Prisma Access Administrator’s Guide
# Table of Contents

## Prisma Access Overview

- Prisma Access Overview
- Prisma Access
- Prisma Access Infrastructure Management
- Manage the Update Cadence and Check the Status of Prisma Access
- Manage Upgrade Options for the GlobalProtect App
- Prisma Access Licensing
- Retrieve the IP Addresses for Prisma Access
- Infrastructure IP Address Overview
- Retrieve the Infrastructure IP Addresses Overview
- Retrieve Public IP Addresses Used by Mobile User Deployments
- Retrieve Public and Loopback IP Addresses
- Plan for IP Address Changes for Mobile Users, Remote Networks, and Service Connections
- How to Calculate Remote Network Bandwidth

## License and Install the Prisma Access Components

- Activate and Install Prisma Access
- Transfer or Update Prisma Access Licenses
  - Supported Update Paths
  - Update Your Prisma Access License from Evaluation to Production
  - Transfer or Update Prisma Access Licenses Between Panorama Appliances
- Configure Panorama Appliances in High Availability for Prisma Access
- HA Prerequisites
- Configure HA

## Prepare the Prisma Access Infrastructure and Service Connections

- 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
  - Verify Service Connection Status
  - Verify Service Connection BGP Status
- Create a Service Connection to Enable Access between Mobile Users and Remote Networks
- How BGP Advertises Mobile User IP Address Pools for Service Connections and Remote Network Connections
- Use Traffic Forwarding Rules with Service Connections
  - Traffic Forwarding Rules with Service Connections Overview
  - Zone Mapping and Security Policies for Forwarded Traffic
  - Requirements to Forward Traffic to Service Connections
  - Create a Service Connection to Use with Traffic Forwarding Rules
  - Create Traffic Forwarding Rules for the Service Connection
- List of Prisma Access Locations
- List of Locations
- List of Locations by Region
# TABLE OF CONTENTS

**Secure Mobile Users with Prisma Access**................................. 103
- Plan To Deploy Prisma Access for Users............................................................. 105
- Configure Prisma Access for Users......................................................................... 107
- Zone Mapping........................................................................................................... 122
- Specify IP Address Pools for Mobile Users............................................................ 123
- How the GlobalProtect App Selects a Prisma Access Gateway............................... 124
- Quick Configs for Mobile User Deployments.......................................................... 125
- Prisma Access with On-Premise Gateways.............................................................. 125
- Manage Priorities for Prisma Access and On-Premise Gateways............................... 127
- Report Website Access Issues................................................................................ 137

**Use Remote Networks to Secure Branches**................................. 139
- Plan to Deploy Prisma Access for Networks......................................................... 141
- Configure Prisma Access for Networks.................................................................. 143
  - Verify Remote Network Connection Status....................................................... 152
  - Verify Remote Connection BGP Status.............................................................. 155
- Quick Configs for Remote Network Deployments.................................................... 157
  - Remote Network Locations with Overlapping Subnets...................................... 157
  - Remote Network Locations with WAN Link..................................................... 158
  - Use Predefined IPSec Templates to Onboard Service and Remote Network Connections................................................................................................................................. 160
- Onboard Remote Networks with Configuration Import............................................ 166
- Configure Quality of Service in Prisma Access...................................................... 169

**Configure User-ID and User-Based Policies with Prisma Access**......179
- Configure User-ID in Prisma Access........................................................................ 181
- Configure User-ID for Remote Network Deployments.............................................. 182
  - Configure User-ID for Prisma Access Using the PAN-OS Integrated User-ID Agent........................................................................................................................................... 183
- Retrieve User-ID Information.................................................................................... 187
  - Retrieve Group Mappings Using a Master Device.............................................. 187
  - Implement User-ID in Security Policies For a Standalone Prisma Access Deployment................................................................................................................................. 191
- Redistribute User-ID Information Between Prisma Access and On-Premise Firewalls......192
  - Redistribute User-ID Information From Prisma Access to an On-Premise Firewall................................................................................................................................. 192
- Redistribute User-ID Information From an On-Premise Firewall to Prisma Access........................................................................................................................................... 194

**Manage Multiple Tenants in Prisma Access**................................. 197
- Multitenancy Overview............................................................................................ 199
- Multitenancy Configuration Overview...................................................................... 200
- Plan Your Multitenant Deployment.......................................................................... 203
- Enable Multitenancy and Migrate the First Tenant.................................................... 204
- Add Tenants to Prisma Access.................................................................................. 211
- Delete a Tenant.......................................................................................................... 215
- Create a Tenant-Level Administrative User............................................................. 216
- Control Role-Based Access for Tenant-Level Administrative Users........................ 218
  - Remove Plugin Access for a Tenant-Level Administrative User......................... 219
- Sort Logs by Device Group ID for External Logging................................................ 223
Create and Configure the Clean Pipe Service .......................... 227

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clean Pipe Overview</td>
<td>229</td>
</tr>
<tr>
<td>Clean Pipe Use Cases</td>
<td>229</td>
</tr>
<tr>
<td>Clean Pipe Examples</td>
<td>229</td>
</tr>
<tr>
<td>Clean Pipe and Partner Interconnect Requirements</td>
<td>230</td>
</tr>
<tr>
<td>Configure the Clean Pipe Service</td>
<td>232</td>
</tr>
<tr>
<td>Enable Multitenancy and Create a Tenant</td>
<td>232</td>
</tr>
<tr>
<td>Complete the Clean Pipe Configuration</td>
<td>236</td>
</tr>
<tr>
<td>Migrate Existing Tenants to the Clean Pipe Service</td>
<td>240</td>
</tr>
</tbody>
</table>
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
- Manage the Update Cadence and Check the Status of Prisma Access
- Manage Upgrade Options for the GlobalProtect App
- Prisma Access Licensing
- Retrieve the IP Addresses for Prisma Access
- Plan for IP Address Changes for Mobile Users, Remote Networks, and Service Connections
- How to Calculate Remote Network Bandwidth
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 (formerly GlobalProtect Cloud Service) 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**—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.

- **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 Manage the Update Cadence and Check the Status of Prisma Access.

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-premise security**—You provide the on-premise security between micro-segmentations of your on-premise 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-premise 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-premise 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.
- **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.
Manage the Update Cadence and Check the Status of Prisma Access

The following table describes how Prisma Access updates its infrastructure components, including content updates, software updates, and plugin updates. The table also notes whether Prisma Access automatically updates the software and how to apply infrastructure updates if they are not automatic.

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.

<table>
<thead>
<tr>
<th>Component</th>
<th>Update Schedule</th>
<th>Cloud Controlled? (Yes/No)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>GlobalProtect app</td>
<td>• Major GlobalProtect App Releases (for example, x.0 or 4.x)—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. For example, given an agent release of 4.0, Prisma Access updates the agent on the portal 7-10 days after the release of 4.0.1. • Minor GlobalProtect App Releases (for example, 4.1.x)—Prisma Access updates the agent on the portal with the latest minor release 7-10 days after the general availability of that release.</td>
<td>Yes</td>
<td>The cloud controls the version of the app that is available for upgrade; you control how and when to roll out the update to the end users. See Manage Upgrade Options for the GlobalProtect App for details.</td>
</tr>
<tr>
<td>Plugin version</td>
<td>Available after the plugin release.</td>
<td>No</td>
<td>You perform the tasks to upgrade the plugin. See Upgrade the Cloud Services Plugin to upgrade the plugin in the Panorama appliance.</td>
</tr>
<tr>
<td>PAN-OS software upgrades in Prisma Access</td>
<td>We upgrade the PAN-OS infrastructure at the same time we release a new version of Prisma Access. We provide you with</td>
<td>Yes</td>
<td>Register for email or text notifications for infrastructure upgrades at the https://</td>
</tr>
<tr>
<td>Component</td>
<td>Update Schedule</td>
<td>Cloud Controlled? (Yes/No)</td>
<td>Comments</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------</td>
<td>-----------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>infrastructure—scheduled</td>
<td>three weeks' notice before a scheduled upgrade.</td>
<td>Yes</td>
<td>status.paloaltonetworks.com/website.</td>
</tr>
<tr>
<td>PAN-OS upgrades in Prisma Access infrastructure—unscheduled</td>
<td>For unscheduled upgrades (for example, an emergency hotfix for zero-day threats), we make every effort to give you 48 hours' notice before an upgrade; however, Prisma Access must occasionally upgrade its infrastructure with a shorter notice time.</td>
<td>Yes</td>
<td>Register for email or text notifications for infrastructure upgrades at the <a href="https://status.paloaltonetworks.com/website">https://status.paloaltonetworks.com/website</a>.</td>
</tr>
<tr>
<td>Panorama version to use with the Cloud Services Plugin</td>
<td>None</td>
<td>No</td>
<td>See Upgrade the Cloud Services Plugin for the supported Panorama versions to use with Prisma Access. To upgrade your Panorama to a new version, see Install Content and Software_Updates for Panorama.</td>
</tr>
<tr>
<td>Applications and threat updates</td>
<td>Daily with a threshold of 24 hours. 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 New App-ID filter to minimize this possible traffic impact.</td>
<td>Yes</td>
<td>We will provide an update via the status.paloaltonetworks.com page 48 hours prior to a cloud upgrade, and 24 hours prior to release of new App-ID version.</td>
</tr>
<tr>
<td>Antivirus protection</td>
<td>Every hour, 10 minutes after the hour</td>
<td>Yes</td>
<td>Prisma Access is always up-to-date with the latest Antivirus release.</td>
</tr>
<tr>
<td>WildFire</td>
<td>Every 5 minutes</td>
<td>Yes</td>
<td>Prisma Access is always up-to-date with the latest WildFire release.</td>
</tr>
<tr>
<td>GlobalProtect Data File</td>
<td>Every hour</td>
<td>Yes</td>
<td>Prisma Access is always up-to-date with the latest GlobalProtect data file release.</td>
</tr>
<tr>
<td>Clientless VPN application signatures</td>
<td>Every hour</td>
<td>Yes</td>
<td>Prisma Access is always up-to-date with the latest Clientless VPN</td>
</tr>
<tr>
<td>Component</td>
<td>Update Schedule</td>
<td>Cloud Controlled? (Yes/No)</td>
<td>Comments</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------</td>
<td>---------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>application signature release.</td>
</tr>
</tbody>
</table>
Manage Upgrade Options for the GlobalProtect App

Prisma Access manages the GlobalProtect app version that Mac OS and Windows users in your organization can download from the Prisma Access portal.

You cannot control the version of the app that is available on the Prisma Access portal; however, you can manage mobile users' access to the GlobalProtect app by completing the following task.

**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 end-users can upgrade the GlobalProtect app software and, if they can, whether they can choose when to upgrade:

- **Allow with Prompt** (default)—Prompt users when a new version is activated on the firewall 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.
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**
- **Other Required Licenses**

**Prisma Access Licenses**

The licenses you need for Prisma Access depend on whether you want to use the service to secure your remote networks, your mobile users, or both:

- **Prisma Access for Networks (formerly GlobalProtect Cloud Service for Remote Networks)**—To license Prisma Access for networks you purchase a bandwidth pool, which you can divide among each remote network location that you onboard in increments of 2 Mbps, 5 Mbps, 10 Mbps, 20 Mbps, 25 Mbps, 50 Mbps, 100 Mbps, 150 Mbps, 300 Mbps, 500 Mbps, or 1000 Mbps.

  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. See [How to Calculate Remote Network Bandwidth](#) for more details about the correct bandwidth to specify for your remote network.

  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.

- **Prisma Access for Users (formerly GlobalProtect Cloud Service for Mobile Users)**—You license Prisma Access for mobile users based on number of users, with tiers from 200 users to more than 50,000 users. Prisma Access for mobile users requires the GlobalProtect app on each supported endpoint. 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.

- **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.

**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 version 8.0.5 or later, 8.1.0 or later except 8.1.2, or 9.0.0 or later with a valid support license. When you license the Prisma Access components, you must tie the auth code to a licensed Panorama serial number.

