paloalto TECHDOCS

GlobalProtect Administrator's Guide

Version 10.1

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

February 22, 2022

Table of Contents

GlobalProtect Overview

Whether checking email from home or updating corporate documents from an airport, the majority of today's employees work outside the physical corporate boundaries. This workforce mobility increases productivity and flexibility while simultaneously introducing significant security risks. Every time users leave the building with their laptops or smart phones, they are bypassing the corporate firewall and associated policies that are designed to protect both the user and the network. GlobalProtect™ solves the security challenges introduced by roaming users by extending the same next-generation firewall-based policies that are enforced within the physical perimeter to all users, no matter where they are located.

The following sections provide conceptual information about the Palo Alto Networks GlobalProtect offering and describe the components and various deployment scenarios for GlobalProtect:

- About the GlobalProtect Components
- What OS Versions are Supported with GlobalProtect?
- What Features Does GlobalProtect Support?
- About GlobalProtect Licenses

About the GlobalProtect Components

GlobalProtect provides a complete infrastructure for managing your mobile workforce to enable secure access for all your users, regardless of what endpoints they are using or where they are located. This infrastructure includes the following components:

- GlobalProtect Portal
- GlobalProtect Gateways
- GlobalProtect App

GlobalProtect Portal

The GlobalProtect portal provides the management functions for your GlobalProtect infrastructure. Every endpoint that participates in the GlobalProtect network receives configuration information from the portal, including information about available gateways as well as any client certificates that may be required to connect to the GlobalProtect gateway(s). In addition, the portal controls the behavior and distribution of the GlobalProtect app software to both macOS and Windows endpoints (on mobile endpoints, the GlobalProtect app is distributed through the Apple App Store for iOS endpoints, Google Play for Android endpoints and Chromebooks, and the Microsoft Store for Windows 10 UWP endpoints). If you are using the Host InformationProfile (HIP) feature, the portal also defines what information to collect from the host, including any custom information you require. You can Set Up Access to the GlobalProtect Portal on an interface on any Palo Alto Networks next-generation firewall.

GlobalProtect Gateways

GlobalProtect gateways provide security enforcement for traffic from GlobalProtect apps. Additionally, if the HIP feature is enabled, the gateway generates a HIP report from the raw host data the apps submit and can use this information in policy enforcement. You can configure different GlobalProtect Gateways to provide security enforcement and/or virtual private network (VPN) access for your remote users, or to apply security policy for access to internal resources.

You can Configure a GlobalProtect Gateway on an interface on any Palo Alto Networks next-generation firewall. You can run both a gateway and a portal on the same firewall, or you can have multiple distributed gateways throughout your enterprise.

GlobalProtect App

The GlobalProtect app software runs on endpoints and enables access to your network resources through the GlobalProtect portals and gateways that you have deployed.

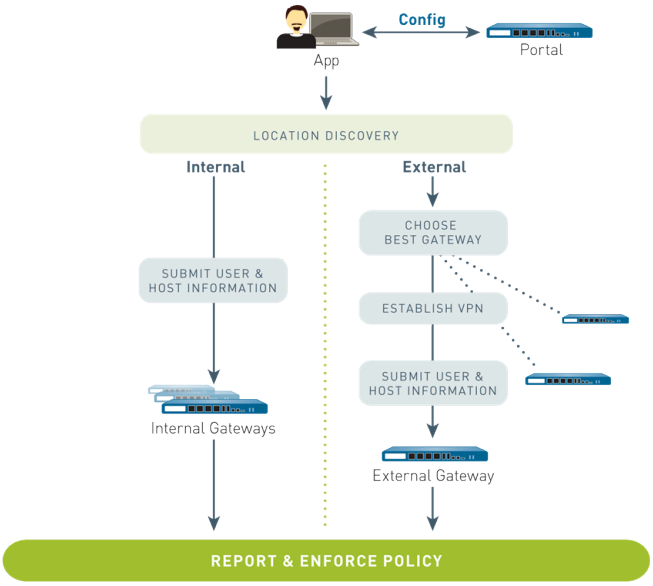
The GlobalProtect app for Windows and macOS endpoints is deployed from the GlobalProtect portal. You can configure the behavior of the app—for example, which tabs the users can see—in the client configuration(s) that you define on the portal. See Define the GlobalProtect Agent Configurations, Customize the GlobalProtect App, and Deploy the GlobalProtect App to End Users for details.

The GlobalProtect app for mobile endpoints (iOS, Android, and Windows UWP) is available through the official store for the endpoint—the Apple App Store for iOS, Google Play for Android,

and the Microsoft Store for Windows UWP. You can alternatively Deploy the GlobalProtect Mobile App Using Workspace ONE or Qualified MDM Vendors.

See What OS Versions are Supported with GlobalProtect? for more details.

The following diagram illustrates how the GlobalProtect portals, gateways, and apps work together to enable secure access for all your users, regardless of what endpoints they are using or where they are located.



What OS Versions are Supported with GlobalProtect?

The GlobalProtect app is supported on common desktops, laptops, tablets, and smart phones. We recommend that you configure GlobalProtect on firewalls running PAN-OS 6.1 or later releases and that your end users install only supported releases of the GlobalProtect app on their endpoints. The minimum GlobalProtect app release varies by operating system; to determine the minimum GlobalProtect app release for a specific operating system, refer to the following topics in the Palo Alto Networks® CompatibilityMatrix:

- Where Can I Install the GlobalProtectApp?
- What X-Auth IPSec Clients are Supported?

Older versions of the GlobalProtect app are still supported on the operating systems and PAN-OS releases with which they were released. For the minimum PAN-OS release support, refer to the GlobalProtect app release notes corresponding to the specific release on the Software Updates site.

About GlobalProtect Licenses

If you want to use GlobalProtect to provide a secure remote access or virtual private network (VPN) solution via single or multiple internal/external gateways, you do not need any GlobalProtect licenses. However, to use some of the more advanced features (such as HIP checks and associated content updates, support for the GlobalProtect mobile app, or IPv6 support) you must purchase an annual GlobalProtect Gateway license. This license must be installed on each firewall running a gateway(s) that:

- Performs HIP checks
- Supports the GlobalProtect app for mobile endpoints
- Supports the GlobalProtect app for Linux endpoints
- Supports the GlobalProtect app for IoT endpoints
- Provides IPv6 connections
- Split tunnels traffic based on the destination domain, application process name, or HTTP/HTTPS video streaming application.
- Supports adding a compromised device to the quarantine list.
- Supports identification of managed devices using the endpoint's serial number on gateways
- Enforces GlobalProtect connections with FQDN exclusions

For GlobalProtect Clientless VPN, you must also install a GlobalProtect Gateway license on the firewall that hosts the Clientless VPN from the GlobalProtect portal. You also need the **GlobalProtect Clientless VPN** dynamic updates to use this feature.

Similarly, for any firewall or GlobalProtect gateway which is acting as Redistribute HIP Reports or client/collector requires a GlobalProtect Gateway license. The only exception is Panorama.

Feature	Gateway License Required?
Single external gateway (Windows and macOS)	—
Single or multiple internal gateways	—
Multiple external gateways	—
GlobalProtect for IoT Devices devices	✓
HIP Checks	✓
Identification of managed devices using the endpoint serial number on gateways	✓
HIP-based policy enforcement based on the endpoint status	✓
App for endpoints running Windows and macOS	—

Feature	Gateway License Required?
Mobile app for endpoints running iOS, Android, Chrome OS, and Windows 10 UWP	✓
App for endpoints running Linux	✓
App for endpoints running IoT	✓
IPv6 for external gateways	✓
IPv6 for internal gateways (change to default behavior—starting with GlobalProtect app 4.1.3, a GlobalProtect subscription is not required for this use case)	—
Clientless VPN (Not supported on multi-VSYS firewalls if the traffic must traverse multiple virtual systems)	✓
Split tunneling based on destination domain, client process, and video streaming application	✓
Split DNS	✓
Adding a compromised device to the quarantine list	✓
GlobalProtect App Log Collection for Troubleshooting Overview (Panorama appliance running 9.0 or later and PAN-OS 8.1 or later)	✓
Enforces GlobalProtect connections with FQDN exclusions	✓
Redistribute HIP Reports	✓

See Activate Licenses for information on installing licenses on the firewall.

Get Started

In order for GlobalProtect™ to run, you must set up the infrastructure that allows all components to communicate. At a basic level, this means setting up the interfaces and zones to which the GlobalProtect end users connect to access the portal and the gateways to the network. Because the GlobalProtect components communicate over secure channels, you must acquire and deploy the required SSL certificates to the various components. The following sections guide you through the GlobalProtect infrastructure setup:

- Create Interfaces and Zones for GlobalProtect
- Enable SSL Between GlobalProtect Components

Create Interfaces and Zones for GlobalProtect

You must configure the following interfaces and zones for your GlobalProtect infrastructure:

- **GlobalProtect portal**—Requires a Layer 3 or loopback interface for the GlobalProtect apps' connection. If the portal and gateway are on the same firewall, they can use the same interface. The portal must be in a zone that is accessible from outside your network, such as a DMZ.
- **GlobalProtect gateways**—The interface and zone requirements for the gateway depend on whether the gateway you are configuring is external or internal, as follows:
  - **External gateways**—Requires a Layer 3 or loopback interface and a logical tunnel interface for the app to establish a connection. The Layer 3/loopback interface must be in an external zone, such as a DMZ. A tunnel interface can be in the same zone as the interface connecting to your internal resources (for example, **`trust`**). For added security and better visibility, you can create a separate zone, such as **`corp-vpn`**. If you create a separate zone for your tunnel interface, you must create security policies that enable traffic to flow between the VPN zone and the trust zone.
  - **Internal gateways**—Requires a Layer 3 or loopback interface in your trust zone. You can also create a tunnel interface for access to your internal gateways, but this is not required.

For tips on how to use a loopback interface to provide access to GlobalProtect on different ports and addresses, refer to Can GlobalProtect Portal Page be Configured to be Accessed on any Port?

For more information about portals and gateways, see About the GlobalProtect Components.

STEP 1 | Configure a Layer 3 interface for each portal and/or gateway you plan to deploy.

If the gateway and portal are on the same firewall, you can use a single interface for both.

As a best practice, use static IP addresses for the portal and gateway.

Do not attach an interface management profile that allows HTTP, HTTPS, Telnet, or SSH on the interface where you have configured a GlobalProtect portal or gateway because this enables access to your management interface from the internet. Follow the Adminstrative Access Best Practices to ensure that you are securing administrative access to your firewalls in a way that will prevent successful attacks.

1. Select **Network** > **Interfaces** > **Ethernet** or **Network** > **Interfaces** > **Loopback**, and then select the interface you want to configure for GlobalProtect. In this example, we are configuring **`ethernet1/1`** as the portal interface.
2. (Ethernet only) Set the **Interface Type** to **Layer3**.
3. On the **Config** tab, select the **Security Zone** to which the portal or gateway interface belongs, as follows:
   - Place portals and external gateways in an untrust zone for access by hosts outside your network, such as **`l3-untrust`**.
   - Place internal gateways in an internal zone, such as **`l3-trust`**.
   - If you have not yet created the zone, add a **New Zone**. In the Zone dialog, define a **Name** for the new zone and then click **OK**.
4. Select the default **Virtual Router**.
5. Assign an IP address to the interface:
   - For an IPv4 address, select **IPv4** and **Add** the IP address and network mask to assign to the interface, for example 203.0.11.100/24.
   - For an IPv6 address, select **IPv6**, **Enable IPv6 on the interface**, and **Add** the IP address and network mask to assign to the interface, for example 2001:1890:12f2:11::10.1.8.160/80.
6. Click **OK** to save the interface configuration.

STEP 2 | On the firewall(s) hosting GlobalProtect gateway(s), configure the logical tunnel interface that will terminate VPN tunnels established by the GlobalProtect apps.

IP addresses are not required on the tunnel interface unless you require dynamic routing. In addition, assigning an IP address to the tunnel interface can be useful for troubleshooting connectivity issues.

Be sure you enable User-ID in the zone where the VPN tunnels terminate.

1. Select **Network** > **Interfaces** > **Tunnel**, and **Add** a tunnel interface.
2. In the **Interface Name** field, enter a numeric suffix, such as **.2**.
3. On the **Config** tab, select the **Security Zone** for VPN tunnel termination, as follows:
   - To use your trust zone as the termination point for the tunnel, select the zone from the drop-down.
   - (Recommended) To create a separate zone for VPN tunnel termination, add a **New Zone**. In the Zone dialog, define a **Name** for new zone (for example, **corp-vpn**), **Enable User Identification**, and then click **OK**.
4. Set the **Virtual Router** to **None**.
5. Assign an IP address to the interface:
   - For an IPv4 address, select **IPv4** and **Add** the IP address and network mask to assign to the interface, for example 203.0.11.100/24.
   - For an IPv6 address, select **IPv6**, **Enable IPv6 on the interface**, and **Add** the IP address and network mask to assign to the interface, for example 2001:1890:12f2:11::10.1.8.160/80.
6. Click **OK** to save the interface configuration.

STEP 3 | If you created a separate zone for tunnel termination of VPN connections, create a security policy to enable traffic flow between the VPN zone and your trust zone.

For example, the following policy rule enables traffic between the **corp-vpn** zone and the **l3-trust** zone.

			Source				Destination				
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	VPN Access	none	corp-vpn	any	any	any	l3-trust	any	adobe-cq ms-exchange ms-office365 sharepoint	application-default	Allow

STEP 4 | **Commit** the configuration.

Enable SSL Between GlobalProtect Components

All interaction between the GlobalProtect components occurs over an SSL/TLS connection. Therefore, you must generate and/or install the required certificates before configuring each component so that you can reference the appropriate certificate(s) in the configurations. The following sections describe the supported methods of certificate deployment, descriptions and best practice guidelines for the various GlobalProtect certificates, and provide instructions for generating and deploying the required certificates:

- About GlobalProtect Certificate Deployment
- GlobalProtect Certificate Best Practices
- Deploy Server Certificates to the GlobalProtect Components

About GlobalProtect Certificate Deployment

There are three basic approaches to Deploy Server Certificates to the GlobalProtect Components:

- (Recommended) **Combination of third-party certificates and self-signed certificates**—Because the GlobalProtect app will be accessing the portal prior to GlobalProtect configuration, the app must trust the certificate to establish an HTTPS connection.
- **Enterprise Certificate Authority**—If you already have your own enterprise CA, you can use this internal CA to issue certificates for each of the GlobalProtect components and then import them onto the firewalls hosting your portal and gateway(s). In this case, you must also ensure that the endpoints trust the root CA certificate used to issue the certificates for the GlobalProtect services to which they must connect.
- **Self-Signed Certificates**—You can generate a self-signed CA certificate on the portal and use it to issue certificates for all of the GlobalProtect components. However, this solution is less secure than the other options and is therefore not recommended. If you do choose this option, end users will see a certificate error the first time they connect to the portal. To prevent this, you can deploy the self-signed root CA certificate to all endpoints manually or using some sort of centralized deployment, such as an Active Directory Group Policy Object (GPO).

GlobalProtect Certificate Best Practices

The following table summarizes the SSL/TLS certificates you will need, depending on which features you plan to use:

Certificate	Usage	Issuing Process/Best Practices
CA certificate	Used to sign certificates issued to the GlobalProtect components.	If you plan on using self-signed certificates, generate a CA certificate using your dedicated CA server or Palo Alto Networks firewall, and then issue GlobalProtect portal and gateway certificates signed by the CA or an intermediate CA.

Certificate	Usage	Issuing Process/Best Practices
Portal server certificate	Enables GlobalProtect apps to establish an HTTPS connection with the portal.	• This certificate is identified in an SSL/TLS service profile. You assign the portal server certificate by selecting its associated service profile in a portal configuration. • Use a certificate from a well-known, third-party CA. This is the most secure option and ensures that the user endpoints can establish a trust relationship with the portal and without requiring you to deploy the root CA certificate. • If you do not use a well-known, public CA, you should export the root CA certificate that was used to generate the portal server certificate to all endpoints that run the GlobalProtect app. Exporting this certificate prevents the end users from seeing certificate warnings during the initial portal login. • The Common Name (CN) and Subject Alternative Name (SAN) fields of the certificate must match the IP address or FQDN of the interface that hosts the portal. • In general, a portal must have its own server certificate. However, if you are deploying a single gateway and portal on the same interface, you must use the same certificate for both the gateway and the portal. • If you configure a gateway and portal on the same interface, we also recommend that you use the same certificate profile and SSL/TLS service profile for both the gateway and portal. If they do not use the same certificate profile and SSL/TLS service profile, the gateway configuration takes precedence over the portal configuration during the SSL handshake.
Gateway server certificate	Enables GlobalProtect apps to establish an HTTPS connection with the gateway.	• This certificate is identified in an SSL/TLS service profile. You assign the gateway server certificate by selecting its associated service profile in a gateway configuration. • Generate a CA certificate on the firewall or CA server and use that CA certificate to generate all gateway certificates. • The CN and the SAN fields of the certificate must match the FQDN or IP address of the

Certificate	Usage	Issuing Process/Best Practices
		interface where you plan to configure the gateway. • The portal can distribute the gateway root CA certificate to the GlobalProtect app based on the configuration (Trusted Root CA list in the Portal configuration Agent tab). However, it is not mandatory for the gateway root CA certificate to be pre-installed in the user's trusted certificate store or for the gateway certificate to be issued by a public CA. • In general, each gateway must have its own server certificate. However, if you are deploying a single gateway and portal on the same interface for basic VPN access, you must use a single server certificate for both components. As a best practice, use a certificate signed by a public CA. • If you configure a gateway and portal on the same interface, we also recommend that you use the same certificate profile and SSL/TLS service profile for both the gateway and portal. If they do not use the same certificate profile and SSL/TLS service profile, the gateway configuration takes precedence over the portal configuration during the SSL handshake.

(Optional) Client certificate	Used to enable mutual authentication when establishing an HTTPS session between the GlobalProtect apps and the gateways/portal. This ensures that only endpoints with valid client certificates are able to authenticate and connect to the network.	• For simplified deployment of client certificates, configure the portal to deploy the client certificate to the apps upon successful login using either of the following methods:
		  • Use a single client certificate across all GlobalProtect apps that receive the same configuration. Assign the **Local** client certificate by uploading the certificate to the portal, and then selecting it in a portal agent configuration.
		  • Use simple certificate enrollment protocol (**SCEP**) to enable the GlobalProtect portal to deploy unique client certificates to your GlobalProtect apps. Enable this by configuring a SCEP profile, and then selecting that profile in a portal agent configuration.

Certificate	Usage	Issuing Process/Best Practices
		• Use one of the following digest algorithms when you generate client certificates for GlobalProtect endpoints: sha1, sha256, sha384, or sha512. • You can use other mechanisms to deploy unique client certificates to each endpoint when authenticating the end user. • Consider testing your configuration without the client certificate first, and then add the client certificate after you are sure that all other configuration settings are correct.
(Optional) Machine certificates	A machine certificate is a client certificate that is issued to an endpoint that resides in the local machine store or system keychain. Each machine certificate identifies the endpoint in the subject field (for example, CN=laptop1.example.com) instead of the user. The certificate ensures that only trusted endpoints can connect to gateways or the portal. Machine certificates are required for users configured with the pre-logon connect method	• Use one of the following digest algorithms when you generate client certificates for GlobalProtect endpoints: sha1, sha256, sha384, or sha512. • If you plan on using the pre-logon feature, use your own PKI infrastructure to deploy machine certificates to each endpoint prior to enabling GlobalProtect access. This approach is important for ensuring security. For more information, see Remote Access VPN with Pre-Logon.

Table: GlobalProtect Certificate Requirements

For details about the types of keys for secure communication between the GlobalProtect endpoint and the portals and gateways, see Reference: GlobalProtect App Cryptographic Functions.

Deploy Server Certificates to the GlobalProtect Components

The following table shows the best practice steps for deploying SSL/TLS certificates to the GlobalProtect components:

- Import a server certificate from a well-known, third-party CA.

  Use a server certificate from a well-known, third-party CA for the GlobalProtect portal. This practice ensures that the end users are able to establish an HTTPS connection without seeing warnings about untrusted certificates.

  The CN and, if applicable, the SAN fields of the certificate must match the FQDN or IP address of the interface where you plan to configure the portal or the device check-in interface on a third-party mobile endpoint management system. Wildcard matches are supported.

  Before you import a certificate, make sure the certificate and key files are accessible from your management system and that you have the passphrase to decrypt the private key.

  1. Select **Device** > **Certificate Management** > **Certificates** > **Device Certificates** and **Import** a new certificate.
  2. Use the **Local** certificate type (default).
  3. Enter a **Certificate Name**.
  4. Enter the path and name to the **Certificate File** received from the CA, or **Browse** to find the file.
  5. Set the **File Format** to **Encrypted Private Key and Certificate (PKCS12)**.
  6. Enter the path and name to the PKCS#12 file in the **Key File** field or **Browse** to find it.
  7. Enter and re-enter the **Passphrase** that was used to encrypt the private key.
  8. Click **OK** to import the certificate and key.

- Create the root CA certificate for issuing self-signed certificates for the GlobalProtect components.

  Create the Root CA certificate on the portal and use it to issue server certificates for the gateways and, optionally, for clients.

  Before deploying self-signed certificates, you must create the root CA certificate that signs the certificates for the GlobalProtect components:

  1. Select **Device** > **Certificate Management** > **Certificates** > **Device Certificates** and **Generate** a new certificate.
  2. Use the **Local** certificate type (default).
  3. Enter a **Certificate Name**, such as GlobalProtect_CA. The certificate name cannot contain spaces.
  4. Do not select a value in the **Signed By** field. Without a selection for **Signed By**, the certificate is self-signed.
  5. Enable the **Certificate Authority** option.
  6. Click **OK** to generate the certificate.

