn\_Device\_Group** device group.

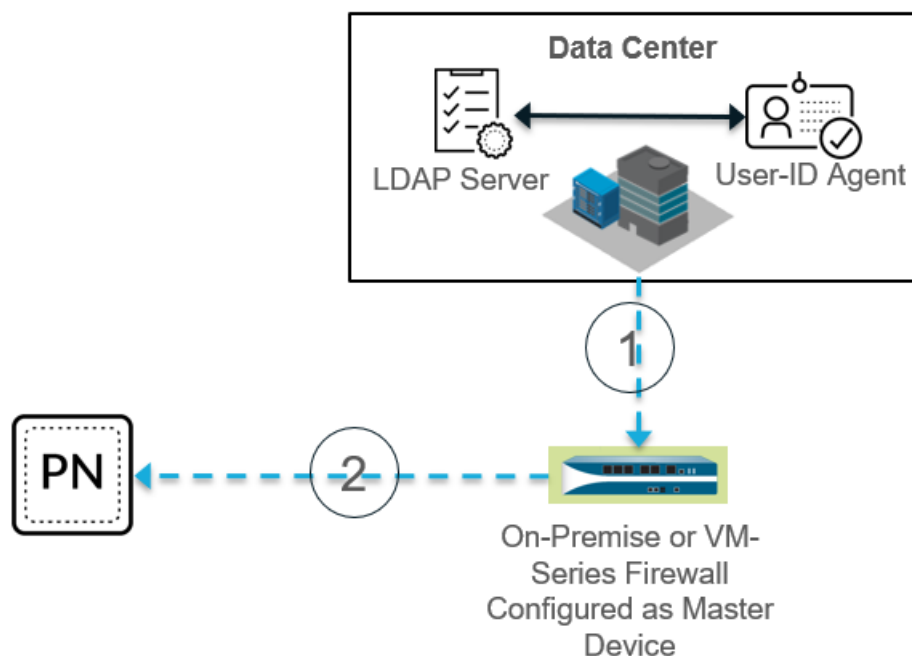
 *Auto-population of users and groups is only applicable to the parent device group that is associated with the master device. Auto-Population of users/groups is not applicable to the child device groups (the **Mobile\_User\_Device\_Group**, **Remote\_Network\_Device\_Group**, or **Service\_Conn\_Device\_Group** device groups). See [Configure an on-premises or VM-Series Firewall as a Master Device](#) for details.*

The Master Devices can serve as the termination point of a remote network connection or service connection, but this connection method is not required for the process to work, as shown in the following example. The following figure shows a User-ID deployment where the administrator has configured an on-premises device as a **Master Device**. Callouts in the figure show the process.

1. A next-generation on-premises or VM-series firewall that the administrator has configured as a Master Device retrieves the latest User-ID information from the LDAP server and User-ID agent in the data center.
2. Panorama gets the list of usernames, user group names, and group mapping information from the Master Device.



We recommend using a [Group Include List](#) in the LDAP server profile, so that you can specify which groups you want to retrieve, instead of retrieving all group information.



## Configure an on-premises or VM-Series Firewall as a Master Device

Use the following procedure to configure an on-premises or VM-series firewall as a Master Device.

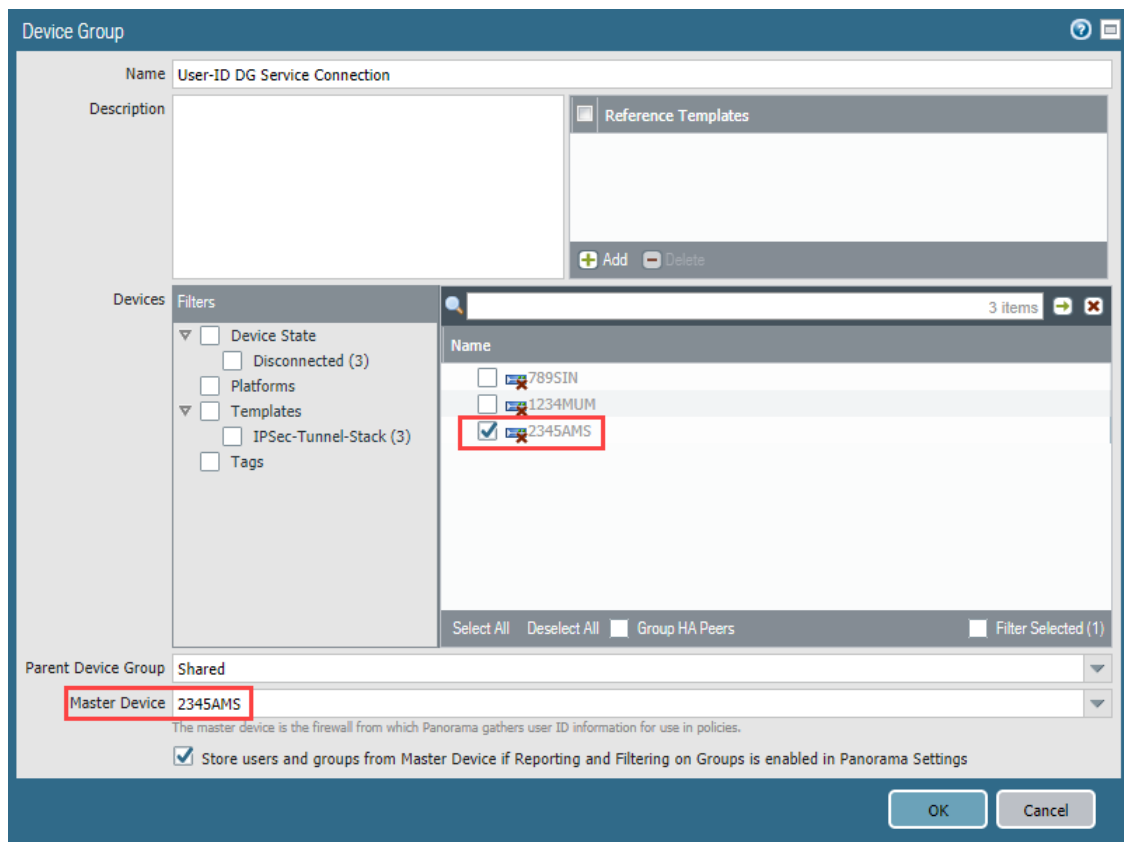
**STEP 1** | Create device groups for mobile users, remote networks, and service connection device groups as required, and specify the on-premises device as the **Master Device**.

1. Select **Panorama > Managed Devices > Device Groups**.
2. **Add** a new device group.
3. Enter a **Name** for the device group.
4. Leave the **Parent Device Group** as **Shared**.
5. In the **Devices** area, select the **Name** of the on-premises or VM-Series device that you want to set as the **Master Device**.
6. Select **Store user and groups from Master Device if Reporting and Filtering on Groups is enabled in Panorama Settings**.

This option allows Panorama to locally store usernames, user group names, and group mapping information that it receives from the Master Device.

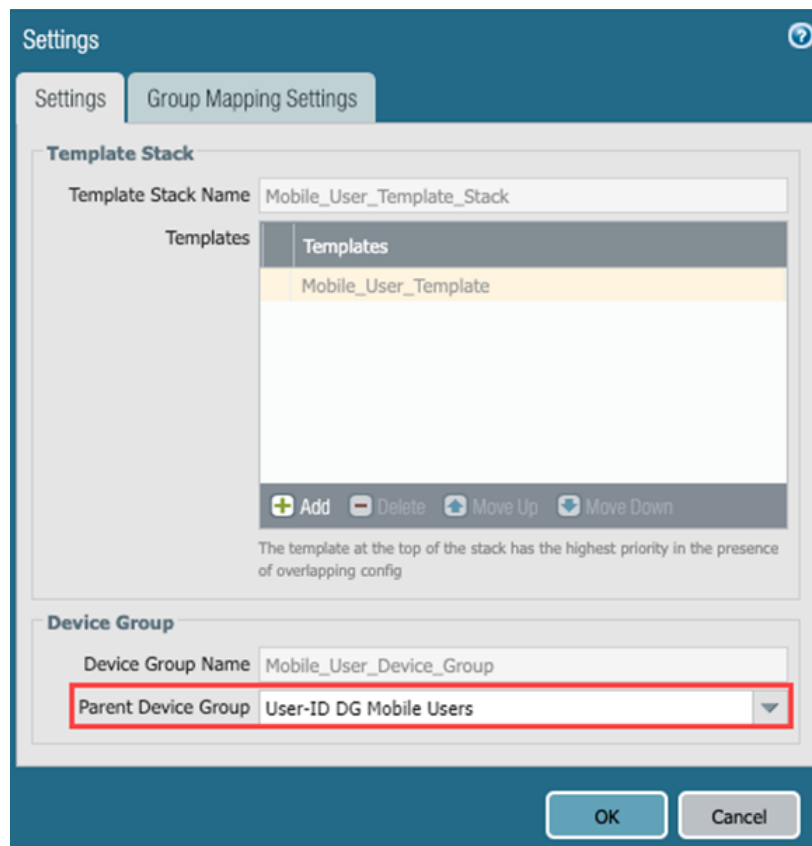
7. Click **OK**.

The following screenshot creates a Master Device to be used for the service connection.



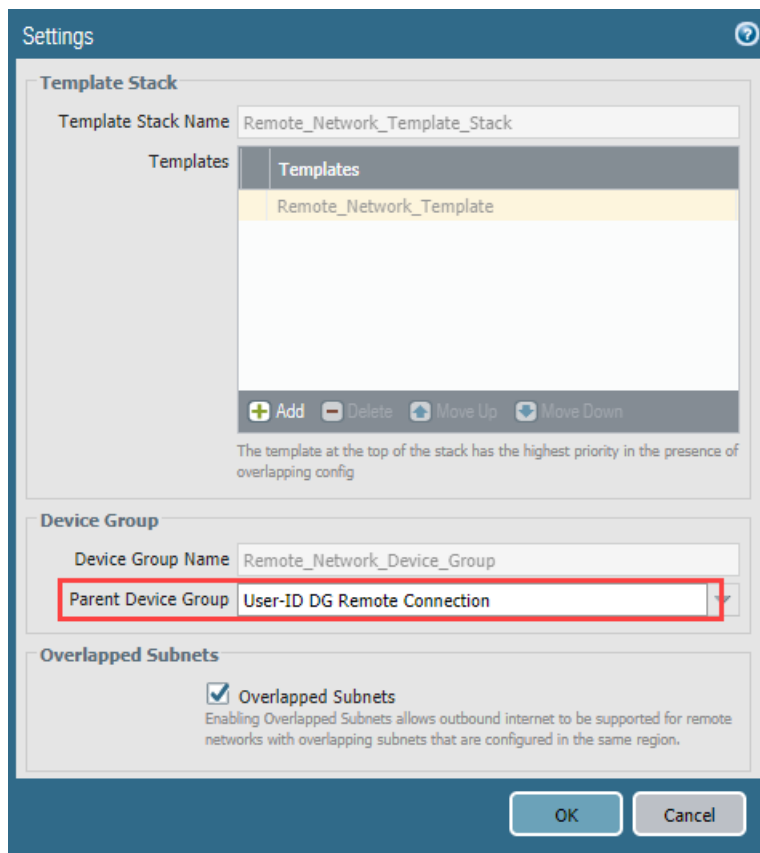
**STEP 2** | Associate the device groups you created for your Prisma Access mobile user, remote network, or service connection deployment.

- To associate the device group with a mobile user deployment, select **Panorama > Cloud Services > Configuration > Mobile Users** and edit the settings by clicking the gear icon in the **Settings** area and associate the device group you created for the service connection with the **Parent Device Group**.




- To associate the device group with a remote network connection, select **Panorama > Cloud Services > Configuration > Remote Networks** and edit the settings by clicking the gear icon in the **Settings** area and associate the device group you created for the remote network connection with the **Parent Device Group**.





- To associate the device group with a service connection, select **Panorama > Cloud Services > Configuration > Service Setup** and edit the settings by clicking the gear icon in the **Settings** area and associate the device group you created for the service connection with the **Parent Device Group**.

The screenshot shows the 'Settings' dialog box with three tabs: 'General', 'Internal Domain List', and 'Logging Service'. The 'Service Infrastructure' section contains fields for 'Infrastructure Subnet' (1.2.3.0/24) and 'Infrastructure BGP AS' (65534). The 'Template Stack' section shows a 'Template Stack Name' of 'Service\_Conn\_Template\_Stack' and a list of templates with 'Service\_Conn\_Template' selected. The 'Device Group' section shows a 'Device Group Name' of 'Service\_Conn\_Device\_Group' and a 'Parent Device Group' dropdown menu with 'User-ID DG Service Connection' selected. The 'Parent Device Group' dropdown is highlighted with a red box. At the bottom are 'OK' and 'Cancel' buttons.

 After you create a parent device group, Prisma Access automatically populates group mapping for the device group that is associated with the master device only. For the previous examples, the auto-population would occur only in the User-ID DG Mobile Users, User-ID DG Remote Connection, and User-ID DG Service Connection device groups, and would not populate to the Mobile\_User\_Device\_Group, Remote\_Network\_Device\_Group, or Service\_Conn\_Device\_Group device groups, respectively.

**STEP 3 |** Click **OK**.

## Implement User-ID in Security Policies For a Standalone Prisma Access Deployment

In a standalone Prisma Access deployment without a Master Device, you can use group-based policy using long-form DN entries in Panorama. Prisma Access uses the DN entries to evaluate the User-ID-based policies you have configured in Panorama.

---

For example, given a User named **Bob Alice** who works in **IT** for Organization **Hooli** in the United States, a matching security policy may have `ou=IT Staff,O=Hooli,C=US` if the policy is to be applied to all IT staff, or `CN=Bob Alice,ou=IT Staff,O=Hooli,C=US` if the policy is only to be applied to Bob Alice.

---

# Redistribute User-ID Information Between Prisma Access and On-Premises Firewalls

After you configure User-ID, you consistently enforce user-based policy for all mobile users and users at remote network locations by [configuring User-ID redistribution](#) to redistribute the User-ID mapping from Prisma Access to all next-generation firewalls that secure access to network resources.

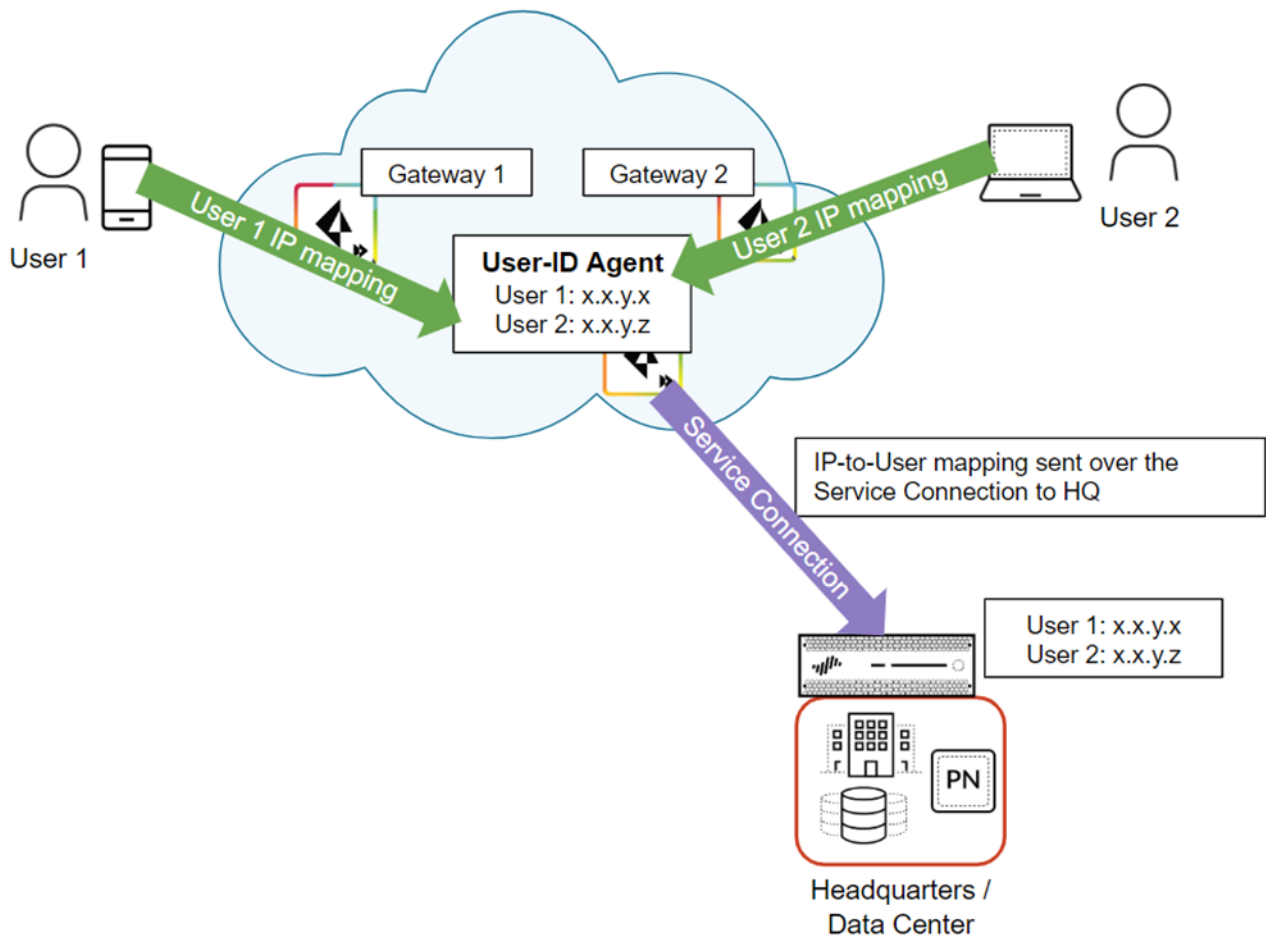
Use one the following methods to redistribute User-ID mapping to mobile users and users in remote networks from an on-premises next-generation firewall and vice versa, depending on the direction in which you want to redistribute the User-IDs:

- [Redistribute User-ID Information From Prisma Access to an On-Premise Firewall](#)
- [Redistribute User-ID Information From an On-Premises Firewall to Prisma Access](#)

## Redistribute User-ID Information From Prisma Access to an On-Premise Firewall

In cases where mobile users need to access a resource on a remote network location or HQ/data center and the resource is secured by an on-premises next-generation firewall with user-based policies, you must [redistribute User-ID mappings](#) from the Prisma Access mobile users and users at remote networks to the on-premises firewall. When the user connects to Prisma Access, it collects this user-to-IP address mapping and stores it.

The following figure shows two mobile users that have an existing IP address-to-username mapping in Prisma Access. Prisma Access then redistributes this mapping by way of a service connection to the on-premises firewall that secures the HQ/data center.



To redistribute User-ID mappings from Prisma Access to an on-premises firewall, complete the following steps.



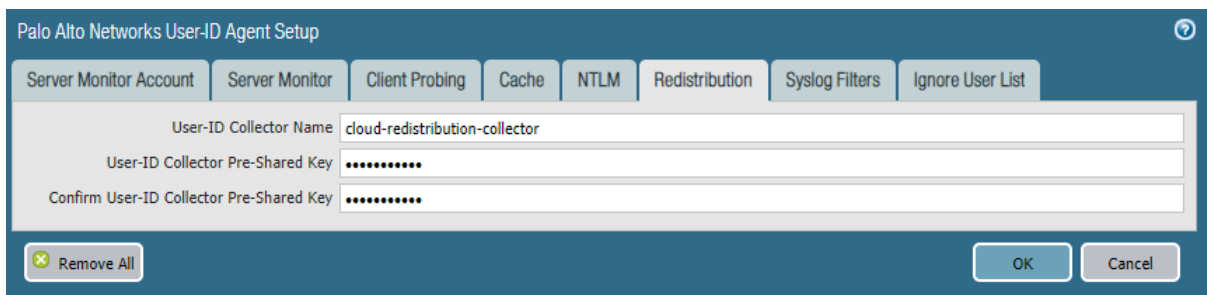
*Before you start this task, find the User-ID Agent Address in Prisma Access by selecting **Panorama > Cloud Services > Status > Network Details**, selecting the **Service Connection** radio button, and viewing the information in the **User-ID Agent Address** field.*

#### STEP 1 | Configure Prisma Access as a User-ID agent that redistributes user mapping information.

1. In the Panorama that manages Prisma Access, select **Device > User Identification > User Mapping > Palo Alto Networks User-ID Agent Setup** (for Panorama 9.1.x Appliances) or **Device > Data Redistribution > Collector Settings** (for Panorama 10.x appliances).

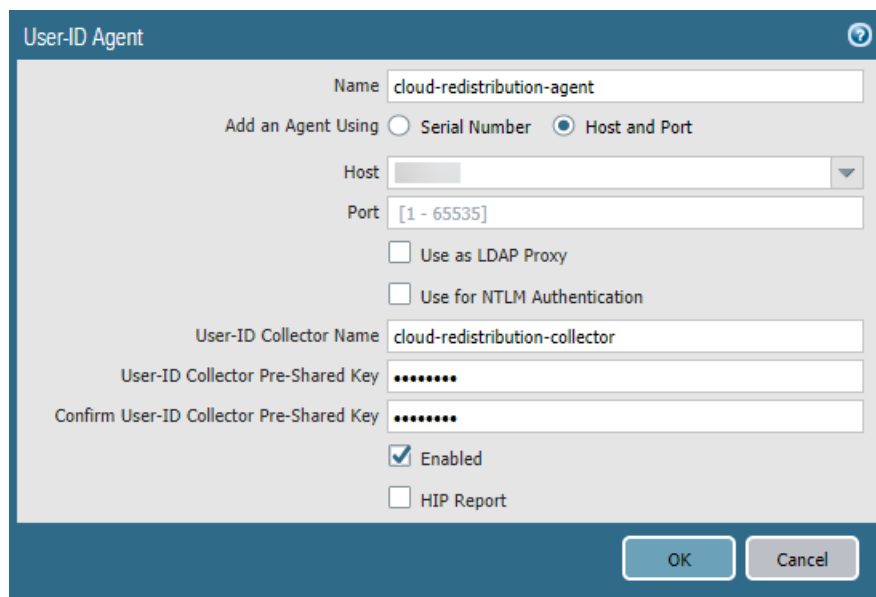
Make sure that you have selected the **Service\_Conn\_Template** in the **Templates** drop-down at the top of the page. The User-ID agent in Prisma Access receives its User-ID mapping from the domain controller in the data center by way of the service connection.

2. Click the gear icon to edit the settings.
3. Select **Redistribution** (Panorama 9.1.x Appliances only).
4. Provide a **User-ID Collector Name** and a **User-ID Collector Pre-Shared Key** to identify Prisma Access as a User-ID agent.
5. Click **OK** to save your changes.



**STEP 2 |** Configure the on-premises firewall to collect the User-ID mapping from Prisma Access.

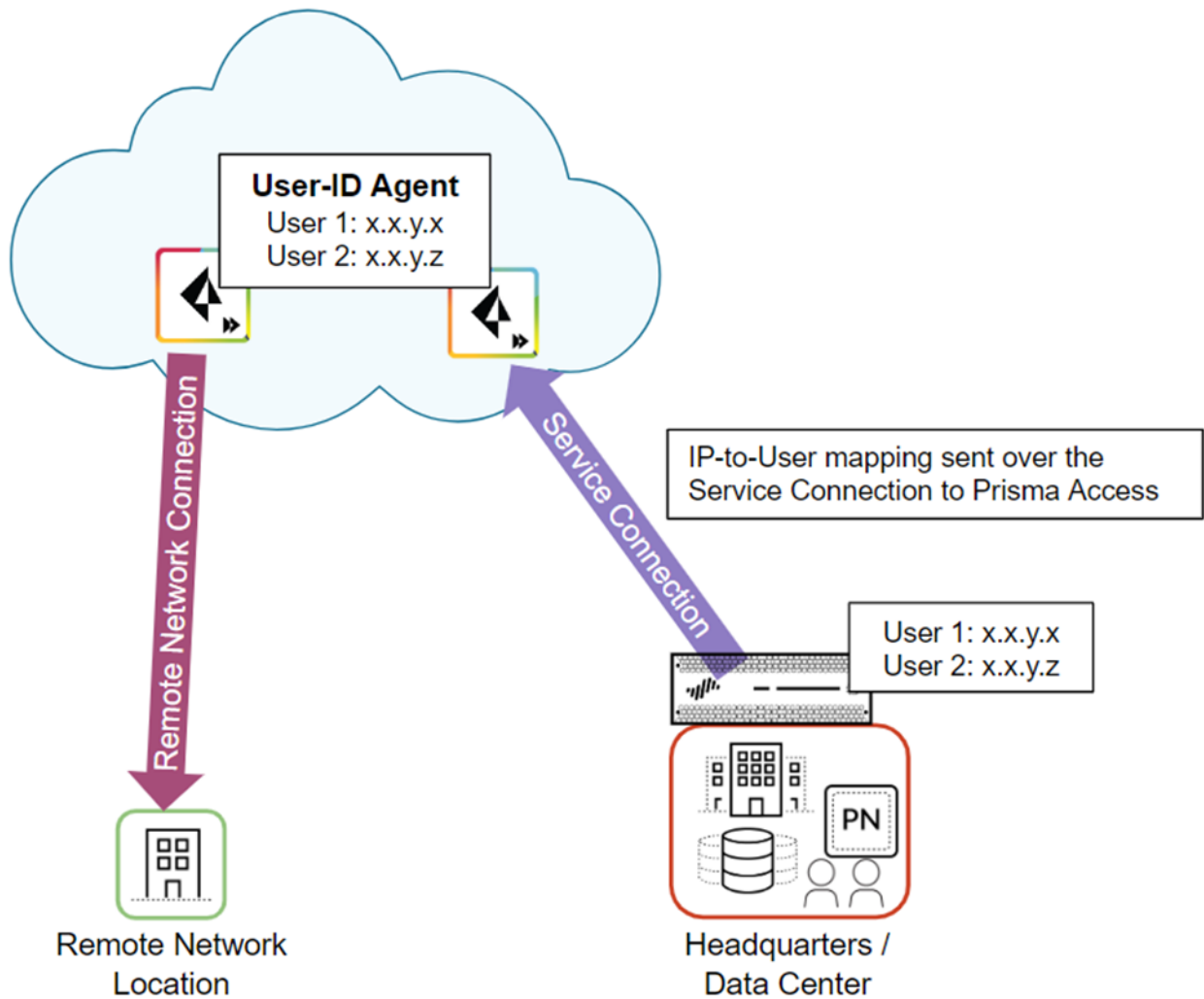
1. From the on-premises firewall, select **Panorama > User Identification > User-ID Agents** (for 9.1.x Panorama appliances) or **Panorama > Data Redistribution > Agents** (for Panorama 10.x appliances).
2. **Add** a User-ID Agent and give it a **Name**.
3. Select **Host and Port**.
4. Enter the **User-ID Agent Address** from Prisma Access in the **Host** field.
5. Enter the **User-ID Collector Name** and **User-ID Collector Pre-Shared Key** for the Prisma Access collector you created in Step 1.
6. Click **OK**.
7. Repeat these steps for each service connection.



## Redistribute User-ID Information From an On-Premises Firewall to Prisma Access

In cases where users are at a branch location or HQ that is secured by an on-premises next-generation firewall with user-based policies, and they need to access resources at another branch location that you have secured with Prisma Access, you must [redistribute User-ID mappings](#) from the on-premises firewall to Prisma Access.

The following figure shows an HQ/Data center with an on-premises next-generation firewall with existing IP address-to-username mapping. Prisma Access connects to the firewall with a service connection, and the on-premises firewall redistributes the mapping to Prisma Access.



To redistribute User-ID mappings from an on-premises firewall to Prisma Access, complete the following steps.

**STEP 1 |** Configure the on-premises firewall to [redistribute User-ID information](#) to Prisma Access.

1. From the on-premises firewall, select **Device > User Identification > User Mapping > Palo Alto Networks User-ID Agent Setup** (for Panorama 9.1.x Appliances) or **Device > Data Redistribution > Collector Settings** (for Panorama 10.x appliances).
2. Click the gear icon to edit the settings.
3. Select **Redistribution** (9.1.x devices only).
4. Provide a **User-ID Collector Name** and a **User-ID Collector Pre-Shared Key** to identify the on-premises firewall as a User-ID agent.
5. Click **OK** to save your changes.

**STEP 2 |** Configure Prisma Access to collect the User-ID mapping from the on-premises firewall.

1. From the Panorama that manages Prisma Access, select **Panorama > User Identification > User-ID Agents** (for 9.1.x Panorama appliances) or **Panorama > Data Redistribution** (for Panorama 10.x appliances).

Make sure that you have selected the **Remote\_Network\_Template** in the **Templates** drop-down at the top of the page.

- 
2. **Add** a User-ID Agent and give it a **Name**.
  3. Select **Host and Port**.
  4. Enter the IP address of the MGT interface or service route that the firewall uses to send user mappings in the **Host** field.

For the MGT interface, you can enter a hostname instead of the IP address.

5. Enter the **User-ID Collector Name** and **User-ID Collector Pre-Shared Key**, using the values for the collector you created for the on-premises firewall in Step 1.
6. Click **OK**.



---

# Get User and Group Information Using Directory Sync

Prisma Access retrieves user and group information from your organization's Active Directory (AD) to enforce user- and group-based policy. You can simplify the retrieval of user and group information by using Palo Alto Networks' [Directory Sync](#) service.

In addition to simplifying user and group information retrieval, integrating Directory Sync with Prisma Access can free up the bandwidth and load on your AD. Without Directory Sync integration, all the remote networks and mobile users' nodes individually communicate with your AD using the service connection.

You can use Directory Sync to retrieve user and group information for Prisma Access for mobile users, remote networks, or both, by completing the following steps.

The Directory Sync integration with Prisma Access has the following implementation restrictions:

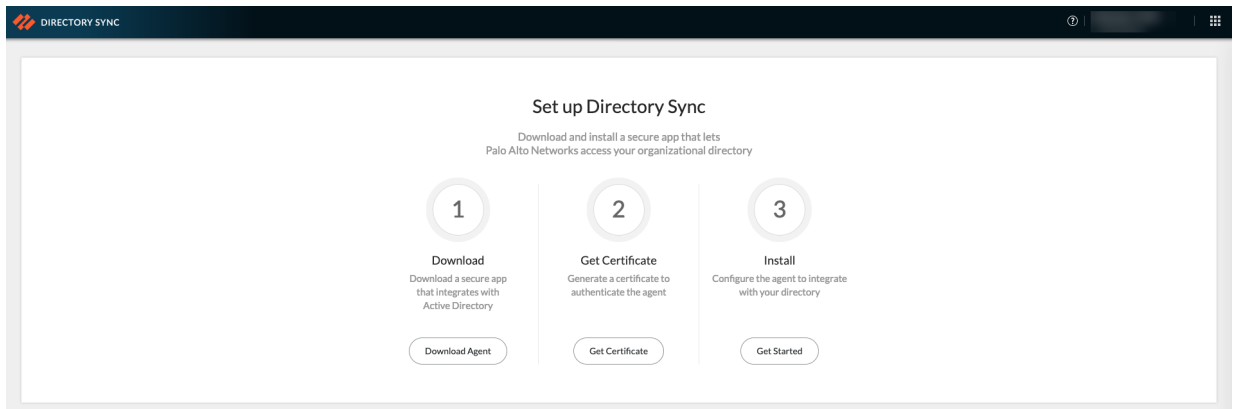
- Make sure that the groups you use with Directory Sync do not have any of the following special characters, because Prisma Access does not support the use of following special characters in groups and commit operations will fail:
  - " (Double quotes)
  - ' (Apostrophe)
  - < (less than sign)
  - > (greater than sign)
  - & (ampersand)
- If you associate Directory Sync with Prisma Access, your user names must use the NetBIOS format that includes the domain. You can specify usernames in email format (*username@domain*), NetBIOS \sAMAccountName format, or User Principal Name (UPN) format (*username@domain.com*).
- Group names must be in the **distinguishedName** format (for example, **CN=Users,CN=Builtin,DC=Example,DC=com**).
- Directory Sync does not apply any settings you specify in the [group include list](#) (**Device > User Identification > Group Mapping Settings > Group Include List**); instead, it retrieves user and group information from your entire configuration, including groups used in all device groups and templates.

**STEP 1 |** [Create a Directory Sync instance](#) for Prisma Access, and make a note of the instance name.

When you [activate Directory Sync](#), it creates an instance. You use the instance name when you associate Directory Sync with Prisma Access in a later step. Optionally, if you need to create a separate instance for Prisma Access, create it and make a note of the instance name.

**STEP 2 |** Set up [Directory Sync](#) on your AD.

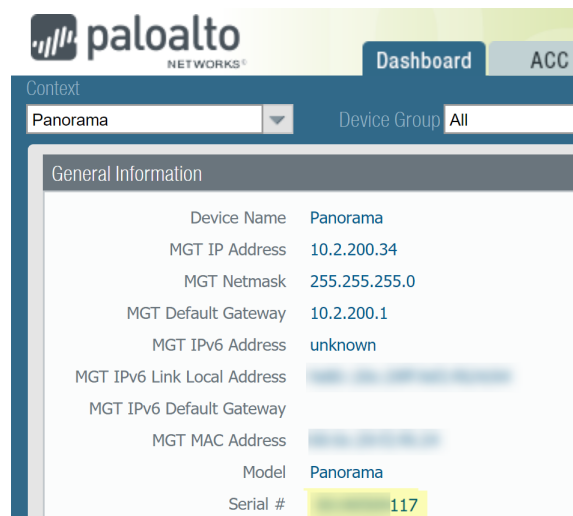
This process includes [installing and configuring a Directory Sync Agent](#) to communicate with your on-premises Active Directory and configuring mutual authentication between the Directory Sync service and the agent.



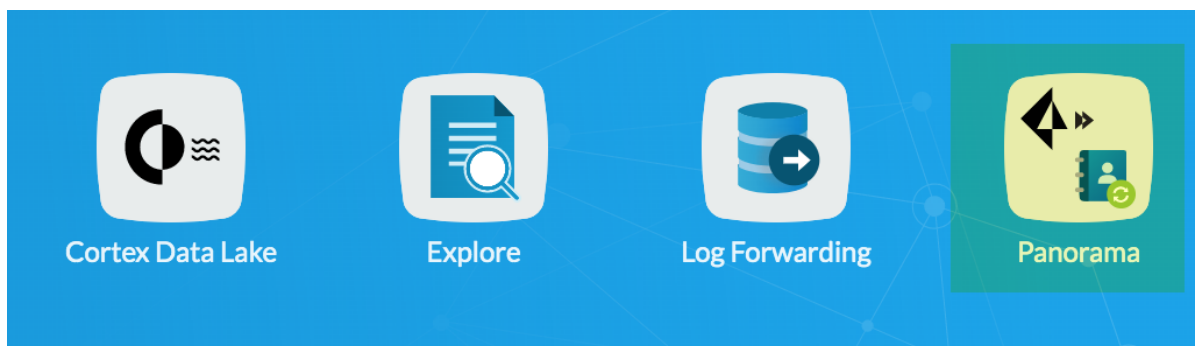
**STEP 3 |** Associate the Panorama that manages Prisma Access with Directory Sync in the hub.

Directory Sync integration with Prisma Access is not supported in a multi-tenant environment.

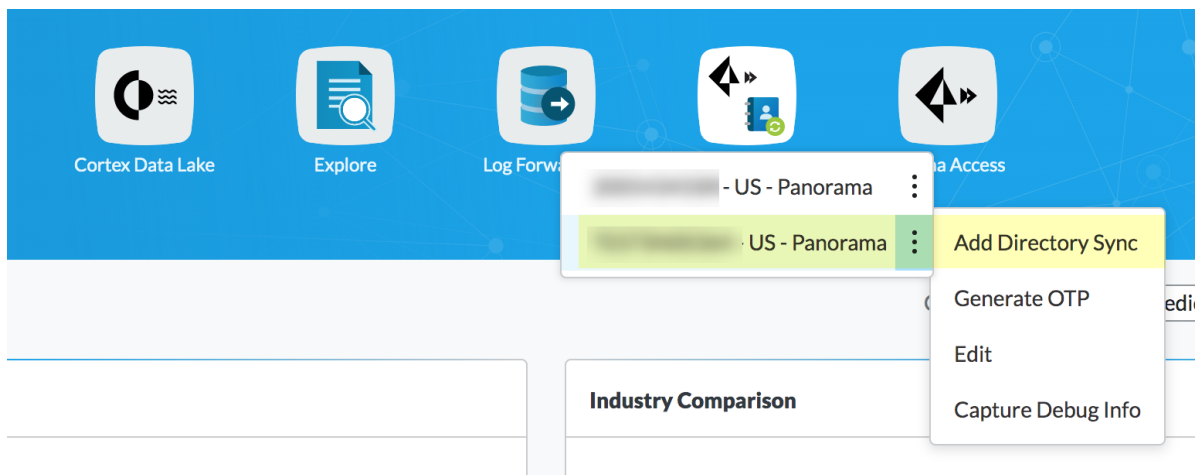
1. Find the serial number of the Panorama that manages Prisma Access by selecting the **Dashboard** and noting the **Serial #** that displays.



2. Log in to the Palo Alto Networks [hub](#) and select **Panorama**.

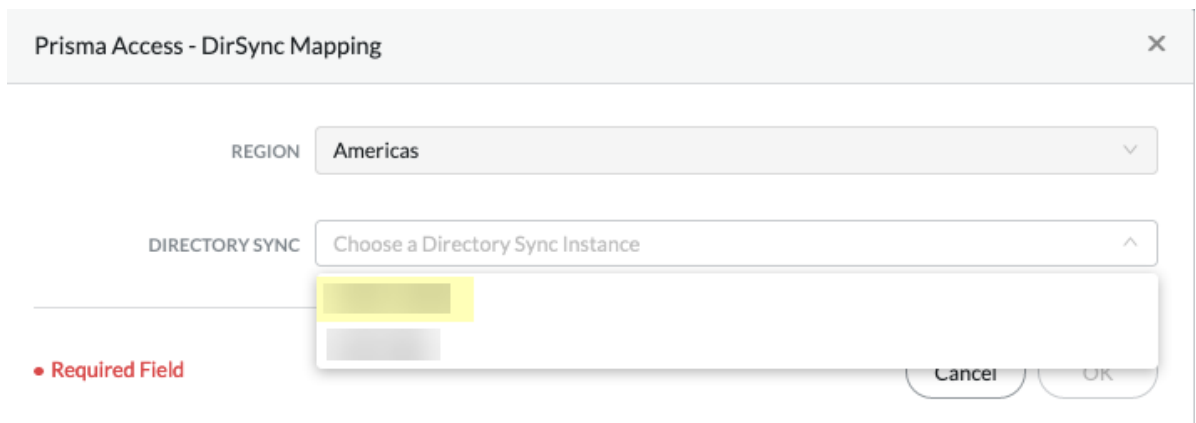


3. Find the serial number of the Panorama that manages Prisma Access, select it, then select **Add Directory Sync**.



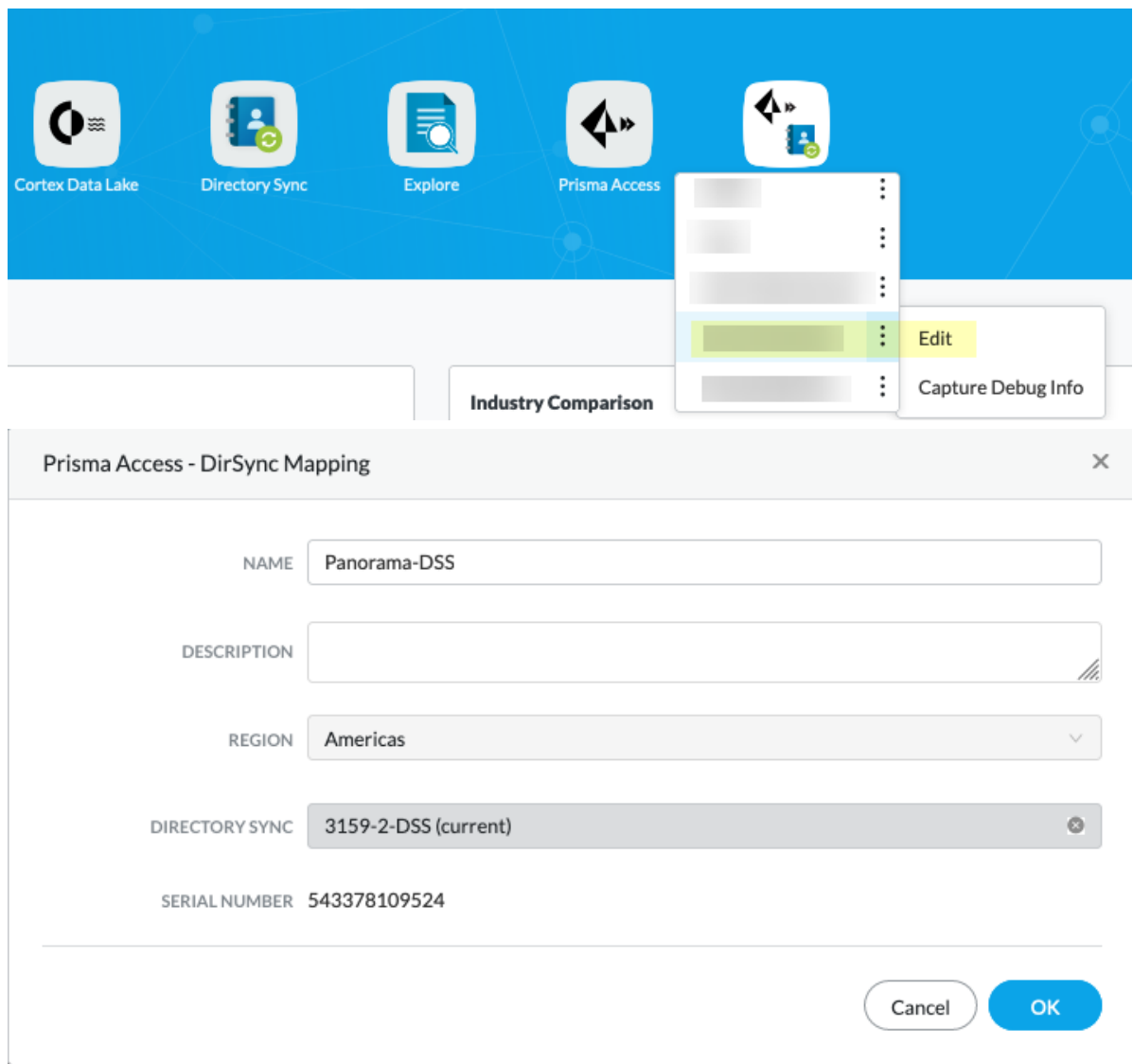
4. Enter the **Directory Sync** instance you retrieved in Step 1.

You do not need to select the **Region**; Directory Sync uses the same region that Prisma Access uses for [Cortex Data Lake](#).



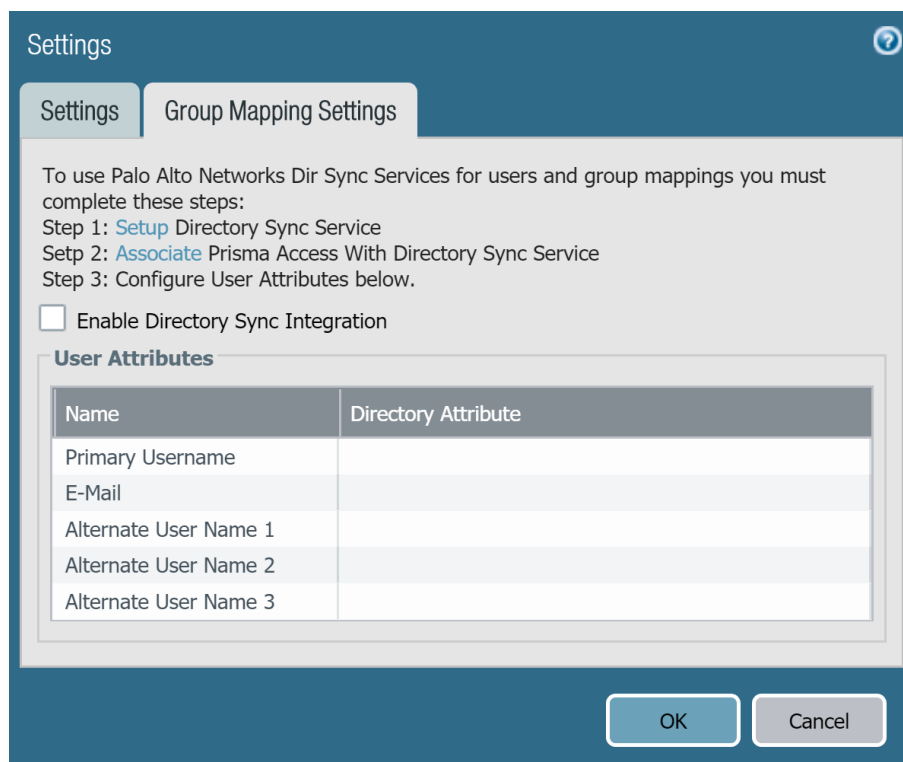
5. Click **OK** when complete.
6. (**Optional**) If you need to edit an existing Directory Sync instance after you create it, select **Prisma Access - DirSync Mapping**, select the Panorama's serial number, select **Edit**, and enter the following information in the window that displays:
  - Enter a **Name** for the Directory Sync - Prisma Access mapping.
  - Optionally, enter a **Description** for the mapping.
  - Select the **Directory Sync** instance name that you noted in Step 1.