  *While using Panorama 9.0 is supported with Prisma Access, upgrading to Panorama 9.0 does not give you access to 9.0 features in Prisma Access. The Prisma Access*
infrastructure supports PAN-OS features up to release 8.1. See What Features Does Prisma Access Support? for a list of supported features.

- **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.
Retrieve the IP Addresses for Prisma Access

If you are manually whitelisting the IP addresses of your Prisma Access infrastructure or 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 whitelist 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 address to change and to plan for those changes, see Plan for IP Address Changes for Mobile Users, Remote Networks, and Service Connections.

- Infrastructure IP Address Overview
- Retrieve the Infrastructure IP Addresses Overview
- Retrieve Public IP Addresses Used by Mobile User Deployments
- Retrieve Public and Loopback IP Addresses

Infrastructure IP Address Overview

Prisma Access uses two different address types that you need to whitelist:

- A **public IP address** is the source IP address used by Prisma Access for requests made to an internet-based source. Whitelist the public IP address 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.

- A **loopback IP address** is the source IP address used by Prisma Access for requests made to an internal source, and is assigned from the infrastructure subnet. Whitelist the loopback IP address to give Prisma Access access to internal resources such as RADIUS or Active Directory authentication servers.

  We recommend that you whitelist the entire infrastructure subnet, because loopback IP addresses for mobile users can change. To find the infrastructure subnet, select Panorama > Cloud Services > Status > Network Details > Service Infrastructure. The subnet displays in the Infrastructure Subnet area.

Retrieve the Infrastructure IP Addresses Overview

Use one of the following methods to retrieve your IP addresses, based on your what addresses you want to retrieve:

- To be notified about public IP addresses changes for mobile user deployments, complete the task in Retrieve Public IP Addresses Used by Mobile User Deployments.

  This script retrieves all the public and reserved IP addresses required for mobile user deployments; however it does not retrieve remote network, service connection, or clean pipe public or loopback IP addresses.

- To be notified about public IP and loopback IP changes for remote networks, service connections, and clean pipes, complete the task in Retrieve Public and Loopback IP Addresses.
The script described in this section does not retrieve the active and reserved public IP addresses for mobile user deployments that you need to whitelist to be prepared for scaling events, added locations, or infrastructure updates.

Retrieve Public IP Addresses Used by Mobile User Deployments

If you are whitelisting public IP addresses to allow mobile users access to SaaS or public applications, Prisma Access provides two sets of public 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 whitelist this 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. 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.**

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.

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

![API Key Generation](image)

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

![IP Change Event Notification](image)
You can specify an IP address or an FQDN to an HTTP or HTTPS web service that is listening for change notifications. For example: http://mydomain/cgi-bin/test1.py. You do not need to commit your change for the notification URL.

**STEP 3** | Enter one 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.

You should also run the API command every time you add a location to your deployment, to retrieve the active and reserved IP addresses that Prisma Access added for the new location.

### Retrieve Public and Loopback IP Addresses

To be notified of public IP addresses for remote networks and loopback IP address changes for service connections, remote network connections, and mobile users, the Cloud Services plugin enables you to specify a URL at which you can be alerted of a change. In addition, we provide an API script you can run to retrieve these addresses.

*This script does not provide you with the reserved public IP address for mobile user gateways; to retrieve those addresses; instead, use the script to retrieve mobile user public IP addresses.*

If you specify a URL to 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"}
```

```
```

When you receive a notification, you must follow a two-step process. First, you must manually or programatically retrieve the list of public IP or loopback IP addresses. Then, you must update the IP addresses in the appropriate whitelist 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 whitelist the new IP addresses.

**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 Steps 1 and 2 in [Retrieve Public IP Addresses Used by Mobile User Deployments](#) 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:

```plaintext
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:

- **fwType**:
  - `gpcs_gp_gw`—Retrieves Prisma Access gateway IP addresses.
  - `gpcs_gp_portal`—Retrieves Prisma Access portal IP addresses.
  - `gpcs_remote_network`—Retrieves Prisma Access remote network addresses.
  - `gpcs_clean_pipe`—Retrieves Prisma Access Clean Pipe IP addresses.

- **addrType**:
  - `public_ip`—Retrieves Prisma Access public IP addresses.
  - `loopback_ip`—Retrieves Prisma Access loopback IP addresses.
  - `egress_ip_list`—Retrieves Prisma Access remote network edge IP addresses.

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.

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 network firewalls:

```bash
curl -k -H header-api-key:1234y9ydxb__0UmzetVTbC8XTyFMaoT4RBZKBjfx419YVufeFG7 "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:

```python
#!/usr/bin/python
import subprocess
import json

api_key = '1234y9ydxb__0UmzetVTbC8XTyFMaoT4RBZKBjfx419YVufeFG7' # 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 whitelists 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 whitelist the required IP addresses 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 Allocation For Remote Network Connections**
- **Loopback IP Address Allocation for Mobile Users**

**IP Address Allocation For Mobile Users**

When you deploy Prisma Access for the first time, it adds two sets of public IP addresses for each Prisma Access portal and gateway: one set that is in active use and another set that is reserved for future use. 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 whitelist them 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 region.
  
  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 whitelist any added or changed addresses.

**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 IP Addresses Used by Mobile User Deployments that Prisma Access assigned and whitelist them in your network. Prisma Access keeps two sets of IP addresses at all times for all active gateways in each location.

**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.

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. Whitelisting both the active and reserved public IP addresses ensures that users can still access the Prisma Access portals and gateways after an infrastructure upgrade.
IP Address Allocation For Remote Network Connections

The IP addresses for the remote network connections are static, and only change in the following cases:

- When a system administrator creates a new remote network connection using the Panorama appliance.

  Prisma Access adds a **Service IP Address** for the new remote network connection. This is also known as the **public_ip** address if you Retrieve the IP Addresses for Prisma Access using an API or automated script. When you Configure Prisma Access for Networks, you use these IP addresses as the peer IP address to set up the IPSec tunnel between the remote network location and Prisma Access for networks.

  Prisma Access always assigns an entirely new IP address for the new connection; if you delete a remote connection, Prisma Access might use that address for a newly-deployed gateway, but will never use that gateway for a new remote or service connection.

- When a change to network bandwidth in a region causes the total bandwidth to exceed 300 Mbps.

  While you can onboard remote networks in increments of 2 Mbps, 5 Mbps, 10 Mbps, 20 Mbps, 25 Mbps, 50 Mbps, 100 Mbps, 150 Mbps, 300 Mbps, 500 Mbps, or 1000 Mbps, the maximum bandwidth available for a single service IP address is 300 Mbps. If the total bandwidth of all remote network connections in a region is 300 Mbps or less, Prisma Access assigns a single service IP address. If the bandwidth exceeds 300 Mbps, Prisma Access provisions an additional service IP address.

  These guidelines apply only when you upgrade an existing connection. A single remote network connection, even a 500 Mbps or 1000 Mbps connection, always receives a single **Service IP Address**, regardless of its size.

The following example shows three remote network connections in the same region, 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 region.
• 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.

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. To Retrieve the IP Addresses for
Prisma Access using an API command or an automated script, specify an addrType of public_ip and a fwType of gpcs_remote_network.

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 whitelist the entire infrastructure subnet 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 and Loopback 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 192.16.0.3 for mobile users from the infrastructure subnet.

After 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).
How to Calculate Remote Network Bandwidth

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.
License 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 download the Prisma Access and Cortex Data Lake licenses, activate them, and install the components as shown in the following sections.

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

Use the following workflow to license Prisma Access and download and install the Cloud Services plugin:

To set up Prisma Access in High Availability (HA) mode with a primary and secondary Panorama, Configure Panorama Appliances in High Availability for Prisma Access before you license and activate Prisma Access.

STEP 1 | Activate the Prisma Access auth codes for the Prisma Access components you purchased (Prisma Access for Networks, Prisma Access for Users, or Prisma Access for Clean Pipe):

You must activate your Cortex Data Lake auth code before activating the Prisma Access auth codes.

1. Log in to the Customer Support Portal (CSP) and select Assets > Cloud Services > Activate Cloud Services Auth-Code.

2. Enter the Authorization Code you received in the email, select the serial number for the Panorama on which you plan to install the Cloud Services plugin, read the End User License Agreement and Support Agreement and then Agree and Submit.
After you see the registration complete message, close the Cloud Services dialog.

**STEP 2 | Verify the Quantity and Part Description of the Prisma Access licenses you just activated.**

**STEP 3 | Download and install the Cloud Services plugin.**

Prisma Access supports Panorama appliances running version 8.0.5 or later, 8.1.0 or later except 8.1.2, and 9.0.0 or later. The way you download and install the plugin depends on whether you are using Panorama version 8.0.5 or later or 8.1.0 or later (including 9.0.0 or later).

*Upgrading to Panorama 9.0 does not give you access to 9.0 features in Prisma Access. The Prisma Access infrastructure supports PAN-OS features up to release 8.1. See What Features Does GlobalProtect Cloud Service Support? for a list of supported features.*

**On Panorama 8.0.x:**

1. Log in to the Customer Support Portal and select Updates > Software Updates.
2. Find the Cloud Services plugin version 1.4.0 in the Panorama Integration Plug In section and download it to your local system. Any other plugin versions are not supported.
Do not rename the plugin file or you will not be able to install it on Panorama.

3. To install the plugin, log in to the Panorama Web Interface of the Panorama you selected when you licensed Prisma Access, select Panorama > Plugins > Upload and Browse for the plugin File that you downloaded from the CSP.

4. Install the plugin.

**On Panorama 8.1.0 and later:**

On Panorama 8.1.0 or later, you can either download the plugin from the CSP and then upload it to Panorama, or you can check for plugin updates directly from Panorama as follows:

1. Select Panorama > Plugins and click Check Now to display the latest cloud_services plugin updates.

2. Download plugin version 1.4.

   *Any other plugin versions are not supported.*

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 4 | 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 5 | Verify your account. You must be a super user on the Customer Support Portal (CSP) to generate the one-time password required to 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.

2. Click Generate OTP.
3. Select the serial number for the Panorama where you installed the Cloud Services plugin and click **Generate OTP**.
4. Click **Copy to Clipboard**.
5. Go back to Panorama and click **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**.
6. Paste the **One-time Password** you just generated and click **OK**.

![Verify Account Window](image)

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

**STEP 6 |** Apply device group changes in the Prisma Access infrastructure.

After you upgrade to version 1.4 software, Prisma Access adds a third device group, `Service_Conn_Device_Group`, and 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 7** | 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.

*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 Update Your Prisma Access License from Evaluation to Production 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.

![Supported Update Paths Table]

*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.*

Update Your Prisma Access License from Evaluation to Production

Use this workflow to update your Prisma Access plugin from an evaluation to a production version.
Before starting this procedure, make sure that your Panorama appliance has active, paid licenses. If your Panorama has an evaluation license, you need to Transfer or Update Prisma Access Licenses Between Panorama Appliances.

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 evaluation cloud service licenses you have installed.
1. Open a SSH console session to the Panorama appliance.
2. Run 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 (formerly Logging Service), 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> deletelicense key [then click tab]
GlobalProtect_Cloud_Service_f_2017_11_07.key 2017/11/07 12:32:51 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> deletelicensekey Logging_Service_2017_11_07.key
successfully removed Logging_Service_2017_11_07.key
admin-Panorama> deletelicensekey
GlobalProtect_Cloud_Service_f_2017_11_07.key
successfully removed GlobalProtect_Cloud_Service_f_2017_11_07.key
admin-Panorama> deletelicensekey
GlobalProtect_Cloud_Service_for_Remote_Networks_2017_11_07.key
successfully removed GlobalProtect_Cloud_Service_for_Remote_Networks_2017_11_07.key
admin-Panorama> deletelicensekey
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 | Complete the one-time password (OTP) verification procedure and verify the Panorama appliance.

