Prisma Access Administrator's Guide (Cloud Managed)

paloaltonetworks.com/documentation

techDOCS paloalto NETWORKS

Contact Information

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

About the Documentation

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

Copyright

Last Revised

October 15, 2019

Table of Contents

Get Started with Prisma Access

Prisma Access helps you deliver consistent security to your remote networks and mobile users. All your users, whether at your headquarters, branch offices, or on the road, connect to Prisma Access to safely use cloud and data center applications as well as the internet. Prisma Access delivers protection at scale with global coverage so you don’t have to worry about things like sizing and deploying firewalls at your branches, or building out and managing appliances in collocation facilities. Palo Alto Networks provides two ways to deploy and manage Prisma Access:

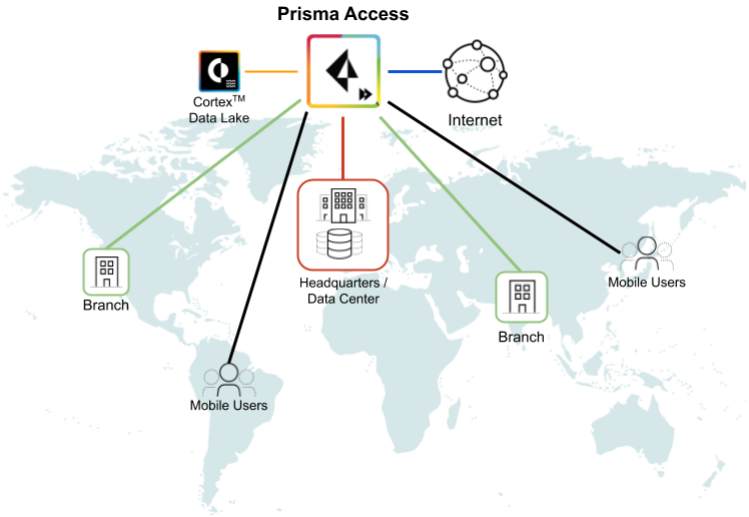
Panorama Managed Prisma Access—If you are already using Panorama to manage your next-gen firewalls, you can deploy Prisma Access with Panorama management to leverage you existing configurations.

Cloud Managed Prisma Access—If you don't have Panorama or if you just want a simplified onboarding and management experience for Prisma Access, use the Prisma Access app on the hub to quickly and easily enable internet access for your Prisma Access users, and then extend connectivity into your HQ, data center, and branch networks.

Prisma Access

To keep your applications and data safe, you must secure all users at all locations all the time. But how do you do this when your footprint is expanding globally, more and more of your users are mobile, and your applications and data are moving out of your network and into the cloud? Prisma Access enables this consistent security by safely enabling your users to access cloud and data center applications as well as the internet whether they are at your headquarters, branch offices, or on the road. Prisma Access consistently inspects all traffic across all ports, enabling secure access to the internet, as well as to your sanctioned SaaS applications, public cloud environments, and data centers and headquarters. Because Prisma Access leverages the next-generation firewall capability, threat prevention, malware prevention, URL filtering, SSL decryption, and application-based policy capabilities are built-in to provide you with the same level of security no matter where your users are or what resources they are accessing. All Prisma Access logs are stored in the Cortex Data Lake, providing centralized analysis, reporting, and forensics across all users, applications, and locations.

Prisma Access delivers protection at scale with global coverage so you don't have to worry about things like sizing and deploying hardware firewalls at your branches or building out and managing appliances in collocation facilities. Prisma Access provides the network infrastructure to connect all of your remote branches, your headquarter sites, data centers, and mobile users without requiring you to build out your own global security infrastructure and expand your operational capacity.



With the Prisma Access, Palo Alto Networks deploys and manages the security infrastructure globally based on what you have licensed:

- **Prisma Access for networks**—Secures traffic to and from your branch offices to the internet, other branches, and to your headquarters and data centers over an IPSec tunnel. You can use any router, SD-WAN edge device, or firewall that supports IPSec to connect your remote networks to Prisma Access. Prisma Access then implements a full-mesh VPN within the security overlay, eliminating the complexity and operational overhead normally associated with branch-to-branch networking. You license Prisma Access for networks based on the total bandwidth you need across all sites. You can then allocate the specific amounts of bandwidth you need at each site.
- **Prisma Access for users**—Provides consistent security for your mobile users whether they are accessing applications at your data center, using SaaS applications, or browsing the internet. You can deploy the GlobalProtect app to your users (available for smartphones, tablets, or laptops running Microsoft Windows, Apple macOS and iOS, Android, Google Chrome OS, and Linux) so that they can tunnel the traffic to Prisma Access for policy enforcement and threat prevention. The GlobalProtect app also provides host information profile (HIP) reporting so that you can create granular policies based on device

state to ensure that endpoints adhere to your security standards—for example, they are equipped with the most up-to-date patches, encryption, and virus definitions—in order to access your most sensitive applications. Or, to enable secure access to users on unmanaged devices, you can enable Clientless VPN. Prisma Access dynamically scales in and out per region based on where your users are at the moment. You license Prisma Access for Users based on the number of users.

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 branches and mobile users, create policies, query logs, and generate reports.

Decide How You Want to Manage Prisma Access

There are two ways you can manage Prisma Access, but you cannot switch between the management interfaces after you activate your Prisma Access license. Therefore, you must decide how you want to manage Prisma Access before begin setting up the product:

- **Panorama Managed Prisma Access**—Use the Cloud Services plugin on Panorama to set up and manage Prisma Access. This is a good option if you are already using Panorama to manage next-generation firewalls and you have common policy that you want to leverage for access to your corporate applications.
- **Cloud Managed Prisma Access**—Use the Prisma Access app on the Palo Alto Networks hub to quickly onboard branches and mobile users through task-driven workflows that allow you to set up and test your environment in minutes. Cloud Managed Prisma Access simplifies the onboarding process by providing predefined internet access and decryption policy rules based on best practices. Quickly set up IPSec tunnels using defaults suitable for the most common IPSec-capable devices and turn on SSL decryption for recommended URL categories.

There are some differences between what is supported on Panorama Managed Prisma Access and Cloud Managed Prisma Access. For a list of feature support in Panorama Managed Prisma Access and Cloud Managed Prisma Access, refer to the compatibility matrix.

After you decide which management option you want to use, get started by following the licensing and activation workflow for you option you have selected:

- To get started with Panorama Managed Prisma Access, perform license activation from the customer support portal (CSP) and install the Cloud Services plugin on Panorama.
- To get started with Cloud Managed Prisma Access, perform license activation from the hub.

License and Activate Prisma Access

Prisma Access provides a flexible licensing scheme so that you can purchase just what you need to secure your remote networks and/or mobile users. In addition, Prisma Access logs to the Cortex Data Lake, so you must deploy Cortex Data Lake before you can proceed with licensing Prisma Access.

Prisma Access Licenses

The following Prisma Access licensing options are available:

- **Prisma Access for networks**—To license Prisma Access for networks, you purchase a bandwidth pool, which you can divide among each 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.

  A remote network's bandwidth speed is enforced equally in both directions. 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.
- **Prisma Access for users**—You license Prisma Access for users based on number of users, with tiers from 200 users to more than 100,000 users. Prisma Access for Users requires the GlobalProtect app on each supported endpoint. You can also enable support for unmanaged devices through Clientless VPN. 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.
- **Service Connections**—The Prisma Access license includes the option to establish service connections that enable connectivity to resources in your headquarters and/or data center locations. The number of service connections you can add depends on your license:
  - If you purchase a Prisma Access for Networks, or if you purchase licenses for both Prisma Access for networks and Prisma Access for users, you can add up to 100 service connections to enable access to services and applications at your corporate network locations. You can add up to three service connections with no license cost; each connection after the third uses 300 Mbps from your licensed remote network bandwidth pool. Prisma Access does not limit the bandwidth over these connections.
  - If you purchase a Prisma Access for users license only, you can establish service connections to up to three of your headquarters or data center sites.

After you purchase your license(s), you will receive an email from Palo Alto Networks order fulfillment with the auth code(s) to Activate Prisma Access.

Activate Prisma Access

To activate Prisma Access you must have the auth codes for the license(s) you purchased. For Cloud Managed Prisma Access, you perform activation from the Palo Alto Networks hub.

The instructions here are for activating Cloud Managed Prisma Access. If you need to license Prisma Access with Panorama Management, follow the instructions for licensing Prisma Access from the Customer Support Portal (CSP).

Before you activate your Prisma Access auth codes, make sure you have done the following:

- Make sure you have a CSP account and you are assigned the roles you need to administer Prisma Access. If you do not already have a CSP account, go to the Customer Support Portal to **Create my account**. When prompted, enter **Your Email Address** to associate with the CSP account and **Submit** to create your account. You can then configure the roles you need to set up Cortex Data Lake and Prisma Access.
- If you don't already have an instance of Cortex Data Like, you must purchase a license before you begin. Because Prisma Access logs to the Cortex Data Lake, you must have a valid license. During the Prisma Access activation, you can associate the Prisma Access instance with an existing Cortex Data Lake instance, or activate a new instance using an auth code.

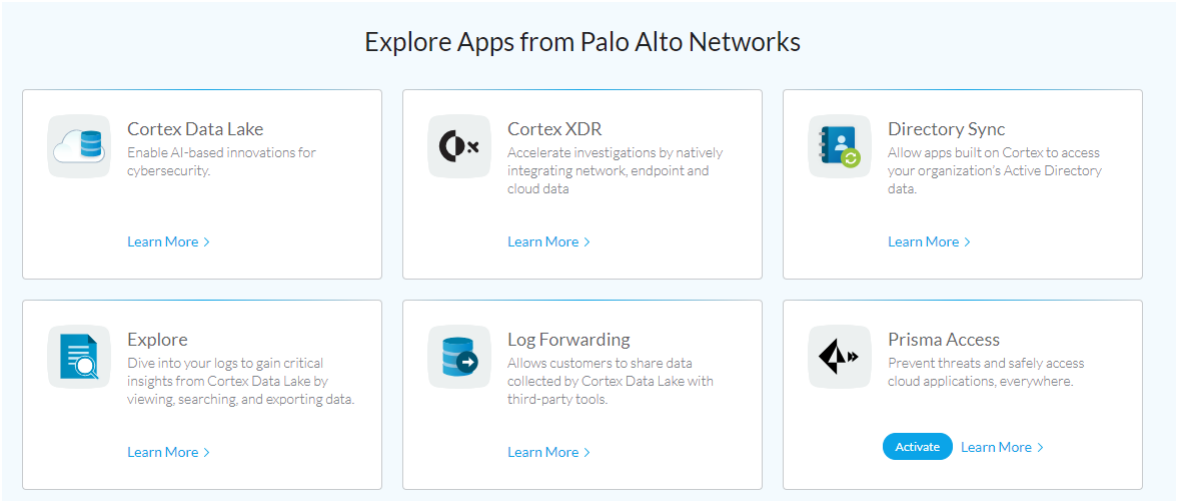
STEP 1 | **Sign In** to the hub.

You can access the hub only if you have a Palo Alto Networks CSP account and are assigned the appropriate role. To configure and manage Cloud Managed Prisma Access, you need have the App Administrator role.

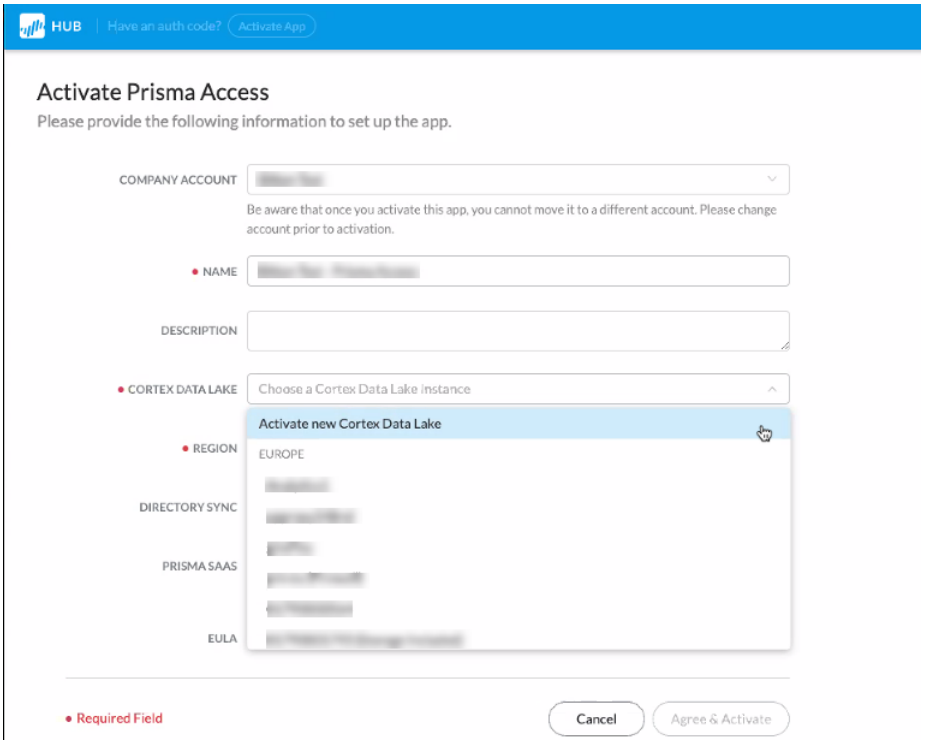
STEP 2 | Activate the Prisma Access app.

Before you can activate Prisma Access for users or Prisma Access for networks, you must activate an instance of the Prisma Access app on the hub.

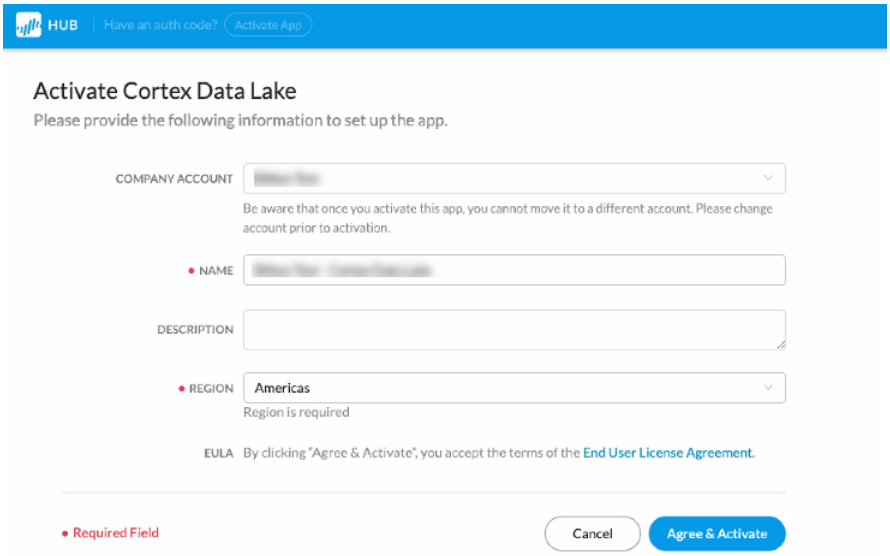
1. From the hub home page, **Activate** Prisma Access in the Explore Apps from Palo Alto Networks area.



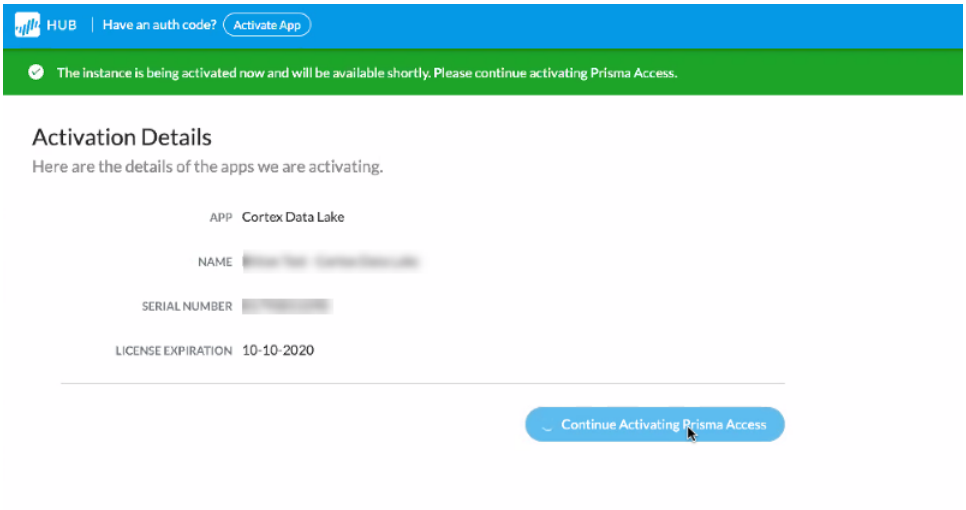
2. Enter an **Instance Name** to identify the Prisma Access app instance.
3. (Optional) Enter a brief **Description** of the Prisma Access app instance.
4. Select the **Cortex Data Lake** instance that you want to associate with your Prisma Access app instance or select **Activate new Cortex Data Lake**.



If you are activating a new Cortex Data Lake instance, enter the auth code when prompted and then enter a **Name** for the instance, select the **Region** in which to deploy Cortex Data Lake, and then **Agree and Activate**.



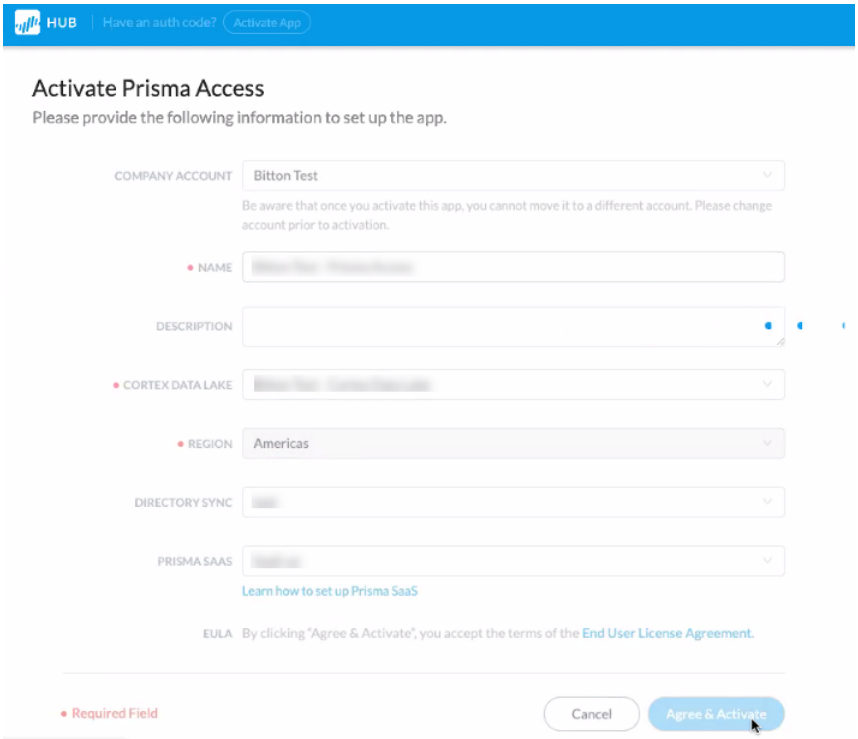
When the Cortex Data Lake activation completes successfully, click **Continue Activating Prisma Access**.



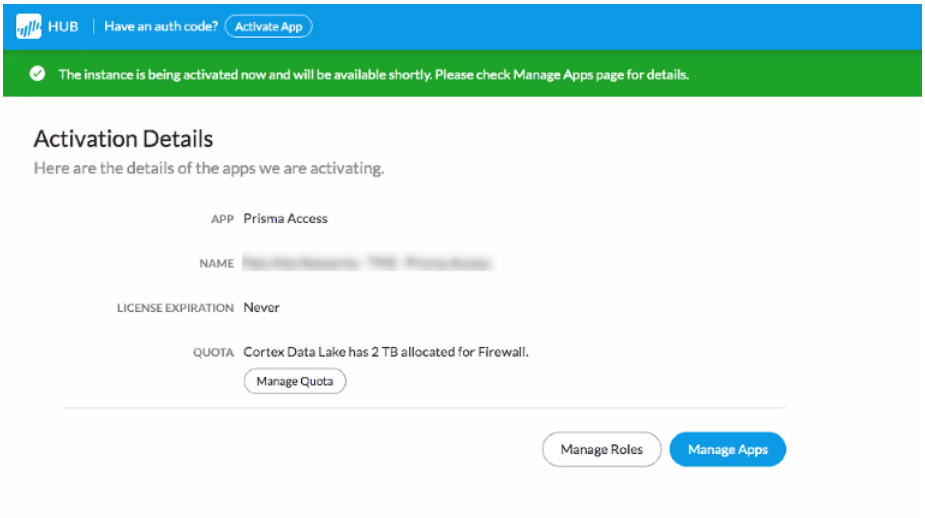
5. Select the **Region** where you want to host the Prisma Access app instance.

   Americas is currently the only region supported for the Prisma Access app instance.
6. (Optional) If you plan to integrate Prisma Access with Prisma SaaS for clientless VPN authentication support, select your **Prisma SaaS** instance.

   Directory Sync is currently not supported so you do not need to select an instance.
7. To activate the Prisma Access cloud management app, **Agree and Activate**.

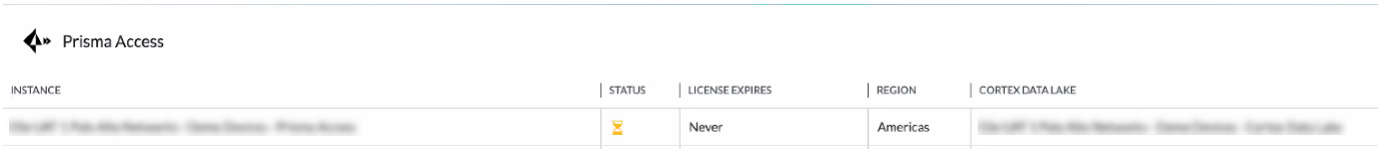


8. When the app instance successfully activates, go to **Manage Apps**.

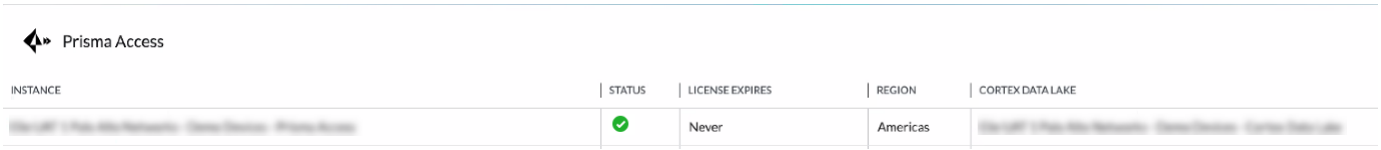


It takes up to seven minutes to deploy the Prisma Access cloud management instance. You must wait until the Prisma Access instance is up and running before you continue to activate your Prisma Access for networks and/or Prisma Access for users licenses.

Verify the Status of your Prisma Access app instance. While the cloud management instance is provisioning, the **Status** shows an hourglass icon.



After provisioning finishes, the **Status** changes to a green check mark.

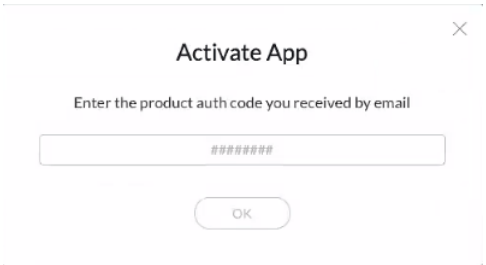


STEP 3 | Activate your Prisma Access for users or Prisma Access for networks license.

After the Prisma Access app instance finishes provisioning, you can activate your Prisma Access licenses.

1. Click on the hub icon to go back to the hub and then click **Activate App**.

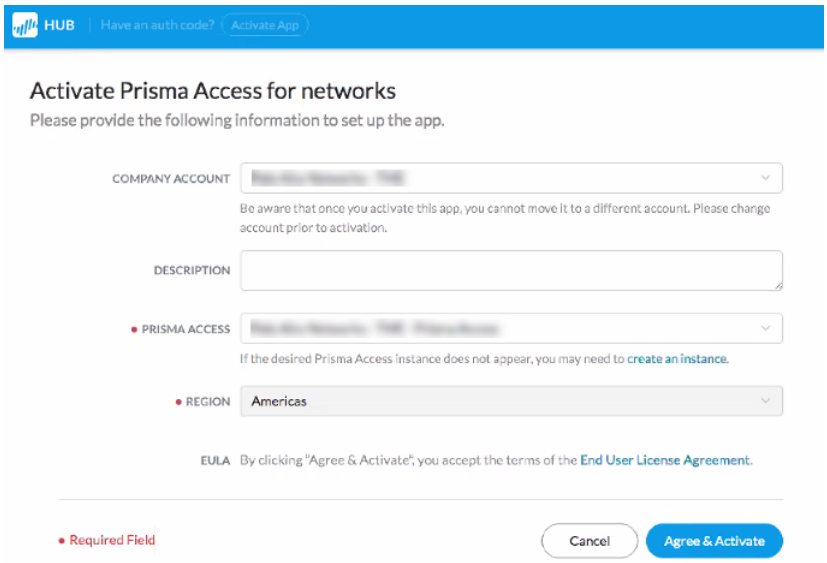
2. **Enter the product auth code you received by email** from Palo Alto Networks order fulfillment and then click **OK**.



3. Configure the following settings for your Prisma Access for users or Prisma Access for networks license:

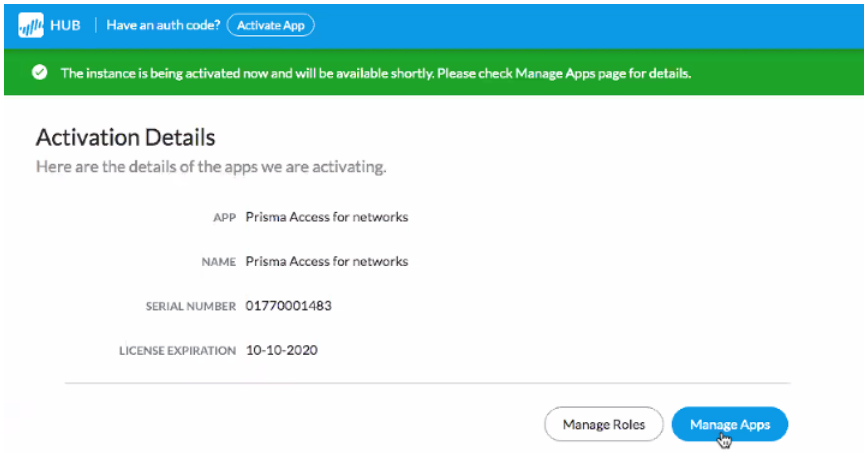
1. (Optional) Enter a brief **Description** of the Prisma Access license.
2. Select the **Region** where you are hosting your Prisma Access app instance.

   Americas is the only supported region currently.
3. Select the **Prisma Access** app instance that you want to associate with this license.



4. **Agree and Activate** to complete activation.

   A green banner displays when activation completes successfully. You can either add a second license, or click **Manage Apps** to verify your licenses.



STEP 4 | (Optional) Add a second license to your Prisma Access app instance.

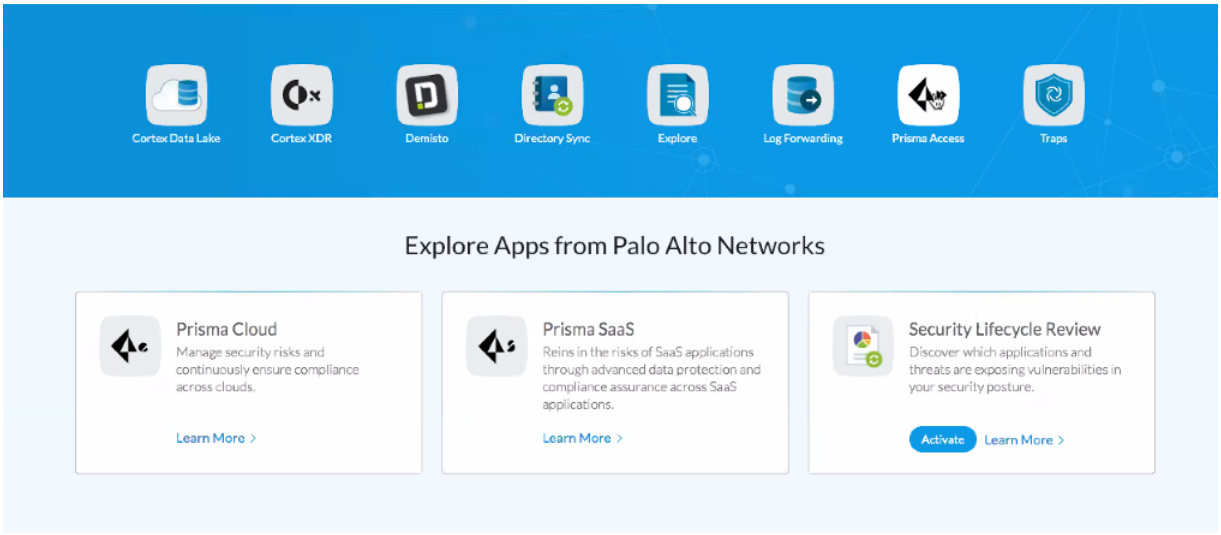
If you purchased both Prisma Access for networks and Prisma Access for users, repeat step 3 to activate the second license. When you finish activating the second license, click **Manage Apps** to verify your licenses

STEP 5 | Verify your licenses.

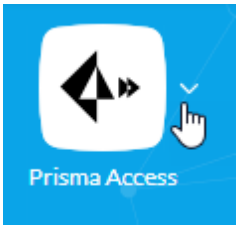
1. From the manage apps page, verify that you see your licenses associated with your Prisma Access app instance:

2. Go back to the hub home page.

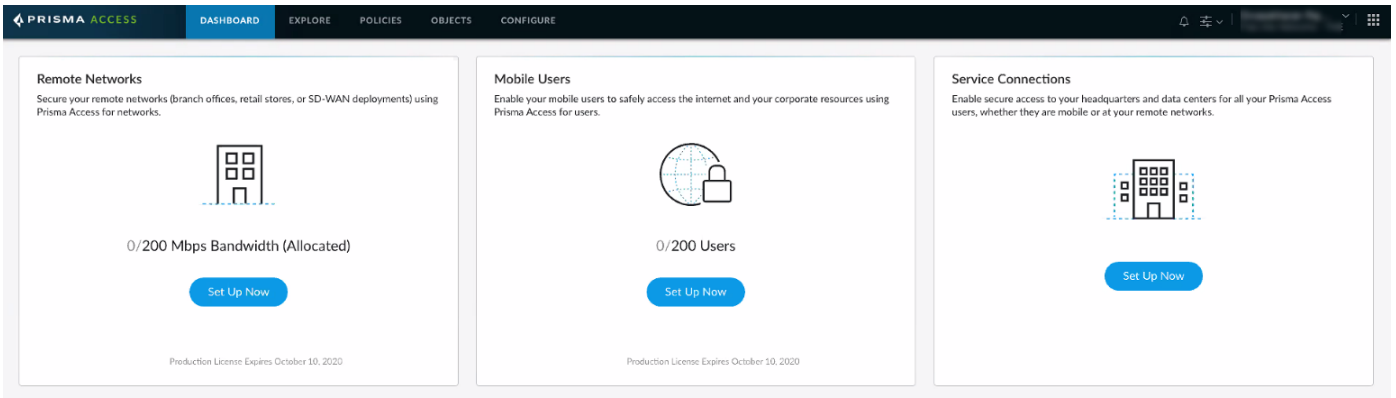
   Prisma Access now shows up on the hub as one of your apps.



   Click on the Prisma Access icon on the hub to launch the app.



3. Verify that the Remote Networks and/or Mobile Users tiles on the **Dashboard** show the correct amount of bandwidth and/or number of users that you licensed.



STEP 6 | Follow the next steps for getting started with Prisma Access:

- ❑ Set Up the Prisma Access for Users Environment.

- Onboard a Remote Network.
- Customize the Predefined Internet Access Security Rules.

Secure Mobile Users with Prisma Access

Securing mobile users from threats is often a complex mix of security and IT infrastructure procurement and setup, bandwidth and uptime requirements in multiple locations throughout the world, while staying within budget. With Prisma Access for users, the entire infrastructure is deployed for you and scales based on the number of active users and their locations. Users can then connect to Prisma Access—using the GlobalProtect app or Clientless VPN—for consistent security policy enforcement even in locations where you do not have a network infrastructure and IT presence.

- Set Up the Prisma Access for Users Environment
- Customize the Mobile User Environment
- Enable Mobile User Authentication for Prisma Access
- Enable SSL Decryption for Mobile User Traffic
- Configure Clientless VPN for Prisma Access
- Enable Mobile Users to Access Corporate Resources Using Service Connections
- Verify and Save Your Mobile User Configuration
- Manage Your Mobile User Configuration
- Monitor the Mobile User Status

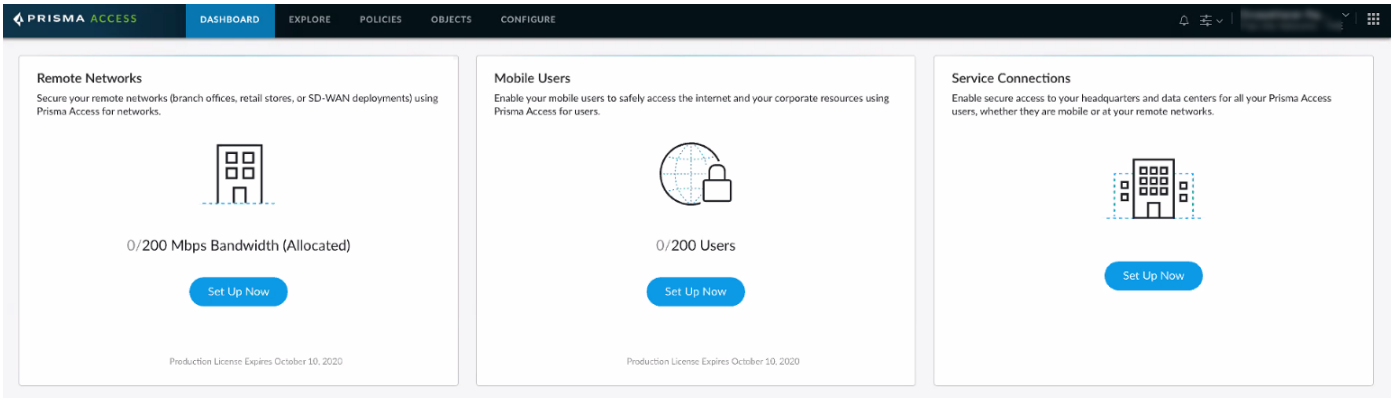
Set Up the Prisma Access for Users Environment

To set up the Prisma Access for users environment you simply need to select the locations and the address for your mobile users to connect to and create some temporary test user accounts. Prisma Access uses this information to provision your mobile user environment. The Prisma Access environment provides predefined security policy rules based on best practices. These rules allow you to securely browse to general internet sites. Review and update these default rules to meet your enterprise needs. After you do this, use your temporary test user accounts to verify that the service is functioning as expected, and that the policy rules are being enforced as expected.

When you initially set up your mobile users environment, Prisma Access requires only the minimal settings required to get the environment provisioned so that you can test it. After you finish testing the environment to make sure it is functioning as expected, you can go back into the environment setup and customize it. For example, if you would prefer to use your company domain in the portal address, you can change the address after environment setup.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | If you are performing a first-time configuration of Prisma Access for users, click **Set Up Now** from the Mobile Users widget on the **Dashboard**. Otherwise select **Configure** > **Mobile Users**.



STEP 3 | Enter a **Portal Address** that mobile users will use to connect to Prisma Access.

Prisma Access uses the address you provide to establish the fully qualified domain name for the Prisma Access for users deployment and publishes it to public domain servers. For example, if you set the GlobalProtect portal address to *acme*, Prisma Access creates a FQDN for acme.gpcloudservice.com and publishes it to public DNS servers. You must use this default domain for initial environment setup. You can come back after your test the environment and customize the portal address to use your company domain.

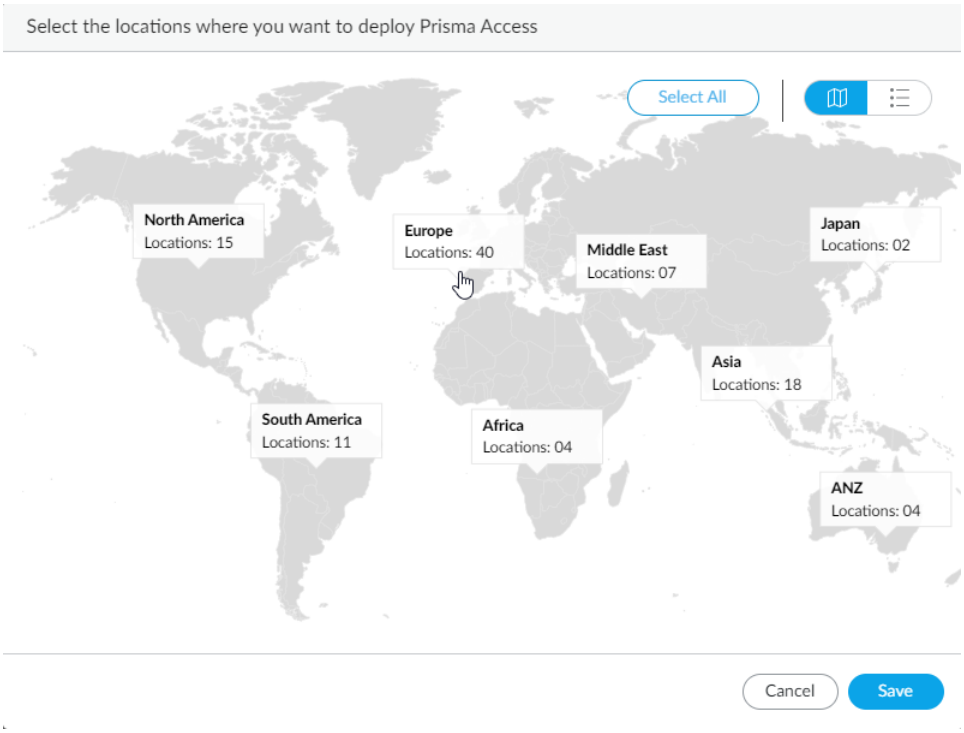
If you want to use your company domain in the portal address instead of the default domain, you can come back and customize the portal address after the provisioning completes successfully.

STEP 4 | Select the **Locations** where you want to deploy Prisma Access for users.

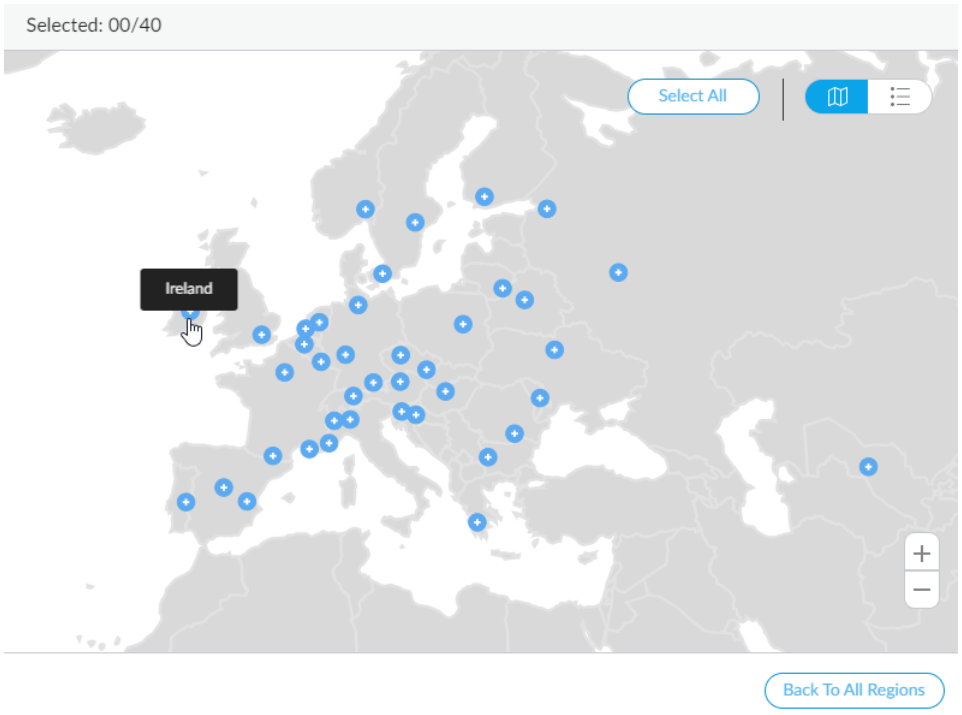
1. Click **Add** to see the list of available regions.

The map displays the global regions where you can deploy Prisma Access for users: North America, South America, Europe, Africa, Middle East, Asia, Japan, and ANZ (Australia and New Zealand). In addition, Prisma Access provides multiple locations within each region to ensure that your users can connect to a location that provides a user experience tailored to the users' locale. For the best performance, **Select All**. Alternatively, select the specific locations within each selected region where your users will need access. By limiting your deployment to a single region, you can have more granular control over your deployed regions and exclude regions required by your policy or industry regulations.

For the best user experience, if you are limiting the number of locations, 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, choose a location that is closest to your users for the best performance.



2. **Select All** to deploy Prisma Access in all available regions and locations or select a specific region.
3. To select specific location within the region, click the corresponding to add a location or click **Select All** to select all locations within the region.



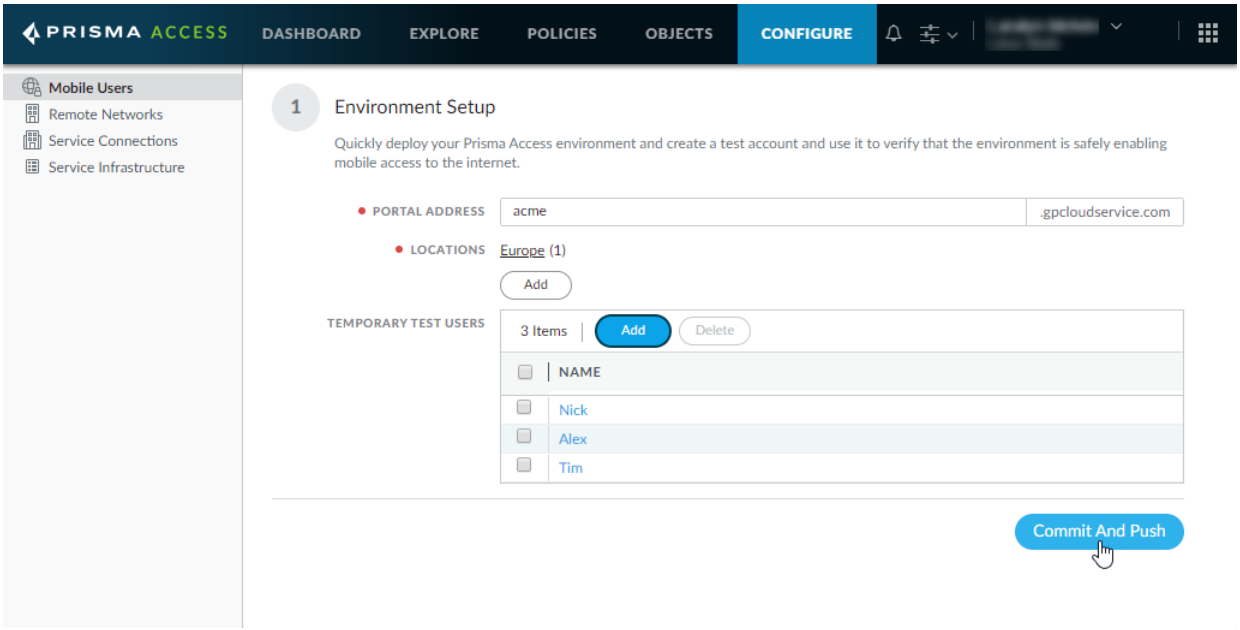
4. Click **Back to All Regions** and then either add additional regions and locations or **Save** your selections.

STEP 5 | **Add** the **Temporary Test Users** that you want to use to test your Prisma Access for users environment.

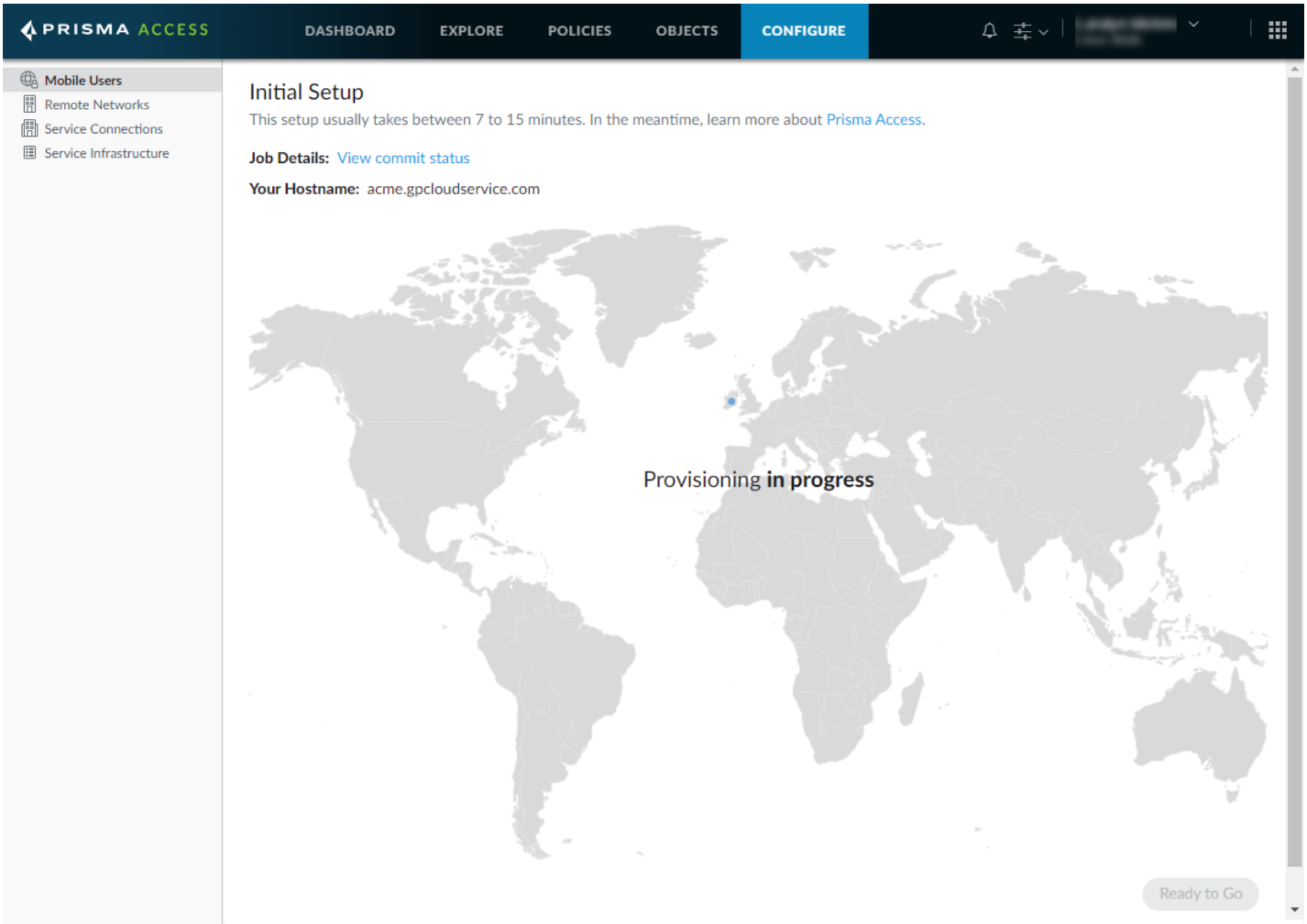
1. Enter a **Name** to identify the test user.
2. Create a **Password** for the test user account and then **Confirm Password**.
3. **Save** your test user account.

The Prisma Access temporary test users should only be used for initial testing of the environment.

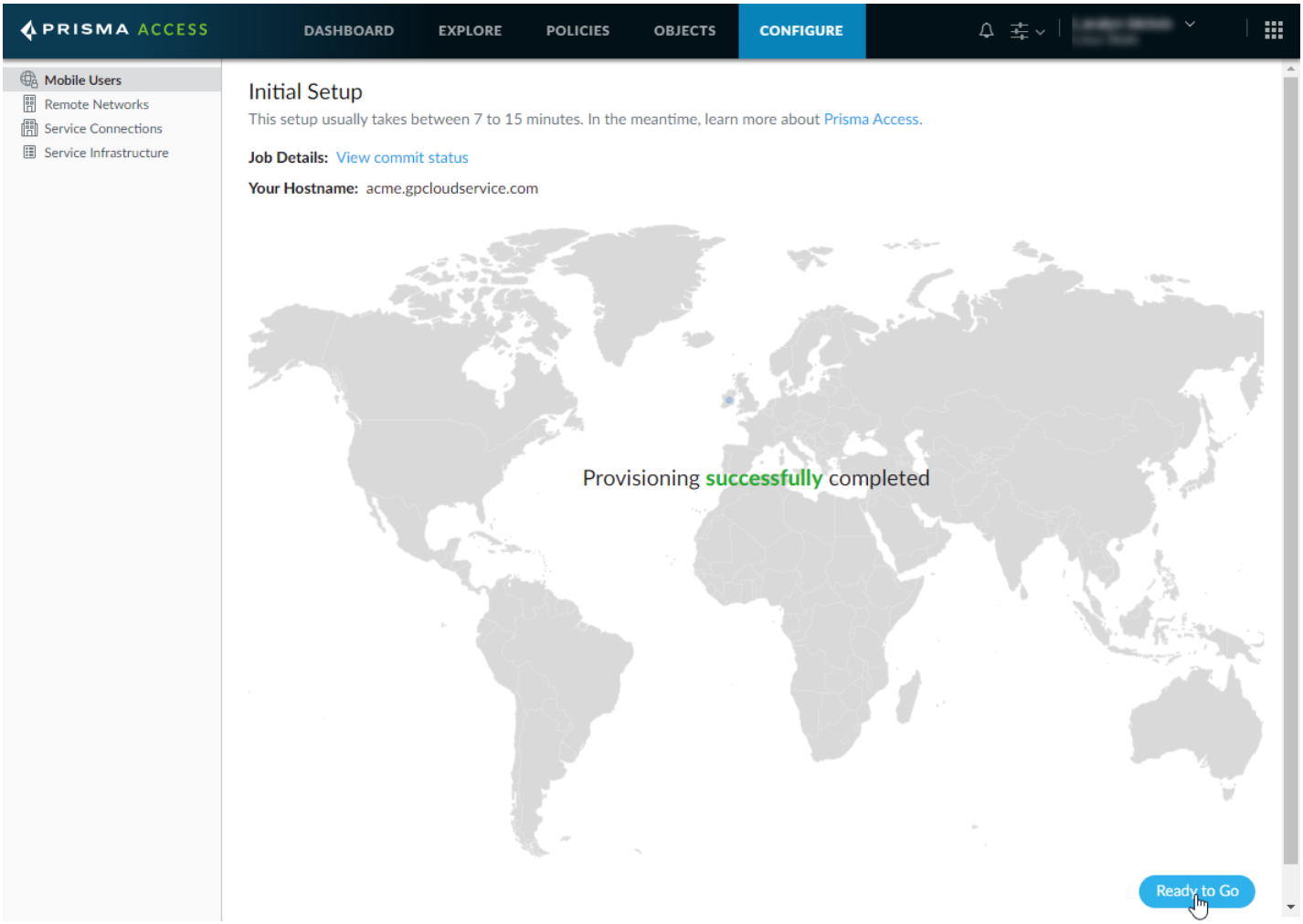
STEP 6 | **Commit and Push** the configuration.



Prisma Access begins provisioning your mobile user environment. The provisioning process can take up to 15 minutes. The map shows a blinking blue dot in the locations where your mobile user environment is being provisioned.



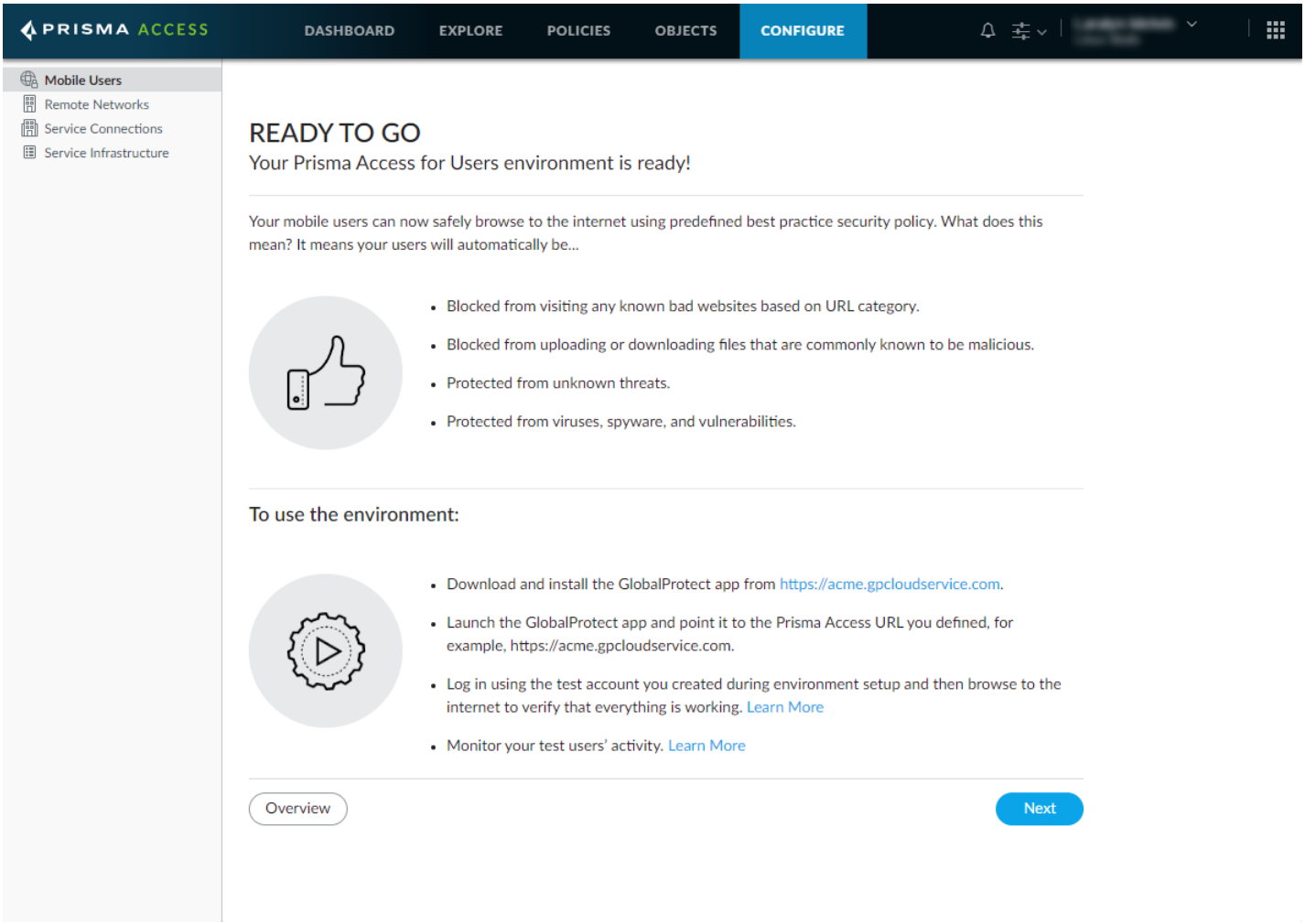
STEP 7 | After provisioning completes, click **Ready to Go**.



STEP 8 | Have your temporary test users test the environment by following the instructions on the screen.

1. Download the GlobalProtect app from the portal address you defined (for example, acme.gpcloudservicecom).
2. Install the GlobalProtect app on your endpoint.

   The GlobalProtect app installation requires administrative rights on the endpoint.
3. Connect to GlobalProtect using your test account credentials.
4. After you connect to GlobalProtect successfully, browse to a public internet website to verify that your mobile user environment is working and that the predefined best practice security policy is enforcing traffic as expected.
5. Monitor test account activity on the Prisma Access **Explore** page.

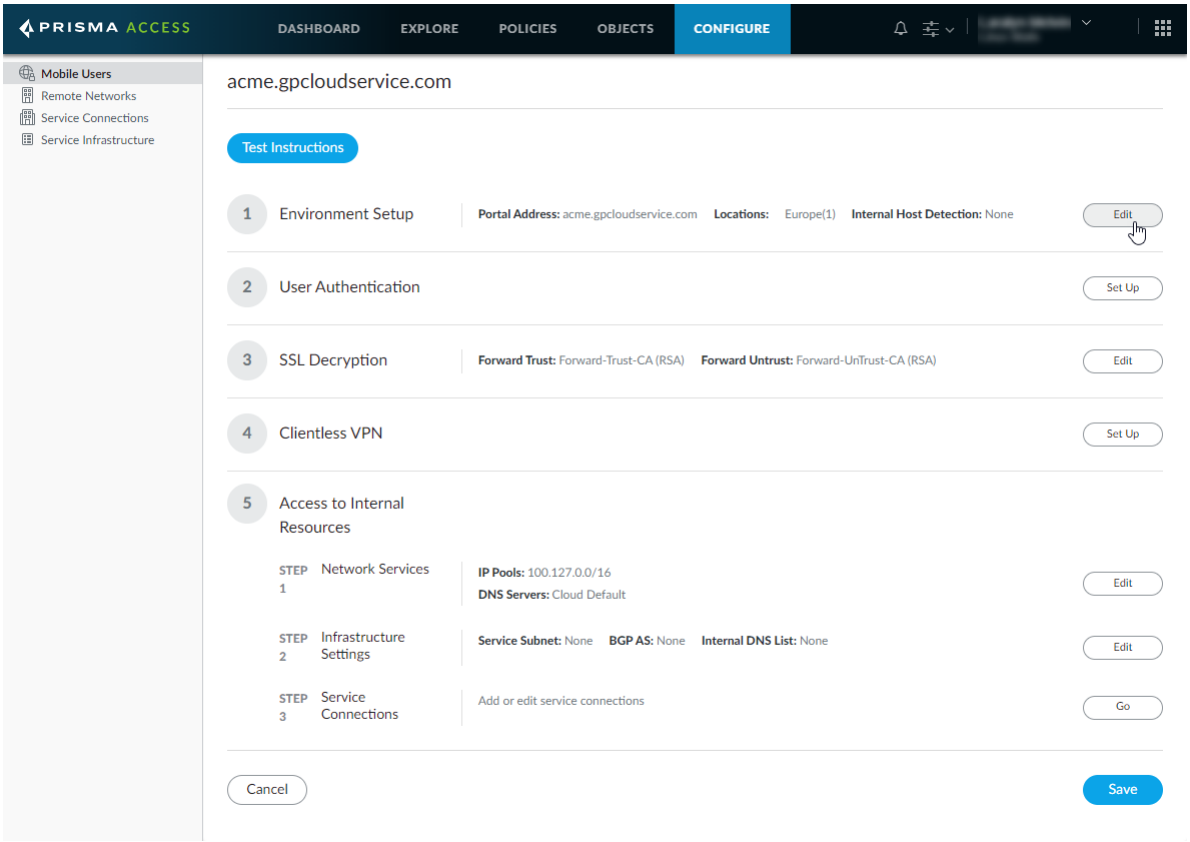


STEP 9 | After you verify that the environment is provisioned properly and that your security policy rules are enforcing traffic as expected, your mobile users can start using the service for general web browsing.

1. If you want to change the portal address to which your mobile users connect to use your company domain name, you can Customize the Mobile User Environment.
2. Customize the Predefined Internet Access Security Rules for your environment or create additional security policy rules.
3. Proceed to Enable Mobile User Authentication for Prisma Access.
4. After your environment is set up the way you want it and you have configured authentication, direct your mobile users to your Prisma Access URL to download the GlobalProtect app.

Customize the Mobile User Environment

When you initially set up your mobile users environment, Prisma Access requires only the minimal settings required to get the environment provisioned so that you can test it. After you finish testing the environment to make sure it is functioning as expected, you can go back into the environment setup and customize it. For example, if you would prefer to use your company domain in the portal address, you can change the address after environment setup. Similarly, if you want to customize how your mobile users connect when they are on your internal network, you can go back and set up internal host detection. To customize the environment after provisioning, **Edit** the Environment Setup from the mobile users configuration summary screen:



You can customize the environment settings at any time based on your enterprise needs:

- Customize the Prisma Access Portal Address
- Enable Internal Host Detection

Customize the Prisma Access Portal Address

By default, Prisma Access uses the *gpcloudservice.com* domain to set up the Prisma Access portal address that your mobile users will need to connect to for secure access to the internet and your HQ and data centers. You must use this default domain when you initially set up and test your environment. If you want to customize the domain name after the initial setup to use your company domain, you can go back and edit the environment settings so that the portal address your users connect to contains your own company domain (for example, prisma-access.acme.com).