- Use the root CA on the portal to generate a self-signed server certificate.

  Generate server certificates for each gateway you plan to deploy and optionally for the management interface of the third-party mobile endpoint management system (if this interface is where the gateways retrieve HIP reports).

  *In the gateway server certificates, the values in the CN and SAN fields must be identical. If the values differ, the GlobalProtect agent detects the mismatch and does not trust the certificate. Self-signed certificates contain a SAN field only if you add a **Host Name** attribute.*

  Alternatively, you can List item.

  1. Select **Device** > **Certificate Management** > **Certificates** > **Device Certificates** and **Generate** a new certificate.
  2. Use the **Local** certificate type (default).
  3. Enter a **Certificate Name**. This name cannot contain spaces.
  4. In the **Common Name** field, enter the FQDN (recommended) or IP address of the interface where you plan to configure the gateway.
  5. In the **Signed By** field, select the GlobalProtect_CA you created.
  6. In the Certificate Attributes area, **Add** and define the attributes that uniquely identify the gateway. Keep in mind that if you add a **Host Name** attribute (which populates the SAN field of the certificate), it must be the same as the value you defined for the **Common Name**.
  7. Configure cryptographic settings for the server certificate, including the encryption **Algorithm**, key length (**Number of Bits**), **Digest** algorithm, and **Expiration** (days).
  8. Click **OK** to generate the certificate.

- Use Simple Certificate Enrollment Protocol (SCEP) to request a server certificate from your enterprise CA.

  Configure separate SCEP profiles for each portal and gateway you plan to deploy. Then use the specific SCEP profile to generate the server certificate for each GlobalProtect component.

  *In portal and gateway server certificates, the value of the CN field must include the FQDN (**recommended**) or IP address of the interface where you plan to configure the portal or gateway and must be identical to the SAN field.*

  To comply with the U.S. Federal Information Processing Standard (FIPS), you must also enable mutual SSL authentication between the SCEP server and the GlobalProtect portal. (FIPS-CC operation is indicated on the firewall login page and in its status bar.)

  After you commit the configuration, the portal attempts to request a CA certificate using the settings in the SCEP profile. If successful, the firewall hosting the portal saves the CA certificate and displays it in the list of **Device Certificates**.

  1. Configure a SCEP Profile for each GlobalProtect portal or gateway:
     1. Enter a **Name** that identifies the SCEP profile and the component to which you deploy the server certificate. If this profile is for a firewall with multiple virtual systems capability, select a virtual system or **Shared** as the **Location** where the profile is available.
     2. (Optional) Configure a **SCEP Challenge**, which is a response mechanism between the PKI and portal for each certificate request. Use either a **Fixed** challenge password that you obtain from the SCEP server or a **Dynamic** password where the portal-client submits a username and OTP of your choice to the SCEP Server. For a Dynamic SCEP challenge, this can be the credentials of the PKI administrator.
     3. Configure the **Server URL** that the portal uses to reach the SCEP server in the PKI (for example, **`http://10.200.101.1/certsrv/mscep/`**).
     4. Enter a string (up to 255 characters in length) in the **CA-IDENT Name** field to identify the SCEP server.
     5. Enter the **Subject** name to use in the certificates generated by the SCEP server. The subject must include a common name (CN) key in the format **`CN=<value>`** where **`<value>`** is the FQDN or IP address of the portal or gateway.
     6. Select the **Subject Alternative Name Type**. To enter the email name in a certificate's subject or Subject Alternative Name extension, select **RFC 822 Name**. You can

also enter the **DNS Name** to use to evaluate certificates, or the **Uniform Resource Identifier** to identify the resource from which the client will obtain the certificate.

7. Configure additional cryptographic settings, including the key length (**Number of Bits**), and **Digest** algorithm for the certificate signing request.
8. Configure the permitted uses of the certificate, either for signing (**Use as digital signature**) or encryption (**Use for key encipherment**).
9. To ensure that the portal is connecting to the correct SCEP server, enter the **CA Certificate Fingerprint**. Obtain this fingerprint from the SCEP server interface in the Thumbprint field.
10. Enable mutual SSL authentication between the SCEP server and the GlobalProtect portal.
11. Click **OK** and then **Commit** the configuration.

2. Select **Device** > **Certificate Management** > **Certificates** > **Device Certificates** and then click **Generate**.
3. Enter a **Certificate Name**. This name cannot contain spaces.
4. Select the **SCEP Profile** to use to automate the process of issuing a server certificate that is signed by the enterprise CA to a portal or gateway, and then click **OK** to generate the certificate. The GlobalProtect portal uses the settings in the SCEP profile to submit a CSR to your enterprise PKI.

- Assign the server certificate you imported or generated to an SSL/TLS service profile.
  1. Select **Device** > **Certificate Management** > **SSL/TLS Service Profile** and **Add** a new SSL/TLS service profile.
  2. Enter a **Name** to identify the profile, and select the server **Certificate** you imported or generated.
  3. Define the range of SSL/TLS versions (**Min Version** to **Max Version**) for communication between GlobalProtect components.

     *The **Max Version** supported is **TLSv1.2**.*

     *To provide the strongest security, set the **Min Version** to **TLSv1.2**.*
  4. Click **OK** to save the SSL/TLS service profile.
  5. **Commit** the changes.

- Deploy the self-signed server certificates.

  - *Export the self-signed server certificates issued by the root CA on the portal and import them onto the gateways.*
  - *Be sure to issue a unique server certificate for each gateway.*
  - *If specifying self-signed certificates, you must distribute the Root CA certificate to the end clients in the portal client configurations.*

  Export the certificate from the portal:

  1. Select **Device** > **Certificate Management** > **Certificates** > **Device Certificates**.
  2. Select the gateway certificate you want to deploy, and then click **Export Certificate**.
  3. Set the **File Format** to **Encrypted Private Key and Certificate (PKCS12)**.
  4. Enter and confirm a **Passphrase** to encrypt the private key.
  5. Click **OK** to download the PKCS12 file to a location of your choice.

  Import the certificate on the gateway:

  1. Select **Device** > **Certificate Management** > **Certificates** > **Device Certificates** and **Import** the certificate.
  2. Enter a **Certificate Name**.
  3. **Browse** to find and select the **Certificate File** you downloaded in the previous step.
  4. Set the **File Format** to **Encrypted Private Key and Certificate (PKCS12)**.
  5. Enter and confirm the **Passphrase** you used to encrypt the private key when you exported it from the portal.
  6. Click **OK** to import the certificate and key.
  7. **Commit** the changes for the gateway.

GlobalProtect User Authentication

The first time a GlobalProtect app connects to the portal, the user is prompted to authenticate to the portal. If authentication succeeds, the GlobalProtect portal sends the GlobalProtect configuration, which includes the list of gateways to which the app can connect, and optionally a client certificate for connecting to the gateways. After successfully downloading and caching the configuration, the app attempts to connect to one of the gateways specified in the configuration. Because these components provide access to your network resources and settings, they also require the end user to authenticate.The appropriate security level required on the portal and gateways varies with the sensitivity of the resources that the gateway protects. GlobalProtect provides a flexible authentication framework that allows you to choose the authentication profile and certificate profile that are appropriate to each component. GlobalProtect provides the following authentication methods:

- **Local Authentication**—Both the user account credentials and the authentication mechanisms are local to the firewall. This authentication mechanism is not scalable because it requires an account for every GlobalProtect user and is, therefore, advisable for only very small deployments.
- **External Authentication**—User authentication functions are performed by external Set Up LDAP Authentication, Set Up Kerberos Authentication, Set Up RADIUS or TACACS+ Authentication, Set Up SAML Authentication, or Set Up RADIUS or TACACS + Authenticationservices (including support for two-factor, token-based authentication mechanisms, such as one-time password (OTP) authentication). To Set Up External Authenticationyou must create a server profile with settings for access to the external authentication service, create an authentication profile that refers to the server profile, and specify client authentication in the portal and gateway configurations and optionally specify the OS of the endpoint that will use these settings. You can use different authentication profiles for each GlobalProtect component.
- **Client Certificate Authentication**—For enhanced security, you can Set Up Client Certificate Authentication to obtain the username and authenticate the user before granting access to the system. GlobalProtect also supports authentication by common access cards (CACs) and smart cards, which rely on a certificate profile. With these cards, the certificate profile must contain the root CA certificate that issued the certificate to the smart card or CAC.
- **Two-Factor Authentication**—With two-factor authentication, the portal or gateway authenticates users through two mechanisms, such as a one-time password (OTP) and Active Directory (AD) login credentials. You can Set Up Two-Factor Authentication by configuring and adding both a certificate profile and authentication profile to the portal and/or gateway configuration. You can configure the portal and gateways to use either the same authentication method or different authentication methods. Regardless, users must successfully authenticate through the two mechanisms that the component demands before they can gain access to the network resources.
- (Windows and macOS only) **Multi-Factor Authentication for Non-Browser-Based Applications**— For sensitive, non-browser-based network resources (for example, financial applications or software development applications) that may require additional authentication, the GlobalProtect app can Configure GlobalProtect to Facilitate Multi-Factor Authentication Notifications required to access these resources.

- (Windows and macOS only) **Single Sign-On**—With single sign-on (SSO), which is enabled by default, the GlobalProtect app uses the user's OS login credentials to automatically authenticate and connect to the GlobalProtect portal and gateway. You can also configure the app to SSO Wrapping for Third-Party Credential Providers on Windows Endpoints to ensure that Windows users can authenticate and connect using a third-party credential provider.
- (Prisma Access only) **Cloud Identity Engine**—The Cloud Identity Engine provides both user identification and user authentication for mobile users in a Panorama Managed Prisma Access—GlobalProtect deployment. Using the Cloud Identity Engine for user authentication and username-to-user group mapping allows you to write security policy based on users and groups, not IP addresses, and helps secure your assets by enforcing behavior-based security actions. By continually syncing the information from your directories, the Cloud Identity Engine ensures that your user information is accurate and up to date and policy enforcement continues based on the mappings even if the SAML identity provider (IdP) is temporarily unavailable. Prisma Access users must be running GlobalProtect app 6.0 or later with a Prisma Access Innovation release 3.0 or later.

How Does the App Know What Credentials to Supply?

By default, the GlobalProtect app attempts to use the same login credentials for the gateway that it used for portal login. In the simplest case, where the gateway and the portal use the same authentication profile and/or certificate profile, the app connects to the gateway transparently.

On a per-app configuration basis, you can also customize which GlobalProtect portal and gateways—internal, external, or manual only—require different credentials (such as unique OTPs). This enables the GlobalProtect portal or gateway to prompt for the unique OTP without first prompting for the credentials specified in the authentication profile.

There are two options for modifying the default app authentication behavior so that authentication is both stronger and faster:

- Cookie Authentication on the Portal or Gateway
- Credential Forwarding to Some or All Gateways

Cookie Authentication on the Portal or Gateway

Cookie authentication simplifies the authentication process for end users because they will no longer be required to log in to both the portal and the gateway in succession or enter multiple OTPs for authenticating to each. This improves the user experience by minimizing the number of times that users must enter credentials. In addition, cookies enable use of a temporary password to re-enable VPN access after the user's password expires.

You can configure cookie authentication settings independently for the portal and for individual gateways (for example, you can impose a shorter cookie lifetime on gateways that protect sensitive resources). After the portal or gateways deploy an authentication cookie to the endpoint, the portal and gateways both rely on the same cookie to authenticate the user. When the app presents the cookie, the portal or gateway evaluates whether the cookie is valid based on the configured cookie lifetime. If the cookie expires, GlobalProtect automatically prompts the user to authenticate with the portal or gateway. When authentication is successful, the portal or gateway issues the replacement authentication cookie to the endpoint, and the validity period starts over.

Consider the following example where you configure the cookie lifetime for the portal—which does not protect sensitive information—as 15 days, but configure the cookie lifetime for gateways—which do protect sensitive information—as 24 hours. When the user first authenticates with the portal, the portal issues the authentication cookie. If after five days, the user attempted to connect to the portal, the authentication cookie would still be valid. However, if after five days the user attempted to connect to the gateway, the gateway would evaluate the cookie lifetime and determine it expired (5 days > 24 hours). The agent would then automatically prompt the user to authenticate with the gateway and, on successful authentication, receive a replacement authentication cookie. The new authentication cookie would then be valid for another 15 days on the portal and another 24 hours on the gateways.

For an example of how to use this option, see Set Up Two-Factor Authentication.

Credential Forwarding to Some or All Gateways

With two-factor authentication, you can specify the portal and/or types of gateways (internal, external, or manual only) that prompt for their own set of credentials. This option speeds up the authentication process when the portal and the gateway require different credentials (either different OTPs or different login credentials entirely). For each portal or gateway that you select, the app does not forward credentials, allowing you to customize the security for different GlobalProtect components. For example, you can have the same security on your portals and internal gateways, while requiring a second factor OTP or a different password for access to those gateways that provide access to your most sensitive resources.

For an example of how to use this option, see Set Up Two-Factor Authentication.

How Does the App Know Which Certificate to Supply?

When you configure GlobalProtect to use client certificates for authentication on macOS or Windows endpoints, GlobalProtect must present a valid client certificate to authenticate with the portal and/or gateways.

For a client certificate to be valid, it must meet the following requirements:

- The certificate is issued by the certificate authority (CA) you defined in the Certificate Profile of your portal and gateway configurations.
- The certificate specifies the client authentication purpose, which the certificate administrator specifies when creating the certificate.
- The certificate is located in the certificate store, as configured in the GlobalProtect portal agent configuration. By default, the GlobalProtect app first looks for a valid certificate in the user store. If none exist, the app then looks in the machine store. If the GlobalProtect app locates a certificate in the user store, it will not look in the machine store because the user store takes precedence. To force the GlobalProtect app to look for certificates in only one certificate store, configure the **Client Certificate Store Lookup** option in the appropriate GlobalProtect portal agent configuration.
- The certificate matches additional purposes specified in the GlobalProtect portal agent configuration. To specify an additional purpose, you must identify the object identifier (OID) for the certificate and configure the **Extended Key Usage OID** value in the appropriate GlobalProtect portal agent configuration. An OID is a numeric value that identifies the application or service for which to use a certificate and that is automatically attached to a certificate when it is created by a certificate authority (CA). For more information on specifying a common or custom OID, see Enable Certificate Selection Based on OID.

When only one client certificate meets the requirements above, the app automatically uses that client certificate for authentication. However, when multiple client certificates meet the these requirements, GlobalProtect prompts the user to select the client certificate from a list of valid client certificates on the endpoint. While GlobalProtect requires users to select the client certificate only when they first connect, users might not know which certificate to select. In this case, we recommend you to narrow the list of available client certificates by certificate purpose (as indicated by the OID) and certificate store. For more information on these and other settings you can configure to customize your app, see Customize the GlobalProtect App.

Set Up External Authentication

The following workflows describe how to set up the GlobalProtect portal and gateways to use an external authentication service. The supported authentication services include LDAP, Kerberos, RADIUS, SAML, and TACACS+.

*GlobalProtect also supports local authentication. To use local authentication, create a local user database (**Device** > **Local User Database**) that contains the users and groups to which you want to allow GlobalProtect access, and then refer to that database in the authentication profile.*

For more information, see GlobalProtect User Authentication.

The options for setting up external authentication include:

- Set Up LDAP Authentication
- Set Up SAML Authentication
- Set Up Kerberos Authentication
- Set Up RADIUS or TACACS+ Authentication

Set Up LDAP Authentication

LDAP is often used by organizations as an authentication service and a central repository for user information. It can also be used to store the role information for application users.

STEP 1 | Create a server profile.

The server profile identifies the external authentication service and instructs the firewall how to connect to that authentication service and access the authentication credentials for your users.

When you use LDAP to connect to Active Directory (AD), you must create a separate LDAP server profile for every AD domain.

1. Select **Device** > **Server Profiles** > **LDAP**, and then **Add** an LDAP server profile.
2. Enter a **Profile Name**, such as **`GP-User-Auth`**.
3. If this profile is for a firewall with multiple virtual systems capability, select a virtual system or **Shared** as the **Location** where the profile is available.
4. Click **Add** in the **Server List** area, and then enter the necessary information for connecting to the authentication server, including the server **Name**, IP address or FQDN of the **LDAP Server**, and **Port**.
5. Select the LDAP server **Type**.
6. Enter the **Bind DN** and **Password** to enable the authentication service to authenticate the firewall.
7. (Optional) If you want the endpoint to use SSL or TLS for a more secure connection with the directory server, enable the option to **Require SSL/TLS secured connection** (enabled by default). The protocol that the endpoint uses depends on the server port:
   - 389 (default)—TLS (Specifically, the device uses the StartTLS operation, which upgrades the initial plaintext connection to TLS.)
   - 636—SSL
   - Any other port—The device first attempts to use TLS. If the directory server doesn't support TLS, the device falls back to SSL.
8. (Optional) For additional security, enable to the option to **Verify Server Certificate for SSL sessions** so that the endpoint verifies the certificate that the directory server presents for SSL/TLS connections. To enable verification, you must also enable the option to **Require SSL/TLS secured connection**. For verification to succeed, the certificate must meet one of the following conditions:
   - It is in the list of device certificates: **Device** > **Certificate Management** > **Certificates** > **Device Certificates.** If necessary, import the certificate into the device.
   - The certificate signer is in the list of trusted certificate authorities: **Device** > **Certificate Management** > **Certificates** > **Default Trusted Certificate Authorities**.
9. Click **OK** to save the server profile.

STEP 2 | (Optional) Create an authentication profile.

The authentication profile specifies the server profile that the portal or gateways use when they authenticate users. On a portal or gateway, you can assign one or more authentication profiles to one or more client authentication profiles. For descriptions of how an authentication profile within a client authentication profile supports granular

user authentication, see Configure a GlobalProtect Gateway and Set Up Access to the GlobalProtect Portal.

To enable users to connect and change their expired passwords without administrative intervention, consider using Remote Access VPN with Pre-Logon.

*If a user's password expires, you can assign a temporary LDAP password to enable them to log in to GlobalProtect. In this case, the temporary password may be used to authenticate to the portal, but the gateway login may fail because the same temporary password cannot be re-used. To prevent this issue, configure an authentication override in the portal configuration (**Network** > **GlobalProtect** > **Portal**) to enable the GlobalProtect app to use a cookie to authenticate to the portal and the temporary password to authenticate to the gateway.*

1. Select **Device** > **Authentication Profile**, and then **Add** a new profile.
2. Enter a **Name** for the profile.
3. Set the **Authentication Type** to **LDAP**.
4. Select the LDAP authentication **Server Profile** that you created in step 1.
5. Enter **sAMAccountName** as the **Login Attribute**.
6. Set the **Password Expiry Warning** to specify the number of days before password expiration that users are notified. By default, users are notified seven days prior to password expiration (range is 1-255). Because users must change their passwords before the end of the expiration period, you must provide a notification period that is adequate for your users in order to ensure continued access to GlobalProtect. To use this feature, you must specify one of the following LDAP server types in your LDAP server profile: **active-directory**, **e-directory**, or **sun**.

   Unless you enable pre-logon, users cannot access GlobalProtect when their passwords expire.
7. Specify the **User Domain** and **Username Modifier**. The endpoint combines the **User Domain** and **Username Modifier** values to modify the domain/username string that a user enters during login. The endpoint uses the modified string for authentication and the **User Domain** value for User-ID group mapping. Modifying user input is useful when the authentication service requires domain/username strings in a particular format but

you do not want to rely on users to enter the domain correctly. You can select from the following options:

- To send only the unmodified user input, leave the **User Domain** blank (the default) and set the **Username Modifier** to the variable **%USERINPUT%** (the default).
- To prepend a domain to the user input, enter a **User Domain** and set the **Username Modifier** to **%USERDOMAIN%\%USERINPUT%**.
- To append a domain to the user input, enter a **User Domain** and set the **Username Modifier** to **%USERINPUT%@%USERDOMAIN%**.

*If the **Username Modifier** includes the **%USERDOMAIN%** variable, the **User Domain** value replaces any domain string that the user enters. If the **User Domain** is blank, tthe device removes any user-entered domain string.*

8. On the **Advanced** tab, **Add** an **Allow List** to select the users and user groups that are allowed to authenticate with this profile. The **all** option allows every user to authenticate with this profile. By default, the list has no entries, which means no users can authenticate.
9. Click **OK**.

STEP 3 | Commit the configuration.

Click **Commit**.

Set Up SAML Authentication

Security Assertion Markup Language (SAML) is an XML-based, open-standard data format used to exchange authentication and authorization data between parties, specifically between an identity provider (IdP) and a service provider. SAML is a product of the OASIS Security Services Technical Committee.

STEP 1 | Create a server profile.

The server profile identifies the external authentication service and instructs the firewall on how to connect to that authentication service and access the authentication credentials for your users.

The following steps describe how you can import a SAML metadata file from the IdP so that the firewall can automatically create a server profile and populate the connection, registration,

and IdP certificate information. If the IdP does not provide a metadata file, select **Device** > **Server Profiles** > **SAML Identity Provider**, and then **Add** a server profile manually.

1. Export the SAML metadata file from the IdP to an endpoint that the firewall can access.

   Refer to your IdP documentation for instructions on how to export the file.
2. Select **Device** > **Server Profiles** > **SAML Identity Provider**.
3. **Import** the metadata file onto the firewall.
4. Enter a **Profile Name** to identify the server profile, such as **`GP-User-Auth`**.
5. **Browse** for the metadata file.
6. Select **Validate Identity Provider Certificate** (default) so that the firewall validates the IdP certificate.