After you generate the OTP, we recommend deleting any existing certificates using CLI from Panorama, then creating the new certificate with the new OTP by entering the following commands, where value is the new OTP:
STEP 6 | 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 a 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](image)

**Activate Licenses**

- [ ] Activate Auth-Code

![Transfer Licenses](image)

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 running software version is 8.0.5 or later, 8.1.0 or later (except 8.1.2), or 9.0.0 or later.

> **You must update your software to these minimum versions for Cortex Data Lake and Prisma Access to work.**
While using Panorama 9.0 is supported with Prisma Access, upgrading to Panorama 9.0 does not give you access to 9.0 features in Prisma Access. The Prisma Access infrastructure supports PAN-OS features up to release 8.1.

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 the firewalls and can use the Panorama appliance to centrally monitor logs. 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 your firewalls.

- 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. 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**, 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 15:14:07.791 -0800 INFO: [hainfo] Data string is primarypanoramasn=<varname>X</varname> &secondarypanoramasn=<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**.

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
- Use Traffic Forwarding Rules with Service Connections
- How BGP Advertises Mobile User IP Address Pools for Service Connections and Remote Network Connections
- List of Prisma Access Locations
Set Up Prima Access

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 | Whitelist the following URLs and ports on any security appliance that you use with the Panorama appliance.

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 whitelist the following URLs and ports on the proxy or proxy server:

- Port 444 (for Cortex Data Lake)
- api.lc.prod.us.cs.paloaltonetworks.com (For Cortex Data Lake)
- api.gpcloudservice.com (for Prisma Access)
- api.paloaltonetworks.com (for Prisma Access)
- apitrusted.paloaltonetworks.com (for Prisma Access)

STEP 2 | Identify your license requirements; then License and Install the Prisma Access Components.

STEP 3 | 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 the cloud service, 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 the 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 on the firewalls deployed in the cloud. For example, any features that require PAN-OS 9.0 are not currently supported. While using Panorama 9.0 is supported with Prisma Access, Prisma Access infrastructure supports PAN-OS features up to release 8.1. See What Features Does Prisma Access Support? for a list of supported features.
STEP 4 | 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 5 | Plan To Deploy Prisma Access for Users and Configure Prisma Access for Users, 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.

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 your changes to get started with the service.
   1. Commit locally on Panorama.
   2. Commit and Push to the cloud service.
   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 the cloud service 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 6 | Plan, create, and configure remote network connections.

1. Add one or more remote networks to the cloud service.

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 7 | Retrieve the IP Addresses for Prisma Access and Retrieve Public IP Addresses Used by Mobile User Deployments.

You whitelist these addresses on your organization's network to limit inbound access to your enterprise network and applications.

STEP 8 | (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-premise authentication server such as RADIUS or Active Directory, whitelist the IP addresses that Prisma Access uses as its source IP address for internal requests (Infrastructure IP Address Overview), or whitelist 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 9 | (Optional)** Forward logs from Cortex Data Lake (formerly Logging Service) to an external Syslog receiver by setting up the Log Forwarding app.
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 does not overlap with other IP addresses you use internally. Prisma Access will use the IP addresses within this subnet to establish a network infrastructure between your remote network locations and mobile users, and service connections to your headquarters and/or data center (if applicable). This will 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). This subnetwork will be an extension to your existing network and therefore cannot overlap with any IP subnets you use within your corporate network, or with the IP address pools you assign for Prisma Access for users.

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

- 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 the 100.64.0.0/15 and 169.254.0.0/16 subnet ranges because Prisma Access reserves those subnets for its internal use.
- The subnet you specify cannot overlap with any subnets you use in your corporate network, or with the IP address pools you plan to use for your Prisma Access for mobile users IP address pools.
- Because the service infrastructure can be very large, you must designate a /24 subnetwork.

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-premise 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.
Your Prisma Access license includes the option to establish service connections to up to 100 of your headquarters and/or data center sites. The first three service connections are included with no license cost; each connection after the third uses 300 Mbps from your licensed remote networks bandwidth pool. Prisma Access does not limit the bandwidth over these connections.

*If you configure Prisma Access to manage multiple tenants, the maximum number of licensed service connections does not increase; you can still configure a maximum of three service connections per license, and each additional service connection uses 300 Mbps from your licensed bandwidth pool.*

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 and Prisma Access does not limit the bandwidth over this connection.
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 remote networks, mobile users and the firewalls in the cloud, 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). This subnetwork will be an extension to your existing network and therefore cannot overlap with any IP subnets you use within your corporate network, or with the IP address pools you assign for Prisma Access for users.

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

**STEP 2 |** On the General tab, an Infrastructure Subnet, for example, 172.16.55.0/24. 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. See Plan the Service Infrastructure and Service Connections for additional recommendations and requirements for this 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 (formerly Logging Service).**

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 Prisma Access.

The Cloud Services plugin automatically adds the following Log Settings (Device > Log Settings) after a new installation or upgrade:

- Log Settings for System logs (system-prisma-access-default), User-ID logs (userid-prisma-access-default), and HIP Match logs (hipmatch-prisma-access-default) are added to the Mobile_User_Template.
- Log Settings for System logs (system-prisma-access-default) and User-ID logs (userid-prisma-access-default) are added to the Remote_Network_Template.
- Log Settings for System logs (system-prisma-access-default) are added to the Service_Conn_Template.

You can use these log setting configurations to automatically forward System, User-ID, and HIP Match logs to Cortex Data Lake. If you are upgrading and have already configured Log Settings, you can disable these by deselecting the check box next to the profile (you cannot delete them).

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) Use traffic forwarding rules to redirect mobile user and remote network internet traffic to service connections by clicking the Traffic Forwarding tab.

Traffic forwarding allows you to redirect mobile user or remote network traffic through a service connection to a security stack for further processing before being sent to the internet. See Use Traffic Forwarding Rules with Service Connections for more information and for configuration details.

STEP 8 | Click OK to save the Service Setup settings.

STEP 9 | 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**.

**Warning:**

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 10** | 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**.

   ![Cortex Data Lake status](image)

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

**STEP 11** | 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 Setup.

STEP 2 | In the Onboarding section, 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.
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** | 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.
To configure BGP:

1. On the BGP tab, select Enable.

2. (Optional) To prevent the BGP peer on the Prisma Access firewall from forwarding routes into your data center/HQ network, select Don't export 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 the Prisma Access does not send BGP advertisements if you select this option, you must configure static routes on the on-premise equipment to establish routes back to Prisma Access.

3. 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.

4. 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.

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 remote network.

6. (Optional) Enter and confirm a Secret passphrase to authenticate BGP peer communications.
STEP 7 | 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-premise device, or both PAN-OS-marked and on-premise-marked traffic. See **Configure Quality of Service in Prisma Access** for details.
STEP 8 | 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 remote network 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.

STEP 9 | 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 select Edit Selections. On the **Prisma Access** tab, make sure **Service setup** is selected, then click **OK** and **Push**.

   Prisma Access should automatically select the components that need to be committed.
STEP 10 | Add more service connections by repeating Step 2 through Step 9.

The first three service connections are included with no license cost; each connection after the third uses 300 Mbps from your licensed remote networks bandwidth pool. After you **Add** your fourth and subsequent network connection, Prisma Access displays a page informing you of your remaining licensed remote networks bandwidth. To confirm your addition, **Allocate 300 Mbps for an additional service connection**; then **Allocate** the bandwidth for the service connection.
STEP 11 | 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 Prisma Access.

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.

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.

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

**Status** tab:
- **Region**—The region where your cloud service infrastructure is deployed for the service connection.
- **Remote Peer**—The corporate location to which this cloud service infrastructure is setting up an IPSec tunnel.
- **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/ headquarter location and the Prisma Access firewall 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 the Prisma Access 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.
- **Tunnel Status**—The operational status of the connection between Prisma Access and your service connection.

**Statistics** tab:
- **Region**—The region where your cloud service infrastructure is deployed for the service connection.
- **Remote Peer**—The corporate location to which this cloud service infrastructure is setting up an IPSec tunnel.
- **Ingress Bandwidth (Mbps)**—The bandwidth from the HQ/data center location to Prisma Access.

  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.
- **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**.

![BGP Status Dialog](image)

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 `bgpAfiIpv4-unicast Counters` area, in the **Incoming Total** and **Outgoing Total** fields.

![BGP Status](image)

- **RIB In**—Routing information that has been received from different peers and is stored in the Routing Information Base (RIB).

![RIB In](image)

- **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 remote 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.
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 Configure Prisma Access for Users, 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.
Use Traffic Forwarding Rules with Service Connections

Prisma Access allows you to create traffic forwarding rules that use policy-based forwarding (PBF) to redirect mobile user and remote network internet traffic to service connections, instead of egressing directly from a remote network connection or mobile user location.

You can create traffic forwarding rules based on source or destination IP addresses or FQDNs. You can also specify URLs, or add a custom URL object, for destination traffic.

Traffic forwarding is not supported with multi-tenant deployments.

- Traffic Forwarding Rules with Service Connections Overview
- Zone Mapping and Security Policies for Forwarded Traffic
- Requirements to Forward Traffic to Service Connections
- Create a Service Connection to Use with Traffic Forwarding Rules
- Create Traffic Forwarding Rules for the Service Connection

Traffic Forwarding Rules with Service Connections Overview

In standard Prisma Access deployments, a service connection provides access to internal network resources, such as authentication services in your headquarters or data center. Since service connections process internal traffic, no internet access is required. Prisma Access expands the scope of service connections that allows you to redirect mobile user or remote network traffic to a third-party security stack for further processing before being sent to the internet.

You can use traffic forwarding rules with service connections with mobile user deployments, remote network deployments, or a combination of both.

The following examples show two types of traffic forwarding deployments.

- The following figure provides an example of a security stack that is deployed from the cloud, and you want to have traffic sent to the example.com website to be directed to this security stack. This stack is located outside of your organization’s internal network; for this reason, you don’t want this service connection to process any internal network traffic.

  To enable this deployment, you create a service connection with a traffic forwarding rule in Panorama that forwards traffic to the example.com website to a service connection you created for this purpose. To configure this service connection to only process forwarded traffic and prevent internal network traffic from using this service connection, select the Dedicated for PBF Only check box when you set up traffic forwarding rules.

  The service connection sends traffic to the security stack, which performs additional processing on the traffic before sending it to the internet. All other internet-directed traffic egresses normally from the mobile user location or remote network connection.

Selecting the Dedicated for PBF Only check box causes Prisma Access to change the zone for the service connections used in this rule from Trust to Untrust, because this location is not part of your organization’s network. Make sure that you check zone.
mapping and security policies for remote networks and mobile users and modify them as required to accommodate this change.

- The following figure provides an example of a security stack being deployed in your organization’s network. In this case, it is an on-premise stack located at your organization’s headquarters. You can use this service connection for internal traffic as well as redirected traffic.

To enable this deployment, you create a service connection with a traffic forwarding rule in Panorama, but deselect the Dedicated for PBF Only check box when you set up traffic forwarding, and configure the security stack to forward traffic to the internet after processing. With this deployment, the zone does not change from Trust, and you would also set the traffic going to example.com in the Trust zone.

Zone Mapping and Security Policies for Forwarded Traffic

If you redirect traffic using a service connection to a security stack that is outside your internal network, the zones for the service connections that are used for the redirection change from Trust to Untrust. If you deploy your security stack as a part of your internal network, zones do not change from Trust. Because you use the service connection to egress internet traffic, you might need to make changes to your zone mapping or security policies. Since you cannot create zones or configure zone mapping for service connections, you make these changes to the mobile users and device groups instead. Complete the following steps to configure zone mapping for traffic forwarding.
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.**

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.

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.

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.
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**.