To configure Prisma Access to use your own domain, you must:

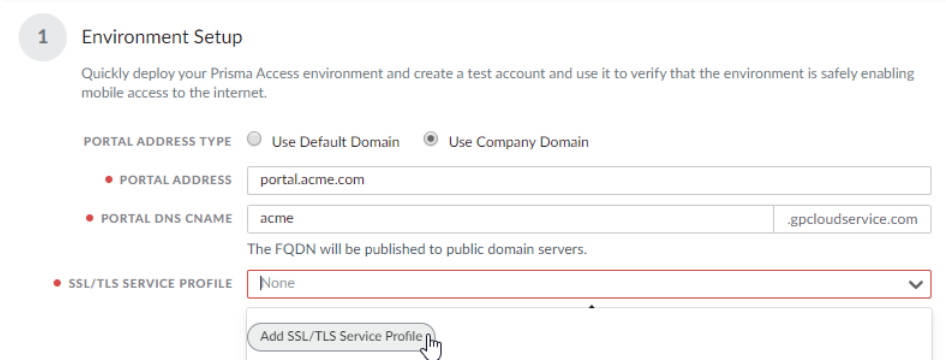
- Obtain certificates for the service.
- Create a DNS CNAME entry on your DNS servers that maps the default portal address using the default domain to the custom portal address that uses your company domain. You need to do this because Prisma Access publishes the portal address you set up to public domain servers during initial provisioning.

STEP 1 | Set the **Portal Address Type** to **Use Company Domain**.

STEP 2 | Enter the fully qualified **Portal Address** you want your mobile users to connect to.

STEP 3 | Enter the **Portal DNS CNAME** to which to map your DNS server entries.

STEP 4 | Click **Add SSL/TLS Service Profile** from the **SSL/TLS Service Profile** drop down.



STEP 5 | Enter a **Name** for the SSL/TLS profile.

STEP 6 | **Import** the **Certificate** you provisioned for your custom domain portal address.

1. Enter the **Certificate Name** and click **Choose File** to upload the **Certificate Fie**.
2. Select the certificate **Format** for the certificate you are importing:
   - **Encrypted Private Key and Certificate (PKCS12)**—The key and certificate are in a single container (Certificate File). Click **Choose File** and browse to the PKCS12 file to import.
   - **Base64 Encoded Certificate (PEM)**—If you select this option, you must import the **Key File** separately from the certificate. To import the PEM certificate and Key File, click **Choose File**.
3. Enter the **Passphrase** to encrypt the key and **Confirm Passphrase** and then click **Save**.

STEP 7 | Define the range of SSL/TLS protocols to allow to connect to Prisma Access:

1. For **Min Version**, select the earliest allowed TLS version (TLSv1.0 is the default).
2. For **Max Version**, select the latest allowed SSL/TLS version.

As a best practice, set the Min Version to TLSv1.2 and the Max Version to Max.

STEP 8 | **Save** the configuration.

STEP 9 | If you have not already done so, configure your DNS servers to point to the Prisma Access DNS CNAME you defined.

STEP 10 | **Save** the environment setup and **Commit and Push** the updated settings.

Enable Internal Host Detection

If you do not require your mobile users to connect to Prisma Access when they are on the internal network, enable internal host detection to enable the GlobalProtect app to determine if it is on an internal or external network.

STEP 1 | Enable **Internal Host Detection**.

STEP 2 | Enter the **IP Address** of a host that can be resolved from the internal network only.

STEP 3 | Enter the DNS **Hostname** that resolves to the IP address you enter.

When a mobile user connects to Prisma Access, the GlobalProtect app attempts to do a reverse DNS lookup on the specified address. If the lookup fails, the GlobalProtect app determines that it is on the external network and then initiates a connection to Prisma Access.

STEP 4 | **Save** the environment setup and **Commit and Push** the updated settings.

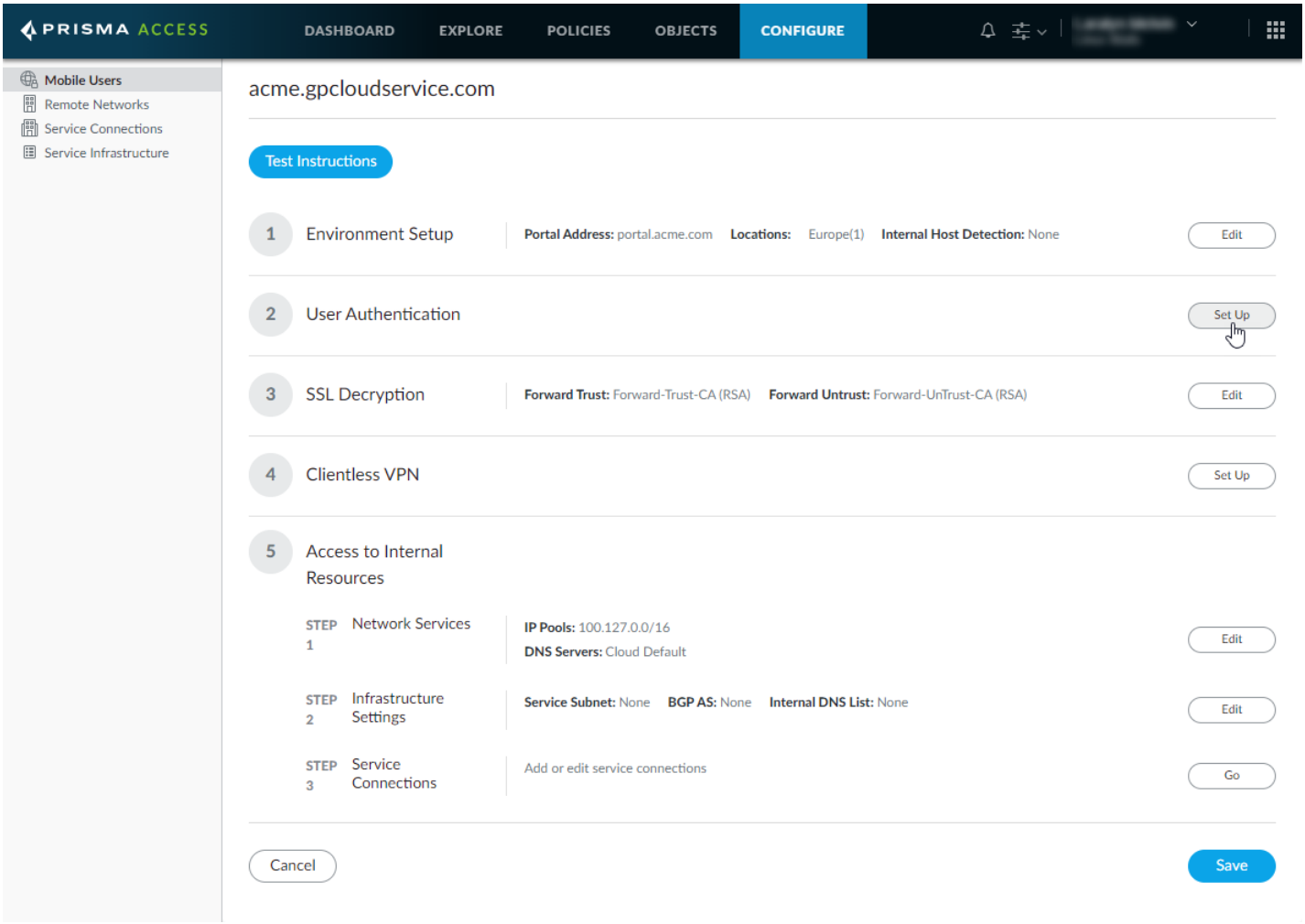
Enable Mobile User Authentication for Prisma Access

Prisma Access for users provides enterprise authentication using SAML. To configure SAML you must configure both your service provider (Prisma Access) and the SAML IdP (such as Okta or Active Directory Federation Services) that you are using with the information they will need to establish a trust relationship.

To establish a SAML trust relationship between Prisma Access (the SP) and your IdP, you will need to configure your IdP with information about Prisma Access, including the public certificate to use to authenticate SAML requests from Prisma Access, and the IP addresses of the Prisma Access portal and gateways. In addition, you will need to configure Prisma Access with information about where to send identity requests, how to validate the authenticity of SAML responses, and what mechanism to use to exchange SAML messages (called binding). If your IdP can export the metadata file that includes this information (as well as the IdP certificate), you can import it into Prisma Access. Otherwise you will need to gather this information from your IdP.

Use the following steps to configure Prisma Access to authenticate mobile users through SAML:

STEP 1 | From your Mobile Users configuration summary (**Configure** > **Mobile Users** > *<mobile-user-config>*), and **Set Up** User Authentication.

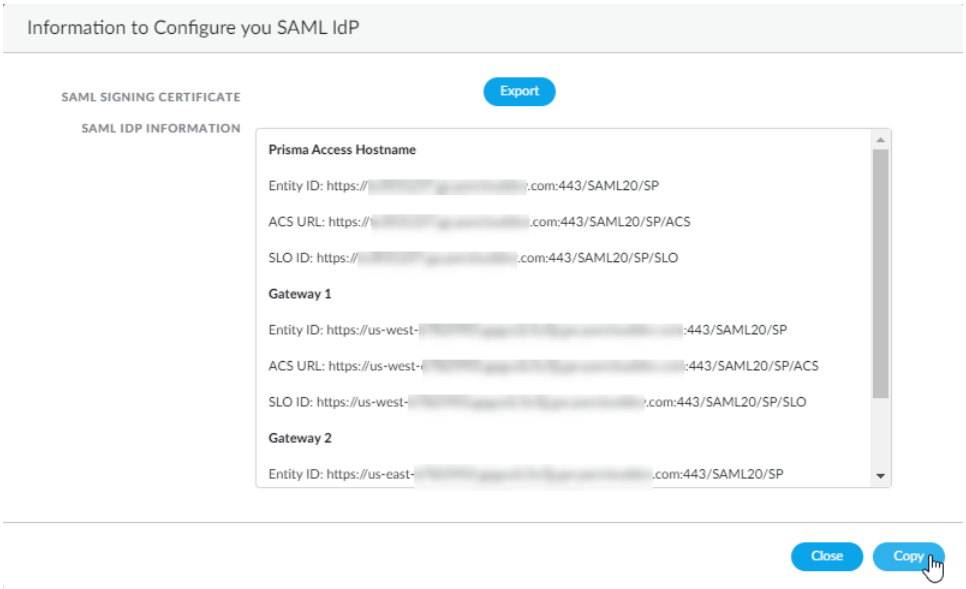


STEP 2 | Configure your IdP with the settings required to establish a trust relationship with Prisma Access (the SAML Service Provider, or SP).

1. (Optional) Specify the certificate for Prisma Access to use to sign SAML authentication messages.

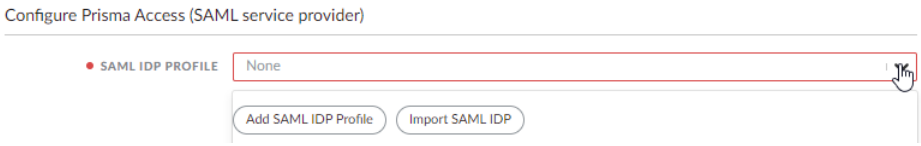
   you only need to select a certificate if you configure Prisma Access to **Sign SAML Messages to IdP** (see Step 2-10). You can select the default **SAML-Signing-Cert** or **Import** a certificate from your enterprise PKI or a trusted third-party CA.
2. To export the Prisma Access signing certificate so that you can import it onto your IdP, click **View Info** and then click **Export**.
3. **Copy** the information that you need to configure on your IdP and then go to your IdP and configure it with the information about Prisma Access.

   The steps for configuring your IdP to work with Prisma Access vary depending on what IdP you are using. If you are using Okta or Active Directory Federation Services, follow the steps in this guide. For other IdP vendors, follow the product documentation.



STEP 3 | Configure Prisma Access to work with your IdP.

There are two ways to configure the IdP settings: you can manually **Add SAML IdP Profile** or **Import SAML IdP** metadata file (which also includes the IdP certificate).



The IdP certificate is limited to the following algorithms:

- *Public key algorithms—RSA (1,024 bits or larger) and ECDSA (all sizes).*
- *Signature algorithms—SHA1, SHA256, SHA384, and SHA512.*

1. To import a metadata file that you exported from your IdP:
   1. Select **Import SAML IdP** from the **SAML IdP Profile** drop-down.
   2. Enter a **Profile Name** to identify the IdP.
   3. Click **Choose File** in the **SAML Metadata** field and browse to the metadata file you exported from your IdP.

4. Enter the **Maximum Time Difference (Seconds)** allowed between the IdP and Prisma Access to ensure successful validation of IdP messages (range is 1 to 900 seconds; default is 60 seconds). If the difference exceeds this value, authentication fails.
5. Click **Save**.

If you import a metadata file that specifies multiple SSO URLs and/or multiple SLO URLs, Prisma Access uses the first URL that specifies a POST or redirect binding method.

2. To manually create an IdP profile with details gathered from your IdP:
    1. Select **Add SAML IdP Profile** from the **SAML IdP Profile** drop-down.
    2. Enter a **Name** for the profile.
    3. Enter the **Identity Provider ID** that you retrieved from your IdP system.
    4. Select or **Import** the **Identity Provider Certificate** that the IdP uses to sign SAML authentication responses.

        Prisma Access uses the public key in the certificate to validate the authenticity of the SAML responses. To import the certificate:

        1. Enter the **Certificate Name**.
        2. Select **Choose File** to import the **Certificate File** for the certificate.
        3. **Save** the certificate settings.
    5. Enter the **Identity Provider SSO URL** that the IdP advertises for its single sign-on (SSO) service.
    6. (Not supported in this release) Enter the **Identity Provider SLO URL** that the IdP advertises for its single logout (SLO) service.
    7. Click **Save**.
    8. Select the **SAML HTTP Binding for SSO Requests to IdP** associated with the **Identity Provider SSO URL**.

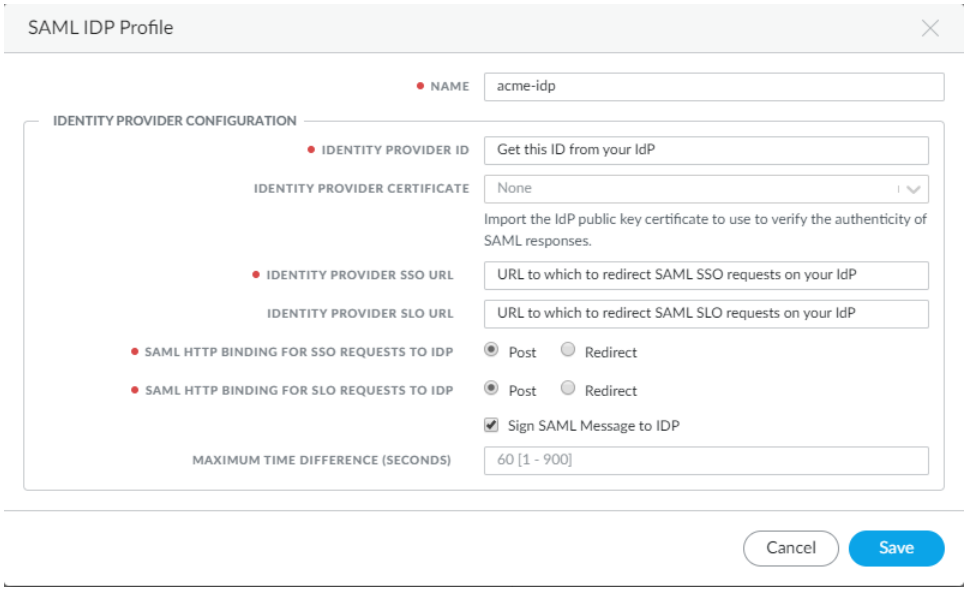
        Prisma Access uses this binding to send SAML messages to the IdP. The HTTP binding options are:

        - **POST**—Prisma Access sends messages using base64-encoded HTML forms.
        - **Redirect**—Prisma Access sends base64-encoded and URL-encoded SSO messages within URL parameters.
    9. (Not supported in this release) Select the **SAML HTTP Binding for SLO Requests to IdP** associated with the **Identity Provider SLO URL**.

        Prisma Access uses this binding to send SAML messages to the IdP. The HTTP binding options are:

        - **POST**—The security processing node sends messages using base64-encoded HTML forms.
        - **Redirect**—The security processing node sends base64-encoded and URL-encoded SLO messages within URL parameters.
    10. Select **Sign SAML Message to IdP** to enable the security processing node to sign messages that it sends to the IdP.

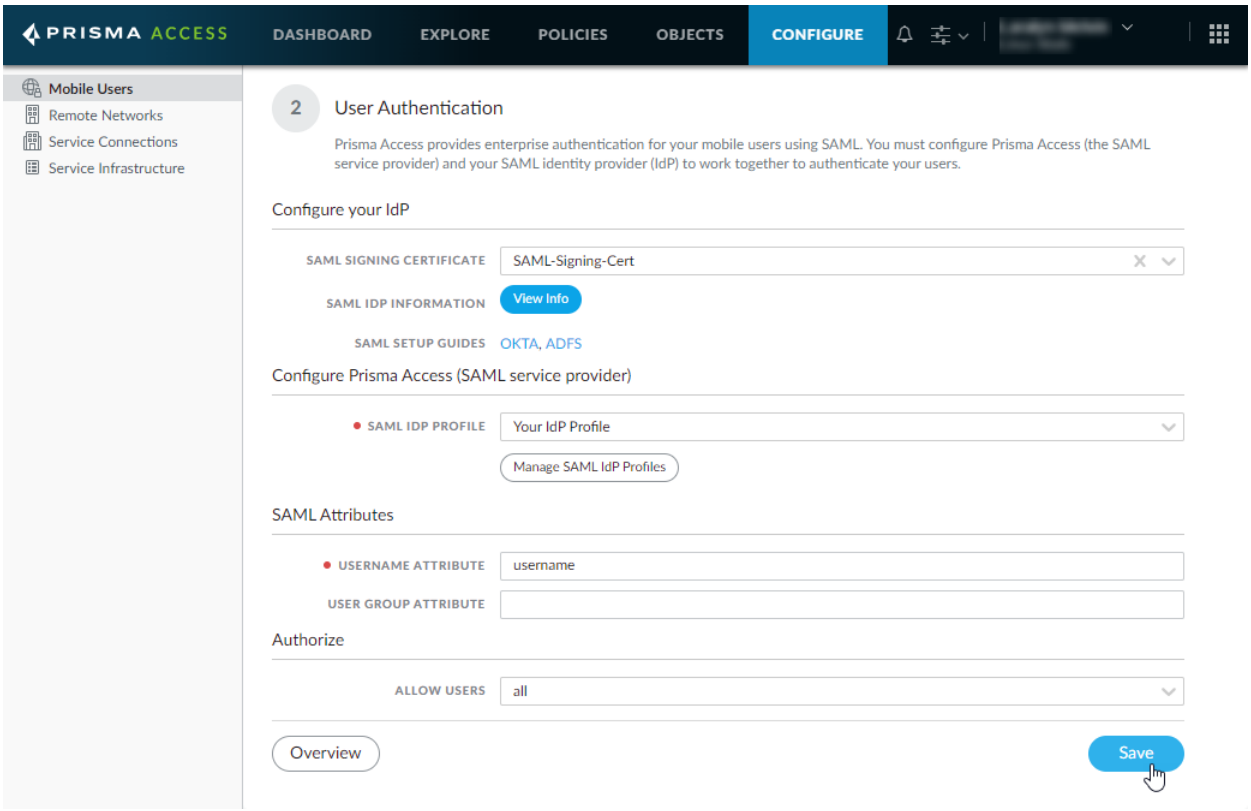
        If you enable this option, you must configure a **SAML Signing Certificate** (see Step 2-1).
    11. Enter the **Maximum Time Difference (Seconds)** allowed between the IdP and Prisma Access to ensure successful validation of IdP messages (range is 1 to 900 seconds; default is 60 seconds). If the difference exceeds this value, authentication fails.



12. **Save** your SAML IdP profile.

STEP 4 | (Optional) Enter the SAML **Username Attribute** that identities the username of an authenticating user in messages from the IdP (default is **`username`**).

STEP 5 | (Not supported in this release) Enter the SAML **User Group Attribute** that identities the user group of an authenticating user in messages from the IdP.



You do not need to add any Allow Users in this release of Prisma Access (Cloud Managed). By default, all users are allowed to authenticate.

STEP 6 | **Save** the settings.

Configure SAML Authentication Using Okta as the IdP for Mobile Users

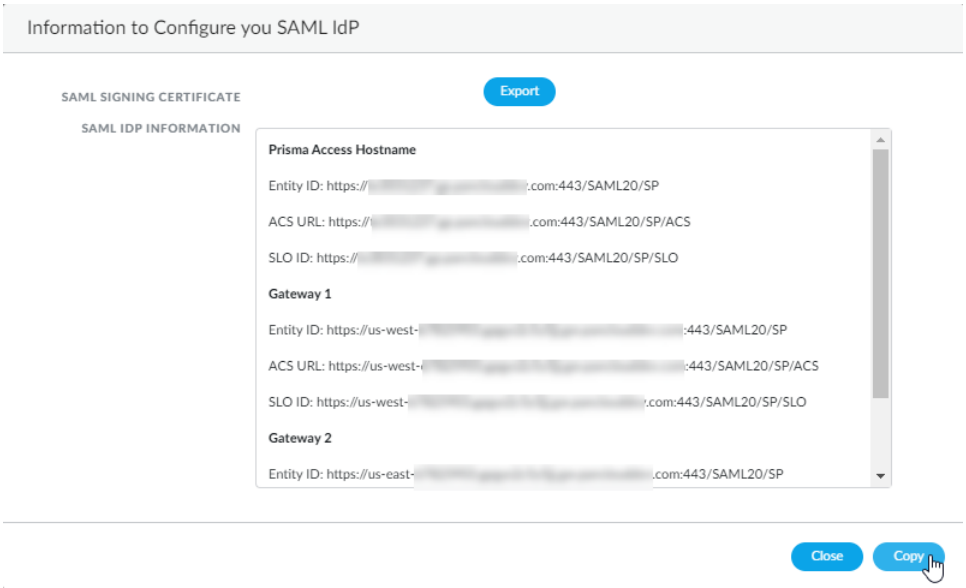
Prisma Access for users provides enterprise authentication via SAML. When a mobile user attempts to connect, Prisma Access (the SAML service provider, or SP) returns an authentication request to the client browser, which in turn sends it to your SAML identity provider (IdP) to authenticate the user. Use the following procedure to configure a trust relationship between Prisma Access and your Okta IdP:

STEP 1 | Enable Mobile User Authentication for Prisma Access.

Complete the steps for defining the Service Provider (SP) settings, including generating or importing the certificate that Prisma Access uses to sign SAML messages that it sends to the identity provider (IdP).

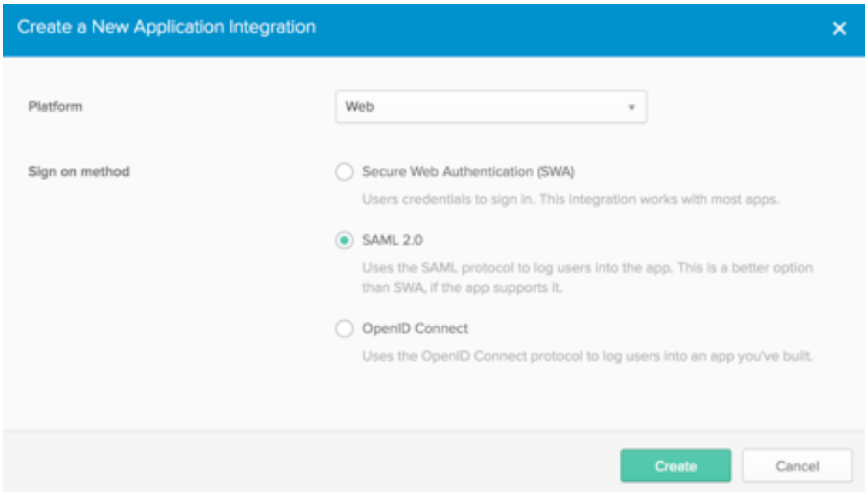
STEP 2 | Export the Information to Configure SAML IdP from Prisma Access.

1. To export the Prisma Access signing certificate so that you can import it onto your IdP, click **View Info** and then click **Export**.
2. **Copy** the information that you need to configure on your IdP and then go to your IdP and configure it with the information about Prisma Access (the Service Provider).

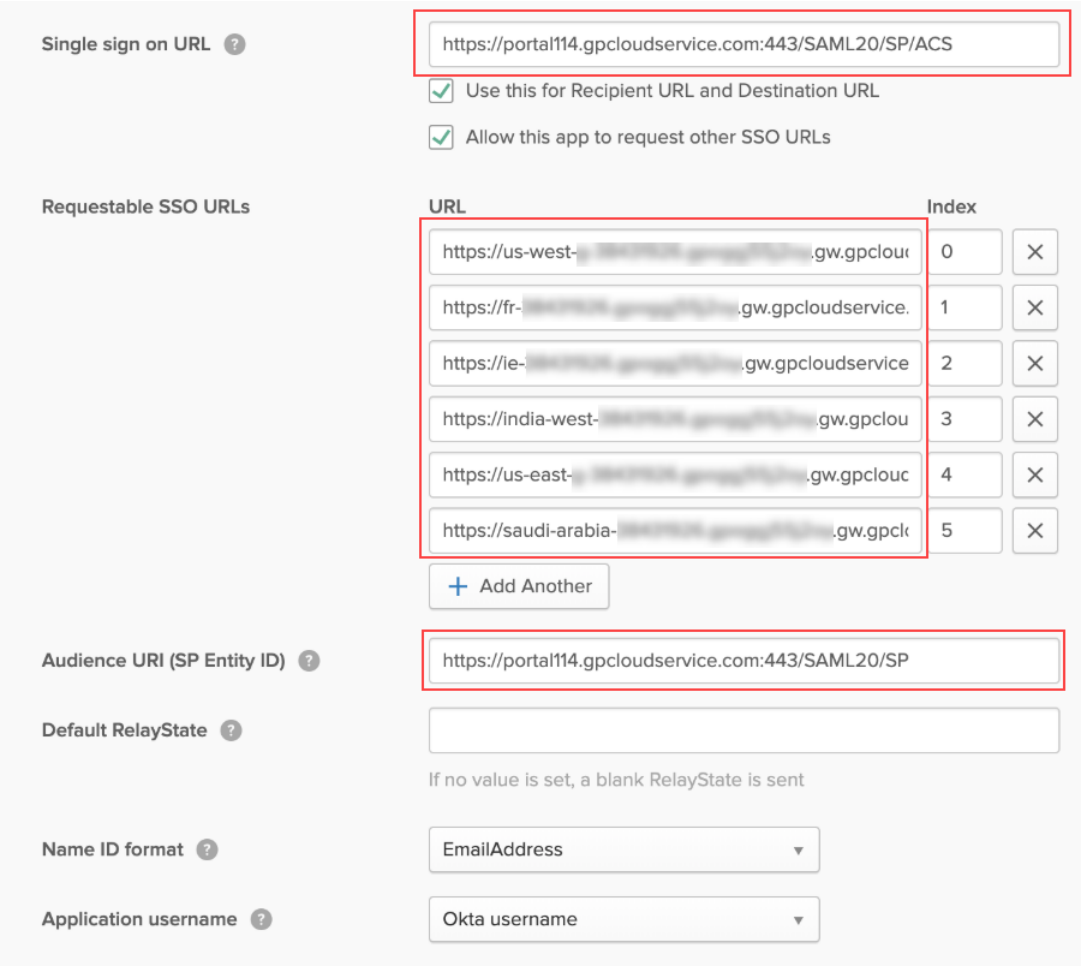


STEP 3 | Log into Okta as an administrator and create and create SAML 2.0 applications for Prisma Access.

1. Create a new application integration for Prisma Access. Specify the Platform Type as **Web** and the sign-on method as **SAML 2.0** and click **Create**.

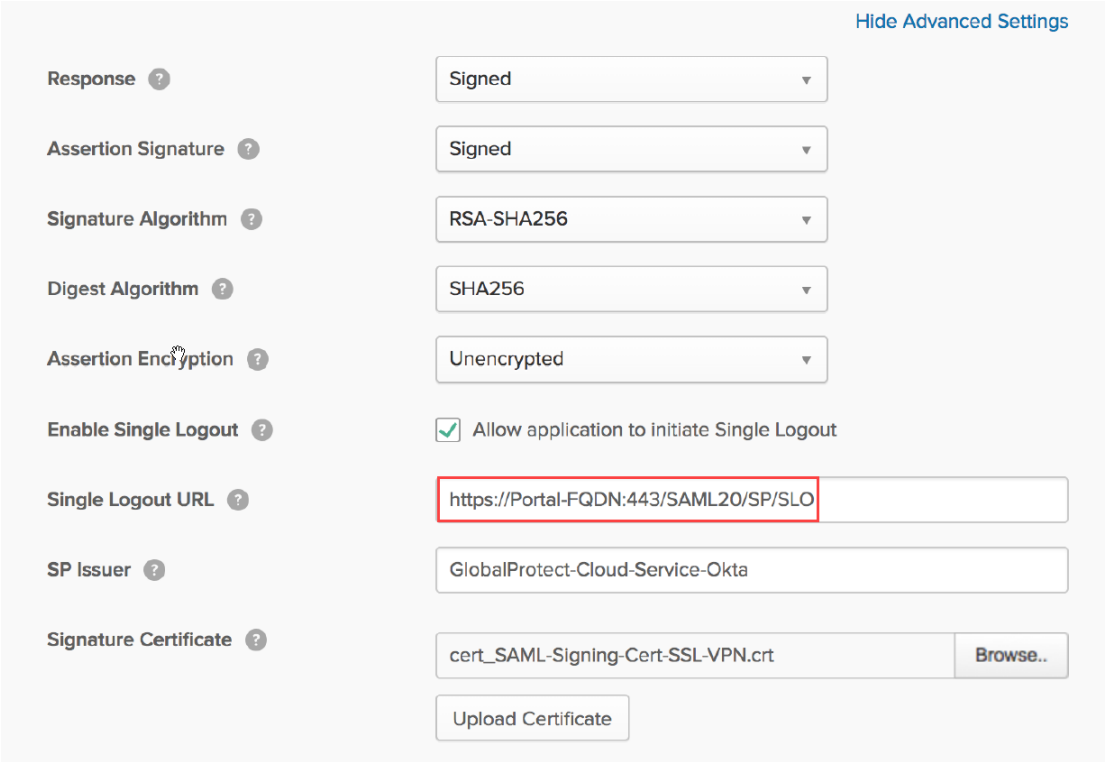


2. Configure the following application integration options:
   - **Single sign on URL**—Enter the URL for the portal (i.e. https://portal114.gpcloudservice.com:443/SAML20/SP/ACS)
   - **Use this for Recipient URL and Destination URL**—Select this check box.
   - **Allow this app to request other SSO URLs**—Select this check box and add the URLs for all Prisma Access gateways on the list you copied in the **Requestable SSO URLs** field.
   - **Audience URI (SP Entity ID)**—Enter the URL for the portal (i.e. https://portal114.gpcloudservice.com:443/SAML20/SP).
   - **Default RelayState**—Leave blank.
   - **Name ID format**—Select **EmailAddress**.
   - **Application username**—Select **Okta Username**.



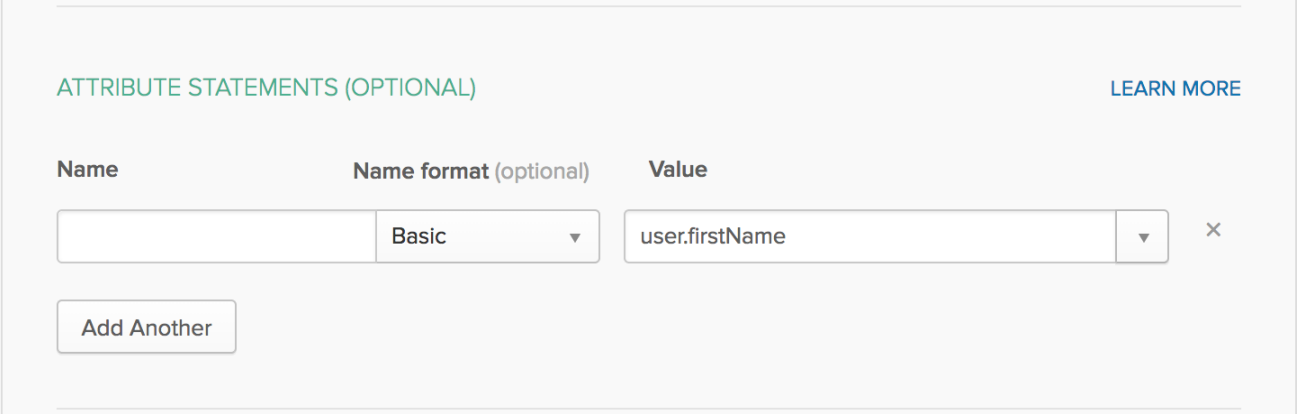
3. Select **Show Advanced Settings** and configure these settings:
   - **Allow application to initiate Single Logout**—Select this check box.
   - **Single Logout URL**—Enter https://*<Prisma Access-FQDN>*:443/SAML20/SP/SLO

     Where *<Prisma-Access-FQDN>* is the FQDN you defined for Prisma Access when you set up the environment.
   - **SP Issuer**—Enter the issuer for the service provider.
   - **Signature Certificate**—**Browse** to and then select the SAML signing certificate that you exported from Prisma Access, then click **Upload Certificate**.



4. In the ATTRIBUTE STATEMENTS (OPTIONAL) area, specify users, Name formats, and values in Okta Expression Language.

   These fields reference, transform and combine attributes to define the Username attribute format to match what you set up on Prisma Access. For example, specify a name format of **Basic** and a Value of **user.firstName**.



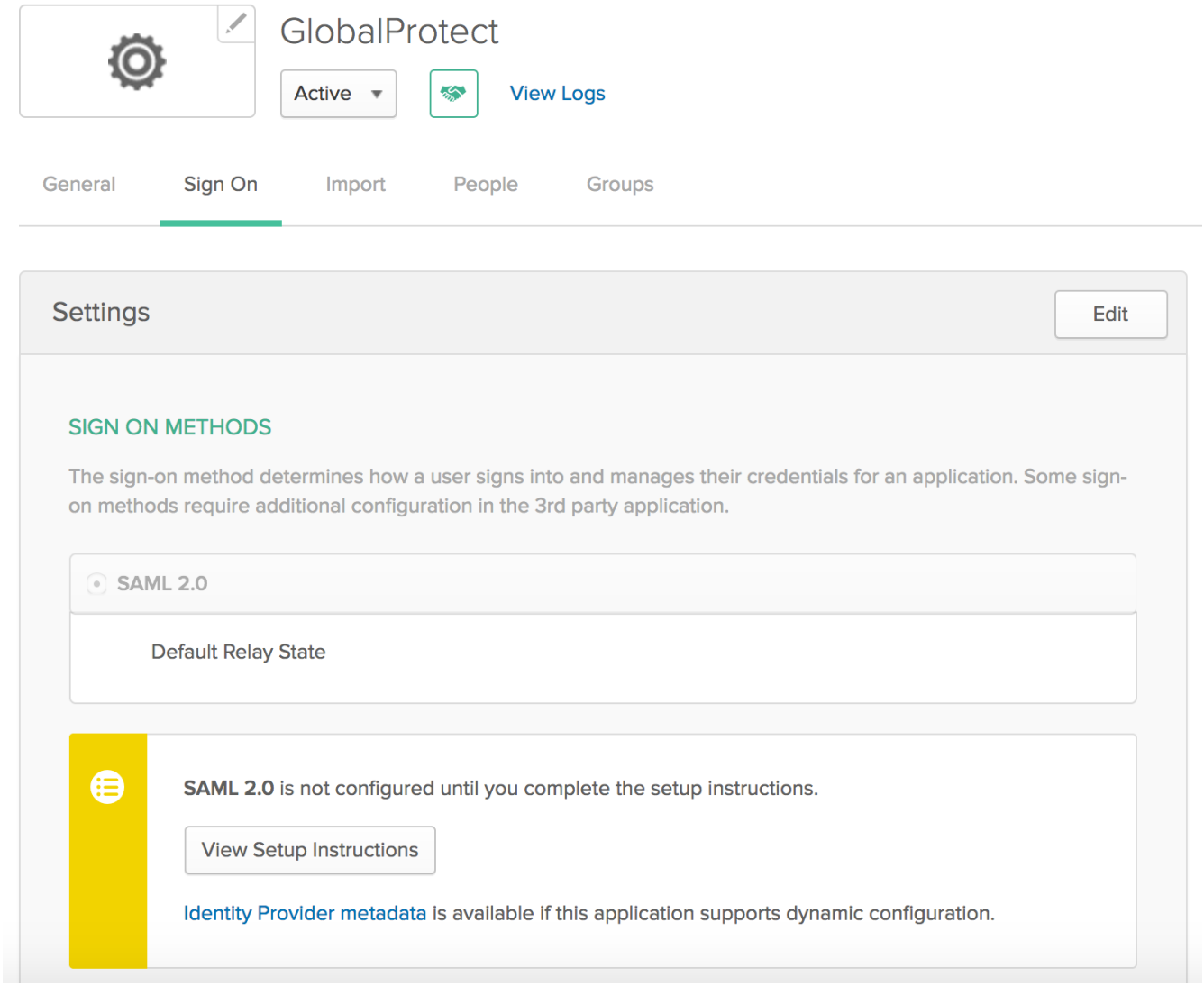
5. Optionally, in the Group Attribute Statements (Optional) area, create group attribute options.

   You can't use group information that's retrieved from the SAML assertion in either security policy rules or the GlobalProtect app configuration.

6. Save the configuration.

STEP 4 | Complete the configuration of the SAML 2.0 web application in Okta and enable the users to use the application. Click **View Setup Instructions** for details.

STEP 5 | To download the metadata files for the portal and gateways, click **Identity Provider metadata** and copy that information.



STEP 6 | Import the metadata file and the CA certificate from Okta into Prisma Access.

1. Log in to the Prisma Access app on the hub and select **Configure** > **Mobile Users** > **Go To Summary** and **Edit** the Enterprise Authentication configuration.
2. In **SAML IdP Profile** click **Add SAML IdP Profile** and **Import** the metadata file you exported from the Okta server.
3. **Save** the IdP profile.

Configure SAML Authentication Using ADFS as the IdP for Mobile Users

Prisma Access users provides enterprise authentication via SAML. When a mobile user attempts to connect, Prisma Access, acting as the SAML service provider, or SP, returns an authentication request to the client browser, which in turn sends it to your SAML identity provider (IdP) to authenticate the user. Use the following procedure to configure a trust relationship between Prisma Access and your Active Directory Federation Services (ADFS) 4.0 IdP.

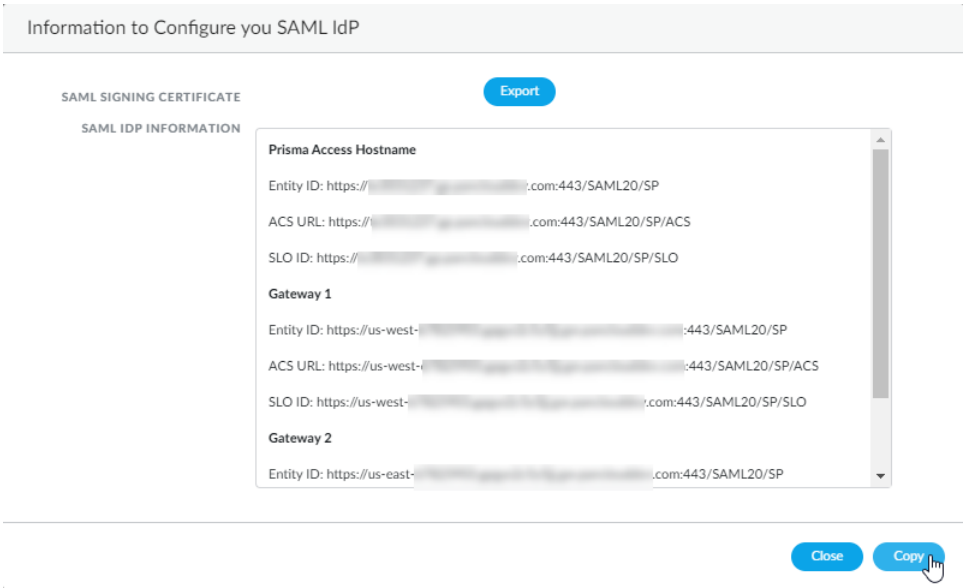
Before you begin, make sure that you can navigate to your AD FS namespace's initiated sign-on page. The URL is in the format **https://<*namespace*><*adfs-server-hostname*>/adfs/ls/idpinitiatedsignon.aspx**, where <*namespace*> is the namespace for the ADFS server (either **adfs.** or, if you use the Secure Token Service (STS), **sts.**) and <*adfs-server-hostname*> is the host name for the ADFS server. An example URL is **https://adfs.acme.com/adfs/ls/idpinitiatedsignon.aspx**.

STEP 1 | Enable Mobile User Authentication for Prisma Access.

Complete the steps for defining the Service Provider (SP) settings, including generating or importing the certificate that Prisma Access uses to sign SAML messages that it sends to the identity provider (IdP).

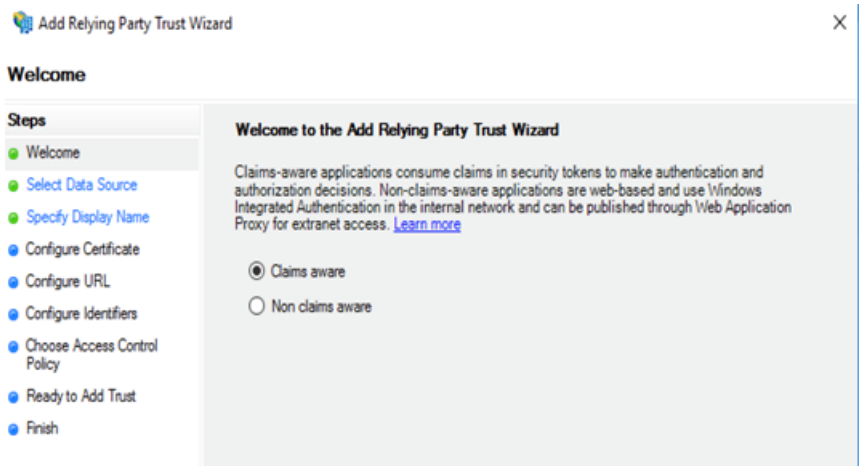
STEP 2 | Export the Information to Configure SAML IdP from Prisma Access.

1. To export the Prisma Access signing certificate so that you can import it onto your IdP, click **View Info** and then click **Export**.
2. **Copy** the information that you need to configure on your IdP and then go to your IdP and configure it with the information about Prisma Access (the Service Provider).

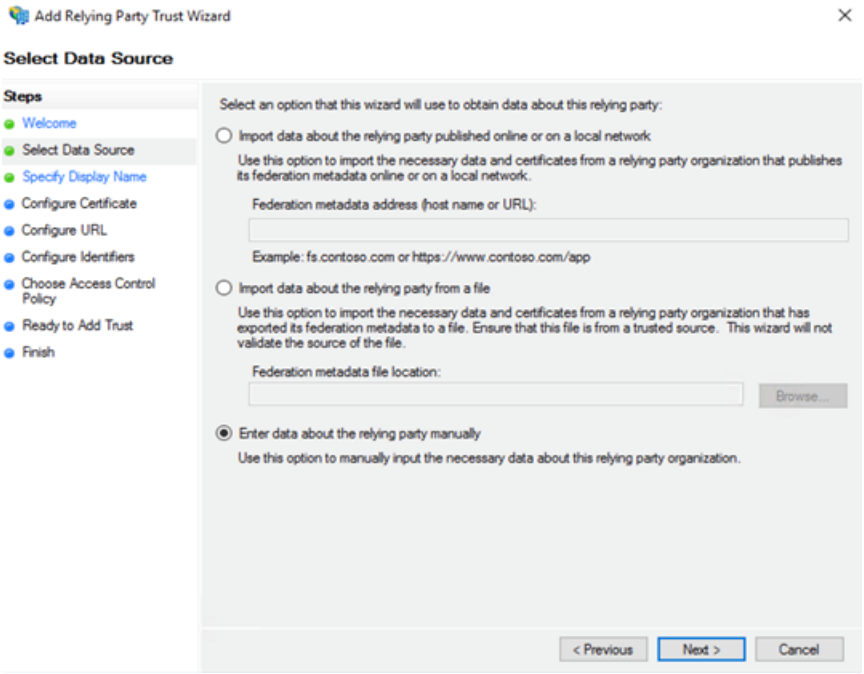


STEP 3 | Add each Prisma Access portal and gateway as a **Relying Party Trust** to the Windows server.

1. On the server running AD FS, start AD FS Management.
2. In the **Navigation Pane**, expand **Trust Relationships**, and then select **Relying Party Trusts**.
3. On the **Actions** menu located in the right column, select **Add Relying Party Trust**.
4. In the **Add Relying Party Trust Wizard** page, select **Claims aware** and click **Start**.

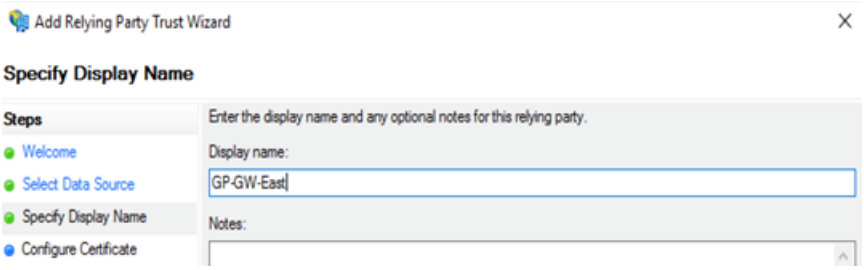


5. In the **Select Data Source** page, select **Enter data about the relying party manually** and click **Next**.



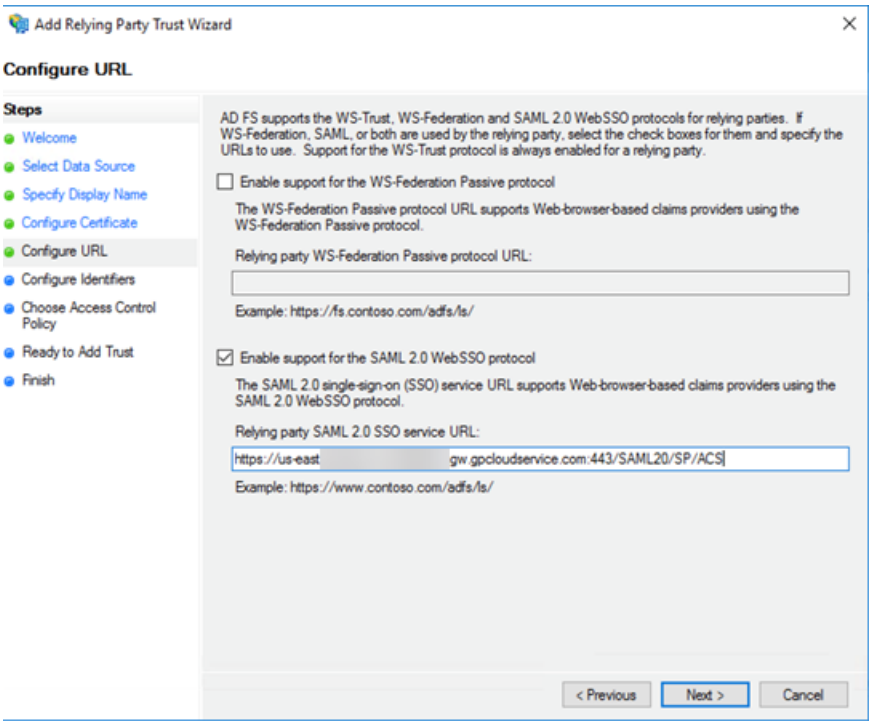
6. In the **Specify Display Name** page, enter the name for the first relying party (one of the IP addresses in the list of security processing nodes you exported from Prisma Access) and click **Next**.

   This example specifies one of the security processing nodes from Prisma Access as a relying party.



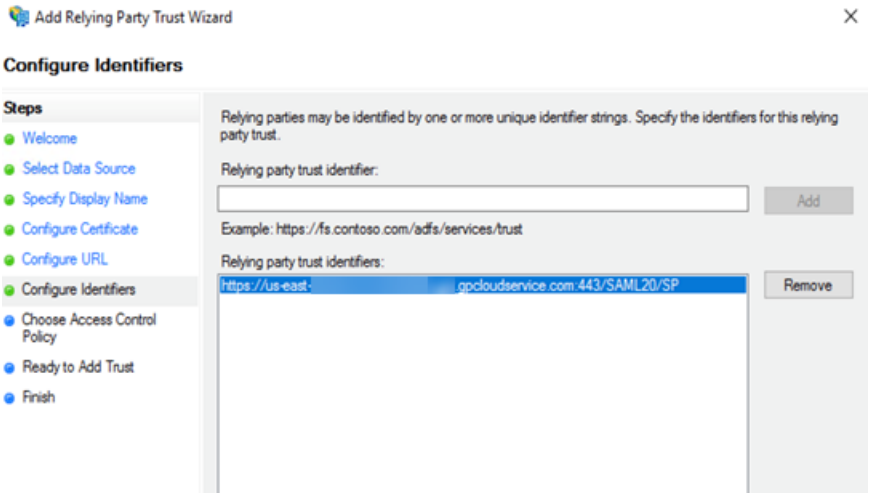
7. In the **Configure URL** page, enter the SAML single sign-on URL you configured for Prisma Access and then click **Next**.

The URL is in the format **https://<*prisma-access-hostname*>:433/SAML20/SP/ACS**, where <*prisma-access-hostname*> is the name of the Prisma Access gateway you are configuring as a relying party trust.

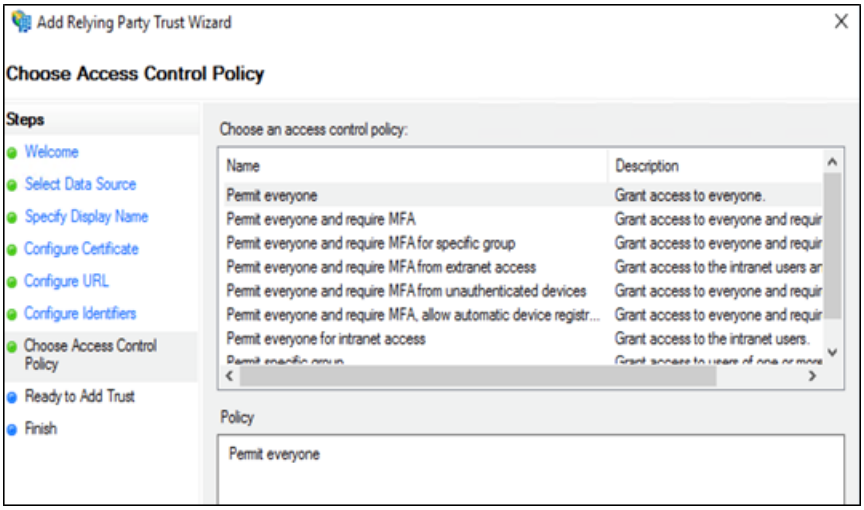


8. In the **Configure Identifiers** page, enter the relying party trust identifier for Prisma Access and then click **Next**.

   The relying party trust identifier URL is in the format **https://<*prisma-access-hostname*>:443/SAML20/SP**, where <*prisma-access-hostname*> is the name of the Prisma Access security processing node you are configuring as a relying party trust.

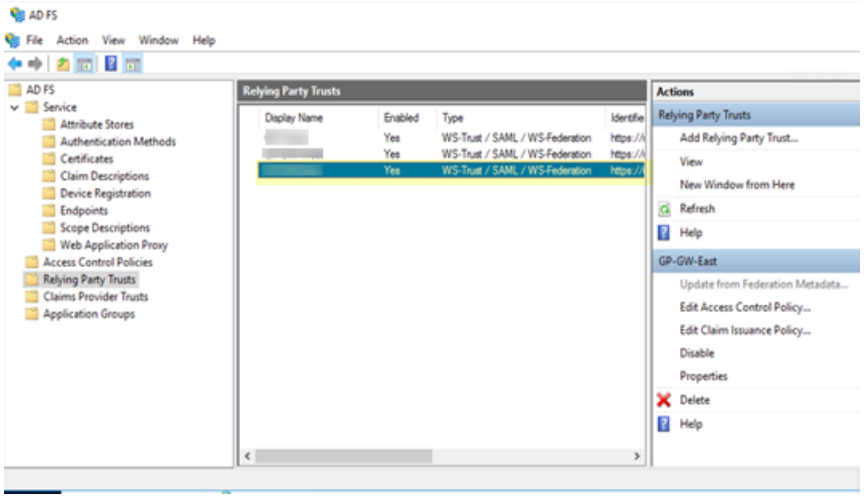


9. In the **Choose Access Control Policy** page, leave the **Policy** as **Permit everyone** and click **Next**.



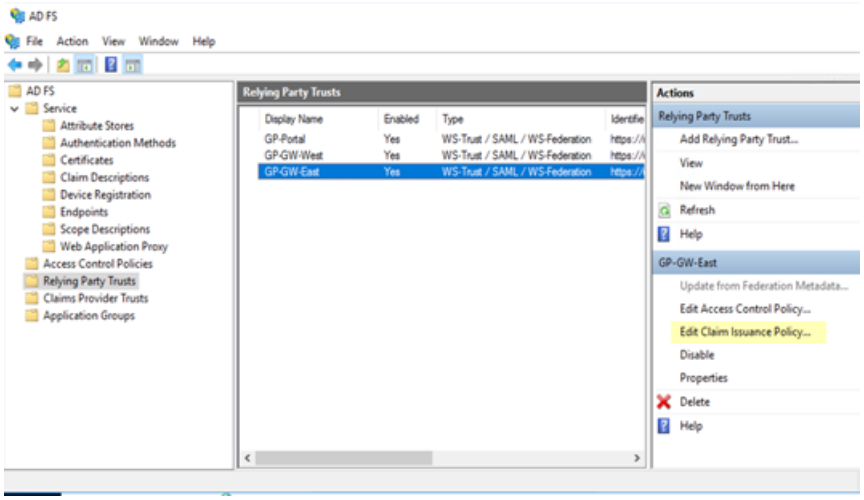
10. Click **Finish**.

    ADFS adds a new **Relying Party Trusts** entry.

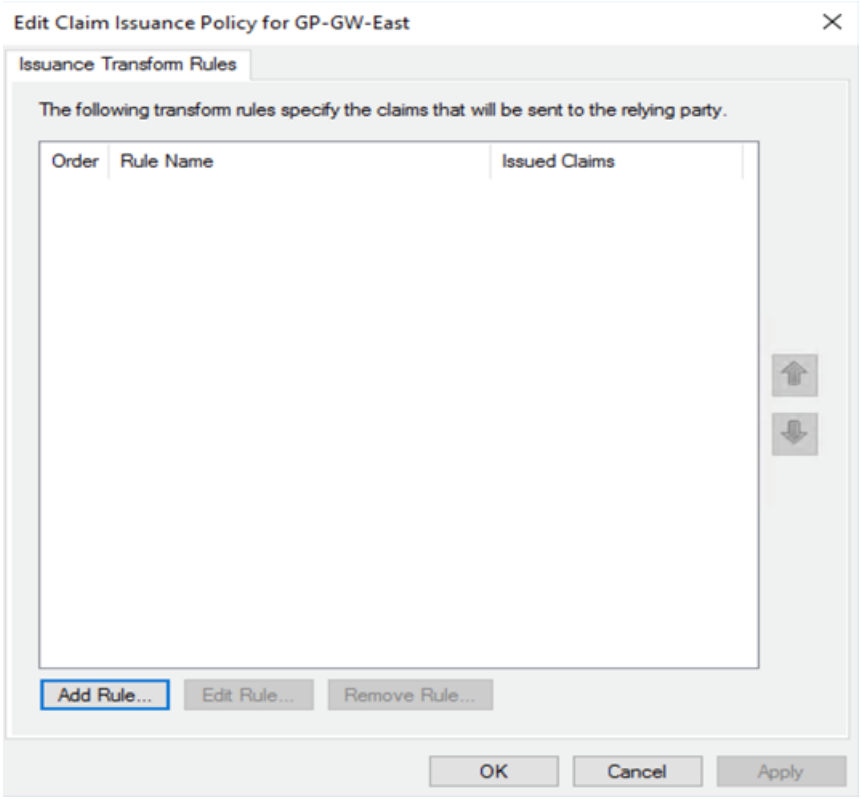


STEP 4 | Add a rule to the relying party trust you created.

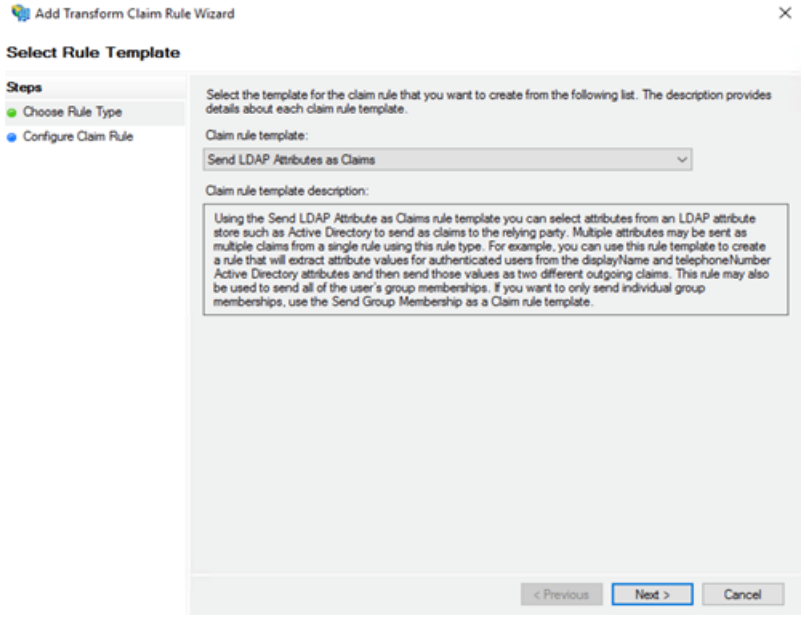
1. In the **Relying Party Trusts** page, find the Prisma Access node you just added in the selections on the right, then select **Edit Claim Issuance Policy**.



2. In the **Edit Claim Issuance Policy** page, click **Add Rule**.

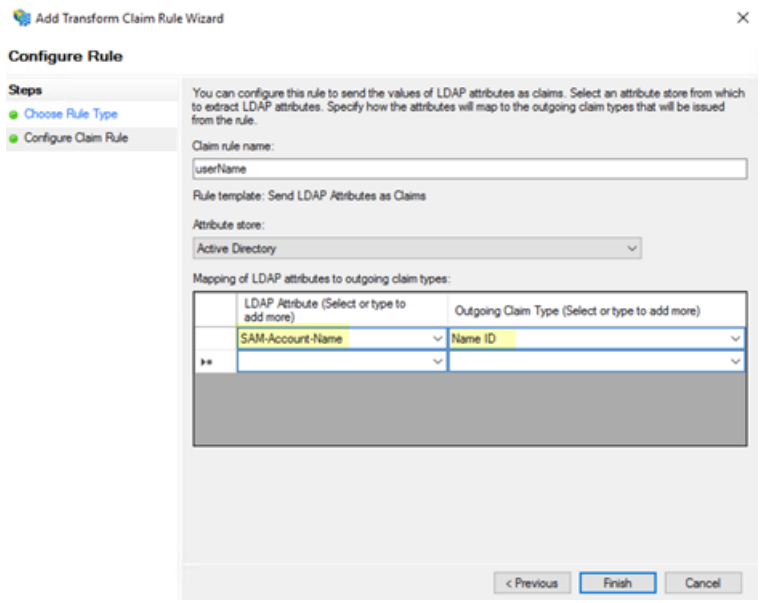


3. In the **Select Rule Template** page, select **Send LDAP attributes as Claims** as the Claim rule template and click **Next**.

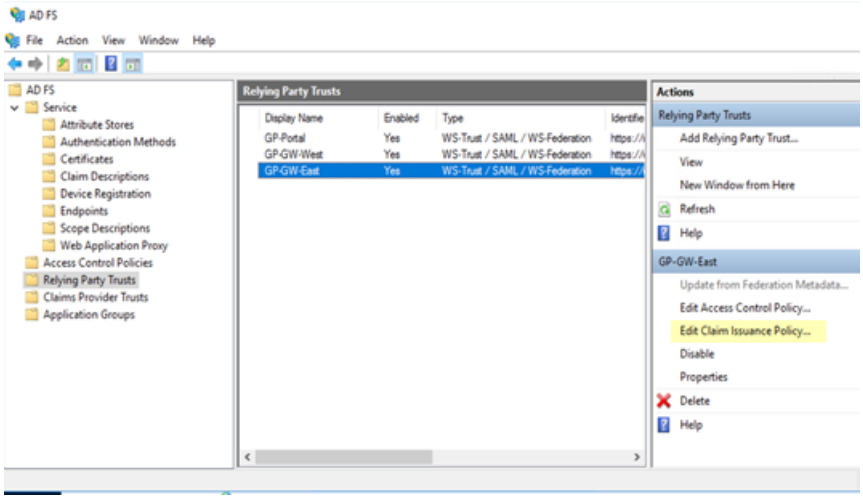


4. In the **Configure Rule** window, add an **LDAP Attribute** of **SAML-Account-Name** and an **Outgoing Claim Type** of **Name ID**.

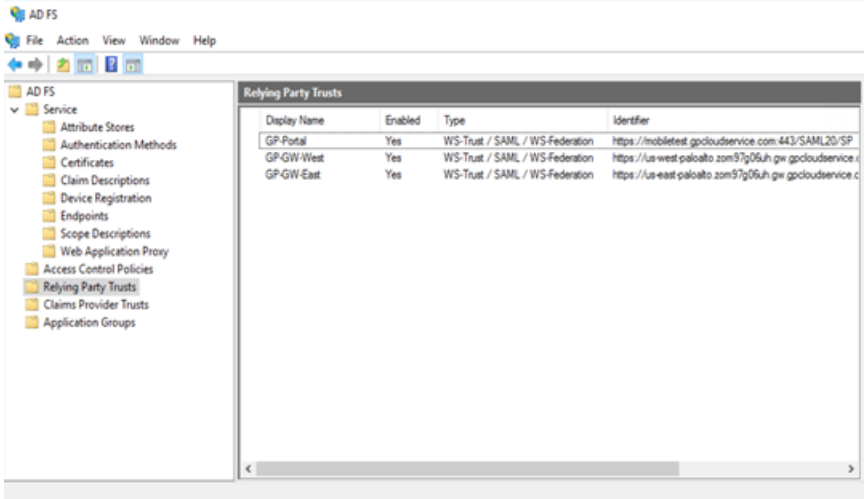
   By default, the Prisma Access security processing nodes expect the **username** attribute in the SAML response from the Identity Provider (IdP).