The **Region** and **Serial Number** fields populate automatically.

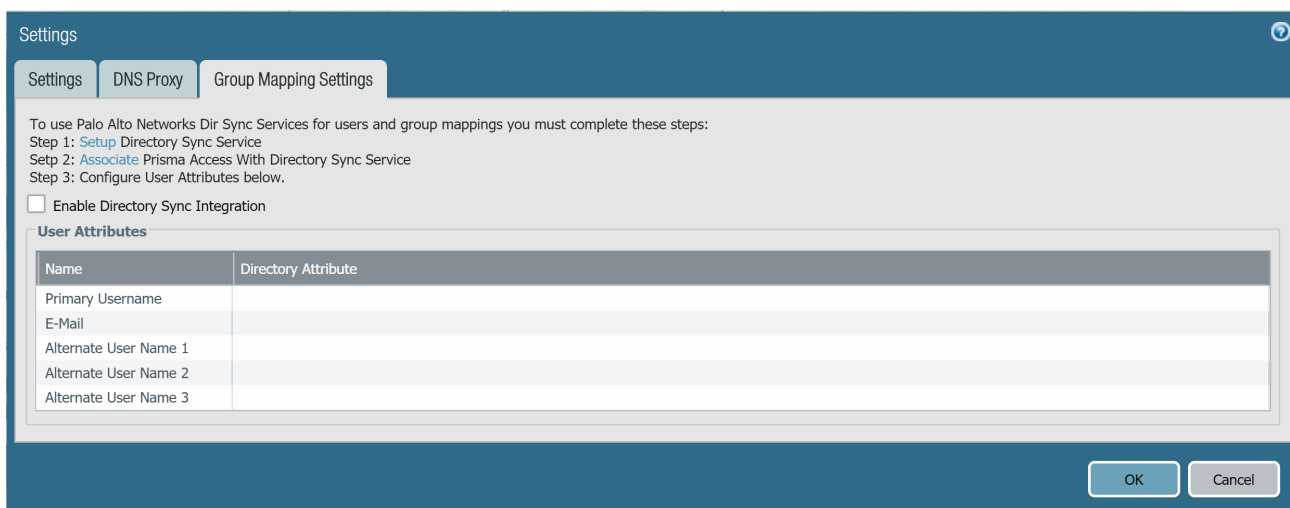


#### STEP 4 | Enable Directory Sync on Prisma Access.

1. On the Panorama that manages Prisma Access, select one of the following tabs:
  - To configure Directory Sync for Prisma Access for mobile users, select **Panorama > Cloud Services > Configuration > Mobile Users**, select the gear icon to edit the settings, then select **Group Mapping Settings**.



- To configure Directory Sync for Prisma Access for remote networks, select **Panorama > Cloud Services > Configuration > Remote Networks**, select the gear icon to edit the settings, then select **Group Mapping Settings**.



2. Select **Enable Directory Sync Integration** to enable Directory Sync with Prisma Access.
3. Enter the following information:
  - Enter the **Primary Username** (the logon name attribute for the user, such as **userPrincipalName** or **sAMAccountName**). This field is required.
  - (Optional) Enter the **E-Mail** attribute (such as **mail**).
  - (Optional) If you use alternate name attributes for the user, enter them. You can enter up to three alternate user names (**Alternate User Name 1**, **Alternate User Name 2**, and **Alternate User Name 3**).
4. Click **OK** when complete.

**STEP 5 | Commit and push (Commit > Commit and Push) your changes.**

**Commit and Push**

Doing a commit will overwrite the Panorama running configuration with the commit scope.

Commit All Changes    Commit Changes Made By: (1) admin

Commit Scope	Location Type
Remote_Network_Device_Group	Device Groups
Mobile_User_Device_Group	Device Groups
other	

Preview Changes   Change Summary   Validate Commit    Group By Location Type

Push Scope	Location Type ▲	Entities
Remote_Network_Device_Group	Prisma Access	
Mobile_User_Device_Group	Prisma Access	

Edit Selections   Remove Selections   Validate Device Group Push   Validate Template Push    Group By Location Type

Note: By default, devices that are associated with the entities in the commit scope are selected, however you may customize the selection.

Enter a description

**Commit And Push**   **Cancel**

# ***Redistribute HIP Information and View HIP Reports***

Use the topics in this section to understand how HIP redistribution works in Prisma Access, including some example use cases, and learn how to configure HIP redistribution and view HIP reports from Panorama.

- > [Redistribute HIP Information with Prisma Access](#)
- > [View HIP Reports from Panorama](#)





---

# Redistribute HIP Information with Prisma Access

To ensure consistent Host Information Profile (HIP) policy enforcement and to simplify policy management, you can [redistribute HIP information](#) received from mobile users and users at remote networks that use the GlobalProtect app from Prisma Access to other gateways, firewalls, and Panorama appliances in your enterprise, including the Panorama that manages Prisma Access. To do so, you enable and configure HIP redistribution in Prisma Access.

- [HIP Redistribution Overview](#)
- [Use Cases for HIP Redistribution](#)
- [Configure HIP Redistribution in Prisma Access](#)

## HIP Redistribution Overview

When a mobile user whose endpoint has the GlobalProtect app installed connects to Prisma Access, Prisma Access collects the user's HIP information from the endpoint's GlobalProtect app, which makes the HIP report available in Prisma Access.



*To use HIP redistribution, users must have the GlobalProtect app installed on their endpoint. While Prisma Access supports [Clientless VPN](#), you cannot redistribute HIP information for Clientless VPN users.*

HIP redistribution is applicable to both mobile users and users at remote networks. However, for users at remote networks, an on-premises gateway must detect that the user is internal to the organization's network using [internal host detection](#) before the on-premises gateway can send HIP information to Prisma Access.



*In Prisma Access, you configure internal host detection when you [configure your mobile user deployment](#).*

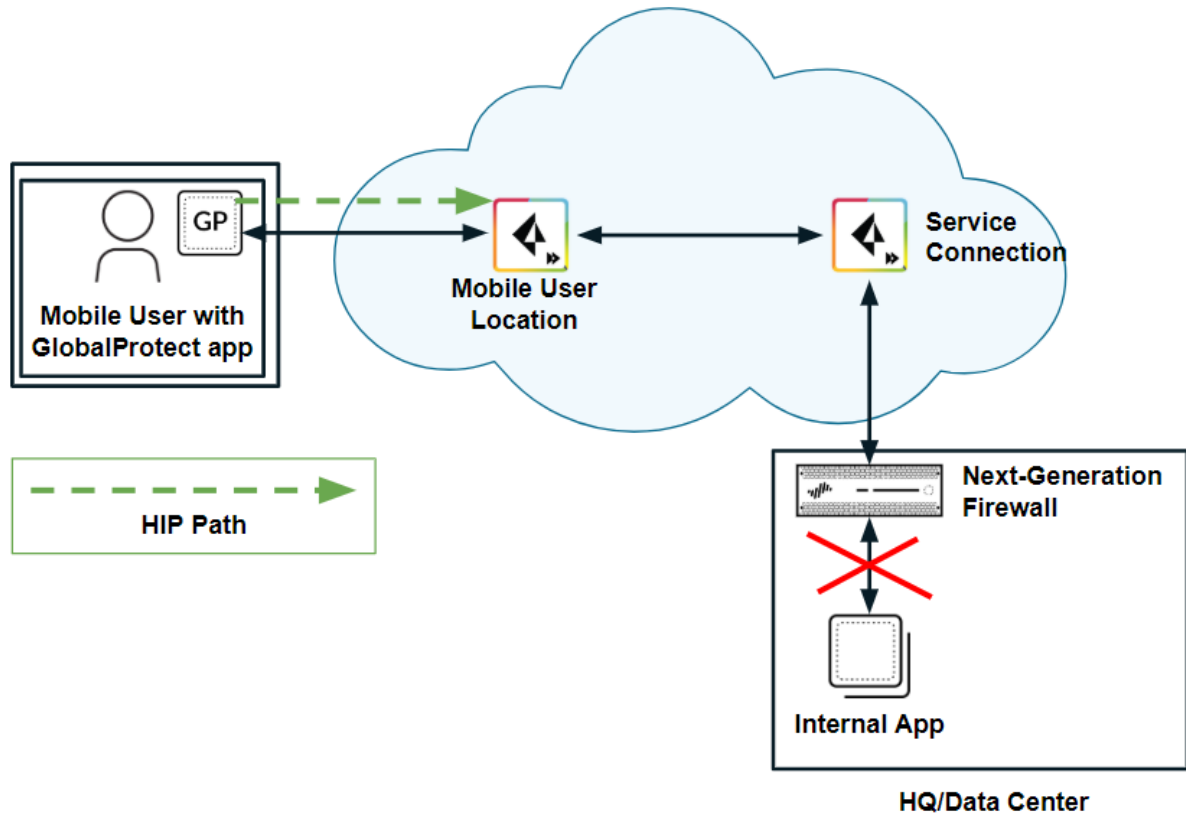
To assure consistent policy enforcement, you can use HIP redistribution to allow Prisma Access to [distribute users' HIP information](#) to other Panorama appliances, gateways, firewalls, and virtual systems in your deployment, as well as distribute HIP information from those devices to Prisma Access [in some cases](#). This ability allows you to consistently apply HIP-based policy enforcement for users' traffic, including policies for internet-bound traffic or for traffic that is accessing an internal application or resource in your organization's headquarters or data center. Redistributing HIP information to the Panorama appliance also lets you [view detailed HIP information](#) for Prisma Access users from that appliance.

## Use Cases for HIP Redistribution

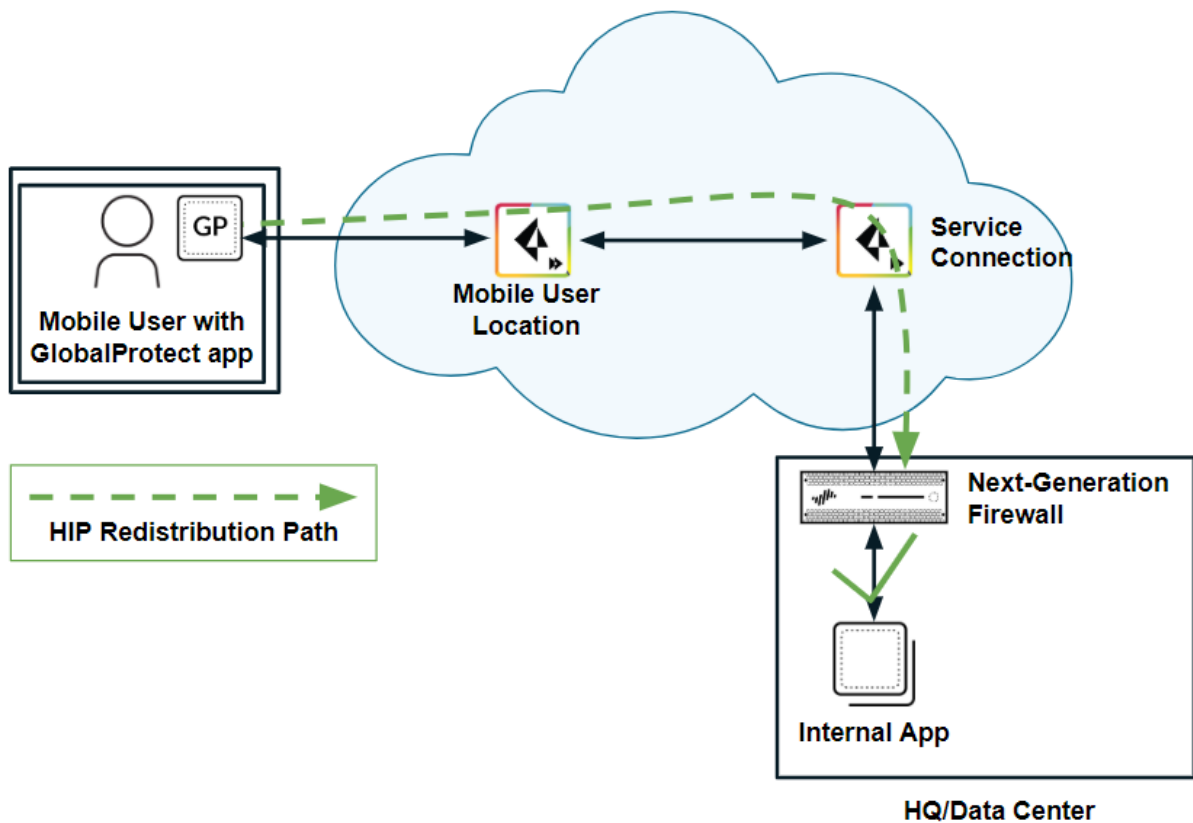
The following section describes some common Prisma Access deployments where HIP redistribution is useful for consistent policy enforcement and HIP report viewing.

- **HIP redistribution from Prisma Access to a next-generation firewall**—If you have a next-generation firewall in your organization's data center or headquarters location, and have configured that firewall with HIP-based security policies, you cannot enforce those policies for Prisma Access mobile users until you redistribute HIP redistribution from Prisma Access to the firewall.

The following figure shows a mobile user whose endpoint is protected with the GlobalProtect app. The user attempts to access an internal app at an HQ/data center whose access is controlled by a next-generation firewall with HIP-based security policies. When the user logs in to the GlobalProtect app, the app collects HIP information and sends it to Prisma Access; however, Prisma Access does not redistribute this information to the on-premises firewall. Since the firewall does not have the user's HIP information, it blocks the user's access to the app.



HIP redistribution allows you to distribute the mobile users' HIP information to the on-premises firewall. The firewall can then check the user's HIP information against its configured security policies and grant the user access to the app.



To redistribute HIP information from Prisma Access to the firewall, you [allow Prisma Access to redistribute HIP information](#), then **Add a User-ID Agent** (Panorama > User Identification > User-ID Agents for 9.1.x Panorama appliances or Panorama > Data Redistribution for Panorama 10.x appliances) on the firewall, and specify the Prisma Access User-ID Agent Address (Panorama > Cloud Services > Status > Network Details > Service Connection > User-ID Agent Address) as the **Host** (10.1.1.1 in the following example) and **5007** as the **Port**.

**Add a Data Redistribution Agent** ?

Name

Enabled

Host

Port

Collectorname

Collector Pre-Shared Key

Confirm Collector Pre-Shared Key

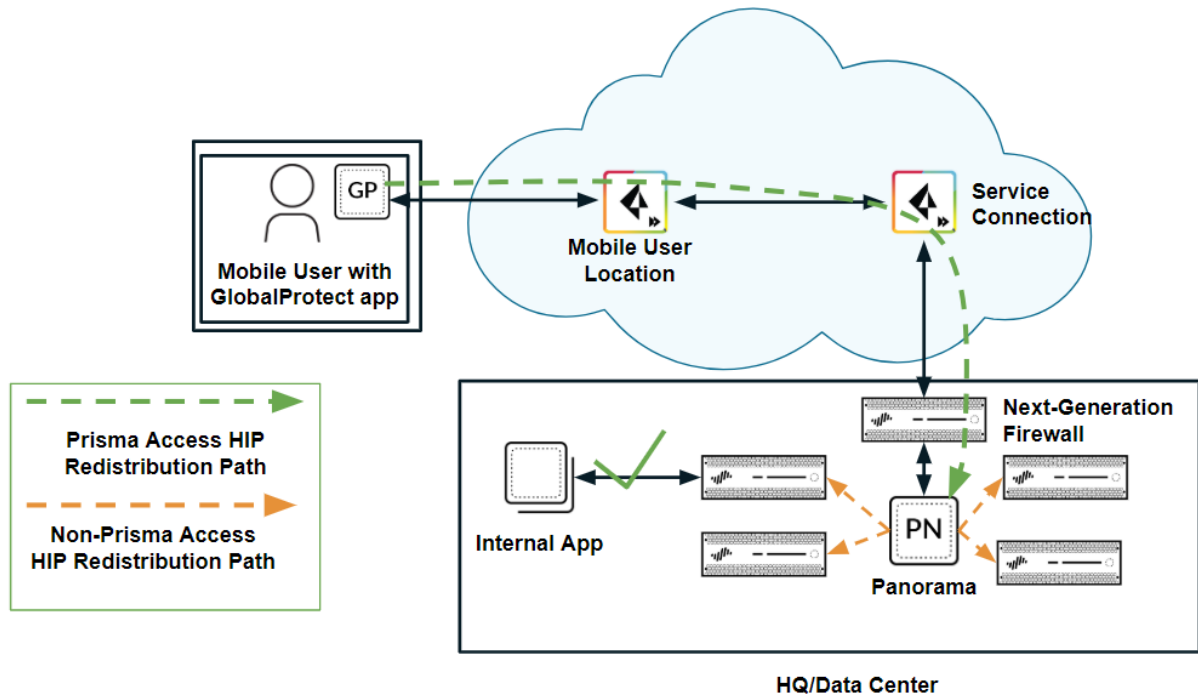
Data type

IP User Mappings  HIP

IP Tags  Quarantine List

User Tags

- HIP redistribution from Prisma Access to Panorama**—If you have multiple firewalls or gateways in your organization with HIP-based security policies, you can redistribute the HIP information from Prisma Access to the Panorama that manages Prisma Access by creating a User-ID agent in Panorama and specifying the Prisma Access **User-ID Agent Address** as the User-ID **Host**. You can then [redistribute HIP reports](#) from that Panorama appliance to the other managed Panorama appliances, gateways, firewalls, and virtual systems in your enterprise, using the same workflow that you use to [redistribute User-ID information to managed firewalls](#) and enforce consistent policy for internal apps and resources, as shown in the following figure.



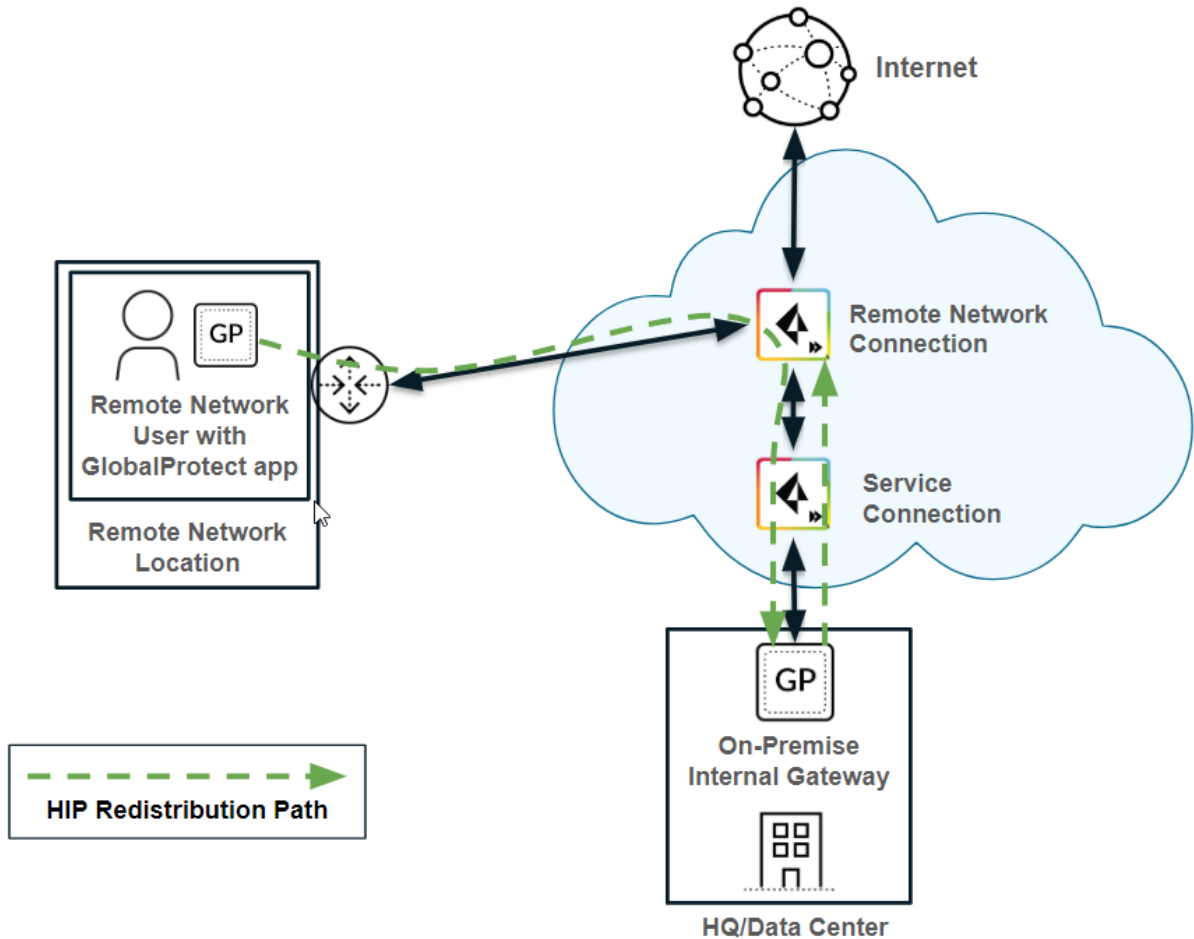
Alternatively, you can configure each internal firewall or gateway in your enterprise to directly collect HIP information from Prisma Access, without using Panorama as a central location, by creating a User-ID Agent in each device. Note, however, that Prisma Access uses service connections to send HIP information, and service connection bandwidth consumption might increase if Prisma Access sends a large number of HIP reports.

- HIP redistribution from a user at a remote network to Prisma Access**—The previous use cases showed Prisma Access collecting HIP information from mobile users. If you want to apply HIP-based policies in Prisma Access for a user at a remote network location, you need a way to distribute the HIP information from the remote network user’s GlobalProtect app to Prisma Access.

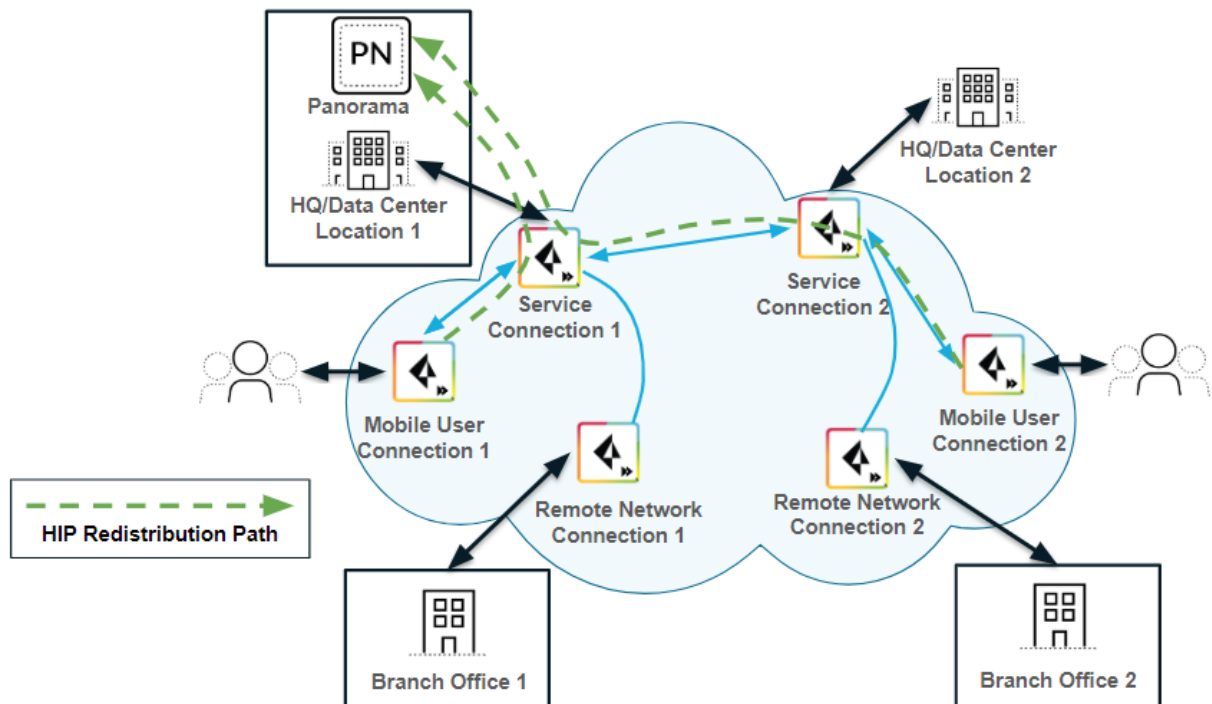
The following example shows a user at a remote network location whose internet access is located on the remote network connection. In Prisma Access, you control the user’s internet access at the remote network location with security policies created in the **Remote\_Network\_Device\_Group** or in a shared device group. To properly enforce the policies at the remote network location for the user, you need to configure Prisma Access to retrieve the user’s HIP information from the internal gateway.

In this example, the GlobalProtect gateway at the HQ/data center that is configured as an internal gateway using [internal host detection](#) checks the user’s HIP information from the user’s GlobalProtect app. The internal gateway detects that the user is inside the remote network location and collects both User-ID and HIP information from the user.

To distribute this HIP information from the internal gateway to Prisma Access, create a User-ID agent in Panorama and specify the IP address of the internal gateway as the host.

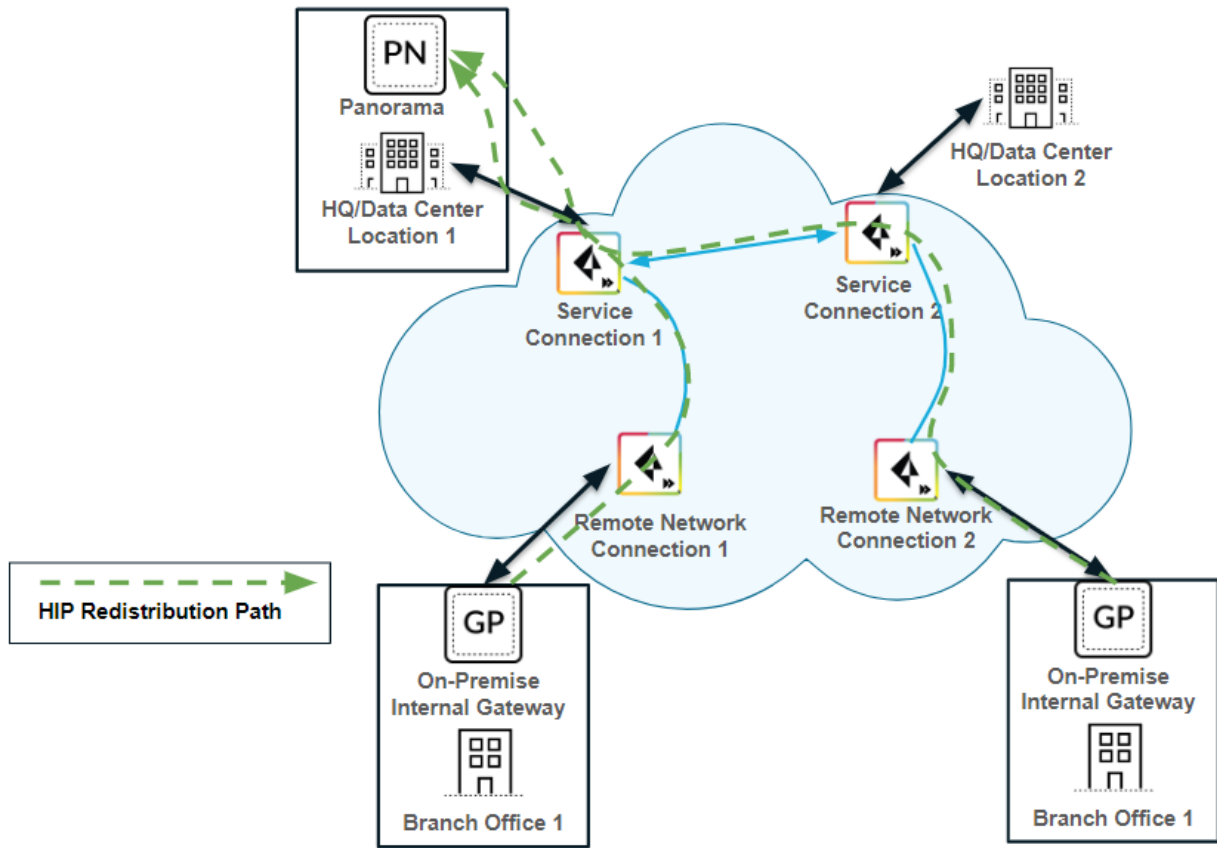


- **View detailed HIP logs from Panorama**—When mobile users log in using the GlobalProtect app, the app sends the HIP information to Prisma Access. Panorama retrieves the log results from Cortex Data Lake to view the results of the HIP Match logs (**Monitor > Logs > HIP Match**); however, you cannot view detailed HIP reports until you configure Panorama to redistribute HIP report details from Prisma Access to Panorama.



To redistribute detailed HIP information from mobile users to Panorama, create a User-ID agent in Panorama and specify the **User-ID Agent Address** (**Panorama > Cloud Services > Status > Network Details > Service Connection > User-ID Agent Address**) as the User-ID host. See [Configure HIP Redistribution in Prisma Access](#) for details.

If you have configured an on-premises gateway as an internal gateway at a remote user location, you can also send the HIP information for users at remote networks to Panorama by creating a User-ID agent in Panorama and specifying the remote network **EBGP Router** address (**Panorama > Cloud Services > Status > Network Details > Remote Networks > EBGP Router**) as the User-ID host. See [Configure HIP Redistribution in Prisma Access](#) for details.



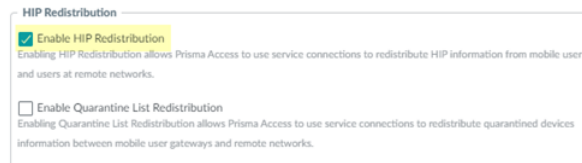
## Configure HIP Redistribution in Prisma Access

To allow Prisma Access to collect and redistribute HIP information, complete the following task.

### STEP 1 | Allow Prisma Access to redistribute HIP information.

1. In Panorama, select **Panorama > Cloud Services > Configuration > Service Setup**.
2. Click the gear icon to edit the settings.
3. In the **Advanced** tab, select **Enable HIP Redistribution**.

Enabling HIP Redistribution enables Prisma Access to redistribute the HIP reports received from the GlobalProtect app to internal firewalls and to Panorama.



### STEP 2 | Configure Panorama to receive HIP reports from Prisma Access.

1. Select **Panorama > Setup > Interfaces**.
2. Select the **Management** interface.
3. Select **User-ID**.

### STEP 3 | Configure Panorama to collect the User-ID mapping from Prisma Access.

1. From the Panorama that manages Prisma Access, select **Panorama > User Identification > User-ID Agents** (for 9.1.x Panorama appliances) or **Panorama > Data Redistribution > Agents** (for Panorama 10.x appliances).
2. **Add** a User-ID Agent and give it a **Name**.
3. Enter one of the following values in the **Host** field, depending on the types of HIP information you want to collect.
  - To collect HIP information for mobile users, enter the **User-ID Agent Address (Panorama > Cloud Services > Status > Network Details > Service Connection > User-ID Agent Address)**.
  - To collect HIP information from users at a remote network locations with an internal gateway, enter the IP address of the internal gateway.
  - To collect HIP information from users are a remote network connection, enter the **EBGP Router address (Panorama > Cloud Services > Status > Network Details > Remote Networks > EBGP Router)** as the User-ID host.
4. Enter **5007** in the port field.

By default, the User-ID agent uses port 5007 to listen for HIP information requests.



*Make sure that your network does not block access to this port between Prisma Access and the Active Directory server or User-ID Agent.*

5. Select **Enabled** to enable Panorama to communicate with the User-ID agent.
6. Select either **HIP** (for 10.x Panorama appliances) or **HIP Report** (for 9.1.x Panorama appliances) to enable Panorama to receive HIP reports from all mobile user locations.
7. Click **OK**.



---

### Add a Data Redistribution Agent ?

Name

Enabled

Host

Port

Collectorname

Collector Pre-Shared Key

Confirm Collector Pre-Shared Key

Data type  IP User Mappings  HIP

IP Tags  Quarantine List

User Tags

**STEP 4 |** Repeat Step 3 for each service connection to which you want to configure HIP report collection.

# View HIP Reports from Panorama

After you configure Prisma Access to [collect and redistribute HIP information](#) to Panorama, use the following workflow to view HIP information in Panorama.

**STEP 1 |** Select **Monitor > Logs > HIP Match** to view HIP information.



The screenshot shows the Palo Alto Panorama interface. The 'Monitor' tab is selected, and the 'Logs' section is expanded to 'HIP Match'. A table displays the following data:

Generate Time	Source IPv4	Serial Number	Source IPv6	Source User	Machine Name	Operating System	HIP	HIP Type	Device SN	Device Name
11/04 15:15:35	10.10.2.2			test		Mac	Apple	object		GP cloud service
11/04 15:15:35	10.10.2.2			test		Mac	HIP_prof	profile		GP cloud service
11/04 15:15:22	10.10.0.2			test		Mac	Apple	object		GP cloud service
11/04 15:15:22	10.10.0.2			test		Mac	HIP_prof	profile		GP cloud service
11/01 12:14:29	10.10.2.4			test		Mac	Apple	object		GP cloud service
11/01 12:14:29	10.10.2.4			test		Mac	HIP_prof	profile		GP cloud service
11/01 10:36:19	10.10.2.4			test		Mac	Apple	object		GP cloud service
11/01 10:36:19	10.10.2.4			test		Mac	HIP_prof	profile		GP cloud service
11/01 10:36:19	10.10.2.4			test		Mac	Apple	object		GP cloud service
11/01 10:35:27	10.10.0.5			test		Mac	Apple	object		GP cloud service
11/01 10:35:27	10.10.0.5			test		Mac	HIP_prof	profile		GP cloud service
11/01 10:35:18	10.10.2.4			test		Mac	Apple	object		GP cloud service
11/01 10:35:18	10.10.2.4			test		Mac	HIP_prof	profile		GP cloud service
11/01 10:33:12	10.10.0.3			test		Windows	Windows	object		GP cloud service
11/01 10:33:12	10.10.0.3			test		Windows	HIP_prof_Win	profile		GP cloud service
11/01 10:30:47	10.10.2.2			test		Windows	HIP_prof_Win	profile		GP cloud service
11/01 10:30:46	10.10.2.2			test		Windows	Windows	object		GP cloud service
10/30 19:08:24	10.10.2.2			test		Windows	Windows	object		GP cloud service
10/30 19:08:24	10.10.2.2			test		Windows	HIP_prof_Win	profile		GP cloud service
10/30 17:50:30	10.10.0.5			test		Mac	Apple	object		GP cloud service
10/30 17:50:30	10.10.0.5			test		Mac	HIP_prof	profile		GP cloud service

**STEP 2 |** Click the icon to the left of a record to view detailed HIP information.

? □ ×
Log Details

<b>Report Generated</b>	11/04/2019 15:15:26		
<b>User Information</b>	User: test	IP Address: 10.10.2.2	
<b>Host Information</b>	Machine Name: Cpe's MacBook (726)	Domain:	
<b>Serial Number</b>	[REDACTED]		
<b>Managed</b>	No		
<b>OS</b>	Apple Mac OS X 10.13.6	Host ID: [REDACTED]	
<b>Client Version</b>	5.1.0-22		
<b>Network Information</b>	<b>Interface</b>	<b>MAC Address</b>	<b>IP Address</b>
	en0	[REDACTED]	10.5.26.107
	en1	[REDACTED]	[REDACTED]

**Anti-Malware**

Software	Vendor	Version	Engine Version	Definition Version	Date	Real Time Protection	Last scanned
Gatekeeper	Apple Inc.	10.13.6				✔	n/a

**Disk Backup**

Software	Vendor	Version	Last Backup
Time Machine	Apple Inc.	1.3	n/a

**Disk Encryption**

Software	Vendor	Version
FileVault	Apple Inc.	10.13.6

Drive	State



# Manage Multiple Tenants in Prisma Access

To allow you to create and manage multiple Prisma Access instances, Prisma Access offers multitenancy, which enables you to create up to 200 instances (tenants) on a single Panorama appliance (or 2 appliances in high availability (HA) mode), with each tenant having their own separate templates and template stacks, device groups, and access domains.

Existing or future non-multitenant deployments are not affected by multitenancy and will continue to function normally. We recommend that you enable multitenancy only if your organization has a need to manage multiple tenants in Prisma Access.

Follow this workflow to create multiple tenants in Panorama for Prisma Access:

- > [Multitenancy Overview](#)
- > [Multitenancy Configuration Overview](#)
- > [Plan your Multitenant Deployment](#)
- > [Enable Multitenancy and Migrate the First Tenant](#)
- > [Add Tenants to Prisma Access](#)
- > [Delete a Tenant](#)
- > [Create Administrative Users for a Single Tenant](#)
- > [Control Role-Based Access for Tenant-Level Administrative Users](#)
- > [Sort Logs by Device Group ID for External Logging](#)

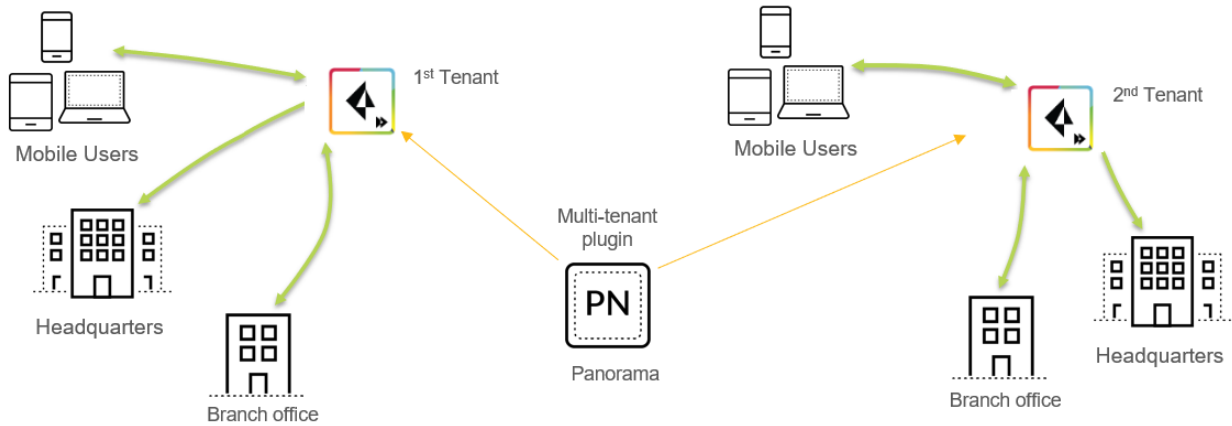
This section only provides the tasks you perform to configure tenants for remote networks, mobile users, or a combination of remote network and mobile user deployments. To configure the Clean Pipe service, see [Create and Configure Prisma Access for Clean Pipe](#).



# Multitenancy Overview

Enabling multitenancy allows you to host multiple instances of Prisma Access on a single Panorama appliance. Each instance is known as a *Tenant*.

Prisma Access tenants get their own dedicated Prisma Access instances and they are not shared between tenants.



---

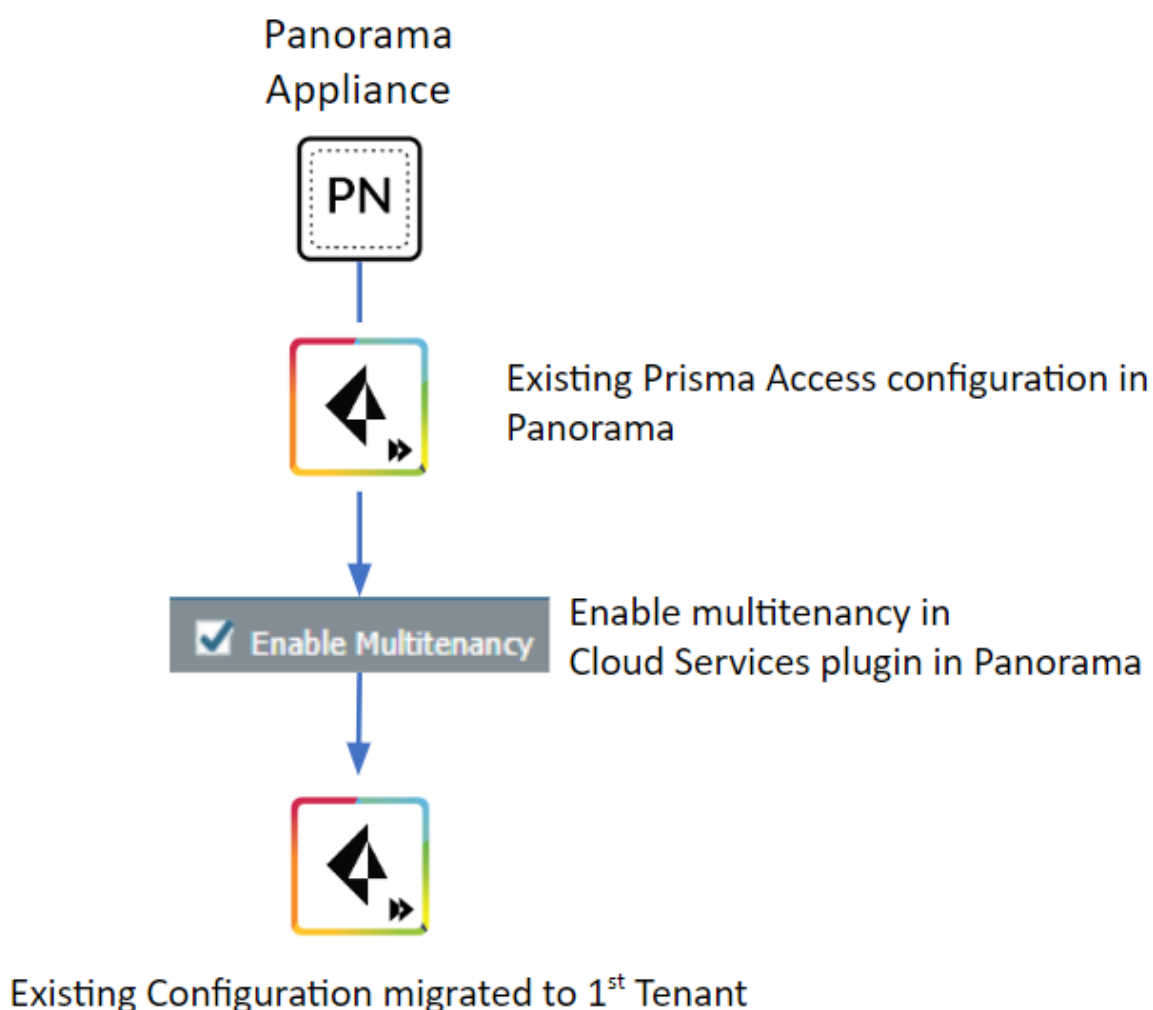
# Multitenancy Configuration Overview

Use the following workflow to enable and configure the ability to manage multiple tenants in a single Panorama appliance.

**STEP 1 |** Enable multitenancy. If you have an existing Prisma Access instance, enabling multitenancy automatically migrates your existing Prisma Access configuration to the first tenant.

You give the first (migrated) tenant a name and specify an access domain. Prisma Access migrates the templates, template stacks, and device groups associated with the existing configuration and associates them with the access domain you create.

After you migrate your initial configuration, the administrative user in Panorama becomes a superuser with the ability to create and manage all Prisma Access tenants.