![Zone Mapping](image)

**Requirements to Forward Traffic to Service Connections**

If you are forwarding traffic from remote network or mobile user traffic to service connections, make sure that your network environment has the following infrastructure requirements:

- Prisma Access must be able to connect to the IPSec-capable device (such as a router or SD-WAN device) that your organization uses to terminate the service connection. 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 or both when you create a service connection. If you use static routing, specify the public IP address used by the organization's IPSec-capable device as the **Peer Address** when you create an IKE gateway.

- 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.

Also note the following limits for traffic forwarding rules:

- You can configure a maximum of 500 wild card (*.example.com) URLs.
  - This number includes both manually entered URLs and URLs that are entered in a custom URL category.
- You can configure a maximum of 100 traffic forwarding rules.

**Create a Service Connection to Use with Traffic Forwarding Rules**

To use traffic forwarding rules with Prisma Access service connections, you first onboard your mobile users and remote networks. You then provide connectivity for the service connection between Prisma Access and the IPSec-capable device on the other side of the service connection.

**STEP 1 |** **Onboard your mobile users and remote networks,** as applicable for your deployment.

You can deploy with mobile user deployments, remote network deployments, or a combination of both.

Prisma Access provides you with predefined IPSec templates for some common IPSec and SD-WAN devices. If the IPSec-capable device that terminates the service connection’s IPSec tunnel is in that list, you can use those predefined templates for that device, which simplifies IPSec tunnel creation; otherwise, create new IKE and IPSec cryptographic profiles as described in this task.

**STEP 2 |** Create IKE and IPSec crypto profiles and an IKE gateway for the service connection.
You will use these profiles to provide connectivity between Prisma Access and the IPSec-capable device on the other side of the service connection.

1. Select Network > Network Profiles > IKE Crypto > Add and Add an IKE crypto profile for the IPSec tunnel.

   Make sure you have specified the Template of Service_Conn_Template before starting this task.

2. Give the profile a name and specify IKE settings.

   Make a note of these settings; you specify the same settings when you configure the IPSec-capable device on the other side of the service connection.

3. Select Network > Network Profiles > IPSec Crypto > Add and Add a new IPSec crypto profile.

4. Specify a name for the profile and specify IPSec crypto parameters.

   Make a note of these parameters; you specify these same parameters when you configure the IPSec-capable device on the other side of the service connection.
5. Select **Network > Network Profiles > IKE Gateways** and **Add** a new **IKE gateway**.

6. Specify a **Name**, **Version**, **Peer IP Address Type**, and **Authentication**, and specify a **Peer Identification** that will be synchronized with the IPSec device on the other side of the service connection.

   You can choose a **Peer IP Address Type** of either **IP** or **Dynamic**.
   
   - If you select **IP**, specify the public IP address of the IPSec-capable device on the other side of the service connection.
   - Select **Dynamic** if the peer IP address or FQDN value is unknown.

   When the peer IP address type is Dynamic, it is up to the peer to initiate the IKE gateway negotiation.

   Make a note of the of the **User FQDN (email address)** or **IP address** that you use for the **Peer Identification**. In addition, if you use a pre-shared key for authentication, make a note of the **Pre-Shared key** that you use; you must match these settings when you configure the IPSec-capable device on the other side of the service connection.

7. Click the **Advanced Options** tab, specify the **IKE Crypto Profile** you just created, and make sure that **Enable Passive Mode** is selected.

   Optionally, **Enable NAT Traversal**. Enabling NAT traversal allows the negotiation to occur even if the other side of the service connection is behind NAT.
8. Select **Network > IPSec Tunnels** and **Add** an **IPSec tunnel**.

9. Select the **IKE Gateway** and **IPSec Crypto Profile** you created earlier in this task.

10. *(Optional)* Select the **Proxy IDs** tab and create a default route for all local and remote prefixes.
Creating this route ensures that all prefixes in the VPN use this IPSec tunnel.

STEP 3 | Onboard a service connection to use as the connection between Prisma Access and the IPSec-capable device.

   Be sure to specify the IPSec Tunnel you created in this procedure.

STEP 4 | Save and Commit your changes.

STEP 5 | On your IPSec-capable device on the other side of the service connection, configure an IPSec tunnel that connects to the in Prisma Access, using the public IP address used by that device, and commit the change on that device so that the tunnel can be established.

Create Traffic Forwarding Rules for the Service Connection

After you create the service connection, create and configure traffic forwarding rules (PBF rules) in the service connection settings to specify the traffic to send to the service connection.

   Use the following steps to specify traffic to send to the service connection:

   • Create a target that associates a group you create with a service connection.
   • Create one or more traffic forwarding rules for the target and specify the traffic that you want to send to the service connection.

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

STEP 2 | Click the gear icon in the Settings area to edit the settings.
STEP 3 | Click the **Traffic Forwarding** tab.

STEP 4 | Create a group and assign a service connection to it.

1. In the **Target Service Connections for Traffic Forwarding** 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 and click **OK**.

You can specify multiple service connections for a single target as long as they are in different locations; however, Prisma Access allows only one service connection location per target. If you specify multiple targets, Prisma Access forwards traffic to the service connection with the shortest path.
3. Choose whether this connection is on your organization’s network.
   
   - Select **Dedicated for PBF Only** if you are deploying this service connection for a device that is not on your organization’s network (for example, a cloud-based device). Prisma Access uses this service connection for PBF traffic only.

     *Selecting Dedicated for PBF Only causes the zone for all service connections to change from Trust to Untrust. Check your zone mapping and security policies to make sure that your network reflects this change.*

   - Deselect **Dedicated for PBF Only** if the device is on your organization's network. You can then process internal network traffic on this service connection as well as forwarded traffic.

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

1. In the **Traffic Forwarding Rules** area, **Add** a traffic forwarding rule.
2. In the **General** tab, **Name** the traffic forwarding rule.
3. In the **Source** tab, specify a **Source** FQDN or IP address that the source traffic must match, or select **Any** to have all traffic go to this target.
You can either manually specify an FQDN or IP address, or you can specify an address object you created in Panorama (Objects > Addresses).

If you use address objects, make them Shared to share them with all device groups in Prisma Access.

4. In the Destination tab, specify the following values:
   - In the Destination area, specify a Destination FQDN, IP address, or shared address object.
     Leave Any selected to pass all traffic to be processed by the rules in the URL area. If you specify rules in the Destination and the URL areas, Prisma Access processes the rules in the Destination area first.
   - In the URL area, enter a URL or shared custom URL category you created in Panorama (Objects > Custom Objects > URL Category) to specify URLs for the traffic forwarding rule.
     If you create a URL Category, make sure that you configure it as Shared.
     You can also enter wildcard URLs (for example, *.example.com).
     Leave Any selected to pass all HTTP and HTTPS traffic with this rule.

     If you have Prisma Access direct all HTTP and HTTPS traffic to the service connection, determine if you have HTTP or HTTPS traffic that should instead use the service connection to travel to an internal destination (for example, an HTTPS server in your organization’s headquarters). To prevent Prisma Access from redirecting internal HTTP or HTTPS traffic, configure another traffic rule for the internal HTTP and HTTPS traffic, specify the Destination as the IP address of the internal server, and deselect Forward in the Action tab, which prevents this traffic from egressing from the service connection.

5. In the Action tab, select the Group Name that you want to apply to the traffic forwarding rule.
6. Enable or disable forwarding for the selected traffic.
   - To enable forwarding for the rules you specify for this traffic, leave Forward selected.
   - To prevent Prisma Access from forwarding traffic for the rules you specify to a service connection, and ensure that this traffic always uses its normal egress path from a remote network connection or mobile user location, deselect Forward.

   For example, select *.example2.com in the Destination tab and deselect the Forward check box in the Action tab to make sure that any remote network or mobile user traffic to *.example2.com follows its normal egress path.

7. Click OK to save your changes.

STEP 6 | Commit your changes locally to make them active in Panorama.

   You only have to perform this step if your configuration includes mobile users; skip this step if your configuration only includes Prisma Access for remote networks with no mobile user configuration.

   1. Select Commit > Commit to Panorama.
   2. Make sure that the device groups, templates, and template stacks are 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.

   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.
List of Prisma Access Locations

The following table lists the available locations for Prisma Access. The locations are sorted by an alphabetical list and by regions. 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.

- List of Locations
- List of Locations by Region

List of Locations

The following table provides an overall list of locations.

<table>
<thead>
<tr>
<th>Locations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Andorra</td>
</tr>
<tr>
<td>Argentina</td>
</tr>
<tr>
<td>Australia East</td>
</tr>
<tr>
<td>Australia South</td>
</tr>
<tr>
<td>Australia Southeast</td>
</tr>
<tr>
<td>Austria</td>
</tr>
<tr>
<td>Bangladesh</td>
</tr>
<tr>
<td>Belarus</td>
</tr>
<tr>
<td>Belgium</td>
</tr>
<tr>
<td>Bolivia</td>
</tr>
<tr>
<td>Brazil Central</td>
</tr>
<tr>
<td>Brazil East</td>
</tr>
<tr>
<td>Brazil South</td>
</tr>
<tr>
<td>Bulgaria</td>
</tr>
<tr>
<td>Cambodia</td>
</tr>
<tr>
<td>Canada Central</td>
</tr>
<tr>
<td>Canada East</td>
</tr>
<tr>
<td>Canada West</td>
</tr>
<tr>
<td>Locations</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>Chile</td>
</tr>
<tr>
<td>Columbia</td>
</tr>
<tr>
<td>Costa Rica</td>
</tr>
<tr>
<td>Croatia</td>
</tr>
<tr>
<td>Czech Republic</td>
</tr>
<tr>
<td>Denmark</td>
</tr>
<tr>
<td>Ecuador</td>
</tr>
<tr>
<td>Egypt</td>
</tr>
<tr>
<td>Finland</td>
</tr>
<tr>
<td>France North</td>
</tr>
<tr>
<td>France South</td>
</tr>
<tr>
<td>Germany Central</td>
</tr>
<tr>
<td>Germany North</td>
</tr>
<tr>
<td>Germany South</td>
</tr>
<tr>
<td>Greece</td>
</tr>
<tr>
<td>Hong Kong</td>
</tr>
<tr>
<td>Hungary</td>
</tr>
<tr>
<td>India North</td>
</tr>
<tr>
<td>India South</td>
</tr>
<tr>
<td>India West</td>
</tr>
<tr>
<td>Indonesia</td>
</tr>
<tr>
<td>Ireland</td>
</tr>
<tr>
<td>Israel</td>
</tr>
<tr>
<td>Italy</td>
</tr>
<tr>
<td>Japan Central</td>
</tr>
<tr>
<td>Japan South</td>
</tr>
<tr>
<td>Locations</td>
</tr>
<tr>
<td>---------------</td>
</tr>
<tr>
<td>Jordan</td>
</tr>
<tr>
<td>Kenya</td>
</tr>
<tr>
<td>Kuwait</td>
</tr>
<tr>
<td>Liechtenstein</td>
</tr>
<tr>
<td>Lithuania</td>
</tr>
<tr>
<td>Luxembourg</td>
</tr>
<tr>
<td>Malaysia</td>
</tr>
<tr>
<td>Mexico Central</td>
</tr>
<tr>
<td>Mexico West</td>
</tr>
<tr>
<td>Moldova</td>
</tr>
<tr>
<td>Monaco</td>
</tr>
<tr>
<td>Myanmar</td>
</tr>
<tr>
<td>Netherlands Central</td>
</tr>
<tr>
<td>Netherlands South</td>
</tr>
<tr>
<td>New Zealand</td>
</tr>
<tr>
<td>Nigeria</td>
</tr>
<tr>
<td>Norway</td>
</tr>
<tr>
<td>Pakistan South</td>
</tr>
<tr>
<td>Pakistan West</td>
</tr>
<tr>
<td>Panama</td>
</tr>
<tr>
<td>Papua New Guinea</td>
</tr>
<tr>
<td>Paraguay</td>
</tr>
<tr>
<td>Peru</td>
</tr>
<tr>
<td>Philippines</td>
</tr>
<tr>
<td>Poland</td>
</tr>
<tr>
<td>Portugal</td>
</tr>
<tr>
<td>Locations</td>
</tr>
<tr>
<td>-------------------------</td>
</tr>
<tr>
<td>Romania</td>
</tr>
<tr>
<td>Russia Central</td>
</tr>
<tr>
<td>Russia Northwest</td>
</tr>
<tr>
<td>Saudi Arabia</td>
</tr>
<tr>
<td>Singapore</td>
</tr>
<tr>
<td>Slovakia</td>
</tr>
<tr>
<td>Slovenia</td>
</tr>
<tr>
<td>South Africa Central</td>
</tr>
<tr>
<td>South Africa West</td>
</tr>
<tr>
<td>South Korea</td>
</tr>
<tr>
<td>Spain Central</td>
</tr>
<tr>
<td>Spain East</td>
</tr>
<tr>
<td>Sweden</td>
</tr>
<tr>
<td>Switzerland</td>
</tr>
<tr>
<td>Taiwan</td>
</tr>
<tr>
<td>Thailand</td>
</tr>
<tr>
<td>Turkey</td>
</tr>
<tr>
<td>UK</td>
</tr>
<tr>
<td>Ukraine</td>
</tr>
<tr>
<td>United Arab Emirates</td>
</tr>
<tr>
<td>US Central</td>
</tr>
<tr>
<td>US East</td>
</tr>
<tr>
<td>US Northeast</td>
</tr>
<tr>
<td>US Northwest</td>
</tr>
<tr>
<td>US South</td>
</tr>
<tr>
<td>US Southeast</td>
</tr>
</tbody>
</table>
## List of Locations by Region

The following table provides you with a list of locations separated by region.