5. Click **Apply** then click **OK**.



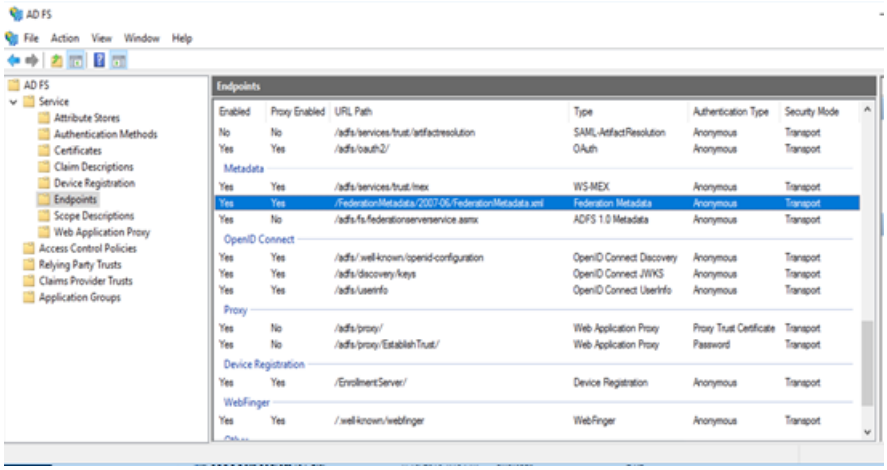
The Prisma Access node displays in the list of **Relying Party Trusts**.



STEP 5 | Add the remaining security processing nodes in Prisma Access as Relying Party Trusts.

STEP 6 | Download the federation metadata XML file and the ADFS CA certificate to a local machine for import into Prisma Access:

1. To download the metadata file, start AD FS Management on the server running ADFS, then select **AD FS** > **Service** > **Endpoints** and find the URL to download the file. The URL is in the format **https://***<adfs-server-hostname>***/FederationMetadata/2007-06/FederationMetadata.xml**, where *<adfs-server-hostname>* is the host name for the ADFS server.
2. If the certificate that the ADFS server uses to sign SAML responses is not signed by a well-known, third-party CA, export the CA certificate so that you can import it into Prisma Access.



STEP 7 | Import the metadata file and the CA certificate (if needed) from ADFS into Prisma Access.

1. Log in to the Prisma Access app on the hub and select **Configure** > **Mobile Users** > **Go To Summary** and **Edit** the Enterprise Authentication configuration.
2. In **SAML IdP Profile** click **Add SAML IdP Profile** and **Import** the metadata file you exported from the ADFS server.
3. **Save** the IdP profile.

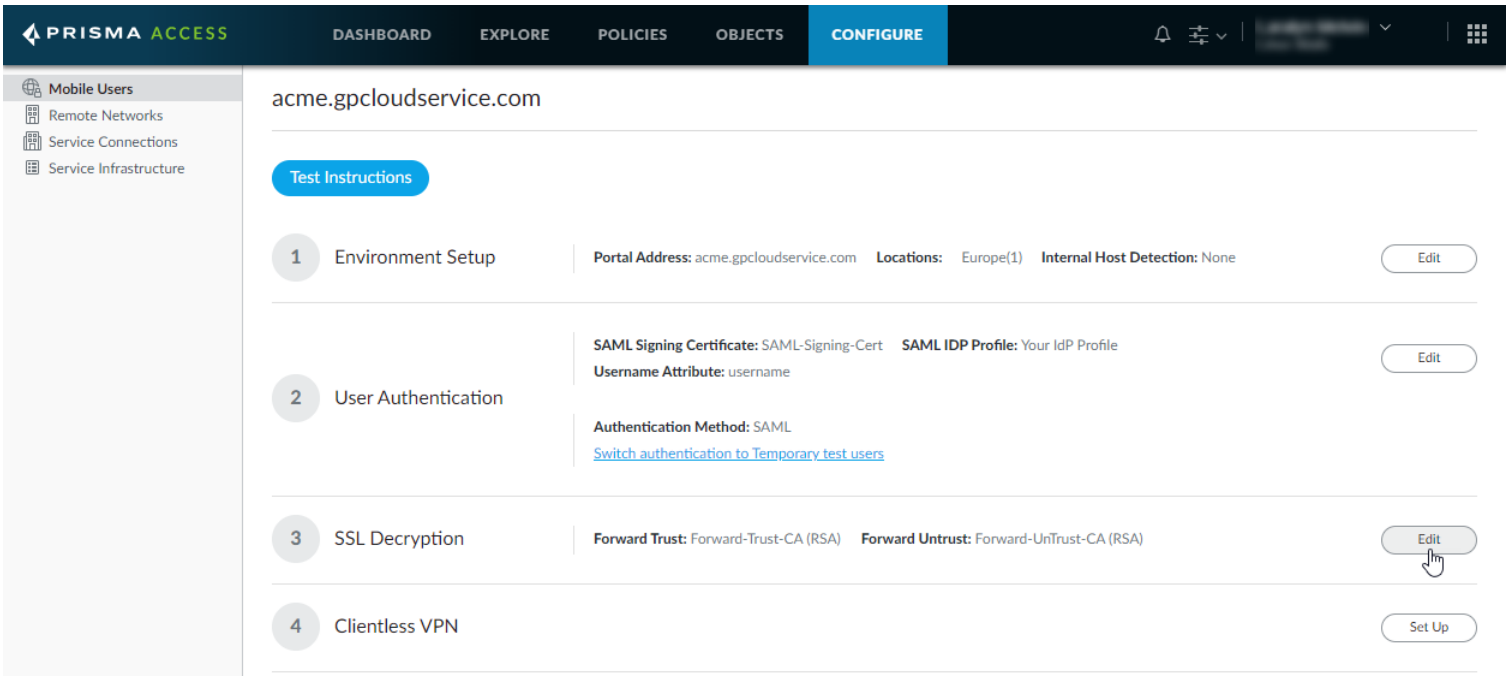
Enable SSL Decryption for Mobile User Traffic

Prisma Access makes it easy for you to decrypt traffic by providing a default SSL decryption policy based on best practices and a default set of certificates to use for SSL decryption. It is important to decrypt traffic because you cannot protect against threats you cannot see. With decryption enabled, you prevent malicious encrypted content from entering your network and sensitive content from leaving your network concealed as encrypted traffic.

If you have already configured SSL decryption for your remote network configuration, you do not need to configure it again.

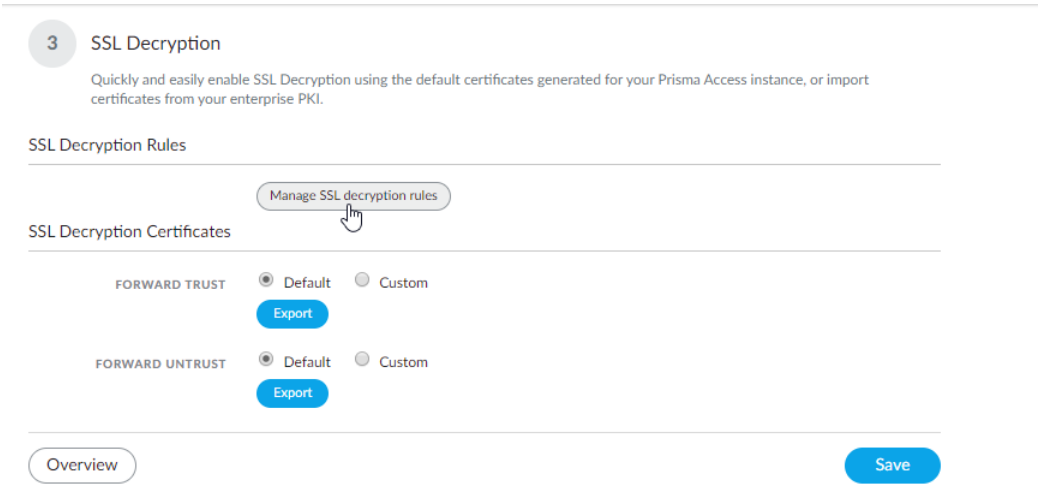
You can either use the default SSL decryption policy and certificates, or customize the SSL decryption settings.

STEP 1 | From your Mobile Users configuration summary (**Configure** > **Mobile Users** > *<mobile-user-config>*), and **Edit** SSL Decryption.

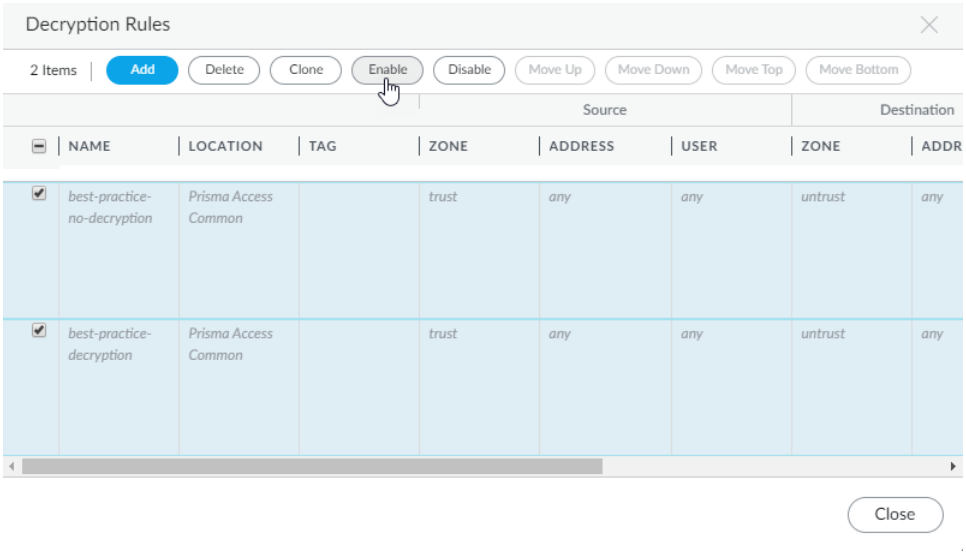


STEP 2 | To enable SSL decryption using custom decryption policy rules and certificates:

1. Click **Manage SSL decryption rules**.



2. Select both best practice rules and **Enable** them and then **Close** the dialog.



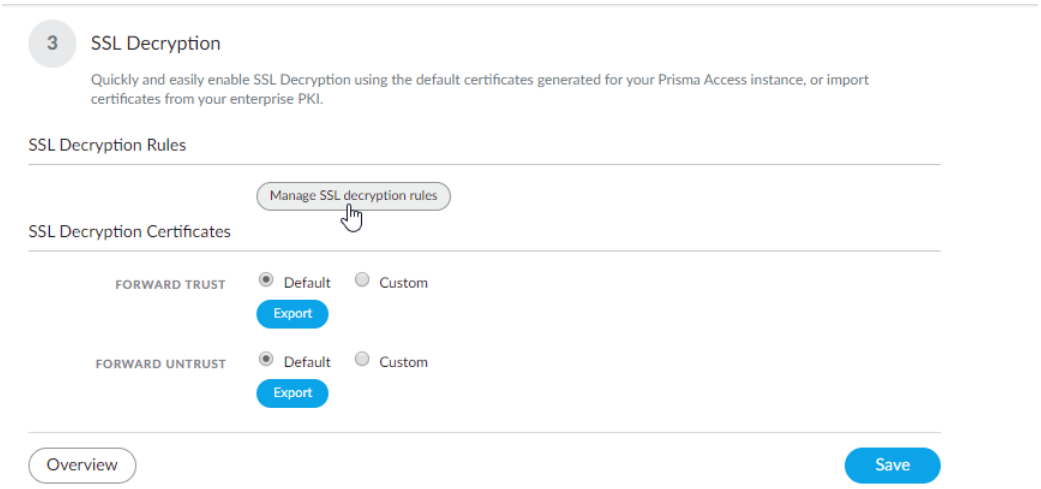
You can also customize the predefined best practice decryption policy rules to suit your environment.

3. **Save** the decryption settings to return to the mobile users configuration summary.

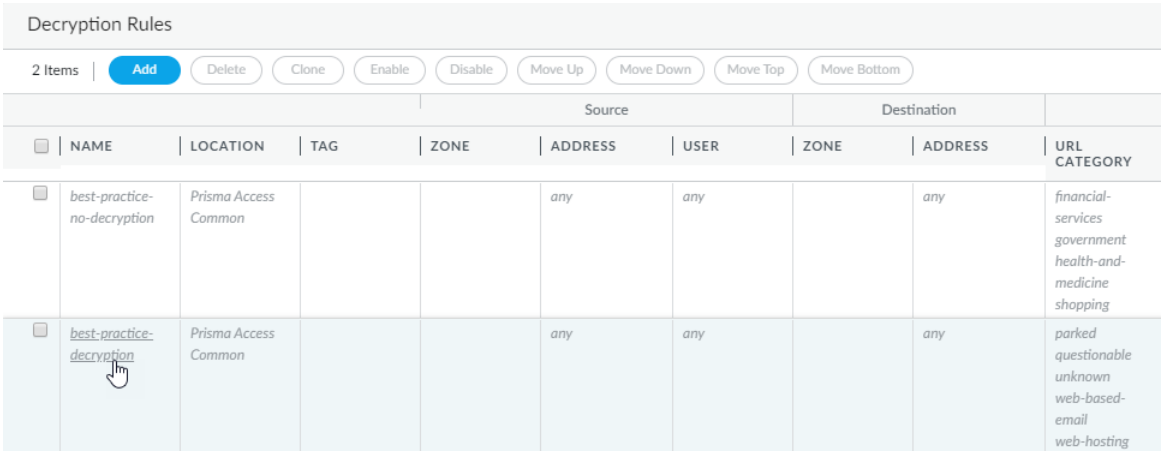
   If you chose to use the predefined certificates, Prisma Access automatically distributes the certificates to your mobile users so that they do not see certificate errors when browsing to trusted sites. Do not distribute the untrust certificate because when a user attempts to access an untrusted site, you want them to see the warnings.

STEP 3 | To enable SSL decryption using custom decryption policy rules and certificates:

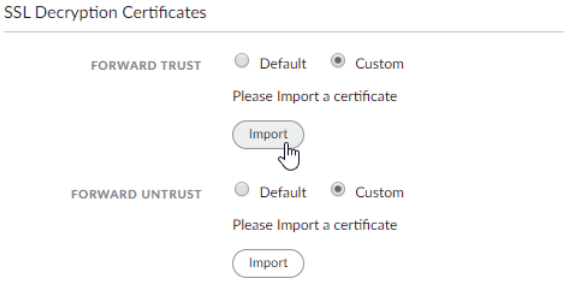
1. Click **Manage SSL decryption rules**.



2. Click on the rule name to edit a best practice decryption rule.

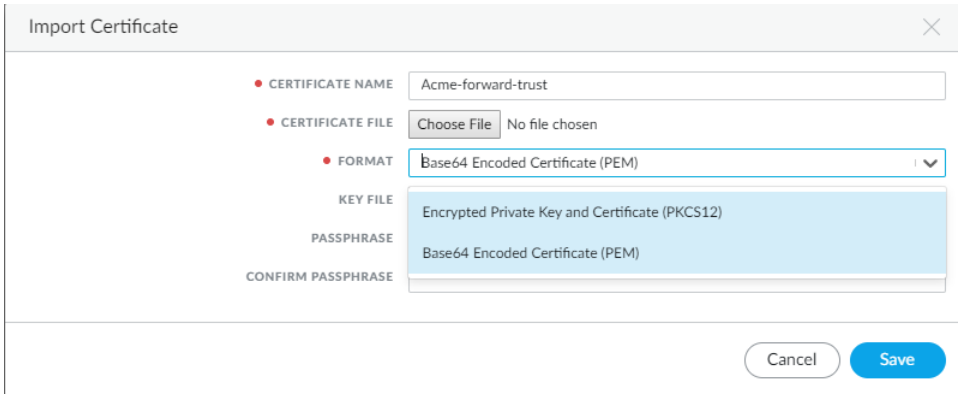


3. Customize the decryption policy rules for your environment and then **Save** the rule.
4. Select both best practice rules and **Enable** them and then **Close** the dialog.
5. To use your own **Custom** certificates, **Import** forward trust and forward untrust certificates with certificates from your enterprise PKI.



6. Define the certificate settings:
    1. Enter the **Certificate Name**.
    2. Select **Choose File** to import the **Certificate File** for the certificate.
    3. If the certificate **Format** is **Base64 Encoded Certificate (PEM)**, the key is in a separate file. In this case you must also click **Choose File** to import the **Key File** for the certificate.

4. Create a **Passphrase** and then **Confirm Passphrase**.



5. **Save** the certificate settings.
7. **Save** the decryption settings to return to the mobile users configuration summary.
8. Distribute the forward trust certificate to your mobile users.

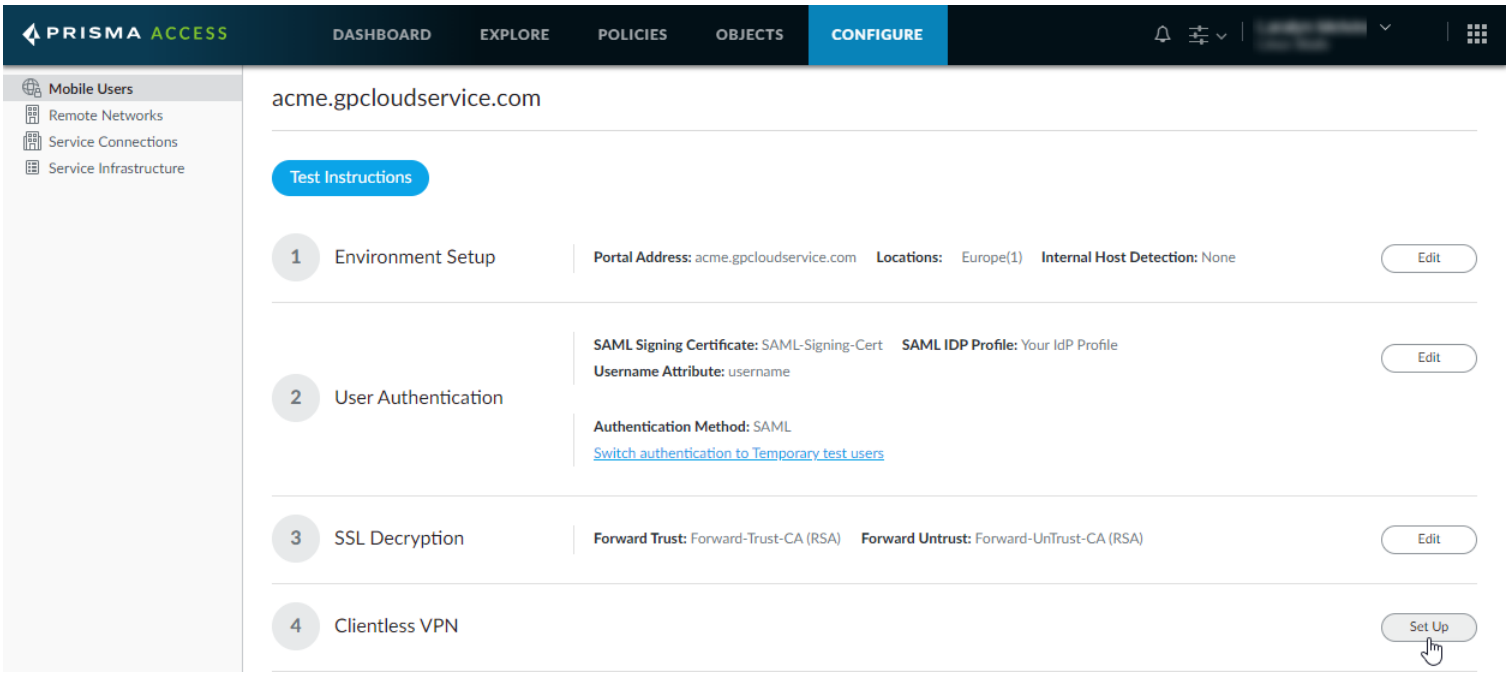
   You must distribute the forward trust certificate to your mobile users so that they do not see certificate errors when browsing to trusted sites. Do not distribute the untrust certificate because when a user attempts to access an untrusted site, you want them to see the warnings.

Configure Clientless VPN for Prisma Access

Clientless VPN enables secure remote access to enterprise applications from SSL-enabled web browsers. With Clientless VPN, end users are not required to install the GlobalProtect app software on their endpoints, which is useful when you need to enable partner or contractor access to applications and safely enable unmanaged assets, including personal endpoints.

Use the following steps to set up Clientless VPN for Prisma Access:

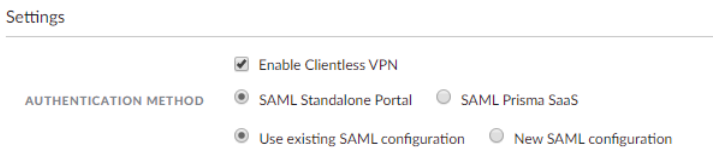
STEP 1 | From your Mobile Users configuration summary (**Configure** > **Mobile Users** > *<mobile-user-config>*), **Set Up** Clientless VPN.



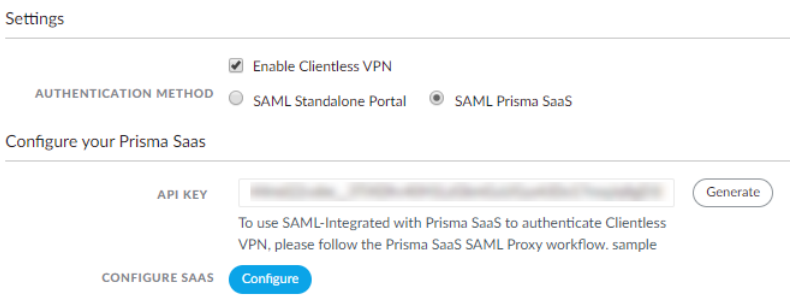
STEP 2 | **Enable Clientless VPN**.

STEP 3 | Select a Clientless VPN **Authentication Method**:

- **SAML Standalone Portal**—If you want to use Prisma Access as your SAML Security Provider (SP) for Clientless VPN, select this option. If you have already configured SAML for Prisma Access, you can choose to **Use existing SAML configuration**. Or, create a **New SAML configuration** to use different SAML configuration for your clientless VPN users.



- **SAML Prisma SaaS**—If you are using Prisma SaaS to secure your sanctioned SaaS applications and you want to use the same SAML configuration that you use for Prisma SaaS to authenticate your Prisma Access clientless VPN users, select this option.



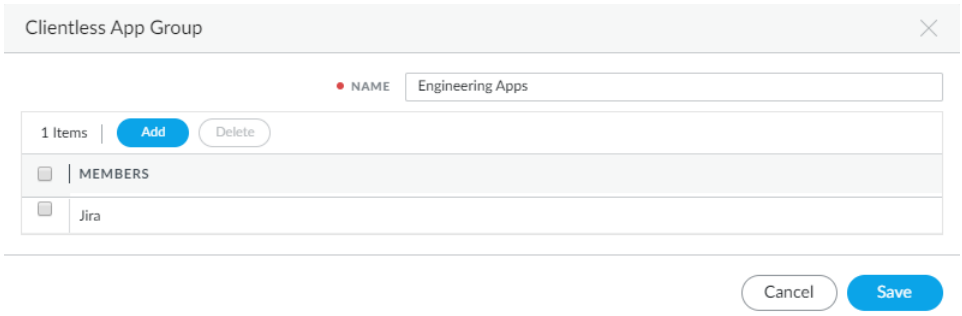
STEP 4 | Configure SAML authentication based on the authentication method you chose:

- To use the Prisma Access SAML standalone portal, you can **Use existing SAML configuration** or **New SAML configuration**. If you are using an existing SAML configuration, Prisma Access uses the same configuration that you set up when you configured user authentication. If you want to create a new SAML configuration for clientless VPN users, follow the SAML configuration steps in Enable Mobile User Authentication for Prisma Access.
- To authenticate clientless VPN users using SAML configured through Prisma SaaS, select **SAML Prisma SaaS**. Copy the API key and then **Configure** Prisma SaaS with the key to enable it to authenticate Prisma Access users.

STEP 5 | Publish the applications that your clientless VPN users can access.

1. **Add** an application group or an individual application.
   - **Add Clientless App**—Enter the following information about the application you are adding:
     - **Name**—A descriptive name for the application (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
     - **Application Home URL**—The URL where the web application is located (up to 4,095 characters).
     - (Optional) **Application Description**—A brief description of the application (up to 255 characters).
     - (Optional) **Application Icon**—An icon to identify the application on the published application page. You can browse to upload the icon.

   - **Add Clientless App Group**—To create a group of applications:
     - **Name**—A descriptive name for the application group (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
     - **Add** applications to the group. You can either add an existing application or **Add Clientless App** to add a new one.



STEP 6 | **Save** the configuration to return to the Mobile Users configuration summary.

Enable Mobile Users to Access Corporate Resources Using Service Connections

To enable Prisma Access for users to enable internet access only you do not need to set up any networking services because Prisma Access provides a default IP address pool and a cloud default DNS server. However, if you want your mobile users to be able to access internal resources at your headquarters or data center or in branch networks you have onboarded to Prisma Access, you will need to define the IP address pools to use to assign IP addresses to your mobile users, set up the Prisma Access service infrastructure, and, to allow access to your headquarters or data center networks, onboard service connections.

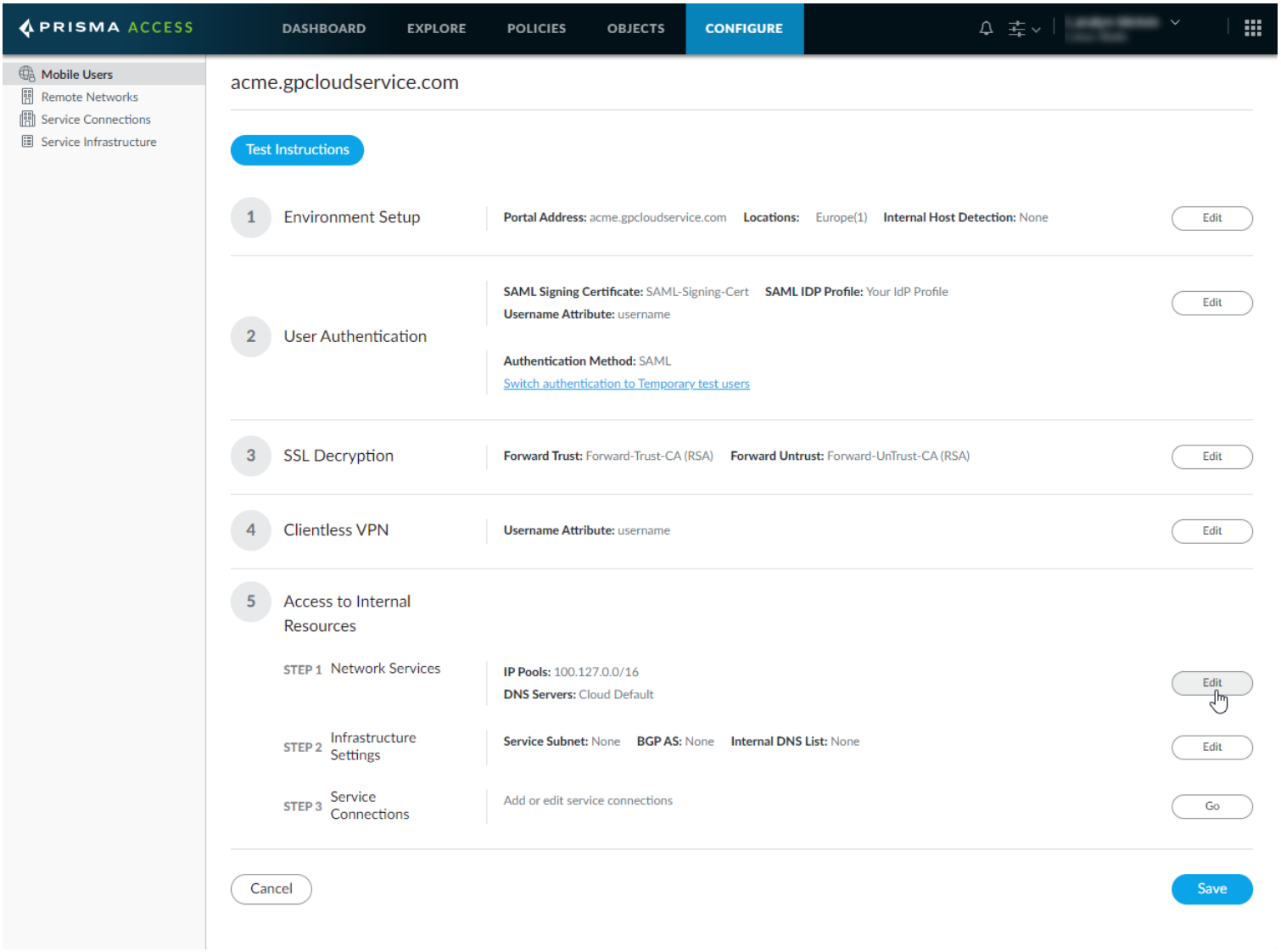
If you want your mobile users to connect to your remote network locations, you must configure at least one service connection, even if you do not plan on using the connection to provide access to your data center or HQ locations. Though all branches are fully meshed, mobile user connections are not. Creating a service connection establishes the hub-and-spoke architecture required to enable mobile user traffic to route to your branch networks. In this case, you can minimally configure the service connection as follows:

- When you onboard the service connection select a **Location** that is close to your mobile users.
- When you Set Up a Primary IPSec Tunnel for Your Service Connection, configure the IPSec peer authentication and tunnel settings using placeholder values.
- When you Enable Routing and Quality of Service for Your Service Connection, add placeholder **IP Subnets**.

  Because Prisma Access does not route any traffic through this tunnel, just make sure the IP subnet you use doesn't conflict or overlap with other configured subnets connected to Prisma Access.

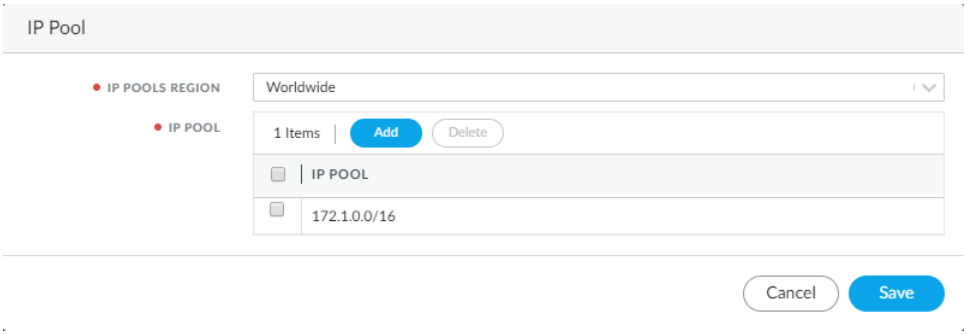
STEP 1 | Launch Prisma Access Cloud Management and select **Configure** > **Mobile Users**, select your mobile users configuration, and **Edit** the Network Services.

STEP 2 | Configure the Network Settings for your mobile users.



1. **Add** the **IP Pools** for Prisma Access to assign to mobile users.
2. Select the **IP Pools Region** to which to assign an IP address pool.

   Select **Worldwide** to use the same IP address pool for all mobile users, or select an available region.You can use a single IP address pool for all mobile users in all regions and locations, 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 a 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 add additional locations to accommodate more mobile users.
3. **Add** an IP address pool to assign to the mobile users in the selected **IP Pools Region**.



The IP address pools you define must meet the following requirements:

- As a best practice, define RFC 1918-compliant IP address pools to prevent IP address conflicts.
- Make sure the IP address pools you define do not overlap with other IP addresses you use internally.
- Make sure the IP address pools you define do not overlap with the infrastructure IP address pool you are using for Prisma Access.
- The IP address pools you designate must not overlap with the 100.64.0.0/15 or 169.254.0.0/16 subnetworks because Prisma Access reserves these subnets for internal use.
- Make sure you designate an IP address pool that allows enough coverage for all mobile users in your organization, based on the following guidelines:
  - If you plan to use a Worldwide address pool deployed in one or two regions the minimum required IP address pool is /23 (512 IP address).
  - If you plan to use a Worldwide address pool deployed in three or more regions the minimum required IP address pool is /19 (8,192 IP addresses), either in a single IP address pool or spread across multiple pools.
  - If you plan to define IP address pools per region, the minimum pool size in any region is /23 (512 IP addresses).
  - You do not need to assign an IP address pool in regions where you do not plan to deploy Prisma Access. For example, select the US East (N. Virginia), US East (Ohio), and US West (N. California), regions only when you onboard Prisma Access for users, you need to specify an IP address pool for the Americas region only. Keep in mind, however, that users in other regions will not be able to connect to Prisma Access.
  - If you plan to define a mix of Worldwide and regional pools, make sure you allocate 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.
  - As a best practice, designate IP address pools so that you have at least one IP address for each unique mobile user in your organization so they can log in simultaneously. If you designate an IP address pool that has a smaller number of IP addresses than your licensed number of users, Prisma Access will display a warning message. However, if you have a limited IP address pool and you do not expect all users to log in concurrently you can bypass the message and use a smaller pool size.

4. **Save** the IP Address pool settings.

   Repeat these steps to add additional IP address pools.
5. **Add** the **DNS Servers** that you want Prisma Access to use to resolve DNS requests from your mobile users.
6. Select the **Network Services Region** for which to configure DNS settings.

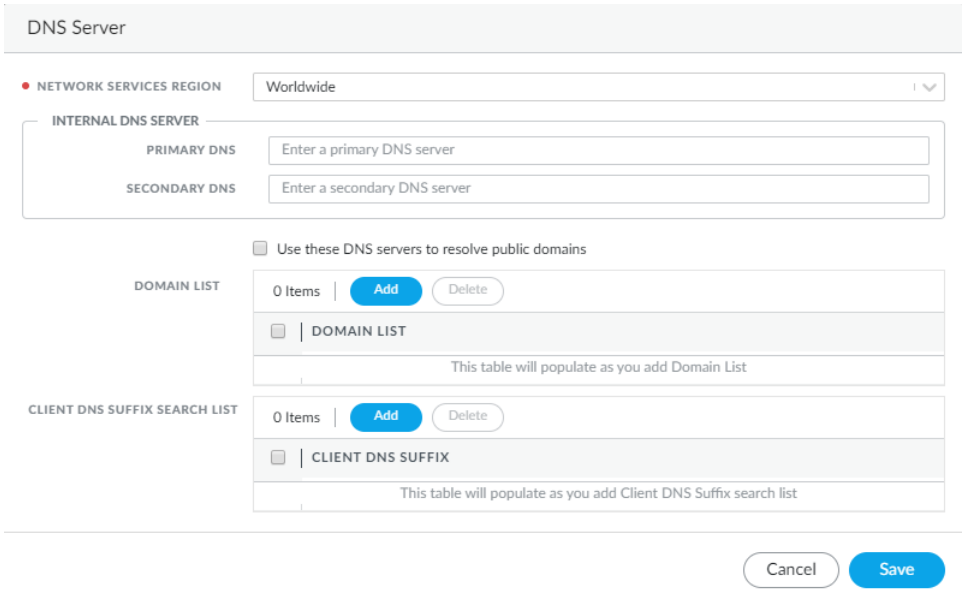
   You can **Add** separate **DNS Servers** configurations for each region where you have mobile users, or configure a **Worldwide** configuration.
7. Enter the IP address of the **Primary DNS** server the to use to resolve internal domains for mobile users in the selected **Network Services Region**.

8. Enter the IP address of the **Secondary DNS** server the to use to resolve internal domains for mobile users in the selected **Network Services Region**.

   The DNS proxy in Prisma Access sends the requests to the DNS servers you specify. The source address in the DNS request is the first IP address in the IP pool you assign to the region. To ensure that your DNS requests can reach the servers you will need to make sure that you allow traffic from all addresses in your mobile user IP address pool to your DNS servers.

9. If you want to use the DNS servers you specified to resolve internal domains to also resolve public domains, select **Use these DNS servers to resolve public domains**.

   If you do not select this option, Prisma Access will use its cloud default DNS serves to resolve requests for public domains.



STEP 3 | If you want your mobile users to be able to access resources on your HQ or data center networks or at other branch locations, you must configure the Prisma Access Infrastructure Settings to enable the network backbone.

If you have not already done this, follow the steps to Configure the Infrastructure Settings and then click **Next**. **Save** your Mobile Users configuration before proceeding to the next step.

STEP 4 | To enable mobile users to access resources on your HQ or data center networks, you must create service connections. If you have not yet created any service connections, **Add or View Service Connection** and then configure the service connection settings.

STEP 5 | Commit and push the mobile users configuration.

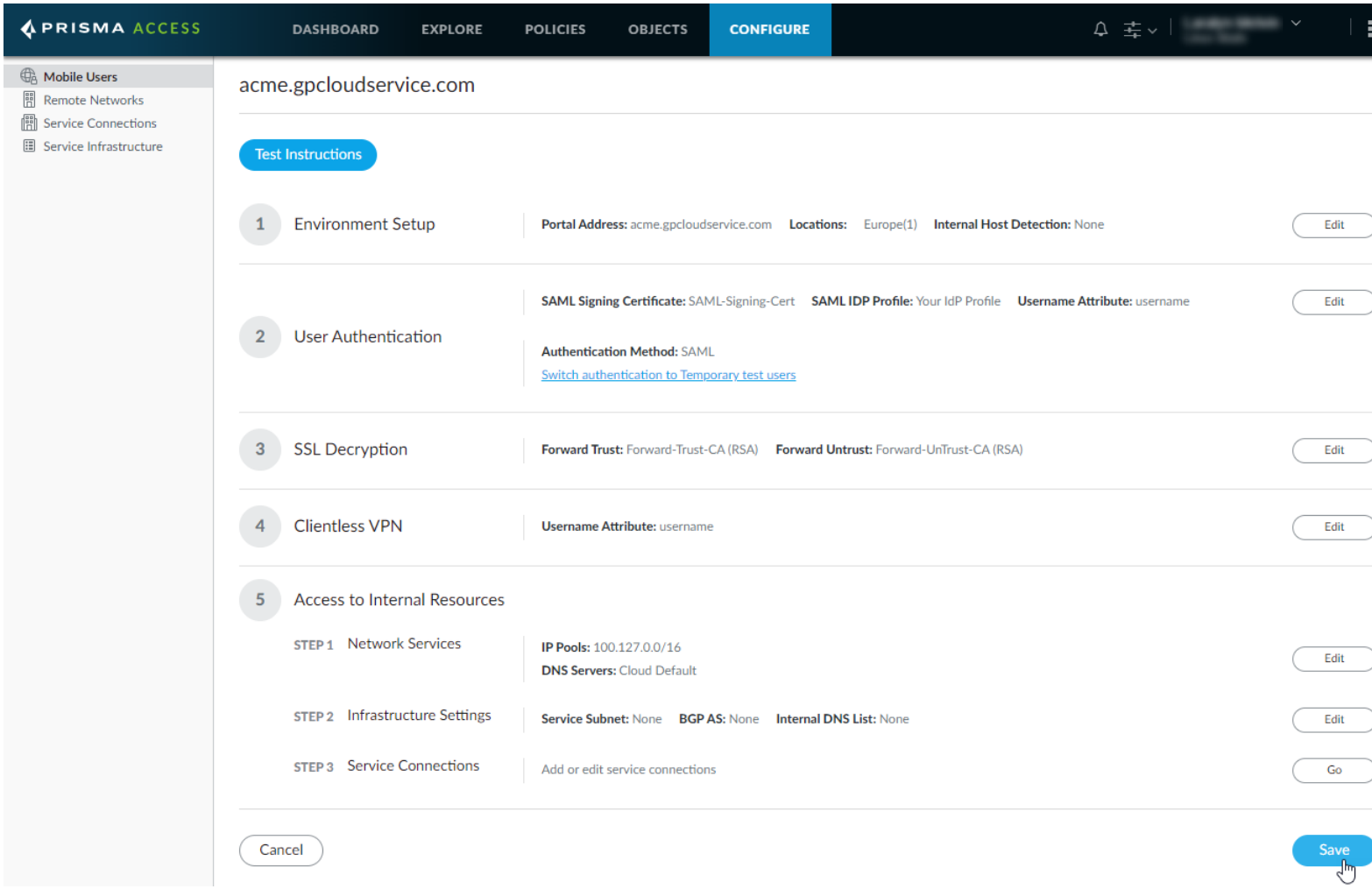
Select **Commit and Push** from the menu.

Verify and Save Your Mobile User Configuration

Use the following steps to verify and save your mobile user configuration:

STEP 1 | From your Mobile Users configuration summary (**Configure** > **Mobile Users** > *<mobile-user-config>*), verify that your entire mobile user configuration is correct.

If you want to modify any of the settings, **Edit** the configuration.



STEP 2 | **Save** the mobile user configuration.

STEP 3 | Commit and push the configuration to your mobile users.

STEP 4 | Go to the **Dashboard** to Monitor the Mobile User Status.

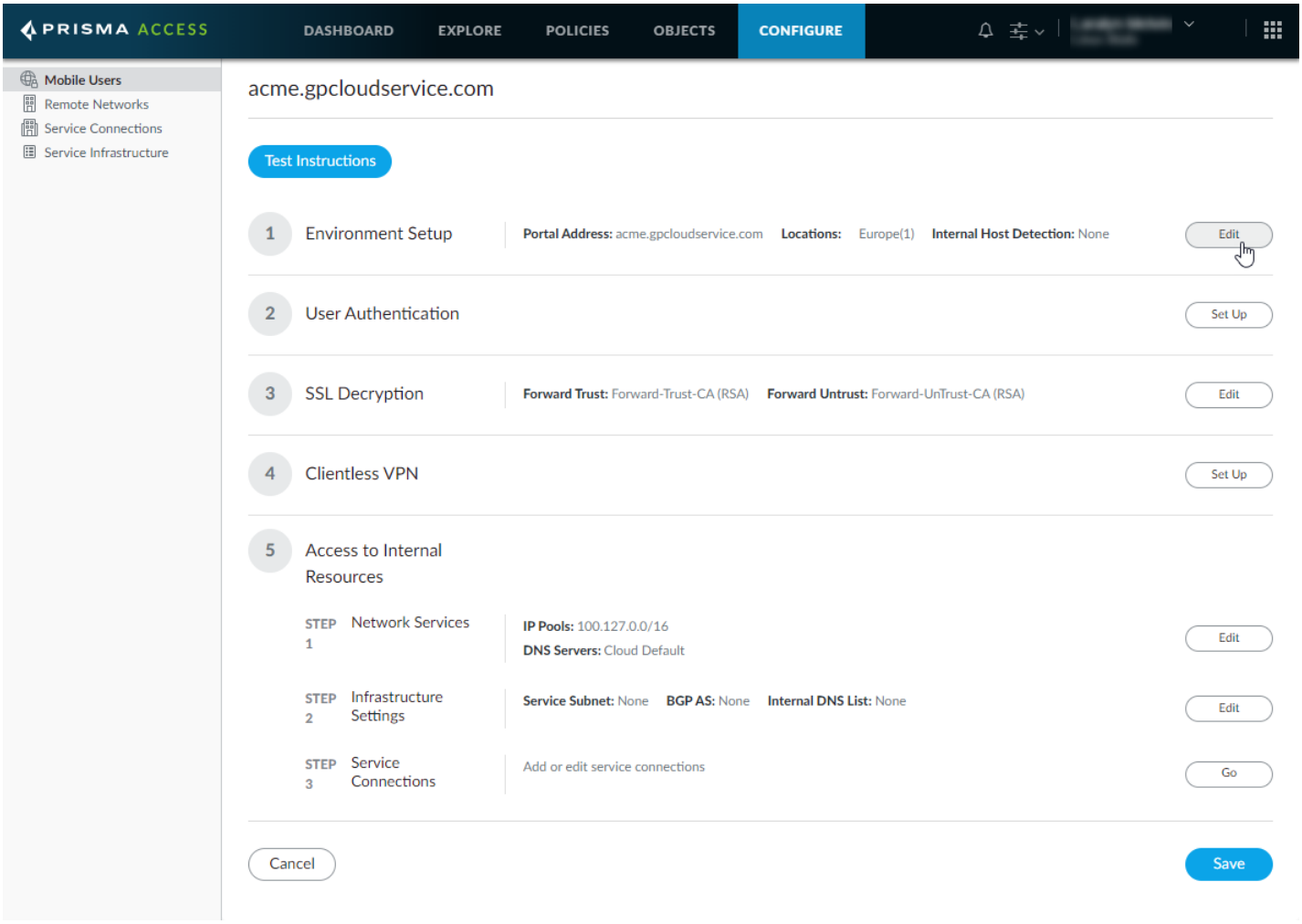
Manage Your Mobile User Configuration

If you need to make any changes to an existing mobile user configuration, use the following steps to view and modify the configuration:

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Select **Configure** > **Mobile Users** > <*mobile-user-config*> and click **Configure** to view your Mobile Users configuration summary.

STEP 3 | To modify an existing configuration in your mobile user configuration, **Edit** the corresponding section.



STEP 4 | After you complete and verify your changes, **Save** the mobile user configuration.

STEP 5 | Commit and push the configuration to Prisma Access.

Monitor the Mobile User Status

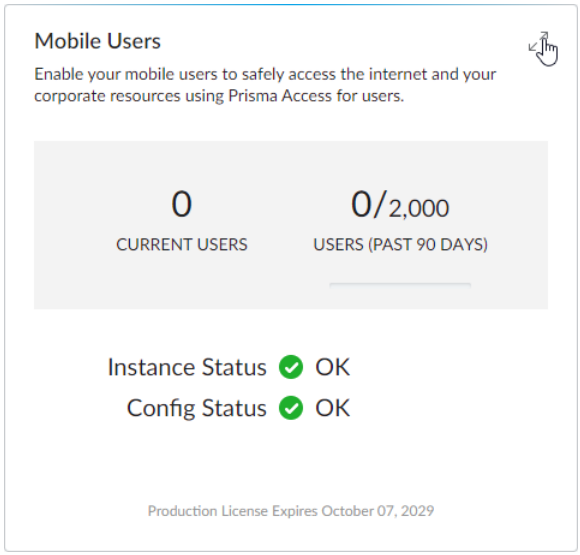
The Prisma Access **Dashboard** provides information on the status of your mobile user environment, remote network environment, and service connections. For mobile users, you can view the following information:

- **Status**—Indicates whether Prisma Access for users is up and running.
- **Config Status**—Indicates the status of your mobile user configuration.
- **License Expires**—Indicates when the Prisma Access users license expires.
- **Current Users**—Indicates the number of mobile users that are currently connected to Prisma Access.
- **Users (Last 90 days)**—Indicates the number of mobile users that have connected to Prisma Access within the last 90 days.

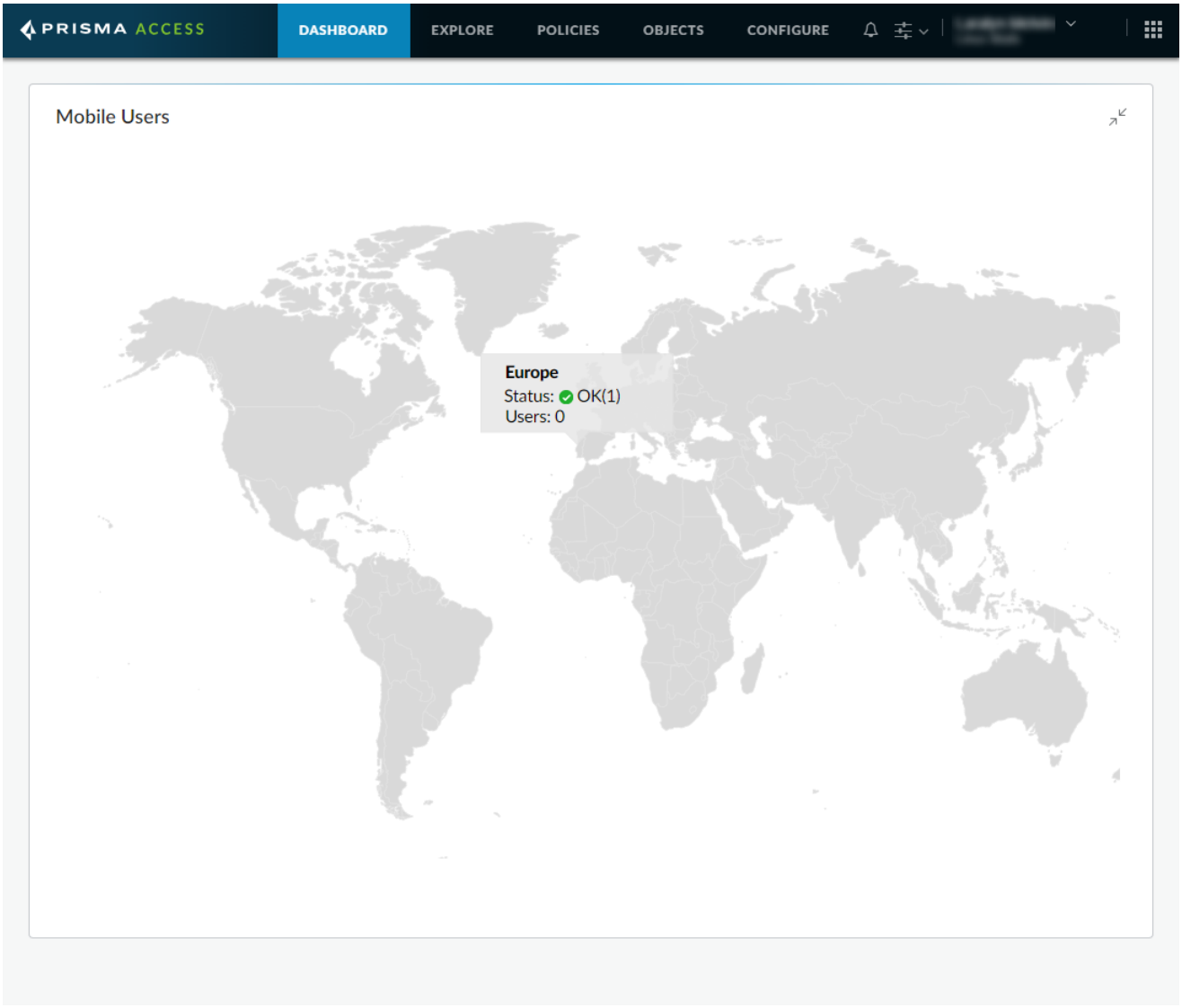
Use the following steps to monitor the status of your mobile user environment:

STEP 1 | Launch Prisma Access Cloud Management.

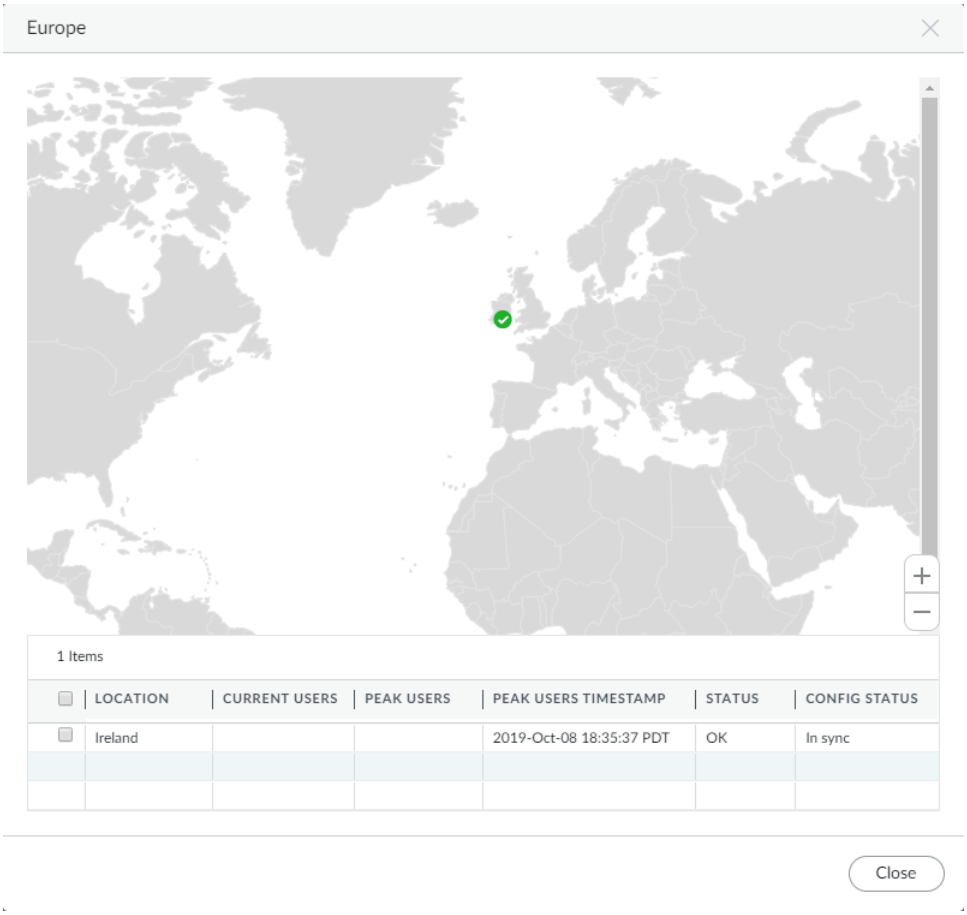
STEP 2 | View information on the status of your mobile user deployment on the **Dashboard**.



STEP 3 | Expand the **Dashboard** widget to see a map showing the locations you have onboarded.



STEP 4 | Drill down into a location for more details.


Europe
1 Items
LOCATION
CURRENT USERS
PEAK USERS
PEAK USERS TIMESTAMP
STATUS
CONFIG STATUS
Ireland
2019-Oct-08 18:35:37 PDT
OK
In sync
Close

Secure Remote Networks with Prisma Access

As your business scales and your office locations become geographically distributed, Prisma Access for networks allows you to onboard your branch networks and deliver best-in-breed security for your users. Prisma Access for networks removes the complexity in configuring and managing endpoints at every branch. It provides an efficient way to add new branches and minimize operational challenges with ensuring that users at these locations are always connected and secure.

For each branch that you want to secure using Prisma Access, you must push the required policy configuration to Prisma Access and onboard each branch so that you can start sending traffic from the branch site to Prisma Access through an IPSec tunnel.

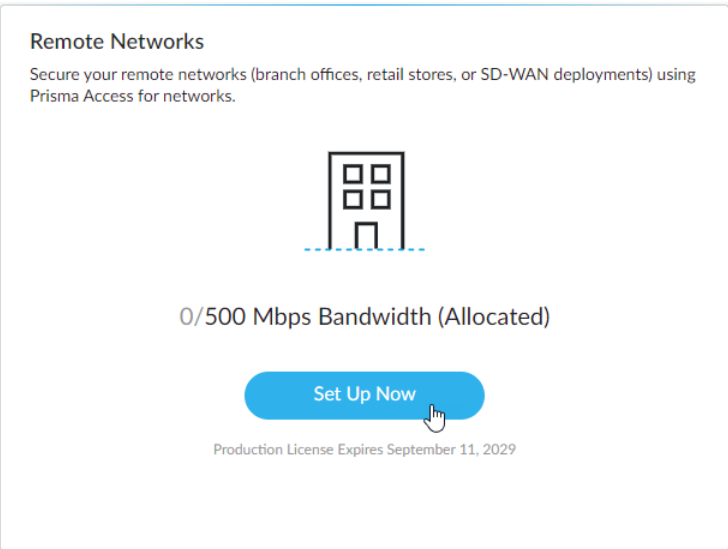
- Onboard a Remote Network
- Set Up a Primary IPSec Tunnel for Your Remote Network
- Set Up a Secondary IPSec Tunnel for Your Remote Network
- Enable Routing and QoS for Your Remote Network
- Enable Remote Networks to Access Internal Resources Using Service Connections
- Verify and Save Your Remote Network Configuration
- Manage Your Remote Network Configuration
- Monitor the Remote Network Status

Onboard a Remote Network

To add a new branch network to Prisma Access, you must specify the location and define the amount of bandwidth to allocate to the branch connection.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | From the **Dashboard**, click **Set Up Now** in the Remote Networks widget.



STEP 3 | **Branch Name** the branch.

STEP 4 | Select the amount of **Bandwidth** you want to allocate to this branch.

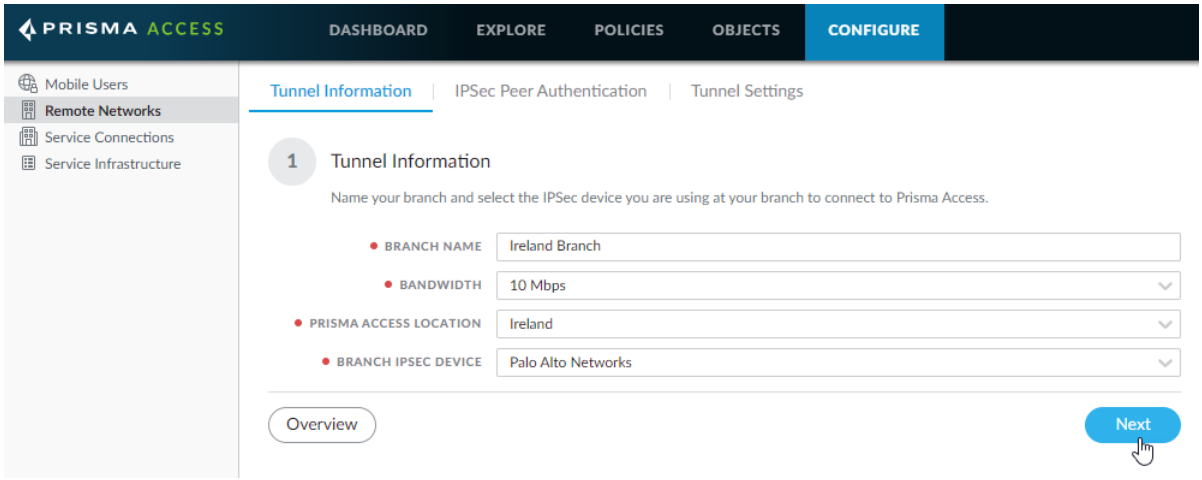
You can see how much of your licensed bandwidth is available on the **Dashboard** Remote Networks widget. To help you determine how much bandwidth a specific site needs, consider the bandwidth available from your ISP at each location. When calculating the amount of bandwidth you need at a site, consider that the bandwidth usage includes both egress and ingress traffic for the remote network connection. For example, if you set the bandwidth at a site to 50 Mbps, Prisma Access provides 50 Mbps of bandwidth on ingress and 50 Mbps of bandwidth on egress. Prisma Access allows bandwidth to go up to 10% over the amount you set for a site without dropping traffic (so, if you allocate 50 Mbps, Prisma Access will allow up to 55 Mbps on ingress and on egress). Calculating bandwidth requirements can be more tricky if you have asymmetric internet connections. In this case you will need to consider bandwidth to and from all of the remote networks in your Prisma Access instance to determine how to configure each site.

STEP 5 | Select the **Prisma Access Location** closest to where your branch is located.

STEP 6 | Select the **Branch IPSec Device** you are using at the branch site to establish an IPSec tunnel with Prisma Access.

Based on the device type you select, Prisma Access automatically populates default IKE crypto and IPSec crypto settings so that you don't have to configure them when you set up your IPSec tunnel(s).

STEP 7 | Click **Next** to Set Up a Primary IPSec Tunnel for Your Remote Network.



Set Up a Primary IPSec Tunnel for Your Remote Network

To secure your branch, all traffic to and from the branch network must go through Prisma Access. To do this, you must create an IPSec tunnel from your branch IPSec device to Prisma Access. The following workflow walks you through the steps to create this primary IPSec tunnel, which Internet Key Exchange (IKE) and IPSec configuration settings. You can optionally Set Up a Secondary IPSec Tunnel for Your Remote Network.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Start from **Configure** > **Remote Networks** > **IPSec Peer Authentication**.

- If you just finished the steps to Onboard a Remote Network, clicking **Next** takes you to this page automatically.
- If you've already onboarded your branch, select **Configure** > **Remote Networks** select the configuration, and **Edit** IPSec Peer Authentication.

STEP 3 | Select an **IKE Protocol Version** for your branch device and Prisma Access to use for IKE negotiation.