   Validation occurs only after you assign the server profile to an authentication profile and **Commit** the changes. The firewall uses the certificate profile within the authentication profile to validate the certificate.
7. Enter the **Maximum Clock Skew**, which is the allowed system time difference (in seconds) between the IdP and the firewall when the firewall validates IdP messages. The default value is 60 seconds, and the range is 1 to 900 seconds.If the difference exceeds this value, authentication fails.
8. Click **OK** to save the server profile.

STEP 2 | (Optional) Create an authentication profile.

The authentication profile specifies the server profile that the portal or gateways use when they authenticate users. On a portal or gateway, you can assign one or more authentication profiles to one or more client authentication profiles. For more information on how an authentication profile within a client authentication profile supports granular

user authentication, see Configure a GlobalProtect Gateway and Set Up Access to the GlobalProtect Portal.

SAML authentication supports Remote Access VPN with Pre-Logon with GlobalProtect app 5.0 and later releases.

1. Select **Device** > **Authentication Profile**, and then **Add** a new authentication profile.
2. Enter a **Name** for the authentication profile.
3. Set the **Authentication Type** to **SAML**.
4. Select the SAML **IdP Server Profile** that you created in step 1.
5. Configure the following options to enable certificate authentication between the firewall and the Set Up SAML Authentication identity provider.
   - The **Certificate for Signing Requests** that the firewall uses to sign messages that it sends to the IdP.
   - The **Certificate Profile** that the firewall uses to validate the IdP certificate.
6. Specify the username and admin role formats.
   - Specify the **Username Attribute** and **User Group Attribute**.

     *Unlike other external authentication types, the SAML authentication profile does not have a **User Domain** attribute.*

   - (Optional) If you plan to use this profile to authenticate the administrative accounts that you manage in the IdP identity store, specify the **Admin Role Attribute** and **Access Domain Attribute**.
7. On the **Advanced** tab, **Add** an **Allow List** to select the users and groups that are allowed to authenticate with this profile. The **all** option allows every user to authenticate with this profile. By default, the list has no entries, which means no users can authenticate.

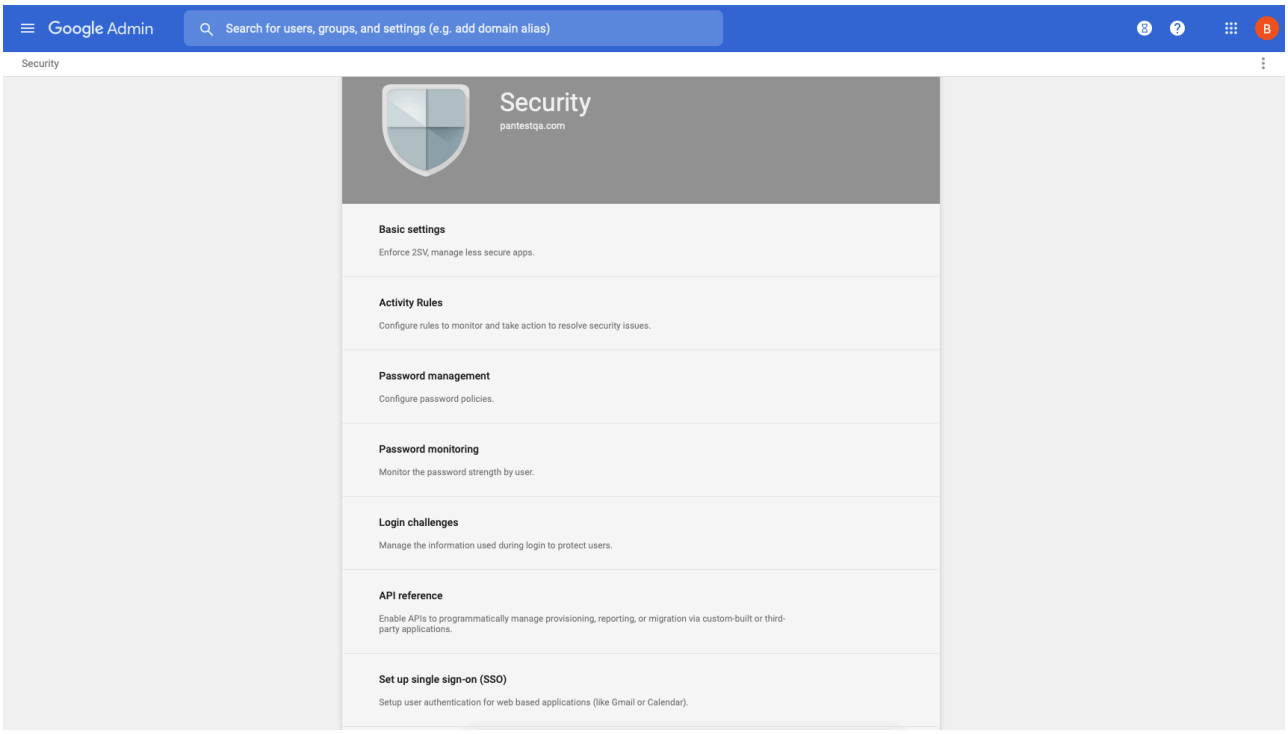
   Make sure the username in the **Allow List** matches the username returned from the SAML IdP server.
8. Click **OK**.

STEP 3 | **Commit** the configuration.

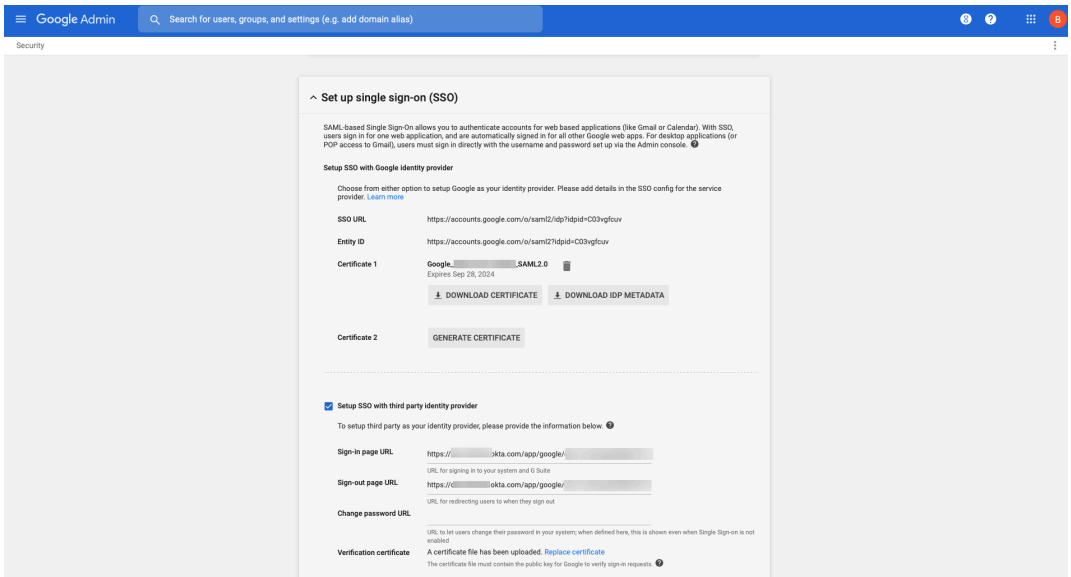
STEP 4 | (Chromebooks only) Enable SAML SSO for Chromebooks.

These steps allow you to set up SAML SSO for the GlobalProtect app for Android on Chromebooks.

1. Sign in to the Google Admin Console and select **Security**.

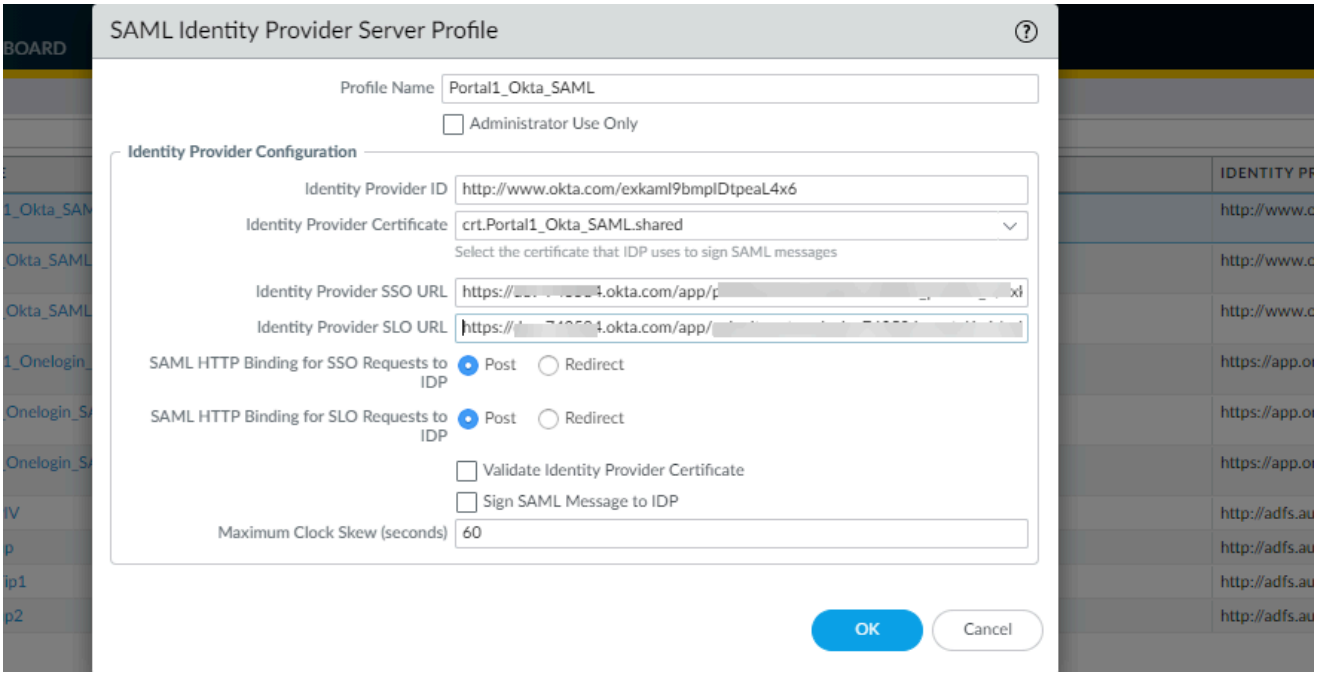


2. Select **Set up single sign-on (SSO)**.
3. (Optional) If you want to set up SSO with any other provider besides Google, select **Setup SSO with third party identity provider** and specify the **Sign-in page URL** and **Sign-out page URL** and upload a valid **Verification certificate**.



4. Configure the SAML identity provider in GlobalProtect.

1. In the GlobalProtect console, select **Device** > **Server Profiles** > **SAML Identity Provider**.
2. Match the values you entered for the IdP in the Google Admin Console.



Use the Default System Browser for SAML Authentication

If you have configured the GlobalProtect portal to authenticate users through SAML authentication, end users can connect to the app or other SAML-enabled applications without having to re-enter their credentials, for a seamless single sign-on (SSO) experience. End users can benefit from using the default system browser for SAML authentication because they can leverage the same login for GlobalProtect with their saved user credentials on the default system browser such as Chrome, Firefox, or Safari.

In addition, on any browser that supports the Web Authentication (WebAuthn) API, you can use the Univeral 2nd Factor (U2F) security tokens such as YubiKeys for multi-factor authentication (MFA) to identify providers (IdPs) such as Onelogin or Okta.

This feature is supported for Windows, macOS, Linux, and Android, and iOS devices starting with GlobalProtect™ app 5.2.

STEP 1 | Change the pre-deployed settings on Windows, macOS, Linux, and Android, and iOS endpoints to use the default system browser for SAML authentication.

You must set the pre-deployed settings on the client endpoints before you can enable the default system browser for SAML authentication. GlobalProtect retrieves these entries only once, when the GlobalProtect app initializes.

If there is no pre-deployed value specified on the end users' Windows or macOS endpoints when using the default system browser for SAML authentication, the **Use Default Browser for SAML Authentication** option is set to **Yes** in the portal configuration, and users upgrade the app from release 5.0.x or release 5.1.x to release 5.2.0 for the first time, the app will open

an embedded browser instead of the default system browser. After users connect to the GlobalProtect app and the **Use Default Browser for SAML Authentication** option is set to **Yes** in the portal configuration, the app will open the default system browser on Windows and macOS endpoints at the next login.

If the **default browser** value is set to **Yes** in the pre-deployed setting of the client machine and the **Use Default Browser for SAML Authentication** option is set to **No** in the portal configuration, end users will not have the best user experience. The app will open the default system browser for SAML authentication for the first time. Because the default browser values differ between the client machine and the portal, the app detects a mismatch and opens an embedded browser at the next login.

*The **Use Default Browser for SAML Authentication** option of the Globalprotect portal and the pre-deployed settings in the client machine must have the same value to provide the best user experience.*

- On Windows endpoints, you can use the System Center Configuration Manager (SCCM) to pre-deploy the GlobalProtect app 5.2 and set the **DEFAULTBROWSER** value to **yes** from the Windows Installer (Msiexec) using the following syntax:

  ```
  msiexec.exe /i GlobalProtect.msi DEFAULTBROWSER=YES
  ```

- On macOS endpoints, set the **default-browser** value to **yes** in the macOS plist (`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`) for the GlobalProtect app using the following syntax:

  ```
  sudo defaults write /Library/Preferences/
  com.paloaltonetworks.GlobalProtect.settings.plist '{"Palo
   Alto Networks" ={GlobalProtect={Settings={default-
  browser=yes;};};};}'
  ```

  You must specify the plist key to launch the default system browser for SAML authentication after GlobalProtect app 5.2 is installed.

  After you add the plist key, you must restart the GlobalProtect app in order for the plist key to take effect. After you restart the GlobalProtect app, the default system browser for SAML authentication launches. To restart the GlobalProtect app:

  - Launch the Finder.
  - Open the Applications folder:
    - From the Finder sidebar, select **Applications**. If you do not see **Applications** in the Finder sidebar, select **Go** > **Applications** from the Finder menu bar.
  - Open the Utilities folder.
  - Launch Terminal.
  - Execute the following commands:

    ```
    username>$ launchctl unload -S Aqua /Library/LaunchAgents/
    com.paloaltonetworks.gp.pangpa.plist
    username>$ launchctl unload -S Aqua /Library/LaunchAgents/
    com.paloaltonetworks.gp.pangps.plist
    ```

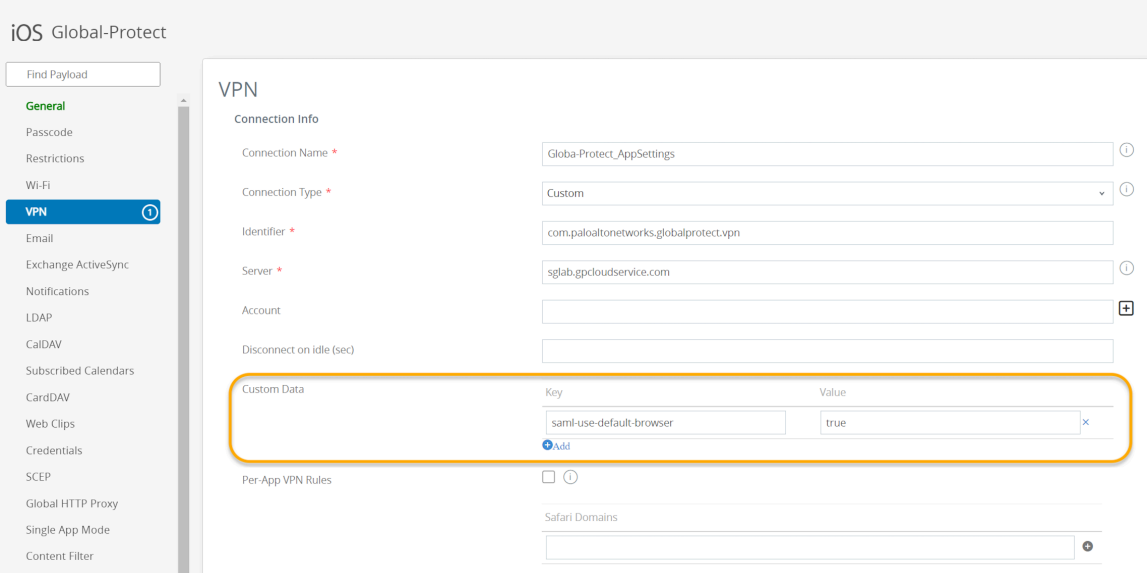


```
username>$ launchctl load -S Aqua /Library/LaunchAgents/
com.paloaltonetworks.gp.pangpa.plist
username>$ launchctl load -S Aqua /Library/LaunchAgents/
com.paloaltonetworks.gp.pangps.plist
```

- On Linux endpoints, set the **default-browser** value to **yes** in the `/opt/paloaltonetworks/globalprotect/pangps.xml` pre-deployment configuration file under `<Settings>`. After you add the **default-browser** value, follow the Deploy App Settings to Linux Endpoints before you reboot the Linux endpoint in order for the change to take effect.
- On Android and iOS endpoints, create a VPN profile by using the supported mobile device management system (MDM) such as Workspace ONE.
  - Log in to Workspace ONE UEM as an administrator.
  - Select an existing VPN profile (**Devices** > **Profiles & Resources** > **Profiles**) in the list.
  - Select **VPN** to add a VPN profile.

    On Android endpoints, enter the **Custom Data Key** (**use_default_browser_for_saml**). Enter the **Custom Data Value** (**true**).

    On iOS endpoints, enter the **Custom Data Key** (**saml-use-default-browser**). Enter the **Custom Data Value** (**true**).



  - Click **Save and Publish** to save your changes.

STEP 2 | Set Up SAML Authentication to authenticate users.

In order for the default system browser for SAML authentication to not open multiple tabs for each connection, we recommend that you configure an authentication override. For more information, see Cookie Authentication on the Portal or Gateway.

STEP 3 | Enable the GlobalProtect app so that end users can leverage the same login for GlobalProtect and their default system browser for SAML authentication.

1. Select **Network** > **GlobalProtect** > **Portals** > ***<portal-config>*** > **Agent** ***<agent-config>*** > **App** > **Use Default Browser for SAML Authentication**.
2. Select **Yes** to enable the GlobalProtect app to open the default system browser for SAML authentication.

   *If single-sign-on (SSO) is enabled, we recommend that you disable it. Set **Use Single Sign-On (Windows)** or **Use Single Sign-On (macOS)** to **No** to disable single sign-on when using the default system browser for SAML authentication.*

STEP 4 | Click **OK** twice.

STEP 5 | **Commit** the configuration.

STEP 6 | Verify that end users can successfully authenticate to the IdP using their saved credentials.

1. Select **Refresh Connection**, **Connect**, or **Enable** on the GlobalProtect app to initiate the connection.

   A new tab on the default browser of the system will open for SAML authentication.
2. Login using the username and password to authenticate on the IdP.
3. After end users can successfully authenticate on the IdP, click **Open GlobalProtect**.
4. Connect to the GlobalProtect app or other SAML-enabled applications without re-entering the user credentials.

Set Up Kerberos Authentication

Kerberos is a computer network authentication protocol that uses *tickets* to allow nodes that communicate over a non-secure network to prove their identity to one another in a secure manner. Kerberos SSO maintains a seamless logon experience by providing accurate User-ID information without user interaction. Networks that support Kerberos SSO require end users to log in only during initial network access. After the initial login, end users can access any Kerberos-enabled service in the network (such as webmail) without having to log in again until the SSO session expires (the SSO session duration is established by the Kerberos administrator). This authentication method helps identify users for user and HIP policy enforcement.

Kerberos authentication is supported on Windows (7, 8, and 10) and macOS (10.10 and later releases) endpoints. Kerberos authentication for macOS endpoints requires a minimum GlobalProtect app version of 4.1.0.

If you enable both Kerberos SSO and an Set Up External Authentication (such as RADIUS), GlobalProtect attempts SSO first. You can configure GlobalProtect to fall back to an external authentication service when SSO fails or you can configure GlobalProtect to use only Kerberos SSO for authentication.

In this implementation, the GlobalProtect portal and gateway act as Kerberos service principals and the GlobalProtect app acts as a user principal that authenticates end users with a Kerberos service ticket from the Key Distribution Center (KDC).

The following items must be in place for the GlobalProtect app for macOS endpoints to support Kerberos SSO:

- A Kerberos infrastructure, which includes a KDC with an authentication server (AS) and a ticket-granting service (TGS).

  The KDC must be reachable from the endpoints on which the GlobalProtect app is running. In most instances, the KDC is reachable only from inside the enterprise network, which means the GlobalProtect app can use Kerberos authentication only when the endpoint is internal. However, if the KDC is reachable from outside the enterprise network (from the Internet), the GlobalProtect app can use Kerberos authentication when the endpoint is external.

  If the user certificate store contains at least one certificate that is issued by the same CA as the certificate used for pre-logon tunnel establishment, you can also use Kerberos authentication with pre-logon to enable the GlobalProtect app to use Kerberos authentication when the endpoint is external.

  When an end user attempts to access protected network resources using Kerberos authentication, the AS grants the user a Ticket to Get Tickets (TGT), which is a service request used to generate service tickets from the TGS. The service ticket is then used to authenticate the end user and establish a service session.
- A Kerberos service account for each GlobalProtect portal and gateway.

  Service accounts are required for creating Kerberos keytabs, which are files that contain the principal name and password of each GlobalProtect portal or gateway.

STEP 1 | Create a Kerberos keytab file.