<table>
<thead>
<tr>
<th>Locations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Africa Region</strong></td>
</tr>
<tr>
<td>Kenya</td>
</tr>
<tr>
<td>Nigeria</td>
</tr>
<tr>
<td>South Africa Central</td>
</tr>
<tr>
<td>South Africa West</td>
</tr>
<tr>
<td><strong>Asia Region</strong></td>
</tr>
<tr>
<td>Bangladesh</td>
</tr>
<tr>
<td>Cambodia</td>
</tr>
<tr>
<td>Hong Kong</td>
</tr>
<tr>
<td>India North</td>
</tr>
<tr>
<td>India South</td>
</tr>
<tr>
<td>India West</td>
</tr>
<tr>
<td>Indonesia</td>
</tr>
<tr>
<td>Malaysia</td>
</tr>
<tr>
<td>Myanmar</td>
</tr>
<tr>
<td>Pakistan South</td>
</tr>
<tr>
<td>Pakistan West</td>
</tr>
<tr>
<td>Locations</td>
</tr>
<tr>
<td>------------------------</td>
</tr>
<tr>
<td>Papua New Guinea</td>
</tr>
<tr>
<td>Philippines</td>
</tr>
<tr>
<td>Singapore</td>
</tr>
<tr>
<td>South Korea</td>
</tr>
<tr>
<td>Taiwan</td>
</tr>
<tr>
<td>Thailand</td>
</tr>
<tr>
<td>Vietnam</td>
</tr>
<tr>
<td><strong>ANZ Region</strong></td>
</tr>
<tr>
<td>Australia East</td>
</tr>
<tr>
<td>Australia South</td>
</tr>
<tr>
<td>Australia Southeast</td>
</tr>
<tr>
<td>New Zealand</td>
</tr>
<tr>
<td><strong>Europe Region</strong></td>
</tr>
<tr>
<td>Andorra</td>
</tr>
<tr>
<td>Austria</td>
</tr>
<tr>
<td>Belarus</td>
</tr>
<tr>
<td>Belgium</td>
</tr>
<tr>
<td>Bulgaria</td>
</tr>
<tr>
<td>Croatia</td>
</tr>
<tr>
<td>Czech Republic</td>
</tr>
<tr>
<td>Denmark</td>
</tr>
<tr>
<td>Finland</td>
</tr>
<tr>
<td>France North</td>
</tr>
<tr>
<td>France South</td>
</tr>
<tr>
<td>Germany Central</td>
</tr>
<tr>
<td>Germany North</td>
</tr>
<tr>
<td>Locations</td>
</tr>
<tr>
<td>--------------------</td>
</tr>
<tr>
<td>Germany South</td>
</tr>
<tr>
<td>Greece</td>
</tr>
<tr>
<td>Hungary</td>
</tr>
<tr>
<td>Ireland</td>
</tr>
<tr>
<td>Italy</td>
</tr>
<tr>
<td>Liechtenstein</td>
</tr>
<tr>
<td>Lithuania</td>
</tr>
<tr>
<td>Luxembourg</td>
</tr>
<tr>
<td>Moldova</td>
</tr>
<tr>
<td>Monaco</td>
</tr>
<tr>
<td>Netherlands Central</td>
</tr>
<tr>
<td>Netherlands South</td>
</tr>
<tr>
<td>Norway</td>
</tr>
<tr>
<td>Poland</td>
</tr>
<tr>
<td>Portugal</td>
</tr>
<tr>
<td>Romania</td>
</tr>
<tr>
<td>Russia Central</td>
</tr>
<tr>
<td>Russia Northwest</td>
</tr>
<tr>
<td>Slovakia</td>
</tr>
<tr>
<td>Slovenia</td>
</tr>
<tr>
<td>Spain Central</td>
</tr>
<tr>
<td>Spain East</td>
</tr>
<tr>
<td>Sweden</td>
</tr>
<tr>
<td>Switzerland</td>
</tr>
<tr>
<td>UK</td>
</tr>
<tr>
<td>Ukraine</td>
</tr>
<tr>
<td>Locations</td>
</tr>
<tr>
<td>----------------------------</td>
</tr>
<tr>
<td>Uzbekistan</td>
</tr>
<tr>
<td><strong>Japan Region</strong></td>
</tr>
<tr>
<td>Japan Central</td>
</tr>
<tr>
<td>Japan South</td>
</tr>
<tr>
<td><strong>Middle East Region</strong></td>
</tr>
<tr>
<td>Egypt</td>
</tr>
<tr>
<td>Israel</td>
</tr>
<tr>
<td>Jordan</td>
</tr>
<tr>
<td>Kuwait</td>
</tr>
<tr>
<td>Saudi Arabia</td>
</tr>
<tr>
<td>Turkey</td>
</tr>
<tr>
<td>United Arab Emirates</td>
</tr>
<tr>
<td><strong>North America Region</strong></td>
</tr>
<tr>
<td>Canada Central</td>
</tr>
<tr>
<td>Canada East</td>
</tr>
<tr>
<td>Canada West</td>
</tr>
<tr>
<td>Costa Rica</td>
</tr>
<tr>
<td>Mexico Central</td>
</tr>
<tr>
<td>Mexico West</td>
</tr>
<tr>
<td>Panama</td>
</tr>
<tr>
<td>US Central</td>
</tr>
<tr>
<td>US East</td>
</tr>
<tr>
<td>US Northeast</td>
</tr>
<tr>
<td>US Northwest</td>
</tr>
<tr>
<td>US South</td>
</tr>
<tr>
<td>US Southeast</td>
</tr>
<tr>
<td>Locations</td>
</tr>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td>US Southwest</td>
</tr>
<tr>
<td>US West</td>
</tr>
<tr>
<td>South America Region</td>
</tr>
<tr>
<td>Argentina</td>
</tr>
<tr>
<td>Bolivia</td>
</tr>
<tr>
<td>Brazil Central</td>
</tr>
<tr>
<td>Brazil East</td>
</tr>
<tr>
<td>Brazil South</td>
</tr>
<tr>
<td>Chile</td>
</tr>
<tr>
<td>Columbia</td>
</tr>
<tr>
<td>Ecuador</td>
</tr>
<tr>
<td>Paraguay</td>
</tr>
<tr>
<td>Peru</td>
</tr>
<tr>
<td>Venezuela</td>
</tr>
</tbody>
</table>
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, ensuring bandwidth and uptime requirements in multiple locations around the globe while staying within your budget. However, with Prisma Access for users (formerly GlobalProtect cloud service for mobile users), all of the infrastructure is deployed for you and scales based on the number of active users and their locations. Users will then connect to Prisma Access for mobile users to receive their VPN configuration, which will route them to the closest Prisma Access gateway 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.

To configure this service, you must supply an IP address pool which will be used to assign IP addresses for the client VPN tunnels. The addresses in this pool must not overlap with other address pools you use internally or the IP subnet you assign when you Enable the Service Infrastructure.

- Plan To Deploy Prisma Access for Users
- Configure Prisma Access for Users
- Zone Mapping
- Specify IP Address Pools for Mobile Users
- How the GlobalProtect App Selects a Prisma Access Gateway
- Quick Configs for Mobile User Deployments
- Report Website Access Issues
Plan To Deploy Prisma Access for Users

Before you begin to Configure Prisma Access for Users, make sure you have the following configuration items ready to ensure that you will be able to successfully enable the service and enforce consistent policy for your mobile users (GlobalProtect endpoints):

Use this checklist to make sure that you have everything ready to deploy your Prisma Access for users.

**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. See Specify IP Address Pools for Mobile Users for minimum IP address requirements.

  *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 the 100.64.0.0/15 and 169.254.0.0/16 subnet ranges because Prisma Access reserves those 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. Note that, if you enable BGP, Prisma Access allocates these pools in Class C (/24) subnet blocks.

You can specify an IP address pool for every region from which your users will need to connect, specify a worldwide IP address pool, or specify pools for regions and Worldwide combined. If you do not assign an IP address to a region (either by specifying an IP address for that region or specifying a Worldwide address), any locations you configure in that region will not have an IP address or networking configuration, and users in that region will not be able to connect.

- **Template**—Prisma Access for users automatically creates a template stack and a top-level template for the cloud service. 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 any existing GlobalProtect portal, GlobalProtect gateway, User-ID, server profiles (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 Configure Prisma Access for Users. Additionally, the 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 to push your security policy, security profiles, and other policy objects (such as application groups and objects, and address groups), HIP objects and profiles as well as authentication policy that the service will need to enforce consistent policy for your remote users.

- **Locations to Onboard**—Prisma Access provides you with worldwide locations where you can Configure Prisma Access for Users. 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 amount of IP addresses to allocate for 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.
• **Portal Hostname**—Prisma Access for users enables you to quickly and easily set up the portal hostname using a default domain name (.gpcloudservice.com). In this case, the cloud service automatically publishes the hostname to public DNS servers and handles all of the certificate generation. However, you can opt to use your own company domain name in the portal hostname. If you plan to use this option, you must obtain your own certificates for the portal and configure an SSL/TLS service profile to point to the certificate prior to configuring the service. Additionally, if you use your own domain name in the portal hostname you will also need to configure your DNS servers to point to the portal DNS CNAME, which will be provided to you during the configuration process.

• **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, you must create and configure a service connection.

    Even if you don’t plan to use the connection to provide access to your internal resources, 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.

- **Post-Installation checklist:**

  • **Whitelist the Public IP Addresses**—After you onboard your locations, you need to Retrieve Public IP Addresses Used by Mobile User Deployments used by each location and whitelist these locations 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.
Configure Prisma Access for Users

When you configure Prisma Access for users, 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. Some of the required settings, such as what authentication profile to use to authenticate mobile users, you may be able to leverage using existing configurations. 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 will need (for example, security policy, zones, User-ID configuration, and other policy objects) go ahead and add them when you onboard. This way you will be able to complete the zone mapping that will be 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 and push it to Prisma Access for users later.

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 that 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 firewall in a hub-and-spoke architecture in order to provide access to the internal networks in your Prisma Access infrastructure.

**STEP 1** | Select Panorama > Cloud Services > Configuration > Mobile Users.

**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, 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, 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 Mobile_User_Template from the top of the stack, which 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.

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 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/Logging Service in a device group that gets pushed to Prisma Access for users. This is the only way that the cloud service will know which logs to forward to Cortex Data Lake.
4. Click OK to save the template stack and device group configuration.