**STEP 2 |** Then, [add tenants to Prisma Access](#).

To deploy multiple tenants, make sure that you have the following license minimums:





To determine the type of Prisma Access license you have from Panorama, select [Panorama > Licenses](#). See [Determine Your License Type from Panorama](#) for details.

- If you have a **Business**, **Business Premium**, **Zero Trust Network Access (ZTNA) Secure Internet Gateway (SIG)**, or **Enterprise** license, use the following minimums as a guideline:

**Prisma Access for Networks and Prisma Access for Users:**

If you have a **Local** Edition, a minimum quantity of 200 units is required for each tenant, and all tenants will be Local.

If you have a **Worldwide** Edition, a minimum quantity of 1,000 units is required to create a **Worldwide** tenant. If you allocate between 200 and 999 units for a tenant, Prisma Access creates a **Local** tenant; if you allocate 1,000 or more units for a tenant, then Prisma Access creates a **Worldwide** tenant.

*Units* correspond to bandwidth in Mbps for Prisma Access for Remote Networks and the number of mobile users for Prisma Access for Users.

- If your license type starts with **GlobalProtect Cloud Service**, use the following minimums as a guideline:

**Prisma Access for Networks**—You must have a minimum of 200 Mbps available in your license for each tenant.

**Prisma Access for Users**—You must have a minimum of 200 mobile users available in your license for each tenant.

In both types of Prisma Access configurations, you can add additional licensing (above these minimums) of either type. You can increase or decrease the bandwidth or mobile user allocation for any tenants after onboarding, as long as you keep the minimum required allocation per tenant, and the overall licensed capacity is not exceeded.

You can set up a multi-tenant configuration for only remote networks, only mobile users, or both. You allocate licenses accordingly to each tenant when you enable multi-tenancy.

If you have a license for remote networks and mobile users, you can set up an individual tenant with only mobile users or only remote networks. For example, if your Prisma Access deployment has a **Worldwide** edition license for mobile users and remote networks, you could set up a tenant for mobile users only, as long as you specify a minimum of 1,000 mobile users for the tenant.

For each tenant you create after the first, Prisma Access automatically creates templates, template stacks, and device groups for each tenant and associates them to the access domain you create. Prisma Access creates this environment to allow you to [create a tenant-level administrative user](#) using an [administrative role](#) based on the tenant's device groups and templates, then creating an administrative user based on that role. In this way, you create an administrative user that has access to a single tenant without allowing that user access to the other tenants that are managed by the Panorama appliance.

Prisma Access creates template stacks, templates, and device group using the following naming convention:

- A service connection template stack with the name of **sc-stk-tenant**, where *tenant* is the tenant's name.
- A service connection template with the name of **sc-tpl-tenant**.
- A service connection device group with the name of **sc-dg-tenant**.
- A mobile user template stack with the name of **mu-stk-tenant**.
- A mobile user template with the name of **mu-tpl-tenant**.
- A mobile user device group with the name of **mu-dg-tenant**.
- A remote network template stack with the name of **rn-stk-tenant**.

- 
- A mobile user template with the name of **rn-tpl-tenant**.
  - A mobile user device group with the name of **rn-dg-tenant**.
  - A Clean Pipe template stack with the name of **cp-stk-tenant**.
  - A Clean Pipe template with the name of **cp-tpl-tenant**.
  - A Clean Pipe device group with the name of **cp-dg-tenant**.

Prisma Access creates template stacks, templates, and device groups for all Prisma Access types, even those for which you might not be licensed. For example, if you purchase a license for remote networks, Prisma Access automatically creates template stacks, templates, and device groups for remote networks, mobile users, and Clean Pipe.

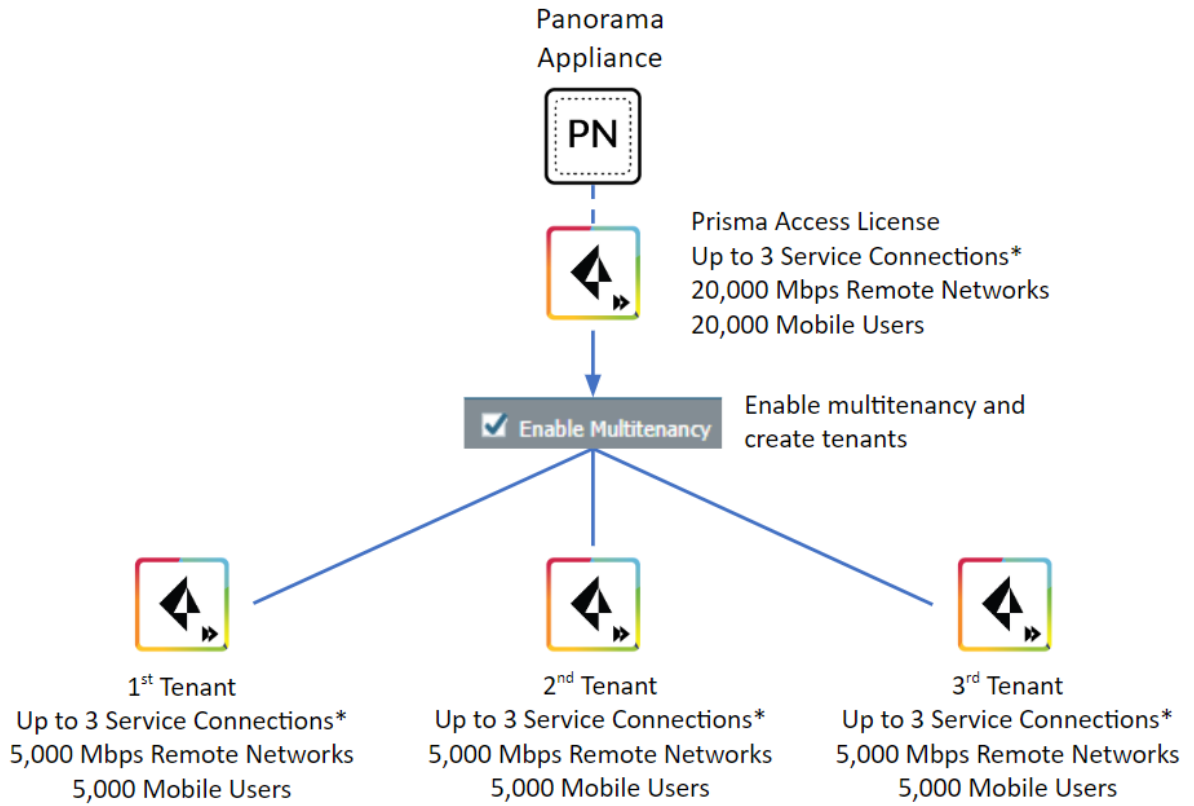
If you add custom templates, they cannot take precedence over the Prisma Access-created templates.

You allocate remote network and mobile user license resources for each tenant based on the license that is associated with the Cloud Services plugin in Panorama.

The following figure shows a sample Prisma Access deployment using a license with a 20,000 Mbps remote network bandwidth pool and 20,000 mobile users. The administrator allocated 5,000 Mbps in remote network bandwidth and 5,000 mobile users for the existing configuration. After the administrator enabled multitenancy, the license allocation migrated along with all other configuration to the first tenant. The administrator then created additional tenants, each with a 5,000 Mbps bandwidth pool for remote networks and 5,000 mobile users for each tenant. Prisma Access allocates the license resources from the overall license allocation. After you complete this configuration, there is 5,000 Mbps of remote network bandwidth and 5,000 mobile users available in the license.



*Each tenant can use up to 3 service connections with no cost to the license. You can add more than 3 service connections to each tenant, however each additional service connection takes 300 Mbps from your remote network license.*



\* Additional service connections take 300 Mbps from remote network license

---

# Plan Your Multitenant Deployment

Before you enable multitenancy, migrate the first tenant, and create additional tenants, make sure that you have all required information and resources to do so by completing the following tasks:

- ❑ If you are migrating an existing single-tenant deployment to a multi-tenant deployment, make a note of the following Prisma Access features that are not supported. See the [Palo Alto Networks Compatibility Matrix](#) for the list of unsupported features.
- ❑ Make a note of your license allocation for remote networks and mobile users.

Open your license (**Panorama > Licenses**) and find the Prisma Access **Total Mbps** (remote networks bandwidth pool) for remote networks and **User Limit** (total number of licensed users) for mobile users.

When you create tenants, you assign resources for remote networks and mobile users from this license allocation. If you run out of the minimum required licensed Mbps for remote networks or mobile users, you cannot create additional tenants.



*You should also make a note of the bandwidth and mobile users allocation for your existing configuration. After you migrate your configuration to the first tenant, check these values to verify that the first tenant migrated correctly.*

- ❑ Make a list of the names you will use to identify each tenant.



*When you create tenant names, avoid using names like Tenant-1, Tenant-2, Tenant-3, and so on. The system logs reserve a small number of characters for the tenant name in the log output and, if tenants have similar names, it can be difficult to associate the tenant with the logs. We recommend using a unique and short name for tenants (for example, Acme or Hooli).*

- ❑ Make a list of the administrative users you will create and assign for each tenant, and note the maximum number of administrative users that can be logged in concurrently.

When administrative users are performing normal multi-tenant operations such as configuration changes and commit operations, we recommend having a maximum of 12 administrative users logged in to Panorama concurrently.

An administrative user who can manage multiple tenants can provision up to 200 tenants at the same time with a single commit operation.

- ❑ Be sure that you have sufficient license resources to enable multiple tenants.

The minimum license allocation for each tenant is 200 Mbps for each remote network or 200 mobile users. You can also create a tenant with only remote networks or mobile users, and can configure tenants in differing configurations on the same Panorama. For example, you could create a tenant with remote networks only, a tenant with mobile users only, or a tenant with both mobile users and remote networks, as long as each tenant meets the minimum license allocation and the relevant licenses are activated and associated with the Panorama where you configure the tenants.

- ❑ When configuring a tenant in multitenancy mode, create a unique name for each IPSec tunnel and IKE gateway for service connections and remote network connections, and try to use a name that will not be duplicated by another tenant. While there is no effect to functionality, you cannot delete an IPSec tunnel or IKE gateway if another tenant is using a tunnel or gateway with the same name.
- ❑ Note that single-tenant users cannot view system logs; only superusers can. You can, however, [sort logs by tenant](#).
- ❑ Note that, when using the multitenancy feature and logged in as a tenant-level administrative user, opening the Panorama Task Manager (clicking **Tasks** at the bottom of the Panorama web interface) shows all tasks for all tenants, including any tasks done at the superuser (Admin) level.


# Enable Multitenancy and Migrate the First Tenant

Use the following workflow to enable multitenancy and migrate your existing configuration to the first tenant you create.

When you enable multitenancy, Prisma Access automatically migrates the following components of your configuration:

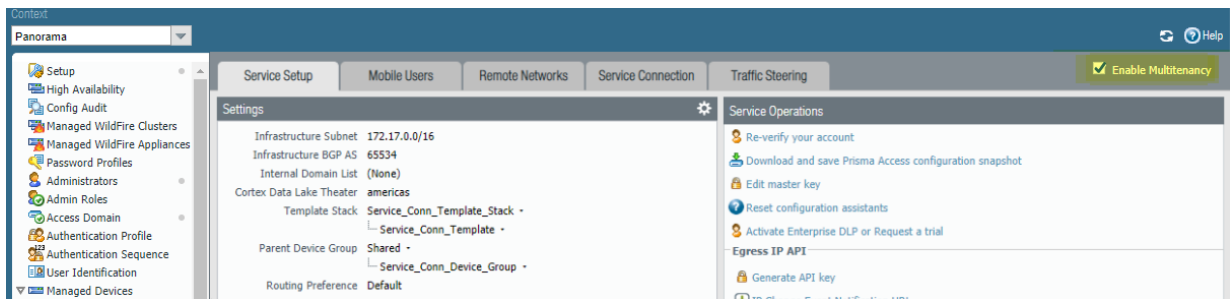
- The amount of licensed bandwidth for remote networks and mobile users.
- All service connection and remote network tunnel onboarding information, including tunnel configuration.
- Existing mobile users onboarding information.
- Cortex Data Lake information.
- The templates, template stacks, and device groups for service connections, remote networks, and mobile users.

Because of these device group changes, you create an [access domain](#) and add the migrated device groups, templates, and template stacks, as shown in the following workflow.


 *If you don't have an existing Prisma Access configuration, and you are creating an all-new multi-tenant deployment, do not use this workflow; instead, complete the steps in [Add Tenants to Prisma Access](#) to create the first tenant.*

**STEP 1 |** Select **Panorama > Cloud Services > Configuration**.

**STEP 2 |** Select **Enable Multitenancy** (located on the upper right of the page).



After you enable multitenancy, Panorama displays a notification informing you that the existing Prisma Access configuration will be moved to the first tenant.

 *After you enable multitenancy, your deployment permanently changes to a multi-tenant deployment, and you cannot revert to single tenant mode.*

**STEP 3 |** Click **OK** to migrate the existing configuration to the first tenant.

The **Tenants** page displays. Three pie charts in the center of the window shows the available licensed bandwidth remaining for remote networks and clean pipe and the remaining licensed number of available mobile users. If you do not have a license for remote networks or mobile users, those choices are dimmed.

**STEP 4 |** Choose the type of deployment you want to use for the tenant.

- For a remote network, mobile user deployment, or to configure both deployment types for a tenant, select **Remote Networks/Mobile Users**.
- For a clean pipe deployment, select **Clean Pipe**.

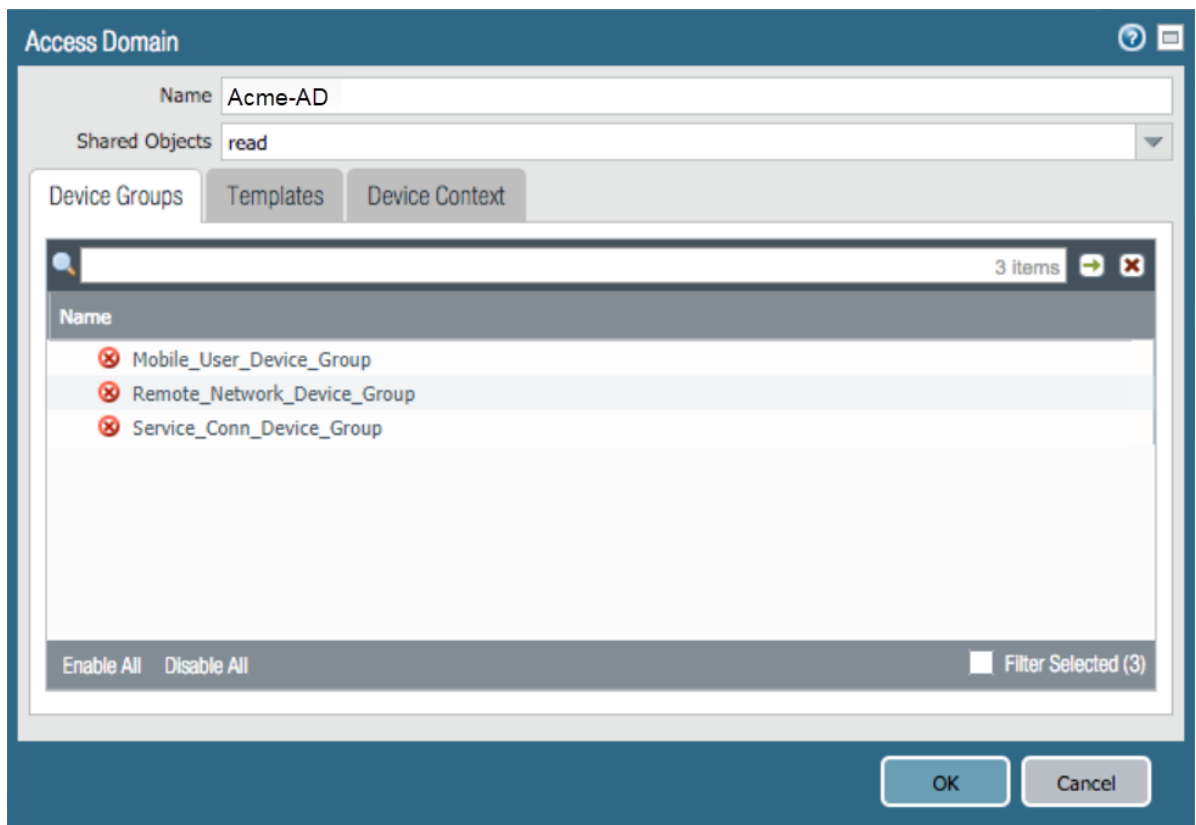
This section only describes how to configure tenants for remote network, mobile user, or both remote network and mobile user deployment types. To configure the clean pipe service, see [Create and Configure Prisma Access for Clean Pipe](#).

Tenant	Bandwidth (Mbps)	%	Tenant	Users	%	Tenant	Bandwidth (Mbps)	%
This Tenant	[200 - 24667]	--%	This Tenant	[200 - 24667]	--%	This Tenant	[100 - 16500]	--%
Unallocated	24667	99%	Unallocated	24667	99%	Unallocated	16500	83%
Total	25000	100%	Total	25000	100%	Total	20000	100%

#### STEP 5 | Migrate the existing configuration to the first tenant.

1. Specify a **Name** for the first tenant.
2. Create a new **Access Domain** by clicking the down arrow selecting **New Access Domain**.
3. Enter a **Name** for the access domain and click **OK**.

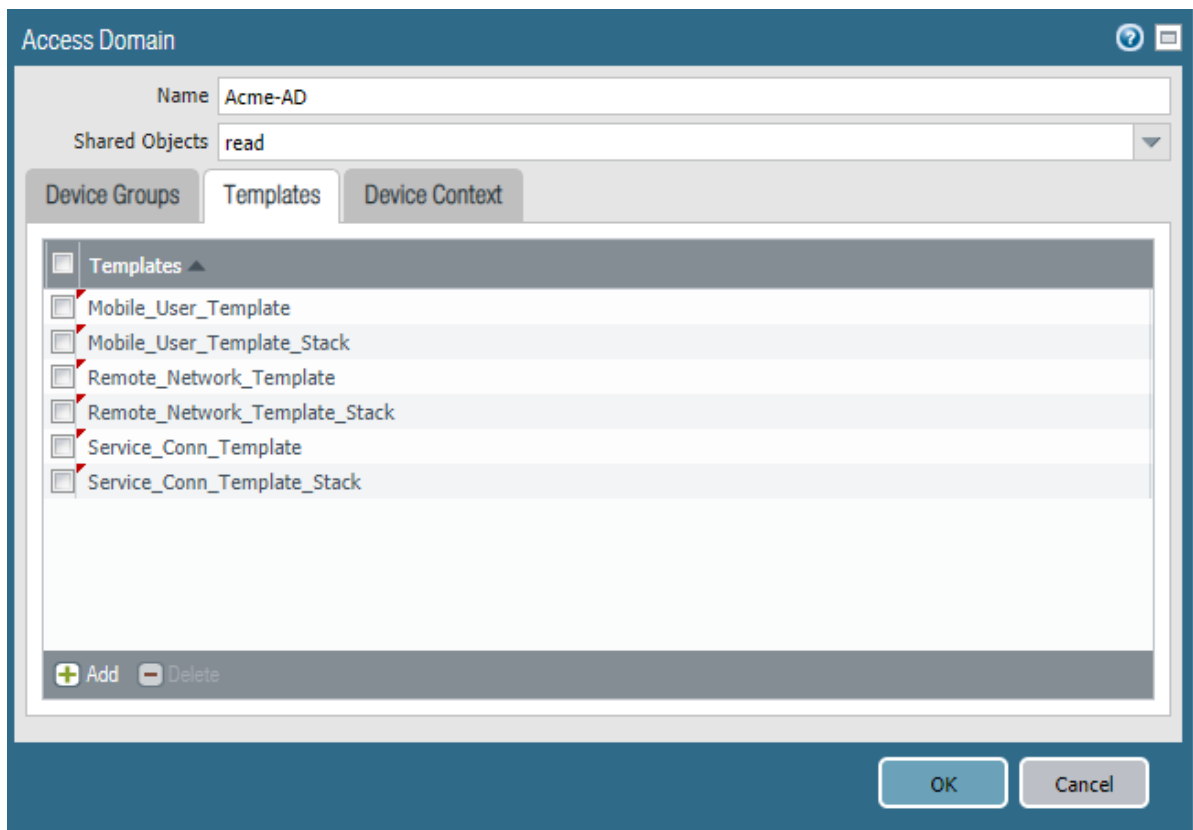
Prisma Access adds the **Mobile\_User\_Device\_Group**, **Remote\_Network\_Device\_Group**, and **Service\_Conn\_Device\_Group** Device Groups to the new access domain.



4. (Optional) Click **Templates** to verify that Prisma Access added the following templates and template stacks:

- **Mobile\_User\_Template**
- **Mobile\_User\_Template\_Stack**
- **Remote\_Network\_Template**
- **Remote\_Network\_Template\_Stack**
- **Service\_Conn\_Template**
- **Service\_Conn\_Template\_Stack**

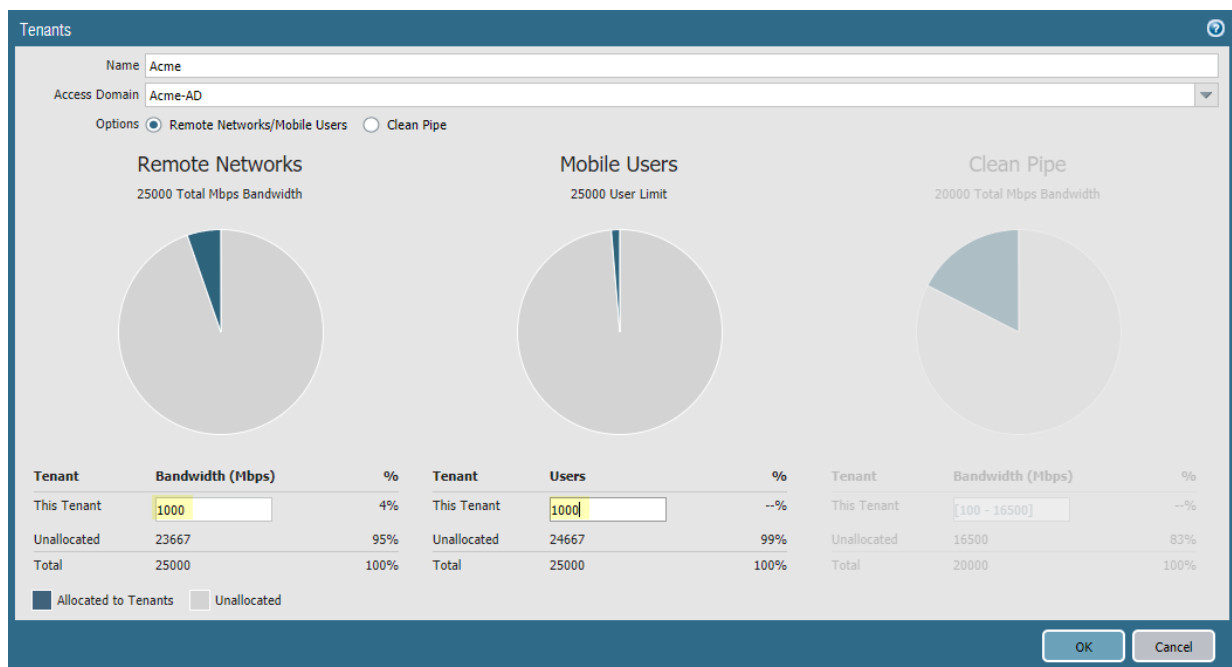
These are the default template stacks and templates for a standard Prisma Access deployment; if you added other templates, be sure that Prisma Access added them.



5. (Optional) If you have other templates associated with this configuration, select them.
6. Click **OK** to close the **Access Domain** page and return to the **Tenants** page.

**STEP 6 |** Make sure that the values in **Bandwidth (Mbps)** for remote networks and **Users** for mobile users are correct.

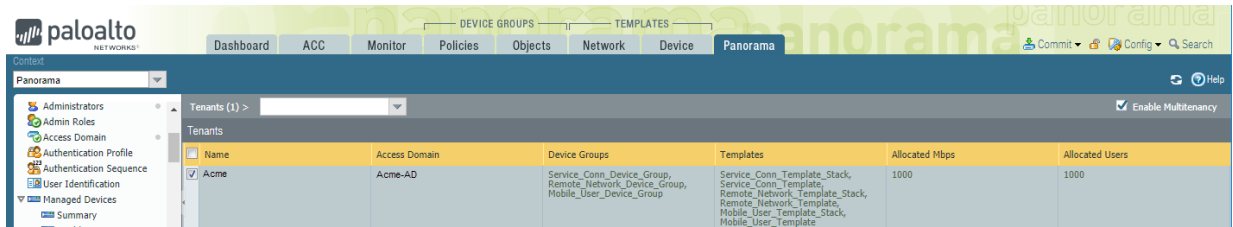
These values automatically migrate from your existing configuration.



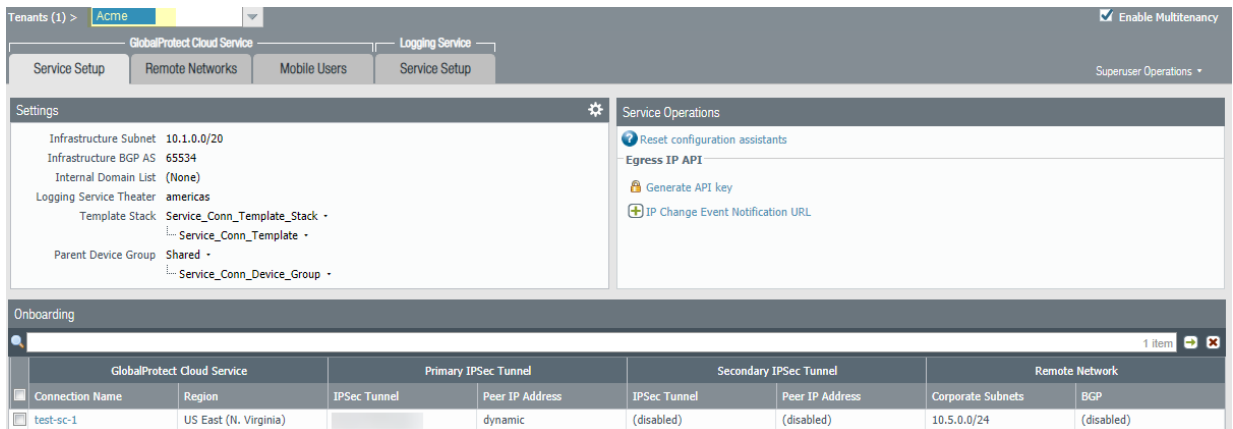


## STEP 7 | Click OK.

The **Panorama > Cloud Services > Configuration** page shows the first tenant successfully migrated, and a **Tenants** drop-down is added above the **Tenants** area.

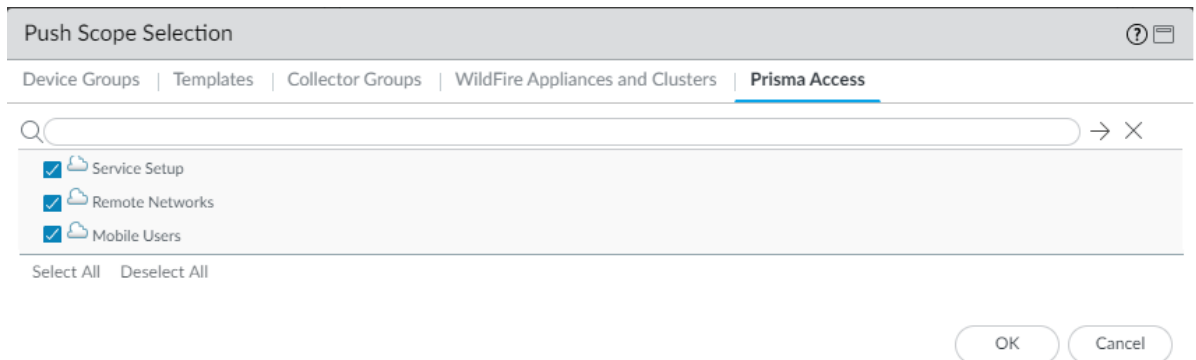


## STEP 8 | Select the tenant you just created in the **Tenants** drop-down to verify that all settings were onboarded.



## STEP 9 | Commit and push your changes to make them active in Prisma Access.

1. Select **Commit > Commit and Push** and **Edit Selections** in the Push Scope.
2. Select **Prisma Access**, then select the tenant you created, **Service Setup**, **Remote Networks**, and **Mobile Users**.



3. Click **OK** to save your changes to the Push Scope.
4. **Commit and Push** your changes.

## STEP 10 | Select **Panorama > Cloud Services > Status**.

The status page shows the status of all tenants. Because you have created only one tenant, that tenant is the only one that is shown. If you select that tenant from the drop-down, you show a detailed status of that tenant.

Tenants (1) >												
Name	Service Connections			Remote Networks				Mobile Users			Logging Service	
	Status	Config	Connections	Status	Config	Peers	Allocated Mbps	Status	Config	Current	Last 90 Days	Status
Acme			1			1	2			0		


Selecting a tenant from the drop-down list returns you to the Status page for that tenant.

**STEP 11** | Continue to [add more tenants](#) to Prisma Access.

# Add Tenants to Prisma Access

After you migrate the existing information as a first tenant, you can create and configure additional tenants. For each tenant you create after the first, Prisma Access creates a separate access domain with its own set of template stacks and templates and its own domain groups.

Use this workflow to add more tenants to Prisma Access.

 *If you are creating an all-new multi-tenant deployment, use this workflow to add the first tenant as well as additional tenants.*

**STEP 1** | Log in to Panorama as a superuser.

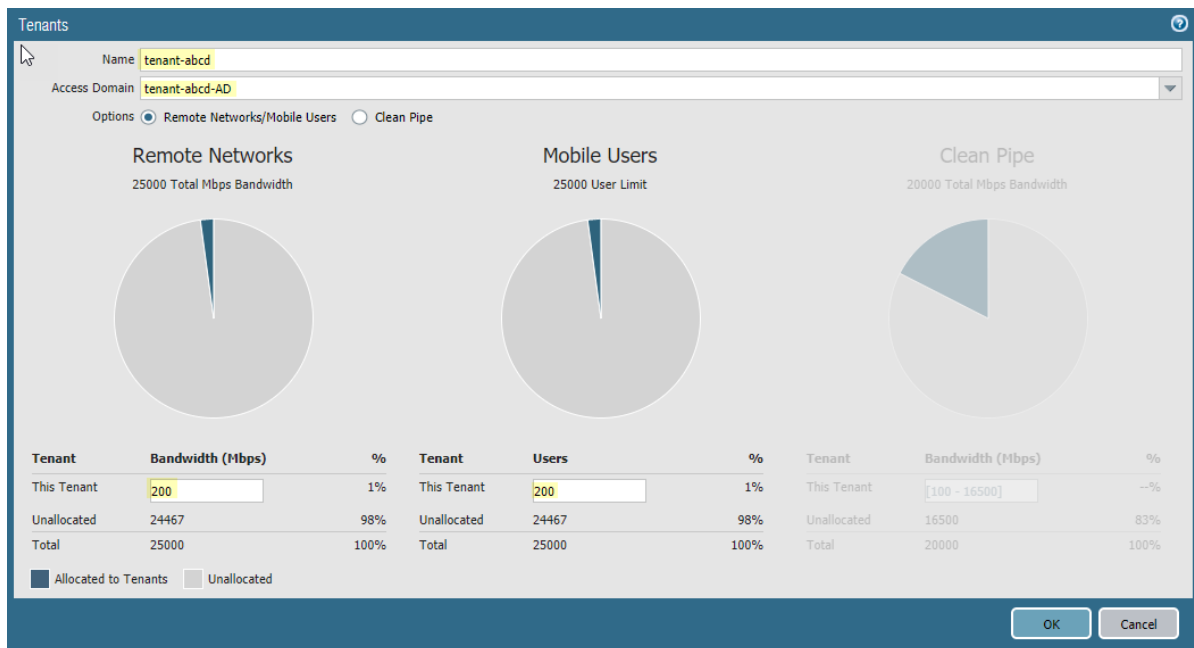
**STEP 2** | Add and configure the tenant.

1. Select **Panorama > Cloud Services > Configuration**, then **Add** a new tenant.

Be sure that you select **Remote Networks/Mobile Users**; to create and configure a Clean Pipe deployment, see [Create and Configure Prisma Access for Clean Pipe](#).

2. Specify a descriptive **Name** for the tenant.
3. **Add** a new **Access Domain**, give it a descriptive **Name**, and click **OK** to return to the **Tenants** window.

After you click **OK**, Prisma Access automatically creates templates, template stacks, and device groups and associates them to the access domain you create.



Tenant	Bandwidth (Mbps)	%
This Tenant	200	1%
Unallocated	24467	98%
Total	25000	100%

Tenant	Users	%
This Tenant	200	1%
Unallocated	24467	98%
Total	25000	100%

Tenant	Bandwidth (Mbps)	%
This Tenant	[100 - 16500]	5%
Unallocated	16500	83%
Total	20000	100%

**STEP 3** | Specify the amount of **Bandwidth (Mbps)** to allocate for the **Remote Networks** and the number of **Users** to allocate for the **Mobile Users**.

**STEP 4** | Make sure that Prisma Access applied the template stack, template, and device group service settings to the service connection settings of the tenant you just created.

1. Select the tenant you created from the **Tenant** drop-down.

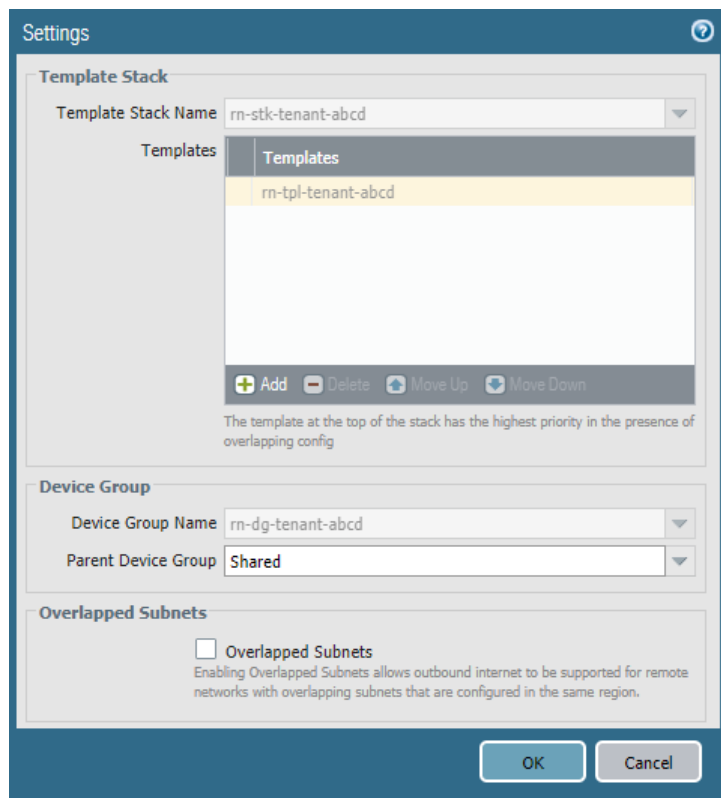
Tenants (17) > tenant-abcd

2. Select **Panorama > Cloud Services > Configuration > Service Setup**.
3. Click the gear icon to the right of the **Settings** area to edit the settings.
4. Make sure that Prisma Access has associated the template stack (**sc-stk-tenant**), template (**sc-tpl-tenant**), and device group (**sc-dg-tenant**) to your service connection settings.
5. Make sure that the **Parent Device Group** is set to **Shared** and click **OK**.

The screenshot shows the 'Settings' dialog box with three tabs: 'General', 'Internal Domain List', and 'Cortex Data Lake'. The 'General' tab is active. The 'Service Infrastructure' section includes 'Infrastructure Subnet' and 'Infrastructure BGP AS'. The 'Template Stack' section includes 'Template Stack Name' (sc-stk-tenant-abcd) and a list of templates (sc-tpl-tenant-abcd). The 'Device Group' section includes 'Device Group Name' (sc-dg-tenant-abcd) and 'Parent Device Group' (Shared). The dialog box has 'OK' and 'Cancel' buttons at the bottom.

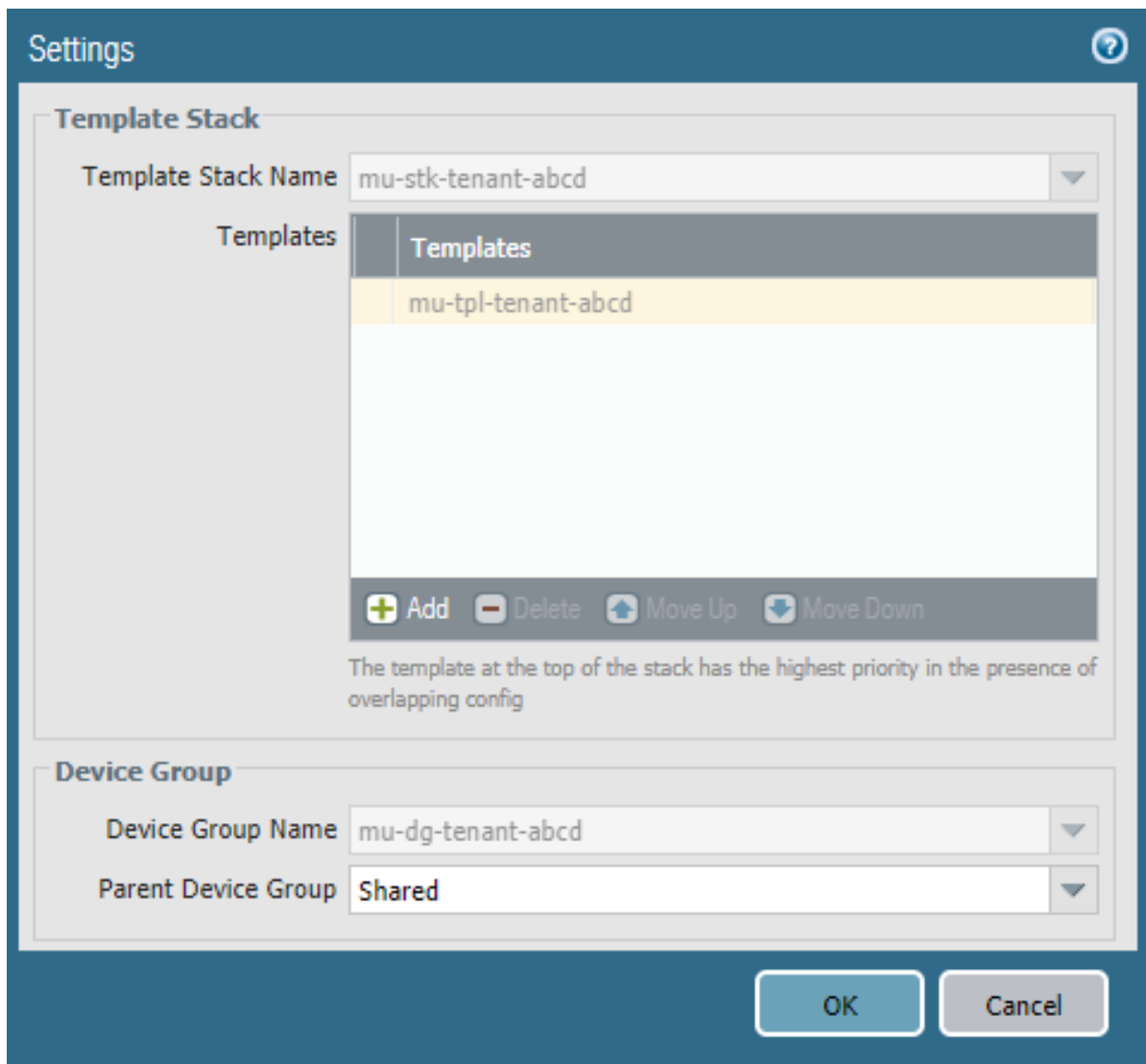
**STEP 5 |** Make sure that Prisma Access applied the template stack, template, and device group to the remote network settings.

1. Select **Panorama > Cloud Services > Configuration > Remote Networks** and click the gear icon to the right of the **Settings** area to edit the settings.
2. Make sure that the Prisma Access has associated the template stack (**rn-stk-tenant**), template (**rn-tpl-tenant**), and device group (**rn-dg-tenant**) to your remote network settings.
3. Make sure that the **Parent Device Group** is set to **Shared** and click **OK**.



**STEP 6** | Make sure that Prisma Access applied the template stack, template, and device group to the mobile user settings.

1. Select **Panorama > Cloud Services > Configuration > Mobile Users** and click the gear icon to the right of the **Settings** area to edit the settings.
2. Make sure that the Prisma Access has associated the template stack (**mu-stk-tenant**), template (**mu-tpl-tenant**), and device group (**mu-dg-tenant**) to your remote network settings.
3. Make sure that the **Parent Device Group** is set to **Shared** and click **OK**.



**STEP 7 | Mobile User deployments only**—Add an infrastructure subnet, then commit and push your changes to make them active in Prisma Access.

These steps are required for the mobile user changes to take effect.

1. Select **Panorama > Cloud Services > Configuration > Service Setup**, click the gear icon to edit the Settings, and configure an [infrastructure subnet](#).
2. Select **Commit > Commit and Push, Edit Selections** in the Push Scope, and make sure that **Mobile Users** is selected.
3. Click **OK** to save your changes to the Push Scope.
4. **Commit** and **Push** your changes.

**STEP 8 |** Continue the configuration of your tenant.

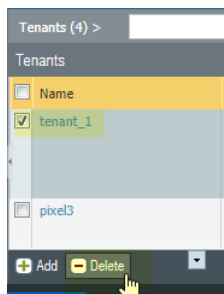
1. [Configure the Service Infrastructure](#).
2. [Create a Service Connection to Allow Access to Your Corporate Resources](#).
3. [Onboard and Configure Remote Networks](#) if you are licensed for remote networks.
4. [Secure Mobile Users With GlobalProtect](#) if you are licensed for remote users.

---


# Delete a Tenant

To delete a tenant, complete the following task.

**STEP 1** | Select **Panorama > Cloud Services > Configuration**, select the tenant, then **Delete** it.




Deleting a tenant also deletes all configuration for the tenant, including permanently removing any IP addresses Prisma Access has assigned for service connections, remote networks, and mobile users.

 *When you delete a tenant, Prisma Access deletes the template and device group set for which you are licensed, but does not delete the unlicensed set. For example, if you have a Prisma Access for Users license and delete a tenant, Prisma Access deletes the mobile user-related template stacks, templates, and device groups but does not delete the set it created for the unlicensed Prisma Access for Networks. You can manually delete these unused template and device group sets after you delete the tenant.*

**STEP 2** | Select **Commit > Commit to Panorama** and **Commit** your changes.

# Create a Tenant-Level Administrative User


You should create an administrative user for each tenant. In that way, a tenant-level administrator can view and make changes to their tenant configuration but doesn't have access to other tenants. To create an administrative user for a specific tenant, complete the following task. For more information about role-based access control (RBAC) for tenant-level administrative users, see [Control Role-Based Access for Tenant-Level Administrative Users](#).