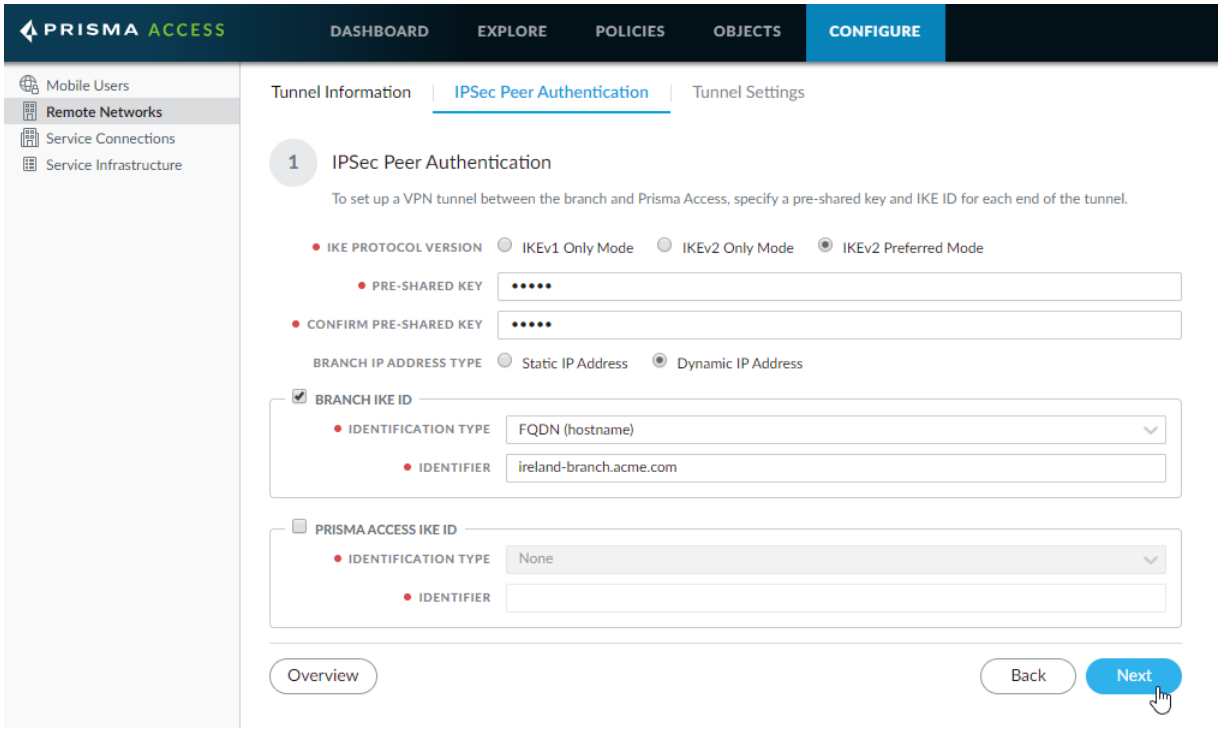
If you select **IKEv1 Only Mode**, Prisma Access can use only the IKEv1 protocol for the negotiation. If you select **IKEv2 Only Mode**, Prisma Access can use only the IKEv2 protocol for the negotiation. If you select **IKEv2 Preferred Mode**, Prisma Access uses the IKEv2 protocol only if your branch device also supports IKEv2. If your does not support IKEv2, Prisma Access falls back to using the IKEv1 protocol.

STEP 4 | Enter the **Pre-Shared Key** that your branch device and Prisma Access to will use to authenticate each other and then **Confirm Pre-Shared Key**.

STEP 5 | For **Branch IP Address Type**, specify whether you want to use a **Static IP Address** or a **Dynamic IP Address** to identify the tunnel endpoint.

- **Static IP Address**—If you select this option, enter the **Static IP Address** on your branch device to use as the endpoint for the IPSec tunnel.
- **Dynamic IP Address**—If you select this option, you must enable either **Branch IKE ID** or **Prisma Access IKE ID** and then supply the **Identification Type** and the corresponding **Identifier**.

Because you do not have the values to use for the Prisma Access IKE ID until the remote network is fully deployed, you would typically want to set the Branch IKE ID rather than the Prisma Access IKE ID. If you want to supply a Prisma Access IKE ID for additional peer validation after the remote network is deployed, enable Prisma Access IKE ID and then select the Identification Type you want to use to identify the Prisma Access IPSec device. You can find the Service IP for the Prisma Access peer on the Remote Networks summary page (Configure > Remote Networks), which you can use as the IKE ID.

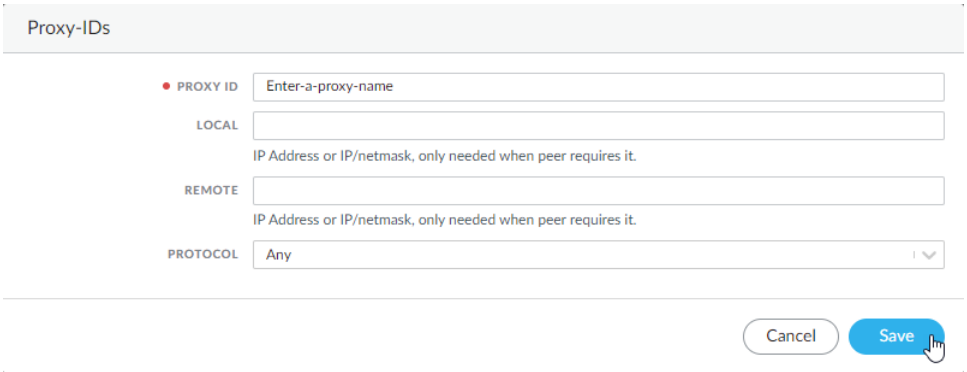


STEP 6 | Click **Next** to continue to the Tunnel Settings.

STEP 7 | If your branch IPSec device uses policy-based VPN, **Add** the Proxy IDs that match your policy.

You will only see the Proxy ID settings if the IPSec device type you selected supports policy-based VPN.

1. Enter a name to identify the **Proxy ID**.
2. Enter the **Local** IP address or subnet of the proxy.
3. Enter the **Remote** IP address or subnet of the proxy.
4. Specify the **Protocol**:
   - **Number**—Allows traffic for a given protocol number.
   - **Any**—Allows TCP and/or UDP traffic.
   - **TCP**—Allows only TCP traffic.
   - **UDP**—Allows only UDP traffic.



5. **Save** the Proxy ID settings.

STEP 8 | Enter a Tunnel Monitoring **IP Address** on the branch network for Prisma Access to use determine whether the tunnel is up and, if your branch IPSec device uses policy-based VPN, enter the associated **Proxy ID**.

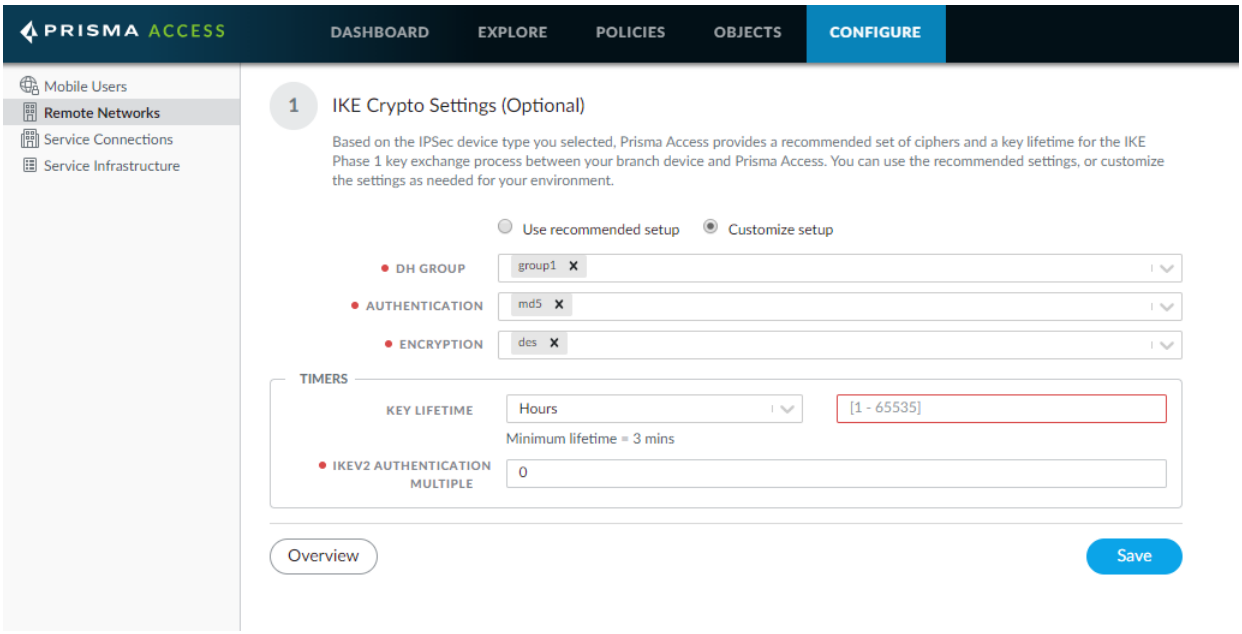
The tunnel monitoring IP address you enter is automatically added to the list of branch subnetworks.

STEP 9 | **Save** the tunnel settings

STEP 10 | (Optional) Customize the IKE crypto settings used to define the encryption and authentication algorithms used for the key exchange process in IKE Phase 1.

Prisma Access automatically configures a default IKE crypto profile based on the **IPSec Device Type** you selected when you onboarded the branch. You can either use the default profile or create a custom profile.

1. Specify whether you want to **Use Recommended Setup**, which enables Prisma Access to automatically identify the recommended IKE crypto settings for you, or **Customize Setup**, which enables you to define your own IKE crypto settings. If you **Customize Setup**, you must configure the following IKE crypto settings:



1. Specify the Diffie-Hellman (DH) groups used to generate symmetrical keys for IKE in the IKE SA negotiation. The Diffie-Hellman algorithm uses the private key of one party and the public key of the other to create a shared secret, which is an encrypted key that both VPN tunnel peers share.

   Prisma Access supports the following DH groups: Group 1 (768 bits), Group 2 (1024 bits—default), Group 5 (1536 bits), Group 14 (2048 bits), Group 19 (256-bit elliptic curve group), and Group 20 (384-bit elliptic curve group). For the strongest security, select the group with the highest number.
2. Specify the authentication algorithm used in the IKE SA negotiation.

   Prisma Access supports the following authentication algorithms: sha1 (160 bits), sha256 (256 bits), sha384 (384 bits), sha512 (512 bits), and md5 (128 bits). You can also select null (no authentication).
3. Specify the encryption algorithm used in the IKE SA negotiation.

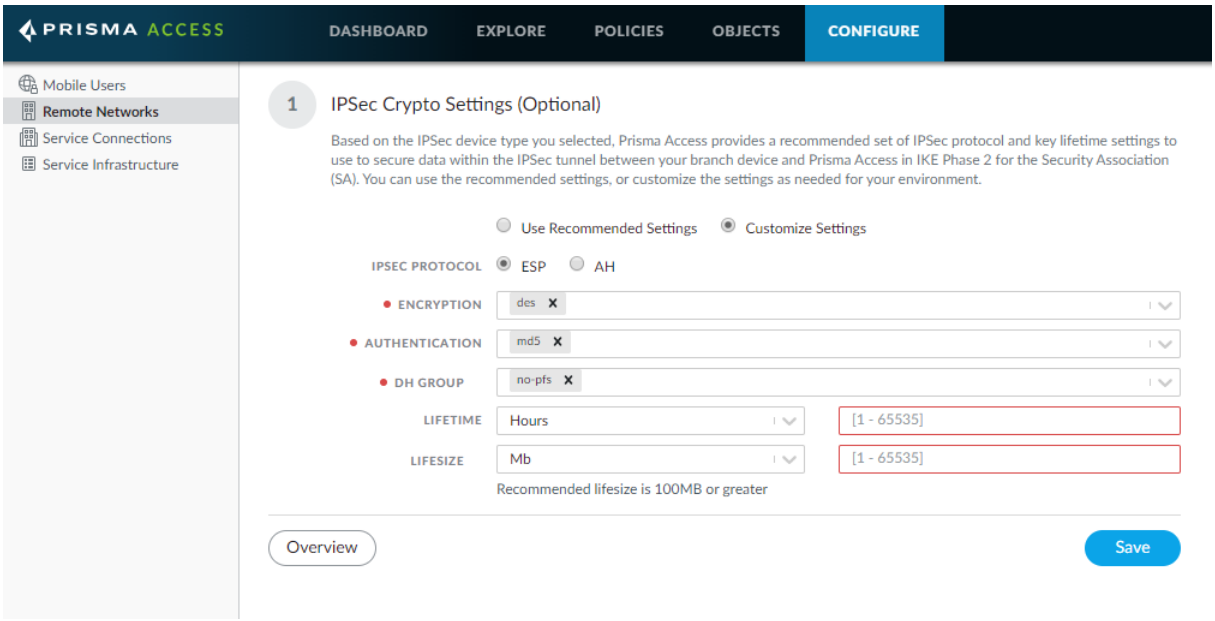
   Prisma Access supports the following encryption algorithms: 3des (168 bits), aes-128-cbc (128 bits), aes-192-cbc (192 bits), aes-256-cbc (256 bits), and des (56 bits). You can also select null (no encryption).

4. In the **Key Lifetime** field, specify the unit and amount of time for which the IKE Phase 1 key is valid (default is 8 hours). For IKEv1, the security association (SA) is not actively re-keyed before the key lifetime expires. The IKEv1 Phase 1 re-key triggers only when the SA expires. For IKEv2, the SA must be re-keyed before the key lifetime expires. If the SA is not re-keyed upon expiration, the SA must begin a new Phase 1 key.
5. Specify the **IKEv2 Authentication Multiple** value that is multiplied by the key lifetime to determine the authentication count (range is 0 to 50; default is 0). The authentication count is the number of times that the security processing node can perform IKEv2 IKE SA re-key before it must start over with IKEv2 re-authentication. The default value of 0 disables the re-authentication feature.
6. **Save** the configuration to return to the Remote Networks configuration summary.

STEP 11 | (Optional) Customize the IPSec crypto profile to define how data is secured within the tunnel when Auto Key IKE automatically generates keys for the IKE SAs during IKE Phase 2.

Prisma Access automatically configures a default IPSec crypto profile based on the **IPSec Device Type** vendor you selected when you onboarded the branch. You can either use the default profile or create a custom profile.

1. Specify whether you want to **Use Recommended Setup**, which enables Prisma Access to automatically identify the recommended IPSec crypto settings for you, or **Customize Setup**, which enables you to define your own IPSec crypto settings. If you **Customize Setup**, you must configure the following IPSec crypto settings:



1. Select an **IPSec Protocol** to secure the data that traverses the VPN tunnel. The Encapsulating Security Payload (**ESP**) protocol encrypts the data, authenticates the source, and verifies the data integrity. The Authentication Header (**AH**) protocol authenticates the source and verifies the data integrity.
2. (ESP protocol only) Specify the encryption algorithm used in the IPSec SA negotiation.

   Prisma Access supports the following encryption algorithms: aes-256-gcm (256 bits), aes-256-cbc (256 bits), aes-192-cbc (192 bits), aes-128-gcm (128 bits), aes-128-cbc (128 bits), 3des (168 bits), and des (56 bits). You can also select null (no encryption).
3. Specify the authentication algorithm used in the IPSec SA negotiation.

Prisma Access supports the following authentication algorithms: sha1 (160 bits), sha256 (256 bits), sha384 (384 bits), sha512 (512 bits), and md5 (128 bits). If you set the IPSec Protocol to ESP, you can also select none (no authentication).

4. Specify the Diffie-Hellman (DH) groups for IKE in the IPSec security association (SA) negotiation.

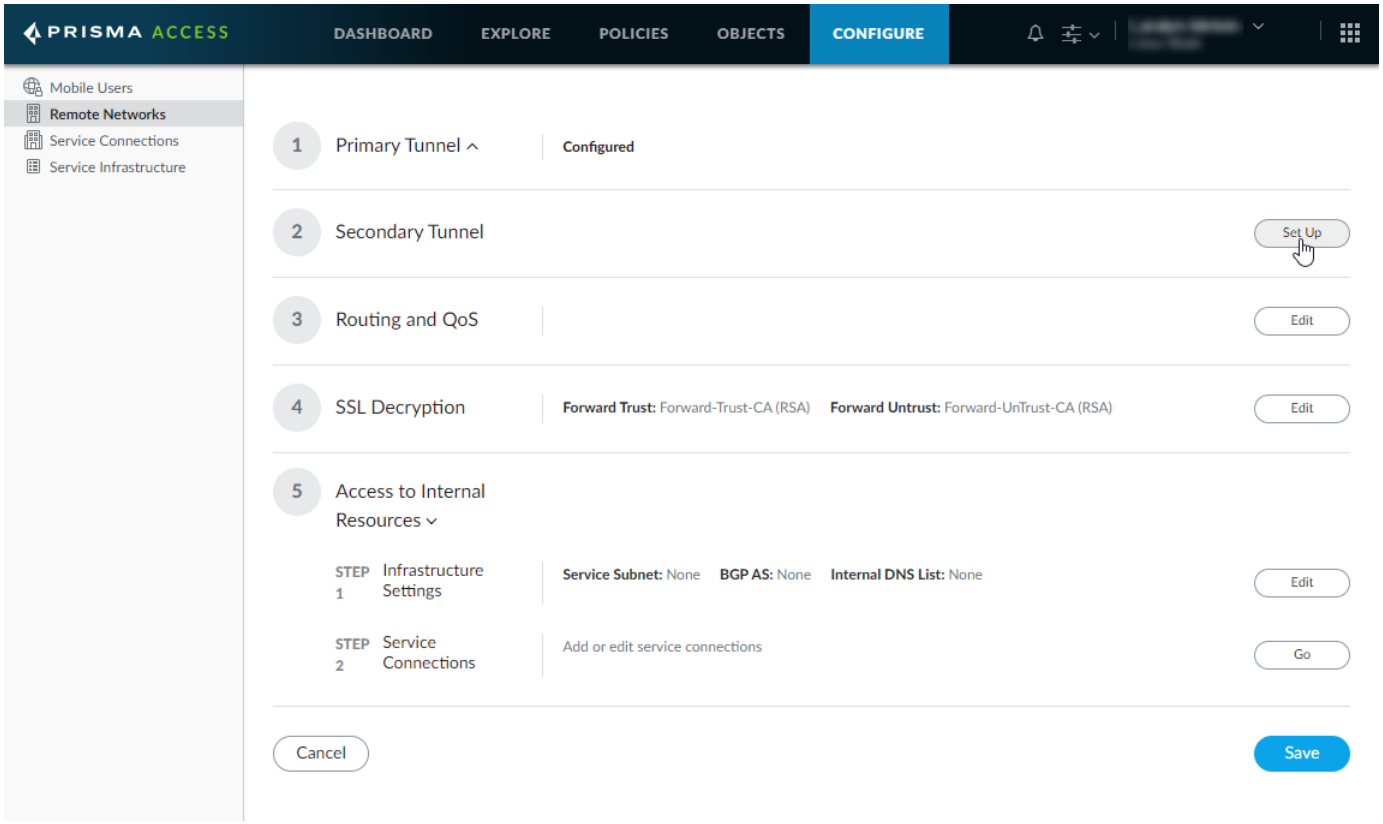
   Prisma Access supports the following DH groups: Group 1 (768 bits), Group 2 (1024 bits—default), Group 5 (1536 bits), Group 14 (2048 bits), Group 19 (256-bit elliptic curve group), and Group 20 (384-bit elliptic curve group). For the strongest security, select the group with the highest number. If you don't want to renew the key that Prisma Access creates during IKE phase 1, select **no-pfs** (no perfect forward secrecy). If you select this option, Prisma Access reuses the current key for the IPSec SA negotiation.
5. In the **Lifetime** field, specify the unit and amount of time during which the negotiated key is valid (default is one hour).
6. In the **Lifesize** field, specify the unit and amount of data that the key can use for encryption.
7. **Save** the configuration to return to the Remote Networks configuration summary.

Set Up a Secondary IPSec Tunnel for Your Remote Network

If the primary IPSec tunnel for your remote network goes down, the remote network falls back to the secondary IPSec tunnel until the primary IPSec tunnel comes back up. If both the primary and secondary IPSec tunnels are up, the primary IPSec tunnel takes priority over the secondary IPSec tunnel.

Use the following steps to set up a secondary IPSec tunnel for your remote network:

STEP 1 | From your Remote Networks configuration summary (**Configure** > **Remote Networks** > *<remote-network-config>*), **Set Up** an IPSec secondary tunnel from the remote site.



STEP 2 | Repeat the steps for configuring the primary IPSec tunnel configuration to configure your secondary IPSec tunnel.

STEP 3 | When you finish configuring the secondary IPSec tunnel, click **Save**.

Enable Routing and QoS for Your Remote Network

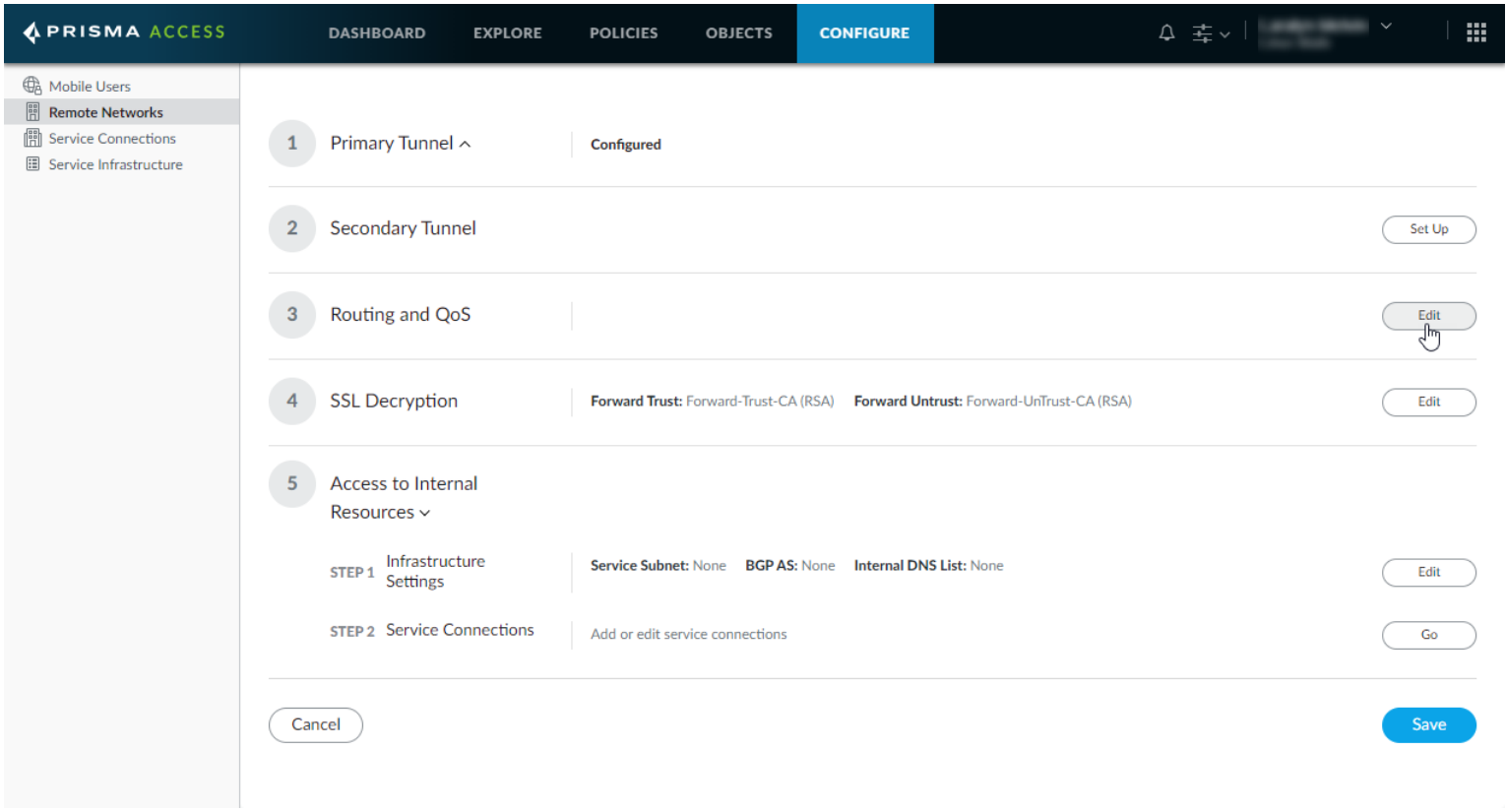
In order for Prisma Access to route traffic to your remote networks, you must provide routing information for the subnetworks that you want to secure using Prisma Access. You can do this in several ways. You can either define a static route to each subnetwork at the remote network location, or configure 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. Optionally, configure QoS to prioritize business-critical traffic or traffic that requires low latency.

- **Static Routes**—To enable static routes to and from your remote site to Prisma Access, identify the subnetworks and/or individual IP addresses at the remote site that you want Prisma Access to secure (for both inbound and outbound traffic). The subnetworks at each branch site much not overlap with each other, with the IP pools that you designated for Prisma Access for Users, or with the infrastructure subnet.
- **BGP**—If you want to enable BGP to dynamically route traffic to and from your remote network, you will need to provide the BGP information for the eBGP router at your branch:
  - **Branch Router Autonomous System (AS) Number**—The AS to which the eBGP router at the remote network belongs. This is called the **Peer AS**.
  - **Router ID**—The IP address assigned as the Router ID of the eBGP router on the remote network. This is called the **Peer Address**.

  If you configure both static routes and BGP routing, the static routes take precedence.
- **QoS**—If you plan to configure Prisma Access security policy rules to apply QoS markings to ingress traffic or you have a device at your branch that marks ingress traffic, you can shape the traffic egressing the remote network by defining a QoS profile that maps the classes you use to maximum and guaranteed bandwidth values. When you onboard the branch, you must select an existing QoS profile or create a new QoS profile.

Use the following steps to configure routing and QoS settings for your remote network:

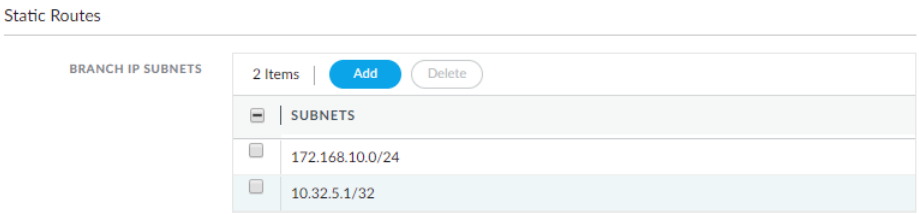
STEP 1 | From your Remote Networks configuration summary (**Configure** > **Remote Networks** > <*remote-network-config*>), and **Edit** Routing and QoS.



STEP 2 | Configure static routes.

If you are using static routes to route traffic and from your branch, **Add** the **IP Subnets** or IP addresses that you want to secure at the branch. Note that if you make any changes to the IP subnets on your branch, you must manually update the static routes.

If you are using BGP for dynamic routing in Prisma Access, you may also want to add static routes



STEP 3 | Configure dynamic routing.

To use dynamic routing to advertise your branch subnets, **Enable BGP** and then configure the following settings:

1. To prevent Prisma Access from forwarding routes into your remote network, select **Don't export routes**.

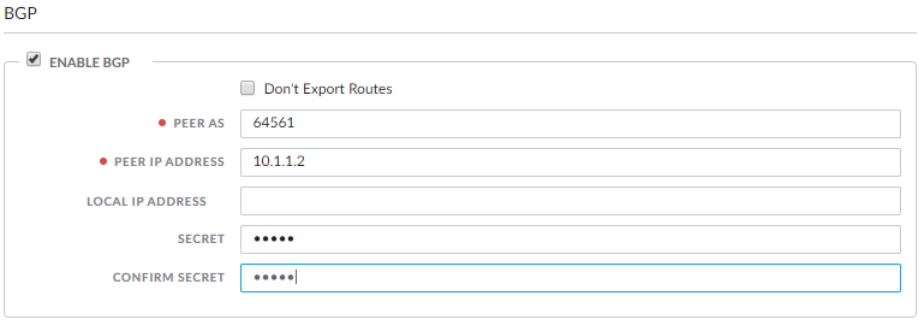
   By default, Prisma Access advertises all BGP routing information, including local routes and all prefixes it receives from other service connections, remote networks, and mobile user subnets. Select this check box to prevent Prisma Access from sending any BGP advertisements, but still use the BGP information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

Because Prisma Access does not send BGP advertisements, if you select this option you must configure static routes on your on-premise equipment to establish routes back to Prisma Access.

2. Enter the **Peer AS**, which is the autonomous system (AS) for your network.

   You must use an RFC 6696-compliant BGP Private AS number.
3. Enter the **Peer IP Address** assigned as the Router ID of the eBGP router on the remote network.
4. Enter the IP address that Prisma Access uses as its **Local IP Address** for BGP.

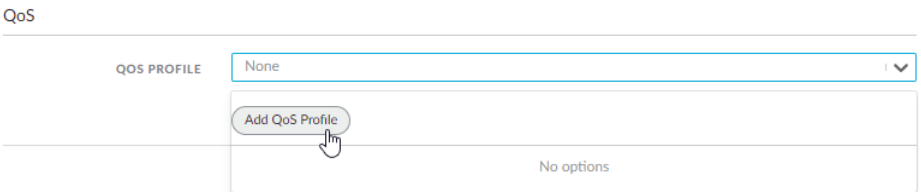
   A local address is only required if your branch device requires it for BGP peering to be successful. Make sure the address you specify does not conflict or overlap with IP addresses in the infrastructure subnet or subnets in the remote network.
5. Enter a **Secret** password to authenticate BGP peer communications and then **Confirm Secret**.



STEP 4 | (Optional) Configure a QoS profile that defines QoS classes needed to shape traffic for this branch network.

You will also need to create a QoS policy rule and assign the QoS profile to in order to enforce QoS on matching branch traffic.

1. From the **QoS Profile** drop down, select **Add QoS Profile**.

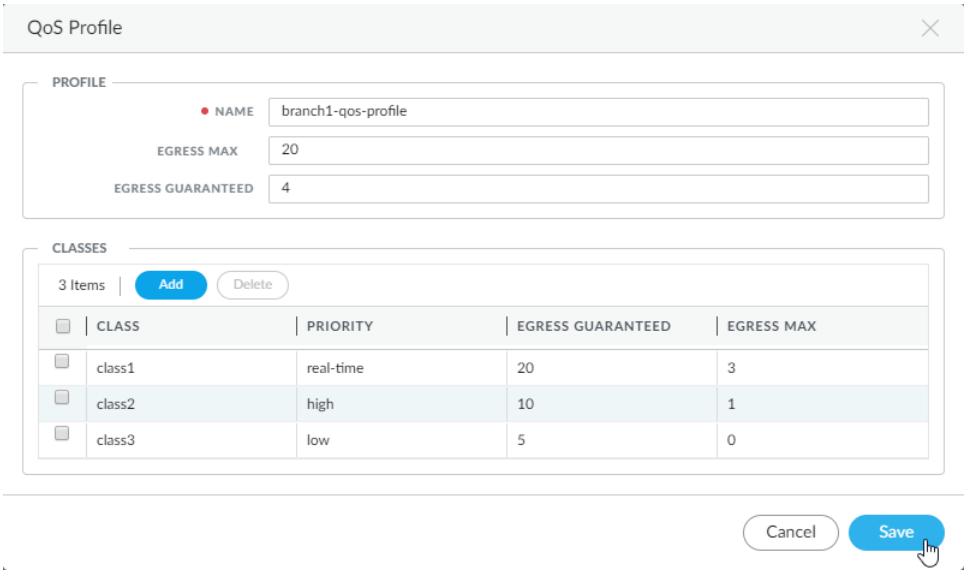


2. Enter a **Name** to identify the QoS profile.
3. Set the bandwidth limits for the QoS profile:
   - Set the maximum throughput (in Mbps) for traffic leaving the remote network connection as the **Egress Max**. You can specify a value up to the maximum licensed bandwidth of your remote network connection.
   - Set the guaranteed bandwidth as the **Egress Guaranteed** (in Mbps). Any traffic that exceeds the **Egress Guaranteed** value is best effort but not guaranteed. Any bandwidth that is guaranteed but unused remains available to all traffic.
4. **Add** the QoS **Classes** that you want to assign to this profile.

   A QoS class determines the priority and bandwidth for traffic matching a QoS policy rule. You can use a QoS profile rule to define QoS classes. There are up to eight definable QoS classes in a single QoS profile. Unless otherwise configured, traffic that does not match a QoS class is assigned a class of 4.
5. Select a QoS **Class** and set the **Priority** for the QoS class (**low priority**, **medium priority**, **high priority**, or **real-time**).

6. Set the **Egress Max** and **Egress Guaranteed** values for the QoS class.

   The **Egress Max** value for the QoS class must not exceed the **Egress Max** value for the QoS profile. In addition, the guaranteed bandwidth assigned to the QoS class is not reserved for that class; unused bandwidth remains available to all traffic. Any class traffic that exceeds the **Egress Guaranteed** value is best effort but not guaranteed.
7. Repeat these steps to **Add** additional classes.



8. **Save** the QoS profile.

STEP 5 | **Save** the routing and QoS configuration.

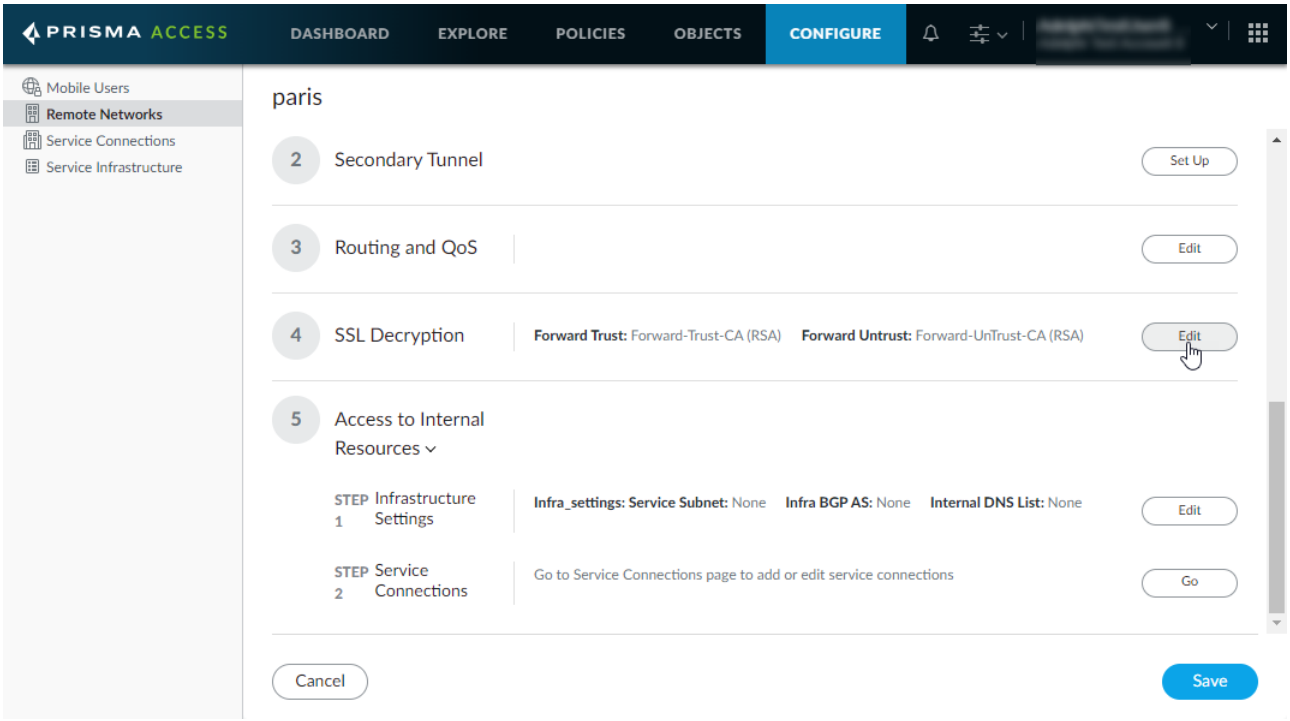
Enable SSL Decryption on the Remote Network

Prisma Access makes it easy for you to decrypt traffic by providing a default SSL decryption policy based on best practices and a default set of certificates to use for SSL decryption. It is important to decrypt traffic because you cannot protect against threats you cannot see. With decryption enabled, you prevent malicious encrypted content from entering your network and sensitive content from leaving your network concealed as encrypted traffic.

If you have already configured SSL decryption for your mobile user configuration, you do not need to configure it again.

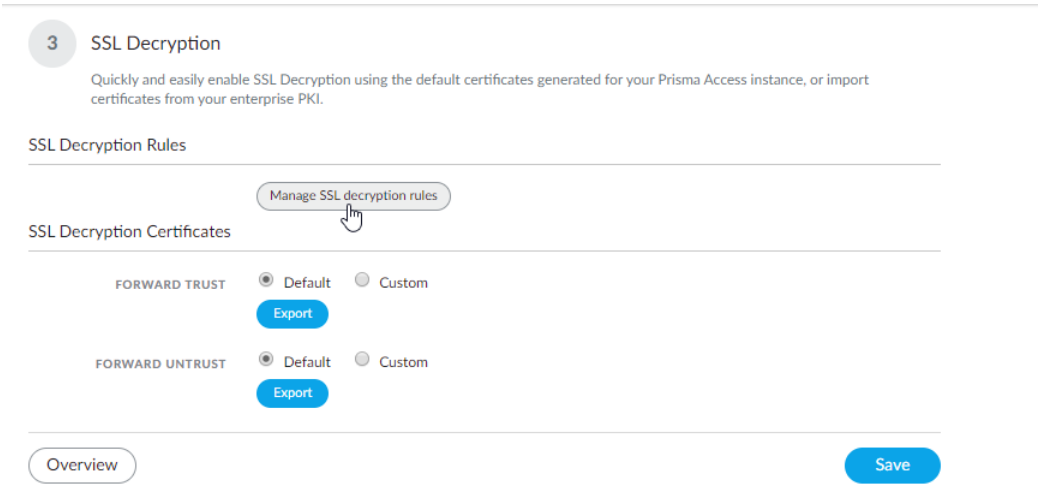
You can either use the default SSL decryption policy and certificates, or customize the SSL decryption settings.

STEP 1 | From your Remote Networks configuration summary (**Configure** > **Remote Networks** > *<remote-network-config>*) and **Edit** SSL Decryption.

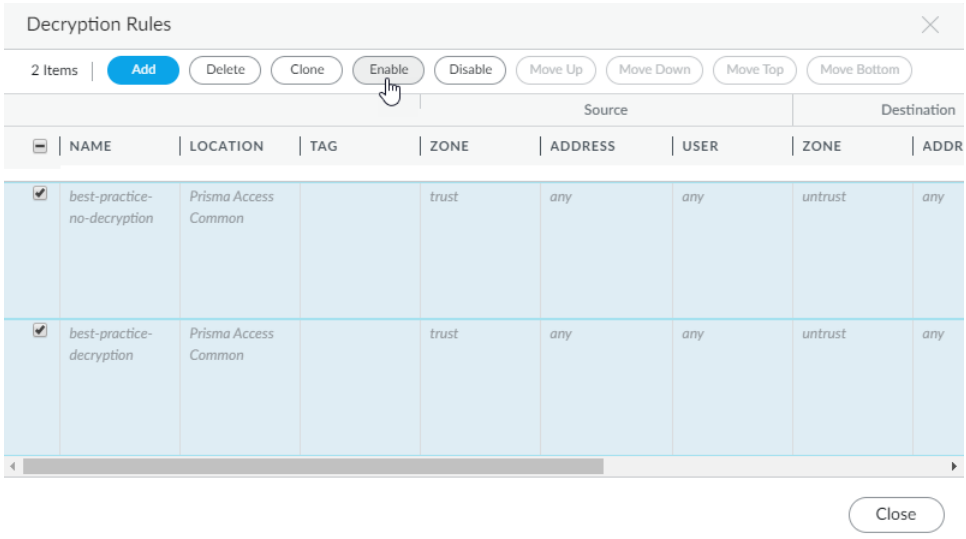


STEP 2 | To enable SSL decryption using custom decryption policy rules and certificates:

1. Click **Manage SSL decryption rules**.

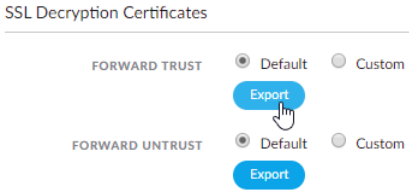


2. Select both best practice rules and **Enable** them and then **Close** the dialog.



3. **Export** the forward trust certificate and distribute it to the users at your branches.

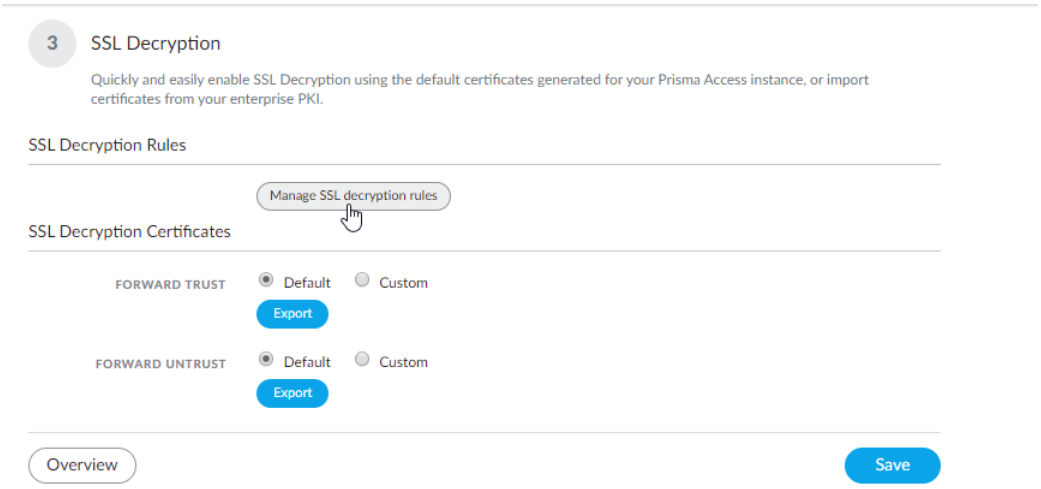
   You must distribute the forward trust certificate to your mobile users so that they do not see certificate errors when browsing to trusted sites. Do not distribute the untrust certificate because when a user attempts to access an untrusted site, you want them to see the warnings.



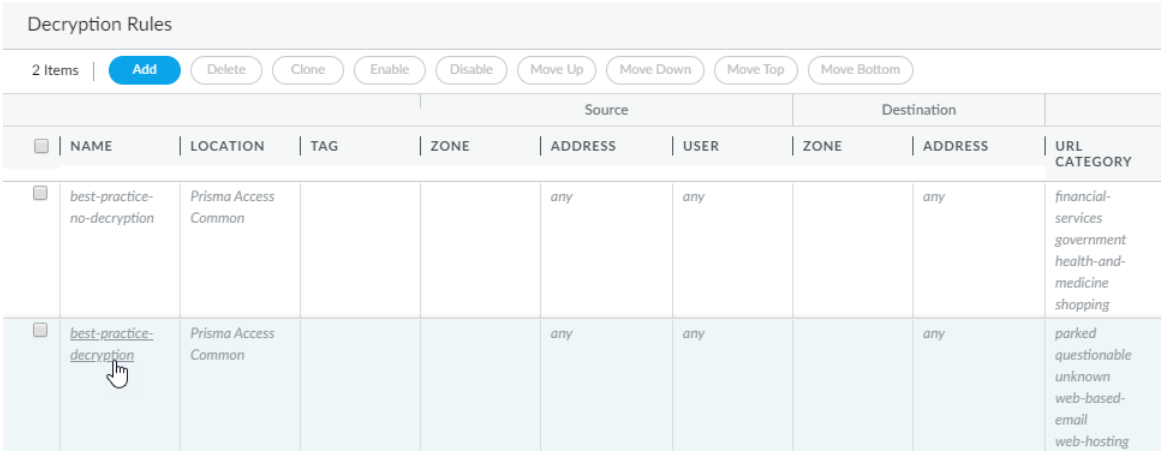
4. **Save** the decryption settings to return to the remote networks configuration summary.

STEP 3 | To enable SSL decryption using custom decryption policy rules and certificates:

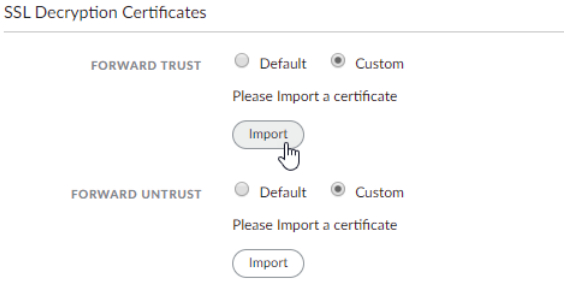
1. Click **Manage SSL decryption rules**.



2. Click on the rule name to edit a best practice decryption rule.

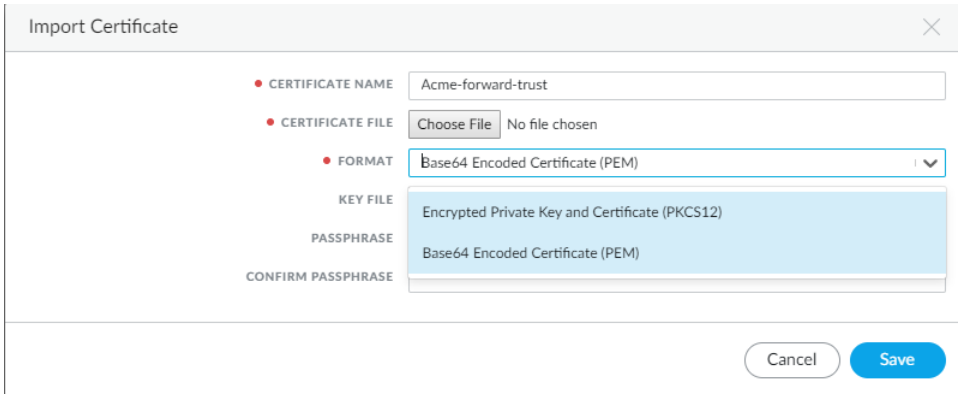


3. Customize the decryption policy rules for your environment and then **Save** the rule and dialog.
4. Select both best practice rules and **Enable** them and then **Close** the dialog.
5. To use your own **Custom** certificates, **Import** forward trust and forward untrust certificates with certificates from your enterprise PKI.



6. Define the certificate settings:
    1. Enter the **Certificate Name**.
    2. Select **Choose File** to import the **Certificate File** for the certificate.
    3. If the certificate **Format** is **Base64 Encoded Certificate (PEM)**, the key is in a separate file. In this case you must also click **Choose File** to import the **Key File** for the certificate.

4. Create a **Passphrase** and then **Confirm Passphrase**.



5. **Save** the certificate settings.
7. **Save** the decryption settings to return to the remote networks configuration summary.
8. Distribute the forward trust certificate to your mobile users.

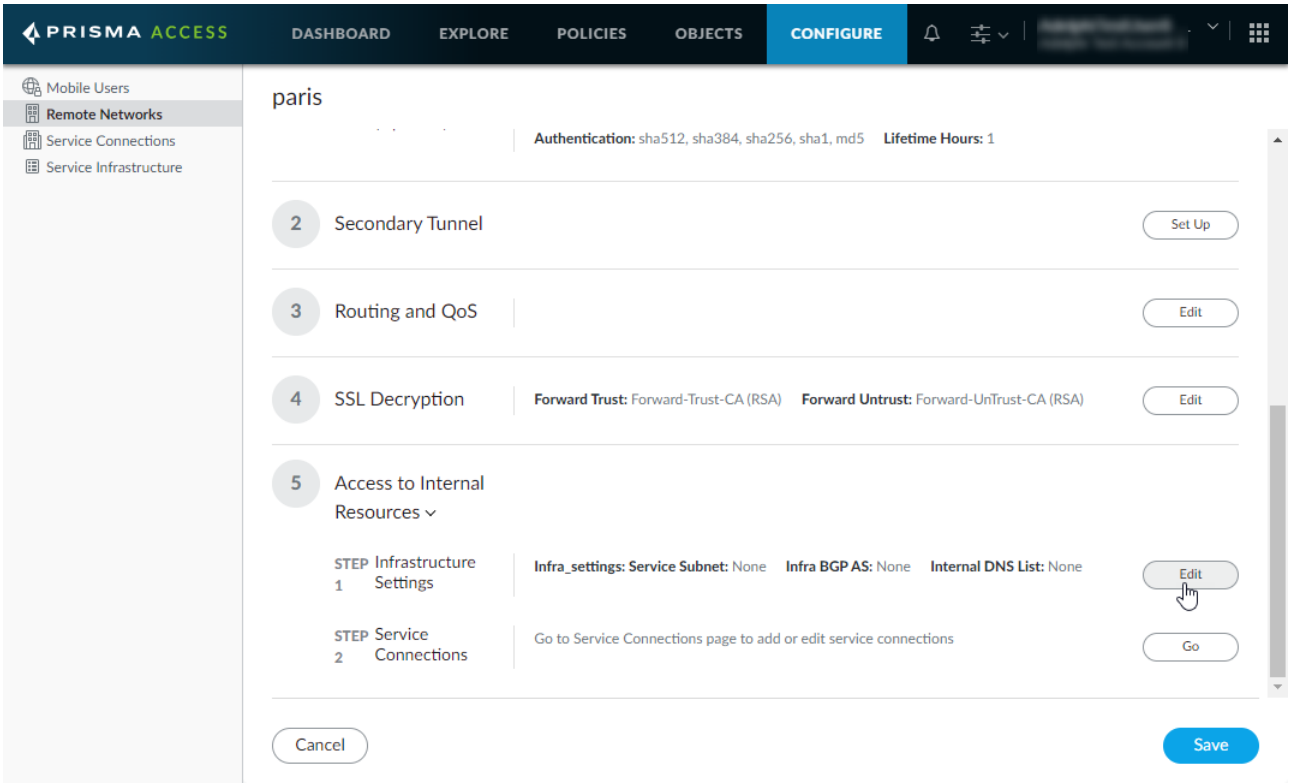
   You must distribute the forward trust certificate to your mobile users so that they do not see certificate errors when browsing to trusted sites. Do not distribute the untrust certificate because when a user attempts to access an untrusted site, you want them to see the warnings.

Enable Remote Networks to Access Internal Resources Using Service Connections

Use the following steps to configure a service connection that allows remote networks access to internal resources on your HQ or data center networks:

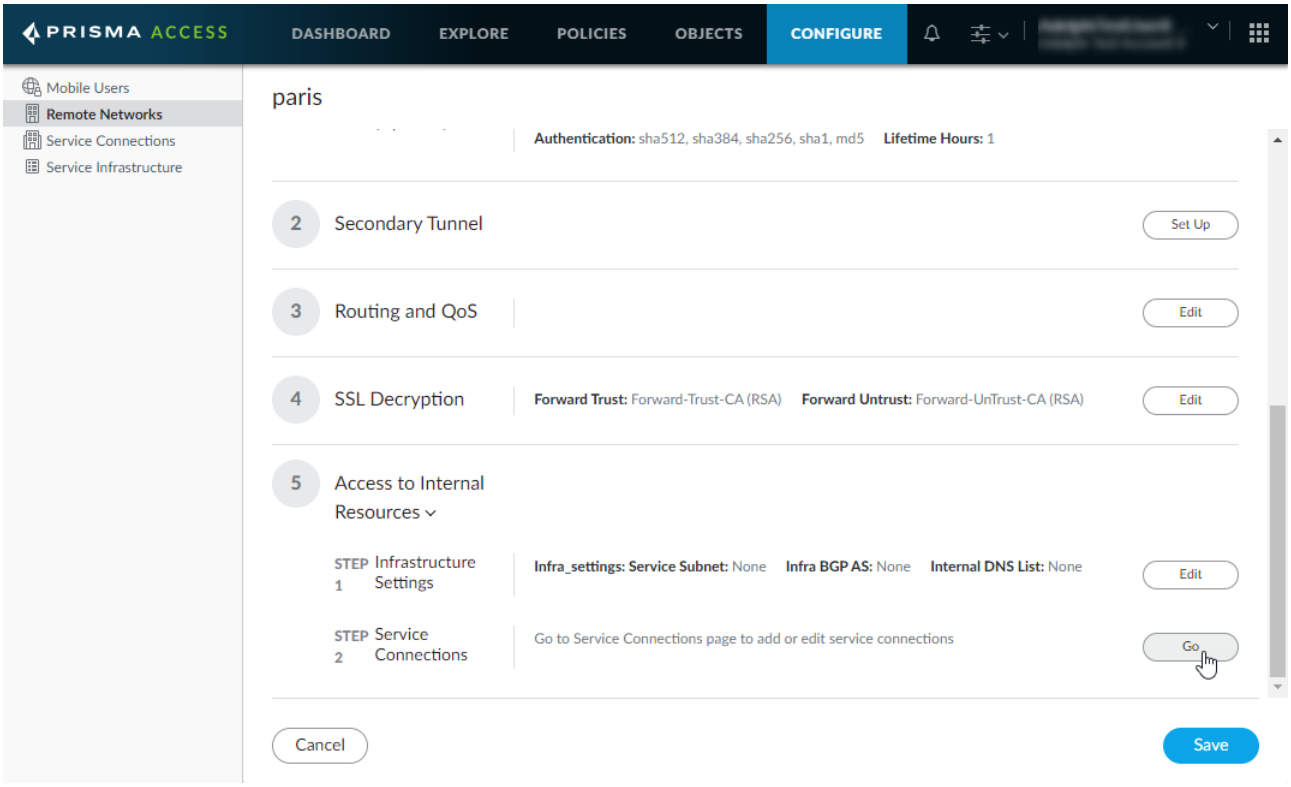
STEP 1 | From your Remote Networks configuration summary (**Configure** > **Remote Networks** > *<remote-network-config>*) and **Edit** the Infrastructure Settings.

STEP 2 | If you have not yet set up your Prisma Access infrastructure, **Edit** the **Infrastructure Settings** and then follow the steps to Set Up the Prisma Access Service Infrastructure.



STEP 3 | If you have not yet set up the service connection that users at this branch will need for access to resources on the HQ or data center network, **Edit** the **Infrastructure Settings** click **Go** and then follow the steps to Enable Access to Internal Resources Using Service Connections.

If you have made changes to your remote network configuration, you are prompted to **Save** the configuration before going to the service connection configuration settings.



STEP 4 | **Save** the configuration to return to the Remote Networks configuration summary.

Verify and Save Your Remote Network Configuration

Use the following steps to verify and save your remote network configuration:

STEP 1 | From your Remote Networks configuration summary (**Configure** > **Remote Networks** > <*remote-network-config*>), verify that your entire remote network configuration is correct.

STEP 2 | **Save** the remote network configuration.

STEP 3 | Commit and push the configuration to your remote networks.

Manage Your Remote Network Configuration

If you need to make any changes to an existing remote network configuration, use the following steps to view and modify the configuration:

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Select **Configure** > **Remote Networks** > *<remote-network-config>* to view your Remote Networks configuration summary.

STEP 3 | To modify an existing setting in your remote network configuration, **Edit** the setting.

STEP 4 | After you complete and verify your changes, **Save** the remote network confguration.

STEP 5 | Commit and push the configuration to Prisma Access.

Monitor the Remote Network Status

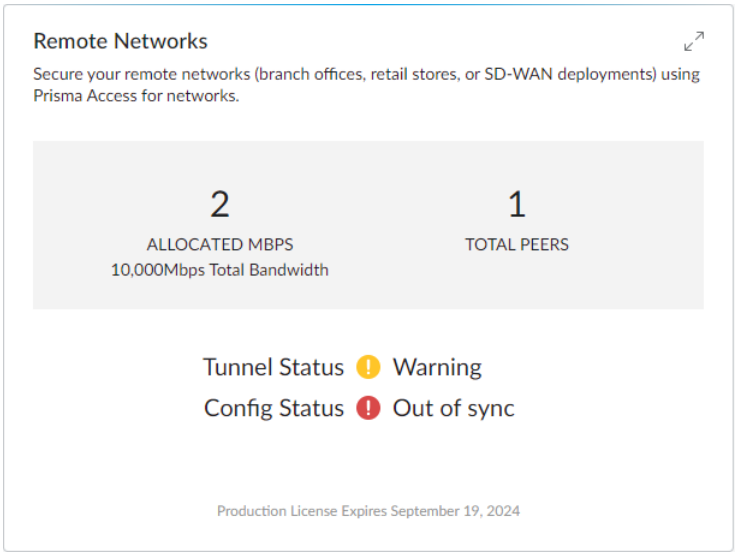
The Prisma Access **Dashboard** provides information on the status of your mobile user environment, remote network environment, and service connections. For remote networks, you can view the following information:

- **Tunnel Status**—Indicates the status of the IPSec tunnels between Prisma Access and your remote networks.
- **Config Status**—Indicates the status of your remote network configurations.
- **Total Peers**—Indicates the number of remote networks you have onboarded.
- **Allocated Mbps**—Indicates the amount of available remote network connection bandwidth (in Mbps) and the percentage of bandwidth that has already been used.
- **License Expires**—Indicates when the Prisma Access for networks license expires.

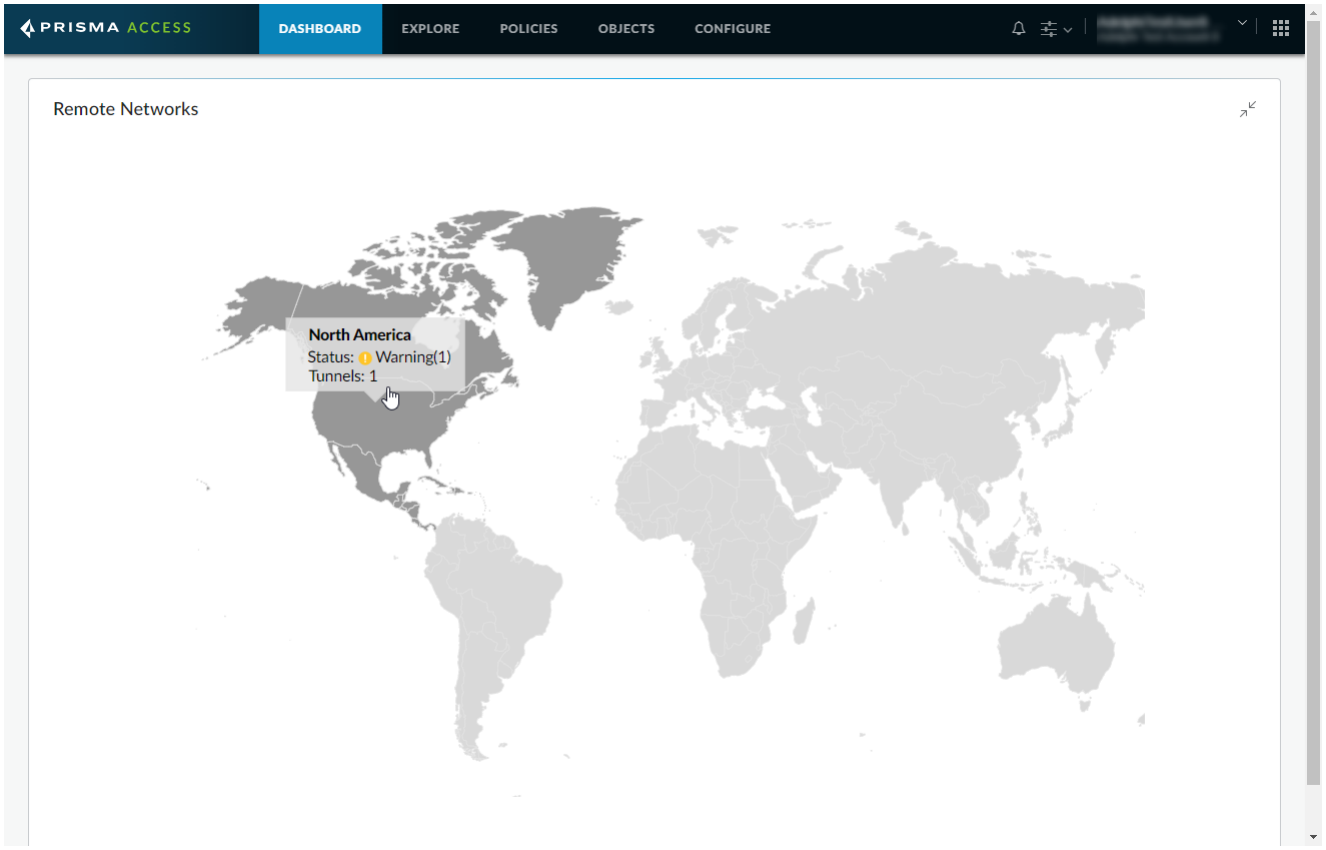
Use the following steps to monitor the status of your remote network environment:

STEP 1 | Launch Prisma Access Cloud Management.

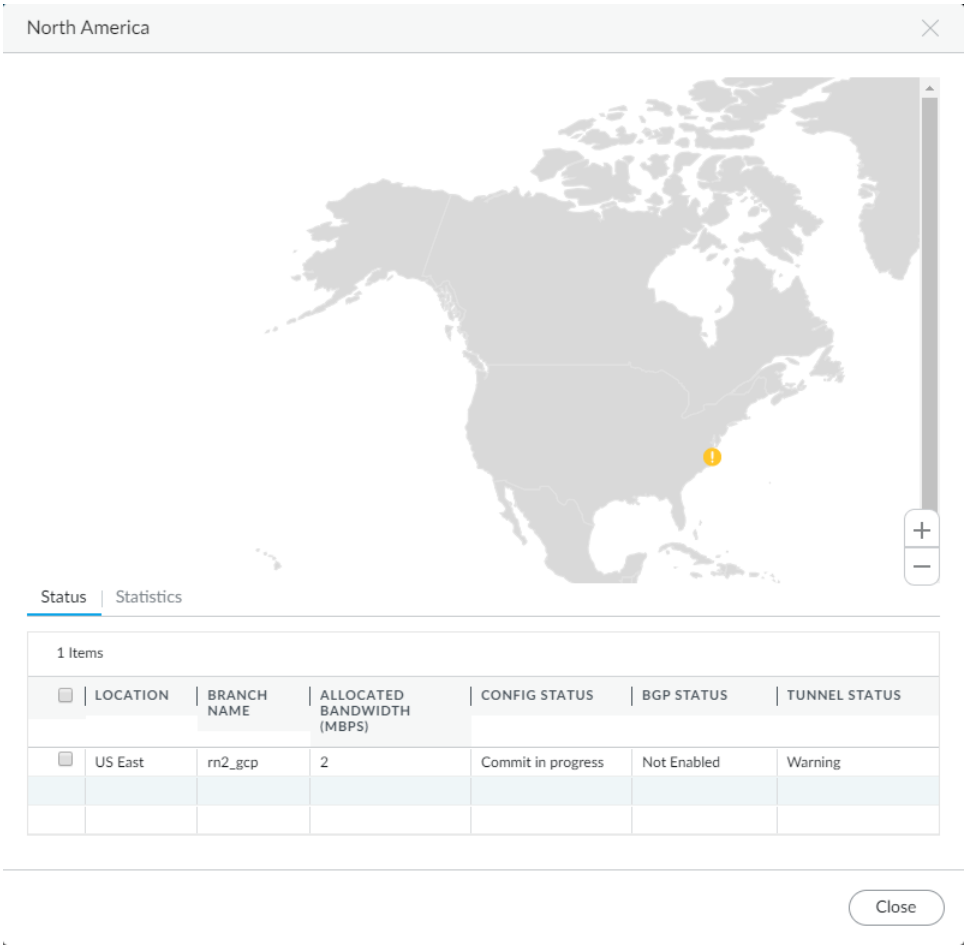
STEP 2 | Select **Dashboard** to view information on the status of your remote network environment, such as the configuration status and amount of available remote network bandwidth.