STEP 3 | 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. This means that you no longer need to worry about configuring interfaces and associating 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.

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 the mappings.

STEP 4 | Configure the GlobalProtect portal and external gateway settings:

You can only configure Prisma Access gateways as external gateways; configuring them as internal gateways is not supported.

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 will use the default domain name: .gpcloudservice.com. In this case all you need to do is 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 mapping 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 use to encrypt the secure cookies that mobile users authenticate to the portal and gateway with.

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 can be reached from the internal network only.
   3. Enter the DNS Hostname for the IP address you entered. Clients that try to connect attempt to do 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.

**STEP 5** 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.

Specifying a single region also reduces the minimum IP address pool that you need to specify (you specify IP address pools in the Step 6). See Specify IP Address Pools for Mobile Users for more information.

> 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, then select a region.
2. Select one or more Prisma Access gateways in that region using the map.

Hovering 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 a button on the lower left of the page. In the list view, the list displays regions sorted by columns, with all locations sorted by region. You can select all sites in a region by clicking All at the top of the column.
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 clicking Add.

- **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.

- **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, to allow all mobile users to log in at the same time. Do not use the 100.64.0.0/15 and 169.254.0.0/16 subnets, because Prisma Access reserves those subnets for its internal use. See Specify IP Address Pools for Mobile Users for more information.

We recommend using an RFC 1918-compliant IP address pool. While the use of non-RFC 1918-compliant (public) IP addresses is supported for mobile users, we do not recommend it because of possible conflicts with internet public IP address space.

STEP 7 | To configure the network settings Prisma Access for users should assign to the virtual adapter of the endpoints, select the 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 a separate networking configuration. You can use a single network services configuration for all GlobalProtect endpoints Worldwide, you can set separate pools for each geographic region where your users are located, or you can specify both a Worldwide and region pools.

- **Region**—Select Worldwide to use the same network settings for all GlobalProtect endpoints using the cloud service, or select an available Region.

  *If you specified an IP address pool for a specific region instead of allocating a global IP address pool, your remote users can connect only to the infrastructure that has been set up in the specified region.*

- Specify the DNS settings that your endpoints should use to resolve your internal domains, both for requests that originate internally and requests that originate externally. If you do not have specific DNS servers you want to direct your mobile endpoints to, the endpoint will Use Cloud Default. If you do specify specific primary and/or secondary DNS servers, the DNS proxy on the gateway where the request originates sends the request to the specified DNS servers. The source address in the DNS request is the first IP address in the IP pool assigned to that gateway. In this case, you will need to make sure that you allow traffic from all addresses in your mobile user IP address pool to your DNS servers.

  - **Primary DNS**—Enter IP address of the primary DNS server the endpoints should use to resolve internal domains.
  - **Secondary DNS**—Enter the IP address of the secondary DNS server the endpoints should use to resolve internal domains.
  - (Optional) **Primary DNS**—If you have an external DNS server that can access your internal domains, specify it here.
  - (Optional) **Secondary DNS**—If you have an external DNS server that can access your internal domains, specify the secondary server here.
  - (Optional) **Domain List**—Add the domains you want the GlobalProtect client to only resolve using your local DNS servers. 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.

  - (Optional) **Client DNS Suffix Search List**—Click Add to specify the suffix that the client should use locally when an unqualified hostname is entered that it cannot resolve, for example, acme.local. Note that you should not enter a wildcard (*) character in front of the domain suffix. You can Add multiple suffixes.
STEP 8 | *(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 the UK when you select locations, you cannot select the 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 9** | Click **OK** to save the Onboarding settings.

**STEP 10** | 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 11** | 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 upgrade:

- Log Settings for System logs (**system-prisma-access-default**), User-ID logs (**userid-prisma-access-default**), and HIP Match logs (**hipmatch-prisma-access-default**) are added to the Mobile_User_Template.
• Log Settings for System logs (system-prisma-access-default) and User-ID logs (userid-prisma-access-default) are added to the Remote_Network_Template.
• Log Settings for System logs (system-prisma-access-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. If you are upgrading and have already configured Log Settings, you can disable these by deselecting the check box next to the profile (you cannot delete them).

**STEP 12 | (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/Logging Service** 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 13 | 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.

**STEP 14 |** 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.

To view information about currently logged in users, or to log out a logged in user, click the hyperlinked number next to Current Users. This screen shows both users logged in with the GlobalProtect app and Clientless VPN users. 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.

To log out a currently logged-in user, 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.
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 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.
STEP 15 | 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 16 | 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 this is not configurable; however, you can Manage Upgrade Options for the GlobalProtect App in Panorama to control the availability of an app version and 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移动应用 from the appropriate app store for their operating systems.
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 on the firewalls it instantiates within the cloud. 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 on the firewalls it deploys, 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.

<table>
<thead>
<tr>
<th>Application</th>
<th>Security Policy Zone</th>
<th>Zone Mapping</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office 365</td>
<td>sanctioned-saas</td>
<td>untrust</td>
<td>allow</td>
</tr>
<tr>
<td>Salesforce</td>
<td>sanctioned-saas</td>
<td>untrust</td>
<td>allow</td>
</tr>
<tr>
<td>Perforce</td>
<td>eng-tools</td>
<td>untrust</td>
<td>allow</td>
</tr>
<tr>
<td>LDAP</td>
<td>dc-apps</td>
<td>trust</td>
<td>allow</td>
</tr>
</tbody>
</table>
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. We recommend having at least one IP address in your IP address pool for each unique mobile user in your organization so they can log in simultaneously. If your pool space is limited, however, you can specify a smaller address pool.

In Panorama, the UI validates the minimum IP address pool and prompts you if changes are required. 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:

- If you specify a Worldwide address pool, a minimum of /23 (512 IP addresses) is required if you have locations deployed in one or two regions. If you have locations in three regions, a minimum /22 (1,096) addresses is required.
  
  You can divide up your total subnets into smaller subnets; the minimum subnet you can specify is /23.

- If you specify IP address pools per region, a minimum of 512 IP addresses (/23 address pool) is required for each region where you have locations deployed.

  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 US East (N. Virginia), US East (Ohio), and US West (N. California), you need to only specify an IP address pool for the Americas region.

- If you specify a mix of Worldwide and regional pools, specify IP address pools to ensure that there are at least 512 IP addresses per region.

  For example, for a three-region deployment, you can specify 1,024 addresses in the Europe region and 512 addresses Worldwide.

  A warning message displays if you specify an IP address pool that is less than the total number of licensed mobile users. If you determine that your deployment will not have all mobile users log in concurrently, you can bypass this message and keep this configuration.
How the GlobalProtect App Selects a Prisma Access Gateway

When a mobile user connects to a Prisma Access gateway, the app uses the following selection process to determine to which gateway it connects.

If you use on-premise gateways with Prisma Access gateways, you can specify priorities in Prisma Access to let mobile users connect to either a specific on-premise GlobalProtect gateway or a Prisma Access gateway. See Manage Priorities for Prisma Access and On-Premise Gateways for details.

- If the mobile user connects in a country that has a Prisma Access gateway, the user connects to the gateway in that country.
- If there is more than one gateway in the country, the mobile user connects to the in-country gateway that has the lowest latency.
- If the mobile user cannot connect to an in-country gateway for any reason, the user connects to the gateway with the lowest latency at the time of connection.
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-Premise Gateways
- Manage Priorities for Prisma Access and On-Premise Gateways
- Configure Quality of Service in Prisma Access
- Report Website Access Issues

Prisma Access with On-Premise 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-Premise Gateways, which allow you to specify priorities for on-premise 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-premise 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-premise 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-premise 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.
Manage Priorities for Prisma Access and On-Premise 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-Premise Gateways, you can set priorities in Prisma Access to let mobile users connect to either a specific on-premise GlobalProtect gateway or a Prisma Access gateway.

You can select an on-premise gateway that is physically closest to your mobile users and allow users to connect to a different gateway (either on-premise 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-premise 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-Premise 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-Premise and Prisma Access Gateways
- Set a Higher Gateway Priority for an On-Premise Gateway
- Set Higher Priorities for Multiple On-Premise Gateways
- Configure Priorities for Prisma Access and On-Premise Gateways
- Allow Mobile Users to Manually Select Specific Prisma Access Gateways
Set Equal Gateway Priorities for On-Premise 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-premise 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-premise gateway. When users change locations, the GlobalProtect app chooses another gateway (either on-premise 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-premise gateways.

In this example, User 1’s GlobalProtect app determines that the Prisma Access gateway has a lower response time than the on-premise gateway, and user 2’s GlobalProtect app determines that the on-premise 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-premise gateway, based on the lower response time.

Set a Higher Gateway Priority for an On-Premise Gateway

In situations where you want to direct mobile users to use an on-premise gateway instead of the Prisma Access gateways, specify the on-premise 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-premise 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-premise gateway. We recommend specifying a source region for the following reasons:
• Specifying a source region for an on-premise 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-premise 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-premise gateway in Indonesia, every mobile user in your organization would prefer the on-premise 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-Premise 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-premise 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-premise 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-premise gateway in Sweden because of the source region and higher gateway priority.

Configure Priorities for Prisma Access and On-Premise Gateways

Use this workflow to configure priorities for a deployment that uses on-premise 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-Premise and Prisma Access Gateways, change the priority from None to Highest.
      - To Set a Higher Gateway Priority for an On-Premise Gateway or Set Higher Priorities for Multiple On-Premise 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-premise 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-premise gateway, or select **Any** to make the gateway available to all regions.

   If you set the priority of on-premise 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-premise gateways because of the higher priority for the on-premise gateways.

4. Select the **Manual** check box to allow users to manually switch to the gateway.

5. Set the **Priority** of the on-premise 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-Premise 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 following sections from the GlobalProtect App User Guide:

- Download and Install the GlobalProtect App for Windows
- Download and Install the GlobalProtect App for Mac
- Use the GlobalProtect App for Chrome_OS
- Use the GlobalProtect App for Linux
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 Prisma Access for Networks
- Configure Prisma Access for Networks
- Quick Configs for Remote Network Deployments
Plan to Deploy Prisma Access for Networks

Prisma Access for networks allows you to pick the geographic locations where you want to deploy a firewall in the cloud-based security infrastructure to secure your remote network locations.

Before you begin to Configure Prisma Access for 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:

- **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 Configure Prisma Access for 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.
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 Configure Prisma Access for 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.
Configure Prisma Access for 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 the cloud service and onboard each remote network so that you can start sending traffic from the remote site through the IPSec tunnel to the firewalls in the cloud.

Before you begin onboarding your remote networks, be sure you go through the steps to Plan to Deploy Prisma Access for 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. 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).
STEP 2 | 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 3 | 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 4 | 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.
STEP 5 | 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 6 | 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. 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 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.
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 7 | 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.
To configure BGP:

1. On the BGP tab, select Enable.
2. (Optional) To prevent the BGP peer on the Prisma Access firewall from forwarding routes into your remote network, select Don't export 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-premise equipment to establish routes back to Prisma Access.
3. Enter the **Peer AS**, which is the autonomous system (AS) to which the firewall virtual router or BGP router at your remote network belongs.

4. 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**.

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 remote network.

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

**STEP 8** 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-premise device, or both PAN-OS-marked and on-premise-marked traffic. See **Configure Quality of Service in Prisma Access** for details.
STEP 9 | 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 earlier.

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.

STEP 10 | 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 11 | 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 your Prisma Access firewall, 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 12 | 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 13 | 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/Logging Service 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 14 | 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.

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:
- **Region**—The region where your cloud service infrastructure is deployed for the remote network location.
- **Remote Peer**—The peer to which the remote network has an IPSec tunnel connection.
- **Allocated Bandwidth (Mbps)**—The amount of bandwidth you allocated for the remote network location.

  *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.*

- **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 the Prisma Access firewall. 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 the Prisma Access 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.

- **Tunnel Status**—The operational status of the connection between Prisma Access and the remote network.