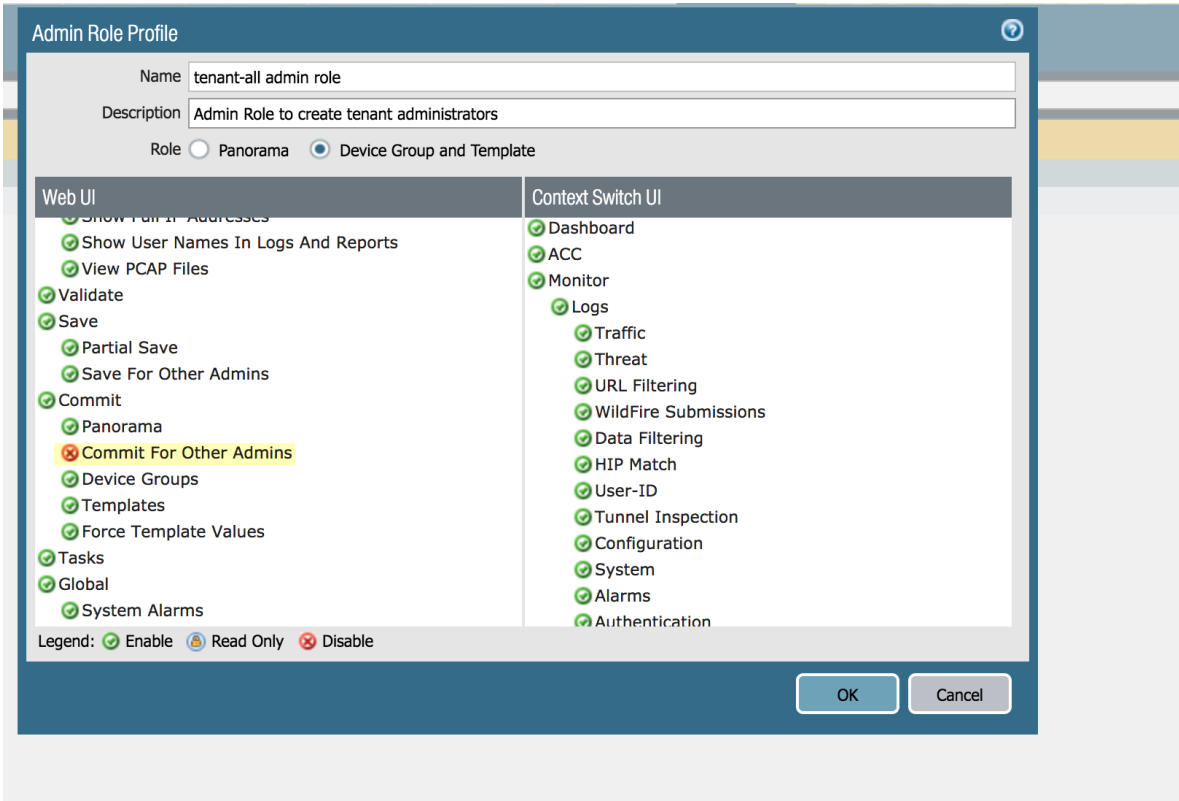
 *Users who manage single tenants cannot see the system logs because the Monitor > Logs > System choice is not available. This limitation applies to all Administrators who have an administrative role of Device Group and Template. Only superusers can view system logs in multitenancy mode.*

## STEP 1 | Create an [administrative role](#) with a type of **Device Group and Template**.

1. Select **Panorama > Admin Roles**.
2. **Add** an Admin Role Profile with a **Role** of **Device Group and Template**.
3. Click **OK**.

You can create a single Admin Role Profile and share it across multiple tenants; however, you must create a separate administrator for each tenant.

 *While you tailor the administrative role for the needs of your organization, we recommend deselecting **Commit for Other Admins**. Deselecting this choice allows a tenant-level user to commit only the changes they have made, and prevents them from unintentionally committing other changes that other tenant-level administrative users have made that are not yet committed.*



**Admin Role Profile**

Name: tenant-all admin role  
Description: Admin Role to create tenant administrators

Role:  Panorama  Device Group and Template

Web UI	Context Switch UI
<input checked="" type="checkbox"/> Show Full IP Addresses	<input checked="" type="checkbox"/> Dashboard
<input checked="" type="checkbox"/> Show User Names In Logs And Reports	<input checked="" type="checkbox"/> ACC
<input checked="" type="checkbox"/> View PCAP Files	<input checked="" type="checkbox"/> Monitor
<input checked="" type="checkbox"/> Validate	<input checked="" type="checkbox"/> Logs
<input checked="" type="checkbox"/> Save	<input checked="" type="checkbox"/> Traffic
<input checked="" type="checkbox"/> Partial Save	<input checked="" type="checkbox"/> Threat
<input checked="" type="checkbox"/> Save For Other Admins	<input checked="" type="checkbox"/> URL Filtering
<input checked="" type="checkbox"/> Commit	<input checked="" type="checkbox"/> WildFire Submissions
<input checked="" type="checkbox"/> Panorama	<input checked="" type="checkbox"/> Data Filtering
<input checked="" type="checkbox"/> <b>Commit For Other Admins</b>	<input checked="" type="checkbox"/> HIP Match
<input checked="" type="checkbox"/> Device Groups	<input checked="" type="checkbox"/> User-ID
<input checked="" type="checkbox"/> Templates	<input checked="" type="checkbox"/> Tunnel Inspection
<input checked="" type="checkbox"/> Force Template Values	<input checked="" type="checkbox"/> Configuration
<input checked="" type="checkbox"/> Tasks	<input checked="" type="checkbox"/> System
<input checked="" type="checkbox"/> Global	<input checked="" type="checkbox"/> Alarms
<input checked="" type="checkbox"/> System Alarms	<input checked="" type="checkbox"/> Authentication

Legend:  Enable  Read Only  Disable

OK Cancel



**STEP 2** | Create and configure an **Administrator** for the tenant.

1. Select **Panorama > Administrators**.
2. **Add** an Administrator.
3. Enter and confirm a **Password** for the new Administrator.
4. Specify an **Administrator Type** of **Device Group and Template Admin**.
5. Specify the **Access Domain** that is associated with the device groups for that tenant.
6. Specify the **Admin Role** that you created in Step 1 for the tenant.

The screenshot shows the 'Administrator' configuration window. The fields are filled as follows:

- Name: Acme
- Authentication Profile: None
- Use only client certificate authentication (Web):
- Password: [masked]
- Confirm Password: [masked]
- Use Public Key Authentication (SSH):
- Administrator Type: Device Group and Template Admin
- Password Profile: None
- Access Domain to Administrator Role: [Search bar with 1 item]

Access Domain	Admin Role
<input checked="" type="checkbox"/> Acme-AD	tenants-all admin role

Buttons: + Add, - Delete, OK, Cancel

**STEP 3** | Click **OK**.

**STEP 4** | Repeat Steps 2 and 3 to add additional users to manage your tenants as required.

**STEP 5** | Select **Commit > Commit to Panorama** and **Commit** your changes.

# Control Role-Based Access for Tenant-Level Administrative Users

If you manage a multi-tenant deployment, you can use role-based access control (RBAC) to [create tenant-level administrative users](#).

To modify RBAC-level access for tenant-level administrative users in Panorama, you [create a tenant-level administrative user](#), use an [Admin Role Profile](#) with a **Role** of **Device Group and Template**, and **Enable**, **Disable**, or give **Read Only** access to areas of the Panorama **Web UI**. Use this method to manage access to all Panorama components for tenant-level users, with the exception of access to the Cloud Services plugin where you manage Prisma Access.

If you want to restrict a tenant-level user from configuring the Prisma Access components in Panorama, you cannot use Admin Roles. To disallow users from configuring Prisma Access-specific configuration tasks, you must [prevent the user from accessing the Cloud Services plugin](#), which also prevents them from viewing it. Using this method, you can create an administrative user for a security professional who has permissions to make changes to security policies and push those changes to Panorama, but cannot view or make any changes to Prisma Access configuration.



*You can either enable or disable access to the Cloud Services plugin for a user, but you cannot give a user read-only access; if a user has access to view the Cloud Services plugin, the user can also make configuration changes to its components, including Prisma Access.*

The following table shows sample tenant-level administrative roles and the steps you perform to create those roles.

Sample Tenant-Level Configuration	Configuration Task
Create a networking-focused user who: <ul style="list-style-type: none"><li>• Can edit plugin configurations</li><li>• Can commit to Panorama</li><li>• Can push configuration to Prisma Access</li></ul>	<a href="#">Create a tenant-level administrative user</a> , enabling <b>Save</b> and <b>Commit</b> permissions in the <b>Admin Role Profile</b> , and disabling or making <b>Read Only</b> any permissions that you don't want the tenant-level administrative user to have.
Create a security-focused user who: <ul style="list-style-type: none"><li>• Can view and make changes to security policies</li><li>• Can commit to Panorama</li><li>• Cannot view, or make changes to, the Cloud Services plugin</li><li>• Cannot push configuration to Prisma Access (requires the superuser to push the configuration)</li></ul>	To prevent a tenant-level administrative user from viewing or accessing the plugin, <a href="#">remove plugin access for a tenant-level administrator</a> . For all other Panorama-related permissions, change the Admin Role permissions for the user.
Create a hybrid user who: <ul style="list-style-type: none"><li>• Has read-only access to the Cloud Services plugin</li></ul>	You cannot make the Cloud Services plugin read-only. You can either view it or disable it.

Sample Tenant-Level Configuration	Configuration Task
<ul style="list-style-type: none"> <li>• Has read-write access to the security policy</li> <li>• Cannot push the configuration to Prisma Access (requires the superuser to push the configuration)</li> </ul>	

## Remove Plugin Access for a Tenant-Level Administrative User

In normal multi-tenant configurations, you use access domains [Add Tenants to Prisma Access](#) and associate each access domain with a tenant. To prevent a tenant-level administrative user from viewing or making configuration changes to Prisma Access, you create an access domain, but you do not associate it with a tenant.

Because you associated the access domain to the device groups and template stacks for the tenant, the tenant-level administrative user has RBAC access at the tenant level and is able to perform configuration for that tenant only. Because you did not associate the access domain with a tenant in Prisma Access, the access domain is unable to view the Cloud Services plugin, which provides access to Prisma Access. In this way, you create a user who can perform tenant-level configuration tasks without being able to access, view, or make configuration changes to Prisma Access.

To remove Prisma Access access for an administrative-level user, complete the following task.

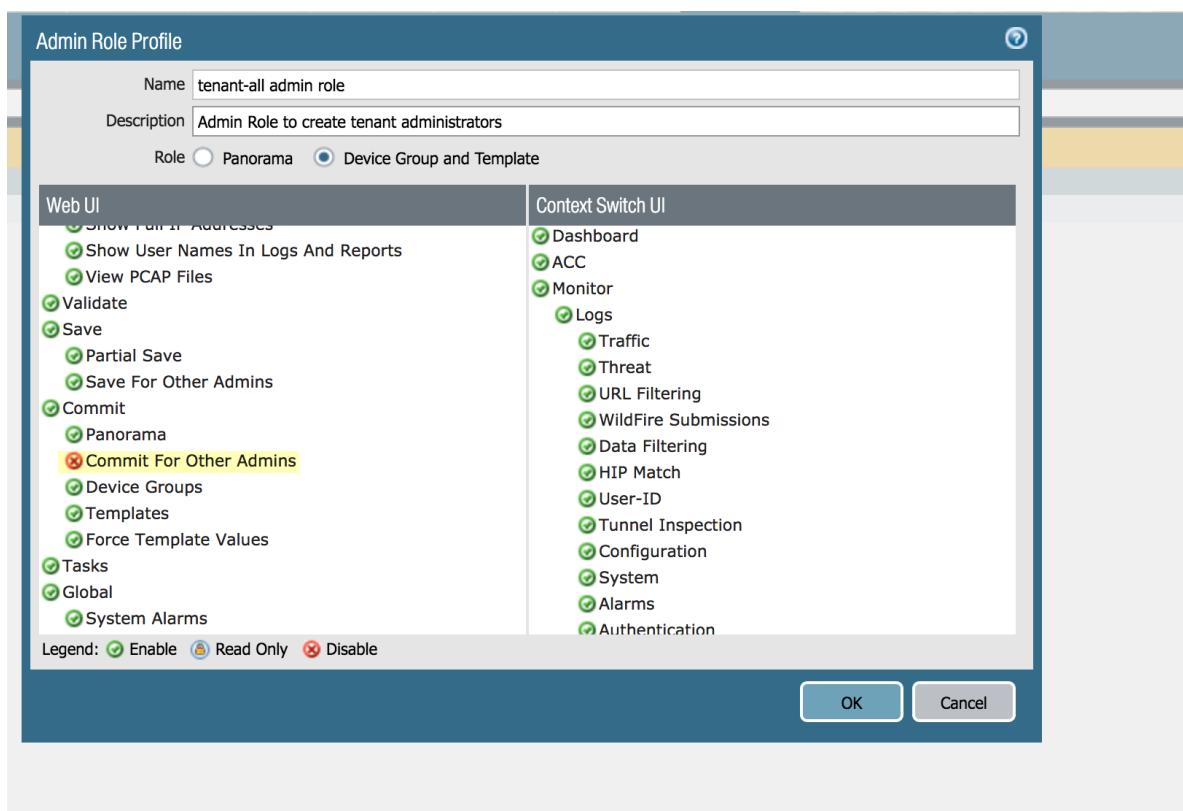


*This task assumes that you have [Add Tenants to Prisma Access](#) templates, template stacks, and device groups for the tenant; you'll be associating them to the tenant-level administrative user.*

### STEP 1 | Create an [administrative role](#) with a type of **Device Group and Template**.

1. Select **Panorama > Admin Roles**.
2. **Add** an Admin Role Profile with a **Role** of **Device Group and Template**.
3. Click **OK**.

You can create a single Admin Role Profile and share it across multiple tenants.

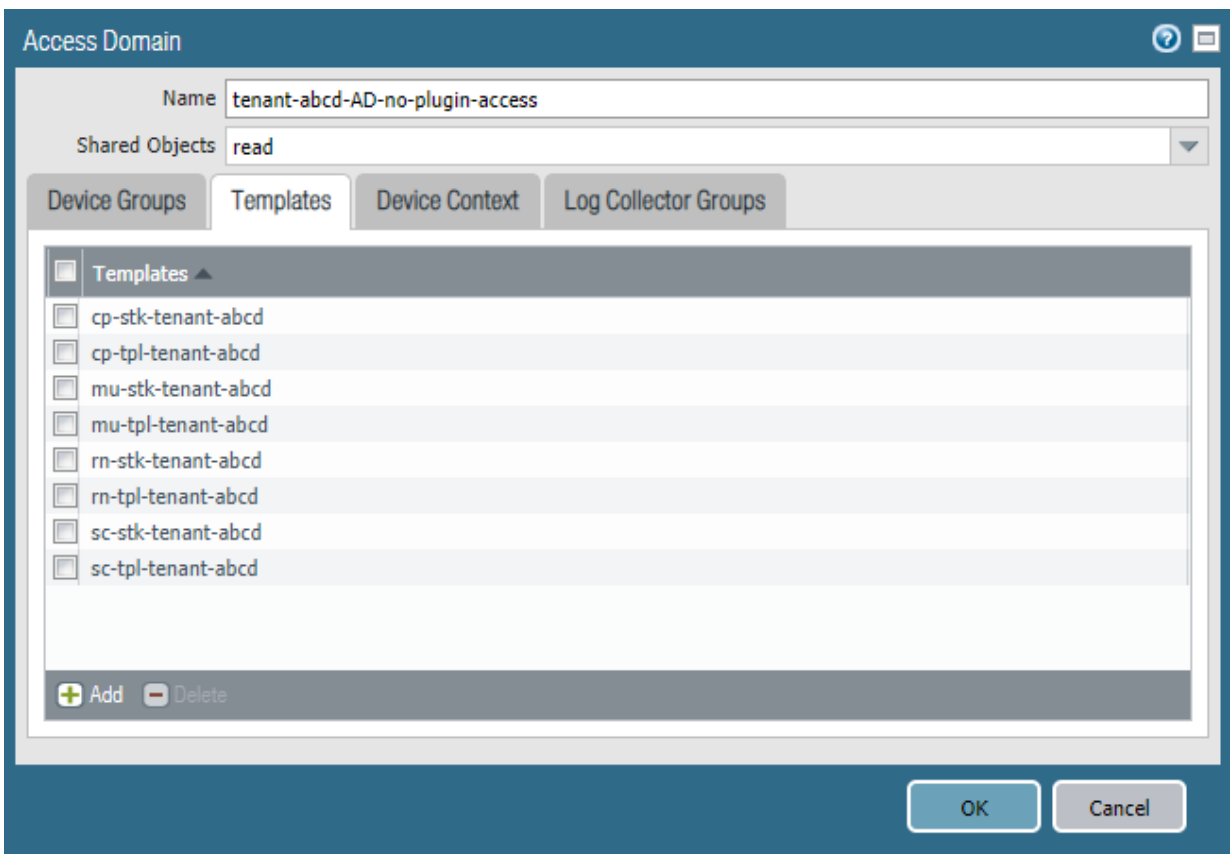
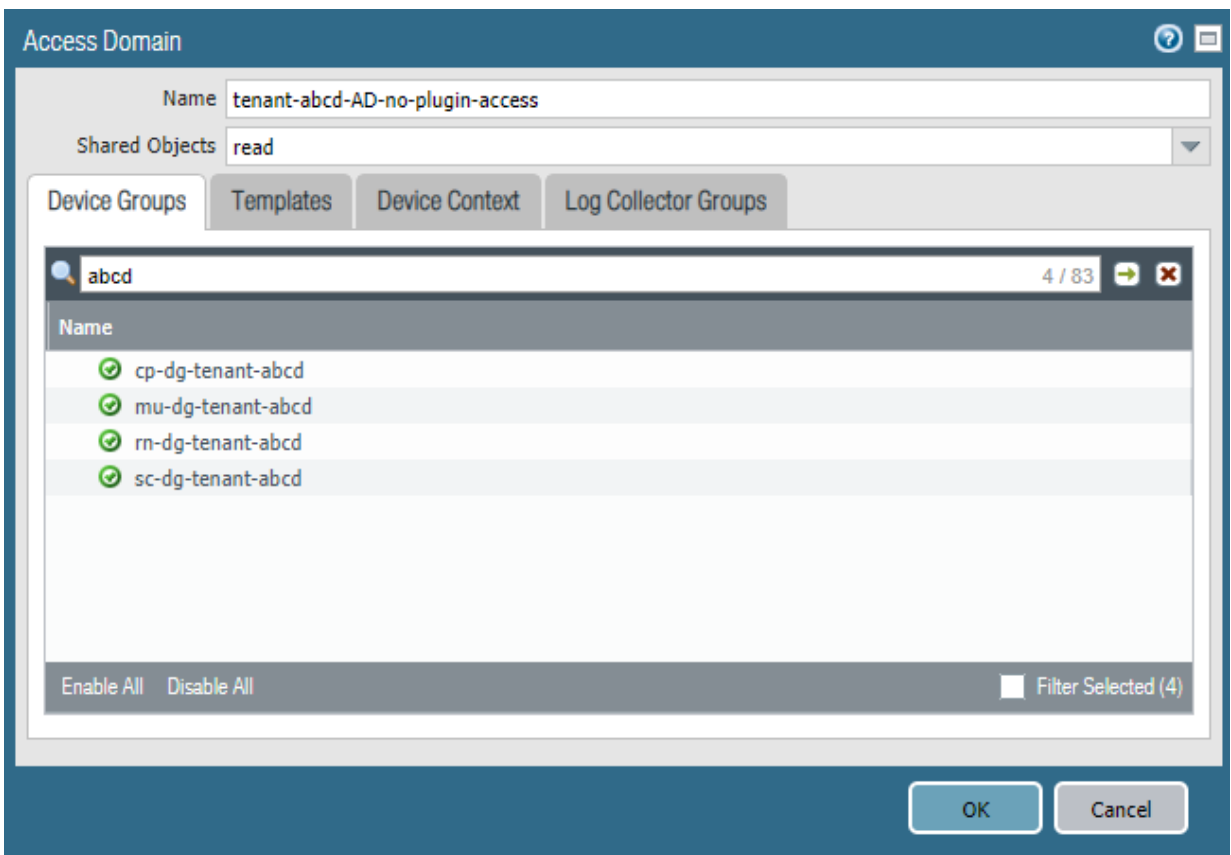


**STEP 2** | Select **Panorama > Access Domain** and **Add** an [Access Domain](#).

**STEP 3** | Specify the **Device Groups** and **Templates** associated with the tenant.



*If you created any device groups that are children or grandchildren of other device groups under the Shared parent device group, select only the device group at the lowest hierarchical level (child or grandchild); do not select the parent or you will have errors on commit.*



**STEP 4** | Create and configure an **Administrator** for the tenant-level administrative user, specifying the Access Domain you just created.

1. Select **Panorama > Administrators**.
2. **Add** an Administrator.
3. Enter and confirm a **Password** for the new Administrator.
4. Specify an **Administrator Type** of **Device Group and Template Admin**.
5. Specify the **Access Domain** that is associated with the device groups for that tenant.
6. Specify the **Admin Role** that you created in Step 1 for the tenant.

When you complete this example, the **abcd-tenant-no-plugin-access** Administrative user will have permissions based on what you defined in the Admin Role profile, but will not be able to view or configure the Cloud Services plugin (including Prisma Access). Note, however, that they will not be able to push any changes that they make to the cloud.

**Administrator**

Name: abcd-tenant-no-plugin-access

Authentication Profile: None

Use only client certificate authentication (Web)

Password: .....

Confirm Password: .....

Use Public Key Authentication (SSH)

Administrator Type: Device Group and Template Admin

Password Profile: None

Access Domain to Administrator Role

Access Domain	Admin Role
<input checked="" type="checkbox"/> tenant-abcd-AD-no-plugin-access	tenant-all admin role

+ Add - Delete

OK Cancel

**STEP 5** | Select **Commit > Commit to Panorama** and **Commit** your changes.

---

# Sort Logs by Device Group ID for External Logging

To sort the logs manually by tenant in Panorama, select **Monitor > Logs** and choose the **Device Group** associated with that tenant to display the logs for that device group. However, if you are forwarding your logs to an external device, you might have a need to sort those logs at the tenant level. To do so, find the device group ID in the logs that is associated with the device group and use that group ID-to-device group mapping to associate the logs with a tenant.

There are four fields associated with the device group in the logs: **DG Hierarchy Level 1**, **DG Hierarchy Level 2**, **DG Hierarchy Level 3**, and **DG Hierarchy Level 4**. These fields show the device group IDs in its hierarchy. The shared device group (level 0) is not included in this structure.

**DG Hierarchy Level 1** refers to the first device group level in the hierarchy. If you added children or grandchildren device groups, the **DG Hierarchy Level 2** through **DG Hierarchy Level 4** fields show the hierarchy from the child group to the great-grandchild group, respectively.

To find logs by tenant, complete the following task.

## STEP 1 | Find the device group IDs associated with the device group.

- To find this information using a CLI command, log into Panorama as a superuser (admin-level user), enter the `show readonly` command in configuration mode, and view the values in the **device-group** heading. The IDs for the device groups display under the device group name. The following example shows that the device ID for the **acme-sc** device group is **20**.

Note that these device groups are at the first level in the hierarchy (**DG Hierarchy Level 1**); you use that information in the query in the next step.

```
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 {
```

- To use an API query, enter the following API command:

```
/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>
```



For more information about using APIs with logs, see [Retrieve Logs \(API\)](#).

**STEP 2 |** Use the device group ID-to-device group name mapping to associate the logs with a tenant.

The following example shows an administrator retrieving the logs for Acme using the [Log Forwarding App](#) to create a [Syslog Forwarding Profile](#). Since the mapping example in [Step 1](#) retrieves the device group-to-device ID of 20 for Acme and the hierarchy is at Level 1, you use that in the query, along with the following parameters:

- A descriptive **Name** for the profile.
- The **Syslog Server** IP address (you can also specify an FQDN).
- The **Port** on which the server is listening.

The default port for Syslog messages over TLS is 6514.

- The **Facility** selected from the drop-down.

The screenshot shows the 'Syslog Forwarding Profile' configuration page. It includes the following fields and options:

- Name:** Syslog-To-EC2
- Syslog Server:** (Empty text input field)
- Port:** 6514
- Facility:** LOG\_USER (Dropdown menu)
- Status Notification:** Enter email address to send status notification (Text input field)
- Forwarding:** A table with columns for LOG VENDOR, LOG TYPE, and FILTER. It contains one entry for 'Firewall' with LOG TYPE 'Traffic' and FILTER '(dg\_hier\_level\_1 eq 20)'. There are '+Add' and '-Delete' buttons below the table.

Buttons for 'Cancel' and 'Save' are located at the bottom right of the form.

**STEP 3 |** Add the **Forwarding** parameters that select the logs you want to forward.

The following example shows the administrator creating a **Traffic** log using a **Custom** filter with a **Query** that selects the logs for Acme, based on the hierarchy level (**DG Hierarchy Level 1**) and the device group (20) you retrieved in [Step 1](#).



## Forwarding



\* Log Vendor: Firewall

\* Log Type: Traffic

Filter:  Predefined  Custom (Beta)

Query: (dg\_hier\_level\_1 eq 20)



# Use DLP With Prisma Access

Enforce your organization's data security standards to prevent accidental data misuse, loss, or theft using Data Loss Prevention (DLP) with the DLP plugin you install in Panorama.

- > [DLP Integration with Prisma Access](#)
- > [What is Enterprise DLP?](#)
- > [Register and Activate DLP on Prisma Access](#)
- > [Monitor DLP Status With the DLP Health and Telemetry App](#)
- > [Save Evidence for Investigative Analysis with Enterprise DLP](#)



---

# DLP Integration with Prisma Access

Data loss prevention (DLP) is a set of tools and processes that allow you to protect sensitive information against unauthorized access, misuse, extraction, or sharing. DLP on Prisma Access enables you to use Prisma Access to enforce your organization's data security standards and prevent the loss of sensitive data across mobile users and remote networks.

Starting with Prisma Access 2.0 Innovation, Prisma Access integrates its DLP capability to allow you to use the same DLP capabilities as that used in Panorama and on next-generation firewalls. This integration provides you with an improved experience that allows you to use the same DLP patterns, profiles, and rules as those used in next-generation firewalls. You activate this capability by [installing the DLP plugin](#) in Panorama.



*If you have an existing DLP on Prisma Access license, the locations of data patterns and data filtering profiles move in Panorama. See [Register and Activate DLP on Prisma Access](#) for details.*

DLP is an add-on license on Prisma Access.

---

# What is Enterprise DLP?

Data loss prevention (DLP) is a set of tools and processes that allow you to protect sensitive information against unauthorized access, misuse, extraction, or sharing. Starting with Prisma Access 2.0 Innovation, Prisma Access integrates DLP with the DLP plugin that you install on the Panorama management server, where you can centrally manage the data patterns and data filtering profiles that enforce your organization's data security standards and prevent the loss of sensitive data across mobile users and remote networks for your managed firewalls. The data patterns and data filtering profiles are designed to work across Prisma Access and any firewall models you manage in Panorama to provide consistent data security across all locations. To leverage Enterprise DLP with Prisma Access and next-generation firewalls, Panorama and managed firewalls must have internet connectivity.

To use the DLP plugin with Prisma Access, the Panorama that manages Prisma Access must be running a minimum version of 10.0.5, and any managed firewalls must be running a minimum PAN-OS release of 10.0.2.

For more information, including a list of what is supported, the steps you perform to create data patterns and data filtering profiles, and viewing logs and snippets, see the [Enterprise Data Loss Prevention \(DLP\) section](#) of the [Panorama Administrator's Guide](#).

---

# Register and Activate DLP on Prisma Access

Data Loss Prevention (DLP) on Prisma Access enables you to secure remote networks and users, and requires an add-on license.

To register and the Enterprise DLP plugin to use with Prisma Access, complete one of the following procedures:

- To register and activate the Enterprise DLP plugin for a new DLP deployment, follow the procedure in [Install the Enterprise DLP Plugin—New DLP Deployments](#).
- To upgrade to the Enterprise DLP plugin for a Prisma Access deployment that uses DLP on Prisma Access, follow the procedure in [Upgrade to the Enterprise DLP Plugin—Existing Enterprise DLP on Prisma Access Deployments](#).

## Preinstallation Requirements

Before you install the Enterprise DLP plugin, make sure that your Prisma Access deployment has the following requirements:

- Make sure that you have purchased the Enterprise DLP add-on license for Prisma Access.

You use the [DLP plugin](#) to activate the DLP functionality for use with Prisma Access, but it requires an Enterprise DLP add-on license, which includes the Authorization code you need when you activate your license on the Palo Alto Networks [Customer Support Portal \(CSP\)](#).

- On the Panorama appliance that manages Prisma Access, make sure that you have the minimum Panorama, content versions, DLP plugin, and Prisma Access versions.
  - The minimum required [Panorama](#) version is 10.0.5.
  - The minimum required [content version](#) is 8334-6362.
  - The minimum required [DLP plugin](#) version is 1.0.3.
  - The minimum required Prisma Access version is 2.0 Innovation and the minimum Cloud Services plugin version is version 2.0.0.h3-innovation.



*The DLP plugin is not supported on 2.0 Preferred; use [Enterprise DLP on Prisma Access](#) instead.*

If you need to upgrade the Panorama or content version, [install the content and software updates on Panorama](#).

- Make sure that you have [installed the device certificate on Panorama](#).
- If you manage on-premise firewalls with Prisma Access, you should [install the device certificate for managed firewalls](#)
- Make sure that your Prisma Access dataplane [has been upgraded](#).

## Install the Enterprise DLP Plugin—New DLP Deployments

After you have completed the [Preinstallation Steps](#), complete the following steps to install the DLP plugin on Panorama.

**STEP 1 |** From the Panorama that manages Prisma Access, select **Panorama > Plugins** and search for the latest version of the DLP plugin.

Prisma Access requires a minimum DLP plugin version of 1.0.3.

**STEP 2 | Download and Install** the Enterprise DLP plugin on Panorama.

**STEP 3 | Commit** your changes to Panorama by selecting **Commit > Commit to Panorama** and **Commit** your configuration changes.

**STEP 4 | (Optional)** if your Panorama manages on-premise firewalls as well as Prisma Access, commit and push the changes to your managed firewalls.

This step is required in order for Enterprise DLP data filtering profile names to appear in Data Filtering logs.

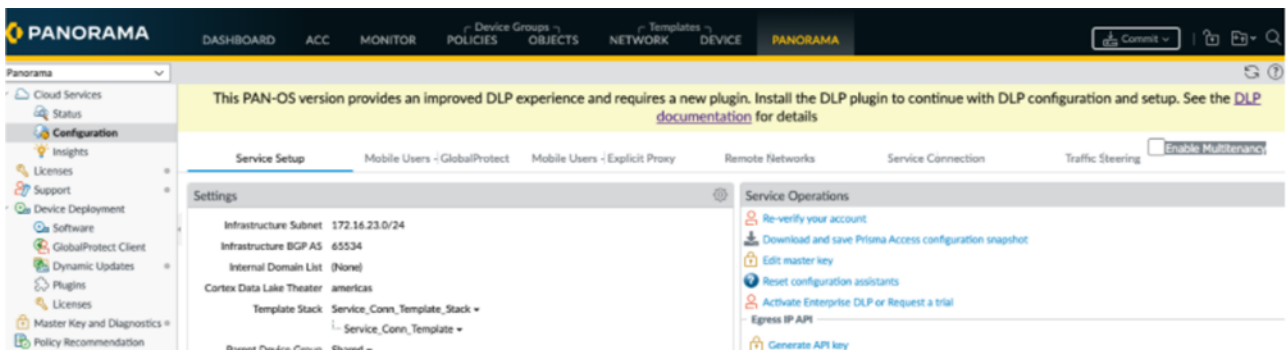
1. Select **Commit > Commit to Panorama** and Commit your configuration changes.
2. Select **Commit > Push to Devices** and **Edit Selections**.
3. Select **Device Groups** and **Include Device and Network Templates** and click **OK**.
4. **Push** your configuration changes to your managed firewalls.

## Upgrade to the Enterprise DLP Plugin—Existing Enterprise DLP on Prisma Access Deployments

If you have an existing DLP on Prisma Access deployment, complete the following steps.

**STEP 1 |** After you have [completed the Enterprise DLP plugin preinstallation requirements](#), have had your [Prisma Access dataplane upgraded](#), and have [upgraded and installed the Cloud Services plugin](#) to a minimum version of the Cloud Services plugin 2.0 Innovation, select **Panorama > Cloud Services > Configuration**.

A banner displays, requesting that you upgrade and install to the Enterprise DLP plugin for an improved DLP experience.



**STEP 2 | Install and activate the DLP plugin.**

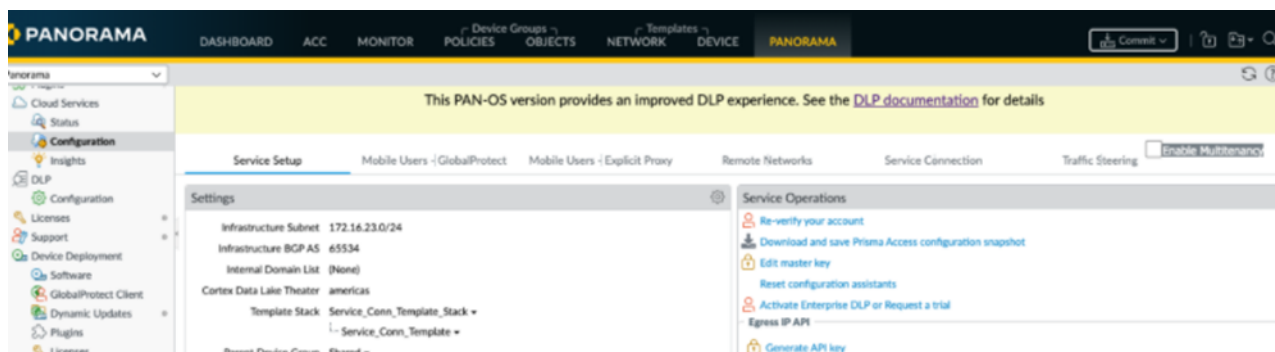
After you upgrade, if you have existing [data patterns](#) and [data filtering profiles](#) that you use for Enterprise DLP on Prisma Access, the migration process moves them to the following locations in Panorama:

- Data patterns move from **Objects > Custom Objects > Data Patterns** to **Objects > DLP > DLP Data Patterns**.
- Data filtering profiles move from **Objects > Security Profiles > Data Filtering** to **Objects > DLP > DLP Data Filters**.
- You do not have to verify that the Panorama and Prisma Access belong to the same CSP account; you have already associated the Panorama serial number with the CSP account [when you installed Prisma Access](#).



- You do not have to activate the Enterprise DLP plugin on Prisma Access. However, if you have managed firewalls, you should complete the steps to enter the auth code for the target managed firewalls.

After the migration process completes, a banner displays indicating that the plugin was installed.



---

# Monitor DLP Status With the DLP Health and Telemetry App

With an Enterprise DLP license, you can access the DLP Health & Telemetry app, which provides visibility into the health of the DLP service in real time. DLP service insights are available for any Palo Alto Networks product where you purchased an Enterprise DLP license.

- [Access the DLP Health and Telemetry Dashboard](#)
- [Monitor DLP Service Status](#)

## Access the DLP Health and Telemetry Dashboard

DLP Health and Telemetry Dashboard is accessible from Enterprise DLP app on the hub. All you need is an [account administrator role](#) or [app administrator role](#) on the hub and a valid Enterprise DLP license associated with that support account.

**STEP 1** | Log in to the hub with your SSO credentials.

**STEP 2** | Select **Enterprise DLP**.



## Monitor DLP Service Status

The Dashboard displays real-time DLP status. If you experience issues with DLP (for example, the Prisma Access web interface doesn't display data patterns or data profiles), verify that the DLP service status is **Operational**.

**PRISMA SAAS**



Operational

November 19 2020 at 2:28 PST

**PRISMA ACCESS**



Operational

November 19 2020 at 2:28 P

**STEP 1** | Log in to Enterprise DLP app.

**STEP 2** | Observe the **DLP Service Status** and the **Last Updated** timestamp.

Status	Description
Operational	DLP services are up and running.
Degraded Experience	DLP services are up and running, but not operating at optimally.
Service Unavailable	DLP services are down.
Planned Maintenance	DLP services are down due to scheduled maintenance.

---

# Save Evidence for Investigative Analysis with Enterprise Data Loss Prevention (DLP)

Create a storage bucket to connect to the DLP app on the hub to automatically store files scanned by the DLP cloud service which match your Enterprise Data Loss Prevention (DLP) data filtering profiles. After a file is successfully stored, you can download the file for further investigation.

- [Set Up Cloud Storage to Save Evidence](#)
- [Download Files for Evidence Analysis](#)

## Set Up Cloud Storage to Save Evidence

Amazon Web Services (AWS) users can configure an S3 bucket to automatically upload all files that match an Enterprise Data Loss Prevention (DLP) data filtering profile for Enterprise DLP leveraged on Prisma Access and Next-Generation Firewalls.

To store your files scanned by the DLP cloud service, you must create an S3 bucket and Identity and Access Management (IAM) role that allows the DLP cloud service access to automatically store files. Palo Alto Networks provides you a JSON data containing the required policy permissions to create the IAM role. Files uploaded to your S3 bucket are automatically named using a unique Report ID for each file. The Report ID is used to search and download specific files for more in depth investigation.

In case of connection issues to your S3 bucket due to configuration error or change in settings on the bucket, an email is automatically generated and sent to the admin that originally connected the DLP app to the storage bucket and to the user who last modified the storage bucket connection settings on the DLP app. This email is sent out every 48 hours until the connection is restored.



*Files that are scanned by the DLP cloud service while the DLP app is disconnected from your storage bucket cannot be stored and are lost. This means that all impacted files are not available for download. However, all snippet data is preserved and can still be viewed on the DLP app on the hub.*

*File storage automatically resumes after the connection status is restored.*

**STEP 1** | [Log in to the Amazon AWS console.](#)

**STEP 2** | Create a public S3 storage bucket to store files scanned by the Enterprise DLP cloud service.

1. Select **Services** > **Storage** > **S3** > **Buckets** and **Create bucket**.
2. Enter a descriptive **Bucket name**.
3. Select the **AWS Region** for the S3 bucket.
4. In the Default encryption section, **Enable** server-side encryption and select your preferred encryption key type.

This is required to successfully associate the S3 bucket with the hub.

### Default encryption

Automatically encrypt new objects stored in this bucket. [Learn more](#)

#### Server-side encryption

- Disable
- Enable

#### Encryption key type

To upload an object with a customer-provided encryption key (SSE-C), use the AWS CLI, AWS SDK, or Amazon S3 REST API.

- Amazon S3 key (SSE-S3)  
An encryption key that Amazon S3 creates, manages, and uses for you. [Learn more](#)
- AWS Key Management Service key (SSE-KMS)  
An encryption key protected by AWS Key Management Service (AWS KMS). [Learn more](#)

## 5. Create bucket.

### STEP 3 | Create the IAM role for the S3 bucket.

This role is required to allow the DLP cloud service to write to the S3 bucket.

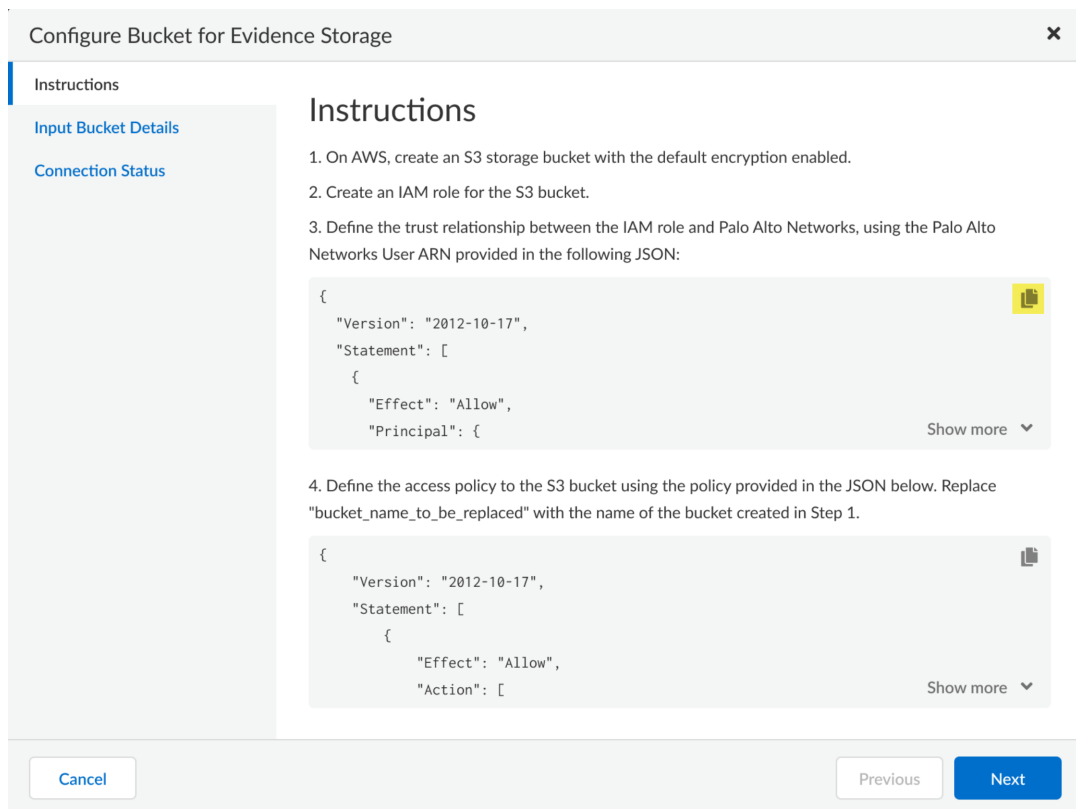
1. Select **Services > Security, Identity, and Compliance > IAM > Access management > Roles and Create role**.
2. For the type of trusted entity, select **S3** from the list displayed in the Choose a use case section.
3. In the Select your use case section, select **S3**.
4. Select **Next: Permissions, Next: Tags and Next: Review**.

The permissions policy to create the trust relationship is configured the following step.

5. Enter a descriptive **Role name** for the IAM role.
6. **Create role**.

### STEP 4 | Configure the trust relationship for the IAM role.

1. Obtain the trust relationship using JSON provided by Palo Alto Networks.
  1. Log in to the [DLP app on the hub](#)
  2. Select **Settings** and **Edit** the Cloud Storage Bucket.
  3. In the **Instructions**, copy the JSON provided to define the trust relationship between the IAM role and Palo Alto Networks.



2. In AWS, select **Services > Security, Identity, and Compliance > IAM > Access management > Roles** and select the IAM role you created.
3. Select **Trust relationships** and **Edit trust relationship**.
4. Paste the trust relationship JSON you copied from the DLP app in the hub to define the trust relationship between the IAM role and Palo Alto Networks.

## Edit Trust Relationship

You can customize trust relationships by editing the following access control policy document.

### Policy Document

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": "arn:aws:iam::289103992286:user/panw_dlp_evidence_storage"
8       },
9       "Action": "sts:AssumeRole"
10    }
11  ]
12 }
```

5. **Update Trust Relationship.**

**STEP 5 |** Create a policy to define the access policy and assign the policy to the IAM role you created.

Palo Alto Networks provides you with a JSON containing the required access policy configuration that you can copy and paste.

1. Obtain the trust relationship using JSON provided by Palo Alto Networks.
  1. Log in to the [DLP app on the hub](#)
  2. Select **Settings** and **Edit** the Cloud Storage Bucket.

3. In the **Instructions**, copy the JSON provided to define the trust relationship between the IAM role and Palo Alto Networks.

Configure Bucket for Evidence Storage

Instructions

Input Bucket Details

Connection Status

### Instructions

1. On AWS, create an S3 storage bucket with the default encryption enabled.
2. Create an IAM role for the S3 bucket.
3. Define the trust relationship between the IAM role and Palo Alto Networks, using the Palo Alto Networks User ARN provided in the following JSON:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
```

Show more

4. Define the access policy to the S3 bucket using the policy provided in the JSON below. Replace "bucket\_name\_to\_be\_replaced" with the name of the bucket created in Step 1.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
```

Show more

Cancel Previous Next

2. In AWS, select **Services > Security, Identity, and Compliance > IAM > Access management > Policies and Create policy.**
3. Select **JSON** and pasted the JSON provided by Palo Alto Networks.

Throughout the JSON, you must delete all instances of `bucket_name_to_be_replaced` with the S3 bucket ARN you created.

You can find the ARN of your S3 bucket by selecting **Services > Storage > S3**. Then select the S3 bucket and view the **Properties**.

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor JSON [Import managed policy](#)

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "s3:GetEncryptionConfiguration",
8         "s3:ListBucket",
9         "s3:GetBucketAcl",
10        "s3:GetBucketLocation"
11      ],
12      "Resource": "arn:aws:s3:::bucket_name_to_be_replaced"
13    },
14    {
15      "Effect": "Allow",
16      "Action": [
17        "s3:PutObject",
18        "s3:GetObject"
19      ],
20      "Resource": "arn:aws:s3:::bucket_name_to_be_replaced/*"
21    },
22    {
23      "Effect": "Allow",
24      "Action": "s3:GetBucketPublicAccessBlock",
25      "Resource": "arn:aws:s3:::bucket_name_to_be_replaced"
26    }
27  ]
28 }

```

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

4. Select **Next: Tags** and **Next: Review**
5. Enter a descriptive **Name** for the access policy and **Create policy**.
6. Select **Roles** and select the IAM role you created.
7. Select **Permissions** > **Attach policies** to select the access policy you created and **Attach policies**.