1. Log in to the KDC using your Kerberos service account credentials.
2. Open a command prompt and then enter the following command:

```
ktpass /princ <principal_name> /pass <password> /crypto
 <algorithm> /ptype KRB5_NT_PRINCIPAL /out <file_name>.keytab
```

*The **<principal_name>** and **<password>** are the principal name and password of the GlobalProtect portal or gateway. The **<algorithm>** must match the algorithm in the service ticket issued by the TGS, which is determined by the Kerberos administrator. If the GlobalProtect portal or gateway is running in FIPS or CC mode, the algorithm must be **aes128-cts-hmac-sha1-96** or **aes256-cts-hmac-sha1-96**. If the portal or gateway is not running in FIPS or CC mode, you can also use **des3-cbc-sha1** or **arcfour-hmac**.*

STEP 2 | Create a server profile for Kerberos authentication.

The server profile identifies the external authentication service and instructs the firewall on how to connect to that authentication service and access the authentication credentials for your users.

1. Select **Device** > **Server Profiles** > **Kerberos**, and then **Add** a Kerberos server profile.
2. Enter a **Profile Name**, such as **`GP-User-Auth`**.
3. If this profile is for a firewall with multiple virtual systems capability, select a virtual system or **Shared** as the **Location** where the profile is available.
4. Click **Add** in the **Servers** area, and then enter the following information for connecting to the authentication server:
   - Server **Name**
   - IP address or FQDN of the **Kerberos Server**
   - **Port**
5. Click **OK** to save the server profile.

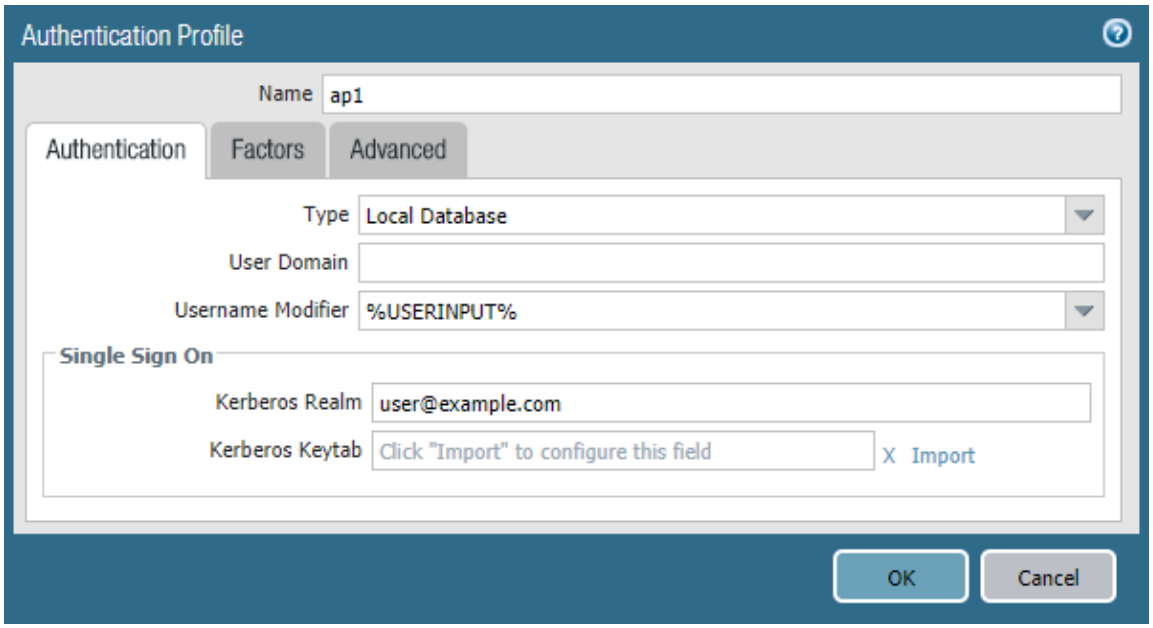
STEP 3 | (Optional) Create an authentication profile.

The authentication profile specifies the server profile that the portal or gateways use when they authenticate users. On a portal or gateway, you can assign one or more authentication profiles in one or more client authentication profile. For information on how an authentication

profile within a client authentication profile supports granular user authentication, see Configure a GlobalProtect Gateway and Set Up Access to the GlobalProtect Portal.

To enable users to connect and change their expired passwords without administrative intervention, consider using Remote Access VPN with Pre-Logon.

1. Select **Device** > **Authentication Profile**, and then **Add** a new profile.



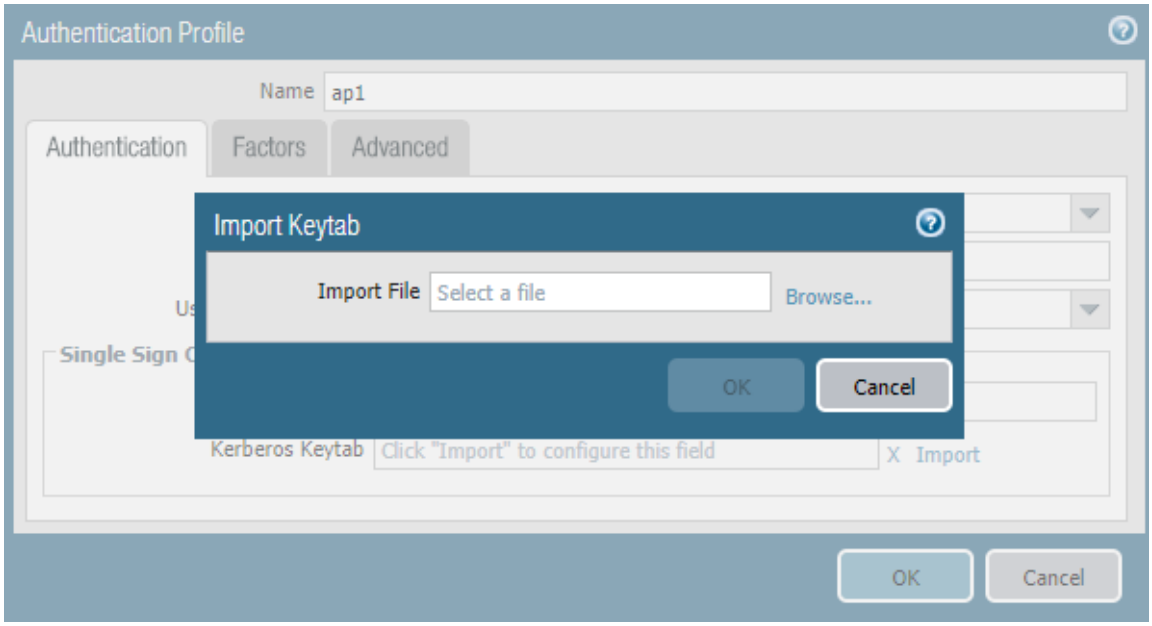
2. Enter a **Name** for the profile, and then select **Kerberos** as the authentication **Type**.
3. Select the Kerberos authentication **Server Profile** that you created in step 1.
4. Specify the **User Domain** and **Username Modifier**. The endpoint combines these values to modify the domain/username string that a user enters during login. The endpoint uses the modified string for authentication and the **User Domain** value for User-ID group mapping. Modifying user inputs is useful when the authentication service requires

domain/username strings in a particular format but you do not want to rely on users entering the domain correctly. You can select from the following options:

- To send the unmodified user input, leave the **User Domain** blank (default) and set the **Username Modifier** to the variable **%USERINPUT%** (default).
- To prepend a domain to the user input, enter a **User Domain** and set the **Username Modifier** to **%USERDOMAIN%\%USERINPUT%**.
- To append a domain to the user input, enter a **User Domain** and set the **Username Modifier** to **%USERINPUT%@%USERDOMAIN%**.

*If the **Username Modifier** includes the **%USERDOMAIN%** variable, the **User Domain** value replaces any domain string that the user enters. If the **User Domain** is blank, the device removes any user-entered domain string.*

5. Configure Kerberos single sign-on (SSO) if your network supports it.
   1. Enter the **Kerberos Realm** (up to 127 characters) to specify the hostname portion of the user login name. For example, the user account name user@EXAMPLE.LOCAL has the realm EXAMPLE.LOCAL.
   2. **Import** a **Kerberos Keytab** file. When prompted, **Browse** for the keytab file, and then click **OK**.



6. On the **Advanced** tab, **Add** an **Allow List** to select the users and user groups that are allowed to authenticate with this profile. The **all** option allows every user to authenticate with this profile. By default, the list has no entries, which means no users can authenticate.

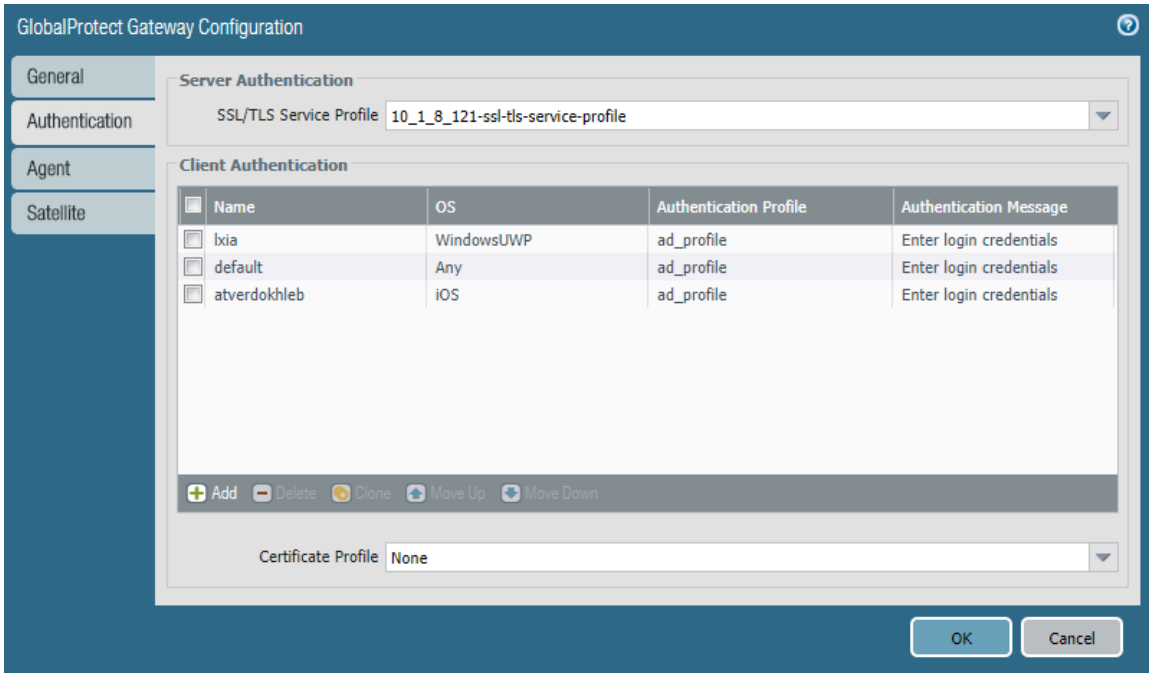
   During authentication, the endpoint first attempts to establish SSO using the keytab. If it is successful, and the user attempting access is in the **Allow List**, authentication succeeds immediately. Otherwise, the authentication process falls back to manual (username/password) authentication using the specified authentication **Type**. The **Type** does not have to be Kerberos. To change this behavior so users can authenticate using only

Kerberos, set **Use Default Authentication on Kerberos Authentication Failure** to **No** in the GlobalProtect portal agent configuration.

7. Click **OK**.

STEP 4 | Assign the authentication profile a gateway.

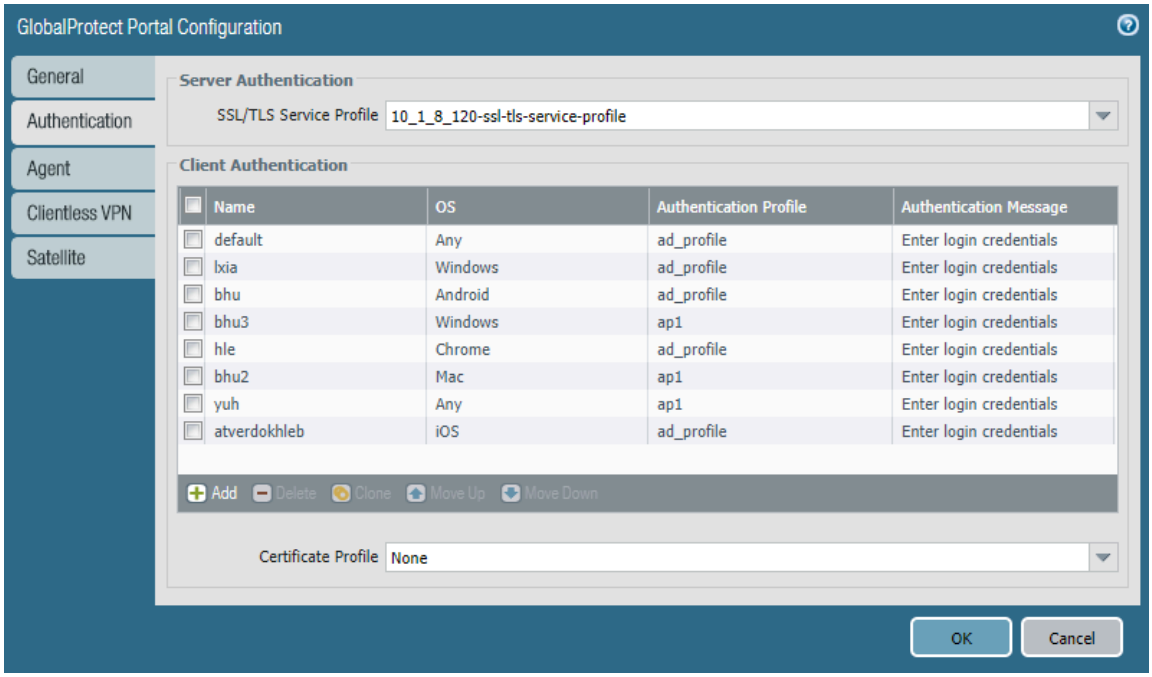
1. Select **Network** > **GlobalProtect** > **Gateways** to modify an existing gateway or **Add** a new one.



2. Select an existing **SSL/TLS Service Profile** for securing the gateway, or **Add** a new service profile (**Network** > **GlobalProtect** > **Gateways** > ***<gateway-config>*** > **Authentication**).
3. **Add** a **Client Authentication** configuration (**Network** > **GlobalProtect** > **Gateways** > ***<gateway-config>*** > **Authentication**), and then configure the following settings:
   - **Name**—Name of the client authentication configuration.
   - **OS**—Operating systems on which the gateway can be accessed.
   - **Authentication Profile**—Authentication profile to which your Kerberos keytab file was imported.
   - (Optional) **Username Label**—Custom username label for GlobalProtect gateway login.
   - (Optional) **Password Label**—Custom password label for GlobalProtect gateway login.
   - (Optional) **Authentication Message**—Message that is displayed when end users authenticate to the gateway.
4. Click **OK** to save your changes.

STEP 5 | Assign the authentication profile to the GlobalProtect portal.

1. Select **Network** > **GlobalProtect** > **Portals**.
2. Select an existing portal or **Add** a new one.



3. Select an existing **SSL/TLS Service Profile** for securing the portal, or **Add** a new service profile (**Network** > **GlobalProtect** > **Portals** > ***<portal-config>*** > **Authentication**).
4. **Add** a **Client Authentication** configuration (**Network** > **GlobalProtect** > **Portals** > ***<portal-config>*** > **Authentication**), and then configure the following settings:
   - **Name**—Name of the client authentication configuration.
   - **OS**—Operating systems on which the portal can be accessed.
   - **Authentication Profile**—Authentication profile to which your Kerberos keytab file is imported.
   - (Optional) **Username Label**—Custom username label for GlobalProtect portal login.
   - (Optional) **Password Label**—Custom password label for GlobalProtect portal login.
   - (Optional) **Authentication Message**—Message that is displayed when end users log in to the portal.
5. Click **OK** to save your changes.

STEP 6 | Commit the configuration.

Click **Commit**.

Set Up RADIUS or TACACS+ Authentication

RADIUS is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. TACACS+ is a well-established authentication protocol, common to UNIX networks, that allows a remote access server to forward a user's login password to an authentication server to determine whether access can be allowed to a given system.

STEP 1 | Create a server profile.

The server profile identifies the external authentication service and instructs the firewall how to connect to that authentication service and access the authentication credentials for your users.

If you want to Enable Delivery of VSAs to a RADIUS Server, you must create a RADIUS server profile.

1. Select **Device** > **Server Profiles**, and then select the profile type (**RADIUS** or **TACACS+**).
2. **Add** a new RADIUS or TACACS+ server profile.
3. Enter a **Profile Name**, such as **`GP-User-Auth`**.
4. If this profile is for a firewall with multiple virtual systems capability, select a virtual system or **Shared** as the **Location** where the profile is available.
5. Configure the following **Server Settings**:
   - **Timeout (sec)**—The number of seconds before a server connection request times out due to lack of response from the authentication server.
   - **Authentication Protocol**—The protocol used to connect to the authentication server. Options include **CHAP**, **PAP**, **PEAP-MSCHAPv2**, **PEAP with GTC**, or **EAP-TTLS with PAP**.

     *If you configure **PEAP-MSCHAPv2** (Protected Extensible Authentication Protocol Microsoft Challenge Handshakie Authentication Protocol version 2) as the authentication protocol, remote users can change their RADIUS or Active Directory (AD) passwords through the GlobalProtect app when their password expires or a RADIUS/AD administrator requires a password change at the next login.*
   - (RADIUS Only) **Retries**—The number of times the firewall attempts to connect to the authentication server before dropping the request.
   - (TACACS+ only) **Use single connection for all authentication**—Option that allows all TACACS+ authentication requests to occur over a single TCP session rather than separate sessions for each request.
6. Click **Add** in the **Servers** area, and then enter the following information for connecting to the authentication server:
   - **Name**
   - **RADIUS** or **TACACS+ Server** (IP address or FQDN of the server)
   - **Secret** (shared secret that enables the authentication service to authenticate the firewall)
   - **Port**
7. Click **OK** to save the server profile.

STEP 2 | (Optional) Create an authentication profile.

The authentication profile specifies the server profile that the portal or gateways use when they authenticate users. On a portal or gateway, you can assign one or more authentication profiles in one or more client authentication profiles. For information on how an authentication

profile within a client authentication profile supports granular user authentication, see Configure a GlobalProtect Gateway and Set Up Access to the GlobalProtect Portal.

To enable users to connect and change their own expired passwords without administrative intervention, consider using Remote Access VPN with Pre-Logon.

1. Select **Device** > **Authentication Profile**, and then **Add** a new profile.
2. Enter a **Name** for the profile.
3. Select the **Authentication Type** (**RADIUS** or **TACACS+**).
4. Select the RADIUS or TACACS+ authentication **Server Profile** that you created in step 1 from the drop-down.
5. (RADIUS only) Enable **Retrieve user group from RADIUS** if you want to include this information in the authentication profile.
6. Specify the **User Domain** and **Username Modifier**. The endpoint combines these values to modify the domain/username string that a user enters during login. The endpoint uses the modified string for authentication and the **User Domain** value for User-ID group mapping. Modifying user inputs is useful when the authentication service requires domain/username strings in a particular format and but you do not want to rely on users entering the domain correctly. You can select from the following options:
   - To send the unmodified user input, leave the **User Domain** blank (the default) and set the **Username Modifier** to the variable **%USERINPUT%** (the default).
   - To prepend a domain to the user input, enter a **User Domain** and set the **Username Modifier** to **%USERDOMAIN%\%USERINPUT%**.
   - To append a domain to the user input, enter a **User Domain** and set the **Username Modifier** to **%USERINPUT%@%USERDOMAIN%**.

   *If the **Username Modifier** includes the **%USERDOMAIN%** variable, the **User Domain** value replaces any domain string that the user enters. If the **User Domain** is blank, the device removes any user-entered domain string.*
7. On the **Advanced** tab, **Add** an **Allow List** to select the users and user groups that are allowed to authenticate with this profile. The **all** option allows every user to authenticate with this profile. By default, the list has no entries, which means no users can authenticate.
8. Click **OK**.

STEP 3 | **Commit** the configuration.

Set Up Client Certificate Authentication

With the optional client certificate authentication, the user presents a client certificate along with a connection request to the GlobalProtect portal or gateway. The portal or gateway can use either a shared or unique client certificate to validate that the user or endpoint belongs to your organization.

- To authenticate the user, one of the certificate fields, such as the Subject Name field, must identify the username.
- To authenticate the endpoint, the Subject field of the certificate must identify the device type instead of the username. (With the pre-logon connect methods, the portal or gateway authenticates the endpoint before the user logs in.)

*If you configure the portal or gateway to authenticate users through client certificate authentication, users will not have the option to **Sign Out** of the GlobalProtect app if they authenticate successfully using only a client certificate.*

For an agent configuration profile that specifies client certificates, each user receives a client certificate. The mechanism for providing the certificates determines whether a certificate is unique to each user or the same for all users under that agent configuration:

- To deploy client certificates that are unique to each user and endpoint, use **SCEP**. When a user first logs in, the portal requests a certificate from the enterprise's PKI. The portal obtains a unique certificate and deploys it to the endpoint.
- To deploy the same client certificate to all users that receive an agent configuration, deploy a certificate that is **Local** to the firewall.

Use an optional certificate profile to verify the client certificate that the endpoint presents with a connection request. The certificate profile specifies the contents of the username and user domain fields; lists CA certificates; criteria for blocking a session; and offers ways to determine the revocation status of CA certificates. Because the certificate is part of the authentication of the endpoint or user for a new session, you must pre-deploy certificates used in certificate profiles to the endpoints before the users' initial portal login.