STEP 3 | Expand the **Dashboard** widget to see a map showing the locations you have onboarded.



STEP 4 | Drill down into a location for more details.



Manage the Prisma Access Service Infrastructure

To set up your 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 that you use internally. Prisma Access uses the IP addresses within this subnet to establish a network infrastructure between your remote network locations and mobile users, and from your service connections to your headquarters and/or data center (if applicable). This infrastructure enables Prisma Access to determine the service routes for services such as DNS, as well as enable other inter-service communication. Because a large number of IP addresses are required to set up the infrastructure, you must use a /24 subnet (for example, 172.16.55.0/24). This subnetwork is an extension of your existing network, and therefore, cannot overlap with any IP subnets that you use within your corporate network or with the IP address pools that you assign to your Prisma Access for users deployment.

Set Up the Prisma Access Service Infrastructure

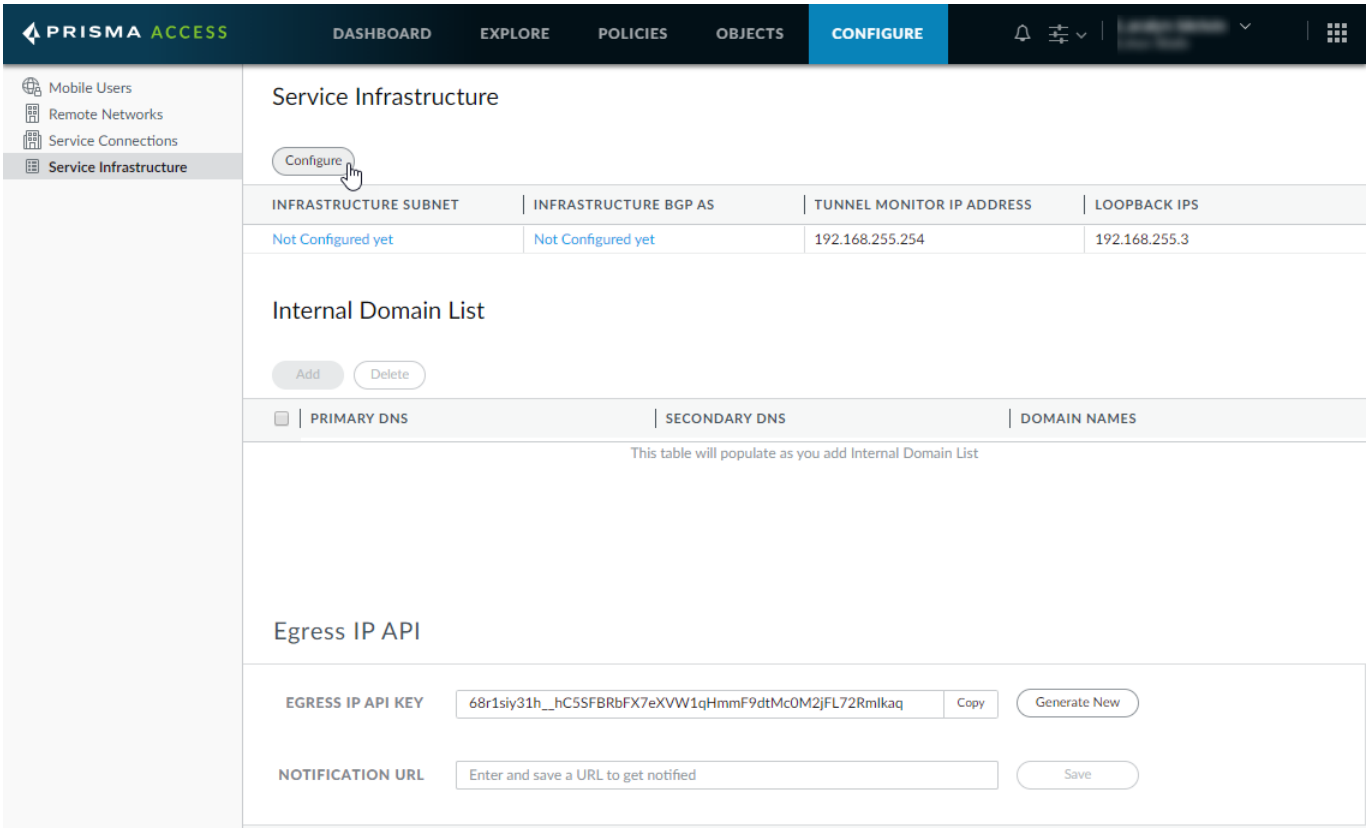
To enable communication between your remote network locations, mobile users, and the HQ or data centers that you plan on connecting to Prisma Access over service connections, you must set up the service infrastructure subnet, which Prisma Access will use to create the network backbone for communication between your branch networks, mobile users and the Prisma Access security infrastructure, as well as with the HQ and data center networks you plan to connect to Prisma Access over service connections. If you use dynamic routing for your remote networks or service connections, you must also configure an RFC 6696-compliant BGP Private AS number.

Use the following recommendations and requirements when you add an infrastructure subnet for Prisma Access:

- Use an RFC 1918-compliant subnet. While the use of non-RFC 1918-compliant (public) IP addresses is supported, it is not recommend because of possible conflicts with the 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 internal use.
- This subnetwork is an extension to your existing network and therefore, cannot overlap with any IP subnets that you use within your corporate network or with the IP address pools that you assign for Prisma Access for users or Prisma Access for networks.
- Because the service infrastructure requires a large number of IP addresses, you must designate a /24 subnetwork (for example, 172.16.55.0/24).

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Select **Configure** > **Service Infrastructure** to **Configure** the service infrastructure.



STEP 3 | Enter an **Infrastructure Subnet** that Prisma Access can use to enable communication between your remote network locations, mobile users, and the HQ or data centers that you plan on connecting to Prisma Access over service connections.

Use an RFC 1918-compliant subnet for the infrastructure subnet. While the use of non-RFC 1918-compliant (public) IP addresses is supported, it is not recommend because of possible conflicts with the internet public IP address space.

STEP 4 | Enter the **Infrastructure BGP AS** you want to use within the Prisma Access infrastructure.

If you want to enable dynamic routing so that Prisma Access can dynamically discover routes to resources in your remote networks and HQ or data center locations, you must use the Border Gateway Protocol (BGP). The **Infrastructure BGP AS** is the autonomous system (AS) number that identifies the routes through which BGP can send traffic. If you do not supply an AS number, Prisma Access uses the default AS number (65534).

If you want to specify your own AS number, you must use an RFC 6996-compliant private AS number. Accepted formats are 4-Byte AS Plain [64512-65534],[4200000000-4294967294] or AS Dot [0.64512-0.65534], [64086.59904-65535.65534] notation.

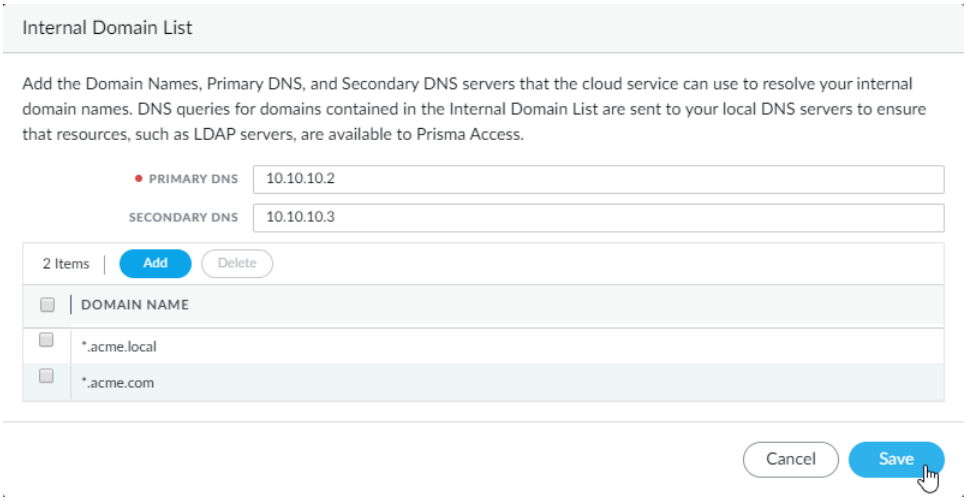
STEP 5 | **Save** the service infrastructure settings.

STEP 6 | To enable Prisma Access to resolve your internal domains, **Add** an **Internal Domain List**.

If you plan on configuring service connections to enable access to resources in your corporate network and you also need Prisma Access to resolve your internal domains, you must define the list of internal domains. DNS queries for domains in the **Internal Domain List** are sent to your local DNS servers to ensure that resources are available to Prisma Access remote network users and mobile users.

1. Enter the **Primary DNS** server and **Secondary DNS** server that Prisma Access should use to resolve the internal domain names.
2. **Add** the internal **Domain Names** that you want Prisma Access to resolve.

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



STEP 7 | **Save** the internal domain list settings.

STEP 8 | If you enable your users to access applications based on source IP address, you will need to get the list of IP addresses that traffic from Prisma Access uses as the source address so that you can whitelist them in your application access policies.

Copy the **Egress IP API Key** to enable use of the Prisma Access Egress IP Address API. Also, because the IP addresses that Prisma Access uses change periodically—for example when you add a new location, when Prisma Access needs to scale resources in an existing location, or when there is an infrastructure upgrade—you need to know when the IP addresses change so that you can update your policy rules, or automate these updates by defining a **Notification URL**. See Retrieve the IP Addresses to Whitelist for Prisma Access for more details.

STEP 9 | Commit and push the service infrastructure configuration.

Click the  menu and select **Commit and Push**.

Retrieve the IP Addresses to Whitelist for Prisma Access

Traffic originating from your Prisma Access mobile users and users at your remote networks uses IP addresses allocated by Prisma Access. If you use security policy rules based on source IP address to enable your Prisma Access users to access internet resources (such as sanctioned SaaS applications or publicly-available partner applications), or applications in your corporate headquarters and data centers, you must get the IP Addresses that Prisma Access uses so that you can whitelist them. Because the IP addresses that Prisma Access uses change periodically—for example when you add a new location, when Prisma Access needs to scale resources in an existing location, or when there is an infrastructure upgrade—you need to know when the IP addresses change so that you can update your policy rules, or automate these updates. The following topics detail the types of IP addresses Prisma Access uses, how to retrieve them, and how to make sure you receive notification of IP address changes.

What IP Addresses do I Need to Whitelist?

Prisma Access uses three different types of IP addresses that you need to whitelist:

- **Public IP Addresses**—When a Prisma Access user (a mobile user or a user at a branch secured by Prisma Access) makes a request to access a resource on the internet, such as a sanctioned SaaS application or a publicly accessible partner application, the source IP address in the request is a public IP address from Prisma Access rather than the IP address of the end user. Therefore, if you use security policy based on source IP address to allow users secured by Prisma Access to access publicly available applications, you will need to get the list of public IP address that Prisma Access uses so that you can whitelist them in your policy rules.

  There are some events that cause the list of public IP addresses that Prisma Access uses to change:

  - **Public IP addresses for Prisma Access for users**— With Prisma Access for mobile users, there are two sets of public IP addresses: active and reserved. Whenever the Prisma Access infrastructure upgrades, the active and reserved public IP addresses swap, and revert back after the upgrade completes. Therefore, for mobile network users you must whitelist both the active and reserved public IP addresses to ensure uninterrupted access.
  - **Public IP addresses for Prisma Access for networks**— With Prisma Access for remote networks, the IP addresses only change when you add a new branch to your deployment or when you increase the bandwidth at an existing branch so that the total bandwidth in the region where the branch is located surpasses 300 Mbps (either at a single branch or across multiple branches). Increasing the bandwidth in a region beyond 300 Mbps causes Prisma Access to provision an additional service IP address. Note that is only the case when you upgrade an existing remote network; if you initially provision a remote network with bandwidth over 300 Mbps, Prisma Access uses a single service IP address for the site.

Subscribe to text or email notices for upcoming scheduled infrastructure upgrades at status.paloaltonetworks.com.

- **Egress IP Addresses**—An egress IP address is an IP address that Prisma Access uses for egress traffic to the internet for both mobile user and remote network traffic.

  All locations have public IP addresses; however, not all locations have egress IP addresses. Among other purposes, Prisma Access uses egress IP addresses so that users receive web pages in the language they expect from a Prisma Access location. Prisma Access has more than 100 locations available to accommodate worldwide deployments and provide a localized experience. Prisma Access maps each location to a compute location based on performance and latency. If you onboard more than one location that maps to the same compute location, two locations might map to the same service IP address. However, the locations might use different egress IP addresses to make sure that the user gets the correct default language for the region. For example, if you deploy two remote networks in Canada: Central Canada and Eastern Canada, both locations map to the Canada compute location, and Prisma Access assigned both locations with the same service IP address. However, because Eastern Canada uses a different default language (French) than Central Canada (English), Prisma Access assigns them different egress IP addresses. If you run the API script for egress IP addresses, you will receive two different IP addresses for these two locations.The following locations do not use egress IP addresses:

  - France North
  - France South
  - Any locations that map to a single compute location (Hong Kong, Ireland, South Korea, Taiwan, United Kingdom)
- **Loopback IP Addresses**—When a Prisma Access user (a mobile user or a user at a branch secured by Prisma Access) makes a request to a resource at your corporate headquarters or data center over a service connection, the source IP address in the request is a loopback IP address that Prisma Access assigns from the infrastructure subnet that you configured when you Set Up the Prisma Access Service Infrastructure. If you are using Prisma Access for users, you should whitelist the entire infrastructure subnet in security policy rules that allow access to resources on your corporate network because the loopback IP addresses change during infrastructure upgrades. If you are only using Prisma Access for networks and you enforce application access based on source IP address, you can whitelist only the service IP address that are currently in use for your existing remote networks, updating the list whenever you add a new branch.

  Subscribe to text or email updates for upcoming scheduled infrastructure upgrades at status.paloaltonetworks.com

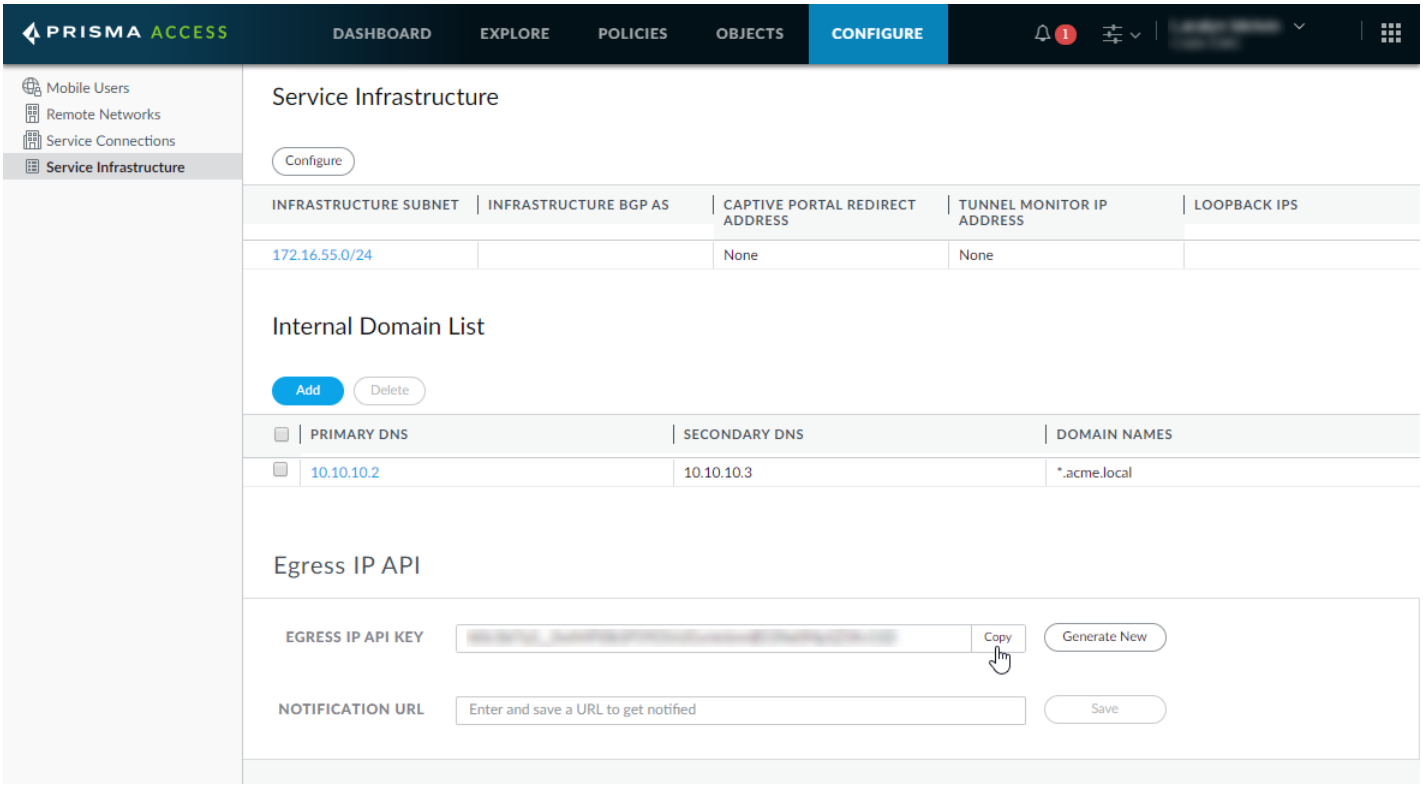
Get your API Key and Set Up IP Address Change Notifications

Because the IP addresses Prisma Access uses can change—for example when you add a new location, when an existing location has a scaling event, or when there is an infrastructure update—you will need to update your security policy to whitelist the IP addresses Prisma Access uses. Prisma Access allows you to specify a notification URL at which you can be alerted of a change. Typically, change happens either because you onboarded or deleted a new remote network location or Prisma Access initiated a change to support the demands from your network, such as scaling out to support a surge in traffic in a specific location.

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.

1. Select **Configure** > **Service Infrastructure**.
2. **Copy** the **Egress IP API Key** for use in the commands for retrieving IP addresses.



To ensure the security of your API key, rotate it periodically by clicking Generate New. You will then need to update the key in all of your scripts.

STEP 2 | Add an **Notification URL** where Prisma Access can send notification of IP address changes in your Prisma Access infrastructure.

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

After you set up the notification URL, Prisma Access uses an HTTP POST request to send the notification. This POST request includes the following notification data in JSON format:

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

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

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

When you receive a notification, you must follow a two-step process. First, you must manually or programatically retrieve the list 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. Use automation scripts to both retrieve and whitelist the new IP addresses.

Retrieve IP Addresses for Mobile User Deployments

Prisma Access provides two sets of public IP and egress IP addresses so that it can automatically add locations during a scaling or other event (for example, when a large number of mobile users join a single gateway):

- One set that is assigned to Prisma Access locations 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 or scale out in an existing location.

If you are enabling application access based on source IP address, to ensure that your mobile users can always access the resources they need whitelist the entire set of IP addresses (including the reserved addresses). If you do not want to whitelist the entire list of IP addresses, you can instead get the list of active IP addresses only.

STEP 1 | Get your API Key and Set Up IP Address Change Notifications.

STEP 2 | If you want to retrieve all mobile user public IP and egress IP addresses, including IP addresses that are reserved for a scaling event and are not currently active use the following command:

```
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"
```

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.

STEP 3 | If you want to retrieve only the currently active public IP, egress IP, and/or loopback IP addresses used in your mobile user deployment, run the following commands:

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

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

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

Keyword/Argument	Description
fwType keyword	
gpcs_gp_gw	Retrieves Prisma Access security processing node IP addresses (for mobile user deployments).
gpcs_gp_portal	Retrieves Prisma Access edge security processing node IP addresses (for mobile user deployments).
addrType keyword (If you do not use this keyword, Prisma Access returns all IP address types)	
public_ip	Retrieves the source IP addresses that Prisma Access uses for requests to access internet resources, such as SaaS applications. For mobile user locations, Prisma Access lists the IP addresses by location.
egress_ip_list	Retrieves the IP addresses that Prisma Access uses with public IP addresses for additional egress traffic to the internet. For mobile user locations, Prisma Access lists the IP addresses by location.
loopback_ip	Retrieves the source IP addresses used by Prisma Access for requests made to internal resources, and is assigned from the service infrastructure IP address pool.

If you don't specify the addrType keyword, Prisma Access retrieves all currently active public IP addresses, egress IP addresses, and loopback IP addresses.

For example, use the following Curl command to manually retrieve the list of active IP addresses for your mobile user deployment you would run the following commands:

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

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

Use the API key and the API endpoint URL either manually or in an automation script where you need to replace *Current API Key* with your API key.

Or, use a simple python script to retrieve the list of all active public IP addresses, egress IP addresses, and loopback IP addresses for your mobile user deployment, for example:

```
#!/usr/bin/python
import subprocess
import json
api_key = '12345abcde' # Replace with your key
```

```
api_end_point = 'https://api.gpcloudservice.com/getAddrList/latest?
fwType=gpcs_gw' # This call retrieves active IP addresses for all your
 mobile user edge security processing nodes
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)
api_end_point = 'https://api.gpcloudservice.com/getAddrList/latest?
fwType=gpcs_portal' # This call retrieves active IP addresses for your
 mobile user security processing nodes
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 4 | Update the whitelists on your on-premises servers or SaaS application policy rules with the IP addresses you retrieved.

Retrieve IP Addresses for Your Remote Networks

You can retrieve the list of source IP addresses that Prisma Access uses for the traffic to the internet, to SaaS applications, or to your internal services using the Prisma Access Egress IP APIs. You will need to get this list if you whitelist access to applications and services based on Source IP to ensure that users at your remote networks can always access the resources they need.

For remote networks, the public or egress IP address might be different from the Service IP Address. Prisma Access maps each remote network location to a compute location based on performance and latency. If you onboard more than one location that maps to the same compute location, two locations might map to the same service IP address. However, the locations might use different egress IP addresses to make sure that the user gets the correct default language for the region.

STEP 1 | Get your API Key and Set Up IP Address Change Notifications.

STEP 2 | Retrieve the public IP addresses, egress IP addresses, and/or loopback IP addresses, for the remote networks you have deployed.

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

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

where you need to replace *Current API Key* with your API key and use one of the following arguments for the $addrType keyword, or retrieve all address types, do not include this keyword:

Keyword/Argument	Description
addrType keyword	
public_ip	Retrieves the source IP addresses that Prisma Access uses for a resource on the internet, such as a SaaS application. For remote networks, Prisma Access lists the IP addresses by remote network name.
egress_ip_list	Retrieves the IP addresses that Prisma Access uses with public IP addresses for additional egress traffic to the internet. For remote networks, Prisma Access lists the IP addresses by remote network name.
loopback_ip	Retrieves the source IP addresses used by Prisma Access for requests for internal resources. Loopback IP addresses are assigned from the infrastructure subnet.

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

For example, use the following Curl command to manually retrieve the list of public IP addresses for all remote network locations:

```
curl -k -H header-api-key:12345abcde "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 your remote network deployment, for example:

```
#!/usr/bin/python
import subprocess
import json
api_key = '12345abcde' # Replace with your key
api_end_point = 'https://api.gpcloudservice.com/getAddrList/latest?
fwType=gpcs_remote_network' # This call retrieves IP addresses for your
 remote network deployments
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.

Manage Prisma Access Service Connections

Service connections enable both mobile users and users at your branch networks to access resources in your HQ or data center. Beyond providing access to corporate resources, service connections allow your mobile users to reach branch locations.

- > Plan Your Service Connection
- > Enable Access to Internal Resources Using Service Connections
- > Manage Your Service Connection Configuration
- > Monitor the Service Connection Status

Plan Your Service Connection

Create service connections to allow Prisma Access to perform the following tasks:

- Allow access to the resources in your HQ or data center.

  If you have corporate resources that your remote networks and mobile users need to access, you must enable Prisma Access to access the corresponding corporate network.
- Allow remote networks and mobile users to communicate with each other.

  Even if you do not need your Prisma Access users to connect to your HQ or data center, you might need to allow your mobile users to access your remote network locations. Service connections are required for this use case because, while all remote network connections are fully meshed, the mobile user infrastructure is not. Minimally configuring a service connections establishes the hub-and-spoke network mobile users need to access a branch network.

To improve network efficiency, place service connections close to the remote network or networks that mobile users access most frequently.

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

Before you begin to configure Prisma Access service connections, gather the following information for each of your HQ or data centers to which you want Prisma Access to be able to connect:

This checklist is only required if you are setting up a service connection to access resources in your HQ or data center. If you are creating a service connection only to allow mobile users to access remote network locations, you do not need to gather this information.

- ❑ IPSec-capable firewall, router, or SD-WAN device connection at your corporate site.
- ❑ 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.
- ❑ List of IP subnetworks at the site.
- ❑ List of internal domains that Prisma Access must be able to resolve.
- ❑ IP address of a corporate access 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.
- ❑ Network reachability settings for the service infrastructure subnet.

  Make the entire service infrastructure subnet reachable from the HQ or data center. Prisma Access uses IP addresses for all control plane traffic from this subnet.

Enable Access to Internal Resources Using Service Connections

To allow access to the resources in your HQ or data center, to give your mobile users access to remote network locations, or both, create a Prisma Access service connection.

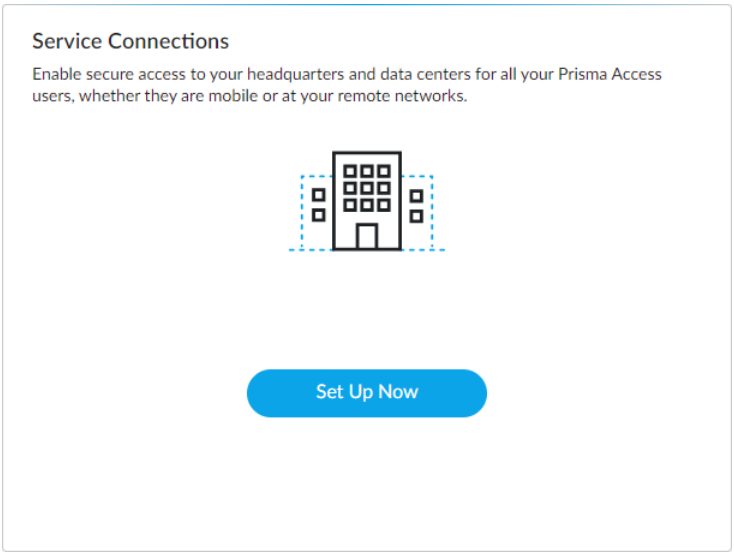
- Onboard a Service Connection
- Set Up a Primary IPSec Tunnel for Your Service Connection
- Set Up a Secondary IPSec Tunnel for Your Service Connection
- Enable Routing and Quality of Service for Your Service Connection
- Verify and Save Your Service Connection Configuration

Onboard a Service Connection

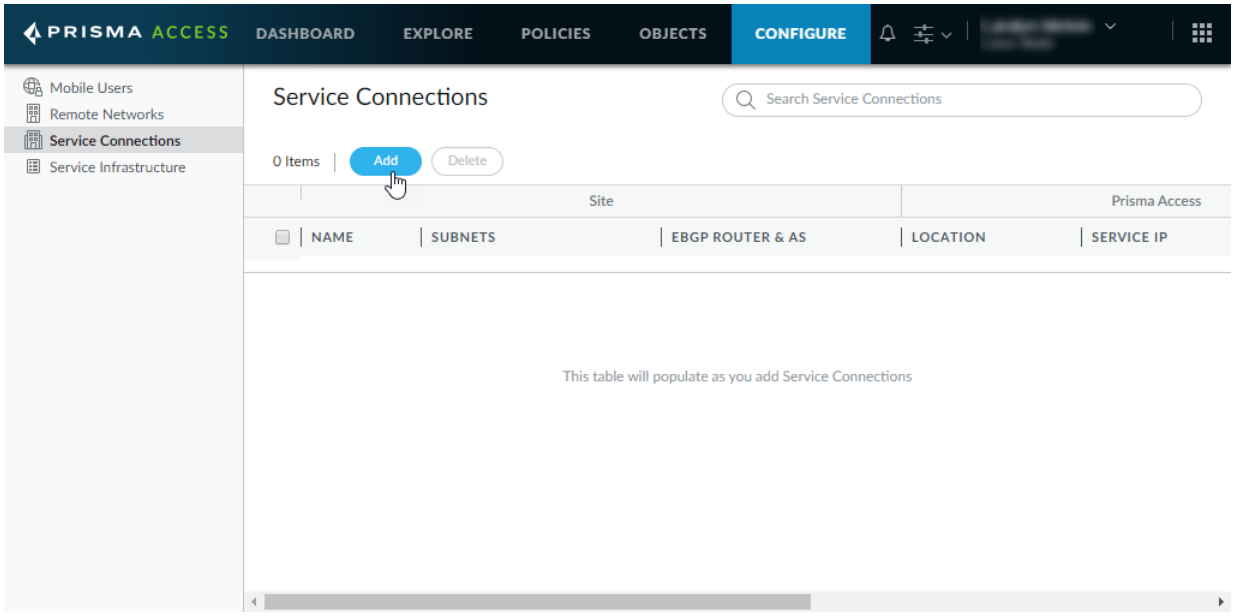
To add a new service connection to Prisma Access define the location and the type of IPSec device you are using to connect the site to Prisma Access.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | From the **Dashboard**, click **Set Up Now** in the Service Connections widget.



STEP 3 | **Add** a Service Connection.



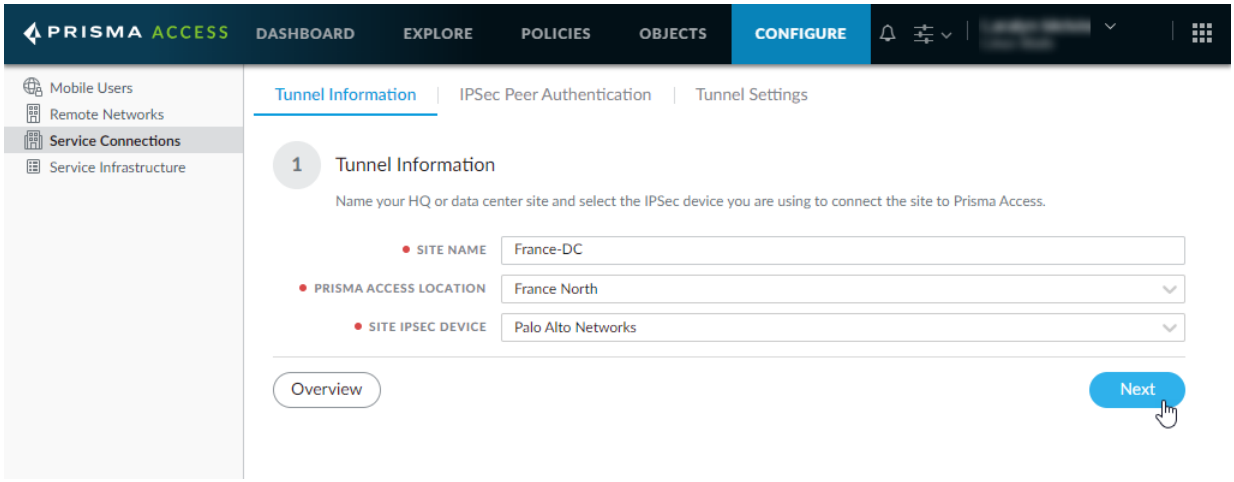
STEP 4 | **Name** the site.

STEP 5 | Select the **Location** where your HQ or data center is located.

STEP 6 | Select the **IPSec Device Type** that you are using at your site to establish an IPSec tunnel with Prisma Access.

Based on the device type you select, Prisma Access automatically populates default IKE crypto and IPSec crypto settings so that you don't have to configure them when you set up your IPSec tunnel(s).

STEP 7 | Click **Next** to Set Up a Primary IPSec Tunnel for Your Service Connection.



Set Up a Primary IPSec Tunnel for Your Service Connection

Use the following steps to set up a primary IPSec tunnel for your service connection:

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Start from the **Configure** > **Service Connections** > **IPSec Peer Authentication**.

- If you just finished the steps to Onboard a Service Connection, clicking **Next** takes you to this page automatically.
- If you've already onboarded your HQ or data center network, select **Configure** > **Service Connections** and then select your service connection and click to **Set Up** or **Edit** IPSec Peer Authentication.

STEP 3 | Select an **IKE Protocol Version** for the IPSec device at your HQ or data center site and Prisma Access to use for IKE negotiation.

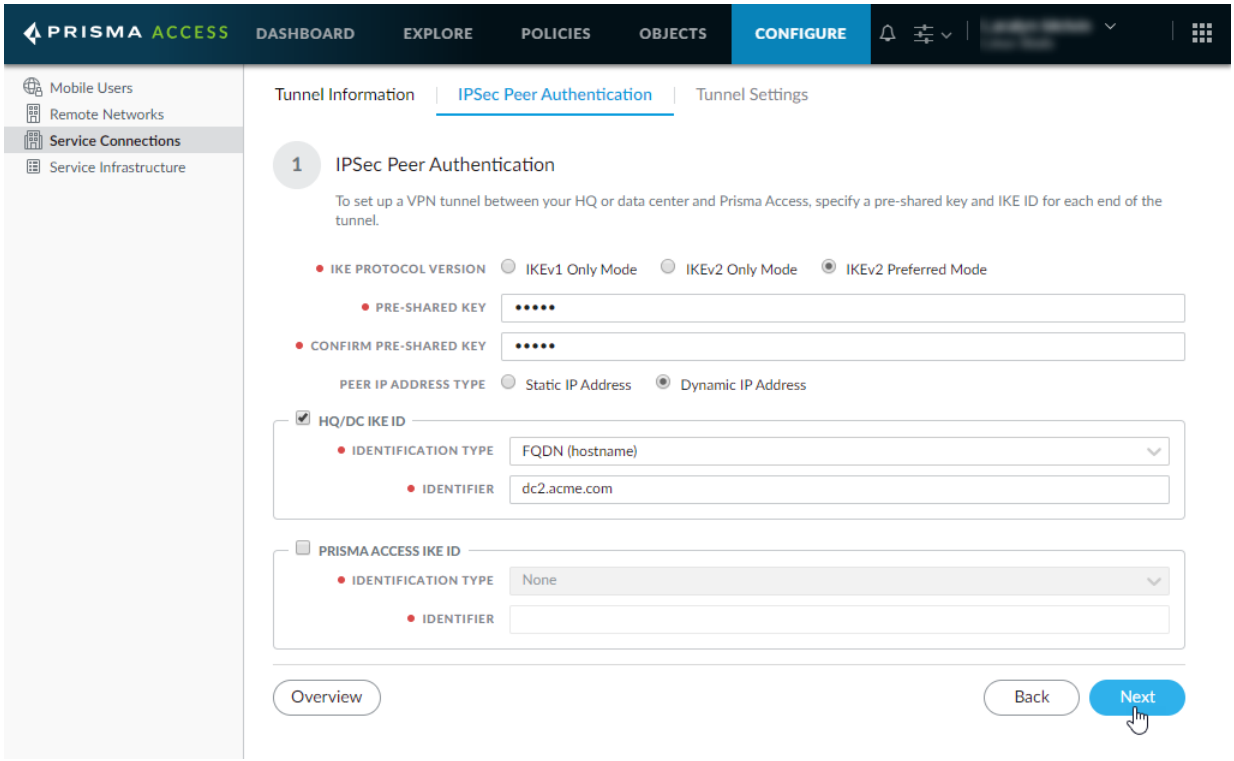
If you select **IKEv1 Only Mode**, Prisma Access can use only the IKEv1 protocol for the negotiation. If you select **IKEv2 Only Mode**, Prisma Access can use only the IKEv2 protocol for the negotiation. If you select **IKEv2 Preferred Mode**, Prisma Access uses the IKEv2 protocol only if your site device also supports IKEv2. If your does not support IKEv2, Prisma Access falls back to using the IKEv1 protocol.

STEP 4 | Enter the **Pre-Shared Key** that your on-premise device and Prisma Access to will use to authenticate each other and then **Confirm Pre-Shared Key**.

STEP 5 | For **Peer IP Address Type**, specify whether you want to use a **Static IP Address** or a **Dynamic IP Address** to identify the tunnel endpoint.

- **Static IP Address**—If you select this option, enter the **Static IP Address** on your on-premise device to use as the endpoint for the IPSec tunnel.
- **Dynamic IP Address**—If you select this option, you must enable either **HQ/DC IKE ID** or **Prisma Access IKE ID** and then supply the **Identification Type** and the corresponding **Identifier**.

Because you do not have the values to use for the Prisma Access IKE ID until the service connection is fully deployed, you would typically want to set the HQ/DC IKE ID rather than the Prisma Access IKE ID. If you want to supply a Prisma Access IKE ID for additional peer validation, after the service connection is deployed, enable Prisma Access IKE ID and then select the Identification Type you want to use to identify the Prisma Access IPSec device. You can find the Service IP for the Prisma Access peer on the Service Connections summary page (Configure > Service Connections), which you can use as the IKE ID.

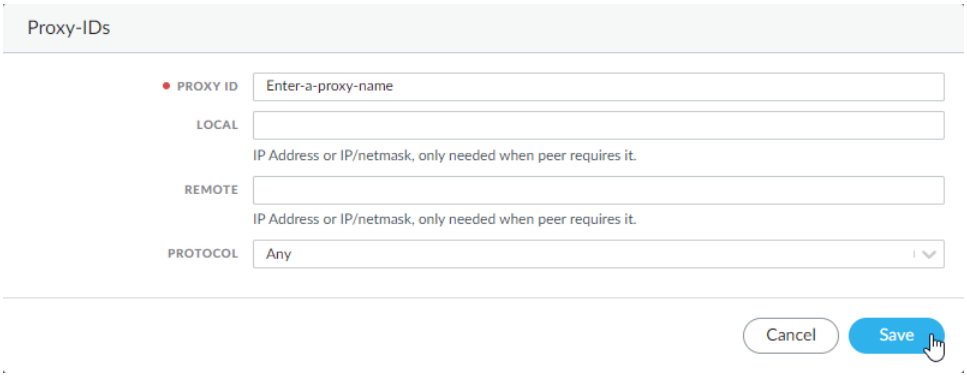


STEP 6 | Click **Next** to continue to the Tunnel Settings.

STEP 7 | If your on-premise IPSec device uses policy-based VPN, **Add** the Proxy IDs that match your policy.

You will only see the Proxy ID settings if the IPSec device type you selected supports policy-based VPN.

1. Enter a name to identify the **Proxy ID**.
2. Enter the **Local** IP address or subnet of the proxy.
3. Enter the **Remote** IP address or subnet of the proxy.
4. Specify the **Protocol**:
   - **Number**—Allows traffic for a given protocol number.
   - **Any**—Allows TCP and/or UDP traffic.
   - **TCP**—Allows only TCP traffic.
   - **UDP**—Allows only UDP traffic.



5. **Save** the Proxy ID settings.

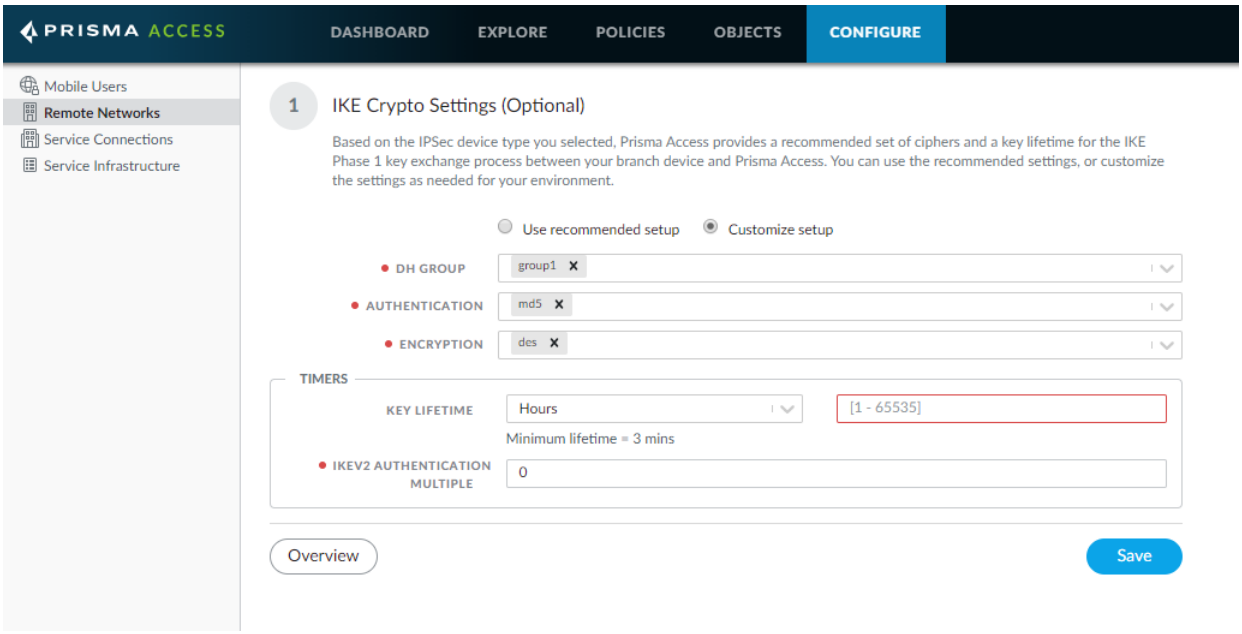
STEP 8 | Enter a Tunnel Monitoring **IP Address** on the HQ or data center network for Prisma Access to use determine whether the tunnel is up and, if your on-premise IPSec device uses policy-based VPN, enter an associated **Proxy ID**.

STEP 9 | **Save** the tunnel settings.

STEP 10 | (Optional) Customize the IKE crypto settings used to define the encryption and authentication algorithms used for the key exchange process in IKE Phase 1.

Prisma Access automatically configures a default IKE crypto profile based on the **IPSec Device Type** you selected when you Onboard a Service Connection. You can either use the default profile or create a custom profile.

1. Specify whether you want to **Use Recommended Setup**, which enables Prisma Access to automatically identify the recommended IKE crypto settings for you, or **Customize Setup**, which enables you to define your own IKE crypto settings. If you **Customize Setup**, you must configure the following IKE crypto settings:



1. Specify the Diffie-Hellman (DH) groups used to generate symmetrical keys for IKE in the IKE SA negotiation. The Diffie-Hellman algorithm uses the private key of one party and the public key of the other to create a shared secret, which is an encrypted key that both VPN tunnel peers share.

   Prisma Access supports the following DH groups: Group 1 (768 bits), Group 2 (1024 bits—default), Group 5 (1536 bits), Group 14 (2048 bits), Group 19 (256-bit elliptic curve group), and Group 20 (384-bit elliptic curve group). For the strongest security, select the group with the highest number.
2. Specify the authentication algorithm used in the IKE SA negotiation.

   Prisma Access supports the following authentication algorithms: sha1 (160 bits), sha256 (256 bits), sha384 (384 bits), sha512 (512 bits), and md5 (128 bits). You can also select null (no authentication).
3. Specify the encryption algorithm used in the IKE SA negotiation.

   Prisma Access supports the following encryption algorithms: 3des (168 bits), aes-128-cbc (128 bits), aes-192-cbc (192 bits), aes-256-cbc (256 bits), and des (56 bits). You can also select null (no encryption).
4. In the **Key Lifetime** field, specify the unit and amount of time for which the IKE Phase 1 key is valid (default is 8 hours). For IKEv1, the security association (SA) is not actively re-keyed before

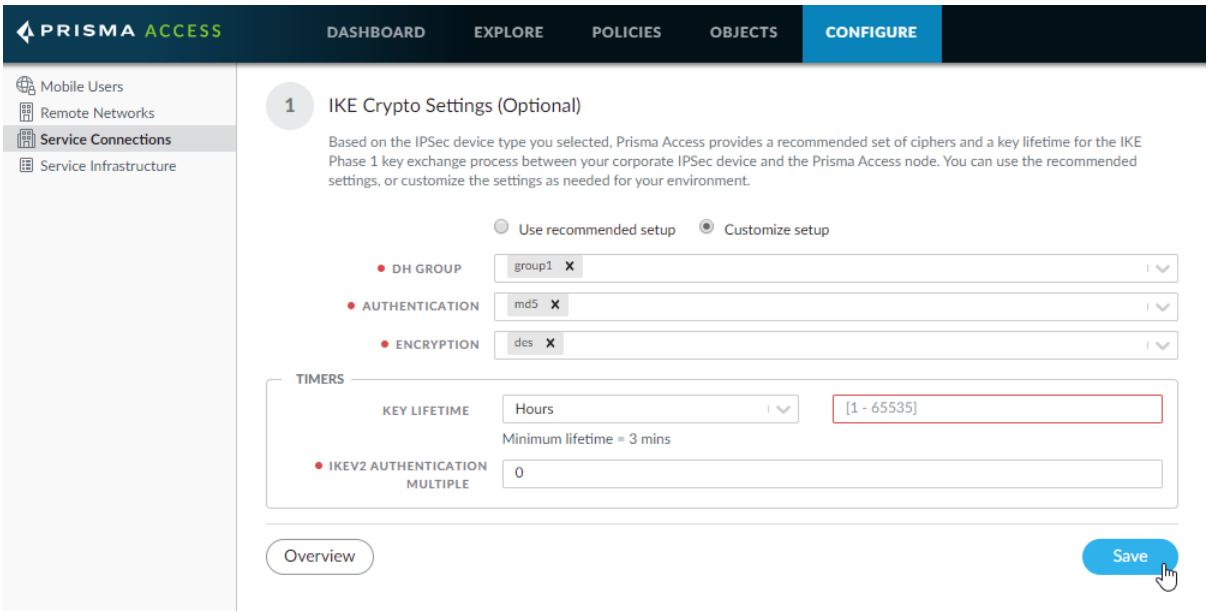
the key lifetime expires. The IKEv1 Phase 1 re-key triggers only when the SA expires. For IKEv2, the SA must be re-keyed before the key lifetime expires. If the SA is not re-keyed upon expiration, the SA must begin a new Phase 1 key.

5. Specify the **IKEv2 Authentication Multiple** value that is multiplied by the key lifetime to determine the authentication count (range is 0 to 50; default is 0). The authentication count is the number of times that the security processing node can perform IKEv2 IKE SA re-key before it must start over with IKEv2 re-authentication. The default value of 0 disables the re-authentication feature.
6. **Save** the configuration to return to the Service Connections configuration summary.

STEP 11 | (Optional) Set up an IPSec crypto profile to define how data is secured within the tunnel when Auto Key IKE automatically generates keys for the IKE SAs during IKE Phase 2.

Prisma Access automatically configures a default IPSec crypto profile based on the **IPSec Device Type** vendor you selected when you onboarded the branch. You can either use the default profile or create a custom profile.

1. Specify whether you want to **Use Recommended Setup**, which enables Prisma Access to automatically identify the recommended IPSec crypto settings for you, or **Customize Setup**, which enables you to define your own IPSec crypto settings. If you **Customize Setup**, you must configure the following IPSec crypto settings:



1. Select an **IPSec Protocol** to secure the data that traverses the VPN tunnel. The Encapsulating Security Payload (**ESP**) protocol encrypts the data, authenticates the source, and verifies the data integrity. The Authentication Header (**AH**) protocol authenticates the source and verifies the data integrity.
2. (ESP protocol only) Specify the encryption algorithm used in the IPSec SA negotiation.

   Prisma Access supports the following encryption algorithms: aes-256-gcm (256 bits), aes-256-cbc (256 bits), aes-192-cbc (192 bits), aes-128-gcm (128 bits), aes-128-cbc (128 bits), 3des (168 bits), and des (56 bits). You can also select null (no encryption).
3. Specify the authentication algorithm used in the IPSec SA negotiation.

   Prisma Access supports the following authentication algorithms: sha1 (160 bits), sha256 (256 bits), sha384 (384 bits), sha512 (512 bits), and md5 (128 bits). If you set the IPSec Protocol to ESP, you can also select none (no authentication).
4. Specify the Diffie-Hellman (DH) groups for IKE in the IPSec security association (SA) negotiation.

Prisma Access supports the following DH groups: Group 1 (768 bits), Group 2 (1024 bits—default), Group 5 (1536 bits), Group 14 (2048 bits), Group 19 (256-bit elliptic curve group), and Group 20 (384-bit elliptic curve group). For the strongest security, select the group with the highest number. If you don't want to renew the key that Prisma Access creates during IKE phase 1, select **no-pfs** (no perfect forward secrecy). If you select this option, Prisma Access reuses the current key for the IPSec SA negotiation.

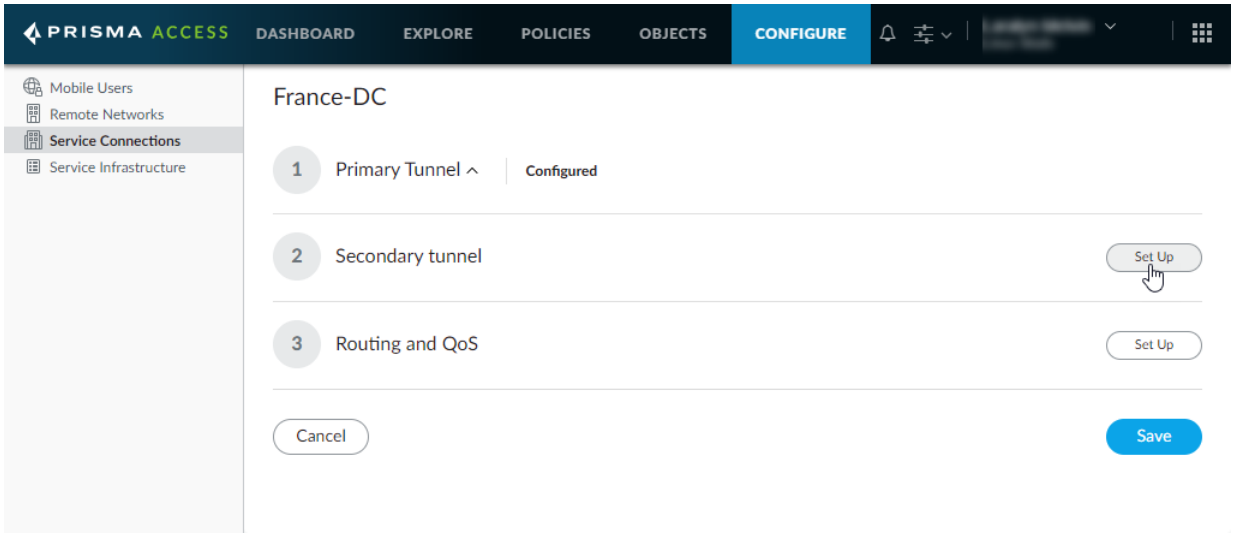
5. In the **Lifetime** field, specify the unit and amount of time during which the negotiated key is valid (default is one hour).
6. In the **Lifesize** field, specify the unit and amount of data that the key can use for encryption.
7. **Save** the configuration to return to the Service Connections configuration summary.

Set Up a Secondary IPSec Tunnel for Your Service Connection

If the primary IPSec tunnel for your service connection goes down, the service connection falls back to the secondary IPSec tunnel until the primary IPSec tunnel comes back up. If both the primary and secondary IPSec tunnels are up, the primary IPSec tunnel takes priority over the secondary IPSec tunnel.

Use the following steps to set up a secondary IPSec tunnel for your service connection:

STEP 1 | From your Service Connections configuration summary (**Configure** > **Service Connections** > <*service-connection-config*>) and **Set Up** or **Edit** the **Secondary tunnel** configuration.



STEP 2 | Repeat the steps for configuring the primary IPSec tunnel to configure your secondary IPSec tunnel.

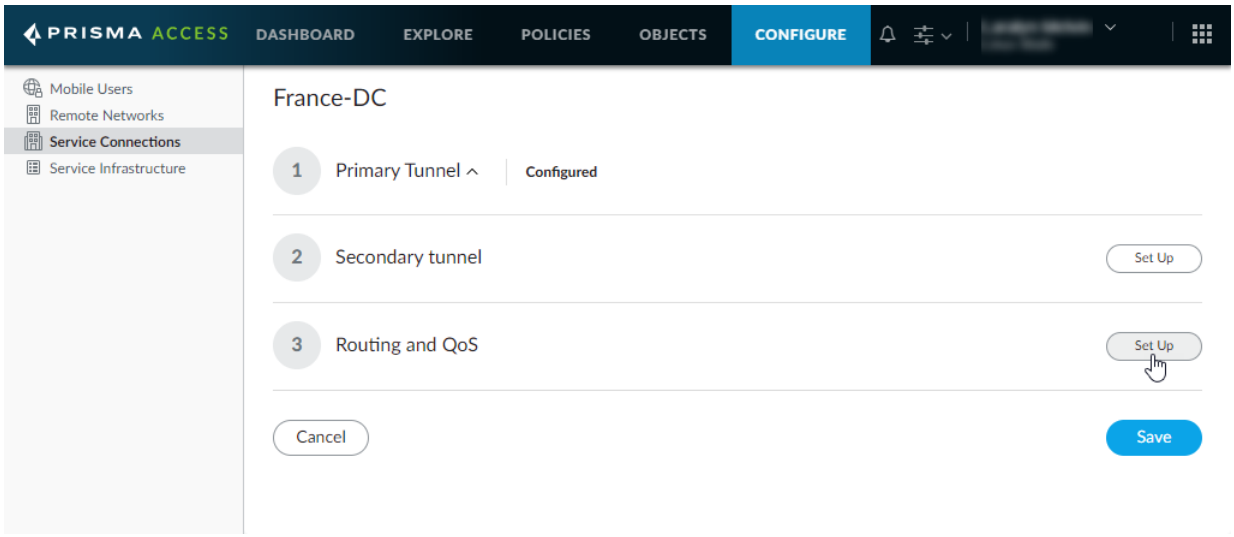
STEP 3 | When you finish configuring the secondary IPSec tunnel, click **Save**.

Enable Routing and Quality of Service for Your Service Connection

Enable routing to the subnetworks or individual IP addresses on your HQ or data center network that your Prisma Access 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.

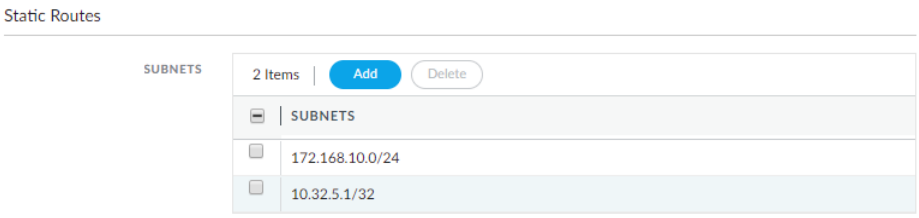
Optionally, you can create QoS profiles to shape QoS traffic for the service connection and apply the profile to traffic that you marked with security policy rules, traffic that you marked with an on-premise device, or both security-policy and on-premise-marked traffic

STEP 1 | From your Service Connections configuration summary (**Configure** > **Service Connections** > *<service-connection-config>*), **Set Up** Routing and QoS.



STEP 2 | Configure static routes.

Add the **IP Subnets** or IP addresses that your Prisma Access users need access to on your HQ or data center network.



STEP 3 | Configure dynamic routing.

To use dynamic routing to advertise your HQ or data center, **Enable BGP** and then configure the following settings:

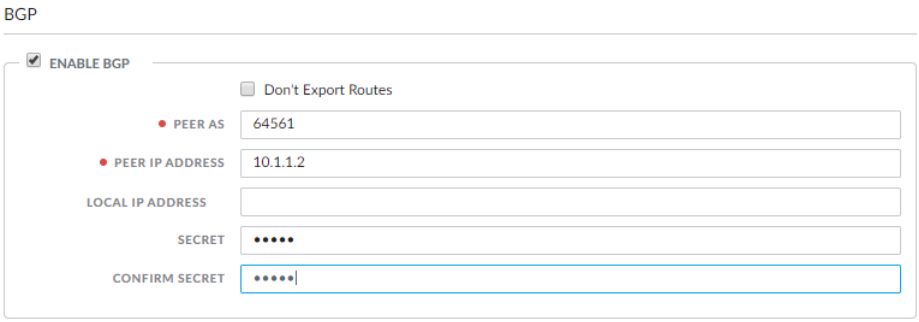
1. To prevent Prisma Access from forwarding routes into your HQ or data center, select **Don't export routes**.

   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.
2. Enter the **Peer AS**, which is the autonomous system (AS) for your network.

   You must use an RFC 6696-compliant BGP Private AS number.
3. Enter the **Peer IP Address** assigned as the Router ID of the eBGP router on your HQ or data center network.
4. Enter the IP address that Prisma Access uses as its **Local IP Address** for BGP.

A local address is only required if your on-premise device requires it for BGP peering to be successful. Make sure the address you specify does not conflict or overlap with IP addresses in the infrastructure subnet or subnets in the remote network.

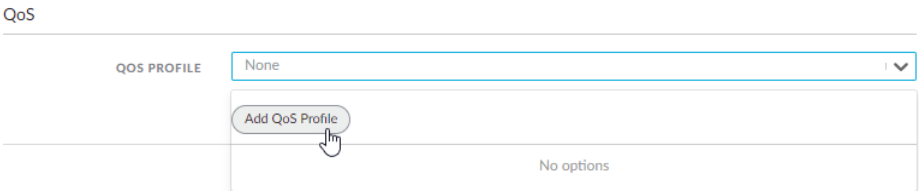
5. Enter a **Secret** password to authenticate BGP peer communications and then **Confirm Secret**.



STEP 4 | (Optional) Configure a QoS profile that defines QoS classes needed to shape traffic for this HQ or data center network.

You will also need to create a QoS policy rule and assign the QoS profile to in order to enforce QoS on matching traffic to or from your data center.

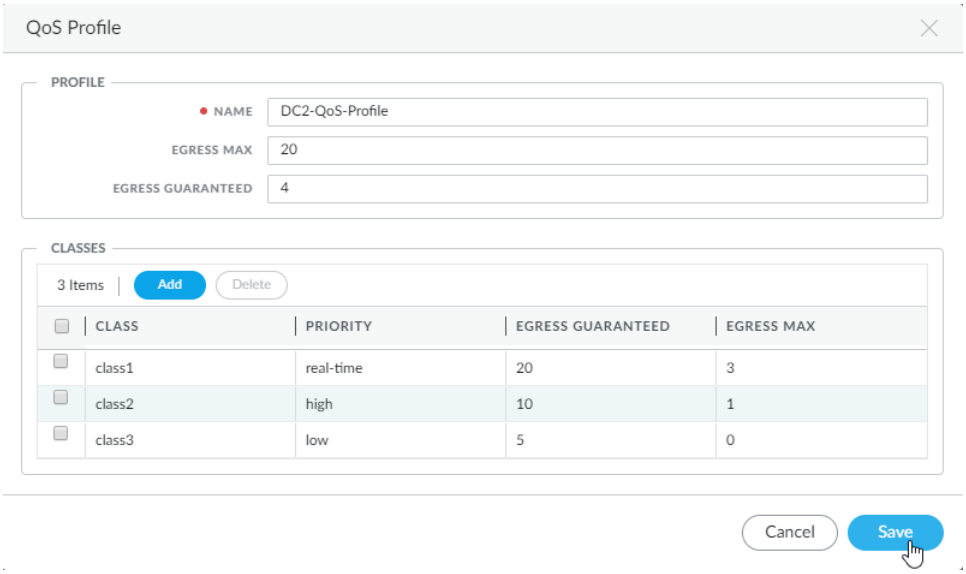
1. From the **QoS Profile** drop down, select **Add QoS Profile**.



2. Enter a **Name** to identify the QoS profile.
3. Set the bandwidth limits for the QoS profile:
   - Set the maximum throughput (in Mbps) for traffic leaving the service connection as the **Egress Max**. For service connections, specify a number of up to 1 Gpbs (1,000 Mbps).
   - Set the guaranteed bandwidth as the **Egress Guaranteed** (in Mbps). Any traffic that exceeds the **Egress Guaranteed** value is best effort but not guaranteed. Any bandwidth that is guaranteed but unused remains available to all traffic.
4. **Add** the QoS **Classes** that you want to assign to this profile.

   A QoS class determines the priority and bandwidth for traffic matching a QoS policy rule. You can use a QoS profile rule to define QoS classes. There are up to eight definable QoS classes in a single QoS profile. Unless otherwise configured, traffic that does not match a QoS class is assigned a class of 4.
5. Select a QoS **Class** and set the **Priority** for the QoS class (**low priority**, **medium priority**, **high priority**, or **real-time**).
6. Set the **Egress Max** and **Egress Guaranteed** values for the QoS class.

   The **Egress Max** value for the QoS class must not exceed the **Egress Max** value for the QoS profile. In addition, the guaranteed bandwidth assigned to the QoS class is not reserved for that class; unused bandwidth remains available to all traffic. Any class traffic that exceeds the **Egress Guaranteed** value is best effort but not guaranteed.
7. Repeat these steps to **Add** additional classes.



8. **Save** the QoS profile.

STEP 5 | **Save** the routing and QoS configuration.

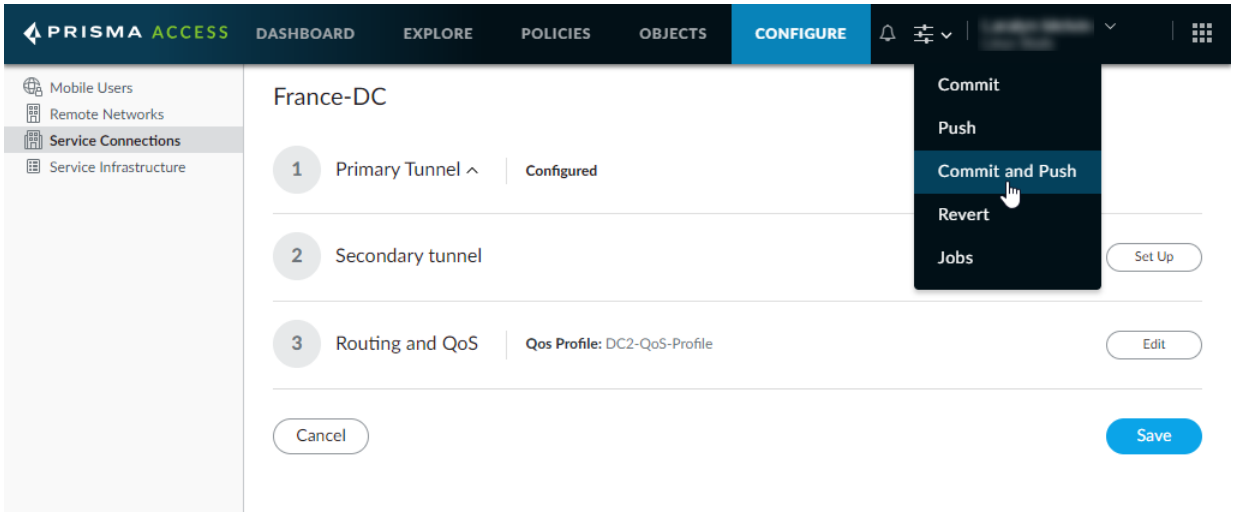
Verify and Save Your Service Connection Configuration

Use the following steps to verify and save your service connection configuration:

STEP 1 | From your Service Connections configuration summary (**Configure** > **Service Connections** > <*service-connection-config*>), verify that your service connection configuration is correct.

STEP 2 | **Save** the service connection configuration.

STEP 3 | Commit and push the configuration to your mobile users or remote networks.



Manage Your Service Connection Configuration

If you need to make any changes to an existing service connection configuration, use the following steps to modify the configuration:

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Select **Configure** > **Service Connections** > *<service-connection-config>* to view your Service Connections configuration summary.

STEP 3 | To modify an existing setting in your service connection configuration, **Edit** the setting.

STEP 4 | After you complete and verify your changes, **Save** the service connection configuration.

STEP 5 | Commit and push the configuration to your mobile users or remote networks.

Monitor the Service Connection Status

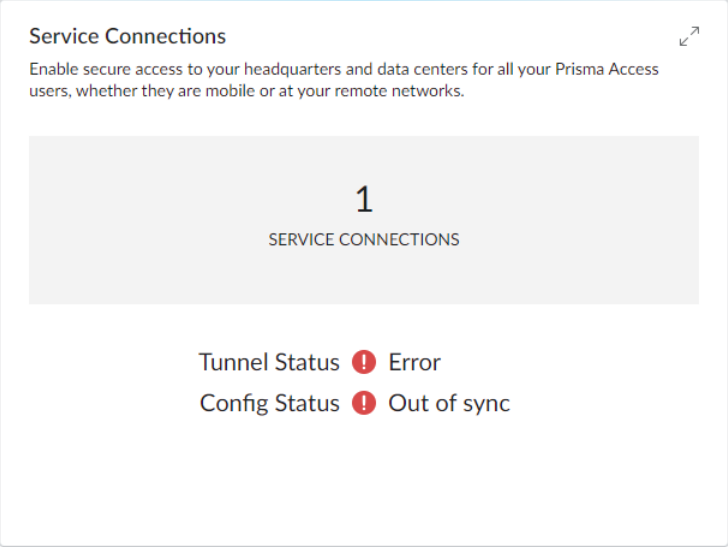
The Prisma Access **Dashboard** provides information on the status of your mobile user environment, remote network environment, and service connections. For service connections, you can view the following information:

- **Status**—Indicates whether your service connections are up and running.
- **Config Status**—Indicates the status of your service connection configuration.
- **Service Connections**—Indicates the number of available service connections.

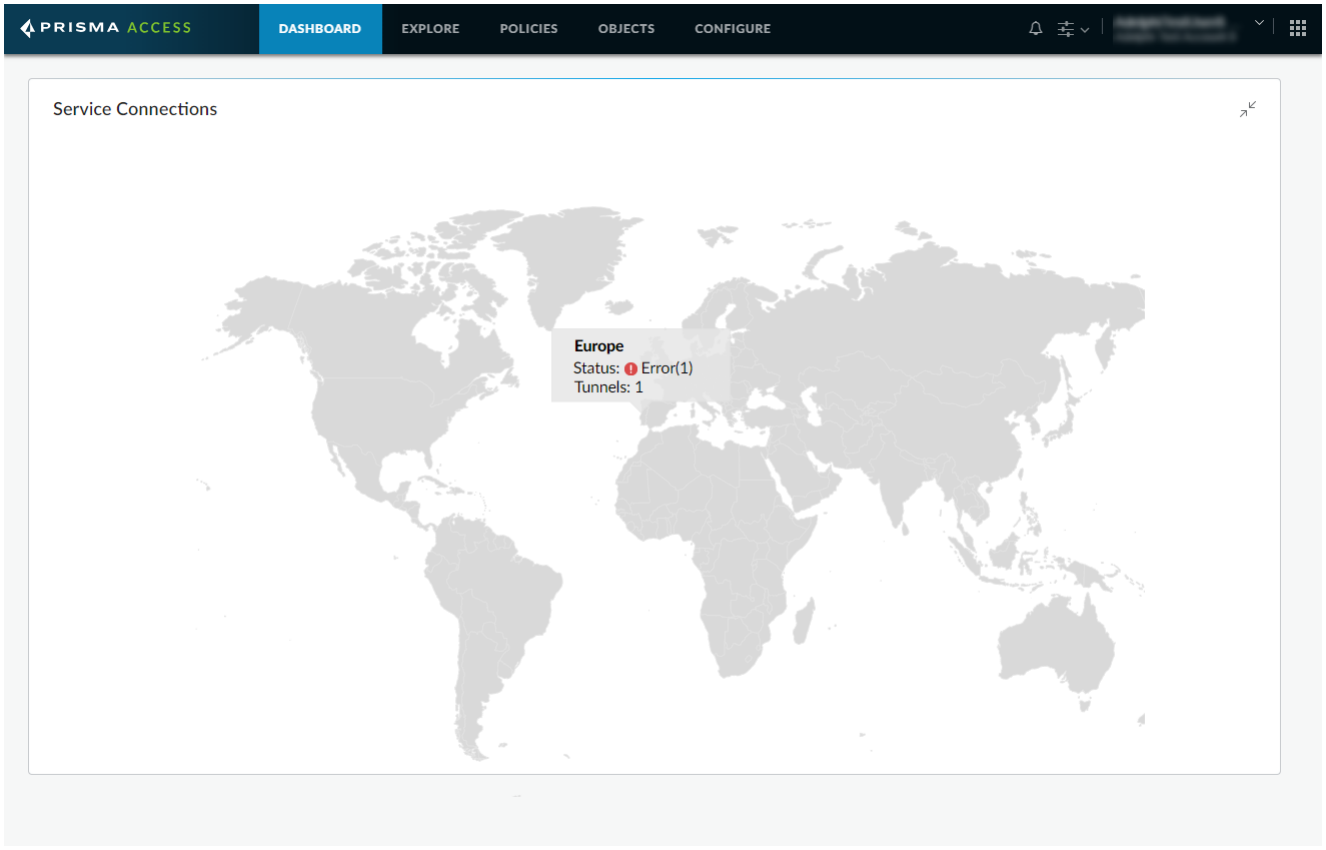
Use the following steps to monitor the status of your service connections:

STEP 1 | Launch Prisma Access Cloud Management.

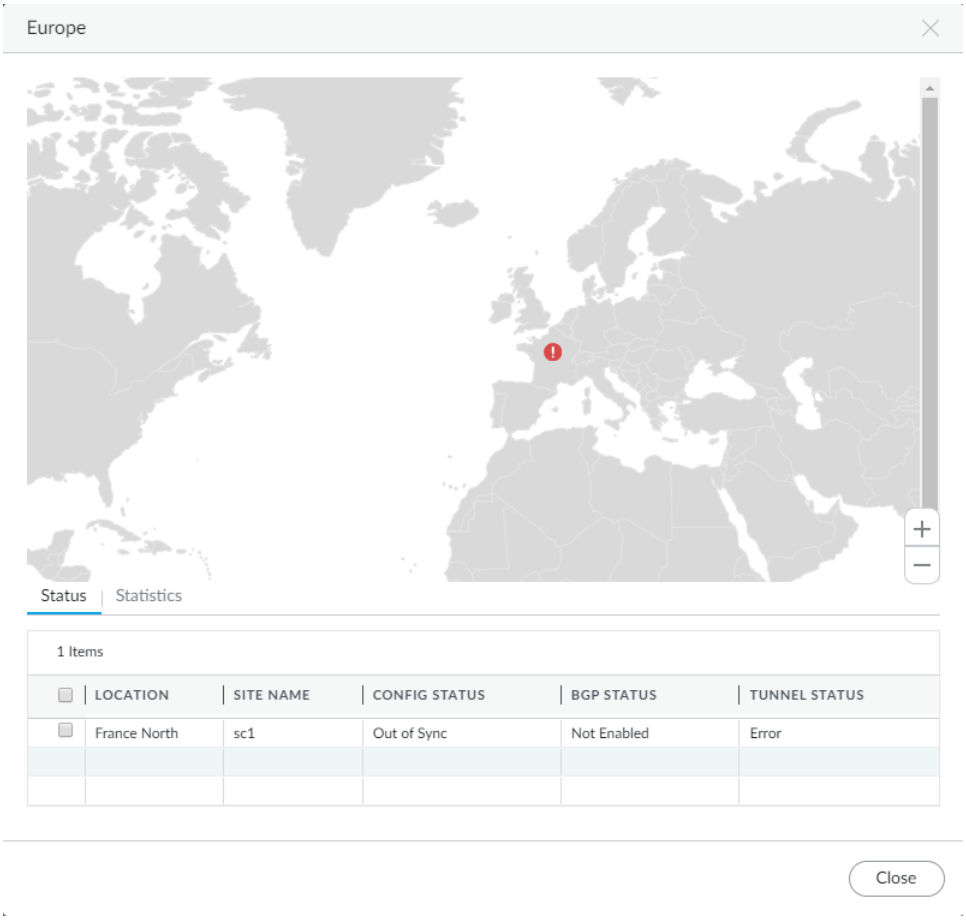
STEP 2 | Select **Dashboard** to view information on the status of your service connections, such as the configuration status and number of available service connections.



STEP 3 | Expand the **Dashboard** widget to see a map showing the locations you have onboarded.



STEP 4 | Drill down into a location for more details.



Create Prisma Access Policy

Create objects in Prisma Access to build your policy rules to block or allow traffic to or from your corporate network or unknown devices on the internet. Enforce policy rules for users in your remote networks, mobile users on managed devices (GlobalProtect) and unmanaged devices (Clientless VPN).

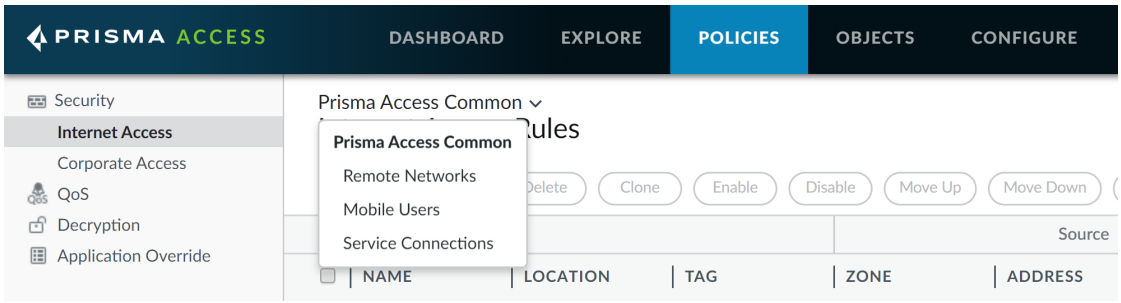
- Organize your Prisma Access Configurations
- Prisma Access Policy
- Prisma Access Policy Types
- Prisma Access Zones
- Prisma Access Objects
- Create a Policy Rule

Organize your Prisma Access Configurations

Use the default configuration groups in Prisma Access to organize the common Prisma Access configurations, and those which are specific to your remote networks, mobile users, and service connections. This enables you to organize your configurations based on common policy requirements without redundant configurations. When configuring a Prisma Access policy or object, use the drop-down as pictured below to select the appropriate configuration group for the policy or object you are configuring.

By default, Prisma Access includes four configuration groups, and additional groups cannot be created:

- **Prisma Access Common**—Parent configuration group. In this group, configure policies and objects that are shared across your remote networks, mobile users, and service connections. The configurations that are part of this group take precedence over those in the Remote Networks, Mobile Users and Service Connection groups.
- **Remote Networks**—Child configuration group. In this group, configure policies and objects that are specific to your on-boarded remote networks. Policies and objects configured in the Mobile Users or Service Connections groups have no impact on your remote network configuration.
- **Mobile Users**—Child configuration group. In this group, configure policies and objects that are specific to your on-boarded mobile users. Policies and objects configured in the Remote Networks or Service Connections groups have no impact on your mobile users configuration.
- **Service Connections**—Child configuration group. In this group, configure policies and objects that are specific to your on-boarded service connections. Policies and objects configured in the Remote Networks or Mobile Users groups have no impact on your service connection configuration.



Prisma Access Policy Types

The different policy types supported on Prisma Access are: Security (Corporate Access and Internet Access), QoS, Decryption, Application Override, and Authentication.

Policy Type	Description
Security	Determine whether to block or allow sessions based on the traffic attributes such as the source and destination zones, the source and destination IP addresses, the application, or user. See Create a Security Policy Rule.
QoS	Identify traffic requiring quality of service treatment, such as preferential treatment using a defined parameter or multiple parameters and assign it a class. See Create a QoS Policy Rule.
Decryption	Identify encrypted traffic that you want to inspect for visibility, control, and granular security. See Create a Decryption Policy Rule.
Application Override	Identify sessions that you do not want processed by the App-ID engine which is a Layer-7 inspection. Traffic matching an application override policy forces Prisma Access to handle the session as a regular stateful inspection at Layer-4. See Create an Application Override Policy Rule.

Prisma Access Policy

Policies enable you to enforce rules and take action when traffic matches a Prisma Access policy rule or when Prisma Access identifies suspicious activity on your network. By default, basic internet access policy rules are created when you onboard new mobile users. This allows you to quickly set up Prisma Access and deploy Palo Alto Networks recommended protection to your end points. More granular policy rules need to be created or to enable access to your corporate network over service connections for example, to address your specific business needs.

Prisma Access Zones

Traffic must pass through Prisma Access in order to manage and control it using policy rules and zones. When creating a policy rule, you must designate specific zones that the rule applies to. For example, because traffic can only flow between zones, you need a security policy to allow the traffic from the source zone to the destination zone. Prisma Access simplifies creating policy rules by automatically setting up your network infrastructure for you. This means that you no longer need to configure the zones you use create policy rules. Instead, Prisma Access automatically configures three zones that you use to build your network security.

Prisma Access supports three zones:

Zone	Description
Trust	Zone containing all trusted and on-boarded IP addresses, service connections, or mobile users within the corporate network.
Untrust	All untrusted IP addresses, service connections, or mobile users outside of the corporate network. By default, any IP address or mobile user that is not trusted is inherently untrusted.
Clientless VPN	Secure remote access to common enterprise web applications that use HTML, HTML5, and Javascript technologies. Users have the advantage of secure access from SSL-enabled web browsers without installing client software. This is useful when you need to enable partner or contractor access to applications, and to safely enable unmanaged assets, including personal devices..

Prisma Access Objects

Prisma Access objects are a single unit, or collective unit that groups IP addresses, applications, services, HIP objects, or security profiles. You reference objects when creating a policy rule, and in the case of policy objects that are a collective unit, you can reference that single object rather than manually selecting multiple individual objects to simplifying the policy definition.

When you create a policy object, it is a best practice to group objects that require similar permissions in the policy. For example, if your organization uses a set of destination IP addresses to that require the same policy enforcement, you can group them as `address` objects in an `address group` and reference that address group in your policy. You can create the following policy objects in Prisma Access:

Object	Description
Addresses, Address Groups, Regions	Allows you to group specific source or destination addresses that require the same policy enforcement. Address objects can include IPv4 and IPv6 address (single IP, range, subnet), or FQDN. Alternatively, you may define a region by the latitude and longitude coordinates or you can select a country and define an IP address or range. You can then group a collection of address objects to create an address group object. See Create Address Objects.
Applications, Application Groups, Application Filters	Allows you to define applications and their risk that are in use by your organization. Additionally, you can group a collection of applications to create an Application Group that require the same policy enforcement and simplifies administration of your rulebase by allowing you to update only the affected application group, rather than multiple policy rules, when there is a change of applications you support. Create an Application Filter to dynamically group applications based on application attributes that you define. This is useful when you want to safely enable access to applications that you do not explicitly sanction, but want users to be able to access. See Create Application Objects.
Services, Service Groups	Allows you to specify the source and destination ports and protocols that a service can use. You also create an custom service on any TCP/UDP port of your choice to restrict application usage to specific ports on your network. After you have created your service objects, you can then group a collection of services to create a Service Group that require the same policy enforcement. See Create Service Objects.
Tags	Create tags to visually group objects using keywords or phrases. You can apply tags to address objects, address groups, services, service groups, and policy rules. See Use Tags to Group and Visually Distinguish Policies and Objects.
HIP Objects, HIP Profiles	Allows you to define objects for the host information profile (HIP) to provide matching criteria for filtering the raw data which gives information about how the device is maintained. This information includes whether data is encrypted, if antivirus signatures are up to date, if the device is jailbroken and more. You can use the device state information to enforce policy. After you have created your HIP objects, you can then group a collection of HIP objects to create a HIP Profile to be evaluated together for monitoring or for policy enforcement. See Create HIP Objects.

Object	Description
External Dynamic Lists	Allows you to define an imported list of IP addresses, URLs, or domain names that you can use in policy rules to block or allow traffic. See External Dynamic List in Prisma Access.
URL Category	Allows you to create a custom URL category object to use in a URL Filtering profile to specify exceptions to URL category enforcement, and to create a custom URL category based on multiple URL categories. See Create a URL Category Object.
Security Profiles	Allows you to create security profiles that instruct Prisma Access to scan applications for threats when attached to a policy rule. When traffic matches the rule defined the policy, the security profile(s) that are attached to the rule are applied for further content inspection. You can create the following security profiles: • Vulnerability Protection • URL Filtering • File Blocking • WildFire Analysis The following security profiles have pre-populated default and best practice profiles. Additional profiles cannot be created: • Antivirus • Anti-Spyware • Decryption See Create a Security Profile.
Security Profile Group	A security profile group is a set of security profiles that are treated as a single unit and then easily added to security policy rules. Add individual security profiles that are often assigned together to profile groups to simplify the creation of security policies. See Create a Security Profile Group.

Create Address Objects

Create one or more address objects, address groups, or region to group specific source or destination addresses that require the same policy enforcement.

- Create an Address Object
- Create an Address Group
- Create a Region Object

Create an Address Object

Create an address object to reuse that same address as a source or destination address in policy rules, filters, or other Prisma Access functions without needing to add the address manually each time.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Select **Objects** > **Addresses** and **Add** a new address object.

STEP 3 | Enter the address **Name**.

STEP 4 | (Optional) Enter a **Description** of the address object.

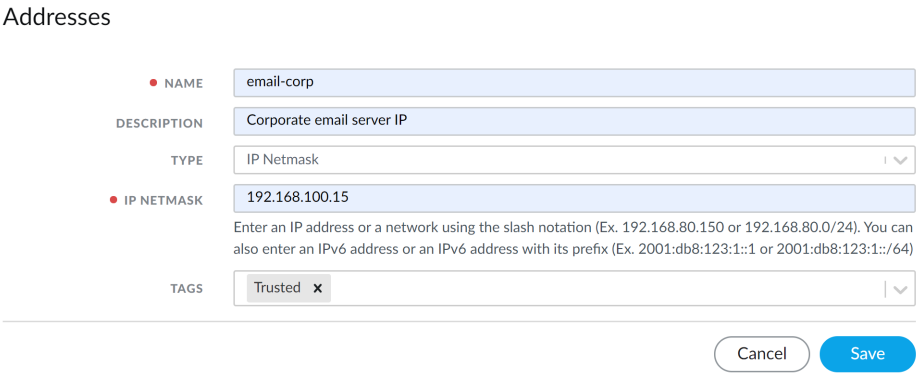
STEP 5 | Select the address object type. You can select IP Netmask, IP Range, or FQDN. For this example, **IP Netmask** is selected.

STEP 6 | Enter the address object type value.

- If you selected **IP Netmask**, enter a static IP address.
- If you selected **IP Range**, enter a an IP range. For example:
  - IPv4 — 10.0.0.1-10.0.0.4
  - IPv6 — 2001:db8:123:1::1-2001:db8:123:1::11

STEP 7 | (Optional) Select one or more **Tags** to apply to the address object.

STEP 8 | **Save** your configuration.



STEP 9 | Select **Commit** and **Commit and Push** your configuration changes.

Create an Address Group

After you create multiple address objects for reuse, create an address group to group these address objects together in order to apply the same policy enforcement to all addresses in the group.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Create the required address objects.

STEP 3 | Select **Objects** > **Address Group** and **Add** a new address group.

STEP 4 | Enter the address group **Name**.

STEP 5 | (Optional) Enter a **Description** of the address group.

STEP 6 | Select the address group **Type**. You can select Static or Dynamic. In this example, **Static** is selected.

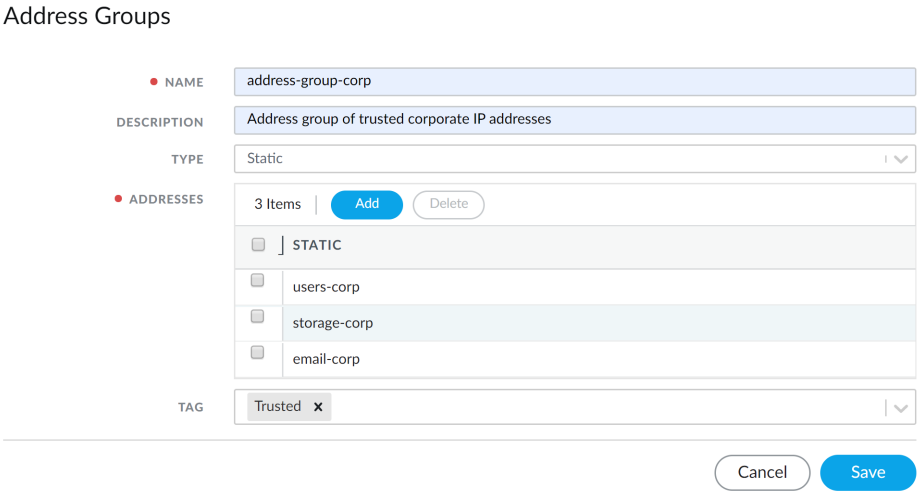
STEP 7 | Add addresses to the address group.

You may only have the same address object type to the selected address group type in the previous step. For example, if you selected Static, you may only add static address objects to the address group.

- If you selected **Static**, **Add** the address objects you want to apply the same policy enforcement to.
- If you selected **Dynamic**, enter a **Filter** using AND and OR operators to create match criteria to dynamically assemble the address group.

STEP 8 | (Optional) Select one or more **Tags** to apply to the address group.

STEP 9 | **Save** your configuration.



STEP 10 | Select **Commit** and **Commit and Push** your configuration changes.

Create a Region Object

Prisma Access supports the creation of policy rules that apply to specified countries or other regions. Create a region object to specify source and destination for policy rules.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Select **Objects** > **Region** and **Add** a new region.

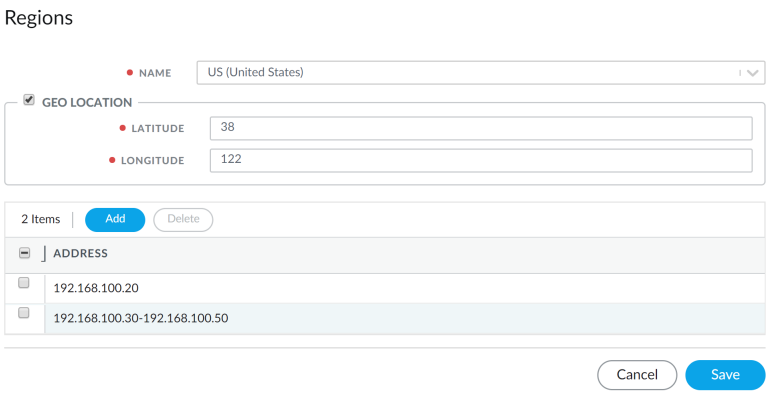
STEP 3 | Select the region **Name** from the drop-down.

STEP 4 | Enable **Geolocation** and specify the region coordinates.

1. Specify the region latitude between -90.0 and 90.0 degrees.
2. Specify the region longitude between -180.0 and 180.0 degrees.

STEP 5 | **Add** one or more IP addresses or address ranges to include in the region object.

STEP 6 | **Save** your configuration.



STEP 7 | Select **Commit** and **Commit and Push** your configuration changes.

Create Application Objects

Create application objects to define the applications you use and their risk. You can group multiple applications that require the same policy enforcement by creating an Application Group to simplify rulebase administration.

- Create an Application Object
- Create an Application Group
- Create an Application Filter

Create an Application Object

Define an application object to attribute to a policy rule. By attributing an application object to a policy rule, you define the security enforcement and access to the sanctioned application.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Select **Objects** > **Application** and **Add** a new application object.

STEP 3 | Define the application **Configuration**.

1. Enter a descriptive **Name** for the application.
2. (Optional) Enter a **Description** for the application.
3. Select the application Properties from the Category, Subcategory Technology, Parent App, and Risk drop-downs.
4. Select the application Characteristics.

STEP 4 | Define the details about the application, such as the underlying protocol, the port number the application runs on, the timeout values, and the types of scanning you want to be able to perform on traffic. **Advanced** application settings.

1. Click Advanced
2. Select the Default protocol method used by the application, and enter the Port, IP Protocol, or Type and Code values depending on the protocol method selected.
3. Configure the Timeouts values, in seconds, for the application.
4. Enable additional scanning on the application based on the security profile attributed to the policy rule the application object is attributed to.
   - Enable (check) **File Types** to allow file type scanning on the application.
   - Enable (check) **Viruses** to allow virus scanning on the application.

- Enable (check) **Data Patterns** to data patterns scanning on the application.

STEP 5 | Define the criteria that Prisma Access uses to match the traffic to the application.

1. Click **Signatures** and **Add** a threat signature or custom signature to the application.
2. Enter a **Signature Name** to identify the signature.
3. (Optional) Enter a **Comment** to describe the signature.
4. Select the **Scope** of the signature.
   - Select **Session** if the signature matches to a full session.
   - Select **Transaction** if the signature applies to a single transaction.
5. Enable **Ordered Condition Match** if the order in which Prisma Access attempts to match the signature definitions is imported. When you have multiple signatures added to an application object, click **Move Up** or **Move Down** to order the signatures as needed when enabled. If matching order is not important, disable (clear) the setting.
6. Specify conditions to define signatures. **Add** the **And Condition** or **Or Conditions** as needed.

STEP 6 | **Save** your configuration.

STEP 7 | Select **Commit** and **Commit and Push** your configuration changes.

Create an Application Group

An application group allows you to group multiple applications that you want to be treated similarly in policy. Application groups allow you to enable access to applications you explicitly sanction and simply administration of your rulebase by allowing you to update the application group with new applications, rather than updating each individual manually when new applications are introduced in your organization.

When deciding how to group applications, consider how you plan to enforce access and create the application group with your policy goals in mind. For example, if there are applications that only IT administrators can access, and there are applications that any known user can access, create application groups that align with each of these policy goals.

STEP 1 | Launch Prisma Access Cloud Management.

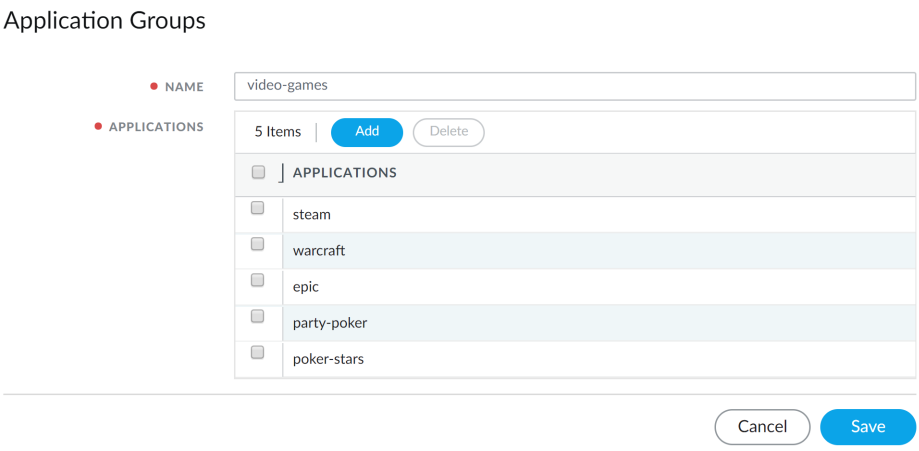
STEP 2 | Create the required application objects.

STEP 3 | Select **Objects** > **Application Groups** and **Add** a new application group.

STEP 4 | Enter the address group **Name**.

STEP 5 | **Add** applications to the application group. In this example, we are adding common video game applications to the application group.

STEP 6 | **Save** your configuration.



STEP 7 | Select **Commit** and **Commit and Push** your configuration changes.

Create an Application Filter

An application filter is an object that dynamically groups applications based on attributes you define. This includes the category, subcategory, technology, risk factor, and characteristics of the applications you want grouped together. As new applications emerge, and new App-IDs are introduced, these new applications are automatically matched and grouped based on the filters you defined. Application filters ease the burden of rulebase management by automatically updating application groups attributed to policy rules so that you do not need to manually edit your policy rules to include the new applications.

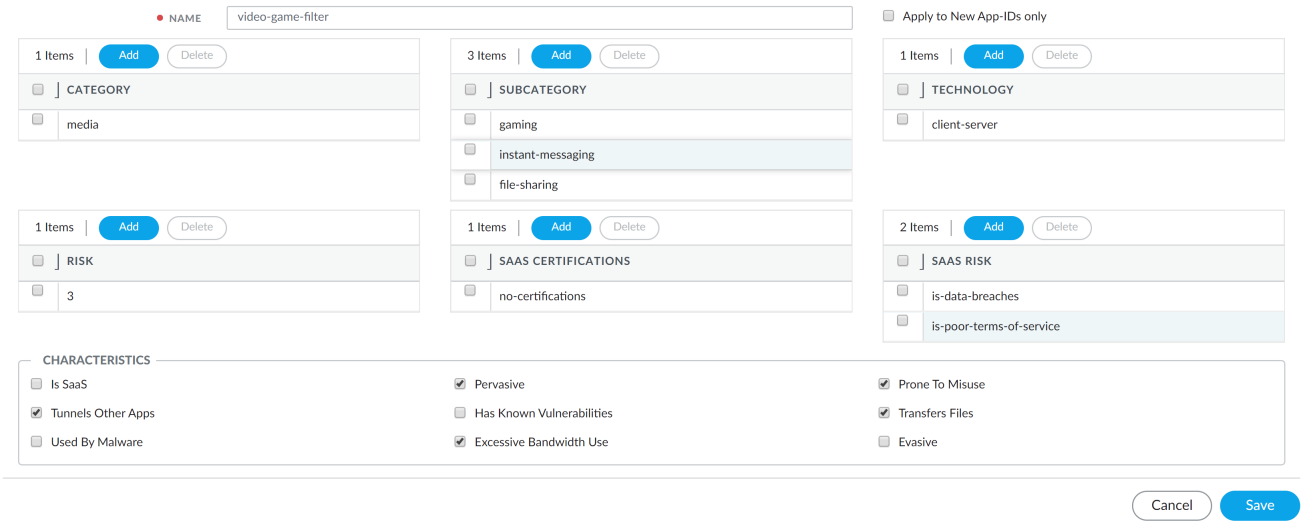
STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Select **Objects** > **Application Filters** and **Add** a new application filter.

STEP 3 | Enter a descriptive **Name** for the application filter.

STEP 4 | **Add** attribute values from the Category, Subcategory, Technology, Risk, SaaS Certifications, SaaS Risk, and Characteristics sections to define the filter.

STEP 5 | **Save** your configuration.



STEP 6 | Select **Commit** and **Commit and Push** your configuration changes.

Create Service Objects

Create a service objects, or group multiple service objects to create a service group, select one or more services to limit the port numbers the applications can use.

- Create a Service Object
- Create a Service Group

Create a Service Object

Service objects allow you to limit the port numbers an application can use when applied to policies you define for specific applications. The default service object for any policy rule is `application-default` where the selected applications in the policy rule are allowed or denied only on their default ports defined by Palo Alto Networks®. This option is beneficial because it prevents applications from running on unusual ports and protocols which, if unintentional, can be a sign of undesired application behavior and usage. However, you can create a service object to limit application functionality to specific ports of your choosing that better align with the specific needs of your organization.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Select **Objects** > **Services** and **Add** a new service object.

STEP 3 | Enter a descriptive **Name** for the service.

STEP 4 | (Optional) Enter a **Description** for the service.

STEP 5 | Select the **Protocol** used by the service.

STEP 6 | Enter the **Destination Port** for application traffic. The port can be a single port number, range (1-65535), or comma separated (80, 8080, 443).

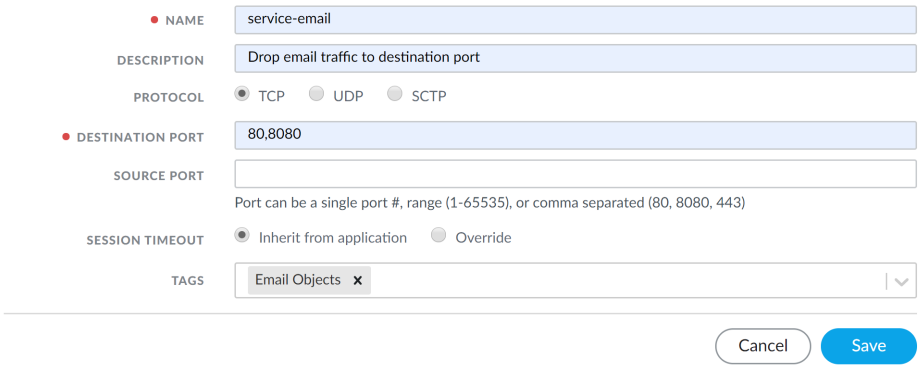
STEP 7 | Enter the **Source Port** for application traffic. The port can be a single port number, range (1-65535), or comma separated (80, 8080, 443).

STEP 8 | Specify the **Session Timeout** for the service. By default, **Inherit from Application** is selected, meaning that no service-base timeouts are applied and the configured application timeouts are applied instead. Select **Override** to set a service-based UDP timeout.

STEP 9 | (Optional) Select one or more **Tags** to apply to the service object.

STEP 10 | **Save** your configuration.

Services



STEP 11 | Select **Commit** and **Commit and Push** your configuration changes.

Create a Service Group

Create a service group to group multiple service objects that have the same security settings and requirements in order to simplify the creation of your policy rules.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Create the required service objects.

STEP 3 | Select **Objects** > **Service Groups** and **Add** a new service group.

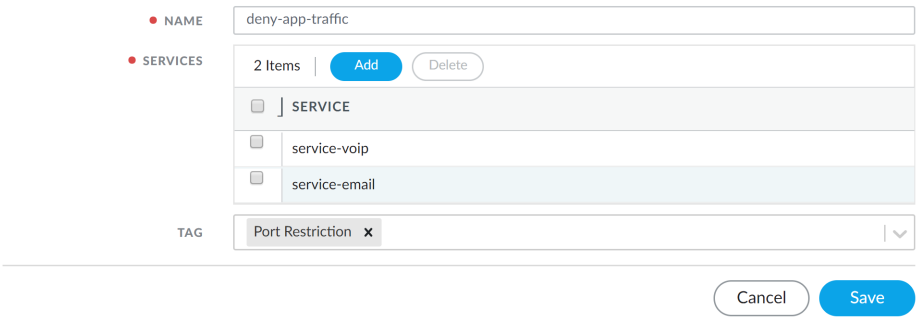
STEP 4 | Enter a descriptive **Name** for the service group.

STEP 5 | **Add** the services to the service groups.

STEP 6 | (Optional) Select one or more **Tags** to apply to the service group.

STEP 7 | **Save** your configuration.

Service Groups



STEP 8 | Select **Commit** and **Commit and Push** your configuration changes.

Use Tags to Group and Visually Distinguish Policies and Objects

Tag policies and objects to group related items and add colors to visually distinguish them from other configured policies and objects for easy scanning. You can tag all Prisma Access policies, as well as address objects, address groups, service objects, and service groups.

You can apply or more tags to any policy rule or object, with up to a maximum of 64 tags. Prisma Access supports up to 10,000 tags.

- Create and Apply a Tag
- Modify Tags

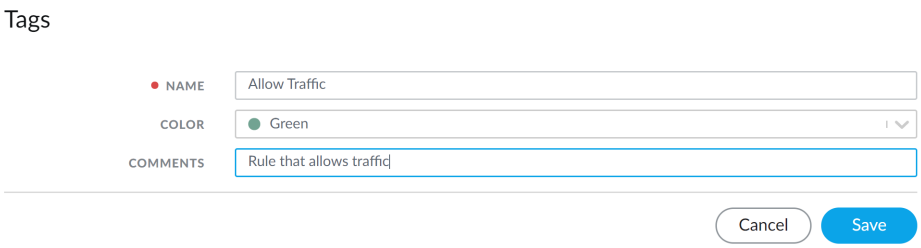
Create and Apply a Tag

Use tags to identify the purpose of a rule or a configuration object to help you organize your rulebase and objects.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Create a tag.

1. Select **Objects** > **Tags** and **Add** a new tag.
2. Enter a **Name** for the tag that clearly describes its purpose.
3. (Optional) Assign one of the 42 predefined colors to the tag. By default, **Color** is **None**.
4. (Optional) Enter **Comments** to describe in greater detail the purpose of the tag.
5. **Save** your configuration.



6. Select **Commit** and **Commit and Push** your configuration changes.

STEP 3 | Apply tags to an address object, address group, service, or service group.

1. Select **Objects**, and for this example, Create a Service Object or edit an existing service object.
2. Add the tag you created in Step 2.
3. Click **Save**.
4. Select **Commit** and **Commit and Push** your configuration changes.

STEP 4 | Apply tags to a policy.

1. Select **Policies** and select any rulebase under it.
2. Create a Policy Rule or edit an existing policy rule.
3. Add the tag you created in Step 2.
4. Click **Save**.
5. Select **Commit** and **Commit and Push** your configuration changes.

Modify Tags

You can modify existing tags already applied to policy rules or configured objects. Once modified, all policies or objects are automatically updated.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Select **Objects** > **Tags** to perform one of the following operations.

- Click the link in the **Name** to edit the properties of the tag.
- Select a tag in the table, and click **Delete** to remove the tag from Prisma Access. All policies and objects to which the tag are applied no longer display the tag.
- Select a tag and click **Clone** to create a duplicate tag witgh the same properties. A numerical suffix is added to the tag name. For example, HQ-1.

STEP 3 | **Save** your configuration changes.

STEP 4 | Select **Commit** and **Commit and Push** your configuration changes.

Create HIP Objects

To enable the use of host information in policy enforcement, create a HIP object based on the host information you want to collect to enforce policy. Create a HIP profile to group multiple HIP objects.

- Create a HIP Object
- Create a HIP Profile

Create a HIP Object

Enable the use of host information in policy enforcement. HIP objects are building blocks that allow you to Create a HIP Profile. Palo Alto Networks recommends keeping your HIP objects specific and focused on matching on one item, such as the presence of a particular type of required software, membership in a specific domain, or the presence of a specific OS. Doing this allows you flexibility to create granular HIP-augmented policies.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Select **Objects** > **HIP Objects** and **Add** a HIP object.

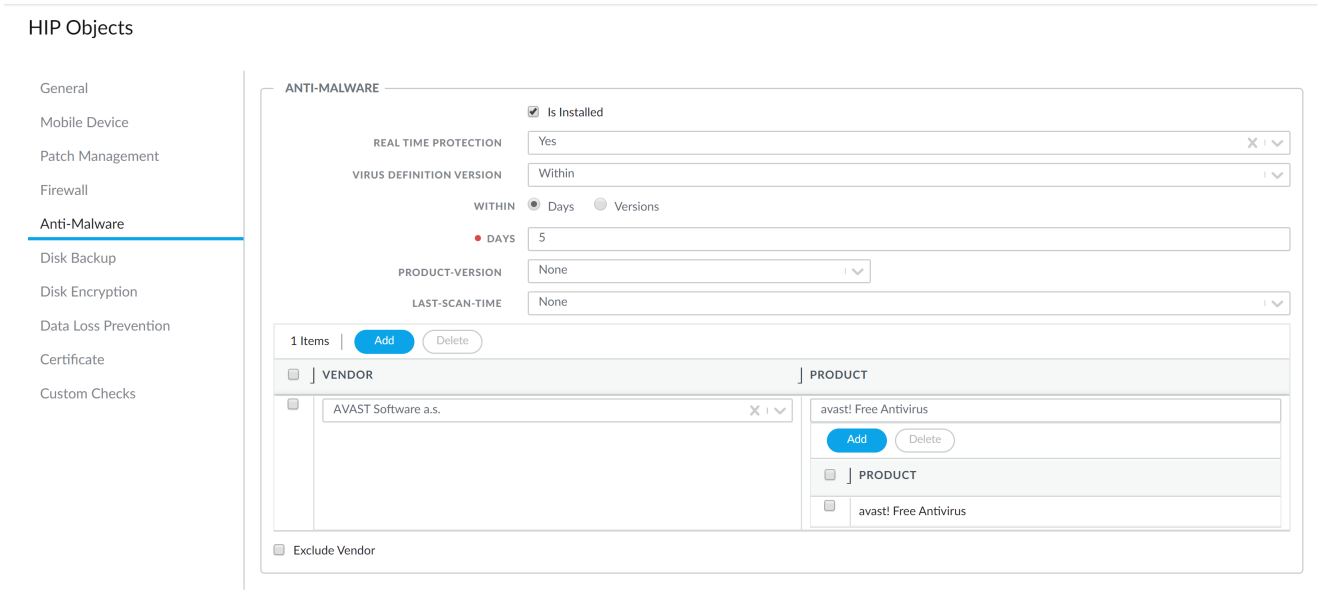
STEP 3 | Enter a **Name** for the HIP object.

STEP 4 | (Optional) Enter a description for the HIP object.

STEP 5 | Select the tab that corresponds to the category of host information you are interested in matching against, and then select the check box to enable the object to match against the category. For example, to create an object that looks for information about antivirus or anti-spyware software, select the **Anti-Malware** tab. The following image shows how to create a HIP object that matches if the endpoint has the AVAST Free Antivirus software application installed, has Real Time Protection enabled, and has virus definitions that have been updated within the last 5 days.

Prisma Access supports in-line creation of Certificate Profiles.

Repeat this step for each category you want to match against in this object.



STEP 6 | **Save** your configuration.

STEP 7 | Select **Commit** and **Commit and Push** your configuration changes.

Create a HIP Profile

HIP profiles allow you to combine multiple HIP objects using Boolean logic. This allows for traffic flow to be evaluated against the resulting HIP profile. If there is a match, the policy rule to which the HIP profile is attached is enforced. If there is no match, the traffic flow is evaluated against the next rule as with any other policy matching criteria.

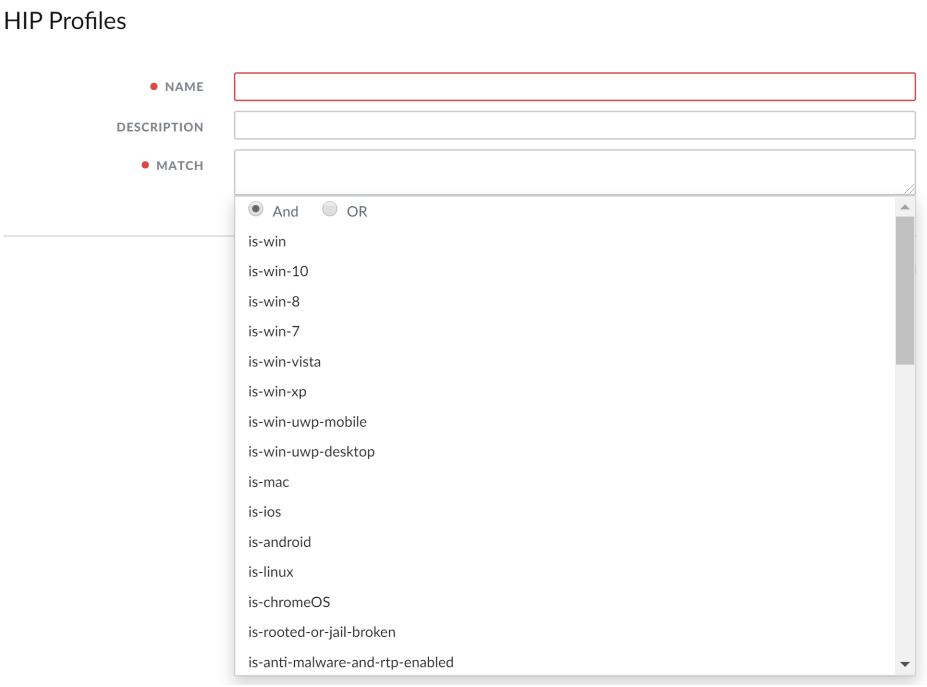
STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Select **Objects** > **HIP Profiles** and **Add** a HIP profile.

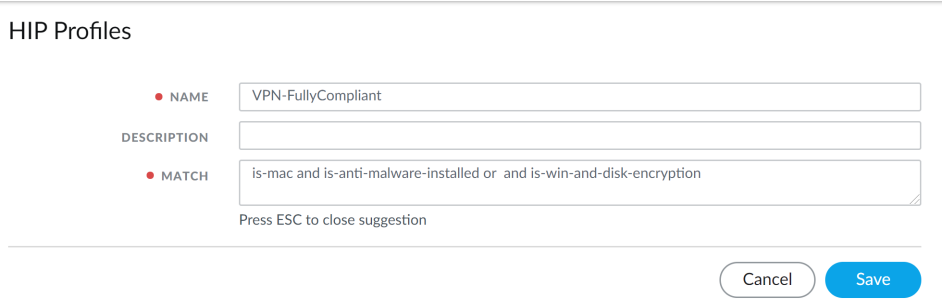
STEP 3 | Enter a **Name** for the HIP profile.

STEP 4 | (Optional) Enter a description for the HIP profile.

STEP 5 | Select the first HIP object or profile you want to use as a match criteria to add it to the **Match** text box.



STEP 6 | Continue adding match criteria as appropriate for the profile you are building, making sure to select the appropriate Boolean operator radio button (**AND** or **OR**) between each addition.



STEP 7 | **Save** your configuration.

STEP 8 | Select **Commit** and **Commit and Push** your configuration changes.

External Dynamic List in Prisma Access

An external dynamic list is a text file that you or another source host on an external web server from which Prisma Access can import IP addresses, URLs, and domains to enforce policies on the entries in the list. Prisma Access dynamically imports new entries in the external dynamic list when updated at the configured interval and enforces policy without need to make additional configuration changes.

- Types of External Dynamic Lists
- Formatting Guidelines for an External Dynamic List
- Built-In External Dynamic Lists
- Configure Access to an External Dynamic List

Types of External Dynamic Lists

An External Dynamic List is a text file containing import objects—IP addresses, URLs, or domains— from an external web server that Prisma Access can use to enforce policy. As you modify the list, Prisma Access dynamically imports the list at the configured interval and enforces policy without you needing to make any configuration changes or commit on Prisma Access. If the web server is not unreachable, Prisma Access uses the last successfully retrieved list for enforcing policy until connection to the web server is restored. but only if the list is not secured with SSL.

To enforce policy on the entries in the list, you must reference the list in a supported policy rule or profile. When you reference multiple lists, you can prioritize the order of evaluation to make sure the most important lists are committed before reaching capacity limits.

Prisma Access supports the following types of external dynamic lists:

- **Predefined IP Address**—A predefined IP address list is a list that refers to the built-in, dynamic IP lists with fixed or "predefined" contents. These Built-In External Dynamic Lists—for bulletproof hosting providers, known malicious, and high-risk IP addresses— are automatically added to Prisma Access. A predefined IP address list can also refer to an EDL that uses one of the built-in lists as a source. Because you cannot modify the contents of a predefined list, you may use one as a source for a different EDL if you want to add or exclude list entries.
- **IP Address**—Enforce policy for a list of source or destination IP addresses that emerge ad hoc by using an external dynamic list of type IP address as the source or destination address object in policy rules and configure Prisma Access to deny or allow access to the IP addresses included in the list. Prisma Access treats an external dynamic list of type IP address as an address object, and all IP addresses included are handled as one address object.
- **URL**—An external dynamic list of type URL allows you to protect your network from new sources of threat or malware using URLs. You can use this list in two ways:
  - As a match criteria in Security policy rules, Decryption policy rules, and QoS policy rules to allow, deny, decrypt, not decrypt, or allocate bandwidth for the URLs.
  - In a URL Filtering profile where you can define more granular actions, such as continue, alert, or override, before you attach the profile to a Security policy rule.
- **Domain**—An external dynamic list of type domain allows you to import custom domain names to Prisma Access to enforce policy. This is very useful if you subscribe to third-party intelligence feeds and want to protect your network from new sources of threat or malware as soon as you learn of a suspicious domain. For each domain you include in the list, Prisma Access creates a custom DNS-based spyware signature so that you can enable DNS sinkholing.

Formatting Guidelines for an External Dynamic List

An external dynamic list of one type—IP address, URL, or Domain—must include entries of that type only. The entries in a predefined list comply with the formatting guidelines for IP address lists.

- IP Address List
- Domain List
- URL List

IP Address List

The external dynamic list can include individual IP addresses, subnet addresses (subnet/mask) or range of IP addresses. The block list can include comments and special characters such as **`*`**, **`:`**, **`;`**, **`#`**, or **`/`**. The syntax of each line in the list is: [<**`IP address`**>, <**`IP/Mask`**>, or <**`IP start range`**>-<**`IP end range`**> [**`space`**] [<**`comment`**>].

Enter each IP address/range/subnet in a new line. URLs or domains are not supported in this list. A subnet or IP address range count as one IP address entry and not as multiple IP addresses. If you add comments,

the comments must be on the same line as the IP address/range/subnet. The space at the end of the IP address is the delimiter that separates a comment from the IP address.

An example IP address list:

```
192.168.20.10/32
 2001:db8:123:1::1 #test IPv6 address
 192.168.20.0/24 ; test internal subnet
 2001:db8:123:1::/64 test internal IPv6 range
 192.168.20.40-192.168.20.50
```

For an IP address that is blocked, you can display a notification page only if the protocol is HTTP.

Domain List

Follow these guidelines when creating domain list entries:

- Enter each domain name in a new line; URLS or IP addresses are not supported in this list.
- Do not prefix the domain name with the protocol, http://, or https://
- The following characters are considered token separators: . / ? & = ; +

  Every string separated by one or two of these characters is a token.
- You can use a caret (^) to indicate an exact match value.

Prisma Access does not support wildcards in external dynamic list type domain.

URL List

Follow these guidelines when creating URL list entries:

- Enter the IP addresses or URLs of websites that you want to enforce seperately from the assocaited URL category.
- List entries must be an exact match and are case-sensitive.
- Enter a string that is an exact match to the website, and possibly a specific subdomain, for which you want to control access.
- Omit http and https from URL entries.

Prisma Access does not support wildcards in external dynamic list type URL.

Built-In External Dynamic Lists

Palo Alto Networks provides built-in IP address external dynamic lists that you can use to protect against malicious attacks.

- **Palo Alto Networks Bulletproof IP Addresses**—Contains IP addresses provided by bulletproof hosting providers. Because bulletproof hosting providers place few, if any, restrictions on content, attackers frequently use these services to host and distribute malicious, illegal, and unethical material.
- **Palo Alto Networks High-Risk IP Addresses**—Contains malicious IP addresses from threat advisories issued by trusted third-party organizations. Palo Alto Networks compiles the list of threat advisories, but does not have direct evidence of the maliciousness of the IP addresses.
- **Palo Alto Networks Known Malicious IP Addresses**—Contains IP addresses that are verified malicious based on WildFire analysis, Unit 42 research, and data gathered from telemetry. Attackers use these IP addresses almost exclusively to distribute malware, initiate command-and-control activity, and launch attacks

Prisma Access receives updates for these feeds in the automatic content updates, allowing Prisma Access to automatically enforce policy based on the latest threat intelligence from Palo Alto Networks. You cannot modify the contents of the build-in lists. Use them as-is, or create a custom external dynamic list that uses one of the lists as a source and exclude entries from the list as needed.

Configure Access to an External Dynamic List

You must establish a connection between Prisma Access and the source that hosts the external dynamic list.

STEP 1 | Find an external dynamic host to use with Prisma Access.

- Create an external dynamic list and host it on a web server. Enter IP addresses, domains, or urls in a blank text file. See Formatting Guidelines for an External Dynamic List for more information on the format requirements for each external dynamic list type.
- Use an existing external dynamic list hosted by another source and verify that it follows the Formatting Guidelines for an External Dynamic List.

STEP 2 | Launch Prisma Access Cloud Management.

STEP 3 | Select **Objects** > **External Dynamic Lists**.

STEP 4 | Click **Add** and enter a descriptive **Name** for the list.

STEP 5 | Select the list **Type**.

If you are using a **Domain List**, you can optionally enable **Automatically expand to include subdomains** to also include the subdomains of a specified domain. For example, if your domain list includes paloaltonetworks.com, all lower level components of the domain name (e.g., *.paloaltonetworks.com) will also be included as part of the list. Keep in mind, when you enable this setting, each domain in a given list requires an additional entry, effectively doubling the number of entries that are consumed.

STEP 6 | Enter the **Source** for the external dynamic list. The source must include the full path to access the list. For example, **`https://1.2.3.4/EDL_IP_2019`**

If you are creating a list of type **Predefined IP**, select a Palo Alto Networks malicious IP address feed to use as a source.

STEP 7 | If the source is secured with SSL (i.e lists with an HTTPs URL), select a **Certificate Profile** to authenticate the server that hosts the list. If a certificate profile does not exist, select **Add Certificate Profile** to create a new certificate profile. The certificate profile you select must have a root CA (certificate authority) and intermediate CA certificates that match the certificates installed on the server you are authenticating.

STEP 8 | Specify the **Check for updates** frequency at which Prisma Access retrieves the list. By default, Prisma Access retrieves the list once every hour and commits the changes.

The interval is relative to the last commit. For example, for the five-minute interval, the commit occurs in five minutes if the last commit was an hour ago.

STEP 9 | (Optional) Select **Exception List** and **Add** any entries to exclude from the External Dynamic List.

You can add up to 100 entries to exclude.

STEP 10 | **Save** your configuration.

STEP 11 | Select **Commit** and **Commit and Push** the configuration changes.

Create a URL Category Object

Create a custom URL category object to add it to a URL Filtering profile. Custom URL category objects allow you to specify exceptions to URL category enforcement in a policy rule, and allows you to create a custom URL category based on multiple URL categories:

- **Define exceptions to URL category enforcement**—Create a custom list of URLs that you want to use to match criteria in a security policy rule. This is a good way to specify exceptions to URL categories where you would like to enforce specific URLs differently than the URL category to which they belong.
- **Define a custom URL category based on multiple PAN-DB categories**—Allows you to target enforcement for websites that match a set of categories. The website or page must match all the categories defined as part of the custom category.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Select **Objects** > **URL Category** and **Add** a URL category object.

STEP 3 | Enter a **Name** for the custom URL category.

STEP 4 | (Optional) Enter a description for the custom URL category.

STEP 5 | Select the category **Type** from the drop-down.

- **URL List**—Add URLs that you want to enforce differently than the URL category to which they belong. Use this list type to define exceptions for URL Category enforcement, or to define a list of URLs as beloning to a custom category.
- **Category Match**—Provide targeted enforcement for websites that match a set of categories. The website must match all the categories as defined as part of the custom category.

STEP 6 | **Add** the website or URL category based on category type selected in the previous step.

STEP 7 | **Save** your configuration.

STEP 8 | Select **Commit** and **Commit and Push** your configuration changes.

Create a Security Profile

Create one or more security profiles to attach to your policy rules for further content inspection for traffic matches.

- View the Default Antivirus Security Profiles
- View the Default Anti-Spyware Security Profiles
- Create a Vulnerability Protection Profile
- Create a URL Filtering Profile
- Create a File Blocking Profile
- Create a WildFire Analysis Profile
- View the Default Decryption Security Profiles

View the Default Antivirus Security Profiles

Antivirus security profiles protect against viruses, worms, trojans, and spyware downloads. Using a stream-based malware prevention engine that inspects traffic the moment the first packet is received, Prisma Access provides protection for your corporate devices without impacting the security processing node performance. This profile scans a variety of malware in executables, PDF files, HTML, and JavaScript viruses

and includes support for scanning inside compressed files and data encoding schemes. You can only add the `default` and `best-practice` antivirus security profiles to security rules or security profile groups. Creating custom antivirus security profiles is not supported.

The actions the security processing node takes when responding to an antivirus threat are:

- **Default**—For each threat signature and Antivirus signature that is defined by Palo Alto Networks, a default action is specified internally. Typically, the default action is an alert or a reset-both. The default action is displayed in parenthesis, for example default (alert) in the threat or Antivirus signature
- **Allow**—Permits the application traffic.
- **Alert**—Generates an alert for each application traffic flow. The alert is saved in the threat log.
- **Drop**—Drops the application traffic.
- **Reset Client**—For TCP, resets the client-side connection. For UDP, drops the connection.
- **Reset Server**—For TCP, resets the server-side connection. For UDP, drops the connection.
- **Reset Both**—For TCP, resets the connection on both client and server ends. For UDP, drops the connection.
- **Block IP**—Blocks traffic from either a source or a source-destination pair. It is configurable for a specified period of time.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Select **Objects** > **Security Profiles** > **Antivirus**.

STEP 3 | Review the **`default`** antivirus security profile. The **`default`** antivirus security profile inspects all of the listed protocol decoders for viruses, and generates alerts for SMPT, IMAP, and POP3 protocols while blocking FTP, HTTP, and SMB protocols.

STEP 4 | Review the **`best-practice`** antivirus security profile.

Prisma Access Common
Antivirus Security Profiles

Search Antivirus Security Profiles

2 Items

			Decoders			
NAME	LOCATION	PACKET CAPTURE	NAME	ACTION	WILDFIRE ACTION	DYNAMIC CLASSIFICATION ACTION
default	predefined		http	default	default	default
			http2	default	default	default
			smtp	default	default	default
			imap	default	default	default
			pop3	default	default	default
			ftp	default	default	default
			smb	default	default	default
best-practice	predefined		ftp	default	reset-both	reset-both
			http	default	reset-both	reset-both
			imap	alert	alert	alert
			pop3	alert	alert	alert
			smb	default	reset-both	reset-both
			smtp	reset-both	reset-both	reset-both

View the Default Anti-Spyware Security Profiles

Anti-Spyware profiles allow you to block malicious traffic from compromised hosts by enabling you to stop compromised hosts from trying to phone-home or beacon out to external command-and-control servers. You can apply various levels of protection between zones. You can only add the `default`, `strict`, `best-practice-strict`, and `best-practice` anti-spyware security profiles to security rules or security profile groups. Creating custom anti-spyware security profiles is not supported.

The actions the security processing node takes when responding to a anti-spyware event are:

- **Default**—For each threat signature and Anti-Spyware signature that is defined by Palo Alto Networks, a default action is specified internally. Typically, the default action is an alert or a reset-both. The default action is displayed in parenthesis, for example default (alert) in the threat or anti-spyware signature.
- **Allow**—Permits the application traffic.
- **Alert**—Generates an alert for each application traffic flow. The alert is saved in the threat log.
- **Drop**—Drops the application traffic.
- **Reset Client**—For TCP, resets the client-side connection. For UDP, drops the connection.
- **Reset Server**—For TC, resets the server-side connection. For UDP, drops the connection.
- **Reset Both**—For TCP, resets the connection on both client and server ends. For UDP, drops the connection.
- **Block IP**—Blocks traffic from either a source or a source-destination pair. It is configurable for a specified period of time.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Select **Objects** > **Security Profiles** > **Anti-Spyware**.

STEP 3 | Review the **`default`**, **`strict`**, **`best-practice-strict`**, and **`best-practice`** anti-spyware security profiles to understand which profiles best address your security needs.

Prisma Access Common
AntiSpyware Security Profiles

Search AntiSpyware Security Profiles

4 Items

NAME	LOCATION	COUNT	RULE NAME	THREAT NAME	SEVERITY	ACTION	PACKET CAPTURE
default	predefined	Rules: 4	simple-critical simple-high simple-medium simple-low	any any any any	critical high medium low	default default default default	disable disable disable disable
strict	predefined	Rules: 5	simple-critical simple-high simple-medium simple-informational simple-low	any any any any any	critical high medium informational low	reset-both reset-both reset-both default default	disable disable disable disable disable
best-practice-strict	predefined	Rules: 5	simple-critical simple-high simple-medium simple-informational simple-low	any any any any any	critical high medium informational low	reset-both reset-both reset-both default default	disable disable disable disable disable
best-practice	predefined	Rules: 5	simple-critical simple-high simple-medium simple-low simple-info	any any any any any	critical high medium low informational	default default default default default	disable disable disable disable disable

Create a Vulnerability Protection Profile

Vulnerability protection profiles allow you to stop attempts to exploit system flaws or gain unauthorized access to your organizations systems. The vulnerability protection profile protects against unwanted threats entering your networks through means such as buffer overflows, illegal code executions, or other attempts to exploit system vulnerabilities.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Select **Objects** > **Vulnerability Protection** and **Add** a profile.

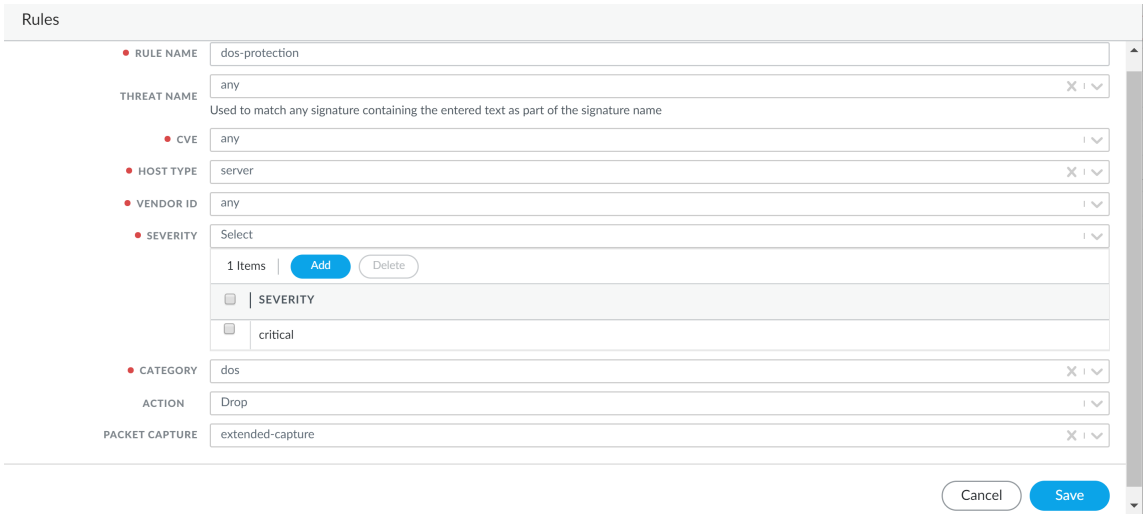
STEP 3 | Enter a **Name** for the vulnerability protection profile.

STEP 4 | (Optional) Enter a description for the vulnerability protection profile.

STEP 5 | **Add** a threat signature.

1. Enter a **Name** for the threat signature.

2. Specify a **Threat Name** using a text string. Prisma Access uses the threat name to match any signature containing the entered text as part of the signature name.
3. Specify the **Action** to take when the rule is triggered.
   - **Default**—For each threat signature that is defined by Palo Alto Networks, a default action is specified internally. Typically the default action is an alert or a reset-both.
   - **Allow**—Permits the application traffic.
   - **Alert**—Generates an alert for each application traffic flow. The alert is saved in the threat log.
   - **Drop**—Drops the application traffic.
   - **Reset Client**—For TCP, resets the client-side connection. For UDP, drops the connection.
   - **Reset Server**—For TCP, resets the server-side connection. For UDP, drops the connection.
   - **Reset Both**—For TCP, resets the connection on both client and server ends. For UDP, drops the connection.
   - **Block IP**—This action blocks traffic from either a source or a source-destination pair. It is configurable for a specified period of time.
4. (Block IP only) Specify whether to track the threat signature from only the **Source**, or both **Source and Destination**, and specify the **Duration** (between 1 and 3600 seconds).
5. Select the **Packet Capture** setting from the drop-down. Select **single-packet** to capture one packet when a threat is detected, or select **extended-capture** to capture from 1 to 50 packets (default is 5 packets). Select **disable** to not capture any packets.
6. Select the **Host Type** from the drop-down to specify whether to limit the signatures for the rule to those that are **client** side, **server** side, or either (**any**).
7. Select a vulnerability **Category** from the drop-down if you want to limit the signatures to those that match that category.
8. **Add** a **CVE** entry to specific common vulnerability and exposures if you want to limit the signatures to those that also match the specified CVEs.
9. **Add** a **Vendor ID** to specify specific vendor ID's you want to limit the signatures to those that match the specified vendor IDs.
10. **Add** a **Severity** if you want to limit the signatures to those that also match the specified severities.
11. **Save** your configuration.



STEP 6 | Add any threat exceptions.

Only create a threat exception if you are sure an identified threat is not a threat (false positive). If you believe you have discovered a false positive, open a support case with Palo Alto Networks to investigate the incorrectly identified threat. When the issue is resolved, remove the exception from the profile immediately.

1. Select the **Exceptions** tab and **Add** a new threat exception.
2. Enter a **Name** for the threat exception.
3. Select the **Packet Capture** setting from the drop-down.
4. Specify the **Action** to take when the rule is triggered.
5. Configure the **Time Attribute** to specify the number of hits per unit of time and whether the threshold applies to source, destination, or to both source and destination.
6. **Add** an **Exempt IP**. When you add an IP address to a threat exception, the threat exception action for that signature will take precedence over the rule's action only if the signature is triggered by a session with either a source or destination IP address matching an IP address in the exception.

STEP 7 | **Save** your configuration.

STEP 8 | Select **Commit** and **Commit and Push** your configuration changes.

Create a URL Filtering Profile

URL Filtering protects your applications, users and other corporate assets against web-based threats while allowing you to control how users interact with online content. Attach a URL Filtering profile to a Security policy rule to compare policy rule traffic matches against the Palo Alto Networks URL filtering database, which contains a listing of millions categorized websites. Use these URL categories as a match criteria to enforce security policies.

STEP 1 | Launch Prisma Access Cloud Management.

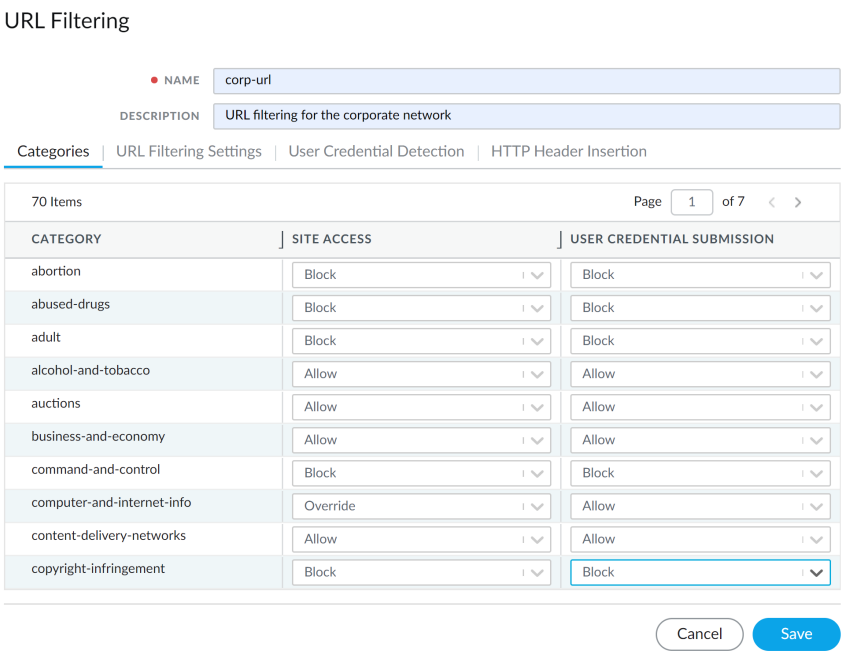
STEP 2 | Select **Objects** > **URL Filtering** and **Add** a profile.

STEP 3 | Enter a **Name** for the URL filtering profile.

STEP 4 | (Optional) Enter a description for the URL filtering profile.

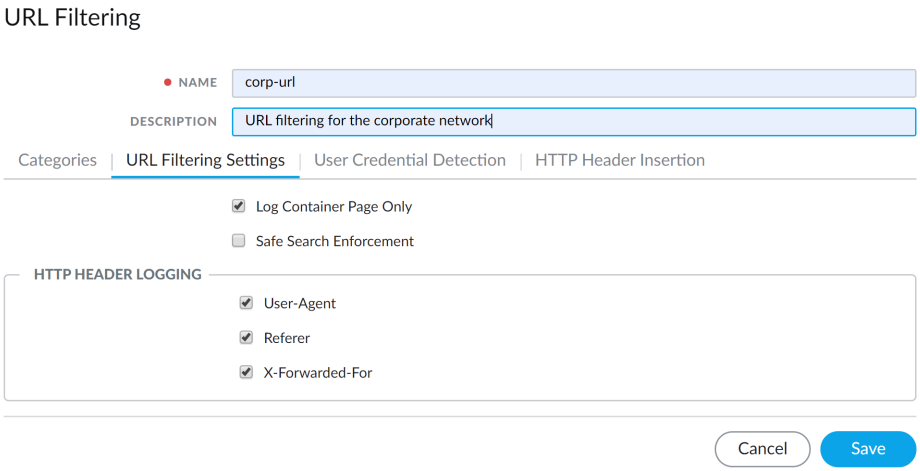
STEP 5 | Select **Categories** and set the site access for each URL category:

- **Alert**—Allows access to the website but adds an alert to the URL log each time a user accesses the URL.
- **Allow**—Allows traffic to the URL category. Allowed traffic is not logged.
- **Block**— Block access the website. If the URL category is set to block, then the User Credential Submission permissions are automatically set to block.
- **Continue**—Displays a warning to users to discourage them for accessing the website. The user must then choose to **Continue** to the website if they decide to ignore the warning.
- **Override**—Display a response page that prompts the user to enter a valid password to gain access to the site.



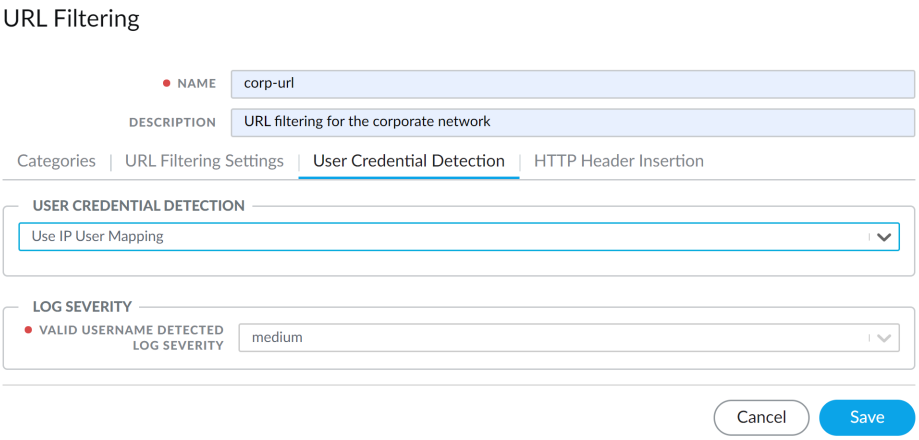
STEP 6 | Set the URL filtering profile settings.

1. Select **URL Filtering Settings** and decide whether you want to enable (check) the following:
   - **Dynamic URL** to enable cloud lookup for categorizing a URL.
   - **Log Container Page Only** so that only the main page that matches the category is logged, and not subsequent pages or categories that may be loaded within the container page. Leave this setting disabled (clear) to log all pages or categories that may be loaded with the container page.
   - **Safe Search Enforcement** to block all traffic that does not match the browser's strict safe search settings.
2. Decide whether to enable (check) HTTP Header Logging for one or more supported HTTP header fields. You can enable one or more of the following to include in the HTTP header.
   - **User Agent** to include the web browser the user used to access the URL.
   - **Refer** to include the web page that redirected (referred) the user to the web page that is being requested.
   - **X Forwarded For** to preserve the IP address of the user who requested the web page.



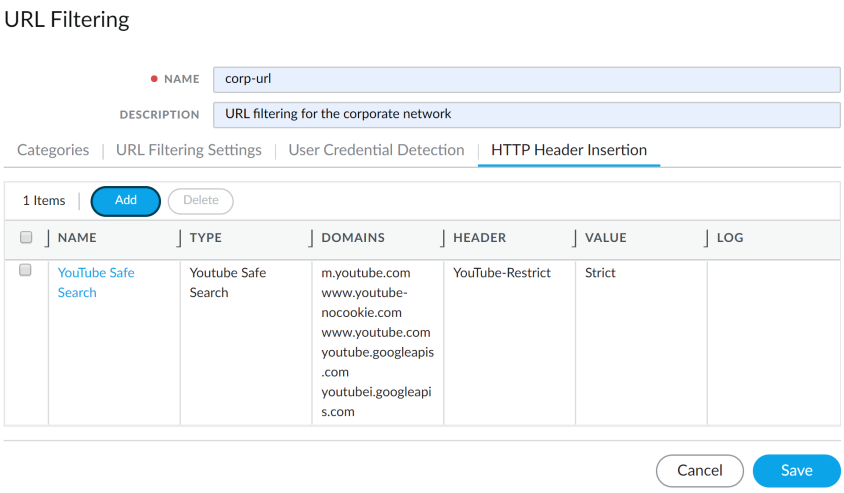
STEP 7 | Configure the URL filtering profile to detect credential submissions to websites that are in allowed URL categories.

1. Select **User Credential Detection**.
2. Select one of the methods from the **User Credential Detection** drop-down:
   - **Use IP Mapping**—Checks for valid corporate username submissions and verifies that the username matches the user logged in the source IP address of the session. To use this method, Prisma Access matches the submitted username against its IP-address-to-username mapping table.
   - **Use Domain Credential Filter**—Checks for valid corporate usernames and password submissions verifies that the username maps to the IP address of the logged in user.
   - **Use Group Mapping**—Checks for valid corporate usernames and password submissions verifies that the username maps to the IP address of the logged in user.
3. Set the **Valid Username Detected Log Severity** Prisma Access uses to log detection of corporate credential submissions. By default, Prisma Access logs these events as medium severity.



STEP 8 | Create custom HTTP Header Insertions to manage access to applications that use HTTP headers to limit access to services.

1. Select **HTTP Header Insertion**.
2. **Add** a new HTTP header insertion and give it a **Name**.
3. Enable (check) **Disable Override** to prevent administrators from overriding the settings of this URL filtering profile. This selection is cleared by default, which means that administrators can override the settings of the URL filtering profile.
4. **Add** the HTTP header **Type**. Entries can be predefined or custom.
5. **Save** your HTTP header insertion entries.



STEP 9 | **Save** your configuration.

STEP 10 | Select **Commit** and **Commit and Push** your configuration changes.

Create a File Blocking Profile

File Blocking security profiles allow you to identify specific file types to monitor or block. For most traffic, block files that are known to carry threats or that have no real use case for upload/download. These include batch files, DLLs, Java class files, help files, Windows shortcuts (.lnk), and BitTorrent files.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Select **Objects** > **File Blocking** and **Add** a profile.

STEP 3 | Enter a **Name** for the file blocking profile.

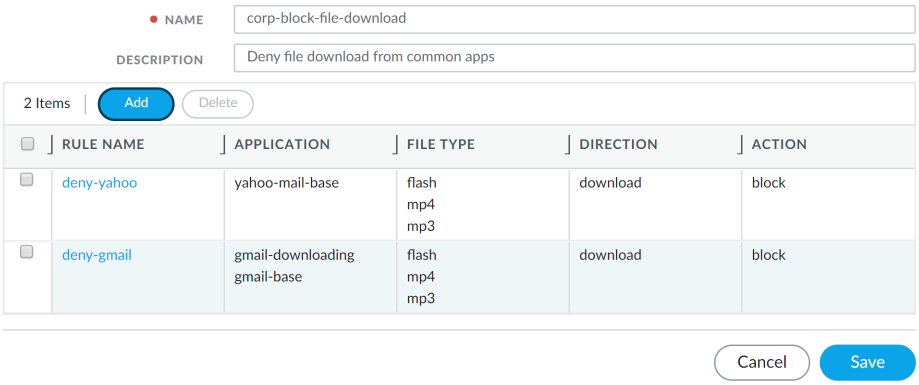
STEP 4 | (Optional) Enter a description for the file blocking profile.

STEP 5 | Configure the file blocking options.

1. **Add** and define a rule for the profile.
2. Enter a **Name** for the rule.
3. **Add** an **Application** for filtering.
4. **Add** a **File Type** for filtering.
5. Specify the **Direction** of file transfer, such as **download**.
6. Specify the **Action** (**alert**, **block**, or **continue**). For example, select **continue** to prompts users for confirmation before they are allowed to download an executable (.exe) file. Alternatively, you can **block** the specified files or trigger an **alert** when a user downloads an executable file.

STEP 6 | **Save** your configuration.

File Blocking



STEP 7 | Select **Commit** and **Commit and Push** your configuration changes.

Create a WildFire Analysis Profile

Specify traffic to forward for analysis based on application, file type, transmission direction to the public WildFire cloud. By forwarding known and unknown malicious traffic to the WildFire cloud allows Palo Alto Networks a valuable source of threat intelligence based on malware variants that signatures successfully prevented but neither WildFire or Prisma Access have seen before.

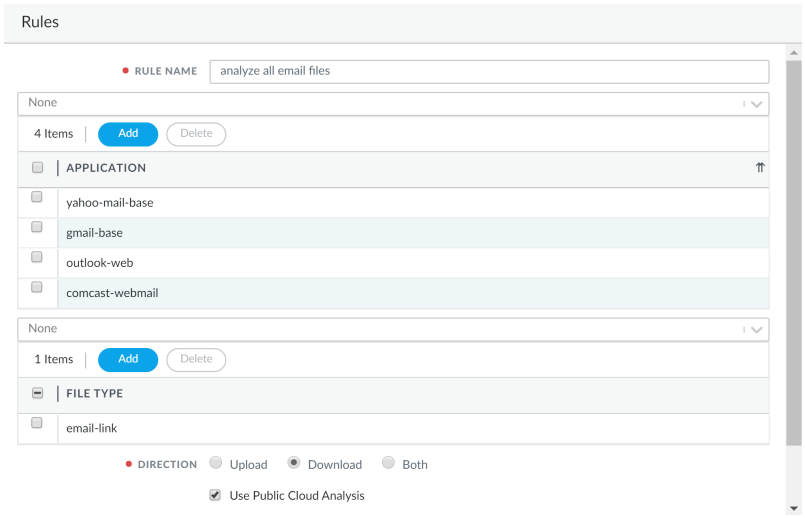
STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Select **Objects** > **WildFire Analysis** and **Add** a profile.

STEP 3 | Enter a **Name** for the WildFire analysis profile.

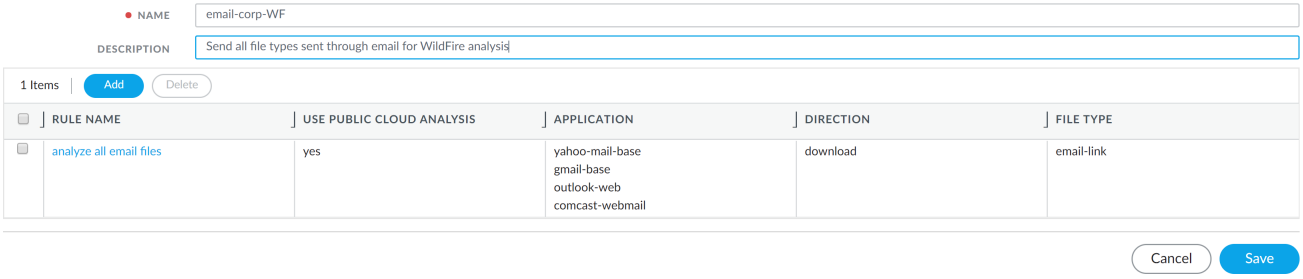
STEP 4 | Configure the WildFire Analysis profile.

1. (Optional) Enter a description for the WildFire analysis profile.
2. **Add** a WildFire Analysis rule and give the rule a descriptive **Name**.
3. Define the profile to match to unknown traffic and to forward samples for analysis based on:
   - **Applications**—Forward files based on the application in use
   - **File Types**—Forward files based on file types, including links contained in email messages. For example, select **PDF** to forward unknown PDFs detected by Prisma Access for analysis.
   - **Direction**—Forward files based on the transmission direction of the file (upload, download, or both). For example, select **both** to forward all unknown PDFs for analysis, regardless of transmission direction.
4. Set the **Analysis** location to the **public-cloud** to forward matching samples to the WildFire public cloud.
5. **Save** the WildFire Analysis rule.



STEP 5 | **Save** your configuration.

WildFire Analysis



STEP 6 | Select **Commit** and **Commit and Push** your configuration changes.

View the Default Decryption Security Profiles

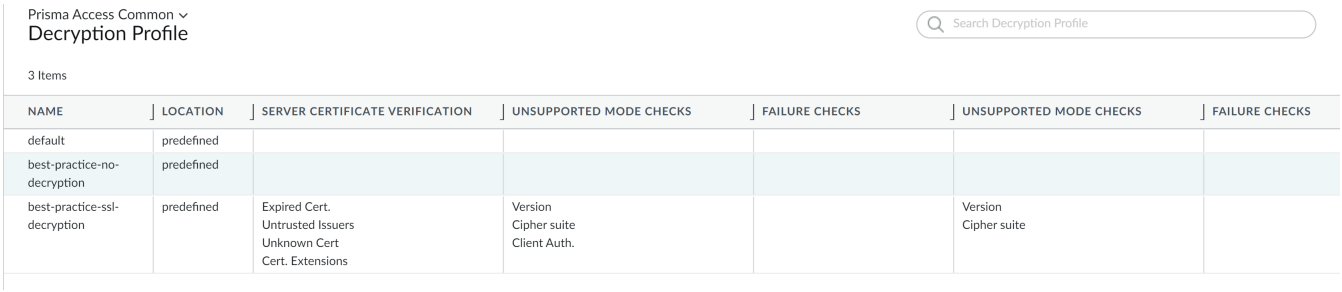
A decryption profile allows you to perform checks on both decrypted traffic and SSL traffic that you choose to exclude from decryption. Prisma Access includes the following default decryption profiles:

- `default`—Enforce the basic recommended protocol versions and cipher suites for decrypted traffic
- `best-practice-no-decryption`—Blocks sessions with expired certificates or untrusted certificate issuers.
- `best-practice-ssl-decryption`—Strict profile that blocks sessions with expired certificates or untrusted certificate issuers, along with additional SSL decryption requirements.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Select **Objects** > **Security Profiles** > **Decryption Profile**.

STEP 3 | Review the **`default`**, **`best-practice-no-decryption`**, and **`best-practice-ssl-decryption`** decryption profiles to understand which profiles best address your security needs.



Create a Security Profile Group

A security profile group is a set of security profiles that are treated as a single object to easily add to security policy rules. Group individual security profiles that are often assigned to a policy rule together to simplify policy creation and management.

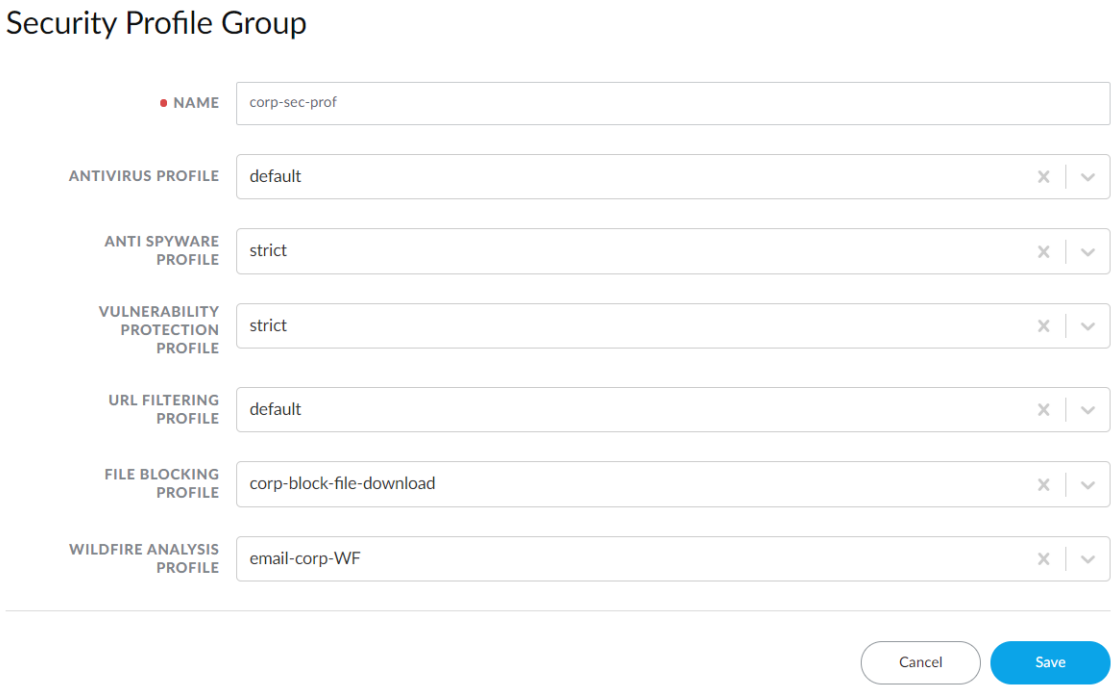
STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Create the required security profiles. See Create a Security Profile for more information on creating each security profile.

STEP 3 | Create the security profile group.

1. Select **Objects** > **Security Profile Group** and **Add** a new profile group.
2. Enter a descriptive **Name** for the security profile group.
3. Add existing profiles to the group using the drop-down for each security profile type. One security profile may be selected for each security profile type.
4. **Save** the new security profile group.

STEP 4 | **Save** your configuration.



STEP 5 | Select **Commit** and **Commit and Push** your configuration changes.

Create a Policy Rule

Prisma Access allows you to create various types of policies to protect your network from threats and disruptions, as well as help you optimize network resource allocation. Rules are evaluated from top to bottom and when traffic matches against the defined rule criteria, subsequent rules are not evaluated. You should order more specific policy rules above the more generic ones to enforce the best match criteria possible. A log is generated for traffic that matches a policy rule when logging is enabled for the rule. Logging options are configurable for each rule.

For corporate access security and decryption, best practice policy rules are available and allow you to quickly protect your corporate network using a Palo Alto Networks best practice security posture. These rules cannot be edited to ensure that you always have a minimum level of security readily available.

- Create a Security Policy Rule
- Create a QoS Policy Rule
- Create a Decryption Policy Rule
- Create an Application Override Policy Rule

Create a Security Policy Rule

Security policy rules determine whether to block or allow a session based on traffic attributes defined in the policy rule. All traffic that passes through the Prisma security processing node is matched against a session and the matching security policy rule is applied to the traffic in that session. You can create the following security policies:

- **Corporate Access**—Allow or deny traffic within your trusted corporate network. Corporate Access security rules allow you to define which users can access corporate assets within the defined trust zone.
- **Internet Access**—Allow or deny traffic from your trust zone to the internet. Internet Access security rules allow you to define whether trusted users and devices can access resources outside of your trusted corporate network. This may include sanctioned applications, social media, or unsanctioned or unknown applications and websites.

To protect your trusted corporate devices:

- Security Policy Actions
- Create an Internet Access Security Rule
- Customize the Predefined Internet Access Security Rules
- Create a Corporate Access Security Rule

Security Policy Actions

For traffic that matches the attributes defined in a security policy, you can apply the following actions:

Action	Description
Allow (default)	Allows the traffic.
Deny	Blocks traffic and enforces the default *Deny Action* defined for the application that is being denied. To view the deny action defined by default for an application, view the application details in **Objects** > **Applications** or check the application details in Applipedia.
Drop	Silently drops the traffic; for an application, it overrides the default deny action. A TCP reset is not sent to the host/application.

Action	Description
	For Layer 3 interfaces, to optionally send an ICMP unreachable response to the client, set Action: **Drop** and enable the **Send ICMP Unreachable** check box. When enabled, the Security Processing Node sends the ICMP code for *communication with the destination is administratively prohibited*—ICMPv4: Type 3, Code 13; ICMPv6: Type 1, Code 1.
Reset client	Sends a TCP reset to the client-side device.
Reset server	Sends a TCP reset to the server-side device.
Reset both	Sends a TCP reset to both the client-side and server-side devices.

A reset is sent only after a session is formed. If the session is blocked before a 3-way handshake is completed, the Security Processing Node will not send the reset.

For a TCP session with a reset action, the Security Processing Node does not send an ICMP Unreachable response.

For a UDP session with a drop or reset action, if the **ICMP Unreachable** check box is selected, the Security Processing Node sends an ICMP message to the client.

Create an Internet Access Security Rule

Internet access security rules allow you to allow or deny traffic from your corporate network to IP addresses or applications on the internet and allows you to specify individual IP addresses or users in the source and destination. These can be things such as sanctioned SaaS applications, social media websites, or malicious or unknown websites. When on-boarding mobile users, Prisma Access creates a default internet access policy.

For example, if you use Google Drive to store business-critical documents, you can create an internet access security rule to allow traffic to Google Drive. At the same time, your marketing team uses social media to promote your products, but you do not want all users to have access to those same social media websites. You can create an internet access security rule to allow traffic for sanctioned social media users, while blocking access to social media sites for all other users.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Select **Policies** > **Security** > **Internet Access** and **Add** a new security rule.

STEP 3 | Enter a **Name** for the security rule.

STEP 4 | (Optional) Enter a **Description** of the policy rule.

STEP 5 | (Optional) Select one or more **Tags** to group the policy rule.

STEP 6 | Define the matching criteria for the traffic source.

1. In the **Source** tab, select a **Zone**. You can select **Trust**, **Clientless VPN**, or both.
2. Specify the **Source** IP address(es) within the selected source zone(s) to which the rule applies. Select **any** to apply the rule to all IP addresses in your trusted corporate network, or **Add** specific IP addresses to which the rule applies. You must Create an Address Object before you can add it as a source in a policy rule.

Selecting the panw-bulletproof-ip-list as a Source IP address is not supported and results in a Push operation failure.

3. Specify the **Users** within the selected source zone(s) and source IP addresses to which the rule applies. Select **any** to apply this to all configured admin roles, or **Add** specific admin roles.
4. Select one or more **HIP Profiles** to add to the security rule to enable the use of host information in policy enforcement. Select **any** to apply all configured HIP profiles to the rule, or **Add** specific HIP profiles to the rule. You must Create a HIP Profile before you can add it to a policy rule.

STEP 7 | Define the matching criteria for the traffic destination.

1. In the **Destination** tab, verify that the **Zone** selected is the **Untrust** zone.
2. Specify the **Destination** IP address(es) within the selected destination zone to which the rule applies. Select **any** to apply the rule to all IP addresses on your corporate network, or **Add** specific IP addresses to which the rule applies. You must Create an Address Object before you can add it as a destination in a policy rule.

Selecting the panw-bulletproof-ip-list as a Destination IP address is not supported and results in a Push operation failure.

STEP 8 | In the **Application** tab, **Select** and **Add** one or more applications you want to block or allow. You can select multiple individual applications, or you can use application groups or application filters. You must Create Application Objects before you can add it as an application in a policy rule. By default, **any** is selected and applies the rule to all application traffic.

STEP 9 | Define the traffic match criteria based on the service used.

1. In the **Services/URL Category** tab, **Add** the **Services** to match the policy rule to. By default, the policy rule is set to decrypt **any** traffic on TCP or UDP ports. You can **Add** a service or service group, and optionally set the rule to **application-default** to match to applications only on the application default ports. You must Create Service Objects before you can add them to a policy rule.
2. In the **Service/URL Category** tab, specify a **URL Category** as a match criteria for the rule. By default, the policy rule is set to **any**.

STEP 10 | Define what actions to take when traffic matches the security policy rule.

1. In the **Actions** tab, select the **Action** to take when traffic is matched to the security rule. Review the Security Policy Actions to determine the correct action to take.
2. Configure the Log Settings when traffic matches the security policy rule, and from the **Log Forwarding** drop-down select the **Logging Service**.

Configuring the Log Settings is required in order to log traffic that matches the policy rule. The security processing node does not log any traffic matches if you do not configure the Log Forwarding to forward logs to the logging service.

3. To change the Quality of Service (QoS) settings on the packets matching the rule, select the **QoS Marking** setting from the drop-down and enter the QoS value in binary form or select a predefined value from the drop-down.

STEP 11 | Attach security profiles to enable the security processing node to scan all allowed traffic for threats.

In the **Actions** tab, select **Profiles** from the **Profiles Type** drop-down and attach the desired security profiles as needed. You must Create a Security Profile before you can attach it to a security rule.

STEP 12 | **Save** your configuration.

STEP 13 | Select **Commit** and **Commit and Push** your configuration changes.

Customize the Predefined Internet Access Security Rules

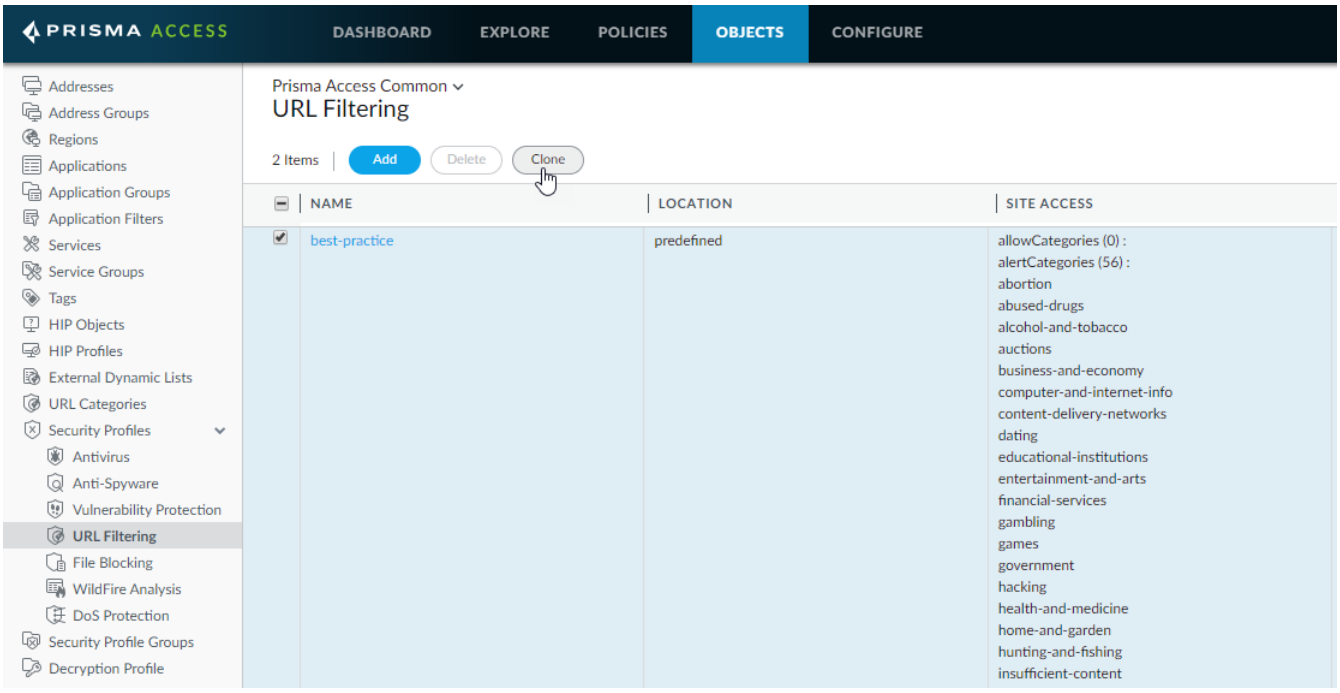
Prisma Access provides predefined internet access security policy rules based on best practices. These rules block known malicious traffic, log high risk traffic, and allow general web browsing. While these predefined rules are good for verifying that Prisma Access is provisioned and working as expected, you should customize these rules to add more granularity for your environment. For example, you might want to customize the allow-general-web-browsing rule to allow specific sanctioned applications or types of applications, or block additional URL categories (beyond those that are already blocked in the best practice URL Filtering profile). In addition, you must modify the rules to enable Prisma Access to forward the corresponding logs to the Cortex Data Lake.

Each predefined internet access security policy rule that allows traffic has a predefined best practice security profile group attached (either *best-practice* or *best-practice-strict*) that scans traffic that matches the rule for known and unknown threats using the best practice security profiles (Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering, File Blocking, and WildFire Analysis). If you want to modify a security profile, you must clone to modify it. You must then also clone the best practice security profile group and then attach the new profile to the profile group.

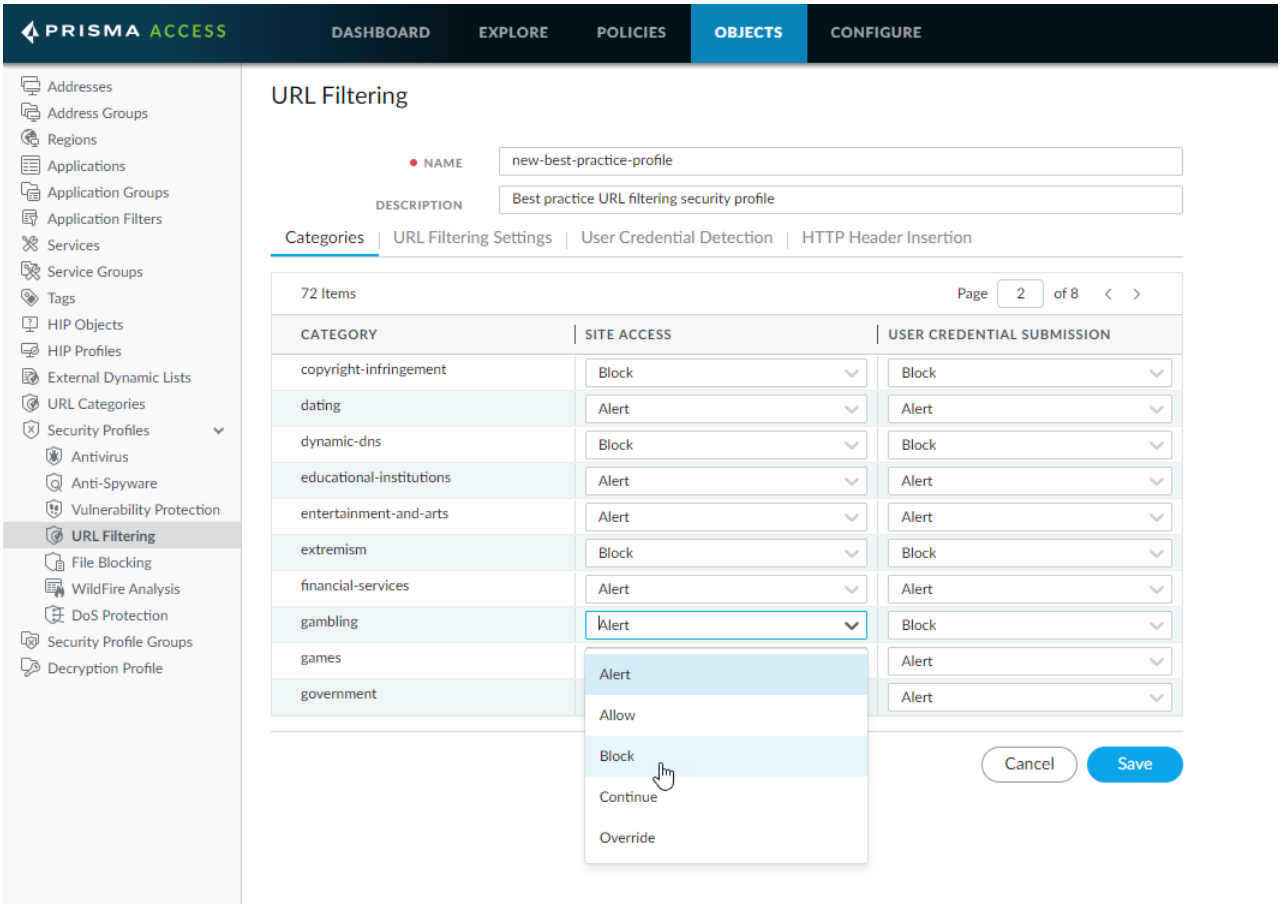
STEP 1 | Modify policy objects as needed for your environment.