#### STEP 6 | Configure the S3 bucket for evidence file storage.

1. Log in to the [DLP app on the hub](#).

If you do not already have access to the DLP app on the hub, see [the hub Getting Started Guide](#). Only Superusers can access the hub.



*Access to evidence storage settings and files on the hub is allowed only for an [account administrator](#) or [app administrator](#) roles with a valid Enterprise DLP license associated with that support account. This is to ensure that only the appropriate users have access to report data and evidence.*

2. Select **Settings** and **Edit** the Public Cloud Storage Bucket.
3. Enter the **S3 Bucket Name** of the bucket you created.
4. Enter the **Role ARN** for the IAM role you created.
5. Select the **AWS Region** where the bucket is located.



6. Select **Next** to verify the connections status your S3 bucket.  
Select **Save** if the hub can successfully connect your bucket.  
If the hub cannot successfully connect your bucket, select **Previous** and edit the bucket connection settings.
7. In the DLP **Settings**, **Enable** storage of sensitive files for the platform in which you are leveraging Enterprise DLP.

You can only enable storage of sensitive files for platform for which you have activated the Enterprise DLP license. For example, you only have the option to enable evidence storage for Next-Generation Firewalls if you activated the Enterprise DLP license on Panorama.

## Download Files for Evidence Analysis

After you successfully [Set Up Cloud Storage to Save Evidence](#) to store files that match your Enterprise Data Loss Prevention (DLP) data filtering profiles, you can download to your local device any files scanned by the DLP cloud service to allow for in-depth investigation.

Files scanned by the DLP cloud service while the DLP app is disconnected from your storage bucket are not stored in your S3 bucket. This means that all impacted files are not available for download. However, all snippet data is preserved and can still be viewed on the DLP app on the hub.

**STEP 1 | Set Up Cloud Storage to Save Evidence** if not already set up.

The files available to download are only files scanned by the DLP cloud service after you successfully connected the DLP app on the hub to your storage bucket.

**STEP 2 | Log in to the DLP app on the hub.**

If you do not already have access to the DLP app on the hub, see [the hub Getting Started Guide](#). Only Superusers can access the hub.

**STEP 3 | Select Reports and enter a Report ID to Search.**

- For Prisma Access users leveraging Enterprise DLP, [log in to the Amazon AWS console](#) and access the S3 storage bucket you connected. The object Name is the Report ID.
- For Panorama users, [log in to the Panorama web interface](#) and select **Monitor > Logs > Data Filtering** and **Filter** the data filtering logs by entering ( **subtype eq dlp** ). Locate the **Report ID** column to obtain the Report ID for the report you want to download.

GENERATE TIME	CAT...	FILE NA...	F... U...	THREAT ID/NAME	FROM ZONE	TO ZONE	REPORT ID
12/03 16:45:25	test	test...		GLBA-2	UID-Client-Zone	UID-Server-Zone	72663124
11/25 11:00:56	test	Posi...		11995143	UID-Client-Zone	UID-Server-Zone	2359559322
11/25 11:00:20	test	Posi...		11995143	UID-Client-Zone	UID-Server-Zone	2359559322
11/24 23:11:11	test	GP...		GLBA-1	UID-Client-Zone	UID-Server-Zone	2393181426
10/27 22:34:25	test	GP...		Last-test	UID-Client-Zone	UID-Server-Zone	1569169488
10/27 22:24:36	test	GP...		1002-c76-alert	UID-Client-Zone	UID-Server-Zone	2285742899
10/27 22:13:40	test	GP...		1002-c76-alert	UID-Client-Zone	UID-Server-Zone	2285742899

**STEP 4 | Review report summary and click the download button to download the file to your device.**

**Report Details**

**Report**

**General**

- Report ID: 3922280160
- Scan Date: March 17 2021 at 10:30 PDT
- Channel:
- Data Profile: Default\_Dummy\_Data\_Profile
- Asset: ccn\_ssn
- Asset Type:
- Asset Size: 153 bytes

**Matching Data Patterns**

By Confidence Level: High (1 Patterns) Medium (1 Patterns) Low (8 Patterns)

National Id - US Social Security Number - SSN  
2 occurrences

Request Snippets

# *IoT Security Integration with Prisma Access*

The following section describes how you configure and use the IoT Security implementation with Prisma Access.

- > [Use IoT Security with Prisma Access](#)
- > [IoT Security Integration with Prisma Access](#)
- > [IoT Security Integration Status with Prisma Access](#)



---

# Use IoT Security with Prisma Access

IoT Security is an on-demand cloud subscription service designed to discover and protect the growing number of connected “things” on your network. Unlike IT devices such as laptop computers that perform a wide variety of tasks, IoT devices tend to be purpose-built with a narrowly defined set of functions. As a result, IoT devices generate unique, identifiable patterns of network behavior. Using machine learning and AI, IoT Security recognizes these behaviors and identifies every device on the network, creating a rich, context-aware inventory that’s dynamically maintained and always up to date.

After it identifies a device and establishes a baseline of its normal network activities, it continues monitoring its network activity so it can detect any unusual behavior indicative of an attack or breach. If it detects such behavior, IoT Security notifies administrators through security alerts in the IoT Security portal and, depending on each administrator’s notification settings, through email and SMS notifications.

You get the same benefits from integrating IoT Security with Prisma Access as you do from integrating it with next-generation firewalls. IoT is available as an add-on; after you purchase the add-on, you [activate your product](#) during [Prisma Access installation](#).

For an overview of the IoT integration with Prisma Access and the steps you take to configure it, see the following sections.

- [IoT Security Integration with Prisma Access](#)
- [IoT Security Integration Status with Prisma Access](#)

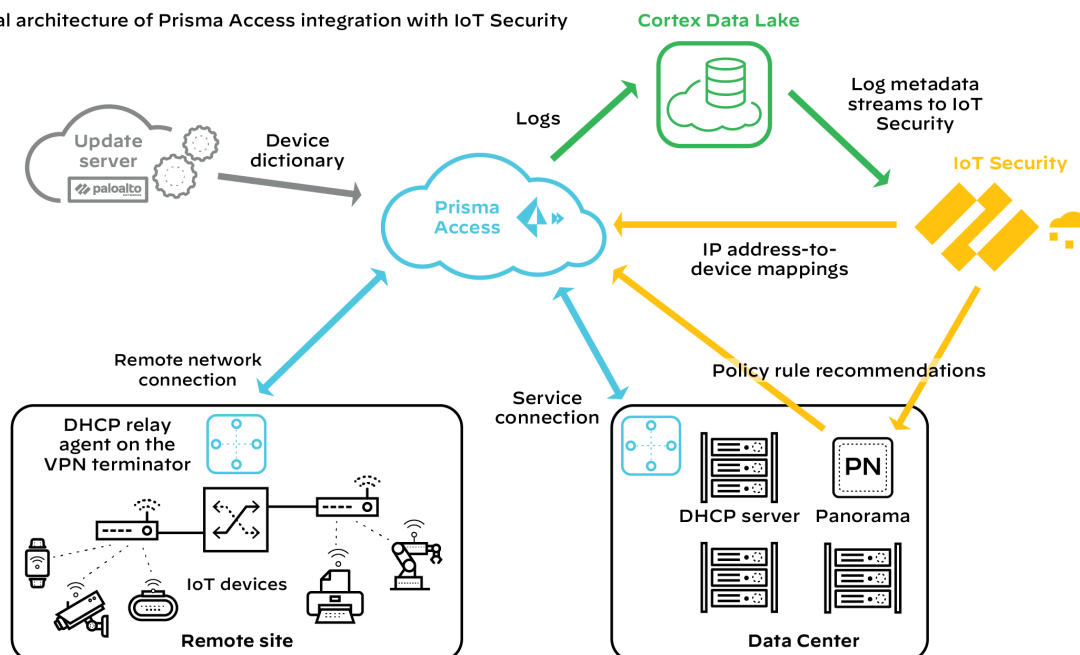
# IoT Security Integration with Prisma Access


[Prisma Access](#) uses a cloud-based infrastructure that lets you avoid the challenges of sizing firewalls and computing resource allocation while securing remote networks and mobile users. To identify IT and IoT devices at your remote sites, detect IoT device vulnerabilities, and discover threats posed to these devices and the network, Prisma Access can integrate with IoT Security through a purchased add-on. In addition, IoT Security also provides Prisma Access with policy rule recommendations through Panorama to permit only acceptable network behavior and block anomalous behavior from your IoT devices.

For IoT Security to identify IT and IoT devices, and analyze risk levels and detect security alerts on IoT devices, it must be able to access network traffic metadata. The more data it has to work with, the more accurate and faster it can be. Therefore, it's critical to do two things to collect as much traffic metadata as possible. First, design your network strategically so that Prisma Access sees all traffic from your remote sites, including DHCP traffic. Then apply policy rules to as much traffic as you can and enable [logging and log forwarding](#) on these rules to send traffic metadata to [Cortex Data Lake](#).

DHCP traffic is particularly important to IoT Security. It provides IoT Security with useful data, including a mapping of the IP address to MAC address of each DHCP client, which is a critical element of the [IP address-to-device mappings](#) used for device identification. To obtain this data, ensure that a DHCP server is in your data center or in a similar centralized site and a DHCP relay agent is on the customer premises equipment (CPE) where the remote network connection terminates at each site. Each relay agent forwards the DHCP messages it receives from DHCP clients through the [Prisma Access service infrastructure](#) to the IP address of the DHCP server. On the policy rule allowing DHCP traffic from the remote sites to the DHCP server, be sure logging and log forwarding are enabled so that Prisma Access sends DHCP traffic logs to Cortex Data Lake. In fact, if you have not already done so, enable logging and log forwarding on all policy rules. With log forwarding enabled, Prisma Access sends its logs to Cortex Data Lake, which then streams metadata to IoT Security for analysis.

Logical architecture of Prisma Access integration with IoT Security



 *Prisma Access cannot forward IoT Security logs for Layer 2 traffic or Layer 3 traffic where both the source and destination are in the same site because such traffic never reaches it. Consequently, identifying these devices might take IoT Security longer and its confidence*

---

*might be lower than it would if a firewall was positioned directly on the network and had access to these types of traffic.*

After IoT Security has sufficient information to identify devices from their network behavior, it provides Prisma Access with IP address-to-device mappings and Panorama with [policy recommendations](#) that the Panorama administrator can import and then push to Prisma Access to enforce policy on IoT device traffic. In addition, Prisma Access downloads device dictionary files from the update server. The device dictionary lists various device attributes with which the Panorama administrator can construct Security policy rules. The combination of IP address-to-device mappings, policy recommendations, and device dictionary files comprise the elements of the [Device-ID](#) feature introduced in PAN-OS 10.0.

### Required Panorama Configuration

To allow the Panorama that manages Prisma Access to communicate with IoT security and to check that you have enabled Enhanced Application Logs on your log forwarding profiles, complete the following steps. These steps are required to enable IoT integration with Prisma Access.

1. Manually configure the address of the edge server to allow Panorama to communicate with IoT Security.
  1. [Log in to the Panorama CLI](#).
  2. Enter `configure` to get into configuration mode.
  3. Enter the following command: `set deviceconfig setting iot edge address iot.services-edge.paloaltonetworks.com`
  4. Enter `commit` to commit the changes to the running configuration.

The configuration looks like this:

```
admin@yourcompany.com(active)> configure
```

```
Entering configuration mode
```

```
[edit]
```

```
admin@yourcompany.com(active)# set deviceconfig setting iot edge address iot.services-edge.paloaltonetworks.com
```

```
[edit]
```

```
admin@yourcompany.com(active)# commit
```

```
Commit job 12345 is in progress. Use Ctrl+C to return to command prompt
```

2. Make sure that your Log Forwarding profiles have the ability to collect [Enhanced Application Logs](#) by selecting **Objects > Log Forwarding** under the **Remote\_Network\_Device\_Group** device group or a parent device group, opening your log forwarding profiles, and making sure that **Enable enhanced application logging to Cortex Data Lake** is selected.

### Requirements for using IoT Security with Prisma Access

To use the IoT Security add-on with Prisma Access, check that your deployment meets the following requirements:

1. Prisma Access is running the Prisma Access 2.0-Innovation release or later.
2. You have purchased and activated licenses for Cortex Data Lake and the IoT Security add-on for Prisma Access.
3. You're using Panorama 10.0 or later to manage Prisma Access.



*With a mixed deployment of Prisma Access and on-premises next-generation firewalls, you must use the same Panorama management system to manage them and the same IoT Security tenant for both.*

4. DHCP is being served from a data center or from some other central site.

- 
5. The Prisma Access infrastructure provides routing from remote sites to data center resources, which include the DHCP server.
  6. A DHCP relay agent on the VPN terminator at all remote sites points to the IP address of the DHCP server in the data center.
  7. Security policy rules in Prisma Access control traffic to the Internet, the data center, and other remote sites. Logging is enabled on these policies and Prisma Access forwards logging data to Cortex Data Lake, which streams it to IoT Security.



*IoT Security uses Enhanced Application logs (EALs), traffic logs (which include DHCP traffic), threat logs, and wildfire logs. Make sure that your policy rules have logging enabled and are forwarding EALs and traffic logs to Cortex Data Lake. Although the last two log types are not required for IoT Security to function, we recommend getting licenses for threat prevention and Wildfire and forwarding their logs as well because they help improve risk assessment and malware detection.*

Once these requirements are met, use IoT Security to monitor traffic metadata, identify IoT devices, detect vulnerabilities, discover threats, and prepare policy rule recommendations. Import policy rule recommendations from IoT Security into Panorama or configure Device-ID policy rules directly in Panorama and then push them to Prisma Access for policy enforcement on IoT device traffic.



# IoT Security Integration Status with Prisma Access

In the Administration section of the IoT Security portal, the Sites and Firewalls pages provide the status of next-generation firewalls with active IoT Security subscriptions. They show the total number of firewalls at each site, the connection status of each firewall, the total number of log events they've forwarded to logging services, and the types of logs they're sending. However, when Prisma Access subscribes to IoT Security through the IoT Security add-on, the information displayed on these pages is unlike that shown for next-generation firewalls.

## Sites

When Prisma Access is using an IoT Security add-on, the site name for it on the **Administration > Sites** page is simply "Prisma Access". Whether a single Prisma Access instance is protecting one or a hundred remote sites, IoT Security remains unaware of their number. From the perspective of IoT Security, the numbers of devices and IoT devices come from a single Prisma Access entity regardless of how many remote sites it protects.

The following screen capture shows a mixed deployment of Prisma Access and several sites with on-premises next-generation firewalls for comparison.

Status	Name	Devices	IoT Devices	Risk	Subnets	Total Log Eve...	Total Firewalls	
	Prisma Access	8420	101	22	7	—	—	
	test-1	433	15	23	10	4B	70	⋮
	test-2	33295	9772	24	148	1.1M	67	⋮
		2363	2363	22				⋮

The Sites page contains the following types of information for Prisma Access:

**Status:** A green cloud means that IoT Security is connected to Prisma Access and is receiving logs. A red cloud with a line through it means that IoT Security does not detect logs forwarded from Prisma Access to Cortex Data Lake.

**Name:** Prisma Access

**Devices:** This is the total number of devices that IoT Security identified across all remote sites under Prisma Access protection.

**IoT Devices:** This is the total number of IoT devices that Prisma Access identified across all its remote sites. This is a subset of the total shown in the Devices column.

**Risk:** This is the overall risk score calculated for all IoT devices protected by Prisma Access.

**Subnets:** This is the total number of subnets across all Prisma Access remote sites. Because IoT Security has no visibility into how many sites Prisma Access is protecting, this total can come from a single site with a single subnet, a single site with multiple subnets, multiple sites each with a single unique subnet, multiple sites with multiple subnets, or any combination of these scenarios.

---

**Total Log Events:** Not shown for Prisma Access

**Total Firewalls:** Not shown for Prisma Access



*Prisma Access does not have an Action menu, which is what pops up when you click the three vertical dots icon on the far right of a row ( ⋮ ). The Action menu provides options to edit a site, assign firewalls to a site, and delete a site. It's available for sites with on-premises next-generation firewalls but not for Prisma Access.*

## Firewalls

This page is not particularly applicable to Prisma Access. If you are using IoT Security exclusively with Prisma Access, the top of the page shows a total of two sites, one for Prisma Access and one for the default site, which is where IoT Security initially assigns on-premises firewalls. The Active and Inactive status will be 1 or 0 depending on whether IoT Security detects any logs from Prisma Access to Cortex Data Lake in the last 30 minutes.

IoT Security displays the number of system alerts relating to Prisma Access. These pertain to the reception of requests from Prisma Access for policy recommendations and IP address-to-device mappings. For example:

```
IoT Security hasn't received any requests for policy recommendations in the past 30 minutes.
```

```
IoT Security is receiving requests for IP address-to-device mappings again.
```

Click the number of system alerts at the top of the Firewalls page to open the Alerts > System Alerts page to see them. The source for Prisma Access system alerts is always `All firewalls`.

The rest of the Firewalls page doesn't have any data relevant to Prisma Access.

SITES **FIREWALLS** 1 Day

Overview

2 Sites    0 Firewalls    0 Active    0 Inactive    0 System Alerts

● Firewall Request Status ⓘ

Firewall Log Type Status

Type	Status	Latest Log	Log Events	Log Bytes
Total	● No Live Data	-	0	0B
EAL	● No Live Data	-	0	B
DHCP	● No Live Data	-	0	B
DHCP ACK	● No Live Data	-	0	B
Traffic	● No Live Data	-	0	B
Threat	● No Live Data	-	0	B
ARP	● No Live Data	-	0	B

Firewalls (0)

Download    Filter

<input type="checkbox"/>	Status	Serial	Host	IoT D...	EAL	DHCP	Traffic	ARP	Soft...	First ...	Lates...	Licen...	Site
No rows to show													

If your deployment includes a mix of Prisma Access and on-premises next-generation firewalls, then this page contains the information mentioned above for Prisma Access and [much more information](#) about firewalls and the logs they provide.



# Create and Configure Prisma Access for Clean Pipe

Use *Prisma Access for Clean Pipe* to quickly and easily configure multiple instances of clean outbound internet connections.

- > [Prisma Access for Clean Pipe Overview](#)
- > [Configure Prisma Access for Clean Pipe](#)



---

# Prisma Access for Clean Pipe Overview

To allow organizations that manage the IT infrastructure of other organizations, such as service providers, MSSPs, or Telcos, to quickly and easily protect outbound internet traffic for their tenants, Palo Alto Networks provides Prisma Access for Clean Pipe. A service provider, MSSP, or Telco can route their customers (configured as tenants) to Prisma Access for Clean Pipe using a Partner Interconnect. After the traffic crosses the Partner Interconnect, it will be sent to a tenant-dedicated instance of the Clean Pipe for security, and then routed to the Internet.

Prisma Access for Clean Pipe also provides an API that you can use to quickly and easily create Clean Pipes for your tenants.

- [Clean Pipe Use Cases](#)
- [Clean Pipe Examples](#)
- [Clean Pipe and Partner Interconnect Requirements](#)

## Clean Pipe Use Cases

Use Prisma Access for Clean Pipe if you meet all of the following use cases:

- You manage a network deployment with a large number of tenants.

For example, you are a service provider, Telco, or MSSP who manages and maintains the networks of many different organizations (up to tens of thousands).

- You want a way for each tenant in your deployment to have their outbound internet traffic secured.
- You need a fast and scalable way to onboard Clean Pipes for the organizations whose networks you manage.
- With the exception of outbound internet security, you do not have additional requirements to protect the mobile users, headquarters, or branch locations of the networks you manage.

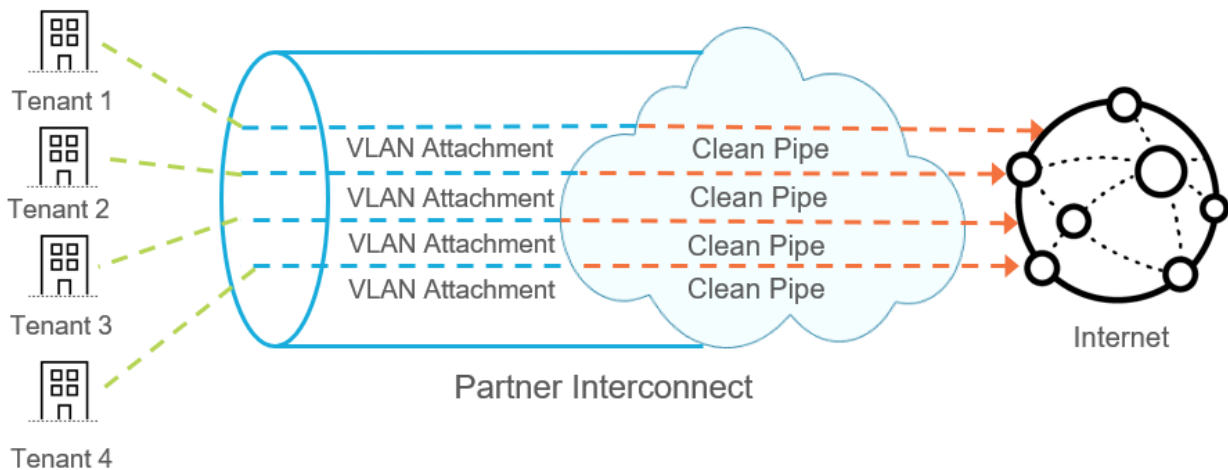
If you have additional security requirements, we recommend [creating multiple tenants in Prisma Access](#) instead of implementing Clean Pipe, which allows you to create and enforce security profiles for separate groups of remote networks and mobile users.

## Clean Pipe Examples

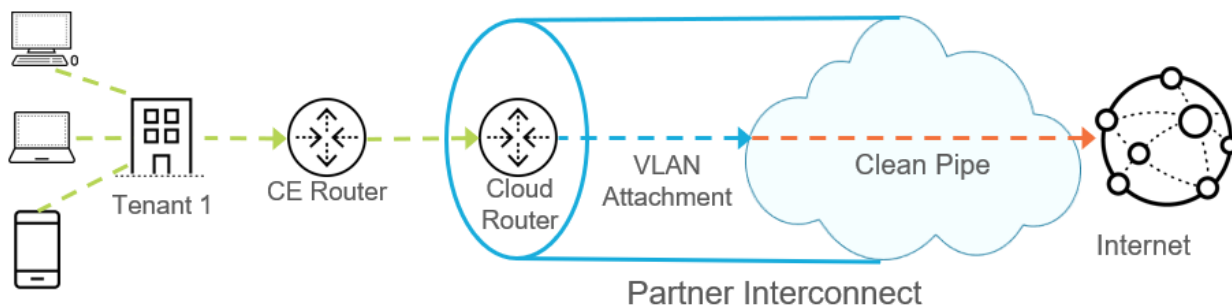
The following figure provides an example of Clean Pipes configured for a single tenant, with multiple Clean Pipes configured for the tenant.

In this example, the service provider manages the internet connectivity for four organizations and wants to protect outbound internet access for them. The service provider creates a Google Cloud Platform (GCP) Partner Interconnect and creates a VLAN attachment for each tenant. The service provider configures Prisma Access for Clean Pipe using Panorama to create security for the VLAN attachment.

This example shows a single Clean Pipe per tenant. You can also create multiple Clean Pipes in a single tenant. Make sure that each Clean Pipe you specify for a tenant uses a different location.



The following figure shows a single Clean Pipe in more detail for a tenant who wants a clean connection to the internet. The Customer Edge (CE) router provides WAN connectivity for the tenant. The CE router connects to a cloud router, and the cloud router provides connectivity for the Partner Interconnect. The service provider creates a VLAN attachment for the tenant, and configures Prisma Access for Clean Pipe in Panorama to provide security for the VLAN attachment, which protects the tenant's internet-based traffic.



## Clean Pipe and Partner Interconnect Requirements

Before you start, be aware of the following Clean Pipe deployment requirements, and be aware of the following differences between Prisma Access for Clean Pipe and other Prisma Access deployments:

- You must have a Prisma Access for Clean Pipe license.
 

The Prisma Access for Clean Pipe license is a separate license from other Prisma Access products. However, the same requirements for purchasing and installing [Panorama and Cortex Data Lake licenses](#) apply to Clean Pipe.
- Prisma Access for Clean Pipe has the following GCP Partner Interconnect requirements:
  - You must be able to create a Partner Interconnect in GCP.
  - You must have the ability to create VLAN attachments in GCP.
  - For Layer 2 (L2) partner interconnects, you must have access to the customer edge (CE) router on the MSSP side and be able to make configuration changes to it.

For more information about GCP configuration, refer to the [GCP documentation](#).

- Be aware of the minimum bandwidth requirements for the Clean Pipe deployment.

The minimum license you can purchase is 1000 Mbps. The minimum bandwidth allocation for each Clean Pipe tenant is 100 Mbps.



---

After you create a tenant, you can create clean pipes in that tenant. Each clean pipe must be a minimum of 100 Mbps. Each Clean Pipe shares the tenant's [access domain](#), [templates](#) and [template stack](#), and [device group](#).

- If configuring multiple Clean Pipes for a single tenant, each Clean Pipe is required to be a unique location. If you want to configure two VLAN attachments for a single Clean Pipe location in an active/backup configuration for intra-zone redundancy, specify the **REDUNDANT** choice when you [add a new Clean Pipe instance](#).
- When creating a connection within a Clean Pipe tenant, match the bandwidth allocation to that of the VLAN attachment. Do not create a VLAN attachment that has a bandwidth that is higher or lower than the connection's bandwidth.
- After you [enable multi-tenancy](#), do not configure your Clean Pipe deployment with any of the other tabs in the Configuration area, with the exception of the **Generate API key** link in the **Service Setup** tab, which lets you generate an API key to [retrieve Clean Pipe IP addresses](#). All configuration is unique to Prisma Access for Clean Pipe and separate from other Prisma Access deployments, such as Prisma Access for Networks or Prisma Access for Users.
- Do not make changes to a Clean Pipe configuration after you commit it. If you change a Clean Pipe after it's been committed, you will receive a commit error when you re-commit it. Instead, delete the existing Clean Pipe and add a new one. Schedule this change during a system downtime window. If you already made changes and have not yet committed, you can revert the changes by editing the Clean Pipe configuration back to their previous values.
- Note that the locations used by Clean Pipe differ from other Prisma Access deployments. Prisma Access for Clean Pipe supports the following locations:
  - 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
- Note the following networking restrictions for Clean Pipe:
  - ICMP is not supported.
  - QoS is supported on ingress (from internet to Clean Pipe direction) only. See [Configure Quality of Service for Clean Pipe](#) for details.
  - User-ID is not supported.
  - Clean Pipe supports session affinity based on source and destination IP addresses and is not configurable.
  - Trust-to-Trust policies are invalid for Clean Pipe, because the traffic is always internet-bound. Only use Trust-to-Untrust policies.

# Configure Prisma Access for Clean Pipe

To set up Prisma Access for Clean Pipe for your tenants, complete the following steps.

- [Enable Multitenancy and Create a Tenant](#)
- [Complete the Clean Pipe Configuration](#)

## Enable Multitenancy and Create a Tenant

To begin the Clean Pipe configuration, you create a [multi-tenant deployment](#) in Panorama and create one or more tenants.

### STEP 1 | Install and activate Prisma Access for Clean Pipe.

Prisma Access for Clean Pipe requires a separate license, and activating it creates Clean Pipe-specific tabs in the Cloud Services plugin. The procedure you use to install Prisma Access for Clean Pipe is the same as the procedure you use to [activate and install a standard Prisma Access license](#), including installing the Cloud Services plugin.

### STEP 2 | [Enable multitenancy](#) if you have not done so already.

1. Select **Panorama > Cloud Services > Configuration**.
2. Select **Enable Multitenancy** (located on the upper right of the page).
3. Click **OK**.

The **Tenants** page displays.

4. In the **Options** area, select **Clean Pipe**.

To configure a tenant for remote networks, mobile users, or both, see [Manage Multiple Tenants in Prisma Access](#).

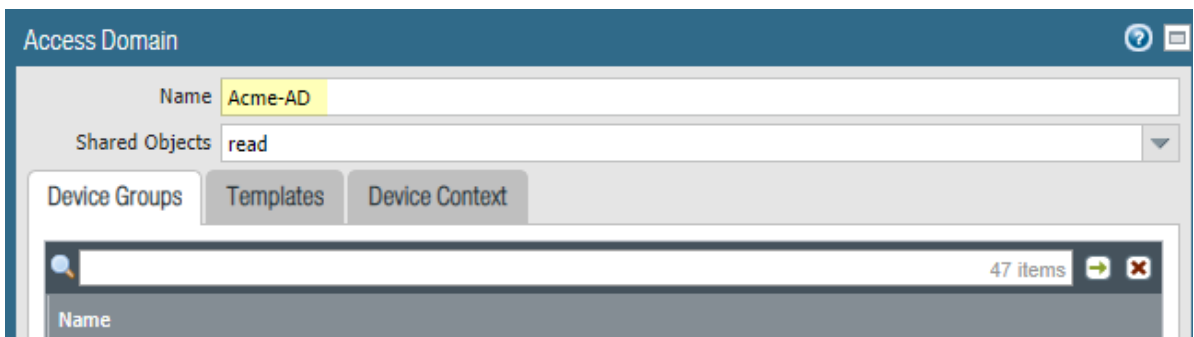
The screenshot shows the 'Tenants' configuration window. At the top, the 'Name' field is set to 'Acme-Clean-Pipe' and the 'Access Domain' is a dropdown menu. Under 'Options', the 'Clean Pipe' radio button is selected. The main area contains three pie charts and three tables. The 'Remote Networks' chart shows 25000 Total Mbps Bandwidth. The 'Mobile Users' chart shows 25000 User Limit. The 'Clean Pipe' chart shows 20000 Total Mbps Bandwidth. Below each chart is a table showing resource allocation for 'This Tenant', 'Unallocated', and 'Total'.

Tenant	Bandwidth (Mbps)	%
This Tenant	[200 - 24667]	--%
Unallocated	24667	99%
Total	25000	100%

Tenant	Users	%
This Tenant	[200 - 24667]	--%
Unallocated	24667	99%
Total	25000	100%

Tenant	Bandwidth (Mbps)	%
This Tenant	[100 - 16500]	--%
Unallocated	16500	83%
Total	20000	100%

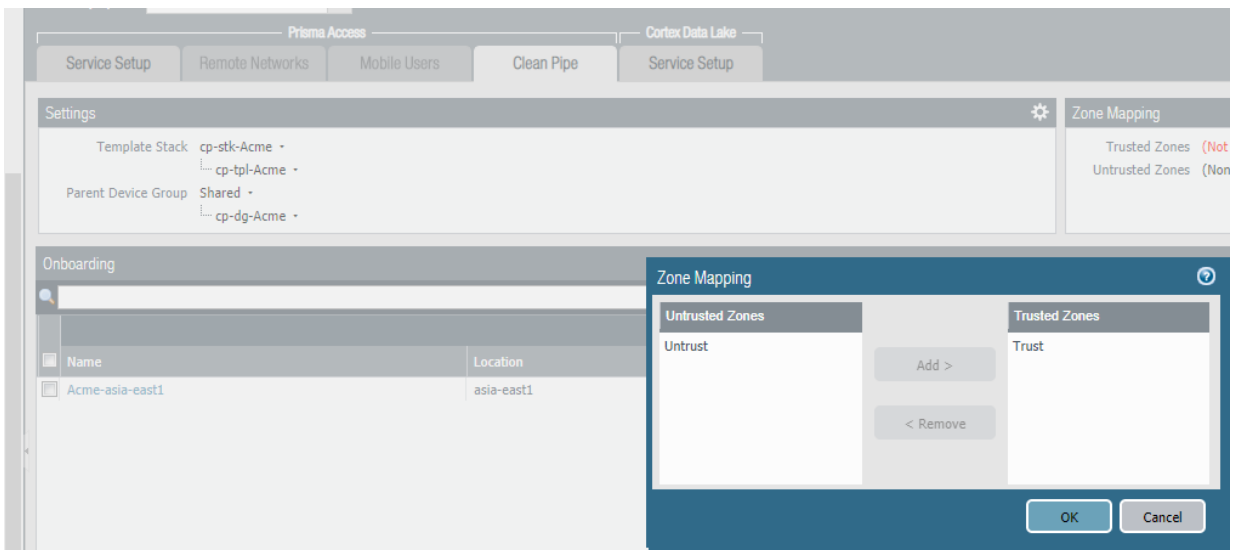
5. Enter a **Name** for the first tenant.
6. Create and configure a new **Access Domain** for the first tenant and click **OK**.



7. In the **Clean Pipe** area, enter a **Bandwidth (Mbps)** for **This Tenant**.  
Enter a minimum of 100 Mbps for each tenant you create.
8. Click **OK**.

**STEP 3 |** Create zones for the tenant and map those zones for the tenant.

1. Select **Network > Zones**.  
Make sure that selected the Clean Pipe **Template** for the tenant you created (**cp-tpl-tenant**).
2. Create zones for the tenant (for example, **Trust** and **Untrust**).
3. Select **Panorama > Cloud Services > Configuration** and select the **Tenant** from the drop-down list.
4. Select the **Clean Pipe** tab.
5. Click the gear icon next to **Zone Mapping** to edit the settings.
6. **Add** and **Remove** the zones you created to [map them to trusted and untrusted zones](#).



**STEP 4 |** Onboard a new Clean Pipe.


1. Select **Panorama > Cloud Services > Configuration > Clean Pipe**.
2. **Add** a new Clean Pipe instance for the tenant, entering the following information:
  - **Name**—Specify a name for the clean pipe.
  - **Bandwidth**—Select the Bandwidth to allocate for the clean pipe.

You can onboard Clean Pipe instances in increments of 100 Mbps, 200 Mbps, 300 Mbps, 400 Mbps, 500 Mbps, 1000 Mbps, 2000 Mbps, 5000 Mbps, and 10000 Mbps. The amount of bandwidth you specify must be within the licensed bandwidth allocation, and it must match the bandwidth of the VLAN attachment you create in the Partner Interconnect.

- **Edge Availability Domain**—Select the availability domain you want for the clean pipe. You can choose **1**, **2**, **ANY**, or **REDUNDANT**.
  - Specify **ANY** for a non-redundant Clean Pipe deployment.
 

Make sure that your cloud provider supports this choice; you must also select **ANY** on the cloud provider side of the partner interconnect. If that choice is not available for your cloud provider, make another choice.
  - To specify two VLAN attachments in the same location in an active/backup configuration in the same location, select **REDUNDANT**.

Prisma Access creates two pairing keys for a **REDUNDANT** configuration (one for each availability zone), and appends the clean pipe name with `zone1` for the first availability zone and `zone2` for the second availability zone. For example, if you specify a **Name** of **San Francisco**, Prisma Access creates two zones named **San Francisco-zone1** and **San Francisco-zone2**.

 *Be sure that you configure the first availability zone (zone1) as the primary zone on your CPE.*

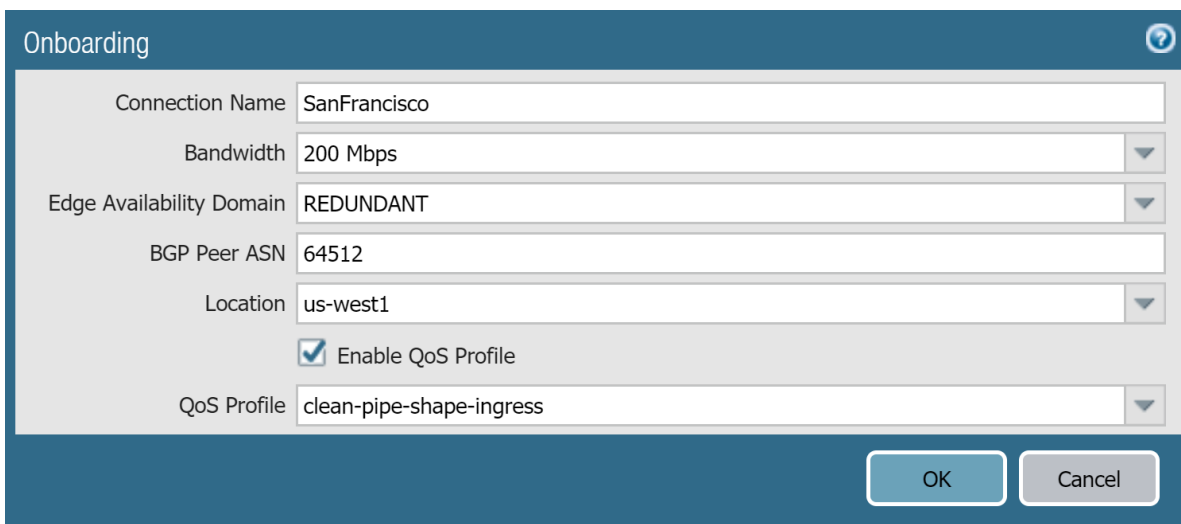
You can also build a pair of clean pipes for a single tenant redundancy in different locations; to do so, specify **1** for the first clean pipe in one location and **2** for the second clean pipe in a different location.

- **BGP Peer ASN**—Enter the BGP Autonomous System Number (ASN).
 

You can specify either a private or public BGP ASN.

Make a note of this value; you configure it on the customer edge (CE) router when you [complete the Clean Pipe configuration](#).
- **Location**—Select the [location](#).
 

We recommend that you use the same location that you use when you [create the VLAN attachment for the partner interconnect](#).
- To enable QoS, select **QoS**, then select the [QoS Profile](#) to use with the clean pipe. Clean Pipe QoS shapes on ingress.



The screenshot shows the 'Onboarding' configuration window for a Clean Pipe. The fields are as follows:

Connection Name	SanFrancisco
Bandwidth	200 Mbps
Edge Availability Domain	REDUNDANT
BGP Peer ASN	64512
Location	us-west1
Enable QoS Profile	<input checked="" type="checkbox"/>
QoS Profile	clean-pipe-shape-ingress

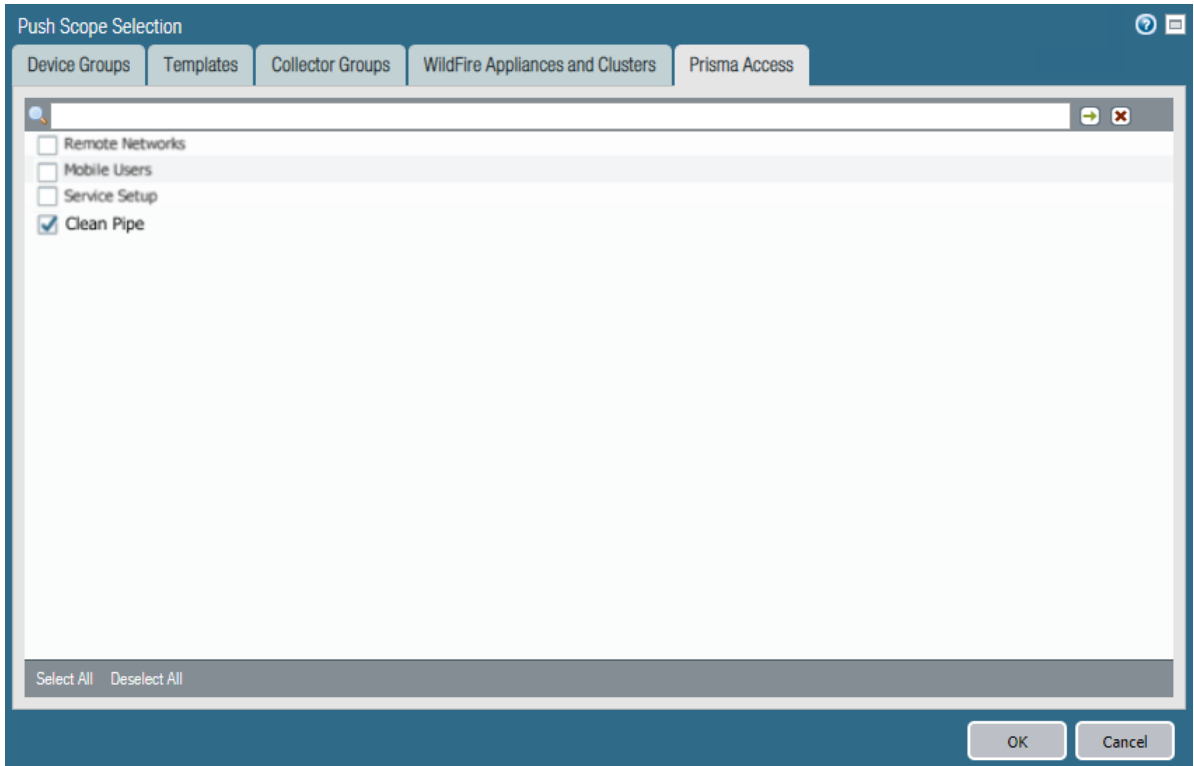
Buttons: OK, Cancel

**STEP 5 |** Add more Clean Pipe instances as required by repeating Step 4.

Be sure that each additional Clean Pipe uses a different location.

**STEP 6 |** Commit and push your changes to make them active in Prisma Access.

1. Select **Commit > Commit and Push** and **Edit Selections** in the Push Scope.
2. Select **Prisma Access**, then select **Clean Pipe**.



3. Click **OK** to save your changes to the Push Scope.
4. **Commit** and **Push** your changes.

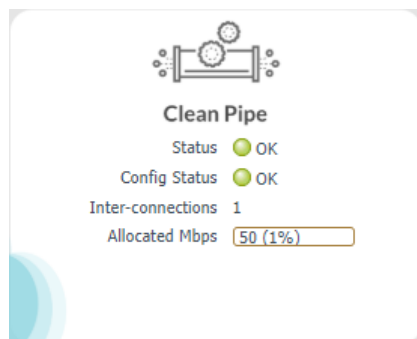
**STEP 7 |** Check that your Clean Pipe has been provisioned.

1. Select **Panorama > Cloud Services > Status**.
2. Select the **Tenant** from the drop-down list at the top of the page.
3. Click **Status**.

The Clean Pipe status displays.

4. Hover over the Clean Pipe **Config Status** and wait until the status changes from **Provisioning in Progress** to **Provisioned**.

This provisioning can take up to 30 minutes.



**STEP 8 |** Click the **Network Details** tab, click the **Clean Pipe** radio button, and make a note of the **Pairing Key**.

The **MSSP CE** and **Cloud Router IP** fields are blank when you start to configure the Clean Pipe. These fields populate after you create the VLAN Attachment when you [complete the Clean Pipe configuration](#).

If you specified a **REDUNDANT** connection, Prisma Access creates two pairing keys, one for each availability zone, and appends the clean pipe name with **zone1** for the first availability zone and **zone2** for the second availability zone. The following screenshot shows the **SanFrancisco** clean pipe with a redundant configuration; Prisma Access has created two pairing keys, one for **SanFrancisco-zone1** and one for **SanFrancisco-zone2**.



*Be sure that you configure the first availability zone (zone1) as the primary zone on your CPE.*

Name	Pairing Key	MSSP CE	Cloud Router IP	MSSP BGP ASN	Cloud Router BGP ASN	Med Val	Zone
LosAngeles		None	None	65100	16550	100	1
SanDiego		None	None	65100	16550	100	1
SanFrancisco-zone1		None	None	65100	16550	100	1
SanFrancisco-zone2		None	None	65100	16550	200	2

**STEP 9 |** Complete the Clean Pipe configuration.

## Complete the Clean Pipe Configuration

To complete configuration of Prisma Access for Clean Pipe, you perform configuration in the Partner Interconnect and in Panorama.



*Make sure that you can access and configure the CE and cloud routers on the Partner Interconnect (non-Prisma access) side of the Partner Interconnect.*

**STEP 1 |** In the Partner Interconnect side of the configuration, create a VLAN attachment, using the **Pairing Key** that you retrieved from Panorama.

For more information about creating VLAN attachments with Partner Interconnects and configuring customer edge (CE) routers to communicate with cloud routers, refer to the Google Cloud documentation at <https://cloud.google.com/interconnect/docs/>

Make sure that the location and bandwidth you select matches the **Location** you specified in Panorama. The service provider you use for the Partner Interconnect uses the pairing key, along with your requested connection location and capacity, to complete the configuration of your VLAN attachment.

**STEP 2 |** After the connection comes up, return to Panorama, select **Panorama > Cloud Services > Status > Network Details > Clean Pipe** and make a note of the **MSSP CE** and **Cloud Router IP** addresses.