**Statistics** tab:

- **Region**—The region where your cloud service infrastructure is deployed for the remote network location.
- **Remote Peer**—The peer to which the remote network has an IPSec tunnel connection.
- **Allocated Bandwidth (Mbps)**—The amount of bandwidth you allocated for the remote network location.

  *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.*

- **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 the Prisma Access firewall. 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 the Prisma Access 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.

- **Tunnel Status**—The operational status of the connection between Prisma Access and the remote network.
Verify Remote Connection BGP Status

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

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 bgpAfiIpv4-unicast Counters area, in the **Incoming Total** and **Outgoing Total** fields.

- **RIB In**—Routing information that has been received from different peers and is stored in the Routing Information Base (RIB).
• **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
- Configure User-ID and User-Based Policies with Prisma Access

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:

- You have two WAN links that you want to combine for one remote network location for a higher bandwidth throughput.

  If you want to configure two WAN links in an active/backup mode, do not use the active/active WAN link deployment model described in this section. Instead, select Enable Secondary WAN and specify a backup WAN when you Configure Prisma Access for Networks.

- You have one fast WAN link and a slower WAN link, you want to add both of them to a remote network, and you want to designate which traffic goes over which link based on subnet or application.

  Depending on the type of firewall, switch, or SD-WAN device available at the remote network location, you can route traffic based on application or subnet. 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 link.

- You want to configure an overlapping subnet deployment by design; for example, if you want to create a separate guest network at a retail store location with different policies.

- 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 either select Overlapped Subnets check box in the remote network Settings when you Configure Prisma Access for Networks, or create two remote networks with overlapping subnets in different locations. Keep in mind, however, that this configuration has the following limitations:

- Sites without overlapping subnets function normally and are not affected in a deployment with sites that have overlapping subnets.

- If you configure overlapping subnets in the same location by selecting Overlapped Subnets in the remote networks setup, the trust zone for that location changes its name from Trust to the name you specified for the remote network connection. This name change is also reflected in the logs you receive from Cortex Data Lake.
There is no inbound remote network-to-remote network traffic. The other remote network locations would not know where route the traffic because multiple remote network locations route to the same subnets. However, users and services at any remote network location can access resources at other remote network locations provided there are no overlapping subnets at the site, and any site can access the internet through Prisma Access.

Traffic from your service connections can not access resources at any remote network location with overlapping subnets because it would not know which remote network location to route the traffic. The remote network locations with overlapping subnets can, however, access resources from service connections.

Mobile users cannot access resources at the remote network locations with overlapping subnets, again because of the inbound routing limitations.

When you select the Overlapped Subnets check box, the source zone in the traffic logs changes to the remote network name that is configured in Panorama > Cloud Services > Configuration > Remote Networks > Onboarding > Name.

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 Prisma Access firewall 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 firewalls 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-premise 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-premise device that is not listed here.

• Cisco appliances:
  • Cisco Integrated Services Routers (ISRs)
  • Cisco Adaptive Security Appliances (ASAs)
• Citrix
• 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-premise 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.
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.
2. Under **Advanced Options**, specify the **IKE Crypto Profile** for the predefined template you want to use.

3. Create a new **IPSec Tunnel**, specifying the new IKE gateway you created, but copying all the other settings from the default template.
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 Configure Prisma Access for 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 Configure Prisma Access for 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 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required? (Y/N)</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The name of the remote network.</td>
<td>Y</td>
</tr>
<tr>
<td>bandwidth</td>
<td>The allocated bandwidth of the remote network. Acceptable values are:</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>• 2 Mbps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 5 Mbps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 10 Mbps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 20 Mbps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 25 Mbps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 50 Mbps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 100 Mbps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 150 Mbps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 300 Mbps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 500 Mbps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1000 Mbps</td>
<td></td>
</tr>
<tr>
<td>region</td>
<td>The remote network's region. See the list of Prisma Access locations for the values to enter. Enter the locations exactly as they are in this document (for example, <strong>US West</strong>, or <strong>Japan South</strong>).</td>
<td>Y</td>
</tr>
<tr>
<td>subnets</td>
<td>Statically routed subnets on the LAN side of the remote network. Separate multiple subnets with commas.</td>
<td>N</td>
</tr>
<tr>
<td>bgp_peer_as</td>
<td>The BGP Autonomous System Number (ASN) of the remote network peer device.</td>
<td>N</td>
</tr>
<tr>
<td>bgp_peer_address</td>
<td>The BGP peer address of the remote network peer device.</td>
<td>N</td>
</tr>
<tr>
<td>tunnel_name</td>
<td>The name of the IPSec tunnel configuration. A unique value is required.</td>
<td>Y</td>
</tr>
<tr>
<td>gateway_name</td>
<td>The name of the IKE Gateway configuration. A unique value is required.</td>
<td>Y</td>
</tr>
<tr>
<td>peer_ip_address</td>
<td>The IP address of the Prisma Access peer device.</td>
<td>N</td>
</tr>
<tr>
<td>local_id_type</td>
<td>The type of IKE ID that Prisma Access presents to the peer device. If you use certificates in the remote network to</td>
<td>N</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Required? (Y/N)</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>local_id_value</td>
<td>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.</td>
<td>N</td>
</tr>
<tr>
<td>peer_id_type</td>
<td>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.</td>
<td>N</td>
</tr>
<tr>
<td>peer_id_value</td>
<td>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.</td>
<td>N</td>
</tr>
<tr>
<td>monitor_ip</td>
<td>The tunnel monitoring IP address the cloud will use to determine that the IPSec tunnel is up and the peer network is reachable. You cannot export a proxy-ID value for the tunnel monitor.</td>
<td>N</td>
</tr>
<tr>
<td>proxy_ids</td>
<td>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:</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td>```</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[{&quot;name&quot;:&quot;proxyidname&quot;,&quot;local&quot;:&quot;1.2.3.4/32&quot;,&quot;remote&quot;:&quot;4.3.2.1/32&quot;,&quot;protocol&quot;:{&quot;udp&quot;:{&quot;local-port&quot;:123,&quot;remote-port&quot;:234}}}</td>
<td></td>
</tr>
<tr>
<td></td>
<td>,{&quot;name&quot;:&quot;proxyidname2&quot;,&quot;local&quot;:&quot;2.3.4.5/32&quot;,&quot;remote&quot;:&quot;3.4.5.6/32&quot;,&quot;protocol&quot;:{&quot;tcp&quot;:{&quot;local-port&quot;:234,&quot;remote-port&quot;:345}}}</td>
<td></td>
</tr>
<tr>
<td>sec_wan_enabled</td>
<td>Specifies whether or not you enable a secondary IPSec tunnel. Acceptable values are yes and no.</td>
<td>N</td>
</tr>
<tr>
<td>sec_tunnel_name</td>
<td>The name of the secondary IPSec tunnel configuration. A unique value is required if you specify a secondary tunnel.</td>
<td>N</td>
</tr>
<tr>
<td>sec_gateway_name</td>
<td>The name of the secondary IKE Gateway configuration. A unique value is required if you specify a secondary tunnel.</td>
<td>N</td>
</tr>
<tr>
<td>sec_peer_ip_address</td>
<td>The IP address of the Prisma Access peer device for the secondary IPSec tunnel.</td>
<td>N</td>
</tr>
<tr>
<td>sec_local_id_type</td>
<td>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</td>
<td>N</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Required? (Y/N)</th>
</tr>
</thead>
<tbody>
<tr>
<td>file</td>
<td>All imported types specified will refer to the Configured Certificate values.</td>
<td>N</td>
</tr>
<tr>
<td>sec_local_id_value</td>
<td>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.</td>
<td>N</td>
</tr>
<tr>
<td>sec_peer_id_type</td>
<td>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.</td>
<td>N</td>
</tr>
<tr>
<td>sec_peer_id_value</td>
<td>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.</td>
<td>N</td>
</tr>
<tr>
<td>sec_monitor_ip</td>
<td>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. You cannot export a proxy-ID value for the tunnel monitor.</td>
<td>N</td>
</tr>
<tr>
<td>sec_proxy_ids</td>
<td>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:</td>
<td>N</td>
</tr>
</tbody>
</table>
|                        | [["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}}}]                                                                                                                                 |                 |

---

### Configure Quality of Service in Prisma Access

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-premise device.

You can assign security policies based on destination and source IP, and you can also Define QoS based on App-ID or User_IDs the same as you define QoS on a next-generation firewall.

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-premise 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-premise devices. Optionally, you can also use on-premise 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-premise device, but not both. If there are differences between the security policies in Prisma Access and the on-premise device, the security policy in Prisma Access overrides the policy in the on-premise 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-premise 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-premise devices, and shapes the traffic on egress to your service connections or remote network connections using QoS profiles.

![QoS Examples Diagram](image)

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-premise firewall at a branch that is connected by Prisma Access with a remote network connection, and the on-premise firewall marks the traffic. This deployment honors the marking set on the on-premise 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-premise device as long as that traffic does not match an overriding security policy on Prisma Access.
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).

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.
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). 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, the firewall passes that traffic on a best-effort basis.
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.

2. Select the QoS profile you created in Step 3 and click OK.
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 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
- Retrieve User-ID Information
- Redistribute User-ID Information Between Prisma Access and On-Premise Firewalls
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-premise 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 User-ID mappings between Prisma Access and on-premise next-generation firewalls.
- For mobile users to access a resource from a remote network connection or service connection that has a next-generation firewall with user-based policies, you must redistribute User-ID mappings from Prisma Access to the firewall.
- For users at a location that is secured by a remote network or service connection with an on-premise firewall to access a resource at another branch location that you have secured with Prisma Access, you must redistribute User-ID mappings from the on-premise firewall to Prisma Access.
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-premise firewall, see Redistribute User-ID Information From Prisma Access to an On-Premise Firewall.

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 Captive Portal.

To authenticate users using MFA, SAML, or Captive 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 captive 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.
• 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, we do not recommend using 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 `wmimgmt.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.

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.
Retrieve User-ID Information

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-Premise 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-premise firewall or a VM-series firewall as a master device.

- To allow Panorama to collect group mapping information from users connected to remote networks, create a device group that specifies the on-premise 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-premise 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.

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-premise device as a Master Device. Callouts in the figure show the process.

1. A next-generation on-premise 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-Premise or VM-Series Firewall as a Master Device

Use the following procedure to configure an on-premise or VM-series firewall as a Master Device.

**STEP 1** | Create device groups for the remote network connection or service connection and specify the on-premise 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-premise or VM-Series device that you want to set as the 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 group you created with the remote network or service connection.

- To associate the device group with a service connection, select **Panorama > Cloud Services > Configuration** and select the **Service Setup** tab under **Prisma Access**; then 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 and select the Remote Networks tab; then 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.
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-Premise 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 of the following methods to redistribute User-ID mapping to mobile users and users in remote networks from an on-premise 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-Premise 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-premise next-generation firewall with user-based policies, you must redistribute User-ID mappings from Prisma Access that secures the remote network location or HQ/data center to the on-premise 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 to the on-premise firewall that protects the HQ/data center that is connected to Prisma Access with a service connection.
To redistribute User-ID mappings from Prisma Access to an on-premise 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**.

   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**.

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-premise firewall to collect the User-ID mapping from Prisma Access.
   1. From the on-premise firewall, select Device > User Identification > User-ID Agents.
   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.

STEP 3 | Repeat these steps for each service connection.

Redistribute User-ID Information From an On-Premise Firewall to Prisma Access

In cases where users are at a branch location or HQ that is secured by an on-premise 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-premise firewall to Prisma Access.

The following figure shows an HQ/Data center with an on-premise next-generation firewall with existing IP address-to-username mapping. Prisma Access connects to the firewall with a service connection, and the on-premise firewall redistributes the mapping to Prisma Access.
To redistribute User-ID mappings from an on-premise firewall to Prisma Access, complete the following steps.