The certificate profile specifies which certificate field contains the username. If the certificate profile specifies Subject in the Username Field, the certificate presented by the endpoint must contain a common-name for the endpoint to connect. If the certificate profile specifies a Subject-Alt with an Email or Principal Name as the Username Field, the certificate from the endpoint must contain the corresponding fields, which will be used as the username when the GlobalProtect app authenticates to the portal or gateway.

GlobalProtect also supports authentication by common access cards (CACs) and smart cards, which rely on a certificate profile. With these cards, the certificate profile must contain the root CA certificate that issued the certificate to the smart card or CAC.

If you specify client certificate authentication, you should not configure a client certificate in the portal configuration because the endpoint provides it when the user connects. For an example of how to configure client certificate authentication, see Remote Access VPN (Certificate Profile).

The methods for deploying client certificates depend on the security requirements for your organization:

- Deploy Shared Client Certificates for Authentication
- Deploy Machine Certificates for Authentication
- Deploy User-Specific Client Certificates for Authentication
- Enable Certificate Selection Based on OID

Deploy Shared Client Certificates for Authentication

To confirm that an endpoint user belongs to your organization, you can use the same client certificate for all endpoints or generate separate certificates to deploy with a particular agent configuration. Use this workflow to issue self-signed client certificates and deploy them from the portal.

If you include a client certificate in the portal configuration for mobile devices, you can only use client certificate authentication in the gateway configuration because the client certificate passphrase is saved in the portal configuration. Additionally, the client certificate can only be used after the certificate is retrieved from the portal configuration.

STEP 1 | Generate a certificate to deploy to multiple GlobalProtect endpoints.

1. Create the root CA certificate for issuing self-signed certificates for the GlobalProtect components.
2. Select **Device** > **Certificate Management** > **Certificates** > **Device Certificates**, and then **Generate** a new certificate.
3. Set the **Certificate Type** to **Local** (default).
4. Enter a **Certificate Name**. This name cannot contain spaces.
5. Enter a **Common Name** to identify this certificate as an app certificate (for example, **`GP_Windows_App`**). Because this certificate will be deployed to all apps using the same agent configuration, it does not need to uniquely identify a specific user or endpoint.
6. In the **Signed By** field, select your root CA.
7. Select an **OCSP Responder** to verify the revocation status of certificates.
8. Click **OK** to generate the certificate.

STEP 2 | Set Up Two-Factor Authentication.

Configure authentication settings in a GlobalProtect portal agent configuration to enable the portal to transparently deploy the client certificate, which is **Local** to the firewall, to apps that receive the configuration.

Deploy Machine Certificates for Authentication

To confirm that the endpoint belongs to your organization, use your own public-key infrastructure (PKI) to issue and distribute machine certificates to each endpoint (recommended) or generate a self-signed machine certificate for export. With the pre-logon connect methods, a machine certificate is required and must be installed on the endpoint before GlobalProtect components grant access.

To confirm that the endpoint belongs to your organization, you must also configure an authentication profile to authenticate the user (see Set Up Two-Factor Authentication).

Use the following workflow to create the client certificate and manually deploy it to an endpoint. For more information, see GlobalProtect User Authentication. For an example configuration, see Remote Access VPN (Certificate Profile).

STEP 1 | Issue client certificates to GlobalProtect apps and endpoints.

This enables the GlobalProtect portal and gateways to validate that the endpoint belongs to your organization.

1. Create the root CA certificate for issuing self-signed certificates for the GlobalProtect components.
2. Select **Device** > **Certificate Management** > **Certificates** > **Device Certificates**, and then click **Generate**.
3. Enter a **Certificate Name**. The certificate name cannot contain any spaces.
4. Enter the IP address or FQDN that will appear on the certificate in the **Common Name** field.
5. Select your root CA from the **Signed By** drop-down.
6. Select an **OCSP Responder** to verify the revocation status of certificates.
7. Configure the **Cryptographic Settings** for the certificate, including the encryption **Algorithm**, key length (**Number of Bits**), **Digest** algorithm (use sha1, sha256, sha384, or sha512), and **Expiration** (in days) for the certificate.

   If the firewall is in FIPS-CC mode and the key generation algorithm is RSA, the RSA keys must be 2,048 bits or 3072 bits.
8. In the **Certificate Attributes** area, **Add** and define the attributes that uniquely identify the endpoints as belonging to your organization. Keep in mind that if you add a **Host Name** attribute (which populates the SAN field of the certificate), it must be the same as the **Common Name** value you defined.
9. Click **OK** to generate the certificate.

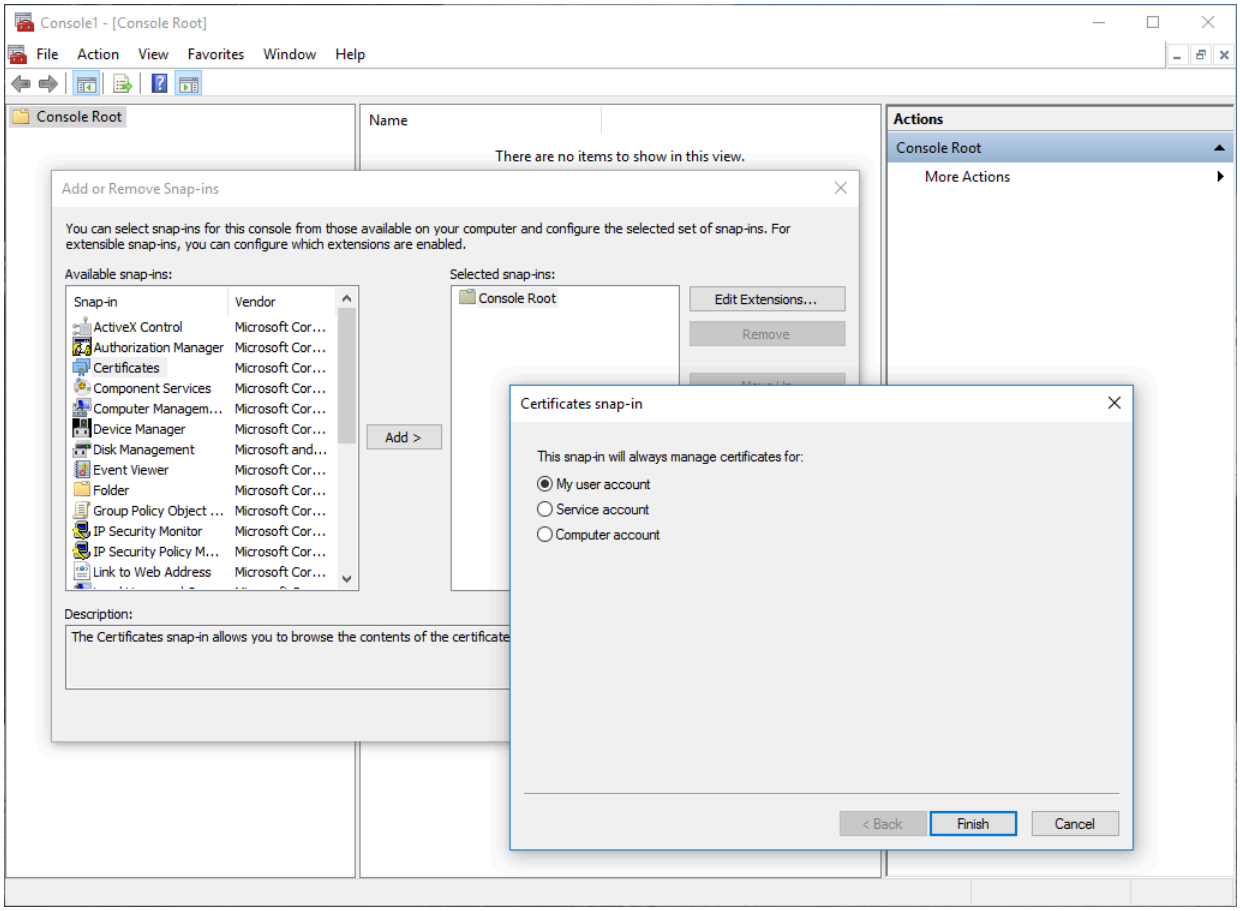
STEP 2 | Install certificates in the personal certificate store on the endpoints.

If you are using unique user certificates or machine certificates, you must install each certificate in the personal certificate store on the endpoint prior to the first portal or gateway connection. Install machine certificates to the Local Computer certificate store on Windows

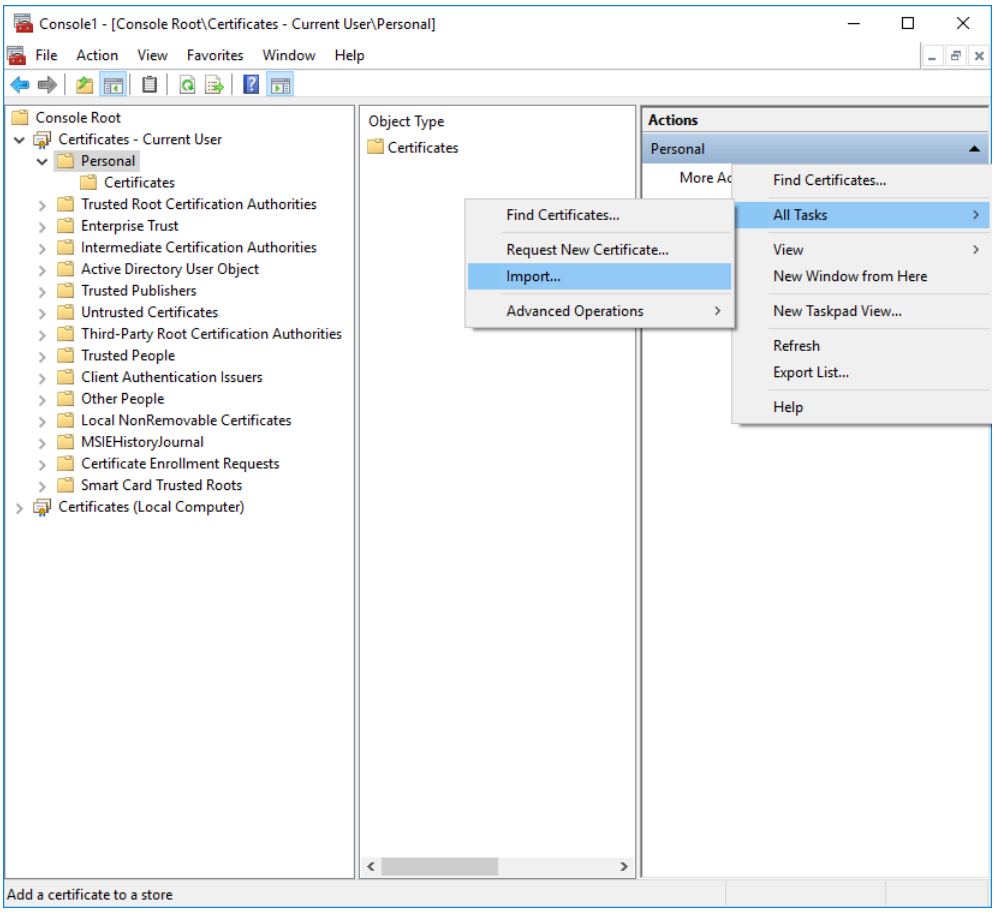
and in the System Keychain on macOS. Install user certificates to the Current User certificate store on Windows and in the Keychain on macOS.

For example, to install a certificate on a Windows system using the Microsoft Management Console:

1. From the command prompt, enter `mmc` to launch the Microsoft Management Console.
2. Select **File** > **Add/Remove Snap-in**.
3. From the list of **Available snap-ins**, select **Certificates**, and then **Add** and select one of the following certificate snap-ins, depending on what type of certificate you are importing:
   - **Computer account**—Select this option if you are importing a machine certificate.
   - **My user account**—Select this option if you are importing a user certificate.



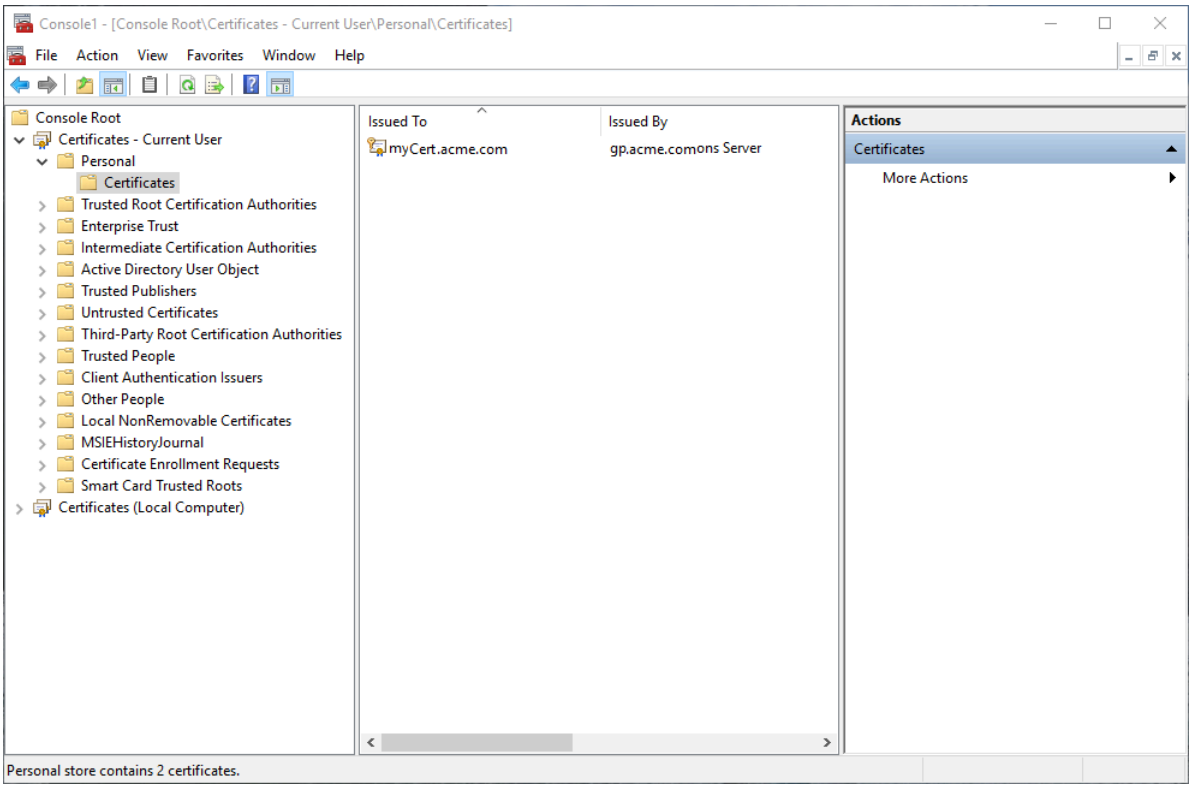
4. From the **Console Root**, expand **Certificates**, and then select **Personal**.
5. In the **Actions** column, select **Personal** > **More Actions** > **All Tasks** > **Import** and follow the steps in the Certificate Import Wizard to import the PKCS file you received from the CA.



6. **Browse** to and select the .p12 certificate file to import (select **Personal Information Exchange** as the file type to browse for) and enter the **Password** that you used to encrypt the private key. Set the **Certificate store** to **Personal**.

STEP 3 | Verify that the certificate has been added to the personal certificate store.

Navigate to the personal certificate store from the **Console Root** (**Certificates** > **Personal** > **Certificates**:



STEP 4 | Import the root CA certificate used to issue the client certificates onto the firewall.

This step is required only if an external CA issued the client certificates, such as a public CA or an enterprise PKI CA. If you are using self-signed certificates, the root CA is already trusted by the portal and gateways.

1. Download the root CA certificate used to issue the client certificates (Base64 format).
2. Import the root CA certificate from the CA that generated the client certificates onto the firewall:
   1. Select **Device** > **Certificate Management** > **Certificates** > **Device Certificates** and click **Import**
   2. Set the **Certificate Type** to **Local** (default).
   3. Enter a **Certificate Name** that identifies the certificate as your client CA certificate.
   4. **Browse** to and select the **Certificate File** you downloaded from the CA.
   5. Set the **File Format** to **Base64 Encoded Certificate (PEM)**, and then click **OK**.
   6. On the **Device Certificates** tab, select the certificate you just imported to open the Certificate Information.
   7. Select **Trusted Root CA** and then click **OK**.

STEP 5 | Create a client certificate profile.

1. Select **Device** > **Certificates** > **Certificate Management** > **Certificate Profile** to **Add** a new certificate profile.
2. Enter a profile **Name**.
3. Select a **Username Field** value to specify which field in the certificate will contain the user's identification information.

   If you plan to configure the portal or gateways to authenticate users with only certificates, you must specify the **Username Field**. This enables GlobalProtect to associate a username with the certificate.

   If you plan to set up the portal or gateway for two-factor authentication, you can leave the default value of **None**, or, to add an additional layer of security, specify a username. If you specify a username, your external authentication service verifies that the username in the client certificate matches the username requesting authentication. This ensures that the user is the one to which the certificate was issued.

   Users cannot change the username that is included in the certificate.
4. In the **CA Certificates** area, click **Add**. Select the Trusted Root CA certificate you imported in step 4 from the **CA Certificate** drop-down, and then click **OK**.

STEP 6 | Save the configuration.

Commit the changes.

Deploy User-Specific Client Certificates for Authentication

To authenticate individual users, you must issue a unique client certificate to each GlobalProtect user and deploy the client certificate to the endpoints prior to enabling GlobalProtect. To automate the generation and deployment of user-specific client certificates, you can configure your GlobalProtect portal to act as a Simple Certificate Enrollment Protocol (SCEP) client to a SCEP server in your enterprise PKI.

If you include a client certificate in the portal configuration for mobile devices, you can only use client certificate authentication in the gateway configuration because the client certificate passphrase is saved in the portal configuration. Additionally, the client certificate can only be used after the certificate is retrieved from the portal configuration.

SCEP operation is dynamic in that the enterprise PKI generates a user-specific certificate when the portal requests it and sends the certificate to the portal. The portal then deploys the certificate to the app transparently. When a user requests access, the app can then present the client certificate to authenticate with the portal or gateway.

The GlobalProtect portal or gateway uses identifying information about the endpoint and the user to evaluate whether to permit access to the user. GlobalProtect blocks access if the host ID is on a device block list or if the session matches any blocking options specified in a certificate profile. If authentication fails due to an invalid SCEP-based client certificate, the GlobalProtect app tries to authenticate with the portal (based on the settings in the authentication profile) and retrieve the certificate. If the app cannot retrieve the certificate from the portal, the endpoint is not able to connect.

STEP 1 | Create a SCEP profile.

1. Select **Device** > **Certificate Management** > **SCEP**, and then **Add** a new SCEP profile.
2. Enter a **Name** to identify the SCEP profile.
3. If this profile is for a firewall with multiple virtual systems capability, select a virtual system or **Shared** as the **Location** where the profile is available.

STEP 2 | (Optional) To make the SCEP-based certificate generation more secure, configure a SCEP challenge-response mechanism between the PKI and portal for each certificate request.

After you configure this mechanism, its operation is invisible, and no further input is necessary.

To comply with the U.S. Federal Information Processing Standard (FIPS), use a **Dynamic SCEP Challenge** and specify a **Server URL** that uses HTTPS (see step 7).

Select one of the following **SCEP Challenge** options:

- **None**—(Default) The SCEP server does not challenge the portal before it issues a certificate.
- **Fixed**—Enter the enrollment challenge **Password** obtained from the SCEP server in the PKI infrastructure.
- **Dynamic**—Enter a **Username** and **Password** of your choice (possibly the credentials of the PKI administrator) and the SCEP **Server URL** where the portal-client submits these credentials. The credentials are used to authenticate with the SCEP server, which transparently generates an OTP password for the portal upon each certificate request (you can see this OTP change after a screen refresh in `The enrollment challengepassword is` field after each certificate request). The PKI transparently passes each new password to the portal, which then uses the password for its certificate request.

STEP 3 | Specify the connection settings between the SCEP server and the portal to enable the portal to request and receive client certificates.

You can include additional information about the endpoint or user by specifying tokens in the **Subject** name of the certificate.

In the **Subject** field of the CSR to the SCEP server, the portal includes the token value as **CN** and Host-ID as **SerialNumber**. The host ID varies by endpoint type: GUID (Windows), MAC address of the interface (macOS), Android ID (Android endpoints), UDID (iOS endpoints), or a unique name that GlobalProtect assigns (Chrome).

1. In the **Configuration** area, enter the **Server URL** that the portal uses to reach the SCEP server in the PKI (for example, `http://10.200.101.1/certsrv/mscep/`).
2. Enter a **CA-IDENT Name** (up to 255 characters in length) to identify the SCEP server.
3. Enter the **Subject** name to use in the certificates generated by the SCEP server. The subject must be a distinguished name in the **<attribute>=<value>** format and

must include a common name (CN) attribute (CN=<**variable**>). The CN supports the following dynamic tokens:

- $USERNAME—Use this token to enable the portal to request certificates for a specific user. To use this variable, you must also Enable Group Mapping. The username entered by the user must match the name in the user-group mapping table.
- $EMAILADDRESS—Use this token to request certificates associated with a specific email address. To use this variable, you must also Enable Group Mapping and configure the **Mail Attributes** in the **Mail Domains** area of the server profile. If GlobalProtect cannot identify an email address for the user, it generates a unique ID and populates the CN with that value.
- $HOSTID—To request certificates for the endpoint only, specify the host ID token. When a user attempts to log in to the portal, the endpoint sends identifying information that includes its host ID value.