These values populate after you enter the **Pairing Key** on the other side of the VLAN attachment.

Name	Pairing Key	MSSP CE	Cloud Router IP
test2		/29	/29

**STEP 3 |** Log in to the CE router and perform the following configuration.

1. Enter the **MSSP CE** address as the local IP address.

2. Enter the **Cloud Router IP** address as the peer IP address.
3. Enter a BGP ASN that matches the **BGP Peer ASN** you entered when you configured the Clean Pipe in Panorama.

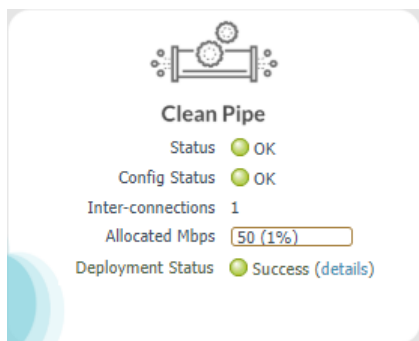
Make sure that you enter these values correctly; you cannot change them.

#### STEP 4 | Check the Clean Pipe status.

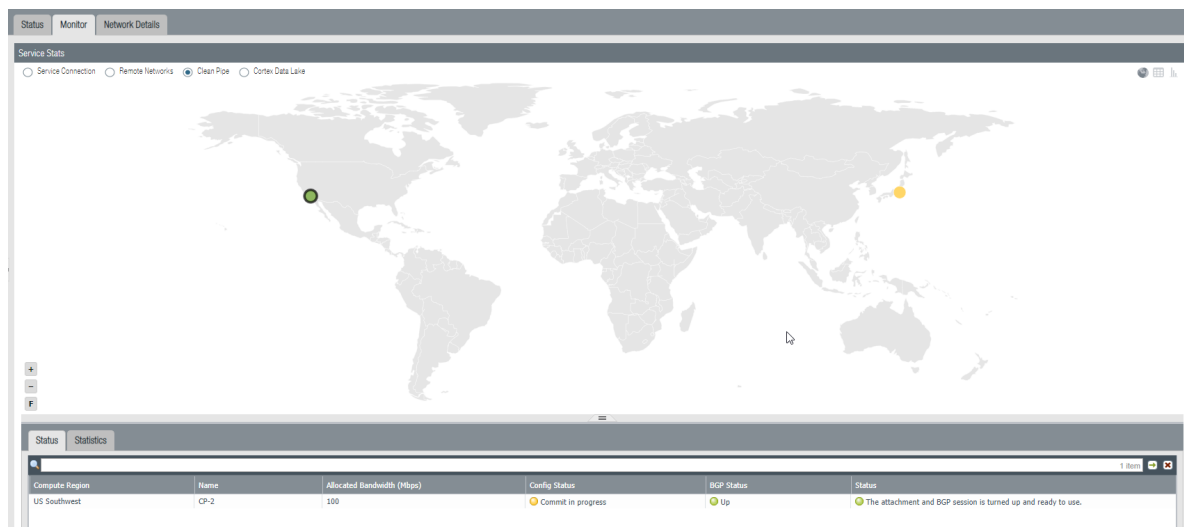
1. In Panorama, select **Panorama > Cloud Services > Status**, select the **Tenant** from the drop-down, and check the Clean Pipe's **Status**.

See the [list of Prisma Access locations](#) for acceptable values.

The **Deployment Status** area allows you to view the progress of onboarding and deployment jobs before they complete, as well as see more information about the status of completed jobs. See [Deployment Progress and Status](#) for details.



2. Select **Panorama > Cloud Services > Status > Clean Pipe**, and click the **Monitor** tab to see a map with the status of the deployed Clean Pipes.



Click the tabs below the map to see additional statistics for the Clean Pipes.

#### Status tab:

- **Compute Region**—The compute region where your cloud service infrastructure is deployed for the clean pipe instance.
- **Name**—The name of the clean pipe instance.
- **Allocated Bandwidth (Mbps)**—The amount of bandwidth you allocated for the clean pipe instance.
- **Config Status**—The status of your last configuration push to the service. If you have made a change locally, and not yet pushed the configuration to the cloud, the status shows **Out of sync**.

---

Hover over the status indicator for more detailed information. After committing and pushing the configuration to Prisma Access, the Config Status changes to **In sync**.

- **BGP Status**—Displays information about the BGP state between the firewall or router at the clean pipe instance and Prisma Access. Although you might temporarily see the status pass through the various BGP states (**idle**, **active**, **open send**, **open pend**, **open confirm**, most commonly, the BGP status shows:

- **Connect**—The router at the clean pipe instance is trying to establish the BGP peer relationship with the cloud firewall.
- **Established**—The BGP peer relationship has been established.

This field will also show if the BGP connection is in an error state:

- **Warning**—There has not been a BGP status update in more than eight minutes. This may indicate an outage on the firewall.
- **Error**—The BGP status is unknown.
- **Status**—The operational status of the connection between Prisma Access and the clean pipe instance.

#### Statistics tab:

- **Region**—The region where your cloud service infrastructure is deployed for the clean pipe instance.
- **Name**—The name of the clean pipe instance.
- **Allocated Bandwidth (Mbps)**—The amount of bandwidth you allocated for the remote network location.
- **QoS**— Select **QoS** to display a page that contains graphical QoS statistics.
- **Avg Egress Bandwidth 5 Min (Mbps)**—The average amount of clean pipe egress bandwidth averaged over 5 minutes.
- **Avg Egress Bandwidth 60 Min (Mbps)**—The average amount of clean pipe egress bandwidth averaged over 60 minutes.
- **Avg Ingress Bandwidth 5 Min (Mbps)**—The average amount of clean pipe ingress bandwidth averaged over 5 minutes.
- **Avg Ingress Bandwidth 60 Min (Mbps)**—The average amount of clean pipe ingress bandwidth averaged over 60 minutes.
- **Egress Peak Bandwidth 1 Hour (Mbps)**—The amount of peak egress bandwidth for the clean pipe instance for the last 1 hour.
- **Egress Peak Bandwidth 24 Hour (Mbps)**—The amount of peak egress bandwidth for the clean pipe instance for the last 24 hours.
- **Egress Peak Bandwidth 7 Days (Mbps)**—The amount of peak egress bandwidth for the clean pipe instance for the last 7 days.
- **Egress Peak Bandwidth 30 Days (Mbps)**—The amount of peak egress bandwidth for the clean pipe instance for the last 30 days.
- **Ingress Peak Bandwidth 1 Hour (Mbps)**—The amount of peak ingress bandwidth for the clean pipe instance for the last 1 hour.
- **Ingress Peak Bandwidth 24 Hour (Mbps)**—The amount of peak ingress bandwidth for the clean pipe instance for the last 24 hours.
- **Ingress Peak Bandwidth 7 Days (Mbps)**—The amount of peak ingress bandwidth for the clean pipe instance for the last 7 days.
- **Ingress Peak Bandwidth 30 Days (Mbps)**—The amount of peak ingress bandwidth for the clean pipe instance for the last 30 days.



# Cloud Management Logs and Reports

Monitor and get visibility in to your Prisma Access environment with logs and reports:

- > Logs

Your logs are automatically-generated and provide an audit trail for system, configuration, and network events. Network logs record all events where Prisma Access acts on your network traffic. For example, entries are recorded when Prisma Access blocks traffic based on a security rule, grants access to a user based on an authentication rule, or shapes traffic based on a QoS rule.

- > Reports

Reports identify key findings that you can use to inform your policy updates and close enterprise security and user productivity gaps. Three reports are currently available: an app report, a Prisma Access usage report, and a user activity report. You can download reports, share them within your organization, and schedule reports to receive regular updates.



---

# Logs

To see your Prisma Access logs, log in to Prisma Access Cloud Management and select **Logs** on the left side navigation pane. Regardless of the management interface you're using for Prisma Access—Panorama or cloud management—you can view your logs in Prisma Access Cloud Management.

A log is an automatically generated, time-stamped file that provides an audit trail for system events or network traffic events that Prisma Access monitors. Log entries contain artifacts, which are properties, activities, or behaviors associated with the logged event, such as the application type or the IP address of an attacker. Each log type records information for a separate event type. For example, Prisma Access may generate a Threat log to record traffic that matches a spyware, vulnerability, or virus signature.

Prisma Access Cloud Management provides Network logs (Traffic, Threat, URL, File, HIP Match) and Common logs (System and Configuration).

You can view details for each log entry, and for threat logs, you can review threat details and see if there are any threat overrides in place.

**STEP 1 | Go to **Logs**.**

**STEP 2 | Select the type of log you want to view.**

Prisma Access supports Network logs (Traffic, Threat, URL, File, HIP Match) and Common logs (System and Configuration).

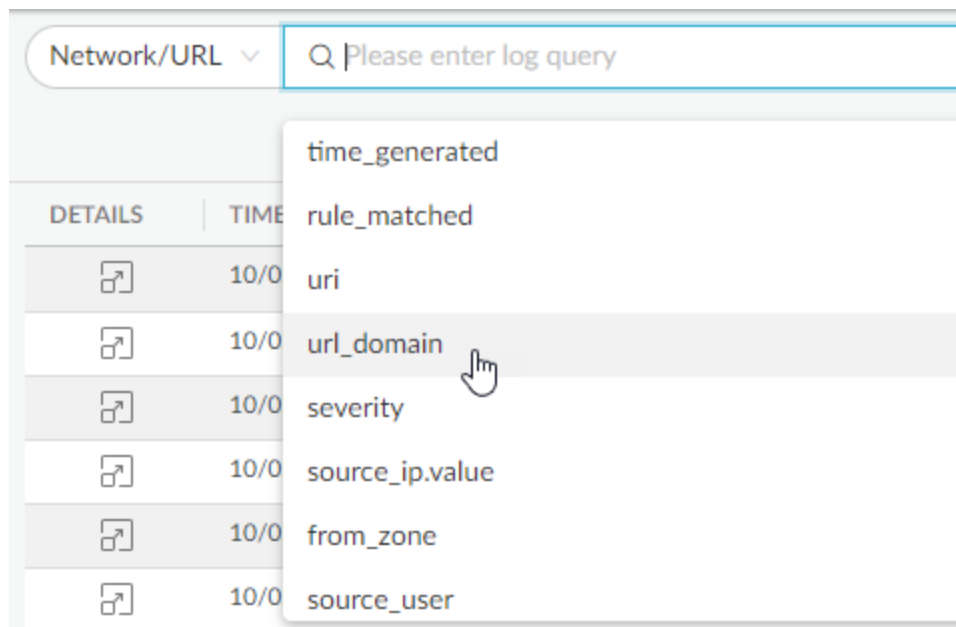
**STEP 3 | Filter for logs.**

- Start by selecting a time range for which you want to view logs. This starts off your log query.

DETAILS	TIME GENERATED ↓	RULE	URL	URL DOMAIN	SEV
	10/02/2019 02:05:19 PM	allow-general-web-browsing	cdn.content.prod.cms.msn.com/singletile/summary/alias/experiencebyname/today?market=en-US&source=appxmanifest&tenant=amp&vertical=news	cdn.content.prod.cms.msn.com	Inf
	10/02/2019 01:37:58 PM	allow-general-web-browsing	cdn.content.prod.cms.msn.com/singletile/summary/alias/experiencebyname/today?market=en-US&source=appxmanifest&tenant=amp&vertical=news	cdn.content.prod.cms.msn.com	Inf
	10/02/2019 01:05:18 PM	allow-general-web-browsing	cdn.content.prod.cms.msn.com/singletile/summary/alias/experiencebyname/today?market=en-US&source=appxmanifest&tenant=amp&vertical=news	cdn.content.prod.cms.msn.com	Inf
	10/02/2019 12:43:19 PM	allow-general-web-browsing	cdn.content.prod.cms.msn.com/singletile/summary/alias/experiencebyname/today?market=en-US&source=appxmanifest&tenant=amp&vertical=news	cdn.content.prod.cms.msn.com	Inf
	10/02/2019 12:08:24 PM	allow-general-web-browsing	cdn.content.prod.cms.msn.com/singletile/summary/alias/experiencebyname/today?market=en-US&source=appxmanifest&tenant=amp&vertical=news	cdn.content.prod.cms.msn.com	Inf
	10/02/2019 11:35:51 AM	allow-general-web-browsing	cdn.content.prod.cms.msn.com/singletile/summary/alias/experiencebyname/today?market=en-US&source=appxmanifest&tenant=amp&vertical=news	cdn.content.prod.cms.msn.com	Inf
	10/02/2019 11:28:24 AM	allow-general-web-browsing	client.wns.windows.com/	client.wns.windows.com	Inf
	10/02/2019 11:27:22 AM	allow-general-web-browsing	client.wns.windows.com/	client.wns.windows.com	Inf
	10/02/2019 11:26:32 AM	allow-general-web-browsing	www.msftconnecttest.com/connecttest.txt	www.msftconnecttest.com	Inf
	10/02/2019 11:26:20 AM	allow-general-web-browsing	www.msftconnecttest.com/connecttest.txt	www.msftconnecttest.com	Inf
	10/01/2019 08:13:51 PM	allow-general-web-browsing	www.msftconnecttest.com/connecttest.txt	www.msftconnecttest.com	Inf
	10/01/2019 08:07:27 PM	allow-general-web-browsing	cdn.content.prod.cms.msn.com/singletile/summary/alias/experiencebyname/today?market=en-US&source=appxmanifest&tenant=amp&vertical=news	cdn.content.prod.cms.msn.com	Inf
	10/01/2019 07:39:55 PM	allow-general-web-browsing	cdn.content.prod.cms.msn.com/singletile/summary/alias/experiencebyname/today?market=en-US&source=appxmanifest&tenant=amp&vertical=news	cdn.content.prod.cms.msn.com	Inf
	10/01/2019 07:24:50 PM	allow-general-web-browsing	www.msftconnecttest.com/connecttest.txt	www.msftconnecttest.com	Inf
	10/01/2019 07:09:11 PM	allow-general-web-browsing	cdn.content.prod.cms.msn.com/singletile/summary/alias/experiencebyname/today?market=en-US&source=appxmanifest&tenant=amp&vertical=news	cdn.content.prod.cms.msn.com	Inf
	10/01/2019 06:48:08 PM	allow-general-web-browsing	www.msftconnecttest.com/connecttest.txt	www.msftconnecttest.com	Inf
	10/01/2019 06:36:09 PM	allow-general-web-browsing	cdn.content.prod.cms.msn.com/singletile/summary/alias/experiencebyname/today?market=en-US&source=appxmanifest&tenant=amp&vertical=news	cdn.content.prod.cms.msn.com	Inf
	10/01/2019 06:05:19 PM	allow-general-web-browsing	cdn.content.prod.cms.msn.com/singletile/summary/alias/experiencebyname/today?market=en-US&source=appxmanifest&tenant=amp&vertical=news	cdn.content.prod.cms.msn.com	Inf
	10/01/2019 05:49:27 PM	allow-general-web-browsing	www.msftconnecttest.com/connecttest.txt	www.msftconnecttest.com	Inf
	10/01/2019 05:39:16 PM	allow-general-web-browsing	cdn.content.prod.cms.msn.com/singletile/summary/alias/experiencebyname/today?market=en-US&source=appxmanifest&tenant=amp&vertical=news	cdn.content.prod.cms.msn.com	Inf
	10/01/2019 12:32:08 PM	new-internet-log-frowarding	client.wns.windows.com/	client.wns.windows.com	Inf
	10/01/2019 12:32:08 PM	new-internet-log-frowarding	client.wns.windows.com/	client.wns.windows.com	Inf
	10/01/2019 12:31:09 PM	new-internet-log-frowarding	www.msftconnecttest.com/connecttest.txt	www.msftconnecttest.com	Inf



- Provide a query string to narrow down the list of logs.

If you do not provide a query string, Explore will retrieve every log record of the type you specify that was created during the time range that you provide – up to 65,536 records.




- Click into an individual cell to add the field and value to the query.

Network/URL severity = 'Informational'

DETAILS	TIME GENERATED ↓	RULE	SEVERITY
	10/02/2019 02:05:19 PM	allow-general-web-browsing	Informational
	10/02/2019 01:37:58 PM	allow-general-web-browsing	Informational

**STEP 4 |** View log entry details.

Click the details  icon to learn more about a log entry.

Log Details ×

GENERAL	SOURCE	DESTINATION
TIME GENERATED: 10/02/2019 02:38:41 PM	SOURCE PORT: [REDACTED]	DESTINATION PORT: 80
SUB TYPE: end	FROM ZONE: trust	TO ZONE: untrust
APPLICATION: web-browsing	INBOUND INTERFACE: tunnel	OUTBOUND INTERFACE: ethernet
ACTION: allow	INBOUND INTERFACE DETAILS UNIT: 1	OUTBOUND INTERFACE DETAILS UNIT: 0
RULE: allow-general-web-browsing	INBOUND INTERFACE DETAILS SLOT: 0	OUTBOUND INTERFACE DETAILS SLOT: 1
SESSION END REASON: tcp-rst-from-client	INBOUND INTERFACE DETAILS PORT: 0	OUTBOUND INTERFACE DETAILS PORT: 1
SESSION ID: 10163	NAT SOURCE PORT: [REDACTED]	NAT DESTINATION PORT: 80
DEVICE SN: [REDACTED]	NAT SOURCE VALUE: [REDACTED]	NAT DEST VALUE: [REDACTED]
DEVICE NAME: GP cloud service	SOURCE UUID: [REDACTED]	DESTINATION UUID: [REDACTED]
PROTOCOL: tcp	SOURCE LOCATION: [REDACTED]	DESTINATION LOCATION: GB
APPLICATION CONTAINER: [REDACTED]	SOURCE USER: [REDACTED]	DESTINATION USER: [REDACTED]
ACTION SOURCE: from-policy	SOURCE ADDRESS: [REDACTED]	DESTINATION ADDRESS: [REDACTED]
IS SAAS APPLICATION: false		
SOURCE USER DOMAIN: gmail		
SOURCE USER NAME: [REDACTED]		
SOURCE USER UUID: [REDACTED]		
DESTINATION USER DOMAIN: [REDACTED]		
DESTINATION USER NAME: [REDACTED]		
DESTINATION USER UUID: [REDACTED]		
VENDOR NAME: Palo Alto Networks		
LOG SOURCE: firewall		
	DETAILS	FLAGS
	BYTES: 6508	NON STANDARD DESTINATION PORT: 0
	REPEAT COUNT: 1	IS DECRYPT MIRROR: false
	BYTES RECEIVED: 6146	IS SYSTEM RETURN: false
	BYTES SENT: 362	IS CONTAINER: false
	CHUNKS TOTAL: 0	IS SERVER TO CLIENT: false
	CHUNKS RECEIVED: 0	IS CLIENT TO SERVER: false
	CHUNKS SENT: 0	

**STEP 5 |** Review threat details and overrides.

See threat details and also check if there are any overrides configured for a threat. A threat override is where you're using a different action to enforce a threat than the default action.

Time Generated ↓	Severity	Subtype	Threat Name Firewall	Threat ID	Threat Category
01/28/2021 08:04:29 PM PST	Medium	spyware	Microsoft Windows MSCOMCTL OCX RCE Stack Buffer Overflow Vulnerability	34766	overflow
01/28/2021 08:04:23 PM PST	Informational	spyware	Drupal Core API SQL Injection Vulnerability	36972	sql-injection
01/28/2021 08:04:22 PM PST	Critical	spyware	29659	29659	unknown
01/28/2021 08:04:22 PM PST	Informational	spyware	28718	28718	unknown
01/28/2021 08:04:20 PM PST	High	spyware	30551	30551	unknown
01/28/2021 08:04:19 PM PST	Informational	spyware	Rat.Gen Command and Control Traffic		code-execution
01/28/2021 08:04:19 PM PST	Informational	spyware			spyware
01/28/2021 08:04:15 PM PST	Critical	spyware			unknown
01/28/2021 08:04:15 PM PST	Critical	spyware			unknown
01/28/2021 08:04:15 PM PST	Critical	spyware	13846	13846	unknown
01/28/2021 08:04:13 PM PST	Critical	spyware	Microsoft Host Integration Server Access of Unallocated Memory Denial of Service Vulnerability	34477	dos
01/28/2021 08:04:12 PM PST	High	spyware	Generic Exploit Host Webpage	37444	exploit-kit

**Override Details**

Name VantomRat.Gen Command and Control Traffic  
ID 18014 - [View in Threat Vault](#)  
Type Spyware  
Description Vantom is a free RAT with multiple features, including password recovery, keylogger, file manager...etc  
Severity **CRITICAL**  
CVE -  
Bugtraq ID -  
Vendor Reference ID -  
Reference <https://www.rekings.com/vantom-rat/>

Location \*  
Prisma Access

**Overrides (Exceptions) (2)** Disassociate Add to Other Profiles

<input type="checkbox"/>	Applied to Profiles	Location	Applied to IP Address...	Action	Packet Capture	Notes
<input type="checkbox"/>	<a href="#">prof_aml_342</a>	Mobile Users Container	none	default	disable	
<input type="checkbox"/>	<a href="#">prof_aml_344</a>	Prisma Access	none	default	disable	

---

# Reports

Keep a pulse on your network with Prisma Access reports. Reports identify key findings that you can use to inform your policy updates and close enterprise security and user productivity gaps.

To locate **Reports**, log in to Prisma Access Cloud Management and find it listed on the left-side navigation pane. Prisma Access Cloud Management reports are available to all Prisma Access users, regardless of the management interface you're using (Panorama or cloud management). The Reports homepage shows you all the reports that are available to you. Open an individual report to:

- Explore the report dashboard
- Download or share a PDF version of the report
- Schedule the report to be regularly delivered to your email inbox, or to other people within your organization

We recommend setting up [Directory Sync](#) to get the most out of reports. Directory Sync gives Prisma Access read-only access to your Active Directory information. Directory Sync is required for the User Activity Report (so you can specify the user for whom you want to generate the report) and also enables you to easily share reports with other members of your organization.

---

your policies, and focus your efforts on maintaining network security so that your users are safe and productive.

# Prisma Access: Reports

Key insights into your Prisma Access environment.  
within your organization, and schedule regular updates.

## Available Reports

There are three reports available: an **App Report**, a **Usage Report**, and a **User Activity Report**.



## App Report

Know the security challenges associated with the applications traversing your network. Key findings here can help you to refine your security policy to control unsanctioned and risk applications.

The **sanctioned apps** you see in this report are apps with the sanctioned tag; go to **Objects > Applications** to see your sanctioned apps or to tag apps as sanctioned.

App report data includes:

- An overview of the applications on your network, including risk, sanction status, bandwidth consumed, and the top users of these applications.
- Most used application types
- Applications with the most data transfer
- The top application types on your network
- The most heavily used applications on your network
- The users with the most applications
- The users with the most data transfer



*If an app is a container app, then the displayed statistics are a roll-up of all the applications in the container. For example, gmail is a container app (there is no app-id for gmail). It groups applications such as gmail-posting, gmail-downloading, gmail-uploading, and so forth. The risk score set for this container app is the highest risk score found for the contained applications. All other metrics are calculated by summing the values found for the contained applications.*

### App Report

Know the security challenges associated with the applications traversing your network. Key findings here help you to refine security rules for unsanctioned and risky applications.

Time Range: Past 30 days

---

#### Application Risks

Your users can directly access many applications without having to go through your network. So, it's important to have a view into the applications they're using and the risks they pose.

Applications by Risk Category

- 70 Apps
- 8 Apps
- 12 Apps
- 18 Apps
- 26 Apps

Unsanctioned Apps

SaaS: 170 | Non-SaaS: 162

Sanctioned Apps

SaaS: 170 | Non-SaaS: 162

[Manage Sanctioned Apps >](#)

---

#### Usage Risks

By Data Transfer

99% of your data is flowing through unsanctioned applications.

Unsanctioned: 2.2 TB | Sanctioned: 94.4 MB

By Users

53% of your users are using unsanctioned applications.

Unsanctioned: 48 Users | Sanctioned: 42 Users

[Manage Sanctioned Apps >](#)

---

#### Top Application Types - Most Data Transfer

Applications in these 10 subcategories transferred the most data in and out of your network.

Application Type	Unsanctioned	Sanctioned	Data Transfer	No. of applications used
file-sharing	257.69 GB	257.69 GB	8.52 MB	
general-business	257.19 GB	257.19 GB	15.46 MB	
management	225.48 GB	225.47 GB	8.97 MB	
instant-messaging	194.41 GB	194.4 GB	5.03 MB	
remote-access	161.84 GB	161.83 GB	7.05 MB	
photo-video	128.98 GB	128.97 GB	2.71 MB	
infrastructure	128.38 GB	128.37 GB	2.65 MB	
audio-streaming	97.7 GB	97.69 GB	7.3 MB	
voip-video	96.67 GB	96.66 GB	8.53 MB	
internet-conferencing	96.14 GB	96.13 GB	3.91 MB	

[Manage Sanctioned Apps >](#)

---

#### Top Application Subcategories

File-Sharing | General-Business | Management | Instant-Messaging | Remote-Access | Photo-Video | Infrastructure

##### 1. file-sharing

#	Application Name	Risk	SaaS	Status	Users	Files	Data Transfer
1	imesh	2	Yes	0	43	2,838	33 GB
2	aerofs	2	Yes	0	43	2,953	32 GB
3	gridftp	2	Yes	0	43	2,888	32 GB
4	instant-l-file-transfer	2	Yes	0	43	3,245	32 GB
5	kazza	2	Yes	0	43	3,147	32 GB
6	100ba0	2	Yes	0	43	2,739	32 GB
7	filegor1	2	Yes	0	43	2,727	32 GB
8	fileserve	2	Yes	0	43	3,202	32 GB
9	aerofs	2	Yes	0	34	0	3 MB
10	100ba0	2	Yes	0	31	0	1 MB

[Manage Sanctioned Apps >](#)

---

#### Top Applications - Most Data Transfer

Rhapsody | Draupnir | Chrome-Remote-Desktop | Ms-Groove | Acronis-Snapdeploy | IMesh | Rabbitmq

##### 3. chrome-remote-desktop

Unsanctioned, Non-SaaS  
Chrome Remote Desktop BETA is the first installation on a capability allowing users to remotely access any...

App Details: Subcategory: remote-access, Poor terms of service: No, Certifications: None

WildFire Stats: Submissions: 32,638, Benign: 4,206, Malicious: 3,918

Data Transfer: 44 Total Users | 32.9 GB Total Data, 16.4 GB Download, 16.4 GB Upload

Risk: 3

Top 10 Users By Data Transferred

User	Total Bytes
mohit@imie.com	4.2 GB
paloaltonetwork@pmohan	4.1 GB
paloaltonetwork@luptage	4.1 GB
paloaltonetwork@krithal	4.1 GB
paloaltonetwork@sgutti	4 GB
paloaltonetwork@kkundu	3.9 GB
paloaltonetwork@jhpwal	3.8 GB
mohit@imie.com	3.8 GB
66.115.126.4	42.1 MB
192.168.90.128	31.6 MB

Top 10 File Types By Bytes

File Type	Bytes
27519	27519
Cisco Adaptive Security Appliance WebV...	32784
20853	20853
HP LeftHand Virtual SAN Appliance Hydr...	11664
CIBC Phishing Site Detection	24483
FreeADJUS data2020_vimax Mesop Buffe...	15074
Phishing Site Detection	37755
34351	34351
22175	22175

---

#### Top 10 Threats

#	Threat Name	Threat ID	Threat Count
1	29542	29542	1
2	10085	10085	1
3	Adobe Reader Memory Corruption Vulnerability	32784	1
4	22809	22809	1
5	11664	11664	1
6	24483	24483	1
7	15074	15074	1
8	Microsoft Internet Explorer Memory Disclosure Vulnerability	37755	1
9	Novell eDirectory Unchecked Length Denial of Service Vulnerability	34351	1
10	22175	22175	1

[Manage Sanctioned Apps >](#)

---

#### Users Sharing the Most Data

These users are transferring the most data in and out of your network.

User	Unsanctioned	Sanctioned	Data Transfer	No. of applications used
paloaltonetwork@krithal	279.69 GB	279.69 GB	6.65 MB	
paloaltonetwork@pmohan	279.09 GB	279.08 GB	14.12 MB	
paloaltonetwork@sgutti	278.92 GB	278.91 GB	11.4 MB	
paloaltonetwork@kkundu	278.6 GB	278.59 GB	9.74 MB	

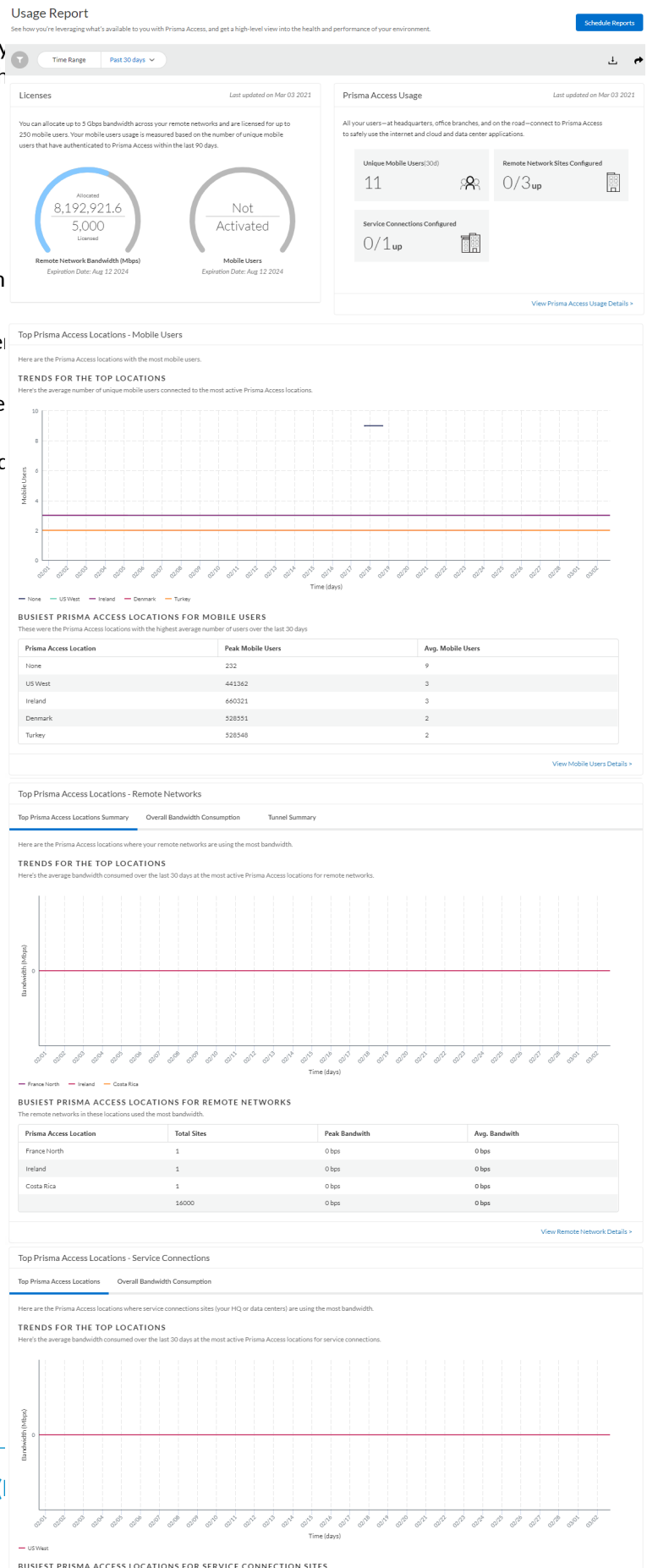
PRISMA ACCESS ADMINISTRATOR'S GUIDE (PANOR)

## Usage Report

See how you're leveraging what's available to you with your Prisma Access license, and get a high level view into the health and performance of your environment.

Usage report data includes:

- An overview of your Prisma Access usage –your licenses, Prisma Access locations, and mobile user capacity and/or bandwidth utilization.
- Top Prisma Access locations for mobile user and remote networks
- Overall bandwidth consumption for remote network and service connection sites, and the highest-consuming remote network and service connection sites
- Tunnel disconnection trends, including the most impacted tunnels



## User Activity Report

Get visibility into an individual users' browsing patterns: their most frequently visited sites, the sites with which they're transferring data, and attempts to access high-risk sites.

The data here is based on what's reported in your URL Filtering logs. This report also depends on Directory Sync—Directory Sync gives Prisma Access read-only access to your Active Directory information, so you can filter this report based on user. If you haven't yet set up Directory Sync [here's how](#).

### User Activity Report

Get visibility into an individual users' browsing patterns: their most frequently visited sites, the sites with which they're transferring data, and attempts to access high-risk sites.

[Schedule Report](#)

Time Range: Past 30 days
Username: sgutti
✕

#### Browsing Summary - Data Transfer

These are the types of sites with which sgutti had the most data transfer.

By Data Transfer
  By Session Count

251.24 GB  
TOTAL DATA TRANSFER

#### Top URL Categories for Data Transfer

Here are the top URL categories for sgutti based on data transfer. You can also see the number of unique URLs visited that fall into each URL category.

#	Category	Unique URLs	Data Transfer
1	custom-category	312	31.01 GB
2	sports	300	31.78 GB
3	2	289	31.53 GB
4	any	305	31.5 GB
5	travel	324	31.43 GB
6	1	309	31.2 GB
7	4	292	31 GB
8	health-and-medicine	305	30.97 GB
9	command-and-control	1,366	0 GB

[View URL Filtering Logs](#)

#### Web Browsing Risk Summary for sgutti

sgutti accessed 5,138 different URLs. Watch out for visits to malicious and high-risk URLs; these sites can expose your network to threats, data loss, and compliance violations. If you see more visits to these sites than you'd expect, adjust your security policy to close the gaps.

##### URLs by risk

- High Risk 0 URLs
- Medium Risk 0 URLs
- Low Risk 0 URLs

##### Malicious URLs

- Malware 3,502 URLs
- Grayware 266 URLs
- Command & Control 5,026 URLs
- Phishing 177 URLs

#### Most Visited Sites

These are the sites sgutti most frequently visited. See the risk level for each site.

#	URL Name	Category	Sessions
1	www.cricket.com	any (11008) (21394)	71,850
2	www.cricket.com	health-and-medicine (11008) (45759)	71,850
3	www.cricket.com	1 (34320)	71,850
4	www.cricket.com	custom-category (11008) (45974)	71,850
5	www.cricket.com	any (11008) (32355)	71,850
6	www.cricket.com	2 (11008) (28879)	71,850
7	www.cricket.com	any (11008) (34425)	71,850
8	www.cricket.com	any (49297)	71,850
9	www.cricket.com	sports (11008) (37570)	71,850
10	www.cricket.com	1 (11008) (39892)	71,850

[View URL Filtering Logs](#)

#### Blocked URLs that sgutti Attempted to Access

Your security policy blocked sgutti from accessing 3,090 different URLs.

##### URLs by risk

- High Risk 0 URLs
- Medium Risk 0 URLs
- Low Risk 0 URLs

##### Malicious URLs

- Malware 0 URLs
- Grayware 1 URL
- Command & Control 3,026 URLs
- Phishing 177 URLs

#### Blocked URLs with the Most Attempted Visits

These are the blocked URLs that sgutti most frequently attempted to access.


#	URL Name	Category	Sessions
1	www.cricket.com	4 (11008) (40642)	71,850
2	www.cricket.com	4 (11008) (30222)	71,850
3	www.cricket.com	sports (11008) (37256)	71,850
4	www.cricket.com	any (11008) (48181)	71,850
5	www.cricket.com	health-and-medicine (11008) (30214)	71,850
6	www.cricket.com	sports (11008) (49797)	71,850
7	www.cricket.com	travel (11008) (39558)	71,850
8	www.cricket.com	1 (11008) (21327)	71,850
9	www.cricket.com	1 (11008) (44970)	71,850
10	www.cricket.com	4 (11008) (24241)	71,850

[View URL Filtering Logs](#)

## Download, Share, and Schedule Reports

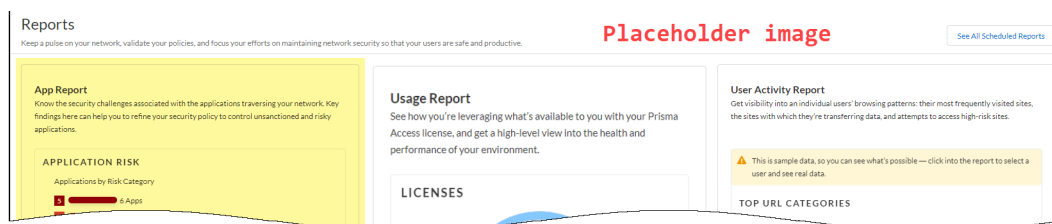
You can share reports within your organization, and also schedule reports so that they're delivered to your email inbox—and your colleagues inboxes—at regular intervals (daily, weekly, or monthly). Reports are delivered as PDFs.

So that you can easily share reports with people in your organization, [set up Directory Sync for Prisma Access](#). Directory Sync gives Prisma Access read-only access to your Active Directory information. With Directory Sync set up, you can easily add recipients to a scheduled report. Prisma Access checks report recipients against Directory Sync, and if it doesn't find a match, performs an extra validation step by checking the email address domain against the email address domains associated with your support account. These checks ensure that Prisma Access reports are not sent outside of your organization.

 *All Prisma Access Cloud Management roles enable you to view, share, and schedule reports, with one exception: Audit Admins can view reports, but cannot share reports or add/edit report schedules.*

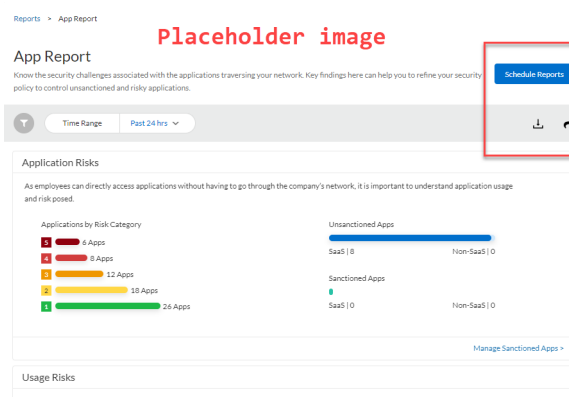
To download, share, or schedule a report:

### STEP 1 | From the Reports home page, open a report.



### STEP 2 | From the report dashboard, choose to download the report, share the report, or schedule the report.

Reports are shared and downloaded as PDFs.



### STEP 3 | If you're scheduling a report, you'll need to continue to define the report parameters including:

- the **Time Period** for which to gather data
- the **Recurrence**, which is the frequency at which you'd like the report to be delivered (daily, weekly, or monthly)

Schedule Report Placeholder image x

**REPORT DETAILS**

Type: **App Report**

Time Period:  Past 24 hrs  Past 7 days  Past 30 days

**REPORT SCHEDULE**

Start Date:

Recurrence:

At:

Add people to share:



# Insights in Prisma Access

Continuously monitor the health and performance of your Prisma Access environment with **Insights** in the Prisma Access app. Visit the hub to get started.

- > [First Look at Insights in Prisma Access](#)
- > [Go to Insights in Prisma Access](#)
- > [Give the Right People Access to Prisma Access](#)
- > [Learn About Prisma Access Alerts](#)
- > [Choose a Preferred Window for Certain Prisma Access Upgrades](#)
- > [Release Updates](#)





# First Look at Insights in Prisma Access

Prisma Access gives you a way to continuously monitor your Prisma Access environment. When an event or status requires your attention, Prisma Access sends you alert notifications so you can quickly pinpoint issues that you can fix and so that you have visibility into the fixes the Prisma Access team is working on.

**Prisma Access > Insights** displays a bird's-eye view of your entire environment:

The screenshot shows the Prisma Access Insights Summary dashboard. On the left is a dark navigation sidebar with the 'ACCESS BY PALO ALTO NETWORKS' logo at the top. Below the logo are several menu items: Insights (selected), Summary, Remote Networks, Mobile Users, Service Connections, Prisma Access Locations, Tunnels, Alerts, Autonomous DEM, Manage, Logs, and Reports. Three callout boxes with arrows point to specific parts of the dashboard:

- The first callout points to the 'Summary' menu item and says: "Monitor the health and performance of your Prisma Access environment".
- The second callout points to the 'Remote Networks' menu item and says: "Verify communication between remote networks, mobile users, and other corporate networks (your HQ and data centers)".
- The third callout points to the 'Alerts' menu item and says: "Zero in on issues that need your attention, and configure alert notifications".

The main content area of the dashboard includes a 'Summary' header, a 'Time Range' dropdown set to 'Last 30 Days', a 'Remote Networks' donut chart showing '19 Remote Networks Alerts', and sections for 'Open Alert Status', 'Connectivity Status', and 'Remote Networks'.

Multiple dashboards give you focused views of your different deployments, your alerts, and the Prisma Access infrastructure. You can adjust and toggle your view to evaluate trends over time or examine data from a different angle. Drill down for details on specific users, sites, connections, or Prisma Access infrastructure components.

This screenshot shows a drill-down view of the 'Remote Networks' dashboard. The top navigation bar includes 'Remote Networks', 'Monitoring Summary', 'Map View', and 'Site List'. A 'Status Distribution' donut chart shows '50 Remote Networks Alerts'. Below this is a '50 Total Sites' section with a table of site details:

Site Name	Site Status	Tunnels (Current)
Canada-Branch-1	Down	0/1 Up
Canada-Branch-1	Up	1/1 Up
Canada-Branch-2	Up	1/1 Up
Canada-Branch-3	Up	1/1 Up
Canada-Branch-4	Up	1/1 Up
Canada-Branch-5	Up	1/1 Up
Canada-Branch-6	Up	1/1 Up

The 'Site List' is selected, showing a detailed view for 'Canada-Branch-1 x'. This view includes a 'Trends' section with a line chart for 'Bandwidth (Mbps)' over time, comparing 'Average Tunnel Ingress', 'Average Tunnel Egress', 'Peak Tunnel Ingress', and 'Peak Tunnel Egress'. Key metrics include 'Maximum allocated - 150.00 Mbps' and a '60% consumption threshold - 120.00 Mbps'. At the bottom, there are sections for 'Health', 'Connectivity', and 'Consumption'.

[Go to Insights](#) to start monitoring your Prisma Access.

---

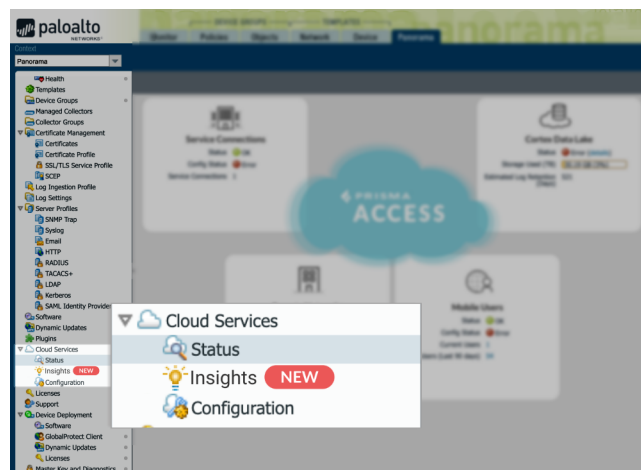
# Go to Insights in Prisma Access

The hub is a single place where you can access the Palo Alto Networks cloud services and apps for your organization. From [the Prisma Access app](#) on the [hub](#), you can select **Insights** to monitor your Prisma Access environment.

To login to the hub, and then to Prisma Access:

- Use the credentials associated with your Palo Alto Networks support account to log in to the [hub](#).
- Confirm that you—and any other users you'd like to access Prisma Access or receive alerts—have the [hub role required to access the app](#). If you are not able to log in to the app, it might be because you are not assigned one of the hub roles that would grant you access.

If you're using Panorama to manage Cloud Managed Prisma Access, you can also select **Insights** directly from Panorama:



This will take you to the hub, where you can then view **Insights** from the Prisma Access app.

---

# Give the Right People Access to Prisma Access

The hub is a single place where you can access the Palo Alto Networks cloud services and apps for your organization. The Prisma Access app is only available to Prisma Access users, and you can find it on the [hub](#). To access the Prisma Access app, you—and any others you'd like to use the app—must be assigned the required [hub role](#). Additionally, users to whom you want to send Prisma Access alert notifications must also have a hub role that grants them access.

Only one of these roles is needed to use Prisma Access and to receive Prisma Access alerts. The role you assign depends on the level of access the user requires and the management interface you're using for Prisma Access (Panorama or the Prisma Access app).