For example, if you wanted to add gambling to the list of URL categories that are already blocked by the best practice URL Filtering profile, you would clone the best-practice URL filtering profile and set the **Site Access** to **Block**.

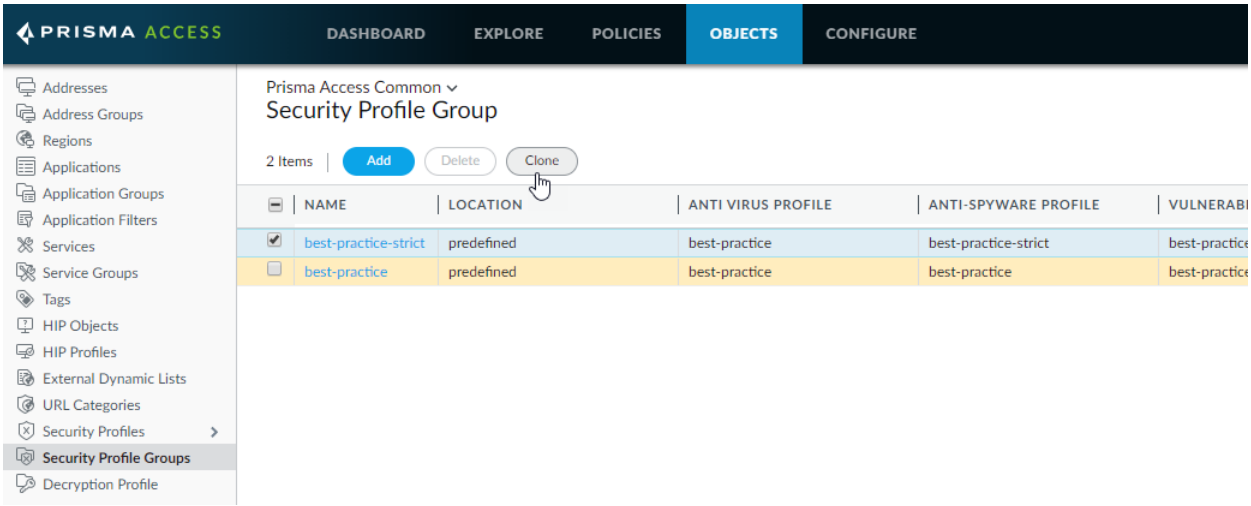
1. Select **Objects** > **Security Profiles** > **URL Filtering**, select the **best-practice** profile and **Clone** it.



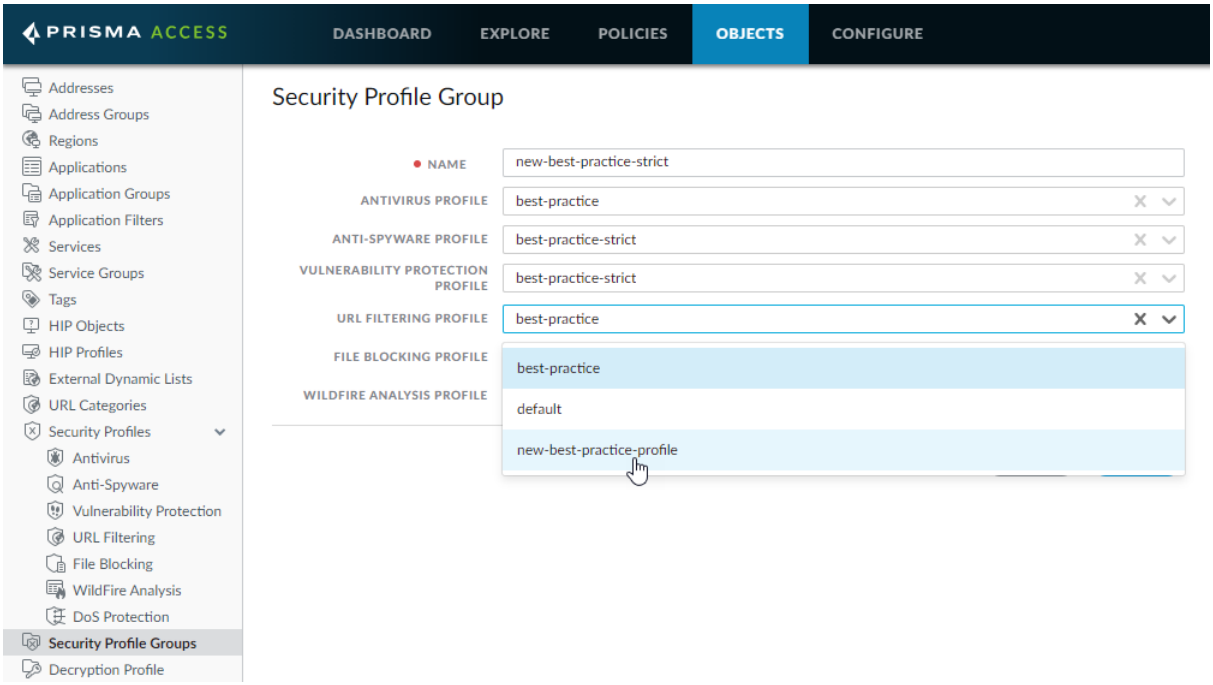
2. Select the cloned profile (named *best-practice-1* by default) and advance to the page with the gambling category and set **Site Access** and, optionally, **User Credential Submission**, to **Block** and then **Save** the new profile.



3. Select **Objects** > **Security Profile Groups**, select the **best-practice-strict** profile group, and **Clone** it.

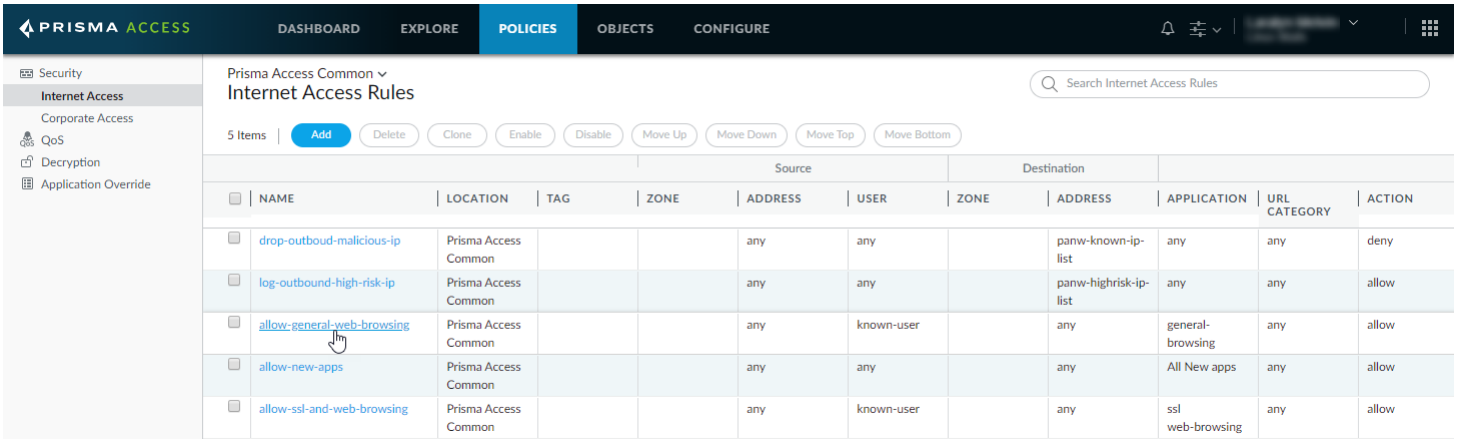


4. Swap out the default best-practice URL Filtering profile with your new profile and **Save** the new security profile group.



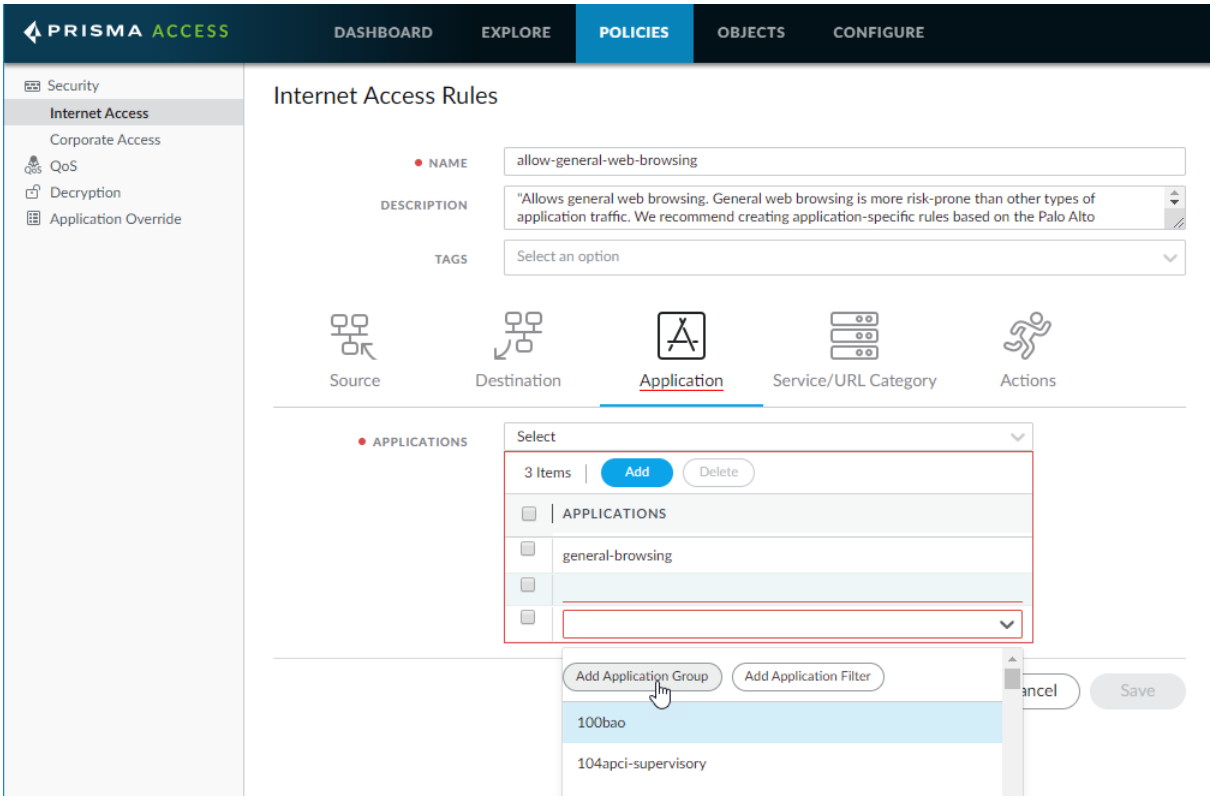
STEP 2 | Select a security policy rule to customize.

1. Select **Policies** > **Security** > **Internet Access**.
2. Click on the rule you want to customize.



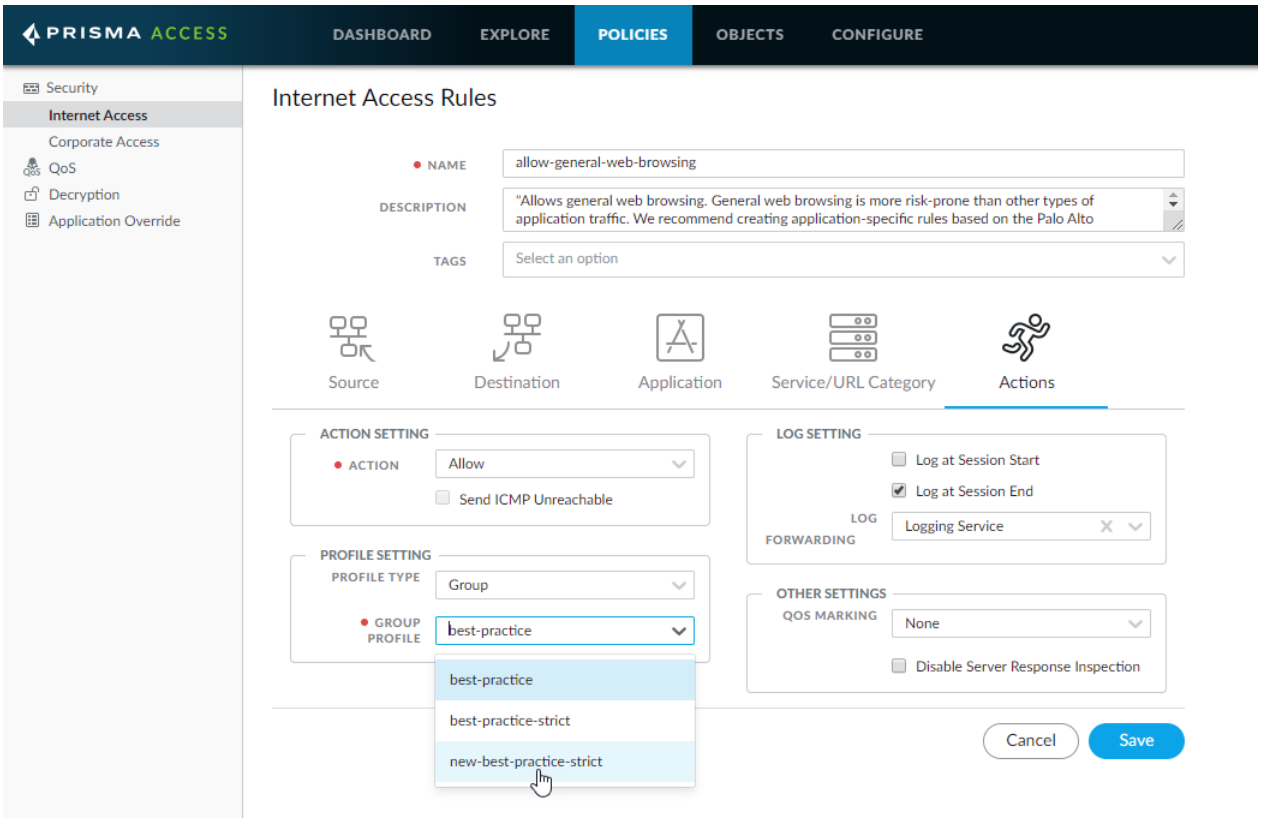
STEP 3 | Modify any of the fields in the security policy rule to meet your needs.

For example, if you wanted to specifically allow access to your sanctioned SaaS applications in the rule, you could **Add** the applications individually, or **Add Application Group**.



STEP 4 | If you modified any security profile objects, attach the new security profile group to the rule.

1. On the **Actions**, select the new security profile group you created as the **Group Profile**.

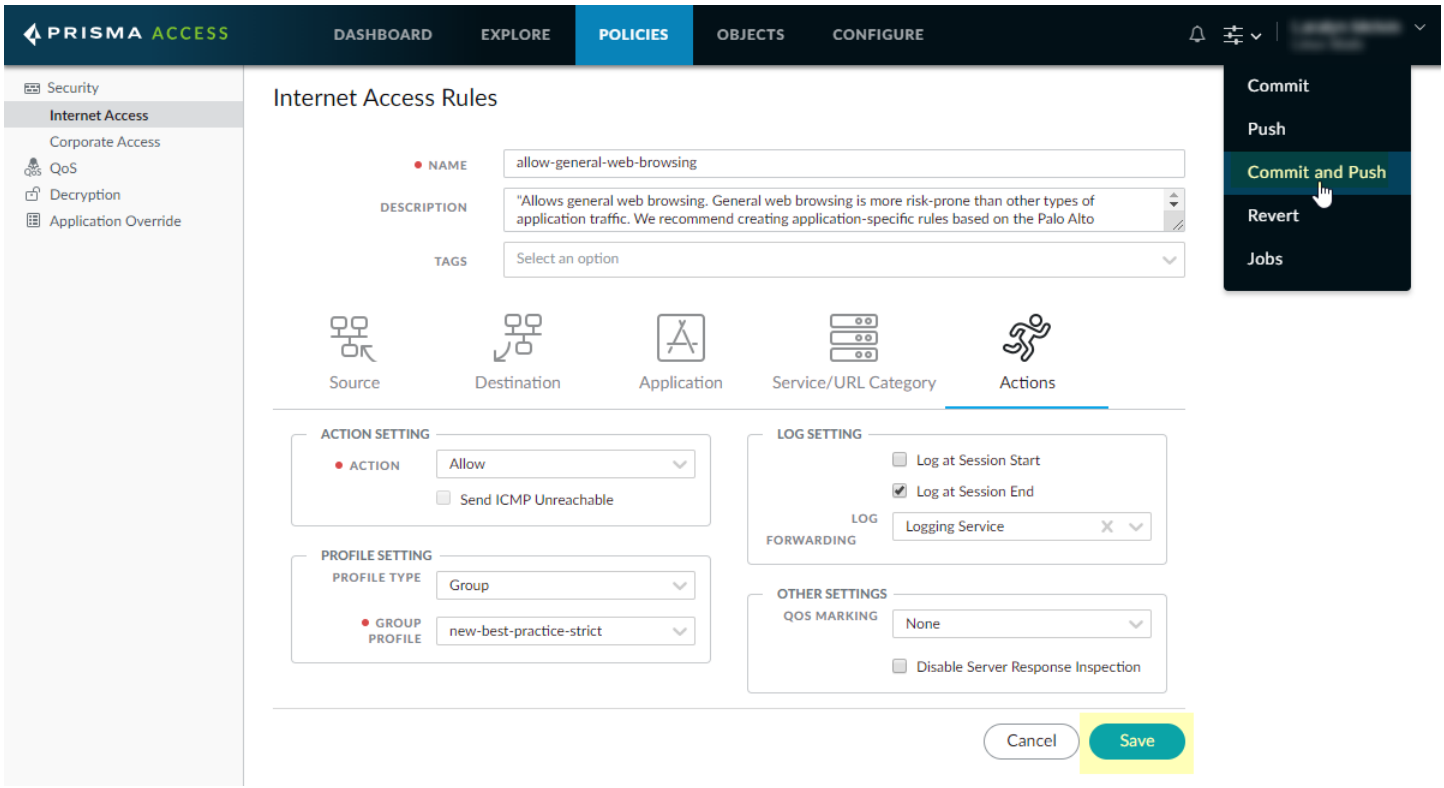


STEP 5 | Forward any logs triggered by the rule to the Cortex Data Lake (formerly Logging Service):

1. Decide whether you want to also **Log at Session Start**.

   By default, the internet access rules **Log at Session End** only.
2. Set **Log Forwarding** to **Logging Service**.

STEP 6 | **Save** the rule and **Commit and Push** your changes.



Create a Corporate Access Security Rule

Corporate access security rules allow you to block or allow traffic within your corporate network, and allows you to specify individual IP addresses or users in the source and destination.

For example, if you have critical IT management systems in your trust zone that you want only sanctioned IT administrators to access, you can create a corporate access security rule to allow access to those sanctioned IT administrators while restricting access to any other user within the network.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Select **Policies** > **Security** > **Corporate Access** and **Add** a new security rule.

STEP 3 | Enter a **Name** for the security rule.

STEP 4 | (Optional) Enter a **Description** of the policy rule.

STEP 5 | (Optional) Select one or more **Tags** to group the policy rule.

STEP 6 | Define the matching criteria for the traffic source.

1. In the **Source** tab, select a **Zone**. You can select **Trust**, **Clientless VPN**, or both.

2. Specify the **Source** IP address(es) within the selected source zone(s) to which the rule applies. Select **any** to apply the rule to all IP addresses in your trusted corporate network, or **Add** specific addresses to which the rule applies. You must Create an Address Object before you can add it as a source in a policy rule.

   Selecting the panw-bulletproof-ip-list as a Source IP address is not supported and results in a Push operation failure.
3. Specify **Users** within the selected source zone(s) and source IP addresses to which the rule applies. Select **any** to apply this to all configured admin roles, or **Add** specific admin roles.
4. Select one or more **HIP Profiles** to add to the security rule to enable the use of host information in policy enforcement. Select **any** to apply all configured HIP profiles to the rule, or **Add** specific HIP profiles to the rule. You must Create a HIP Profile before you can add it to a policy rule.

STEP 7 | Define the matching criteria for the traffic destination.

1. In the **Destination** tab, verify that the **Zone** selected is the **Trust** zone.
2. Specify the **Destination** IP address(es) within the selected destination zone to which the rule applies. Select **any** to apply the rule to all IP addresses on your corporate network, or **Add** specific IP addresses to which the rule applies. You must Create an Address Object before you can add it as a destination in a policy rule.

   Selecting the panw-bulletproof-ip-list as a Destination IP address is not supported and results in a Push operation failure.

STEP 8 | In the **Application** tab, **Add** one or more applications you want to block or allow. You can select multiple individual applications, or you can use application groups or application filters. You must Create Application Objects before you can add it as an application in a policy rule. By default, **any** is selected and applies the rule to all application traffic.

STEP 9 | Define the traffic match criteria based on the service used.

1. In the **Services/URL Category** tab, **Select** and **Add** the **Services** to match the policy rule to. By default, the policy rule is set to decrypt **any** traffic on TCP or UDP ports. You can **Add** a service or service group, and optionally set the rule to **application-default** to match to applications only on the application default ports. You must Create Service Objects before you can add them to a policy rule.
2. In the **Service/URL Category** tab, specify a **URL Category** as a match criteria for the rule. By default, the policy rule is set to **any**.

STEP 10 | Define what actions to take when traffic matches the security policy rule.

1. In the **Actions** tab, select the **Action** to take when traffic is matched to the security rule. Review the Security Policy Actions to determine the correct action to take.
2. Configure the Log Settings when traffic matches the security policy rule, and from the **Log Forwarding** drop-down select the **Logging Service**.

   Configuring the Log Settings is required in order to log traffic that matches the policy rule. The security processing node does not log any traffic matches if you do not configure the Log Forwarding to forward logs to the logging service.
3. To change the Quality of Service (QoS) settings on the packets matching the rule, select the **QoS Marking** setting from the drop-down and enter the QoS value in binary form or select a predefined value from the drop-down.

STEP 11 | Attach security profiles to enable the security processing node to scan all allowed traffic for threats.

In the **Actions** tab, select **Profiles** from the **Profiles Type** drop-down and attach the desired security profiles as needed. You must Create a Security Profile before you can attach it to a security rule.

STEP 12 | **Save** your configuration.

STEP 13 | Select **Commit** and **Commit and Push** your configuration changes.

Create a QoS Policy Rule

Quality of Service (QoS) policy rules to identify traffic that requires preferential treatment or bandwidth limiting. QoS rules allow you to enact policies on a network that ensure its ability to dependably run high-priority applications and traffic under limited network capacity. You can configure traffic QoS treatment using the following codepoints:

- **Expedited Forwarding (EF)**—Used to request low loss, low latency and guaranteed bandwidth for traffic. Packets with EF codepoint values are typically guaranteed highest priority delivery.
- **Assured Forwarding (AF)**—Used to provide reliable delivery for applications. PAckets with AF codepoints indicate a request for traffic to receive higher priority treatment than best effort service provides. Packets with EF codepoint take precedence over packets with AF codepoint.
- **Class Selector (CS)**—Used to provide backwards compatibility with network IP addresses that use the IP precedence field to mark priority traffic.
- **IP Precedence (ToS)**—Used by legacy network IP addresses to mark priority traffic.
- **Custom Codepoint**—Create a custom codepoint to match traffic by entering a **Codepoint Name** and **Binary Value**.

For example, you can create a QoS policy rule to prioritize voice communications, such as voice over IP (VOIP), to ensure consistent packet transmission. This ensures that voice communication are consistent.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Select **Policies** > **QoS** and **Add** a new QoS rule.

STEP 3 | Enter a **Name** for the QoS rule.

STEP 4 | (Optional) Enter a **Description** of the policy rule.

STEP 5 | (Optional) Select one or more **Tags** to group the policy rule.

STEP 6 | Define the QoS treatment the traffic receives based on DSCP value.

1. Select **DSCP/TOS** and select **Codepoints**.

   By default, Any is selected 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. If this satisifies your QoS requirements, continue to Step 7.

2. **Add** a new codepoint and Select the **Type** of DSCP/ToS codepoint marking for rule to match to traffic.
3. Specify the **Codepoint** value to match the QoS policy to traffic on a more granular level. For example, with **Assured Forwarding (AF)** selected, further specify the codepoint value such as **AF11**.

   When Expedited Forwarding (EF) is selected, a granular Codepoint value cannot be specified. The QoS policy rule matches to traffic marked with any EF codepoint value.

STEP 7 | Select **Class** and choose the QoS **Class** to determine the priority and bandwidth for traffic matching the policy rule.

STEP 8 | **Save** your configuration.

STEP 9 | Select **Commit** and **Commit and Push** your configuration changes.

Create a Decryption Policy Rule

Decryption policy rules allow you to define traffic to decrypt and the type of decryption you want to perform on the indicated traffic. Decryption policy rules are created when onboarding mobile users. These are best practice policies for decrypting non-financial, non-personal, and non-healthcare related traffic. You can perform the following types of decryption:

- **SSL Forward Proxy**—Use to decrypt and inspect SSL/TLS traffic from internal users to the web. This type of decryption prevents malware concealed as SSL encrypted traffic by decrypting traffic so that the security processing nodes can apply security policies to the traffic.
- **SSH Proxy**—Use to decrypt inbound and outbound SSH connections, and ensures attackers do not use SSH to tunnel unwanted applications and content.
- **Certificate**—Use a certificate you upload to decrypt inbound and outbound traffic.

For example, an attacker compromises a website that uses SSL encryption. Users visit that website and unknowingly download and exploit malware, that then uses the infected endpoint to move laterally through the network to compromise other system. Create an decryption policy using SSL Forward Proxy to decrypt and inspect the SSL traffic.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Select **Policies** > **Security** > **Decryption** and **Add** a new decryption rule or **Clone** the default best practice rules.

STEP 3 | Enter a **Name** for the decryption rule.

STEP 4 | (Optional) Enter a **Description** of the policy rule.

STEP 5 | (Optional) Select one or more **Tags** to group the policy rule.

STEP 6 | Define the matching criteria for the traffic source.

1. In the **Source** tab, select a **Zone**. You can select **Trust**, **Clientless VPN**, or both.
2. Specify the **Source** IP address(es) within the selected source zone(s) to which the rule applies. Select **any** to apply the rule to all IP addresses in your trusted corporate network, or **Add** specific IP addresses to which the rule applies. You must Create an Address Object before you can add it as a source in a policy rule.
3. Specify the **Users** within the selected source zone(s) and source IP addresses to which the rule applies. Select **any** to apply this to all configured admin roles, or **Add** specific admin roles.

STEP 7 | Define the matching criteria for the traffic destination.

1. In the **Destination** tab, select the **Zone** the traffic is intended for. You can select **Trust**, **Untrust**, or both.
2. Specify the **Destination** IP address(es) within the selected destination zone to which the rule applies. Select **any** to apply the rule to all IP addresses on your corporate network, or **Add** specific IP addresses to which the rule applies. You must Create an Address Object before you can add it as a destination in a policy rule.

STEP 8 | Define the traffic match criteria based on the service used.

1. In the **Services/URL Category** tab, **Add** the **Services** to match the policy rule to. By default, the policy rule is set to decrypt **any** traffic on TCP or UDP ports. You can **Add** a service or service group, and optionally set the rule to **application-default** to match to applications only on the application default ports. You must Create Service Objects before you can add them to a policy rule.
2. In the **Service/URL Category** tab, specify a **URL Category** as a match criteria for the rule. By default, the policy rule is set to **any**.

STEP 9 | Configure the rule to either decrypt matching traffic or to exclude traffic from decryption.

1. In the **Options** tab, select the **Action** the security processing node takes on matching traffic.
2. Select the **Type** of decryption the security processing node performs on matching traffic.
3. Add a Decryption Profile to block and control what traffic is decrypted.

STEP 10 | **Save** your configuration.

STEP 11 | Select **Commit** and **Commit and Push** your configuration changes.

Create an Application Override Policy Rule

Create an application override policy to designate applications be processed using fast path Layer-4 inspection instead of using the App-ID for Layer-7 inspection. This forces the security enforcement node to handle the session as a regular stateful inspection and saves application processing times.

You can create an application override policy rule when you do not want traffic inspection for custom applications between known IP addresses. For example, if you have a custom application on a non-standard port that you know users accessing the application are sanctioned, and both are in the Trust zone, you can override the application inspection requirements. for the trusted users accessing the custom application.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Select **Policies** > **Security** > **Application Override** and **Add** a new application override rule.

STEP 3 | Enter a **Name** for the application override rule.

STEP 4 | (Optional) Enter a **Description** of the policy rule.

STEP 5 | (Optional) Select one or more **Tags** to group the policy rule.

STEP 6 | Define the matching criteria for the traffic source.

1. In the **Source** tab, select a **Zone**. You can select **Trust**, **Clientless VPN**, or both.
2. Specify the **Source** IP address(es) within the selected source zone(s) to which the rule applies. Select **any** to apply the rule to all IP addresses in your trusted corporate network, or **Add** specific IP addresses to which the rule applies. You must Create an Address Object before you can add it as a source in a policy rule.

STEP 7 | Define the matching criteria for the traffic destination.

1. In the **Destination** tab, select the **Zone** the traffic is intended for. You can select **Trust**, **Untrust**, or both.
2. Specify the **Destination** IP address(es) within the selected destination zone to which the rule applies. Select **any** to apply the rule to all IP addresses on your corporate network, or **Add** specific IP addresses to which the rule applies. You must Create an Address Object before you can add it as a destination in a policy rule.

STEP 8 | Define the protocol and applications to override.

1. In the **Protocol/Application** tab, select the **Protocol** used by the application.
2. Enter the **Port** number or range used for communication with the application.
3. Select the **Application** to override.

STEP 9 | **Save** your configuration.

STEP 10 | Select **Commit** and **Commit and Push** your configuration changes.

Administer Prisma Access

Administering Prisma Access is a combination of managing the configurations for your mobile users, remote networks, service connections, and policy as well as monitoring the status of the service and understanding when changes in the service impact your deployment.

- Launch Prisma Access Cloud Management
- Commit, Push, and Revert Prisma Access Configuration Changes
- View the Prisma Access Jobs
- Monitor Prisma Access
- Prisma Access Shared Management Model
- Release Cadence for Prisma Access Infrastructure Updates
- Check the Status of Prisma Access

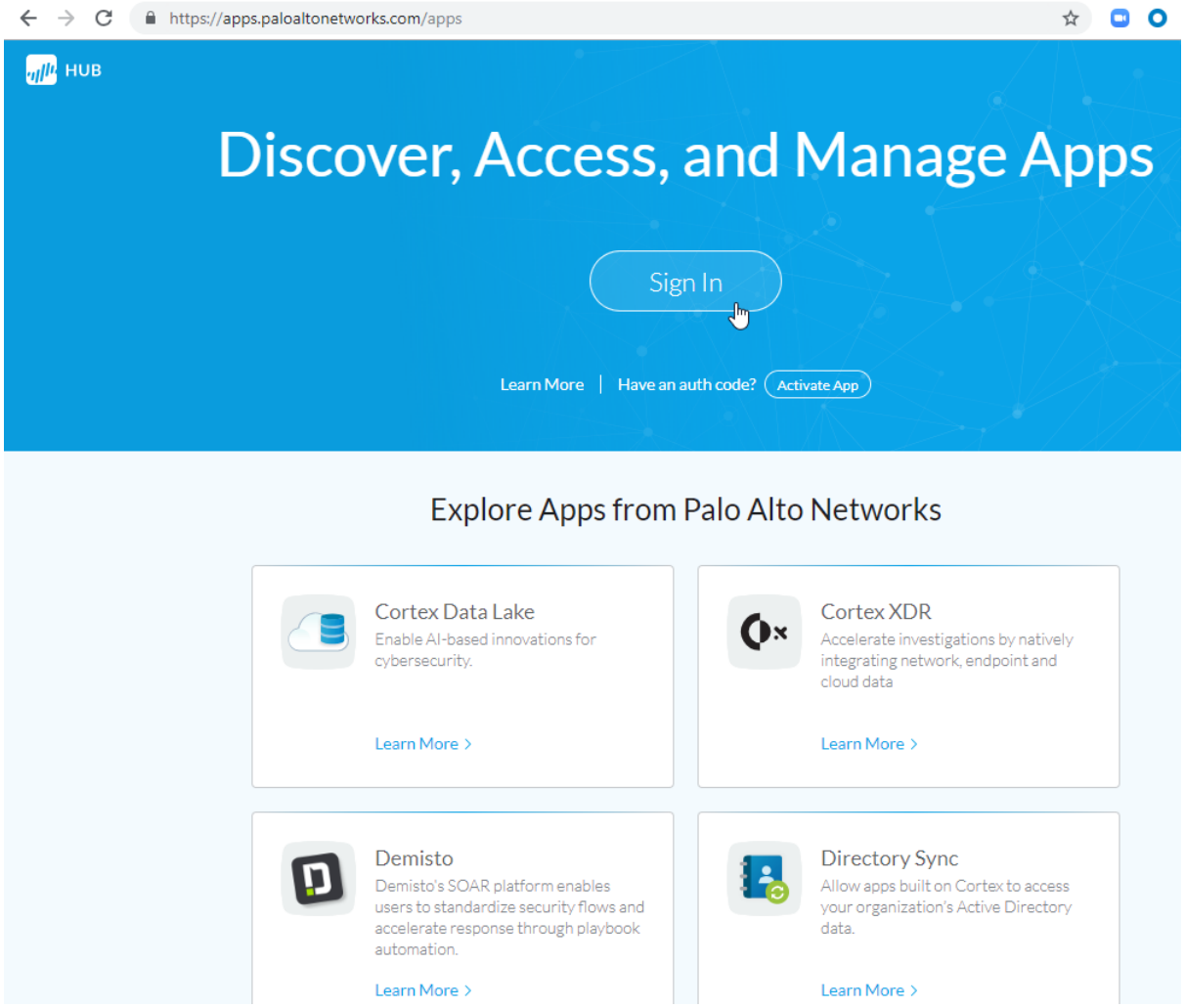
Launch Prisma Access Cloud Management

The following web browsers are supported for access to Prisma Access (Cloud Managed):

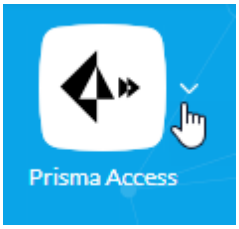
- Internet Explorer 11+
- Firefox 3.6+
- Safari 5+
- Chrome 11+

Perform the following tasks to launch Prisma Access cloud management.

STEP 1 | Launch an internet browser and **Sign In** to the hub.



STEP 2 | Launch the Prisma Access app.



Commit, Push, and Revert Prisma Access Configuration Changes

After you make configuration changes and are ready to apply them to your security processing nodes, you need to commit and push the configuration. Based on the administrative privileges allotted to your admin role, you can commit and push all pending configuration changes made by all admins, or just configuration changes you made.

Prisma Access queues commit and push requests so that you can initiate a new commit while a previous commit is taking place. Commits and pushes are performed in the order they are initiated. When you initiate a commit, the security processing node checks the validity of the changes before activating them.

- Commit All Configuration Changes
- Commit Your Own Configuration Changes
- Revert Prisma Access Configuration

Commit All Configuration Changes

Admin roles with sufficient privileges may commit all pending configuration changes made by any administrator on Prisma Access.

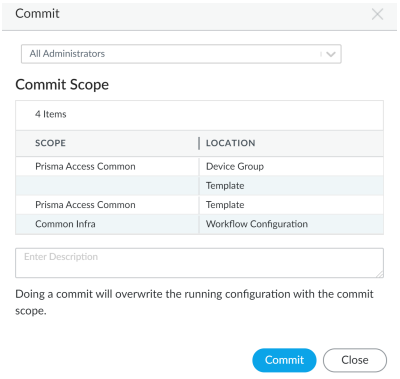
STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Select **Commit** (▭) and **Commit** your configuration changes.

STEP 3 | Select **All Administrators** to commit all pending configuration changes made by all Prisma Access admins.

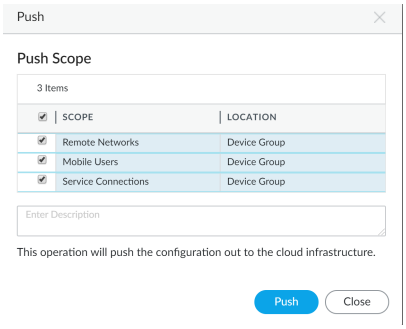
STEP 4 | (Optional) Enter a commit description to describe the purpose of the configuration changes for audit purposes.

STEP 5 | **Commit** the configuration changes.



STEP 6 | Select **Commit** (▭) and **Push** your configuration changes.

STEP 7 | Select the committed policies or objects, and **Push** the configuration changes



Commit Your Own Configuration Changes

You have the option to only commit your own configuration changes only. Doing this allows you to only commit those changes that you know are complete, and avoids potential disruption of service in the event a different admin user is not ready to apply their configuration changes to the security processing node.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Select **Commit** (▬) and **Commit** your configuration changes.

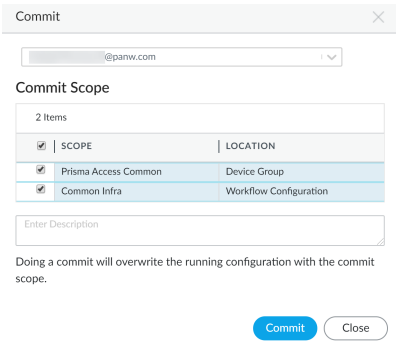
STEP 3 | Select **<Admin Email>** to Commit only the pending configuration changes made by the logged in admin.

STEP 4 | Select and verify the changes that the commit enacts.

This is useful to validate that all the intended configuration changes are applied, and to identify any changes that should not be committed.

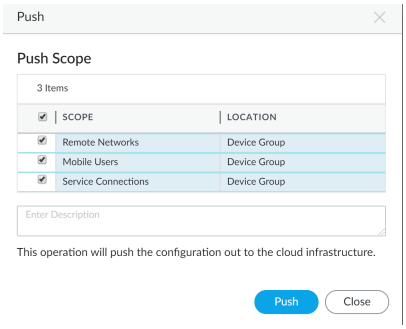
STEP 5 | (Optional) Enter a commit description to describe the purpose of the configuration changes for audit purposes.

STEP 6 | **Commit** the configuration changes.



STEP 7 | Select **Commit** (▬) and **Push** your configuration changes.

STEP 8 | Select the committed policies or objects, and **Push** the configuration changes



Revert Prisma Access Configuration

In the event a Prisma Access configuration was commit in error, or a configuration change was pushed that caused network or security disruption, you have the ability to revert the Prisma Access configuration to the most recent running Prisma Access configuration. This allows you to revert the Prisma Access configuration back to a running configuration you know is functional and does not compromise your network security. You do not have the option to select a specific running configuration. Prisma Access automatically selects the last known running configuration and reverts to it.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Click **Commit** () and **Revert** the Prisma Access configuration.

STEP 3 | **Revert** the running configuration if you are certain the Prisma Access configuration must be reverted to the last running configuration. You are prompted to verify whether to revert the running configuration.

View the Prisma Access Jobs

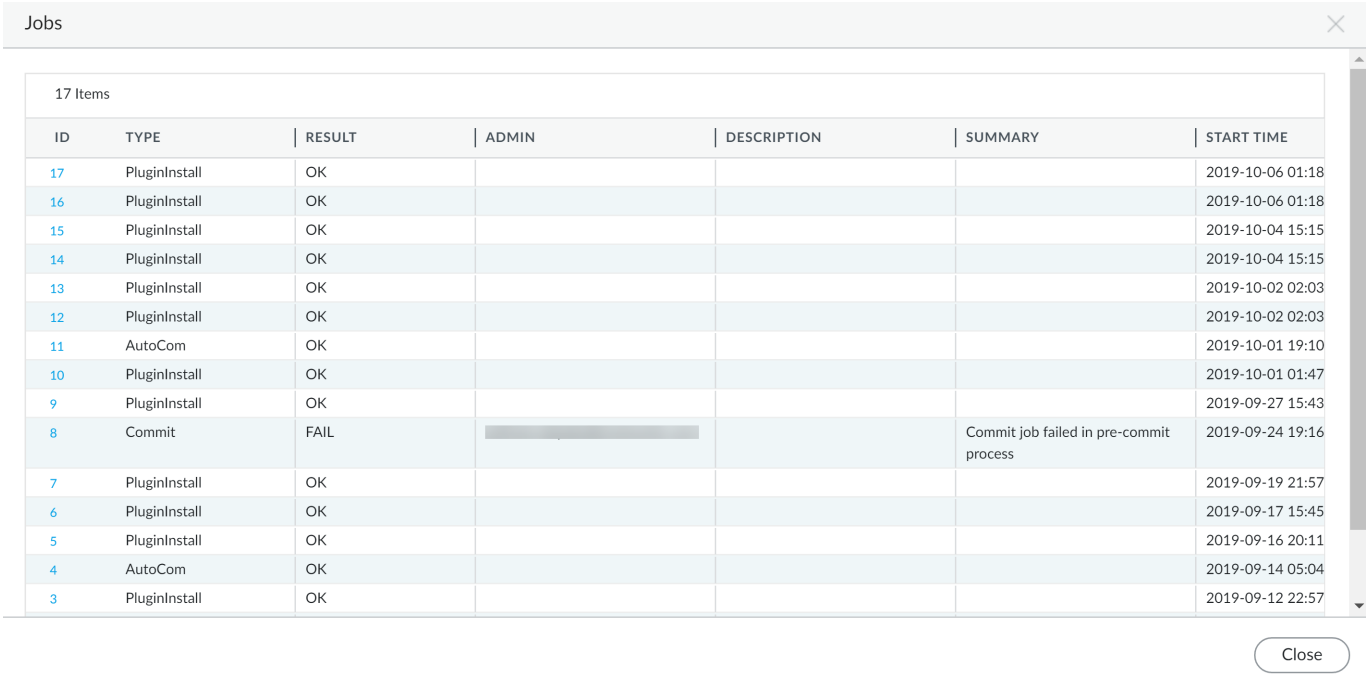
You can view the **Jobs** history on Prisma Access to display details about operations that admins initiated, as well as automatic content and license updates. This includes any configuration commits, pushes and reverts. You can use the Jobs view to troubleshoot failed operations, investigate warnings associated with completed commits, or cancel pending commits.

STEP 1 | Launch Prisma Access Cloud Management.

STEP 2 | Click **Commit** ( ) and view the Prisma Access **Jobs**.

STEP 3 | Perform any of the following tasks:

- **Investigate warnings or failures**—Read the entries in the Summary column for warning or failure details.
- **View a commit description**—If an administrator entered a commit description, you can refer to the Description column to understand the purpose of the commit.
- **Check the position of an operation in the queue**—View the operation position and status to determine the position of the operation.



Monitor Prisma Access

Prisma Access provides built-in visibility into your Prisma Access environment from the **Explore** tab. Explore provides different views into system and configuration events as well as into your Prisma Access user traffic and SaaS application usage.

- View Prisma Access Logs
- Monitor Prisma Access Network Activity
- Monitor SaaS Application Usage

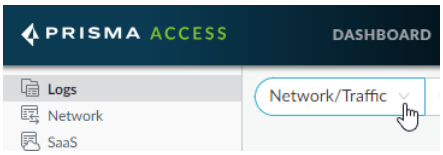
View Prisma Access Logs

A log is an automatically generated, time-stamped file that provides an audit trail for system events or network traffic events that Prisma Access monitors. Log entries contain artifacts, which are properties, activities, or behaviors associated with the logged event, such as the application type or the IP address of an attacker. Each log type records information for a separate event type. For example, Prisma Access may generate a Threat log to record traffic that matches a spyware, vulnerability, or virus signature.

Prisma Access provides Network logs (Traffic, Threat, URL, File, HIP Match) and Common logs (System and Configuration).

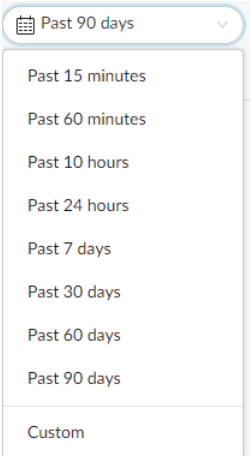
STEP 1 | Select **Explore** > **Logs**.

STEP 2 | Select the type of log you want to view:

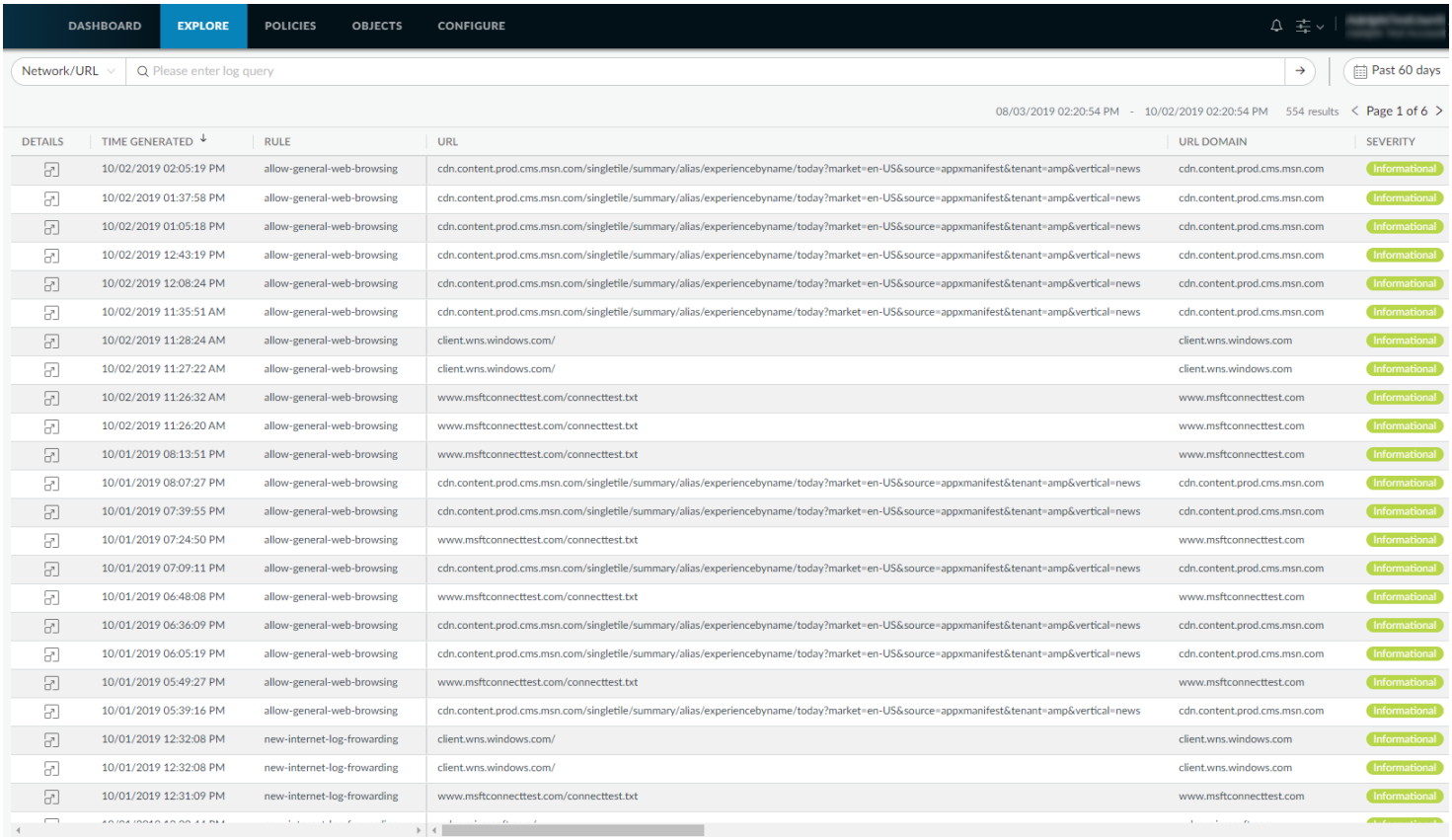


Prisma Access supports Network logs (Traffic, Threat, URL, File, HIP Match) and Common logs (System and Configuration).

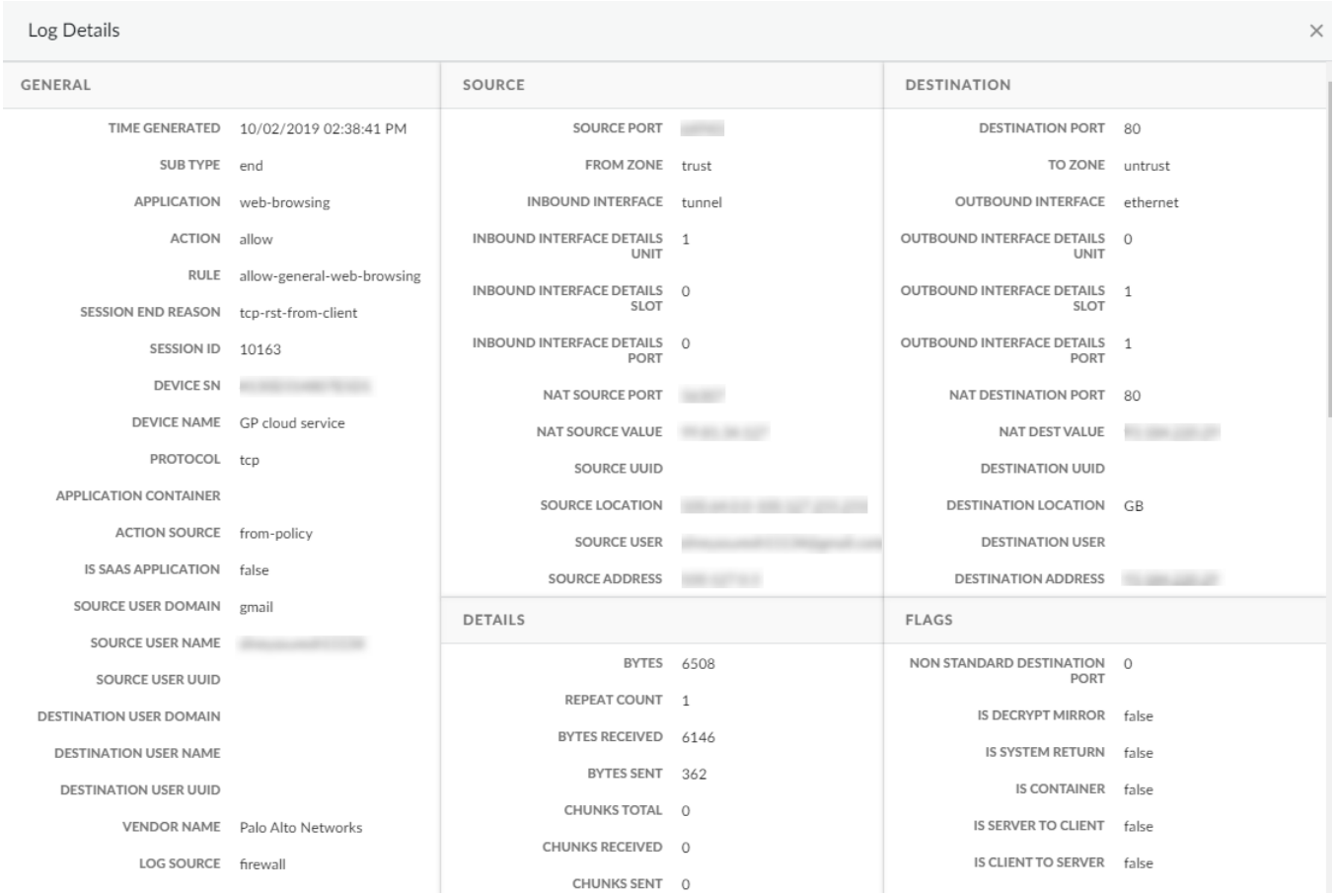
STEP 3 | Select the time range for which you want to view logs.



Selecting a time range starts the query and a list of logs that match the selected log type during the selected time range display.



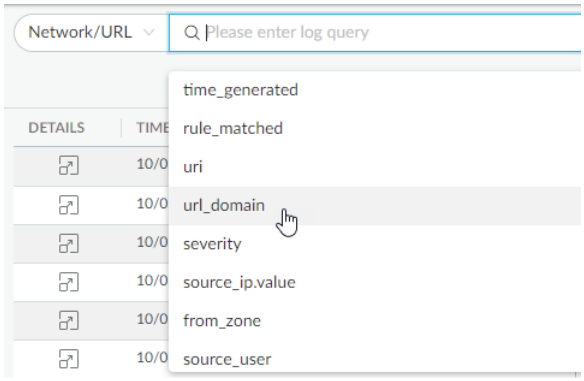
STEP 4 | To view more detail about a specific log, click the details icon.



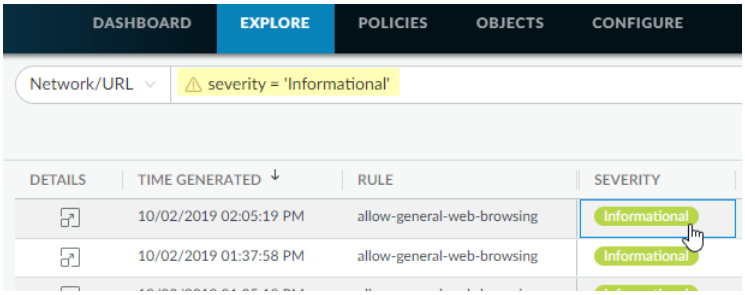
STEP 5 | (optional) Provide a query string to narrow down the list of logs.

If you do not provide a query string, Explore will retrieve every log record of the type you specify that was created during the time range that you provide — up to 65,536 records.

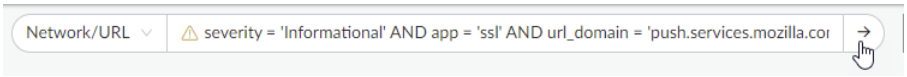
- Click into the query field to see the list of available field names



- Click into an individual cell to add the field and value to the query.



- Continue adding filtering criteria and then submit your query to see the matching set of logs.



STEP 6 | (Optional) **Export** the current list of logs to a .CSV file.

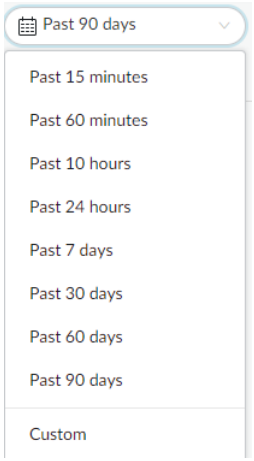
For more information on how to use Explore to

Monitor Prisma Access Network Activity

The Prisma Access **Explore** > **Network** page provides a graphical view into your mobile user and branch network activity based on Traffic, Threat, URL Filtering, and File log data. Use the widgets on this screen to interact with and visualize network usage patterns, traffic patterns, and suspicious activity and anomalies.

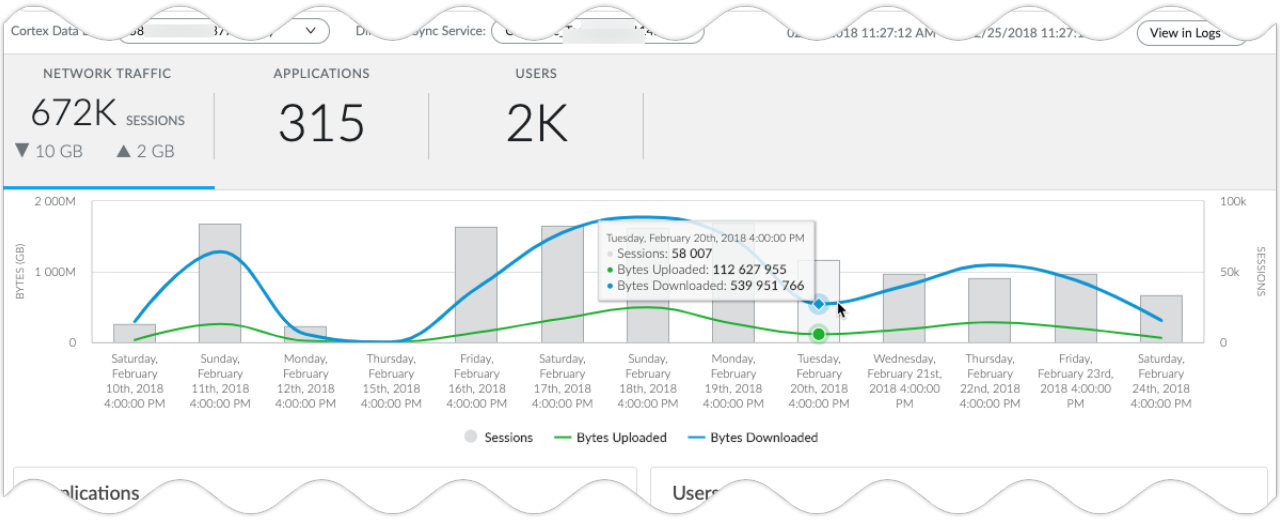
The top of the Network page provides three graphs that you can use to examine your network usage: Network Traffic, Applications, and Users. Beneath the graph, you will find a series of widgets designed to help you quickly understand how your network is being used. For example, the Applications widget displays the top ten applications your Prisma Access users are accessing. The Threats widget shows the threats—viruses, spyware, vulnerability exploits—that Prisma Access has prevented.

- Select the time range for which you want to view network activity.



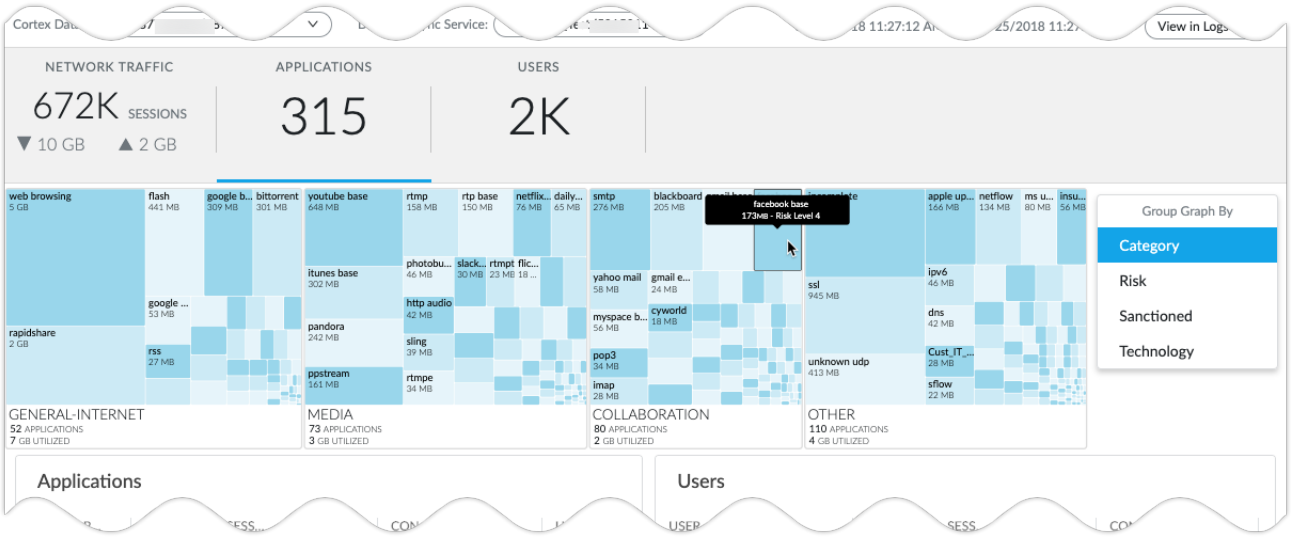
- Select **Network Traffic** to see a graph showing the total number of sessions, outbound and inbound traffic volume for the selected time frame (this is the default view).

  Hover over a specific point in the graph to see metrics for that particular point in time.

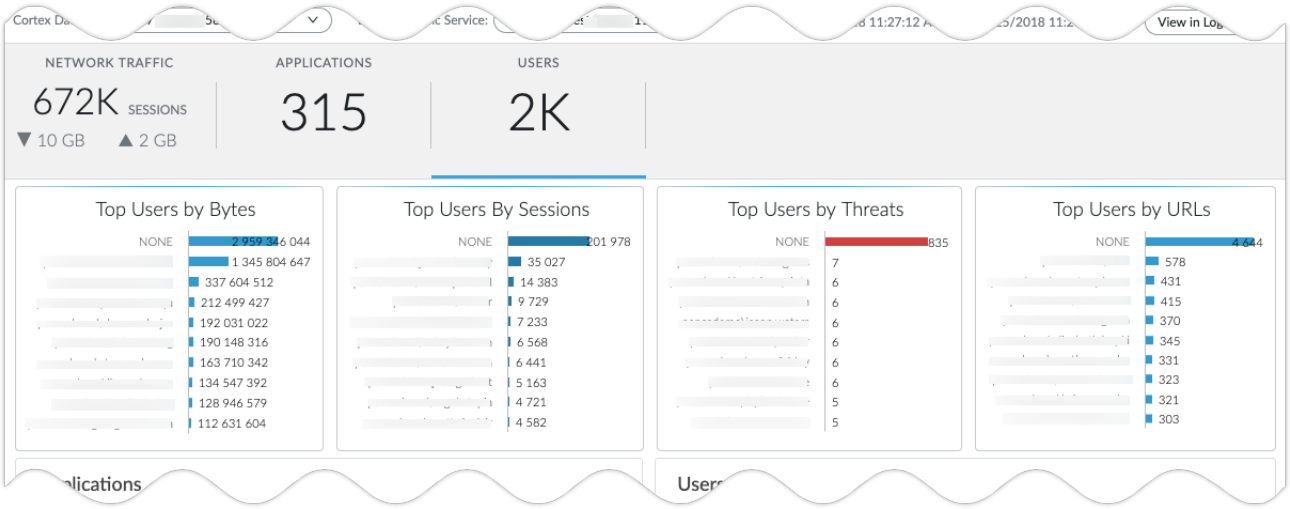


- Select **Applications** to see a graph showing what applications Prisma Access users were using during the time range that you specified.

  You can group applications in the graph by category (General-Internet, Media, Collaboration, or Other), risk (levels 1 -5, plus applications with an undefined risk level), sanctioned (whether the application has been explicitly allowed for use), or technology (Browser-based, Client-Server, and Other). Hover over a specific application in the graph to see its risk level, as well as how much data it has transferred over your network over the time frame you are examining.



- Select **Users** to see a graph showing the top ten most active Prisma Access users during the selected time range, and the amount of traffic that they transferred. User **NONE** represents traffic that cannot be matched to a specific user.



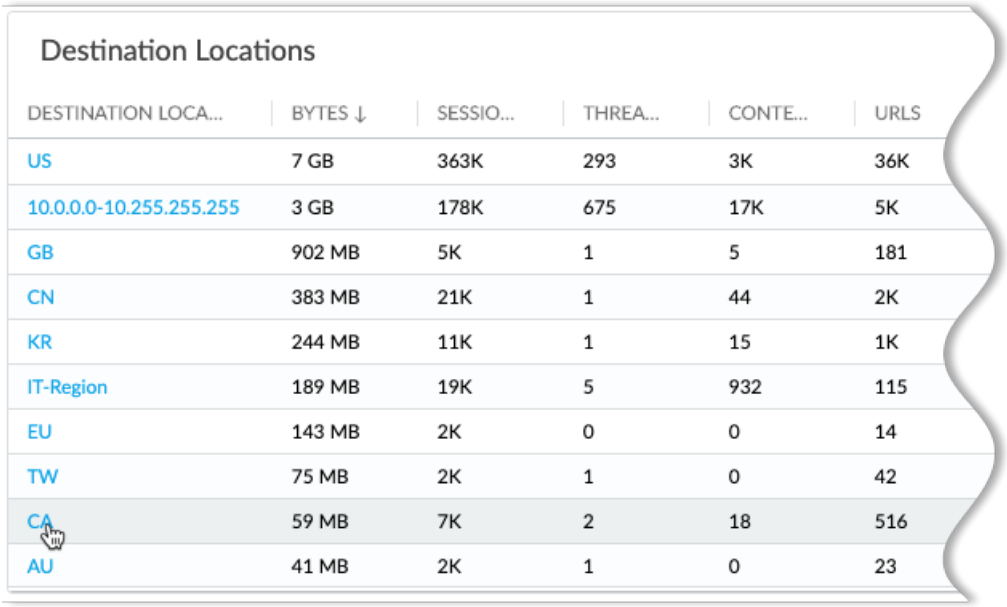
- Use the widgets to monitor network events and trends during the selected time range.

Widget	Description
Applications	Displays the top ten applications in use. Use this widget to monitor top application usage sorted on risk, bytes, sessions, threats, content (files and patterns), URLs visited, and number of users.
Users	Displays the top ten most active users who have generated the largest volume of traffic and consumed network resources to obtain content. Use this widget to monitor top users sorted on bytes, sessions, threats, content (files and patterns), and URLs visited.
Source IPs	Displays the top ten IP addresses or host names of the devices that have initiated activity. Use this widget to monitor top source IPs sorted on bytes, sessions, threats, content (files and patterns), and URLs visited.
Destination IPs	Displays the IP addresses or host names of the top ten destinations that were accessed by users. Use this widget to monitor top destination IPs sorted on bytes, sessions, threats, content (files and patterns), and URLs visited.
Source Locations	Displays the top ten locations around the world from where users initiated network activity. Use this widget to monitor top locations sorted on bytes, sessions, threats, content (files and patterns), and URLs visited.
Destination Locations	Displays the top ten destination locations around the world from where your users are accessing content. Use this widget to monitor top locations sorted on bytes, sessions, threats, content (files and patterns), and URLs visited.
Rules	Displays the top ten policy rules that have allowed the most traffic. Use this widget to view the most commonly used rules, monitor the usage patterns, and to assess whether the rules are effective in securing access. Metrics are provided for bytes, sessions, threats, content (files and patterns), and URLs visited.

Widget	Description
Threats	Displays the threats seen in your users' traffic. This information is based on signature matches in Anti-virus, Anti-Spyware, and Vulnerability Protection profiles and viruses reported by WildFire.
WildFire Submissions	Displays the applications that generated the most WildFire submissions. This widget uses the malicious and benign verdict from the WildFire submissions log.
Files	Displays the files and data that Prisma Access blocked due matches to a File Blocking security profile or a Data Filtering security profile in a security policy rule.
URL Filtering	Displays the URLs that Prisma Access blocked on based on criteria defined in a URL Filtering security profile attached to a security policy rule.

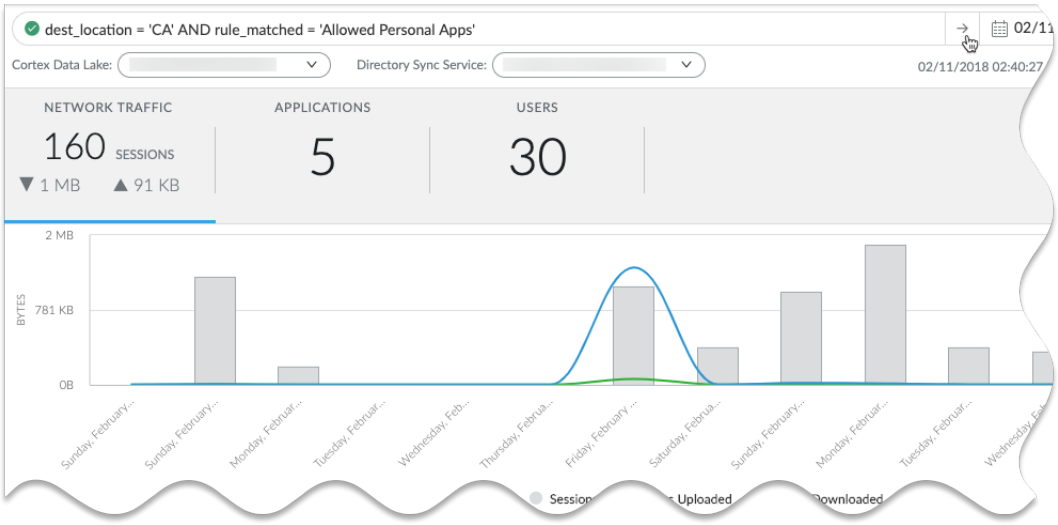
- Filter the data to focus on a particular segment of network activity.

  You can click on the left-most links in the widgets to help you build your query. For example, if you click on a destination in the **Destination Locations** widget:



  then the appropriate location is added to the filter field:

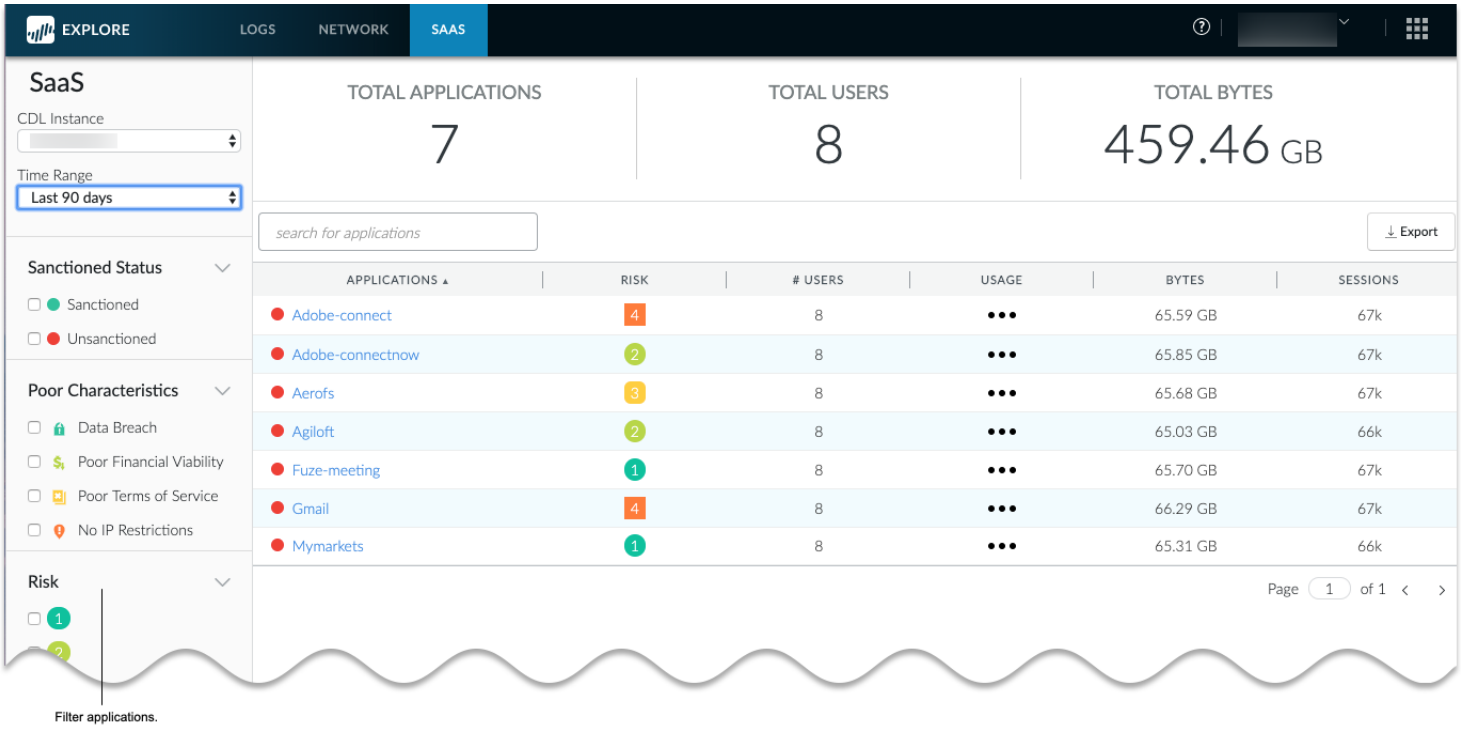
  Clicking additional links in the widgets adds them to the filter using a Boolean AND. When you're done adding filters, click → to submit the query. Your graphs and widgets will refresh using the filtered data.



Monitor SaaS Application Usage

You can monitor the SaaS application usage of your Prisma Access users from the **Explore** > **SaaS** tab. You can also

If an app is a container app, then the displayed statistics are a roll-up of all the applications in the container. For example, gmail is a container app (there is no app-id for gmail). It groups applications such as gmail-posting, gmail-downloading, gmail-uploading, and so forth. The risk score set for this container app is the highest risk score found for the contained applications. All other metrics are calculated by summing the values found for the contained applications.

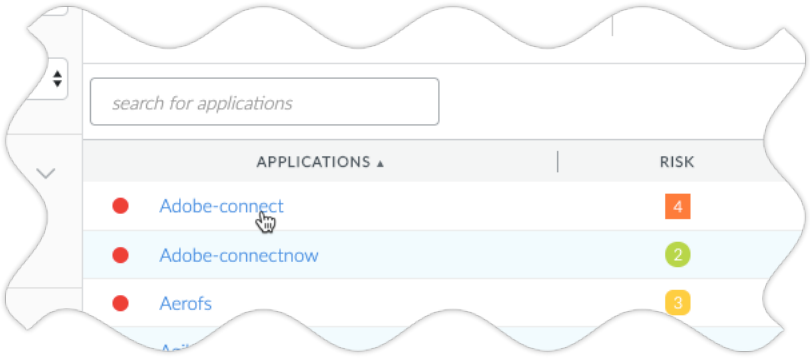


- Set the **Time Range** for which to use SaaS application usage data.

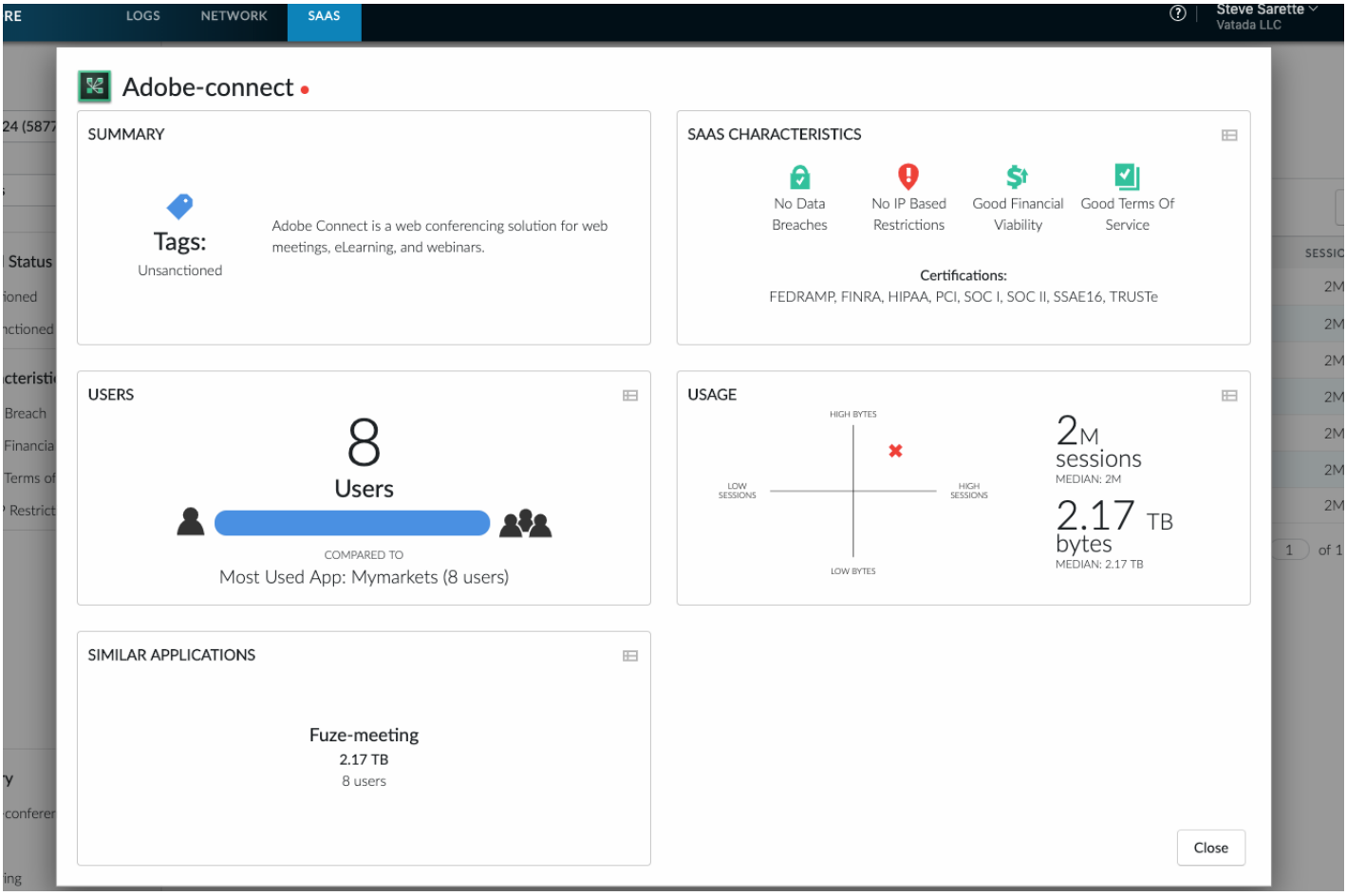
  You can view usage information based on a time range of the past 7, 30, and 90 days.

- Filter SaaS data by clicking on an attribute in the left-hand pane.

- Get additional information about an application by clicking on its name in the Applications column.



The details display in a pop-up window.



Prisma Access Shared Management Model

With Prisma Access you can ensure consistent security across all of your geographic locations and your expanding mobile workforce without the operational overhead of having to deploy equipment and manage it all over the world. However, only you know how to best secure your users and your most valuable resources and sensitive applications. To enable you to have full control over your security policy without the responsibility of deploying and maintaining the infrastructure, Prisma Access employs a shared management model. The following table defines the shared management ownership responsibilities:

Management of...	Palo Alto Networks Responsibility	Your Responsibility
Cortex Data Lake	Maintaining the logging infrastructure and delivery of Prisma Access logs.	Purchasing the appropriate amount of log storage.
OS Updates in the Prisma Access Infrastructure	Upgrading all security processing nodes in your Prisma Access instance.	
Content Updates	Keeping all security processing nodes in your Prisma Access instance up-to-date with the latest content updates.	Reviewing the content release notes and understanding how new or updated App-IDs impact your policy.
Users	Deploying security processing nodes in the selected locations.	Onboarding mobile users and providing mobile device connectivity to the user gateways (for example, providing an ISP).
User Authentication		Configuring enterprise authentication.
Mobile Device Management (MDM)		(Optional) Managing mobile user devices with your own MDM.
Fault Tolerance	Guaranteeing the availability of the service in all locations.	
Auto Scaling	Automatically scaling the service whenever you add service connections or branch networks (or add bandwidth at a branch), or when needed to support the number of mobile users in a given region and location.	
Provisioning	Provisioning security processing nodes as needed to support your licensed Prisma Access services.	

Management of...	Palo Alto Networks Responsibility	Your Responsibility
Policy Management and Creation	(Cloud Managed only) Creating best practice internet access security policy rules and security profiles.	Creating granular security policy and policy objects.
Log Analysis and Forensics	Generating logs.	Analyzing logs, running reports, configuring log forwarding, and integrating with other log analysis tools.
On-premise Security		Securing between micro-segmentations of your on-premise network. In some deployments, you can also direct all traffic to Prisma Access to secure it.
Networking	Establishing full-mesh networking within the Prisma Access infrastructure, as well as secure internet access.	Providing an IPSec-capable device at each branch and corporate network you plan to connect to Prisma Access.
Monitoring	Monitoring all of the networking infrastructure within Prisma Access and providing status information.	Monitoring all on-premise networking devices connected to Prisma Access.
Remote Network Onboarding	Deploying the Prisma Access networking infrastructure to support the remote network.	Onboarding each remote network that you want Prisma Access to secure.
Corporate Access	Deploying the network infrastructure within Prisma Access to enable branch and mobile user access to your corporate network.	Onboarding the service connection to your corporate and data center locations and managing the IPSec-capable device at each location.
IP Address Pools	Deploying the Prisma Access infrastructure within the provided IP address space.	Providing IP address pools for the service infrastructure, the branch locations, and/or your mobile users.
Panorama Updates (Panorama managed only)		Upgrading Panorama to a version that supports the Cloud Services plugin.
Cloud Services Plugin Updates (Panorama managed only)	Informing you when a new version of the plugin is available.	Upgrading to the required version of the Cloud Services plugin.

Release Cadence for Prisma Access Infrastructure Updates

The following table describes how Prisma Access updates its infrastructure components, including content and software updates. This table also indicates whether Prisma Access automatically updates the software. If any updates are not automatic, you can learn how to apply those infrastructure updates.

You can also check the status of all cloud services from the Hub.

Component	Update Schedule	Comments
GlobalProtect app	• **Major GlobalProtect App Releases (for example, *x*.0 or 4.*x*)**—Prisma Access updates the app 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 app release of 4.0, Prisma Access updates the app 7-10 days after the 4.0.1 release. • **Minor GlobalProtect App Releases (for example, 4.1.*x*)**—Prisma Access updates the app with the latest minor release 7-10 days after the general availability of that release.	The cloud controls the version of the app that is available for upgrade.
PAN-OS software upgrades in the Prisma Access infrastructure—scheduled	Palo Alto Networks® upgrades the PAN-OS infrastructure when a new version of Prisma Access is released. Palo Alto Networks® provide you with three weeks' notice before a scheduled upgrade.	Sign up to receive infrastructure upgrades by email or text notifications at the Hub.
PAN-OS software upgrades in the Prisma Access infrastructure—unscheduled	For unscheduled upgrades (for example, an emergency hotfix for zero-day threats), Palo Alto Networks® makes every effort to give you 48 hours' notice before the upgrade. However, Prisma Access may occasionally upgrade its infrastructure with shorter notice.	Sign up to receive infrastructure upgrades by email or text notifications at the Hub.
Applications and threat updates	Daily with a threshold of 24 hours. Palo Alto Networks® releases 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.	Palo Alto Networks® provides an update through the Hub 48 hours prior to a cloud upgrade, and 24 hours prior to the release of a new App-ID version.
Antivirus protection	Every hour, 10 minutes after the hour	Prisma Access is always up-to-date with the latest Antivirus release.

Component	Update Schedule	Comments
WildFire	Every 15 minutes	Prisma Access is always up-to-date with the latest WildFire release.
GlobalProtect Data File	Every hour	Prisma Access is always up-to-date with the latest GlobalProtect data file release.
Clientless VPN application signatures	Every hour	Prisma Access is always up-to-date with the latest Clientless VPN application signature release.

Check the Status of Prisma Access

You can retrieve the status of all cloud services, including Prisma Access and Cortex Data Lake, and a historical record of the service uptime by accessing the app instance from the hub.

You can also sign up for email or text message notifications so that you are notified when infrastructure updates are planned; when updates occur; and when Palo Alto Networks® creates, updates, or resolves an incident. To sign up for email updates, go to the Resources section of the hub home page and then select **Service Status**. You can then **Subscribe** to specific updates and incidents for your cloud services.