When the GlobalProtect portal pushes the SCEP settings to the app, the CN portion of the subject name is replaced with the actual value (username, host ID, or email address) of the certificate owner (for example, **O=acme,CN=johndoe**).

4. Select the **Subject Alternative Name Type**:
   - **RFC 822 Name**—Enter the email name in a certificate's subject or Subject Alternative Name extension.
   - **DNS Name**—Enter the DNS name used to evaluate certificates.
   - **Uniform Resource Identifier**—Enter the name of the resource from which the app will obtain the certificate.
   - **None**—Do not specify attributes for the certificate.

STEP 4 | (Optional) Configure **Cryptographic Settings** for the certificate.

- Select the **Number of Bits** (key length) for the certificate.

  If the firewall is in FIPS-CC mode and the key generation algorithm is RSA. The RSA keys must be 2,048 bits or larger.
- Select the **Digest for CSR** which indicates the digest algorithm for the certificate signing request (CSR): sha1, sha256, sha384, or sha512.

STEP 5 | (Optional) Configure the permitted uses of the certificate, either for signing or encryption.

- To use this certificate for signing, select the **Use as digital signature** check box. This option enables the endpoint to use the private key in the certificate to validate a digital signature.
- To use this certificate for encryption, select the **Use for key encipherment** check box. This option enables the app to use the private key in the certificate to encrypt data exchanged over the HTTPS connection established with the certificates issued by the SCEP server.

STEP 6 | (Optional) To ensure that the portal is connecting to the correct SCEP server, enter the **CA Certificate Fingerprint**. Obtain this fingerprint from the **Thumbprint** field of the SCEP server interface.

1. Enter the URL for the SCEP server's administrative UI (for example, **http://<hostname or IP>/CertSrv/mscep_admin/**).
2. Copy the thumbprint and enter it in the **CA Certificate Fingerprint** field.

STEP 7 | Enable mutual SSL authentication between the SCEP server and the GlobalProtect portal. This is required to comply with the U.S. Federal Information Processing Standard (FIPS).

FIPS-CC operation is indicated on the firewall login page and its status bar.

Select the SCEP server's root **CA Certificate**. Optionally, you can enable mutual SSL authentication between the SCEP server and the GlobalProtect portal by selecting a **Client Certificate**.

STEP 8 | Save and commit the configuration.

1. Click **OK** to save the settings.
2. **Commit** the configuration.

The portal attempts to request a CA certificate using the settings in the SCEP profile, and then saves it to the firewall hosting the portal. If successful, the CA certificate is shown in **Device** > **Certificate Management** > **Certificates**.

STEP 9 | (Optional) If the portal fails to obtain the certificate after saving the SCEP profile, you can manually generate a certificate signing request (CSR) from the portal.

1. Select **Device** > **Certificate Management** > **Certificates** > **Device Certificates**, and then **Generate** a new certificate.
2. Select **SCEP** as the **Certificate Type**.
3. Enter a **Certificate Name**. This name cannot contain spaces.
4. Select the **SCEP Profile** to use to submit a CSR to your enterprise PKI.
5. Click **OK** to submit the request and generate the certificate.

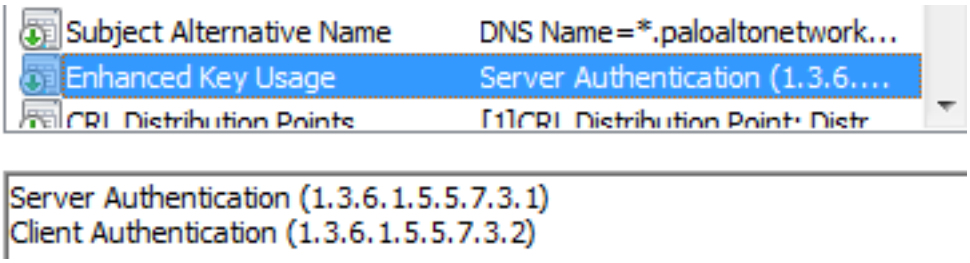
STEP 10 | Set Up Two-Factor Authentication.

Assign the SCEP profile a GlobalProtect portal agent configuration to enable the portal to transparently request and deploy client certificates to apps that receive the configuration.

Enable Certificate Selection Based on OID

If you deploy multiple certificates to your end user devices for distinct use cases--for example machine certificates, user certificates, and email encryption certificates all issued by the same certificate authority--it can be difficult to distinguish which certificate to use in which use case. To help with this, you can designate a specific object identifier (OID) that you want GlobalProtect to use to identify which certificate to use. This simplifies and improves the certificate selection process when your macOS or Windows endpoints have multiple certificates installed.

An OID is a numeric value that identifies the application or service for which a certificate is used. When the certificate authority (CA) creates the certificate, the CA automatically includes the OID in the Enhanced Key Usage field.



When you create the certificate, you can specify the OID to identify the certificate's purpose. By default, GlobalProtect automatically filters the certificates for those that specify a Client Authentication purpose (OID 1.3.6.1.5.5.7.3.2) so it is not necessary to specify the OID associated with Client Authentication. However, if you want to use a different OID to distinguish the certificate you want GlobalProtect to select, you can specify a different certificate usage when you create the certificate and then instruct GlobalProtect to select the certificate with the corresponding OID. Some of the most commonly used OIDs are:

- 1.3.6.1.5.5.7.3.1—Server Authentication
- 1.3.6.1.5.5.7.3.3—Code Signing
- 1.3.6.1.5.5.7.3.4—Email Protection
- 1.3.6.1.5.5.7.3.5—IPSec End System
- 1.3.6.1.5.5.7.3.6—IPSec Tunnel
- 1.3.6.1.5.5.7.3.7—IPSec User
- 1.3.6.1.5.5.7.3.8—Time Stamping
- 1.3.6.1.5.5.7.3.9—OCSP Signing

For example, say your endpoints have four client certificates installed, but the one you want your users to select has the OID 1.3.6.1.5.5.7.3.1. Rather than having the GlobalProtect app to present all four client certificates to the user, you can specify the **Extended Key Usage OID** in the Customize the GlobalProtect App for the users whose endpoints have multiple client certificates. Keep in mind that if multiple client certificates on the endpoint have the matching OID, GlobalProtect will prompt the user to select the client certificate from the filtered list.

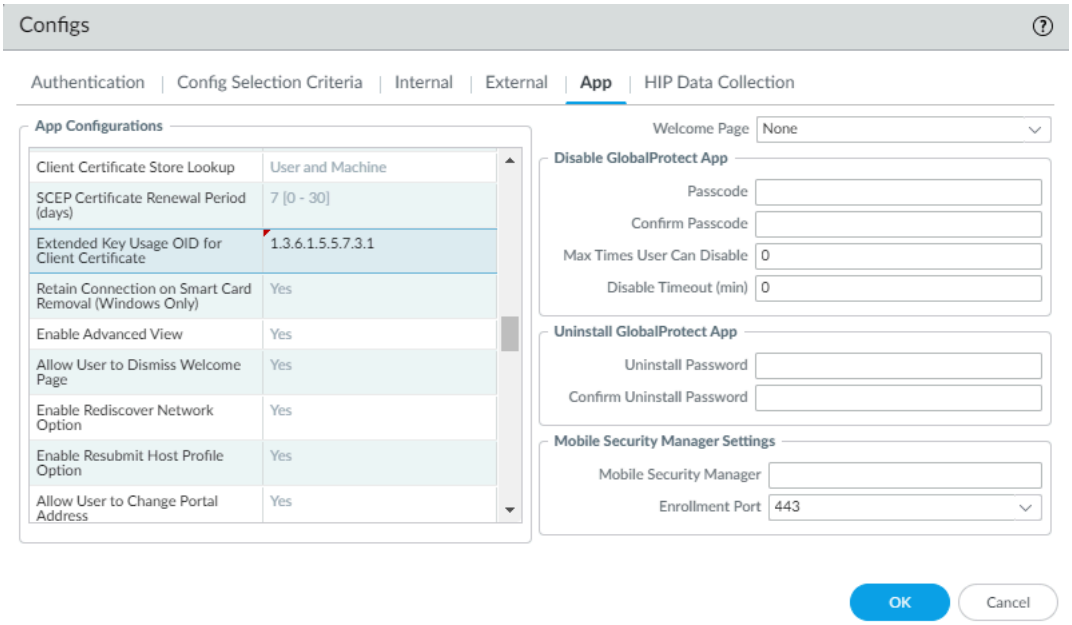
GlobalProtect uses only the Extended Key Usage OID field of the certificate and does not evaluate any other certificate fields such as Subject Name to determine whether to present the certificates. Note that the Extended Key Usage OID value is different from the Certificate Template Information OID. For other certificate selection requirements, see How Does the App Know Which Certificate to Supply?

To configure the OID as a requirement for certificate selection:

STEP 1 | (Optional) Create or edit the client certificate and note the associated OID.

1. Open the Certificate Templates snap-in.
2. In the Details pane, create or edit the certificate template you want to modify, and then click Properties.
3. On the **Extensions** tab, select **Application Policies** > **Edit**.
4. In the Edit Application Policies Extension dialog box, click **Add**.
5. In Add Application Policy, ensure that the application you are creating does not exist, and then click **New**.
6. In the New Application Policy dialog box, provide the name for the new application policy (for example GlobalProtect Authentication).
7. Note the generated object identifier, and then click **OK**.

STEP 2 | Specify the certificate's object identifier (OID) in the Extended Key Usage OID field as part of the appropriate Customize the GlobalProtect App.



Set Up Two-Factor Authentication

If you require strong authentication to protect sensitive assets or comply with regulatory requirements, such as PCI, SOX, or HIPAA, configure GlobalProtect to use an authentication service that uses a two-factor authentication scheme. A two-factor authentication scheme requires two things: something the end user knows (such as a PIN or password) and something the end user has (a hardware or software token/OTP, smart card, or certificate). You can also enable two-factor authentication using a combination of external authentication services, and client and certificate profiles.

Two-factor authentication supports Remote Access VPN with Pre-Logon *with GlobalProtect app 5.0 and later releases.*

The following topics provide examples on how to set up two-factor authentication on GlobalProtect:

- Enable Two-Factor Authentication Using Certificate and Authentication Profiles
- Enable Two-Factor Authentication Using One-Time Passwords (OTPs)
- Enable Two-Factor Authentication Using Smart Cards
- Enable Two-Factor Authentication Using a Software Token Application

Enable Two-Factor Authentication Using Certificate and Authentication Profiles

The following workflow describes how to configure GlobalProtect to require users to authenticate to both a certificate profile and an authentication profile. The user must successfully authenticate using both methods in order to connect to the portal/gateway. For more details on this configuration, see Remote Access VPN with Two-Factor Authentication.

If the certificate profile specifies a **Username Field**, from which GlobalProtect can obtain a username, the external authentication service automatically uses that username to authenticate the user to the external authentication service specified in the authentication profile. For example, if the **Username Field** in the certificate profile is set to **Subject**, the common-name field value of the certificate is used as the username when the authentication server tries to authenticate the user. If you do not want to force users to authenticate with a username from the certificate, make sure the **Username Field** in the certificate profile is set to **None**. See Remote Access VPN with Two-Factor Authentication for an example configuration.

STEP 1 | Create an authentication server profile.

The authentication server profile determines how the firewall connects to an external authentication service and retrieves the authentication credentials for your users.

If you are using LDAP to connect to Active Directory (AD), you must create a separate LDAP server profile for every AD domain.

1. Select **Device** > **Server Profiles** and a profile type (**LDAP**, **Kerberos**, **RADIUS**, or **TACACS+**).
2. **Add** a new server profile.
3. Enter a **Profile Name**, such as **`gp-user-auth`**.
4. (LDAP Only) Select the LDAP server **Type** (**active-directory**, **e-directory**, **sun**, or **other**).
5. Click **Add** in the **Servers** or **Servers List** area (depending on the type of server profile), and then enter the following information for connections to the authentication service:
   - **Name** of the server
   - IP address of FQDN of the **Server**
   - **Port**
6. (RADIUS, TACACS+, and LDAP only) Specify the following settings to enable the firewall to authenticate to the authentication service:
   - RADIUS and TACACS+—Enter the shared **Secret** when adding the server entry.
   - LDAP—Enter the **Bind DN** and **Password**.
7. (LDAP only) If you want the endpoint to use SSL or TLS for a more secure connection with the directory server, enable the option to **Require SSL/TLS secured connection** (enabled by default). The protocol that the endpoint uses depends on the server **Port** in the **Server list**:
   - 389 (default)—TLS (specifically, the endpoint uses the StartTLS operation to upgrade the initial plaintext connection to TLS).
   - 636—SSL.
   - Any other port—The endpoint first attempts to use TLS. If the directory server does not support TLS, the endpoint uses SSL.
8. (LDAP only) For additional security, enable the option to **Verify Server Certificate for SSL sessions** so that the endpoint verifies the certificate that the directory server presents for SSL/TLS connections. To enable verification, you also must enable the option to **Require SSL/TLS secured connection**. In order for verification to succeed, one of the following conditions must be true:
   - The certificate is in the list of device certificates: **Device** > **Certificate Management** > **Certificates** > **Device Certificates**. Import the certificate into the endpoint if necessary.
   - The certificate signer is in the list of trusted certificate authorities: **Device** > **Certificate Management** > **Certificates** > **Default Trusted Certificate Authorities**.
9. Click **OK** to save the server profile.

STEP 2 | Create an authentication profile that identifies the service for authenticating users. You later have the option of assigning the profile on the portal and gateways.

1. Select **Device** > **Authentication Profile**, and then **Add** a new profile.
2. Enter a **Name** for the profile.
3. Select the **Authentication Type**.
4. Select the **Server Profile** you created in step 1.
5. (LDAP Only) Enter **sAMAccountName** as the **Login Attribute**.
6. Click **OK** to save the authentication profile.

STEP 3 | Create a client certificate profile that the portal uses to authenticate the client certificates that come from user endpoints.

When you configure two-factor authentication to use client certificates, the external authentication service uses the username value to authenticate the user, if specified, in the client certificate. This ensures that the user who is logging is in is actually the user to whom the certificate was issued.

1. Select **Device** > **Certificate Management** > **Certificate Profile**, and then **Add** a new certificate profile.
2. Enter a **Name** for the profile.
3. Select one of the following **Username Field** values:
   - If you intend for the client certificate to authenticate individual users, select the certificate field that identifies the user.
   - If you are deploying the client certificate from the portal, select **None**.
   - If you are setting up a certificate profile for use with a pre-logon connect method, select **None**.
4. **Add** the **CA Certificates** that you want to assign to the profile, and then configure the following settings:
   1. Select the **CA certificate**, either a trusted root CA certificate or the CA certificate from a SCEP server. If necessary, import the certificate.
   2. (Optional) Enter the **Default OCSP URL**.
   3. (Optional) Select a certificate for **OCSP Verify Certificate**.
   4. (Optional) Enter the **Template Name** for the template that was used to sign the certificate.
5. (Optional) Select the following options to specify when to block the user's requested session:
   1. Status of certificate is unknown.
   2. GlobalProtect component does not retrieve certificate status within the number of seconds in **Certificate Status Timeout**.
   3. Serial number attribute in the subject of a client certificate does not match the host ID that the GlobalProtect app reports for the endpoint.
   4. Certificates have expired.
6. Click **OK**.

STEP 4 | (Optional) Issue client certificates to GlobalProtect clients and endpoints.

To deploy client certificates transparently, configure your portal to distribute a shared client certificate to your endpoints or configure the portal to use SCEP to request and deploy unique client certificates for each user.

1. Use your enterprise PKI or a public CA to issue a client certificate to each GlobalProtect user.
2. For the pre-logon connect methods, install certificates in the personal certificate store on the endpoint.

STEP 5 | Save the GlobalProtect configuration.

Click **Commit**.

Enable Two-Factor Authentication Using One-Time Passwords (OTPs)

Use this workflow to configure two-factor authentication using one-time passwords (OTPs) on the portal and gateways. When a user requests access, the portal or gateway prompts the user to enter an OTP. The authentication service sends the OTP as a token to the user's RSA device.

Setting up a two-factor authentication scheme is similar to setting up other types of authentication. The two-factor authentication scheme requires you to configure:

- A server profile (usually for a RADIUS service for two-factor authentication) assigned to an authentication profile.
- A client authentication profile that includes the authentication profile for the service that these components use.

By default, the app supplies the same credentials used to log in to the portal and gateway. In the case of OTP authentication, this behavior causes the authentication to initially fail on the gateway and, because of the delay this causes in prompting the user for a login, the user's OTP may expire. To prevent this, you must configure the portals and gateways that prompt for the OTP instead of using the same credentials on a per-app configuration basis.

You can also reduce the frequency in which users are prompted for OTPs by configuring an authentication override. This enables the portals and gateways to generate and accept a secure encrypted cookie to authenticate the user for a specified amount of time. The portals and/or gateways do not require a new OTP until the cookie expires, thus reducing the number of times users must provide an OTP.

STEP 1 | After you have configured the back-end RADIUS service to generate tokens for the OTPs and ensured users have any necessary devices (such as a hardware token), set up a RADIUS server to interact with the firewall.

For specific instructions, refer to the documentation for your RADIUS server. In most cases, you need to set up an authentication agent and a client configuration on the RADIUS server to enable communication between the firewall and the RADIUS server. You must also define the shared secret to use for encrypting sessions between the firewall and the RADIUS server.

STEP 2 | On each firewall that hosts the gateways and/or portal, create a RADIUS server profile. (For a small deployment, one firewall can host the portal and gateways.)

1. Select **Device** > **Server Profiles** > **RADIUS**.
2. **Add** a new profile.
3. Enter a **Profile Name** for this RADIUS profile.
4. In the **Servers** area, **Add** a RADIUS instance, and then enter the following:
   - A descriptive **Name** to identify this RADIUS server.
   - The IP address of the **RADIUS Server**.
   - The shared **Secret** for encrypting sessions between the firewall and the RADIUS server.
   - The **Port** number on which the RADIUS server listens for authentication requests (default 1812).
5. Click **OK** to save the profile.

STEP 3 | Create an authentication profile.

1. Select **Device** > **Authentication Profile** and **Add** a new profile.
2. Enter a **Name** for the profile. The name cannot contain spaces.
3. Select **RADIUS** as the authentication service **Type**.
4. Select the **Server Profile** you created for accessing your RADIUS server.
5. Enter the **User Domain** name. The firewall uses this value for matching authenticating users against Allow List entries and for User-ID group mapping.
6. Select a **Username Modifier** to modify the username/domain format expected by the RADIUS server.
7. Click **OK** to save the authentication profile.

STEP 4 | Assign the authentication profile to the GlobalProtect portal and/or gateway.

You can configure multiple client authentication configurations for the portal and gateways. For each client authentication configuration, you can specify the authentication profile to apply to endpoints of a specific OS.

This step describes how to add the authentication profile to the portal or gateway configuration. For additional details on setting up these components, see GlobalProtect Portals and GlobalProtect Gateways.

1. Select **Network** > **GlobalProtect** > **Portals** or **Gateways**.
2. Select an existing portal or gateway configuration, or **Add** a new one. If you are adding a new portal or gateway, specify its name, location, and network parameters.
3. On the **Authentication** tab, select an **SSL/TLS service Profile** or **Add** a new profile.
4. **Add** a new **Client Authentication** configuration, and then configure the following settings:
   - The **Name** of the client authentication configuration.
   - The endpoint **OS** to which this configuration applies.
   - The **Authentication Profile** you created in Create an authentication profile.
   - (Optional) A custom **Username Label**.
   - (Optional) A custom **Password Label**.
   - (Optional) A custom **Authentication Message**.
5. Click **OK** to save the configuration.

STEP 5 | (Optional) Configure the portal or gateway to prompt for a username and password or only a password each time the user logs in. Saved passwords are not supported with two-factor authentication using OTPs because the user must enter a dynamic password each time they log in.

This step describes how to configure the password setting in a portal agent configuration. For additional details, see Customize the GlobalProtect App.

1. Select **Network** > **GlobalProtect** > **Portals**, and then select an existing portal configuration.
2. On the GlobalProtect Portal Configuration dialog, select **Agent**.
3. Select an existing agent configuration or **Add** a new one.
4. On the **Authentication** tab, set **Save User Credentials** to **Save Username Only** or **No**. This setting enables GlobalProtect to prompt users for dynamic passwords on each component that you select in the following step.
5. Click **OK** twice to save the configuration.

STEP 6 | Select the GlobalProtect components—portal and types of gateways—that prompt for dynamic passwords, such as OTPs.

1. Select **Network** > **GlobalProtect** > **Portals**, and then select an existing portal configuration.
2. On the GlobalProtect Portal Configuration dialog, select **Agent**.
3. Select an existing agent configuration or **Add** a new one.
4. On the **Authentication** tab, select the **Components that Require Dynamic Passwords (Two-Factor Authentication)**. When selected, the portal and/or types of gateways prompt for OTPs.

   *Do not select the **Components that Require Dynamic Passwords (Two-Factor Authentication)** option for any components that use SAML authentication.*
5. Click **OK** twice to save the configuration.

STEP 7 | If single sign-on (SSO) is enabled, disable it. Because the agent configuration specifies RADIUS as the authentication service, Kerberos SSO is not supported.

This step describes how to disable SSO. For more details, see Define the GlobalProtect Agent Configurations.

1. Select **Network** > **GlobalProtect** > **Portals**, and then select an existing portal configuration.
2. On the GlobalProtect Portal Configuration dialog, select **Agent**.
3. Select an existing agent configuration or **Add** a new one.
4. On the **App** tab, set **Use Single Sign-on (Windows Only)** to **No**.
5. Click **OK** twice to save the configuration.