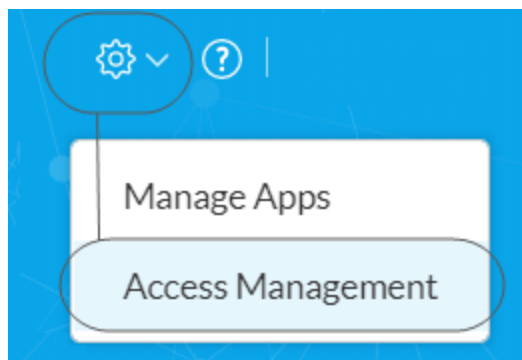
- ❑ **Account Administrator**—The account administrator role on the hub is automatically assigned to the first user from your organization to register on the Palo Alto Networks customer support portal. However, other users can also have this role; there's no limit to the number of users to which you can assign this or any other role. Account administrators can access any of your organization's apps, and you must be an account administrator to assign roles to other users.
- ❑ **(Panorama Managed Prisma Access) A Panorama role**—A Panorama app administrator and instance administrator can access and use the Prisma Access app.

Granting a user a Panorama role on the hub does not affect or impact Panorama access permissions. Right now, the Panorama hub role only controls access to the Prisma Access app.

- ❑ **(Cloud Managed Prisma Access only) A Prisma Access role**—A Prisma Access app administrator and instance administrator can access and use the Prisma Access app.

Here's how to view your hub role assignments and assign hub roles for Insights to other members of your support account:

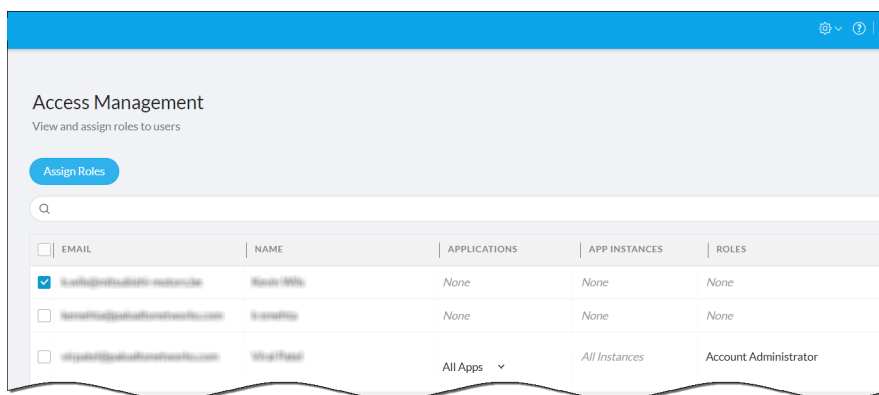
- View hub role assignments.
  1. Use the credentials associated with your Palo Alto Networks support account to log in to the [hub](#).
  2. Click the settings gear that's located on the top right of the page, and select **Access Management**.



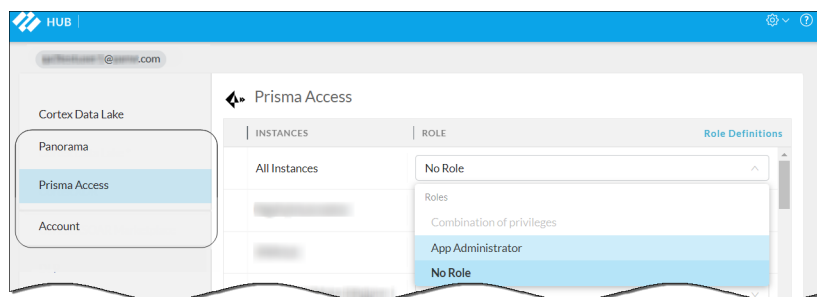
3. The Access Management page lists all the users in your organization and the roles to which they're assigned.

Account administrators have access to all of your organization's apps. Other roles are specific to apps or even app instances.


- Assign a user one of the roles required for Insights.
  1. On the [hub Access Management page](#), search for and select the user to whom you want to assign a role.




2. Click **Assign Roles**.
3. Assign roles at the account level, app level, or instance level.



- **Account**—Assign the **Account Administrator** role to the user. Account administrators can access all apps associated with this account.
- **Panorama**—Assign the Panorama **App Administrator** or **Instance Administrator** roles to the user. Depending on the access level you choose, the user will be able to access Insights data and receive alerts for all your Panorama Managed Prisma Access instances or only specific instances. Granting a user a Panorama role on the hub does not affect or impact Panorama access permissions. Right now, the Panorama hub role only controls access to the Insights app.

 *This role is for Panorama Managed Prisma Access users only. Do not use this role if you're using the Prisma Access app for Cloud Managed Prisma Access.*

- **Prisma Access**—Assign the Prisma Access **App Administrator** or **Instance Administrator** roles to the user. Depending on the access level you choose, the user will be able to access Insights data and receive alerts for all your Cloud Managed Prisma Access instances or only specific instances. This is the same role required to access the Prisma Access app for Cloud Managed Prisma Access. Granting users this role will mean they can also access the Prisma Access app.

 *This role is for Cloud Managed Prisma Access users only. Do not use this role if you're using Panorama to manage Prisma Access.*

---

# Learn About Prisma Access Alerts

Prisma Access alerts you when something is not right in your environment. Alerts details describe the issue, give you context, and guide you to a resolution. Alerts also let you know if there's an issue impacting the Prisma Access cloud infrastructure, so that you're aware as the Prisma Access team works on a fix.

Prisma Access enables you to set up alert notifications so that you can receive alerts directly in your email inbox.

Alerts are resolved only when the issue that triggered the alert is fixed; you cannot manually resolve alerts. Users subscribed to alert notifications receive a notification both when Prisma Access first detects an issue and when it is resolved.

- [All Prisma Access Alerts](#)
- [Investigate Alerts in Prisma Access](#)
- [Turn on Alert Notifications](#)

## All Prisma Access Alerts

Prisma Access provides two types of alerts:

- [Environment Alerts](#) describe the status of your Prisma Access environment, especially if something is not working as expected.

Prisma Access generates alerts when an issue is raised, and also when it's resolved so that you know it's been addressed. You cannot manually resolve alerts—an alert is only considered resolved when the issue triggering the alert has been fixed. Some alerts let you know about issues that the Prisma Access team is working on; others let you know about issues that you can resolve with a configuration update.

- [Upgrade Notifications](#) alert you about upcoming software upgrades and status for upgrades that are in-progress or completed.



*Also subscribe to [status updates for Palo Alto Networks cloud services](#).*

[Turn on Alert Notifications](#) to receive email updates when Prisma Access detects an issue and when it is resolved.

## Environment Alerts

Alert	Scope	What does this mean?	What action can you take?
<b>A Prisma Access location is down</b>	Remote Networks	A Prisma Access location has been down for more than two minutes, and we're working on a fix. Check the status of remote network sites in this location to see how they are impacted.	Check the status of remote network sites in this location to see how they are impacted, and hang in there while the Prisma Access team works to fix this. We'll send you a notification to let you know when we've resolved this.

Alert	Scope	What does this mean?	What action can you take?
<b>A remote network site is not connected to Prisma Access</b>	Remote Networks	All tunnels connecting a remote network site Prisma Access are down.	Check the IPSec tunnel configuration for this remote network site.
<b>A tunnel is down (and tunnel monitoring is not enabled)</b>	Remote Networks	The tunnel has been down for more than five minutes. Note that you do not have tunnel monitoring configured.	Check the configuration for the remote network site and the IPSec tunnel that is down.  Also consider turning on tunnel monitoring to proactively detect tunnel connectivity issues.
<b>A tunnel is down (and tunnel monitoring is enabled)</b>	Remote Networks	Tunnel monitoring detects that a tunnel has been down for more than five minutes.	Check the configuration for the remote network site and the IPSec tunnel that is down.
<b>A remote site reached 80% capacity and sustained it for one hour (non-aggregate bandwidth deployment)</b>	Remote Networks	The remote network experienced sustained usage at 80% capacity for the last hour.	Monitor the remote network site bandwidth utilization in Prisma Access while you continue with regular business operations.
<b>A remote site reached 90% utilization and sustained it for ten minutes (non-aggregate bandwidth deployment)</b>	Remote Networks	The remote network experienced sustained usage at 90% capacity for 10 minutes.	Monitor the remote network site bandwidth utilization in Prisma Access while you continue with regular business operations.
<b>A Prisma Access location is down</b>	Mobile Users	This Prisma Access location has been down for more than two minutes, and we're working on a fix. In the meantime, mobile users in this location automatically connect to another of your Prisma Access locations.	Hang in there while the Prisma Access team works to fix this. We'll send you a notification to let you know when we've resolved this.
<b>A Prisma Access login portal is down</b>	Mobile Users	The impact to your users is minimal when a single Prisma Access login portal is down. If all Prisma Access login portals are down, only Prisma Access users who are connecting for	Hang in there while the Prisma Access team works on a fix. We'll send you a notification to let you know when we've resolved this.

Alert	Scope	What does this mean?	What action can you take?
		the first time are impacted. These users must wait for the portal to be up before they can successfully log in.	
<b>75% of The IP address pool blocks configured for Worldwide coverage of mobile users are being utilized and 25% pool blocks are available for future allocation</b>	Mobile Users	One IP address pool block unit is a /24 subnet (254 IP addresses) and Allocation of a pool block does not result in utilization of all 254 IP addresses in the pool block, 25% of pool blocks are still available to be allocated to the existing mobile user gateways or new ones as user count increases.	Monitor pool block utilization in Prisma Access while you continue with regular business operations.
<b>90% of The IP address pool blocks configured for Worldwide coverage of mobile users are being utilized and 10% pool blocks are available for future allocation</b>	Mobile Users	One IP address pool block unit is a /24 subnet (254 IP addresses) and Allocation of a pool block does not result in utilization of all 254 IP addresses in the pool block, 10% of pool blocks are still available to be allocated to the existing mobile user gateways or new ones as user count increases.	Monitor pool block utilization in Prisma Access while you continue with regular business operations.
<b>A Prisma Access Mobile User Gateway was automatically scaled to provide more capacity</b>	Mobile Users	New public IP addresses have been added to the reserved public IP address pool.	If you use an allow list with SaaS applications or third-party providers, make sure to add the new IP addresses to the allow list.
<b>A service connection is down</b>	Service Connection	All Prisma Access nodes that process traffic for this service connection are down. We're aware of this issue and working on a fix.	Hang in there while the Prisma Access team works on a fix. We'll send you a notification to let you know when we've resolved this.
<b>A service connection tunnel is down</b>	Service Connection	A service connection tunnel has been down for at least two minutes.  If this is the only tunnel configured for the service connection (there's no secondary tunnel configured), this might mean that the connection between an HQ or	Check the IPSec tunnel configuration for this service connection.

Alert	Scope	What does this mean?	What action can you take?
		data center and Prisma Access is down.	
<b>A service connection tunnel is flapping</b>	Service Connection	A service connection tunnel has disconnected from Prisma Access (and then reconnected) at least two times in the last five minutes.	Check the IPSec tunnel configuration for this service connection.
<b>A service connection has been at 80% capacity for the past hour</b>	Service Connection	The service connection is experiencing sustained usage at 80% capacity for the last hour.	Monitor bandwidth utilization for the service connection on Prisma Access while you continue with regular business operations.
<b>A service connection reached 90% capacity and sustained it for the last ten minutes</b>	Service Connection	The service connection is experiencing sustained use at 90% capacity.	Monitor bandwidth utilization for the service connection on Prisma Access while you continue with regular business operations.
<b>A Prisma Access location has lost connectivity to some SaaS applications</b>	Prisma Access Location	A Prisma Access Location has not been able to connect to some SaaS applications for more than five minutes. This impacts mobile users and remote network sites connecting to this location.	Hang in there while the Prisma Access team works on a fix. We'll send you a notification to let you know when we've resolved this.
<b>A Prisma Access location has lost internet connectivity</b>	Prisma Access Location	A Prisma Access location has not been able to reach the internet for more than five minutes.  This impacts mobile users and remote network sites connecting to this location.	Hang in there while the Prisma Access team works on a fix. We'll send you a notification to let you know when we've resolved this.

## Upgrade Notifications

Alert	What does this mean?	What action can you take?
<b>Planned Software Upgrade</b>	Informs you 21 days ahead of a scheduled software upgrade. You have the options to choose the Prisma Access locations you want to upgrade first, and set a preferred upgrade time window.	Select your upgrade preferences, including a preferred time window from the list of available options and the Prisma Access locations you would like to upgrade first. See <a href="#">Choose a Preferred Window for Certain Prisma Access Upgrades</a> for details.

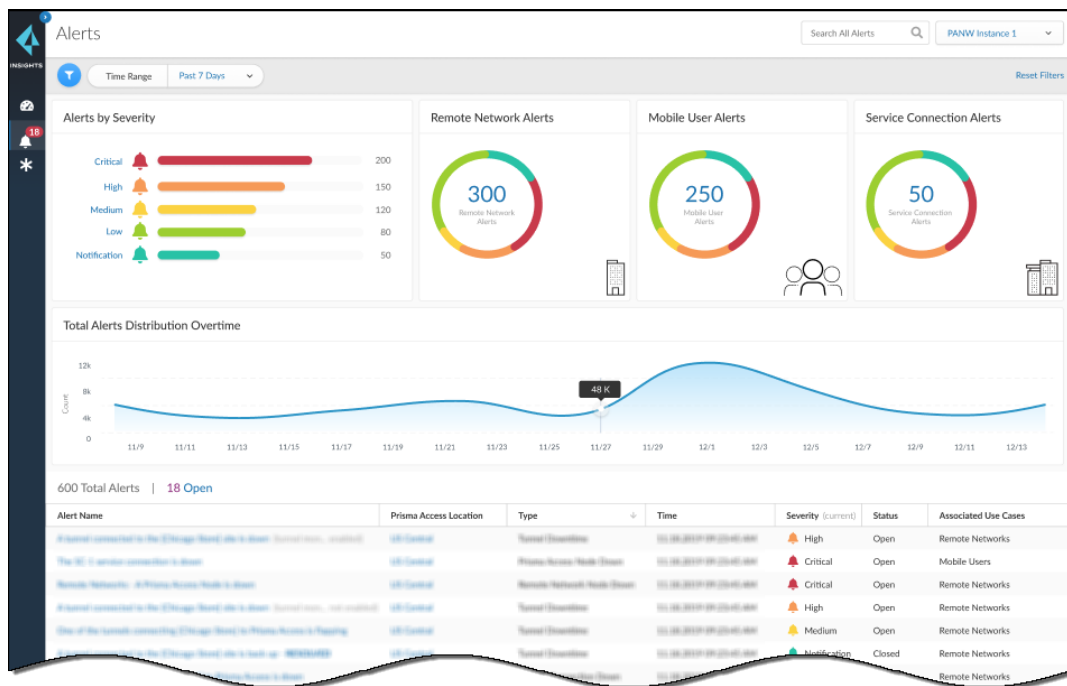


Alert	What does this mean?	What action can you take?
		<p>If you have not yet done so, make sure that you have Panorama Managed –retrieved and added Prisma Access IP addresses Cloud Managed – Retrieve the IP Addresses to Allow for Prisma Access</p> <p>to your organization’s allow lists, including both reserved and active IP addresses. After a dataplane upgrade, the reserved IP addresses for mobile user gateways and portals become active, and the active IP addresses become reserved.</p>
<b>Software Upgrade Preference Confirmation</b>	Confirms that you’ve chosen a time window and a Prisma Access location for a software upgrade to take place.	Plan for the upgrade window. You can make configuration changes and commit and push your changes during this time.
<b>Three Day Notice for a Software Upgrade</b>	Lets you know that a software upgrade is scheduled for three days from now.	Plan for the upgrade window. You can make configuration changes and commit and push your changes during this time.
<b>24 Hour Notice for a Software Upgrade</b>	Lets you know that a software upgrade is scheduled for 24 hours from now.	Plan for the upgrade window. You can make configuration changes and commit and push your changes during this time. When the software upgrade is in progress, you will not be able to commit and push your changes on your Prisma Access deployment.
<b>A Software Upgrade is in Progress</b>	Alerts you to a software upgrade that is in progress, and the Prisma Access locations that are being upgraded.	When the software upgrade is in progress, you can make configuration changes but cannot commit and push your changes on your Prisma Access deployment.
<b>A Software Upgrade for a Prisma Access Location is Complete</b>	<p>If your upgrade preferences include a Prisma Access location to upgrade first, this notification lets you know that this location is upgraded successfully.</p> <p>The Prisma Access team now has this location under advanced monitoring.</p> <p>Your remaining Prisma Access locations will be upgraded seven days from now, at local time based on your preferred time window.</p>	For the remaining Prisma Access locations, if any in your deployment, that will be upgraded, we’ll notify you three days and 24 hours in advance. We will also notify when the upgrade is in progress, and when it is complete. When the software upgrade is in progress for remaining Prisma Access locations, you can make configuration changes but cannot commit and push your changes on your Prisma Access deployment.
<b>Software Upgrades for all Prisma Access Locations</b>	All your Prisma Access locations are successfully upgraded.	You can make configuration changes and commit and push your changes at this time. The new Cloud Services plugin will be released when all your Prisma

Alert	What does this mean?	What action can you take?
are Completed Successfully		Access locations are upgraded. Monitor your notifications from Prisma Access to see when the new plugin is available to upgrade.
Software Upgrade Roll-Back	The Prisma Access team closely monitors Prisma Access locations following a software upgrade. We've found something unexpected, and are rolling Prisma Access back to the software version that was previously running on your Prisma Access locations.	While roll-back is in progress, you cannot commit and push changes to Prisma Access. You'll receive a notification when the roll-back is complete.
Canceled Software Upgrade	A scheduled software upgrade is canceled.	There's no impact to you. The Prisma Access team will let you know when the next upgrade is scheduled.

## Investigate Alerts in Prisma Access

Prisma Access shows you open and resolved alerts from the past 30 days, though you can narrow your alert view to focus in on specific time periods.








Click on an alert to learn more about the what's happening and the impact to your mobile users and remote sites.

# A tunnel connected to the [Chicago Store] site is down

**HIGH**

Tunnel monitoring detects that the tunnel has been down for more than five minutes.

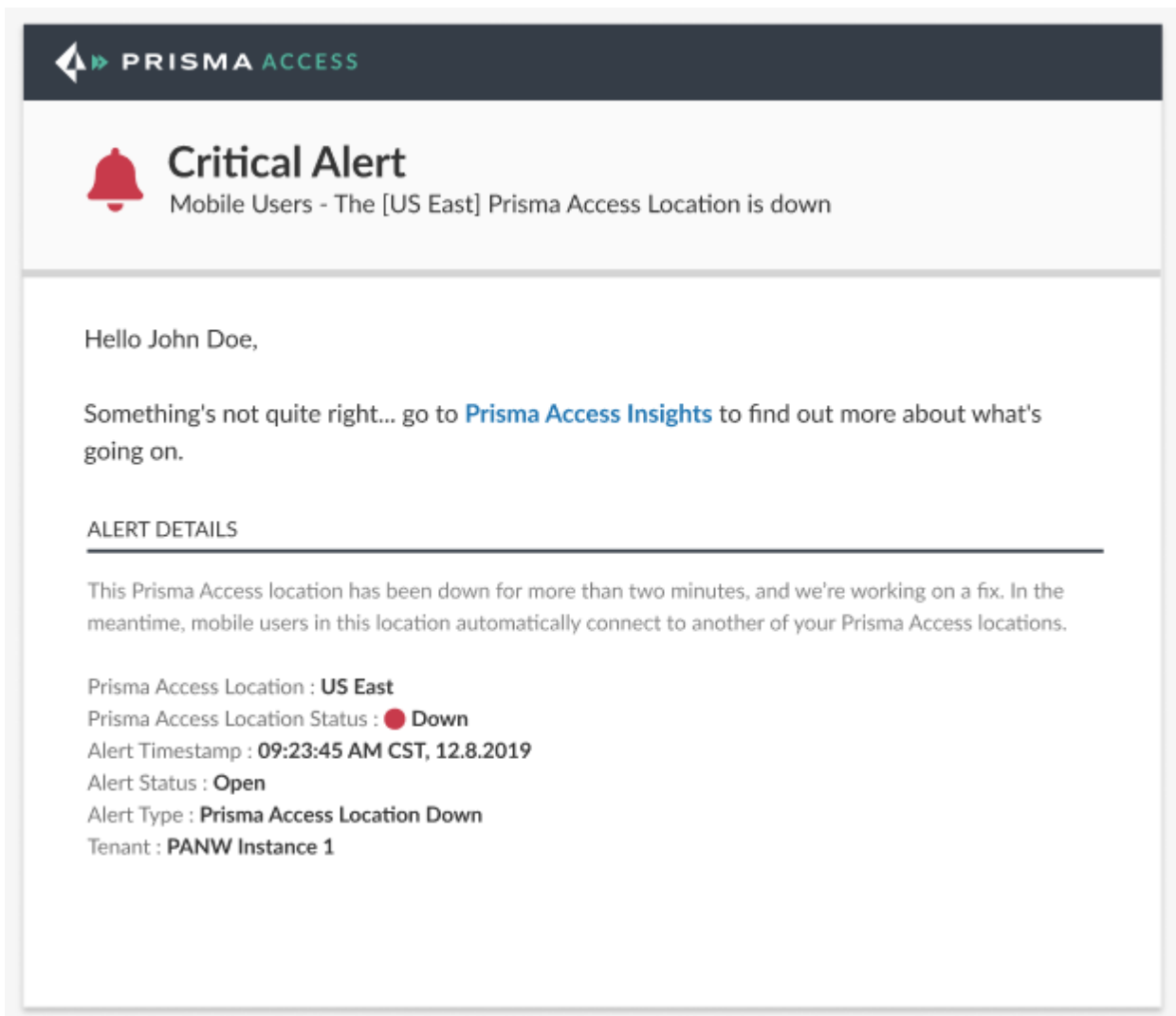
## Health and Connectivity

 Impacted Site	Chicago Store
 Tunnel Name	Chicago Store Tunnel 1
Tunnel Status	 <b>Down</b>   This IPsec tunnel has been down for more than five minutes
Alert Timestamp	Sep 20, 2019 12:40 PM
Alert Status	Open
Alert Type	Tunnel Downtime
 Prisma Access Location	 <b>Up</b>   US Central
Tenant	PANW Instance 1

## Turn on Alert Notifications

Enable Prisma Access to send email alerts when it initially detects an issue and when the issue is resolved. These alert notifications describe the issue and impact, and include a link to Prisma Access where you can investigate further.

The Palo Alto Networks email address from which you receive alert notifications is [noreply@paloaltonetworks.com](mailto:noreply@paloaltonetworks.com).



To send alert notifications to an email destination:

**STEP 1** | [Grant access](#) for the people whom you want to receive alert notifications.

To receive alerts, you must be a Prisma Access admin. There are three types of admin roles, but only account administrators can grant users access to an app. Go to the [hub](#) to check role assignments and assign roles.

**STEP 2** | Log in to Prisma Access from the [hub](#).

**STEP 3** | Go to **Alerts > Alert Subscription > + Add Users**.

**STEP 4** | Enter the email addresses, separated by commas, to which Prisma Access should send alert notifications.

The email addresses to which Prisma Access sends alerts must be the same email addresses associated with users in your Palo Alto Networks support account.

**STEP 5** | In a multitenant deployment, select the sub-tenants for which you want users to receive notifications or **All Sub-Tenants** if you want them to receive notifications from all sub-tenants.

---

STEP 6 | **Add** the users.

---

# Choose a Preferred Window for Certain Prisma Access Upgrades

For certain Prisma Access upgrades—*learn about the different types of [Cloud Managed](#) and [Panorama Managed updates](#)*—Prisma Access Insights lets you make upgrade preferences:

- **Time Window**

Select a preferred time window, from the list of available options, for the upgrade.

- **Prisma Access Locations**

Choose the Prisma Access locations you want to upgrade first.

You can choose a collection of Prisma Access locations to upgrade first. Palo Alto Networks uses your preference to begin the roll out to the first set of Prisma Access locations and the remaining locations, if any will be upgraded seven days later based on the time preference you provided. Prisma Access Insights [provides you with notifications](#) that inform you of the progress of the upgrade and when it is complete, whether or not you select all locations or a subset of them.

After the first set of Prisma Access locations is upgraded successfully, the Prisma Access team monitors these locations for seven days, and then continues to upgrade all remaining Prisma Access locations. The remaining Prisma Access locations are upgraded at local time based on your time preference.

When upgrade preferences are available for a release, Prisma Access will notify you. Enable alerts to get notifications when an upgrade preference is available, and go to the Prisma Access app to submit your preferences:

## STEP 1 | [Turn on alert notifications](#) to get upgrade notifications delivered to your email inbox.

We'll send you notifications:

- When the option to choose your upgrade preferences (time window and Prisma Access locations) is available
- To confirm upgrade preferences
- To give you 21-day, three day, and 24 hour notice ahead of a scheduled upgrade
- When a Prisma Access location upgrade is in progress
- When a Prisma Access location upgrade is complete
- When all Prisma Access locations are successfully upgraded

## STEP 2 | After you are notified that an upgrade window preference is available, go to the Prisma Access app to choose your preferred upgrade window.

1. [Go to Prisma Access.](#)
2. You'll see a banner in the app that guides you to set upgrade preferences.
3. You'll see an option to choose your upgrade time.

Choose your preferred upgrade time window from the selections available, along with a set of Prisma Access locations you want upgraded during this window.

After you've submitted your upgrade preferences, you'll receive a Prisma Access notification confirming your preferences. You cannot change your upgrade preferences after you've submitted them.

# Release Updates

Here's where you can learn about the latest features related to the Insights capability in Prisma Access and the known issues the team is working on to improve your experience:

- [What's New](#)
- [Known Issues](#)

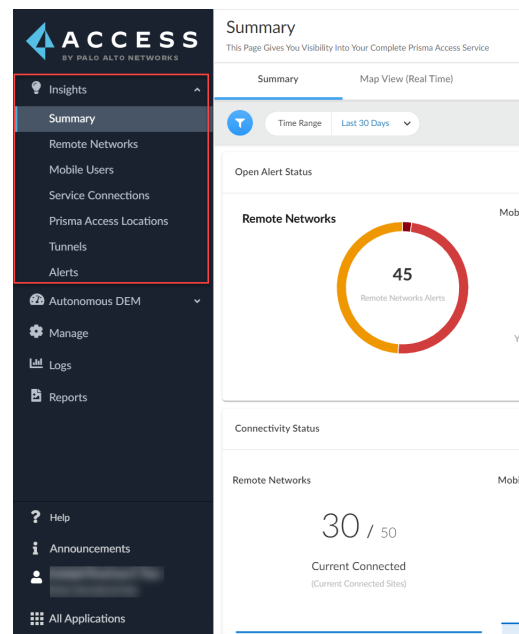
## What's New

Here's what's new in Prisma Access Insights:

### New Features in February 2021

#### Integration with Prisma Access App

To centralize monitoring and management in a single application, Prisma Access Insights is now located within the Prisma Access app.



#### Summary Dashboard

**Real-Time Data**—To help you better understand the current load on your system and take the appropriate action, the Summary dashboard now emphasizes real-time, actionable data, such as total open alerts and currently connected users.

**Map View**—A geographic map of your Prisma Access locations enables you to assess the real-time status of each location by its number of connected users, functioning remote network nodes, and service connection sites.

---

**Remote Networks**

**Map View Interactions**—To help you visualize and monitor your deployment, the Remote Networks dashboard now provides an interactive map of your Prisma Access locations. Clicking on a location presents you with additional details, such as aggregate bandwidth, so that you can take proactive measures.



**Aggregated Bandwidth Chart Tools**—You can now identify trends in your network traffic by toggling specific metrics on the Aggregated Bandwidth chart, such as averages and peaks for incoming and outgoing traffic.

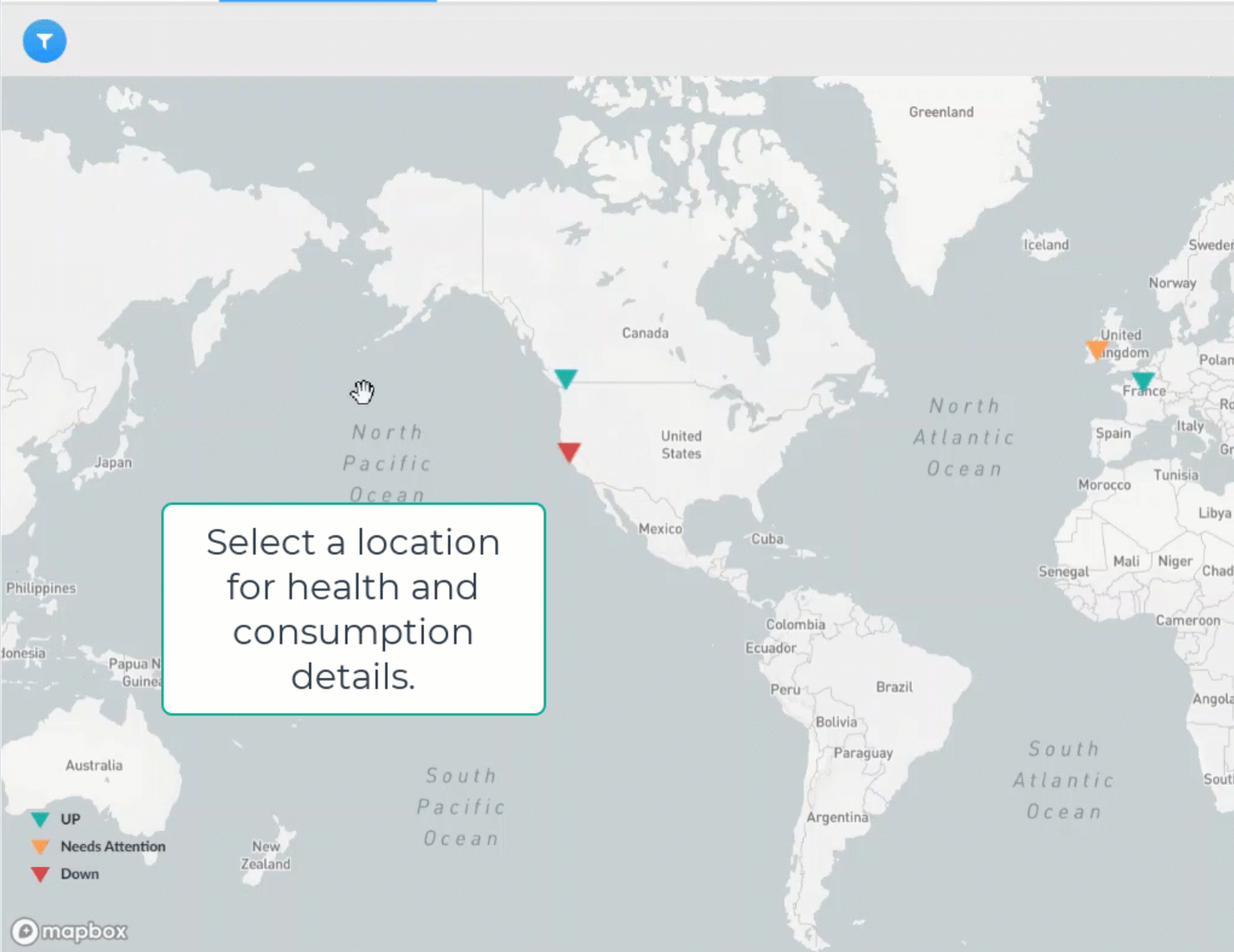
## Remote Networks

Search All Sites

Monitoring Summary

Map View

Site List



## Mobile Users

**IP Address Pool Visibility**—The Mobile Users dashboard now gives you real-time visibility into the capacity of your IP address pools so that you can take action well before space runs out.

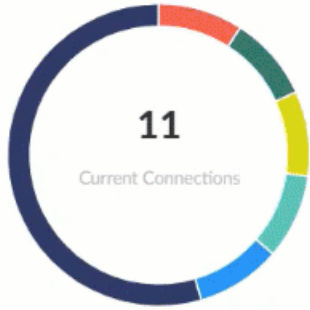
**User Flight Paths**—To help you keep track of the number and location of your mobile users, you can now click on a Prisma Access site to reveal a flight path between the site and uniquely connected users.

To help you visualize distance, the flight path is in different colors; green is less than 500 miles and orange is more than 500 miles. When you select a flight path, you can view the connection details and more details on the Mobile Users details page.

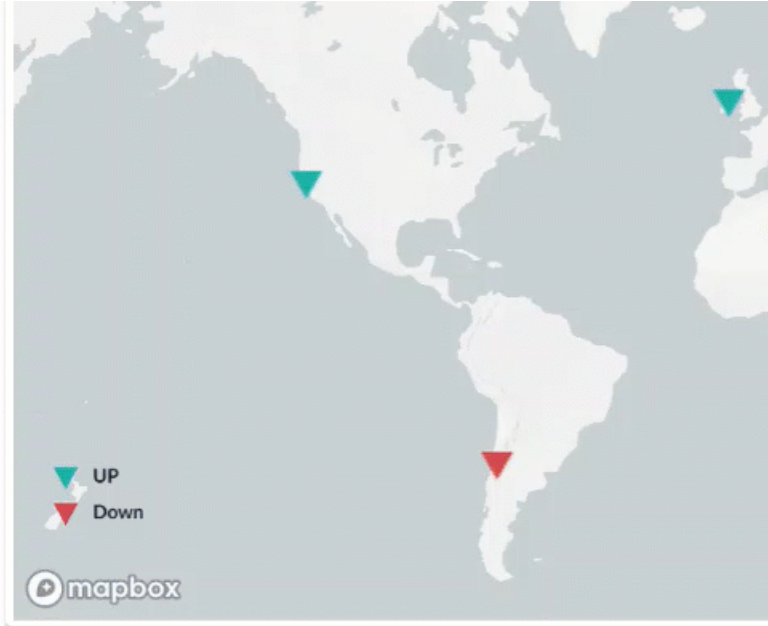
New Features in February 2021

[View all Mobile User Alerts >](#)

GlobalProtect Version Distribution



- v 4.0.2 | 1 Users
- v 5.1.1 | 1 Users
- v 4.1.6 | 1 Users
- v 3.0.1 | 1 Users
- v 5.1.5 | 1 Users
- Others | 6 Users



IP Pools Reaching Maximum Capacity

Real Time

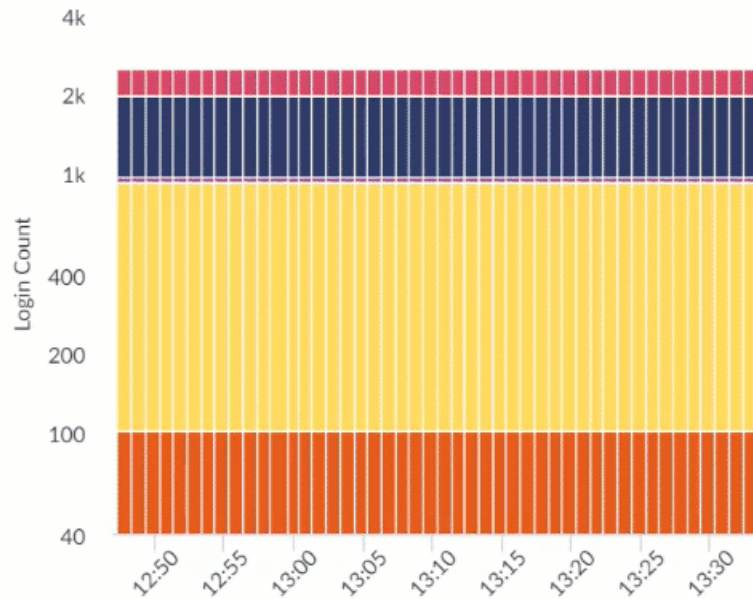
0% AMERICAS

50% APAC

0% EUROPE

99% WORLDWIDE

Top 5 Most Active Prisma Access Locations for Mobile Users



<https://www.paloaltonetworks.com/insights/sase-mobile-users>

**Service Connections**

**Service Connections Dashboard**—For better visibility into your Prisma Access service connection locations, a dedicated dashboard now shows you the operational status of your locations as well as aggregate bandwidth levels.

---

## New Features in February 2021

Like Remote Networks, the new dashboard features a list of sites with an aggregate bandwidth chart that enables you to identify trends in your network traffic by toggling specific metrics, such as averages and peaks for incoming and outgoing traffic. Using filters, you can visualize the bandwidth consumption trend per service connection.

# Service Connections

Monitoring Summary

Service Connections List



Time Range

Last 1 Hour

## Top 5 Open Alerts by Severity



Everything looks good!  
You do not have any alerts for the selected time filter

[View all SC User Alerts >](#)

## Service Connection and Tunnel Status

Real Time

Service Connections

## Deployed Prisma Access Locations



### Alerts

**Updated Workflow for Alert Subscriptions**—As part of the Insights integration with the Prisma Access app, you can now [configure alert notifications](#) from **Alerts > Alert Subscription > + Add Users**.

## New Features in February 2021

The screenshot shows the Prisma Access Alerts page. The left navigation menu is visible, with 'Alerts' highlighted. The main content area shows the 'Alert Subscription' tab selected. A search bar at the top right contains 'Ontexinternationalbvba'. Below the search bar, there are two tabs: 'Alert List' and 'Alert Subscription'. The 'Alert Subscription' tab is active, displaying a list of steps to subscribe users for alerts:

- 1 Create a CSP Account for the new Admins  
*Skip this step if they already have a CSP Account*
- 2 Give the new admin a Network Admin role on the Hub  
*Whoever has a Network Admin role on Hub can Access Prisma Access Insights.*
- 3 Add the emails for new Admins below to send them alert notifications  
*Once you enter these email addresses, they will be validated before you hit add and then alert notifications will be sent to them.*

Below the steps, there is a table showing the total number of admins and a list of admin email IDs with their corresponding tenants subscribed.

1 Total Admins

Admin Email ID	Tenants Subscribed	Action
<a href="#">c@d.com</a>	1	

The URL at the bottom of the screenshot is <https://dev-lawkes1.prismaaccess.paloaltonetworks.com/insights/sase-alerts>.

**Remote Network and Service Connection Utilization**—Prisma Access now features new alerts to help you monitor your remote networks, service connections and mobile users. The new alerts for remote networks and service connections help you manage bandwidth utilization by triggering when throughput levels become too high.

**Mobile User IP Pool Capacity**—The new alerts for mobile users assist in IP address management by letting you know when IP pools are reaching capacity or when a mobile user gateway automatically scales for more capacity.

### Multitenancy Support

If you have multiple Prisma Access tenants associated with one Panorama, you can now switch between those tenants for individual management.

## New Features in February 2021

Additionally, you can configure which users receive alerts from specific tenants to ensure that administrators are only notified about relevant issues.

## Known Issues

These are the issues we're currently working on.

ID	Description
DIT-14540	The Tunnels page on Prisma Access Insights displays an incorrect number of Service Connections.
DIT-13498	Due to an event parsing issue, the Mobile Users dashboard may not accurately reflect the number of unique connected users.
CYR-17008	Insights does not provide visibility or monitoring for Prisma Access Clean Pipe, the outbound internet security solution for managed service providers, and mobile users using an explicit proxy for connecting to Prisma Access.
PAI-543	For tables where you can <b>Export to CSV</b> , the column labels that displays in the user interface are in some cases different from the exported file, and the status of Up and Down are depicted with a numerical value in the file.
PAI-508	Due to an event parsing issue, the <b>Mobile Users</b> dashboard may not accurately reflect the number of unique connected users.
PAI-437	The status of an inactive remote network node may appear as Warning in <b>Remote Networks &gt; Site List &gt; Site Details</b> .
PAI-434	When there are more than 10,000 entries in the Mobile Users List on <b>Dashboards Mobile Users &gt; Mobile Users</b> , there is a delay in the time to load the page details.
PAI-422	Navigating to new pages in Insights removes a blue checkmark that normally appears next to the currently selected sub-tenant in the sub-tenant drop-down.

ID	Description
	<b>Workaround:</b> Reselect the sub-tenant in the drop-down to restore the checkmark.
PAI-421	Some of the sub-tenant names in the sub-tenant drop-down may have an inconsistent format.
PAI-401	If you enter the email addresses of multiple users in <b>Alerts &gt; Alert Subscription &gt; + Add Users</b> and do not separate each address with a comma (,), you are unable to <b>Add</b> them. <b>Workaround:</b> Enter a comma between each email address.
PAI-383	If you attempt to access Prisma Access Insights in a second tab while you already have one open, the second tab will fail to load. <b>Workaround:</b> Use a single tab to work in Access Insights.
PAI-376	When a license has expired, the License Expiration Dates widget on the <b>Summary</b> page shows a negative number of days remaining until the license expires.
PAI-368	In tables that display tunnels and site lists for Service Connections and Remote Networks, when you rename or delete a tunnel configuration on Prisma Access, the data in <b>Dashboards &gt; Remote Networks/Service Connections/Mobile Users &gt; Site List</b> does not display the current status. The information is displayed for 30 days after the change, and the tunnel status displays as <code>Not Available</code> .
PAI-296	When you <b>Export to CSV</b> , the resultant CSV file has the following issues: <ul style="list-style-type: none"> <li>• The column title names do not match the columns in the user interface.</li> <li>• The file includes additional columns not in the user interface.</li> <li>• The status of a site may appear as a number. 0 is Down and 1 is Up.</li> <li>• If you have applied a filter, the CSV includes data outside the scope of the filter.</li> </ul>
PAI-197	If you have more than one service connection or remote network node at a site, the state of that site in your <b>Remote Networks &gt; Site List</b> or <b>Service Connection &gt; Site List</b> can appear both Up and Down simultaneously.



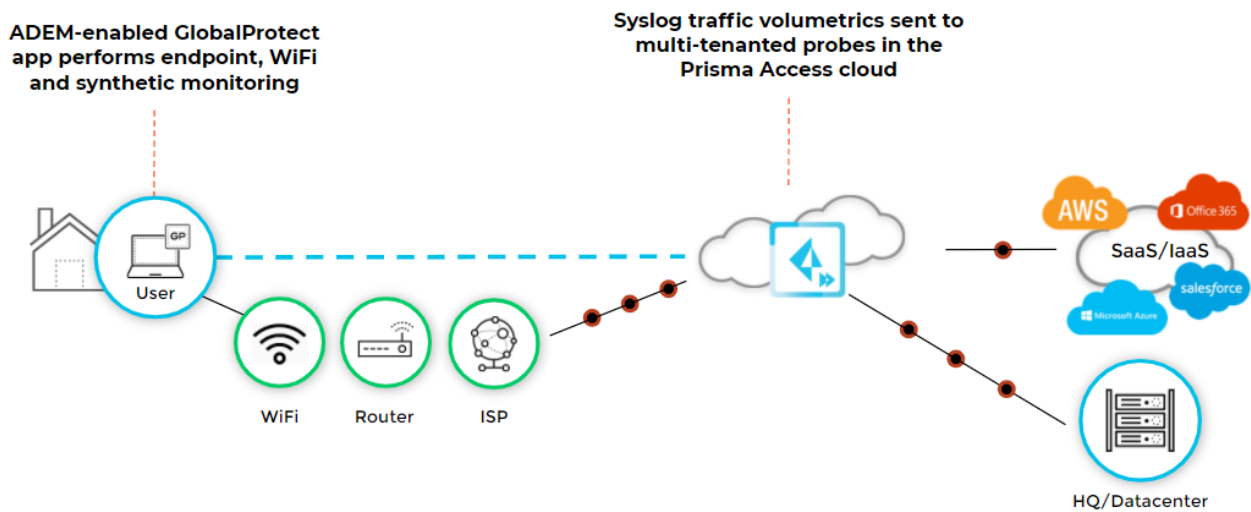
# ***Autonomous DEM in Prisma Access***

- > [Autonomous DEM](#)
- > [ADEM Monitoring and Tests](#)
- > [Get Started with Autonomous DEM](#)
- > [Enable Autonomous DEM for Your Mobile Users](#)
- > [Go to Autonomous DEM in Prisma Access](#)
- > [First Look at Autonomous DEM in Prisma Access](#)
- > [Set up an Autonomous DEM Application Test](#)
- > [Manage Autonomous DEM Users](#)
- > [Known Issues—Autonomous DEM](#)



# Autonomous DEM

Autonomous Digital Experience Management (DEM) is a service that provides native, end-to-end visibility and insights for all user traffic in your Secure Access Service Edge (SASE) environment. Autonomous DEM functionality is natively integrated into the GlobalProtect app and Prisma Access and therefore does not require you to deploy any additional appliances or agents. Because of this native integration, the ADEM service enables [synthetic tests](#) for applications you specify both from the endpoint and from the different vantage points in Prisma Access. ADEM continuously monitors real user traffic as it crosses each segment from the endpoint to the application and identifies baseline metrics for each application, and automatically remediates and issues within the Prisma Access cloud. In addition, ADEM provides visibility into any deviations or events that degrade the user experience across each segment between the end user and the application, whether it's the endpoint, WiFi, LAN, router, ISP, Prisma Access, or the application (SaaS, IaaS, or data center). ADEM continuously monitors every segment in the service delivery path and provides insights that help you quickly isolate the segment which is causing digital experience problems and simplify remediation.