**STEP 1 | Configure the on-premise firewall to redistribute User-ID information to Prisma Access.**

1. From the on-premise firewall, select **Device > User Identification > User Mapping > Palo Alto Networks User-ID Agent Setup**.
2. Click the gear icon to edit the settings.
3. Select **Redistribution**.
4. Provide a **User-ID Collector Name** and a **User-ID Collector Pre-Shared Key** to identify the on-premise 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-premise firewall.**

1. From the Panorama that manages Prisma Access, select **Device > User Identification > User-ID Agents**.
2. Make sure that you have selected the **Remote_Network_Template** in the **Templates** drop-down at the top of the page.
3. Add a User-ID Agent and give it a **Name**.
4. Select **Host and Port**.
   - 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-premise firewall in Step 1.
6. Click **OK**.
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 100 instances 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 instances of 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
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.**

*If you deploy Prisma Access for remote networks in multi-mode, you must have a minimum of 200 Mbps available in your license for each tenant. If you deploy Prisma Access for mobile users in multi-mode, 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 on a per-tenant basis. 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.

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 remote network template with the name of `rn-tpl-tenant`.
- A remote network 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.
Enable Multitenancy and create tenants

1st Tenant
Up to 3 Service Connections*
5,000 Mbps Remote Networks
5,000 Mobile Users

2nd Tenant
Up to 3 Service Connections*
5,000 Mbps Remote Networks
5,000 Mobile Users

3rd Tenant
Up to 3 Service Connections*
5,000 Mbps Remote Networks
5,000 Mobile Users

* 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:

- Make sure that your Panorama is running the minimum required version of 8.1.6 or later. If your version is earlier than 8.1.6, update your Panorama version.

  **After you have enabled multitenancy, do not downgrade either the Cloud Services plugin version or the Panorama version. Doing so can cause your configuration to go out of sync.**

- 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 100 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.

- 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 multi-tenancy 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.

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, we recommend not disabling it. Clearing the Enable Multitenancy option removes all the tenants that you have created except the first one, including all configuration for those tenants, and reverts the first tenant’s configuration back to a non-multitenant Prisma Access deployment.

STEP 3 | Click OK to migrate the existing configuration to the first tenant.

The Tenants page displays, showing the available licensed bandwidth remaining for remote networks and the remaining licensed number of mobile users. If you do not have a license for remote networks or mobile users, those choices are dimmed.
STEP 4 | 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 and selecting New Access Domain.

3. **(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.
4. (Optional) If you have other templates associated with this configuration, select them.
5. Click OK to close the Access Domain page and return to the Tenants page.

STEP 5 | 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 6 | 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 7 | Select the tenant you just created in the **Tenants** drop-down to verify that all settings were onboarded.
STEP 8 | Commit your changes locally to make them active in Panorama.

You only have to perform this step if your configuration includes mobile users; skip this step if your configuration only includes Prisma Access for remote networks with no mobile user configuration.

1. Select **Commit > Commit to Panorama**.
2. Make sure that the device groups, templates, and template stacks are part of the **Commit Scope**.
3. Click **OK** to save your changes to the Push Scope.
4. **Commit** your changes.

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.

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.

**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.
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.

**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.
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.

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) Commit your changes locally to make them active in Panorama.

A local commit is required for the mobile user changes to take effect.

1. Select Commit > Commit to Panorama.
2. Make sure that the device groups, templates, and template stacks are part of the Commit Scope.
3. Click OK to save your changes to the Push Scope.
4. Commit 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. Configure Prisma Access for Networks if you are licensed for remote networks.
4. Configure Prisma Access for Users 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 deleted 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](image-url)
**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.

![Administrator Configuration](image)

**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.

<table>
<thead>
<tr>
<th>Sample Tenant-Level Configuration</th>
<th>Configuration Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a networking-focused user who:</td>
<td>Create a tenant-level administrative user, enabling Save and Commit permissions in the Admin Role Profile, and disabling or making Read Only any permissions that you don’t want the tenant-level administrative user to have.</td>
</tr>
<tr>
<td>• Can edit plugin configurations</td>
<td></td>
</tr>
<tr>
<td>• Can commit to Panorama</td>
<td></td>
</tr>
<tr>
<td>• Can push configuration to Prisma Access</td>
<td></td>
</tr>
<tr>
<td>Create a security-focused user who:</td>
<td>To prevent a tenant-level administrative user from viewing or accessing the plugin, remove plugin access for a tenant-level administrator. For all other Panorama-related permissions, change the Admin Role permissions for the user.</td>
</tr>
<tr>
<td>• Can view and make changes to security policies</td>
<td></td>
</tr>
<tr>
<td>• Can commit to Panorama</td>
<td></td>
</tr>
<tr>
<td>• Cannot view, or make changes to, the Cloud Services plugin</td>
<td></td>
</tr>
<tr>
<td>• Cannot push configuration to Prisma Access (requires the superuser to push the configuration)</td>
<td></td>
</tr>
<tr>
<td>Create a hybrid user who:</td>
<td>You cannot make the Cloud Services plugin read-only. You can either view it or disable it.</td>
</tr>
<tr>
<td>• Has read-only access to the Cloud Services plugin</td>
<td></td>
</tr>
</tbody>
</table>
Sample Tenant-Level Configuration | Configuration Task
--- | ---
- Has read-write access to the security policy
- Cannot push the configuration to Prisma Access (requires the superuser to push the configuration)

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.

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.

```plaintext
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:

```plaintext
/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.

<table>
<thead>
<tr>
<th>Syslog Forwarding Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>* Name: Syslog-To-EC2</td>
</tr>
<tr>
<td>* SyslogServer:</td>
</tr>
<tr>
<td>* Port: 6514</td>
</tr>
<tr>
<td>* Facility: LOG_USER</td>
</tr>
<tr>
<td>Status Notification: Enter email address to send status notification</td>
</tr>
<tr>
<td>* Forwarding:</td>
</tr>
<tr>
<td>LOG VENDOR</td>
</tr>
<tr>
<td>Firewall</td>
</tr>
</tbody>
</table>

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:** Custom (Beta)
- **Query:** `(dg_hier_level_1 eq 20)`
Create and Configure the Clean Pipe Service

Use the Clean Pipe service to quickly and easily configure multiple instances of clean outbound internet connections.

> Clean Pipe Overview
> Configure the Clean Pipe Service
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 the Clean Pipe service. A service provider, MSSP, or Telco can route their customers (configured as tenants) to the Clean Pipe service 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.

The Clean Pipe service 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 the Clean Pipe service if you have one or more 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 the Clean Pipe service 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 the Clean Pipe service 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 Clean Pipe and Prisma Access:

- You must have a Clean Pipe service 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.

- The Clean Pipe service 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.
  - 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.

• Specify a unique location when you configure more than one clean pipe for a tenant; you cannot configure multiple clean pipes that use the same location for a single tenant.
• When you create a Clean Pipe tenant, match its bandwidth to the bandwidth of the partner interconnect VLAN attachment that you create for the tenant. Do not create a VLAN attachment that has a bandwidth that is higher or lower than the tenant’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 the Clean Pipe service and separate from other Prisma Access-specific configurations.
• 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. The Clean Pipe service 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:
  • Clean Pipe does not support ICMP.
  • 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 the Clean Pipe Service

To set up the Clean Pipe service for your tenants, complete the following steps.

- Enable Multitenancy and Create a Tenant
- Complete the Clean Pipe Configuration
- Migrate Existing Tenants to the Clean Pipe Service

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 the Clean Pipe service.

The Clean Pipe service 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.

If you have already created tenants, migrate the existing tenants to the clean pipe service.

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. Enter a Name for the first tenant.
5. Create and configure a new Access Domain for the first tenant and click OK.
6. In the **Clean Pipe** area, enter a **Bandwidth (Mbps)** for **This Tenant**.

   Enter a minimum of 200 Mbps for each tenant you create.

7. 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 for the tenant you created.

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 a 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, or ANY.

If you build a pair of clean pipes for a single tenant redundancy, configure them in Panorama in different locations, but specify 1 for the first clean pipe and 2 for the second clean pipe. Enter ANY for a non-redundant clean pipe deployment.

• **BGP Peer ASN**—Enter the BGP Autonomous System Number (ASN).

You must specify a private BGP ASN between 64512 and 65534. 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. If you specify another location for the tenant for redundancy, specify another location that is geographically closest to the VLAN attachment location. For example, if you specify a location in asia-east1, specify the second location in asia-east2.

---

**STEP 5** | Add more Clean Pipe instances as required by competing Step 4.

Be sure that each additional Clean Pipe uses a different location.

**STEP 6** | Commit your changes locally to make them active in Panorama.

*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. Since it takes some time (up to 30 minutes) to create a new Clean Pipe, 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.*

1. Select **Commit > Commit to Panorama**.
2. Make sure that the device groups, templates, and template stacks are 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.

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 8** | 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 9 | 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**.

STEP 10 | **Complete the Clean Pipe configuration.**

**Complete the Clean Pipe Configuration**

To complete configuration of the Clean Pipe service, 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) and 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.

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.
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.

• **Avg Egress Bandwidth 1 Min (Mbps)**—The average amount of clean pipe egress bandwidth averaged over 1 minute.

• **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 1 Min (Mbps)**—The average amount of clean pipe ingress bandwidth averaged over 1 minute.

• **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.

### Migrate Existing Tenants to the Clean Pipe Service

When you create a new multi-tenant deployment for the Clean Pipe service, Prisma Access automatically adds clean pipe-specific template stacks, templates, and device groups to the Access Domain for each tenant you create. If you have an existing multi-tenant deployment for mobile users or remote networks and purchase a Clean Pipe license, you can add clean pipes to existing tenants; however, you must create separate template stacks, templates, and device groups that are specific to Clean Pipe.

#### STEP 1 | Make a note of the name of the tenants you will migrate to Clean Pipe.

You create templates, template stack, and device groups for each tenant to which you want to add clean pipes. Use the following naming conventions when you create them:

- The **Template Stack Name** must be `cp-stk-tenant`, where `tenant` is the tenant's name.
- The **Templates** name must be `cp-tpl-tenant`.
- The **Device Group Name** must be `cp-dg-tenant`.

#### STEP 2 | Add a template and configure a template stack for the tenant that you want to migrate to the clean pipe service.

1. In Panorama, select **Panorama > Templates**.
2. **Add** a template and give it a **Name** in the format `cp-tpl-tenant`, where `tenant` is the tenant's name.

![Template](image)

3. **Add Stack** and give it a **Name** in the format `cp-stk-tenant`, where `tenant` is the tenant's name, then **Add** the service connection template you just created to this template stack.
STEP 3 | **Add a device group** for the tenant that you want to migrate to clean pipe.

1. Select **Panorama > Device Groups**, then click **Add**.
2. **Add** a device group and give it a **Name** in the format `cp-dg-tenant`, where `tenant` is the tenant’s name.
STEP 4 | Commit your changes locally to make them active in Panorama.

STEP 5 | Apply the template stack, template, and device groups you created to the existing tenant.

1. Select the existing tenant from the Tenant drop-down.
2. Select Panorama > Cloud Services > Configuration > Clean Pipe.
3. Click the gear icon to the right of the Settings area to edit the settings.
4. Select the Template Stack Name, Templates, and Device Group Name that you created; then, click OK.
5. Make sure that the Parent Device Group is set to Shared.

![Settings Screen](image)

STEP 6 | Onboard a new Clean Pipe for the existing tenant.

STEP 7 | *(Optional)* Create additional Clean Pipe instances for the tenant as required by competing Step 6.

Be sure that each additional Clean Pipe uses a different location.

STEP 8 | Commit your changes locally to make them active in Panorama..
STEP 9 | Commit and push your changes to make them active in Prisma Access.

STEP 10 | Check that your Clean Pipe has been provisioned.

STEP 11 | 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.

STEP 12 | Complete the Clean Pipe configuration.

STEP 13 | *(Optional)* Associate more tenants and add more clean pipes by completing Steps 2 through 12.