STEP 8 | (Optional) To minimize the number of times a user must provide credentials, configure an authentication override.

By default, the portal or gateways authenticate the user with an authentication profile and optional certificate profile. With authentication override, the portal or gateway authenticates the user with an encrypted cookie that it has deployed to the endpoint. While the cookie is

valid, the user can log in without entering regular credentials or an OTP. For more information, see Cookie Authentication on the Portal or Gateway.

If you must immediately block access to an endpoint whose cookie has not yet expired (for example, if the endpoint is lost or stolen), you can Identification and Quarantine of Compromised Devices Overview and License Requirements *by adding the device to a quarantine list.*

For more details, see GlobalProtect Portals and GlobalProtect Gateways.

1. Select **Network** > **GlobalProtect** > **Portals** or **Gateways**.
2. Select an existing portal or gateway configuration, or **Add** a new one.
3. Depending on whether you are configuring a portal or gateway, select one of the following:
   - **GlobalProtect Portal Configuration**—On the GlobalProtect Portal Configuration dialog, select **Agent** > ***<agent-config>*** > **Authentication**.
   - **GlobalProtect Gateway Configuration**—On the GlobalProtect Gateway Configuration dialog, select **Agent** > **Client Settings** > ***<client-setting>*** > **Authentication Override**.
4. Configure the following **Authentication Override** settings:
   - **Name** of the authentication override.
   - **Generate cookie for authentication override**—Enables the portal or gateway to generate encrypted, endpoint-specific cookies. After users successfully authenticate, the portal or gateway issue the authentication cookie to the endpoint.

     The authentication cookie includes the following fields:
     - `user`—Username that is used to authenticate the user.
     - `domain`—Domain name of the user.
     - `os`—Application name that is used on the device.
     - `hostID`—Unique ID that is assigned by GlobalProtect to identify the host.
     - `gen time`—Date and time that the authentication cookie was generated.
     - `ip`—IP address of the device that is used to successfully authenticate to GlobalProtect and to obtain the cookie.
   - **Accept cookie for authentication override**—Instructs the portal or gateway to authenticate the user through a valid, encrypted cookie. When the endpoint presents

a valid cookie, the portal or gateway verifies that the cookie was encrypted by the portal or gateway, decrypts the cookie, and then authenticates the user.

The GlobalProtect app must know the username of the connecting user in order to match and retrieve the associated authentication cookies from the user's endpoint. After the app retrieves the cookies, it sends them to the portal or gateway for user authentication.

(Windows only) If you set the List item. *option to* ***Yes*** *(SSO is enabled) in the portal agent configuration (****Network*** *>* ***GlobalProtect*** *>* ***Portals*** *>* ***<portal-config>*** *>* ***Agent*** *>* ***<agent-config>.*** *>* ***App****), the GlobalProtect app uses the Windows username to retrieve the local authentication cookie for the user. If you set the* ***Use Single Sign-On*** *option to* ***No*** *(SSO is disabled), you must enable the GlobalProtect app to* List item. *in order for the app to retrieve the authentication cookie for the user. Set the* ***Save User Credentials*** *option to* ***Yes*** *to save both the username and password or* ***Save Username Only*** *to save only the username.*

(macOS only) Because macOS endpoints do not support single sign-on, you must enable the GlobalProtect app to ***Save User Credentials*** *in order for the app to retrieve the authentication cookie for the user. Set the* ***Save User Credentials*** *option to* ***Yes*** *to save both the username and password or* ***Save Username Only*** *to save only the username.*

- **Cookie Lifetime**—Specifies the hours, days, or weeks that the cookie is valid. Typical lifetime is 24 hours for gateways—which protect sensitive information—or 15 days for the portal. The range for hours is 1–72; for weeks, 1–52; and for days, 1–365. After the cookie expires on either the portal or gateway (whichever occurs first), the portal or gateway prompts the user to authenticate, and subsequently encrypts a new cookie to send to the endpoint.
- **Certificate to Encrypt/Decrypt Cookie**—Specifies the RSA certificate to use to encrypt and decrypt the cookie. You must use the same certificate on the portal and gateways.

  As a best practice, configure the RSA certificate to use the strongest digest algorithm that your network supports.

  The portal and gateways use the RSA encrypt padding scheme PKCS#1 V1.5 to generate the cookie (using the public key of the certificate) and decrypt the cookie (using the private key of the certificate).

5. Click **OK** twice to save the configuration.

STEP 9 | **Commit** the configuration.

STEP 10 | Verify the configuration.

From an endpoint running the GlobalProtect app, try to connect to the gateway or portal on which you enabled OTP authentication. You should see prompts similar to the following:

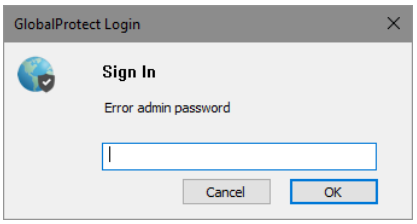


Figure 1: OTP Pop-Up Prompt

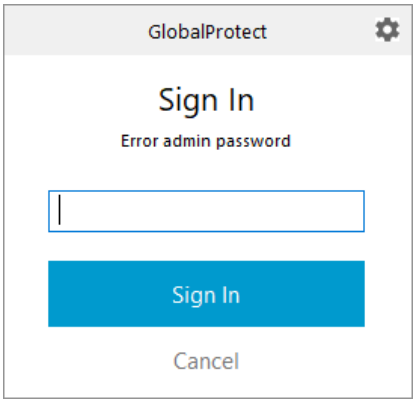


Figure 2: OTP Prompt on the GlobalProtect Status Panel

Enable Two-Factor Authentication Using Smart Cards

If you want to enable your end users to authenticate using a smart card or common access card (CAC), you must import the Root CA certificate that issued the certificates contained on the CAC or smart cards onto the portal and gateway. You can then create a certificate profile that includes that Root CA and apply it to your portal and/or gateway configurations to enable use of the smart card in the authentication process.

Two-factor authentication using smart cards is supported on macOS and Windows endpoints.

STEP 1 | Set up your smart card infrastructure.

This procedure assumes that you have deployed smart cards and smart card readers to your end users.

For specific instructions, refer to the documentation for the authentication provider software.

In most cases, the smart card infrastructure setup involves the generating of certificates for end users and participating servers, which are the GlobalProtect portal and gateway(s) in this use case.

STEP 2 | Import the Root CA certificate that issued the client certificates contained on the end user smart cards.

Make sure the certificate is accessible from your management system, and then complete the following steps:

1. Select **Device** > **Certificate Management** > **Certificates** > **Device Certificates**, and then **Import** a certificate.
2. Enter a **Certificate Name**.
3. Enter the path and name of the **Certificate File** received from the CA, or **Browse** to locate the file.
4. Select **Base64 Encoded Certificate (PEM)** from the **File Format** drop-down, and then click **OK** to import the certificate.

STEP 3 | Create the certificate profile on each portal/gateway on which you plan to use CAC or smart card authentication.

For details on other certificate profile fields, such as whether to use CRL or OCSP, refer to the online help.

1. Select **Device** > **Certificate Management** > **Certificate Profile**.
2. Select an existing certificate profile or **Add** a new one.
3. Enter a **Name** for the certificate profile.
4. Select the certificate **Username Field** that PAN-OS uses to match the IP address for User-ID–either **Subject** to use a common name, **Subject Alt: Email** to use an email address, or **Subject Alt: Principal Name** to use the Principal Name.
5. In the **CA Certificates** area, **Add** the trusted root CA certificate you imported in step 2 to the certificate profile. When prompted, select the **CA Certificate**, and then click **OK**.
6. Click **OK** to save the certificate profile.

STEP 4 | Assign the certificate profile to the portal or gateway. This step describes how to add the certificate profile to the portal or gateway configuration. For details on setting up these components, see GlobalProtect Portals and GlobalProtect Gateways.

1. Select **Network** > **GlobalProtect** > **Portals** or **Gateways**
2. Select an existing portal or gateway configuration or **Add** a new one.
3. On the GlobalProtect Gateway Configuration dialog, select **Authentication**.
4. Select the **Certificate Profile** you just created.
5. Click **OK** to save the configuration.

STEP 5 | **Commit** the configuration.

STEP 6 | Verify the configuration.

From an endpoint running the GlobalProtect app, try to connect to the gateway or portal on which you set up smart card-enabled authentication. When prompted, insert your smart card and verify that you can successfully authenticate to GlobalProtect.

Enable Two-Factor Authentication Using a Software Token Application

If your organization uses a software token (soft token) application, such as RSA SecurID, to implement two-factor authentication, users are required to first open their software token app and enter their PIN to obtain a passcode, then enter the passcode in their GlobalProtect app in the **Password** field. This two-step process complicates the login process.

To simplify the login process and improve the users' experience, GlobalProtect offers seamless soft-token authentication. The user enters the RSA PIN in the GlobalProtect **Password** field, and GlobalProtect retrieves the passcode from RSA and proceeds with the connection without the user taking the extra step of opening the RSA application.

This feature is supported for all three RSA modes: PinPad Style (PIN integrated with token code), Fob Style (PIN followed by token code) and Pinless mode. For PinPad and Fob Style, the user enters the PIN in the **Password** field and GlobalProtect retrieves the passcode. In Pinless mode, the Password field is grayed out and users enter their username.

This feature is supported for Windows devices starting with GlobalProtect™ app 5.1.

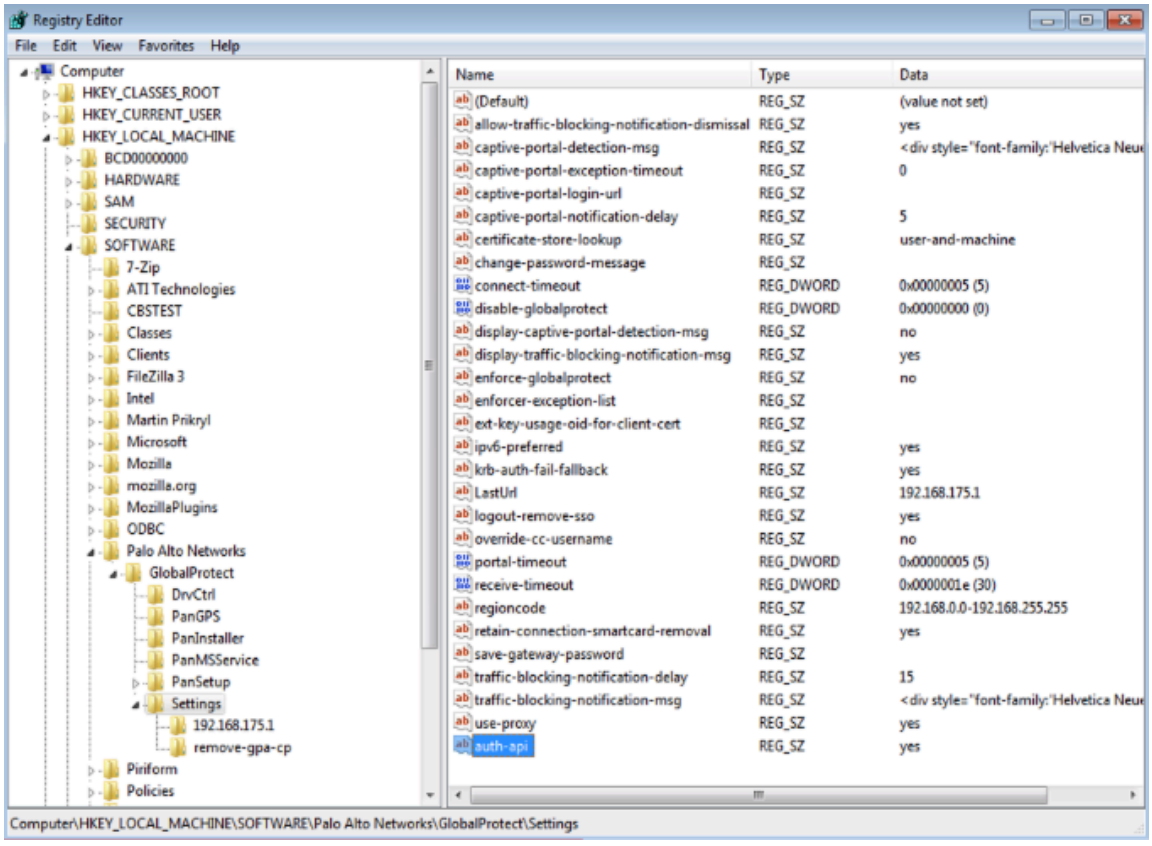
STEP 1 | Change the registry keys on the client Windows devices to enable seamless soft-token authentication.

You must change the Windows registry on the clients' Windows devices before you can enable seamless soft-token authentication. GlobalProtect retrieves this registry entry only once, when the GlobalProtect app initializes.

1. Open the Windows Registry Editor and select **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Palo Alto Networks** > **GlobalProtect** > **Settings**.
2. Change the **auth-api** value to **yes**.

*Because auth-api is set as **yes** in the client machine, you should configure the portal and gateways with RSA-based authentication. No other authentication profile is supported because GlobalProtect will attempt to retrieve the passcode.*

Because the portal and gateway use RSA Authentication, we recommend that you enable cookie-based authentication on gateways. The token that is retrieved for the portal may still be active when GlobalProtect tries to get passcode for the gateway, and authentication may fail because the passcode was already used. Therefore, we suggest that you generate an Authentication Override cookie on the portal and Accept the cookie on the gateway.



STEP 2 | Configure the portal and gateway with RSA-based authentication.

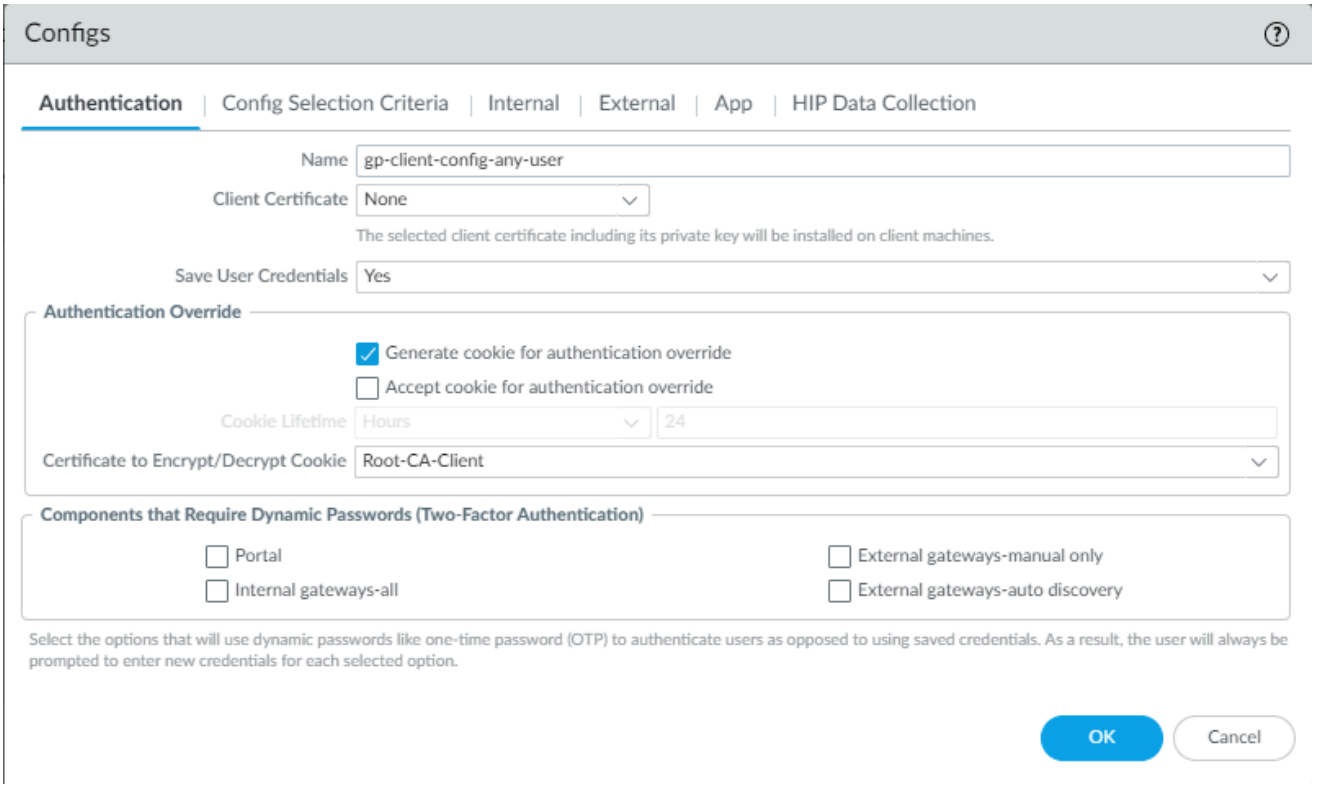
STEP 3 | Enable cookie-based authentication on the GlobalProtect portal.

Specifying GlobalProtect to override an existing authentication allows GlobalProtect to overwrite an existing passcode with a newly-created passcode.

1. Select **Network** > **GlobalProtect** > **Portals** > ***<portal-config>***; then select the **Agent** tab.
2. **Add** an Agent config or select an existing one.
3. Select **Generate cookie for authentication override**.

   The authentication cookie includes the following fields:

   - `user`—Username that is used to authenticate the user.
   - `domain`—Domain name of the user.
   - `os`—Application name that is used on the device.
   - `hostID`—Unique ID that is assigned by GlobalProtect to identify the host.
   - `gen time`—Date and time that the authentication cookie was generated.
   - `ip`—IP address of the device that is used to successfully authenticate to GlobalProtect and to obtain the cookie.

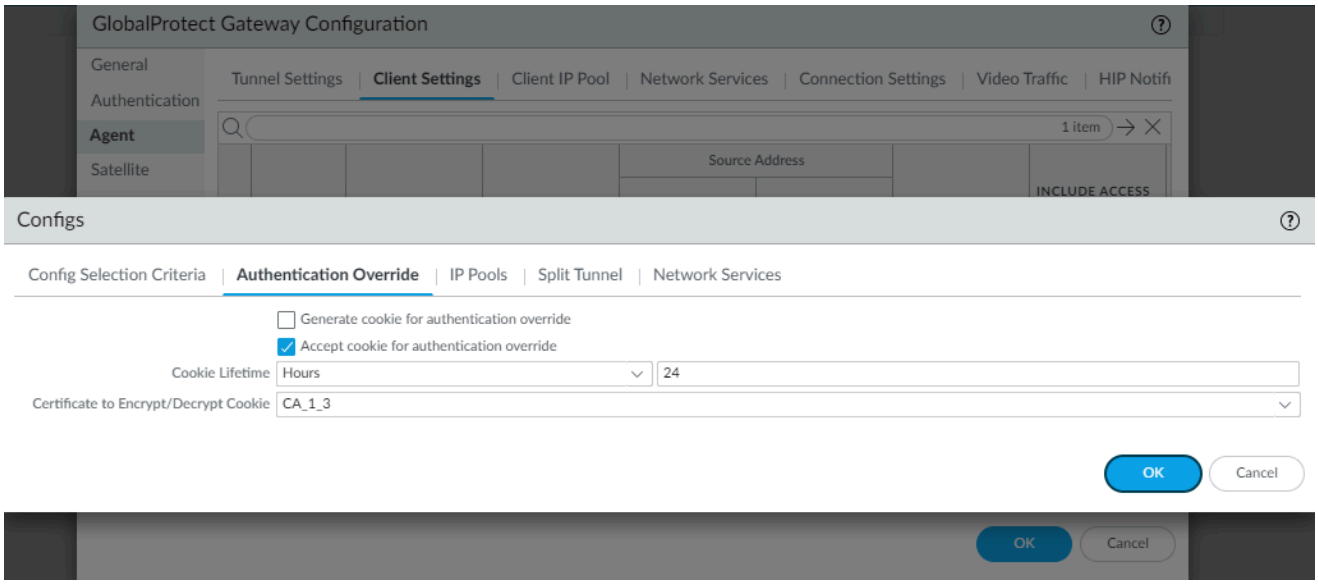


STEP 4 | Enable the GlobalProtect gateway to accept cookies for authentication overrides.

1. Select **Network** > **GlobalProtect** > **Gateways** > ***<gateway>*** and select the **Agent** tab.
2. Select **Client Settings**, then select the GlobalProtect client config or add a new one.
3. Select **Authentication Override**; then, select **Accept cookie for authentication override**.