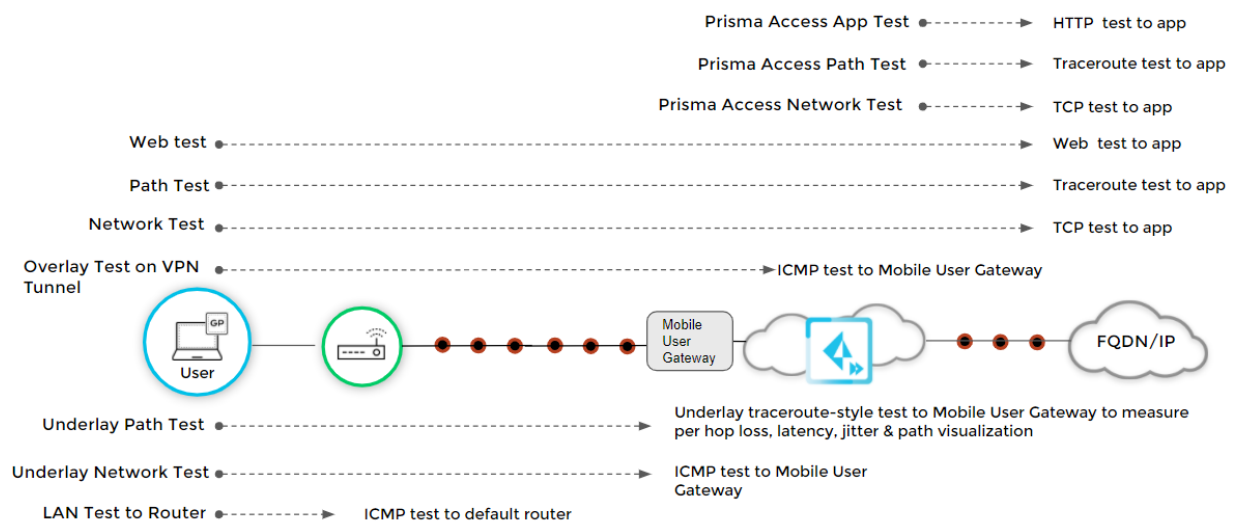


# ADEM Monitoring and Tests

One of the advantages of Autonomous DEM (ADEM) is that it is continuously monitoring each segment in your Secure Access Service Edge (SASE) environment from the user all the way to the application, even if the users and the applications they are accessing are not on your network. ADEM uses a variety of monitoring techniques to determine baseline performance levels, and alert you to changes in performance that lead to degraded user experience.

- **Endpoint monitoring**—As soon as an app test is assigned to a user, the ADEM service begins gathering health telemetry about the device and the WiFi connectivity to help determine whether the device or the WiFi is the cause of any performance issues. Information collected includes:
  - CPU utilization
  - Memory utilization
  - Disk usage
  - Disk queue length
  - Battery level
  - WiFi information (SSID, RX and TX utilization, BSSID, and Channel)
- **Real user traffic visibility**—ADEM continuously provides visibility into real traffic usage between your users and the applications they are accessing, including traffic to SaaS applications, Infrastructure as a Service (IaaS) applications, or other internet-based applications, as well as traffic to applications in your own data center.
- **Synthetic Monitoring**—The DEM-enabled GlobalProtect apps and the ADEM probes within Prisma Access use synthetic tests to baseline end-to-end network quality metrics—latency, jitter, and loss—for each segment from the end user to the monitored applications. In addition, the ADEM agents and probes also use synthetic tests to collect web performance metrics, which capture metrics about the HTTP/HTTPS transactions to a specific application, including application availability and uptime, HTTP latency, DNS lookup, SSL connect, time-to-first-byte, and data transfer rate. In order to run synthetic tests—to SaaS applications or applications in your data center through Prisma Access or via split tunneling—the endpoint must be connected to the VPN.

Because the synthetic tests are layered, they give a good baseline view of the digital experience segment-by-segment across all monitored applications, and allow you to quickly visualize when and where a change occurred that led to degradation of your users' digital experience.



---

# Get Started with Autonomous DEM

To enable Autonomous Digital Experience Management (ADEM) for your Prisma Access mobile users, you must already have a Prisma Access for Users license. You can then apply your ADEM license to your Windows and MacOS users to enable them to run synthetic tests that continuously monitor your users' digital experience on those apps.

Autonomous DEM is supported on GlobalProtect app version 5.2.6 running on Windows or MacOS endpoints only.

- You must be using Cloud Managed Prisma Access or the 2.0 Innovation Release of Panorama Managed Prisma Access with an active Prisma Access for Users license.

You can use ADEM whether you are using Panorama Managed Prisma Access or Cloud Managed Prisma Access, but you will [manage ADEM](#) from the Cloud Management console.

- Purchase Autonomous DEM license for your mobile users.

If you purchased an Autonomous DEM license with a new Prisma Access subscription, you will activate ADEM during the Prisma Access activation process. If you purchased an add-on Autonomous DEM license for an existing Prisma Access subscription, activation will happen automatically.

With an active ADEM license, you can configure up to 10 synthetic tests per user (though the number of tests aren't limited at the user level, so you could configure five tests for one user and 15 tests for another).

- Verify that the users for which you want to enable ADEM are running a compatible version of the GlobalProtect app.

ADEM requires GlobalProtect app version 5.2.6 or later and is only supported on Windows and MacOS endpoints.

- Enable ADEM in the GlobalProtect app.

The steps you use to enable ADEM depends on whether you are using [Panorama Managed Prisma Access](#) or [Cloud Managed Prisma Access](#).

- Configure security policy to allow your ADEM-enabled GlobalProtect users to connect to the ADEM service and run synthetic tests.

Required security policy includes allowing access to HTTPS, TCP, and ICMP. Optionally you may also need to allow access to HTTP, depending on how you plan to configure your app tests.

- Use the Autonomous DEM Summary and Applications dashboards to within the [Prisma Access Cloud Management console](#) to get a sense of the baseline digital experience score for your SASE environment as a whole, and for each individual application.

Even before you begin configuring app tests to monitor specific applications, you can [use the Applications dashboard](#) to get an overall view of the applications in use across your network and use this information to decide which applications you want to monitor.

- Add app tests for the users and applications you want to monitor.

- 
- Use the [ADEM dashboards](#) to monitor the digital experience of users and applications across your SASE environment and use the information to troubleshoot issues as they arise.

# Enable Autonomous DEM for Your Mobile Users

To enable Autonomous Digital Experience Management (ADEM) for your Prisma Access mobile users, you must enable ADEM in the agent configuration on the GlobalProtect portal. After you enable ADEM in the GlobalProtect agent config, the GlobalProtect portal will automatically push the ADEM capabilities and the required authentication certificate to the selected users the next time they connect.

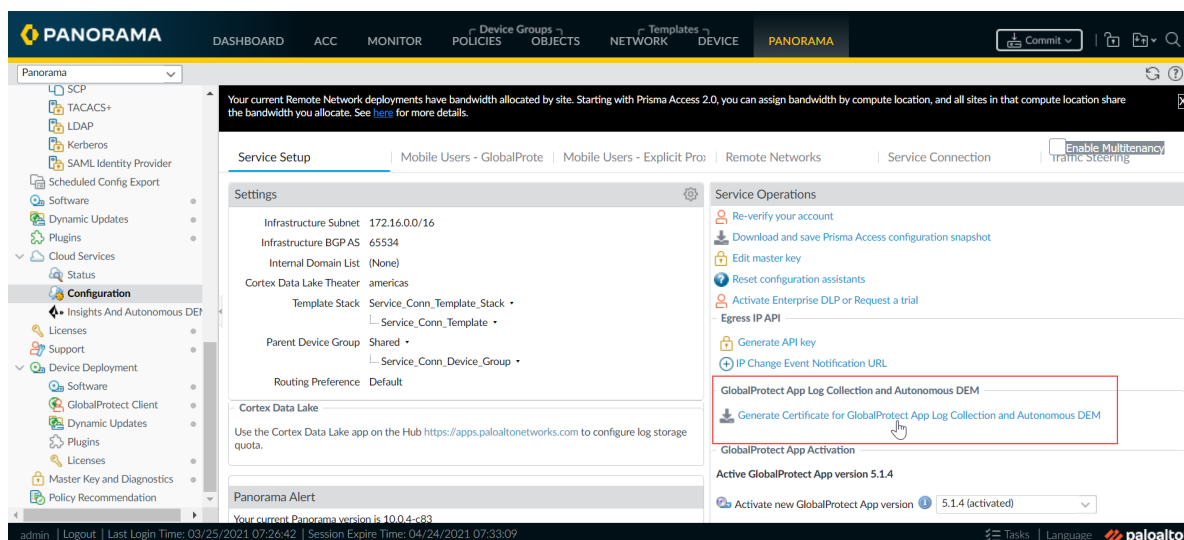
Autonomous DEM is supported on GlobalProtect app version 5.2.6 or later running on Windows or MacOS endpoints only. Because you may not have licensed Autonomous DEM for all of your mobile users, you can clone the default agent configuration on the portal and restrict it to the supported operating systems and the specific users or groups on which you want to enable ADEM.

After the GlobalProtect app receives the ADEM configuration, it uses the corresponding certificate to authenticate to the ADEM service. After the agent registers, you will be able to assign app tests to the user.

To enable Autonomous DEM for your GlobalProtect users:

## STEP 1 | Generate the certificate the agent will use to authenticate to the Autonomous DEM service.

1. From Panorama, select **Panorama > Cloud Services > Configuration > Service Setup**.
2. In the GlobalProtect App Log Collection section under Service Operators, click **Generate Certificate for GlobalProtect App Collection and Autonomous DEM**.



A confirmation message indicates that the certificate was successfully generated in the Mobile\_User\_Template Shared location.

## STEP 2 | Configure the portal to push the DEM settings to the GlobalProtect agent.

1. Select **Network > GlobalProtect > Portals > GlobalProtect Portal**.
2. To create an agent configuration to push to your DEM users only, in the **Mobile\_User\_Template**, select the GlobalProtect Portal Configuration.
3. On the **Agent** tab, select the DEFAULT agent configuration and **Clone** it and give it a new **Name**.
4. To enable the portal to push the DEM authentication certificate you just generated to the end user systems, on the **Authentication** tab set **Client Certificate** to **Local** and then select the **globalprotect\_app\_log\_cert**.

Configs ?

Authentication | Config Selection Criteria | Internal | External | App | HIP Data Collection

Name: ADEM config

Client Certificate: Local | globalprotect\_app\_log\_cert

The selected client certificate including its private key will be installed on client machines.

Save User Credentials: Yes

**Authentication Override**

Generate cookie for authentication override

Accept cookie for authentication override

Cookie Lifetime: Hours | 24

Certificate to Encrypt/Decrypt Cookie: Authentication Cookie Cert

**Components that Require Dynamic Passwords (Two-Factor Authentication)**

Portal  External gateways-manual only

Internal gateways-all  External gateways-auto discovery

Select the options that will use dynamic passwords like one-time password (OTP) to authenticate users as opposed to using saved credentials. As a result, the user will always be prompted to enter new credentials for each selected option.

- To ensure that this agent configuration is only pushed to agents running on supported operating systems, on the **Config Selection Criteria > User/User Group** tab, click **Add** in the **OS** column and select **Mac** and/or **Windows** only).
- If you only want to deploy the DEM configuration to a subset of your Mac and/or Windows users, in the User/User Group column **Add** the specific users or user groups to push this configuration to.

Configs ?

Authentication | **Config Selection Criteria** | Internal | External | App | HIP Data Collection

**User/User Group** | Device Checks | Custom Checks

OS	User/User Group
<input type="checkbox"/> Any	<input type="checkbox"/> select
<input type="checkbox"/> os ^	<input type="checkbox"/> USER/USER GROUP ^
<input type="checkbox"/> Windows	<input type="checkbox"/> gpuser1
<input checked="" type="checkbox"/> Mac	<input type="checkbox"/> user1
	<input checked="" type="checkbox"/> user2

+ Add - Delete

- To enable Autonomous DEM functionality for the selected users, on the **App** tab, enable **Autonomous DEM endpoint agent for Prisma Access (Windows & Mac Only)**.  
You can select whether to let users enable and disable ADEM by selecting **Install and user can enable/disable agent from GlobalProtect** or **Install and user cannot enable/disable agent from GlobalProtect**.



- Also on the **App** tab, set **Enable Autonomous DEM and GlobalProtect App Log Collection for Troubleshooting** to **Yes** to enable the GlobalProtect app to use the certificate you just created to authenticate to the DEM service.

Configs
?

Authentication
Config Selection Criteria
Internal
External
App
HIP Data Collection

**App Configurations**

Enable Autonomous DEM and GlobalProtect App Log Collection for Troubleshooting	Yes
Run Diagnostics Tests for These Destination Web Servers	
Autonomous DEM endpoint agent for Prisma Access (Windows & MAC only)	Install and user can enable/disable agent from GlobalProtect
Device Added to Quarantine Message	Your security policy has restricted access to the network from this device. If the issue persists, contact your administrator.
Device Removed from Quarantine Message	Your security policy has restored access to the network from this device. If you still cannot access the network, contact your administrator.
Display Status Panel at Startup (Windows Only)	No

Welcome Page None

**Disable GlobalProtect App**

Passcode

Confirm Passcode

Max Times User Can Disable

Disable Timeout (min)

**Uninstall GlobalProtect App**

Uninstall Password

Confirm Uninstall Password

**Mobile Security Manager Settings**

Mobile Security Manager

Enrollment Port 443

OK
Cancel

- Click **OK** to save the new app configuration settings and click **OK** again to save the portal configuration.

**STEP 3 |** Make sure you have security policy rules required to allow the GlobalProtect app to connect to the ADEM service and run the synthetic tests.

- To enable the GlobalProtect users to connect to and register with the ADEM service and to run the synthetic application tests, make sure there is a security policy rule that allows traffic to HTTPS-based applications.
- To enable the app to run network monitoring tests, you must have a security policy rule to allow ICMP and TCP traffic.
- (Optional) If you plan to run synthetic tests that use HTTP, you must also have a security policy rule to allow the GlobalProtect users to access applications over HTTP.

**STEP 4 |** Commit all your changes to Panorama and push the configuration changes to Prisma Access.

- Click **Commit > Commit to Panorama**.
- Click **Commit > Push to Devices** and click **Edit Selections**.
- On the Prisma Access tab, make sure **Prisma Access for users** is selected and then click **OK**.
- Click **Push**.

# Go to Autonomous DEM in Prisma Access

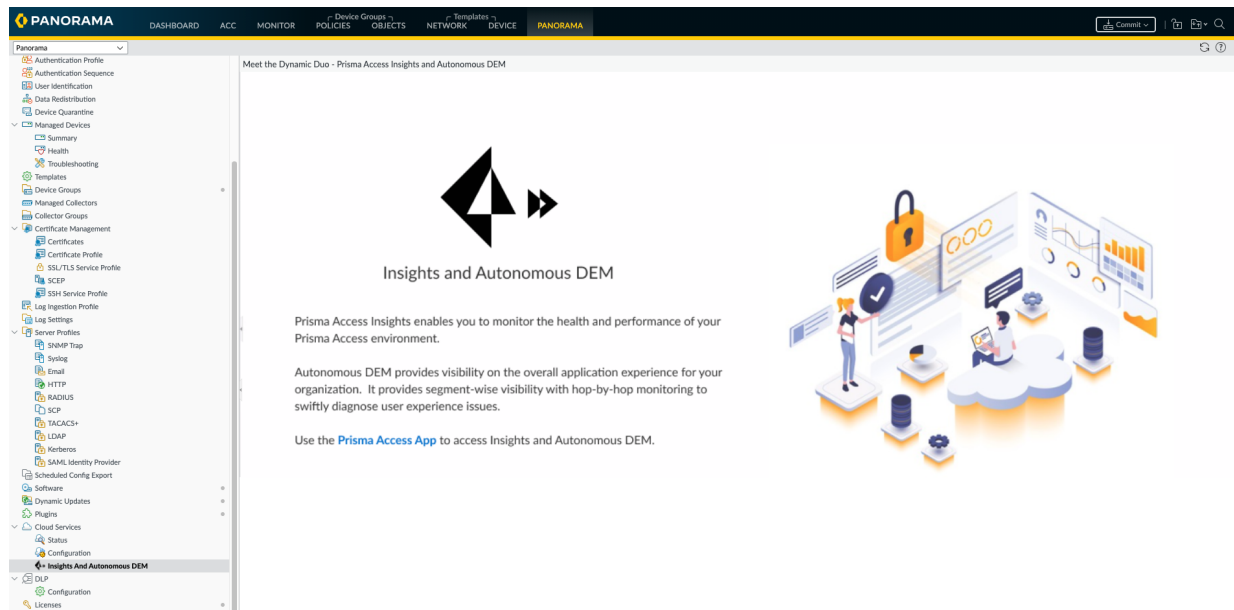
The hub is a single place where you can access the Palo Alto Networks cloud services and apps for your organization. From the [Prisma Access app](#) on the [hub](#), you can select **Autonomous DEM** to monitor the digital experience across your SASE environment and use the metrics to identify users or applications that are experiencing a degradation and pinpoint the cause. To access Autonomous DEM you must have an active Prisma Access for Users license as well as an Autonomous DEM license.

To log in to the hub, and then to Prisma Access:

- To go to Autonomous DEM from the Prisma Access app on the hub:
  1. Use the credentials associated with your Palo Alto Networks support account to log in to the [hub](#).
  2. Launch the Prisma Access app.

- To go to Autonomous DEM from Panorama:

Select **Panorama > Cloud Services > Insights And Autonomous DEM** to launch the Prisma Access app on the hub.



- From the Prisma Access app, select **Autonomous DEM**.

If you have activated your Autonomous DEM license, you will be able start monitoring the digital experience of your SASE users. If you have not yet activated your license, the ADEM functionality will be locked.

**ACCESS**  
BY PALO ALTO NETWORKS

- Insights
- Autonomous DEM
- Summary**
- Applications
- Users
- Prisma Access Locations
- Settings
- Manage
- Logs
- Reports

## Summary

Proactively monitor the digital experience for applications and users across your organization.

Find users, apps, or Prisma Acce:

Experience Trends

Time Range Past 3 hours

Reset Filters

**NEW**

### Meet Autonomous Digital Experience Management

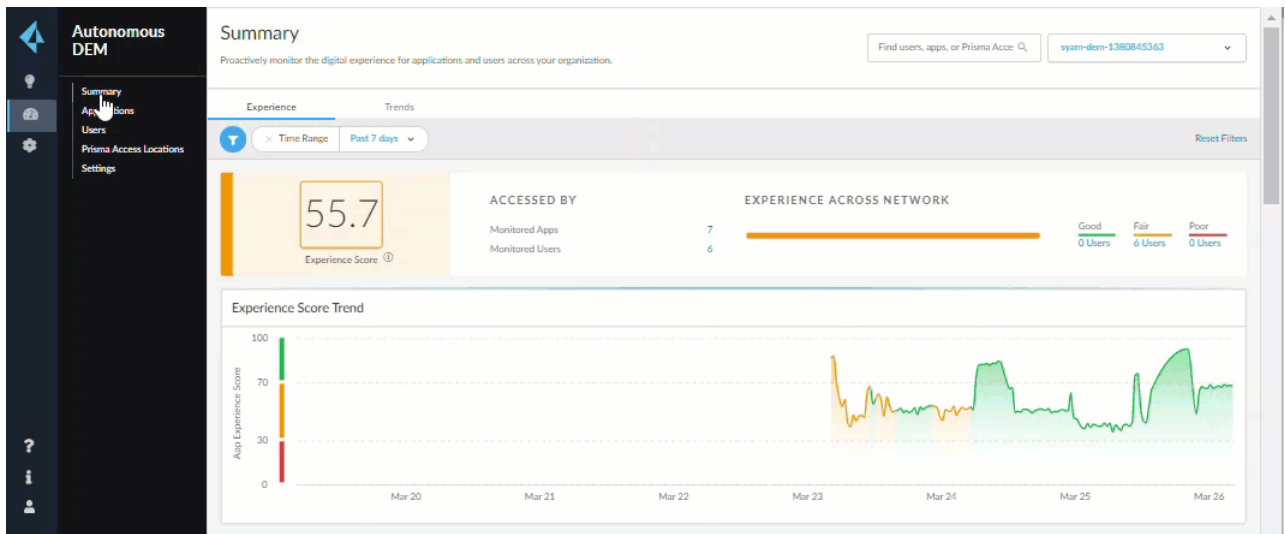
The Summary dashboard provides visibility into overall user and application experience status, trends, maps, and hot spots for your organization. [Learn more](#)

To get started, please contact your Sales Representative.

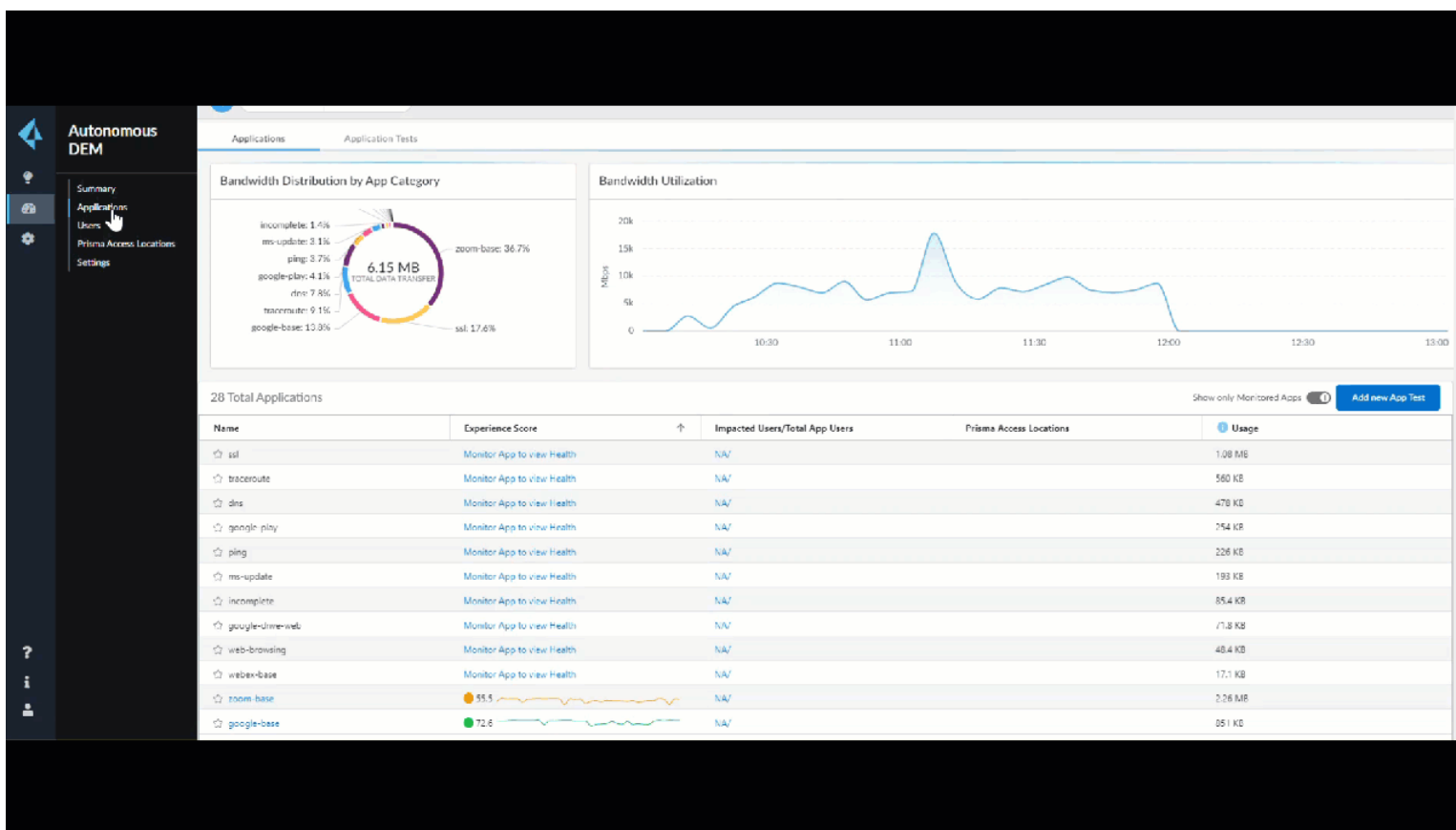
# First Look at Autonomous DEM in Prisma Access

Autonomous DEM (ADEM) is a service that provides native, end-to-end visibility and insights into the digital experience of your Secure Access Service Edge (SASE) users.

- From the **Autonomous DEM > Summary**, you can quickly assess whether there are any system-wide or network-wide issues you should be looking into.

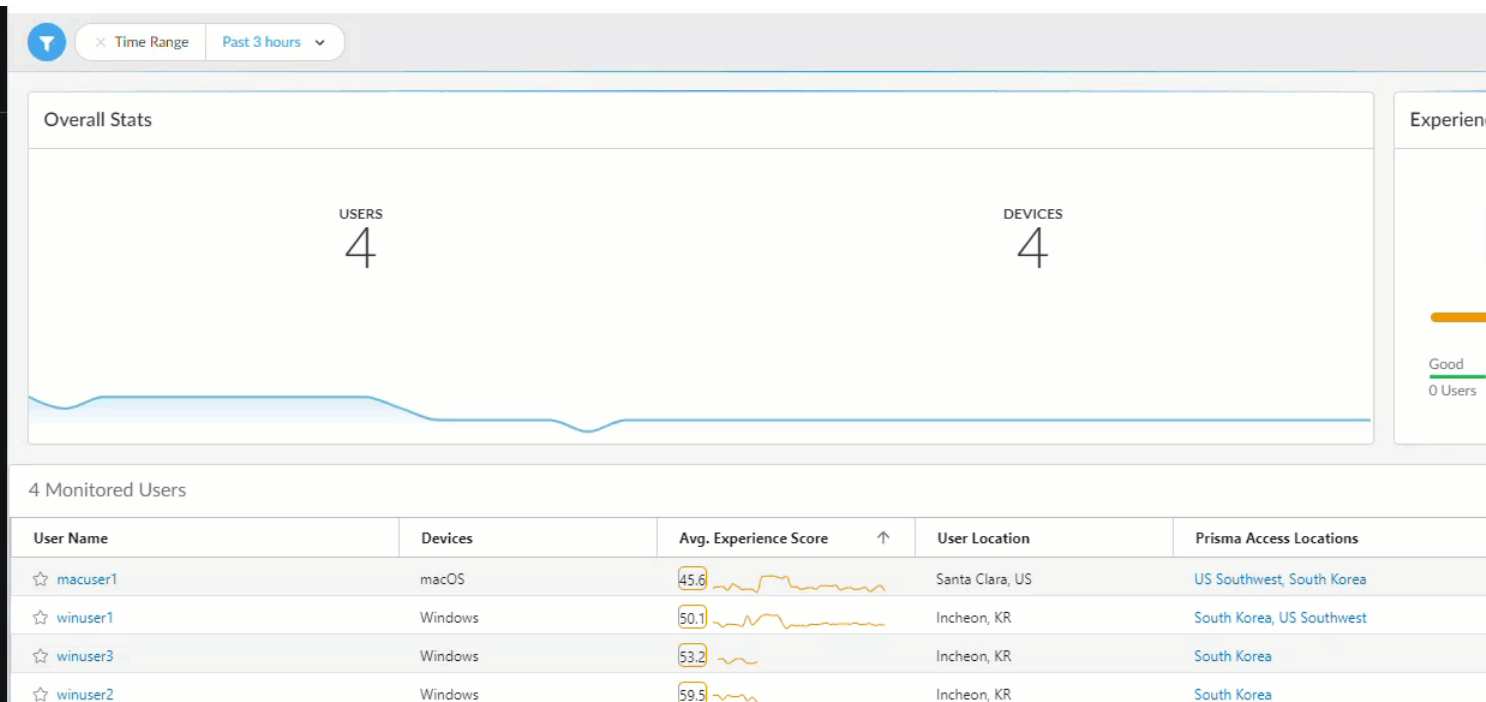


- The first thing to look at is the *Experience score*, which is a weighted average of end-to-end application performance metrics for all monitored applications across all users. A fair or poor experience score lets you know right away that there are performance issues impacting a large number of your users. However, because the experience score is weighted, it may not uncover performance issues in monitored apps or locations that have a smaller number of users.
  - Get a sense of the distribution of app performance across all monitored apps and users, and drill-down into any apps that are performing poorly to begin to pinpoint where the issue is.
  - View the network-wide score trend, and pinpoint when the digital experience began to degrade
  - Identify what segment of the network might be causing issues within your organization from the endpoints all the way to the applications.
  - See which area of the network might be causing experience issues for your users and quickly see if there are system-wide or network-wide issues you should be looking into.
- ADEM also lets you quickly troubleshoot scenarios where your users are reporting issues with specific applications. Use **Autonomous DEM > Applications** to quickly isolate and identify application-specific performance issues.



- Survey all applications running across your organization.
- For applications for which you're running **app tests**, you can see the Experience Score of each individual application, as well as the number of users for each application, and where the application is being used.
- Drill down into an application to see detailed information about the application your users are complaining about.
- Here you can see how many users are accessing the application, and view the performance trend to see when the experience started to decline.
- For impacted users, you can also see which segment of the network is causing the issue, whether it is the users' local WiFi network, the ISP or WAN, or the application itself.
- Finally, ADEM also helps you resolve performance issues reported by a specific user starting from **Autonomous DEM > Users**.

From here you get an overall view of the experiences and the experience trend for all your ADEM users, as well a per-user view of the digital experience across your SASE environment. From here, you can drill down into details for the specific user who is reporting performance issues.



- Immediately when you drill down, alerts at the top of the page highlight any experience issues the specific user is having, such as low device memory or high CPU usage.
- The experience score will also give you an indication of the overall digital experience for the user.
- The user's application experience trend chart shows when the experience score began to decline for this user, and also shows any significant events that could have been a catalyst for the decline, such as an OS upgrade or a GP app upgrade that may have caused high CPU usage or low available memory on the user's device.
- Finally, you can also see which segment of the network—device, local LAN or Wi-Fi network, ISP or WAN, Mobile User gateway, or the application itself—might be the cause of the issue.

# Set up an Autonomous DEM Application Test

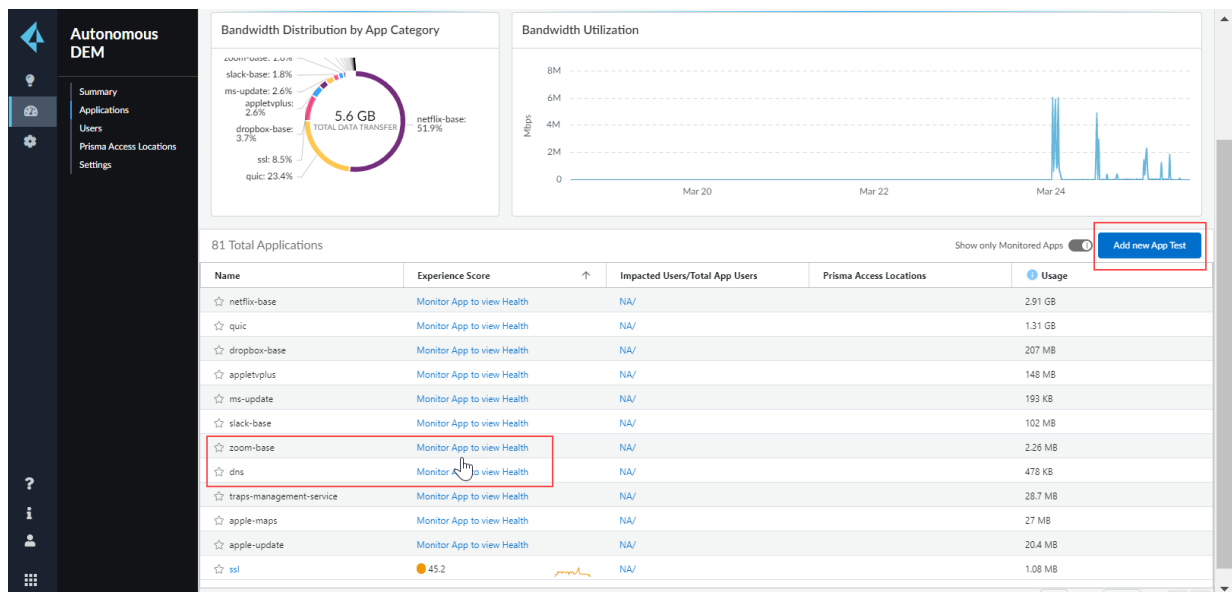
After you've [surveyed the applications running on your network](#) and determined which applications you want to monitor, you can create an [app tests](#). As you create app tests, keep in mind that although you can create app tests targeted to multiple users, the number of tests is based on the number of app tests each individual user runs (for example, if you an app test for Slack and target it to 1000 users, this would count against your license as 1000 tests).

In order to run synthetic tests—to SaaS applications or applications in your data center through Prisma Access or via split tunneling—the endpoint must be connected to the VPN. In addition, you must have security policy rules that allow the synthetic test traffic over ICMP, TCP, HTTPS, and optionally HTTP (depending on how you configure your app tests).

To create an app test:

**STEP 1 |** From the Prisma Access app on the hub, select **Autonomous DEM > Applications**.

**STEP 2 |** Click **Add new App Test** or, click the **Monitor App** link to view the Health link that corresponds to a specific application in the application list.



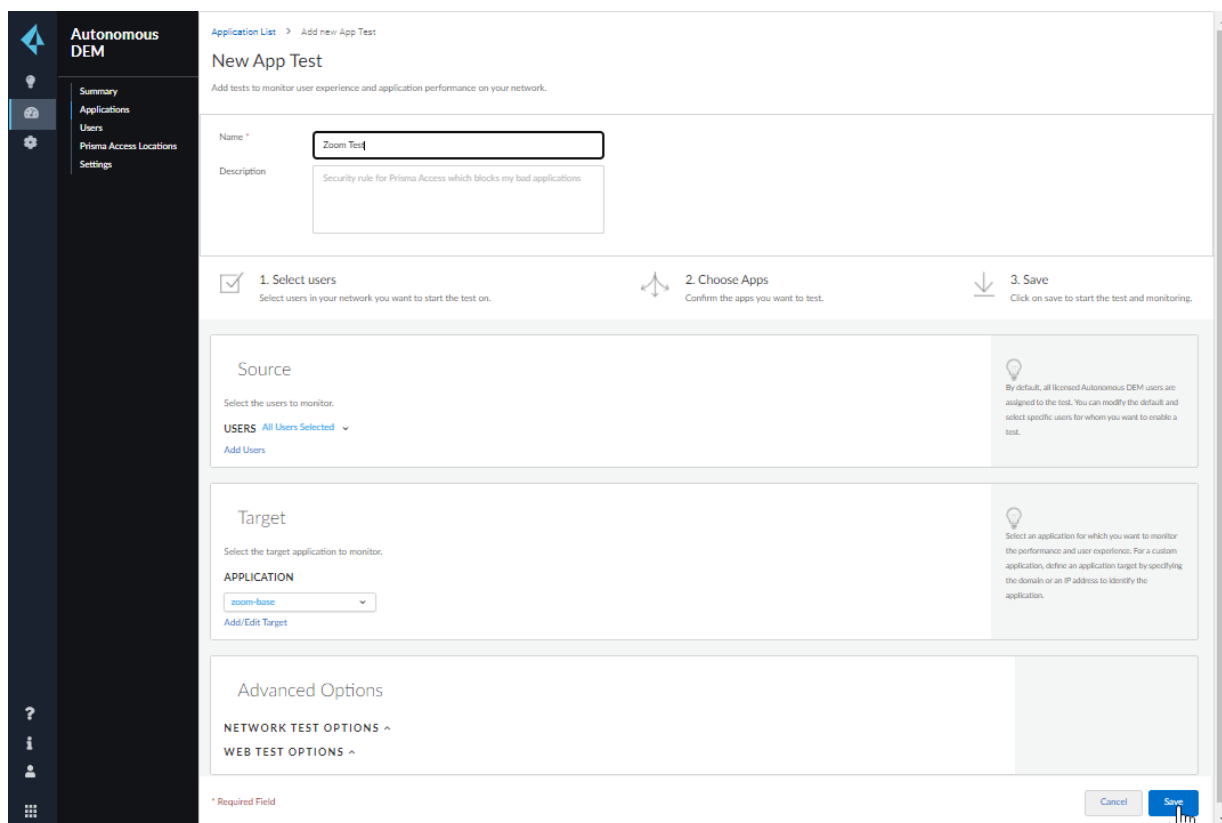
**STEP 3 |** Name the new app test.

**STEP 4 |** Define the Source Users that you want to run this app test. By default, all licensed ADEM users are assigned to run the test. If you want to limit this app test to specific users, **Add Users** and then select the users you want to run the test.

**STEP 5 |** Identify the application you want to test as the Target. If you selected an application from the applications list, the application name is automatically populated. Otherwise, begin typing the **Application** name to see a list of applications from which to select.



*If you don't see the application you want to create a test for, you can create a custom test by entering the associated domain name or IP address.*



#### STEP 6 | (Optional) Define **Advanced Options** as needed.

By default ADEM sets the **Network Test Options** and **Web Test Options** based on the applications you selected. However, you can customize these options if needed in your environment.

#### STEP 7 | **Save** the app test.

The next time the selected users connect to Prisma Access they will receive the new app test settings and begin running the tests. After the app tests start running, the ADEM service collects sample data from all assigned users every five minutes.



# Manage Autonomous DEM Users

After you purchase and activate your Autonomous DEM (ADEM) license for your Prisma Access users, you can enable ADEM for specific Prisma Access users and assign app tests to them. Use the following steps to begin monitoring your users' digital experiences with ADEM:

## STEP 1 | Enable ADEM for your Prisma Access users.

ADEM is supported for your Prisma Access mobile users with Windows or MacOS endpoints running GlobalProtect version 5.2.6 or later.

The steps for enabling ADEM for your users depends on if you are using [Panorama Managed Prisma Accessor](#) [Cloud Managed Prisma Access](#). After you enable ADEM for a user, the ADEM configuration will be pushed to the GlobalProtect app the next time the user connects and the app will register with the ADEM service.

## STEP 2 | To see all registered ADEM users, from the Prisma Access app on the hub select **Autonomous DEM > Settings > Endpoint Agent Management**.

This tab shows all registered ADEM users and indicates whether the user is online (the user device is sending keep-alive messages to the ADEM service) or offline (the ADEM service has not received a keep-alive message from the user device in the last then minutes), when the user device was last seen, the username, device type, and hostname of the ADEM user, and what ADEM agent version they are running.

User	Device	Hostname	Last Seen	First Seen	User Status	Monitoring State	Endpoint Agent Version	Action
<input type="checkbox"/> winuser1	Windows	DFWWIN014FSDF	Less than a minute ago	1 days ago	Online	Enabled	2.0.11	
<input type="checkbox"/> winuser2	Windows	WIN10-SABBAS	2 hours ago	1 days ago	Offline	Enabled	2.0.8	
<input type="checkbox"/> macuser1	macOS	gpqa's MacBook ...	5 mins ago	12 hours ago	Online	Enabled	2.0.11	
<input type="checkbox"/> winuser3	Windows	AUTO-WIN10	2 hours ago	12 hours ago	Offline	Enabled	2.0.8	

## STEP 3 | Assign app tests to your registered ADEM users.

When you [create a new app test](#), you can assign it to all registered ADEM users (default) or choose specific users to assign a test to. If you have already created a test to be assigned to all registered ADEM users, any tests will automatically start running on an endpoint as soon as it registers with ADEM. Once a test is started on an endpoint, it will send metrics from the app test to the ADEM service every five minutes.

## STEP 4 | To temporarily stop an endpoint from running assigned app tests, select the user for whom you want to suspend app tests and toggle the **Monitoring State**.

---

Note that if you disable monitoring, the user is still counted as a licensed ADEM user.

**STEP 5** | To unregister an endpoint from ADEM, select the user(s) to remove and then click the trash can icon in the **Action** column.

Unregistering a user frees up an ADEM license.

**STEP 6** | To set the upgrade preferences for selected users, click **Upgrade Now** or **Auto Upgrade** from the **Upgrade Options** menu.

# Known Issues—Autonomous DEM

These are the issues we're currently working on.

ID	Description
CYR-17136	<p>If only one custom application is defined on Prisma Access, the custom application does not display on Autonomous DEM for setting up a synthetic test. This is not an issue for well-known applications.</p> <p><b>Workaround:</b> Define at least two custom applications on Prisma Access, to configure synthetic test for custom application performance monitoring on Autonomous DEM.</p>
DEM-105	<p>Autonomous DEM does not run network performance tests to the service connection, and hence the network performance metrics are not measured for service connections. The service connection is included when tracing the network path from the endpoint to the application.</p>
DEM-137	<p>The license usage count that displays on <b>Settings &gt; License Details</b> displays the number of unique endpoints that are connected to the Autonomous DEM service, instead of unique users. The license count is incremented based on number of endpoint agents connected.</p>
DEM-183	<p>When you install GlobalProtect app 5.2.6 on macOS devices, the pop-up prompt appears, prompting end users for administrative privileges to modify system settings.</p> <p><b>Workaround:</b> Select <b>OK</b> so that the pop-up prompt does not appear again.</p>
DEM-191	<p>Synthetic tests from Prisma Access location vantage points are performed on all Prisma Access locations within a given region, even if you have not deployed the infrastructure to that specific location. You may see additional locations on the <b>Prisma Access Locations</b> page.</p>
DEM-198	<p><b>Prisma Access Locations &gt; Topology View</b> does not visually identify the hop details.</p>
DEM-238	<p>If you have enabled SSL Decryption on Prisma Access, the endpoint agent cannot register to the Autonomous DEM portal successfully. To enable the endpoint agent to successfully connect and communicate with the ADEM portal, you must add the FDQN to an allow list. Note that the allow list is required only for endpoint agent and ADEM connectivity and is not required for synthetic tests; synthetic tests comply with the SSL Decryption policy.</p> <p><b>Workaround:</b> You must add a policy rule with no decrypt for the DEM Portal FQDNs listed below so that the endpoint agent can register with the portal.</p> <ul style="list-style-type: none"><li>• agents.dem.prismaaccess.com</li><li>• agents.jp1.ap-northeast-1.dem.prismaaccess.com</li><li>• agents.sg1.ap-southeast-1.dem.prismaaccess.com</li><li>• agents.au1.ap-southeast-2.dem.prismaaccess.com</li><li>• agents.ca1.ca-central-1.dem.prismaaccess.com</li><li>• agents.eu1.eu-central-1.dem.prismaaccess.com</li><li>• agents.uk1.eu-west-2.dem.prismaaccess.com</li><li>• agents.us1.us-east-2.dem.prismaaccess.com</li></ul>

---

ID	Description
DEM-242	<p>The synthetic tests may not run for application performance monitoring from Windows endpoints if SSL Decryption is enabled on Prisma Access.</p> <p><b>Workaround:</b> Enable <b>Ignore SSL warnings and errors</b> on <b>Applications &gt; New App Test &gt; Advanced Options &gt; Web Test Options</b>, for synthetic tests.</p>
DEM-253	<p>For applications that are being split tunneled, the synthetic test does not perform a trace path to display a hop-by-hop detailed topology on the <b>User &gt; User Details</b> page for the specific application. The telemetry from the application and network performance tests are collected and available on Autonomous DEM.</p>
GPC-13015	<p>Autonomous DEM is not supported with Config Selection Criteria for device checks in the GlobalProtect portal configuration.</p> <p><b>Workaround:</b> Do not use a certificate profile for <b>Device Selection Criteria</b> in your GlobalProtect portal configuration, to use Autonomous DEM for user experience and application performance monitoring.</p>