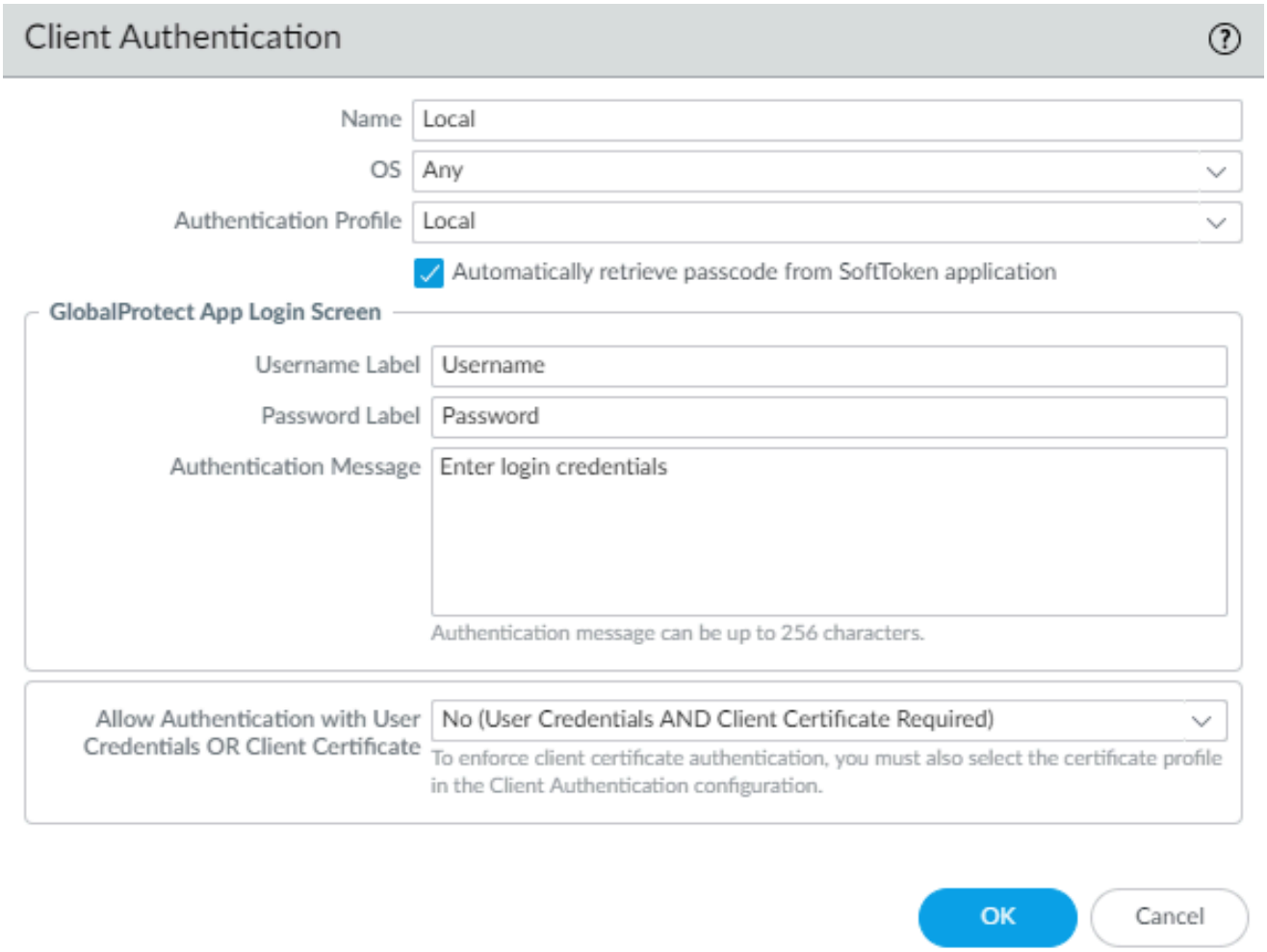
   The authentication cookie includes the following fields:

   - `user`—Username that is used to authenticate the user.
   - `domain`—Domain name of the user.
   - `os`—Application name that is used on the device.
   - `hostID`—Unique ID that is assigned by GlobalProtect to identify the host.
   - `gen time`—Date and time that the authentication cookie was generated.
   - `ip`—IP address of the device that is used to successfully authenticate to GlobalProtect and to obtain the cookie.



STEP 5 | Select **Network** > **GlobalProtect** > **Portals** > ***<portal-config>***; then select the **Authentication** tab.

STEP 6 | **Add** a new client authentication profile or select an existing one; then, select **Automatically retrieve passcode from SoftToken application**.



Set Up Authentication for strongSwan Ubuntu and CentOS Endpoints

To extend GlobalProtect access to strongSwan Ubuntu and CentOS endpoints, set up authentication for these endpoints.

To view the minimum GlobalProtect release version that supports strongSwan on Ubuntu Linux and CentOS, see What OS Versions are Supported with GlobalProtect?.

To connect to the GlobalProtect gateway, the user must successfully authenticate. The following workflows show examples of how to enable authentication for strongSwan endpoints. For complete information about strongSwan, see the strongSwan wiki.

- Enable Authentication Using a Certificate Profile
- Enable Authentication Using an Authentication Profile
- Enable Authentication Using Two-Factor Authentication

Enable Authentication Using a Certificate Profile

The following workflow shows how to enable authentication for strongSwan clients using a certificate profile.

STEP 1 | Configure an IPsec tunnel for the GlobalProtect gateway for communicating with a strongSwan client.

Extended authentication (X-Auth) is not supported for Prisma Access deployments.

1. Select **Network** > **GlobalProtect** > **Gateways**.
2. Select an existing gateway or **Add** a new one.
3. On the **Authentication** tab of the GlobalProtect Gateway Configuration dialog, select the **Certificate Profile** that you want to use for authentication.
4. Select **Agent** > **Tunnel Settings** to enable **Tunnel Mode** and specify the following settings to set up the tunnel:
   - Select the check box to **Enable X-Auth Support**.
   - If a **Group Name** and **Group Password** are already configured, remove them.
   - Click **OK** to save the settings.

STEP 2 | Verify that the default connection settings in the `conn %default` section of the IPsec tunnel configuration file (`ipsec.conf`) are correctly defined for the strongSwan client.

The `ipsec.conf` file is usually found in the `/etc` folder.

The configurations in this procedure are tested and verified for the following releases:

- *Ubuntu 14.0.4 with strongSwan 5.1.2 and CentOS 6.5 with strongSwan 5.1.3 for PAN-OS 6.1.*
- *Ubuntu 14.0.4 with strongSwan 5.2.1 for PAN-OS 7.0.*

The configurations in this procedure can be used for reference if you are using a different version of strongSwan. Refer to the strongSwan wiki for more information.

Modify the following settings in the `conn %default` section of the `ipsec.conf` file to these recommended settings.

```
ikelifetime=20m
reauth=yes
rekey=yes
keylife=10m
rekeymargin=3m
rekeyfuzz=0%
keyingtries=1
type=tunnel
```

STEP 3 | Modify the strongSwan client's IPsec configuration file (`ipsec.conf`) and the IPsec password file (`ipsec.secrets`) to use recommended settings.

The `ipsec.secrets` file is usually found in the `/etc` folder.

Use the strongSwan client username as the certificate's common name.

Modify the following items in the `ipsec.conf` file to these recommended settings.

```
conn <connection name>
keyexchange=ikev1
authby=rsasig
ike=aes-sha1-modp1024,aes256
left=<strongSwan/Linux-client-IP-address>
leftcert=<client certificate with the strongSwan client username
 used as the certificate's common name>
leftsourceip=%config
leftauth2=xauth
right=<GlobalProtect-Gateway-IP-address>
rightid="CN=<Subject-name-of-gateway-certificate>"
rightsubnet=0.0.0.0/0
auto=add
```

Modify the following items in the `ipsec.conf` file to these recommended settings.

```
:RSA
<private key file> "<passphrase if used>"
```


STEP 4 | Start strongSwan IPsec services and connect to the IPsec tunnel that you want the strongSwan client to use when authenticating to the GlobalProtect gateway.

Use the `config <name>` variable to name the tunnel configuration.

- Ubuntu:

```
ipsec start
ipsec up <name>
```

- CentOS:

```
strongSwan start
strongswan up <name>
```

STEP 5 | Verify that the tunnel is set up correctly and the VPN connection is established to both the strongSwan client and the GlobalProtect gateway.

1. Verify the detailed status information on a specific connection (by naming the connection) or verify the status information for all connections from the strongSwan client:
   - Ubuntu:

     ```
     ipsec statusall [<connection name>]
     ```

   - CentOS:

     ```
     strongswan statusall [<connection name>]
     ```

2. Select **Network** > **GlobalProtect** > **Gateways**. In the **Info** column, select **Remote Users** for the gateway configured for the connection to the strongSwan client. The strongSwan client should be listed under **Current Users**.

Enable Authentication Using an Authentication Profile

The following workflow shows how to enable authentication for strongSwan clients using an authentication profile. The authentication profile specifies which server profile to use when authenticating strongSwan clients.

STEP 1 | Set up the IPsec tunnel that the GlobalProtect gateway will use for communicating with a strongSwan client.

Extended authentication (X-Auth) is not supported for Prisma Access deployments.

1. Select **Network** > **GlobalProtect** > **Gateways**.
2. Select an existing gateway or **Add** a new one.
3. On the **Authentication** tab of the GlobalProtect Gateway Configuration dialog, select the **Authentication Profile** you want to use.
4. Select **Agent** > **Tunnel Settings** to enable **Tunnel Mode** and specify the following settings to set up the tunnel:
   - Select the check box to **Enable X-Auth Support**.
   - Enter a **Group Name** and **Group Password** if they are not yet configured.
   - Click **OK** to save these tunnel settings.

STEP 2 | Verify that the default connection settings in the `conn %default` section of the IPsec tunnel configuration file (`ipsec.conf`) are correctly defined for the strongSwan client.

The `ipsec.conf` file is usually found in the `/etc` folder.

The configurations in this procedure are tested and verified for the following releases:

- *Ubuntu 14.0.4 with strongSwan 5.1.2 and CentOS 6.5 with strongSwan 5.1.3 for PAN-OS 6.1.*
- *Ubuntu 14.0.4 with strongSwan 5.2.1 for PAN-OS 7.0.*

The configurations in this procedure can be used for reference if you are using a different version of strongSwan. Refer to the strongSwan wiki for more information.

In the `conn %default` section of the `ipsec.conf` file, configure the following recommended settings:

```
ikelifetime=20m
reauth=yes
rekey=yes
keylife=10m
rekeymargin=3m
rekeyfuzz=0%
keyingtries=1
type=tunnel
```


STEP 3 | Modify the strongSwan client's IPsec configuration file (`ipsec.conf`) and the IPsec password file (`ipsec.secrets`) to use recommended settings.

The `ipsec.secrets` file is usually found in the `/etc` folder.

Use the strongSwan client username as the certificate's common name.

Configure the following recommended settings in the `ipsec.conf` file:

```
conn <connection name>
keyexchange=ikev1
ikelifetime=1440m
keylife=60m
aggressive=yes
ike=aes-sha1-modp1024,aes256
esp=aes-sha1
xauth=client
left=<strongSwan/Linux-client-IP-address>
leftid=@#<hex of Group Name configured in the GlobalProtect
 gateway>
leftsourceip=%modeconfig
leftauth=psk
rightauth=psk
leftauth2=xauth
right=<gateway-IP-address>
rightsubnet=0.0.0.0/0
xauth_identity=<LDAP username>
auto=add
```

Configure the following recommended settings in the `ipsec.secrets` file:

```
: PSK <Group Password configured in the gateway>
 <username> : XAUTH “<user password>”
```

STEP 4 | Start strongSwan IPsec services and connect to the IPsec tunnel that you want the strongSwan client to use when authenticating to the GlobalProtect gateway.

- Ubuntu:

```
ipsec start
ipsec up <name>
```

- CentOS:

```
strongSwan start
strongswan up <name>
```


STEP 5 | Verify that the tunnel is set up correctly and the VPN connection is established to both the strongSwan client and the GlobalProtect gateway.

1. Verify the detailed status information on a specific connection (by naming the connection) or verify the status information for all connections from the strongSwan client:
   - Ubuntu:

     ```
     ipsec statusall [<connection name>]
     ```

   - CentOS:

     ```
     strongswan statusall [<connection name>]
     ```

2. Select **Network** > **GlobalProtect** > **Gateways**. In the **Info** column, select **Remote Users** for the gateway configured for the connection to the strongSwan client. The strongSwan client should be listed under **Current Users**.

Enable Authentication Using Two-Factor Authentication

With two-factor authentication, the strongSwan client needs to successfully authenticate using both a certificate profile and an authentication profile to connect to the GlobalProtect gateway. The following workflow shows how to enable authentication for strongSwan clients using two-factor authentication.

STEP 1 | Set up the IPsec tunnel that the GlobalProtect gateway will use for communicating with a strongSwan client.

Extended authentication (X-Auth) is not supported for Prisma Access deployments.

1. Select **Network** > **GlobalProtect** > **Gateways**.
2. Select an existing gateway or **Add** a new one.
3. On the **Authentication** tab of the GlobalProtect Gateway Configuration dialog, select the **Certificate Profile** and **Authentication Profile** that you want to use.
4. Select **Agent** > **Tunnel Settings** to enable **Tunnel Mode** and specify the following settings to set up the tunnel:
   - Select the check box to **Enable X-Auth Support**.
   - If a **Group Name** and **Group Password** are already configured, remove them.
   - Click **OK** to save these tunnel settings.

STEP 2 | Verify that the default connection settings in the `conn %default` section of the IPsec tunnel configuration file (`ipsec.conf`) are correctly defined for the strongSwan client.

The `ipsec.conf` file usually resides in the `/etc` folder.

The configurations in this procedure are tested and verified for the following releases:

- *Ubuntu 14.0.4 with strongSwan 5.1.2 and CentOS 6.5 with strongSwan 5.1.3 for PAN-OS 6.1.*
- *Ubuntu 14.0.4 with strongSwan 5.2.1 for PAN-OS 7.0.*

Use the configurations in this procedure as a reference if you are using a different version of strongSwan. Refer to the strongSwan wiki for more information.

Configure the following recommended settings in the `ipsec.conf` file:

```
ikelifetime=20m
reauth=yes
rekey=yes
keylife=10m
rekeymargin=3m
rekeyfuzz=0%
keyingtries=1
type=tunnel
```

STEP 3 | Modify the strongSwan client's IPsec configuration file (`ipsec.conf`) and the IPsec password file (`ipsec.secrets`) to use recommended settings.

The `ipsec.secrets` file is usually found in the `/etc` folder.

Use the strongSwan client username as the certificate's common name.

Configure the following recommended settings in the `ipsec.conf` file:

```
conn <connection name>
keyexchange=ikev1
authby=xauthrsasig
ike=aes-sha1-modp1024
esp=aes-sha1
xauth=client
left=<strongSwan/Linux-client-IP-address>
leftcert=<client-certificate-without-password>
leftsourceip=%config
right=<GlobalProtect-gateway-IP-address>
rightid=%anyCN=<Subject-name-of-gateway-cert>”
rightsubnet=0.0.0.0/0
leftauth2=xauth
xauth_identity=<LDAP username>
auto=add
```

Configure the following recommended settings in the `ipsec.secrets` file:

```
<username> :XAUTH “<user password>”
```



```
::RSA <private key file> “<passphrase if used>”
```

STEP 4 | Start strongSwan IPsec services and connect to the IPsec tunnel that you want the strongSwan client to use when authenticating to the GlobalProtect gateway.

- Ubuntu:

```
ipsec start
ipsec up <name>
```

- CentOS:

```
strongSwan start
strongswan up <name>
```

STEP 5 | Verify that the tunnel is set up correctly and the VPN connection is established to both the strongSwan client and the GlobalProtect gateway.

1. Verify the detailed status information on a specific connection (by naming the connection) or verify the status information for all connections from the strongSwan client:
   - Ubuntu:

     ```
     ipsec statusall [<connection name>]
     ```

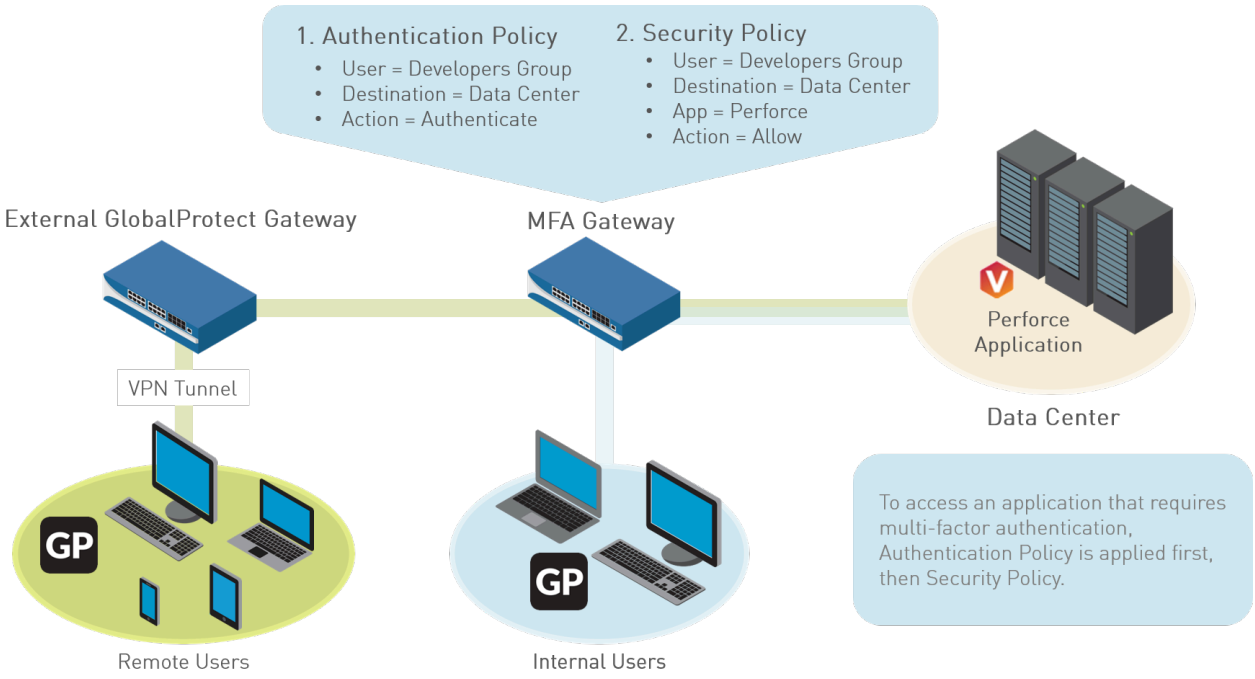
   - CentOS:

     ```
     strongswan statusall [<connection name>]
     ```

2. Select **Network** > **GlobalProtect** > **Gateways**. In the **Info** column, select **Remote Users** for the gateway configured for the connection to the strongSwan client. The strongSwan client should be listed under **Current Users**.

Configure GlobalProtect to Facilitate Multi-Factor Authentication Notifications

To protect critical applications and stop attackers from using stolen credentials to conduct lateral movement throughout your network, you can configure policy-based multi-factor authentication. This ensures that each user responds to multiple authentication challenges of different types (factors) before they can access highly sensitive services and applications.



If a user session matches the Authentication policy, the type of application or service determines the user experience for notifications about the authentication challenge:

- (Windows or macOS endpoints only) **Non-browser-based applications**—To facilitate MFA notifications for non-HTTP applications (such as Perforce) on Windows or macOS endpoints, a GlobalProtect app is required. When a session matches an Authentication policy rule, the firewall sends a UDP notification to the GlobalProtect app with an embedded URL link to the Authentication Portal page. The GlobalProtect app then displays this message as a pop up notification to the user.
- **Browser-based applications**—Browser-based applications do not require GlobalProtect to display notification messages to the user. When the firewall identifies a session as web-browsing traffic (based on App-ID), the firewall automatically presents the user with Authentication Portal page (previously called the Captive Portal page) specified in the Authentication policy rule.

To configure GlobalProtect to display MFA notifications for non-browser-based applications, use the following workflow:

STEP 1 | Before you configure GlobalProtect, configure multi-factor authentication on the firewall.

> *If you are using two-factor authentication with GlobalProtect to authenticate to the gateway or portal, a RADIUS server profile is required. If you are using GlobalProtect to notify the user about an authentication policy match (UDP message), a Multi Factor Authentication server profile is sufficient.*

To use multi-factor authentication for protecting sensitive resources, the easiest solution is to integrate the firewall with an MFA vendor that is already established in your network. When your MFA structure is ready, you can start configuring the components of your authentication policy.

- Enable Captive Portal to record authentication timestamps and update user mappings.
- Create server profiles that define how the firewall will connect to the services that authenticate users.
- Assign the server profiles to an Authentication profile which specifies authentication parameters.
- Configure a Security policy rule that allows users to access the resources that require authentication.

STEP 2 | (External gateways only) For GlobalProtect to support multi-factor authentication on external gateways, you must configure a response page for the ingress tunnel interface on the firewall:

1. Select **Device** > **Response Pages** > **MFA Login Page**.
2. Select and then **Export** the **Predefined** template to a location of your choice.
3. On your endpoint, use an HTML editor to customize the downloaded response page and save it with a unique filename.
4. Return to the **MFA Login Page** dialog on the firewall, **Import** your customized page, **Browse** to select the **Import File**, and select the **Destination** (virtual system or shared location). Click **OK**, and then click **Close**.

STEP 3 | (External gateways only) Enable **Response Pages** as a permitted service on the **Interface Mgmt** profile:

1. Select **Network** > **Network Profiles** > **Interface Mgmt** and then select the profile.
2. In the **Permitted Services** area, select **Response Pages** and click **OK**.

STEP 4 | (External gateways only) Attach the **Interface Mgmt** profile to a tunnel interface:

1. Select **Network** > **Interfaces** > **Tunnel**, and the tunnel interface on which you want to use the response page.
2. Select **Advanced**, and then select the **Interface Mgmt** profile you configured in the previous step as the **Management Profile**.

STEP 5 | (External gateways only) **Enable User Identification** on the Zone associated with the tunnel interface (**Network** > **Zones** > **<tunnel-zone**).

STEP 6 | Configure GlobalProtect clients to support multi-factor authentication notifications for non-browser-based applications.

1. Select **Network** > **GlobalProtect** > **Portals** and select a portal configuration (or **Add** one).
2. Select **Agent**, and then select an existing agent configuration or **Add** a new one.
3. On the **App** tab, specify the following:
   - Set **Enable Inbound Authentication Prompts from MFA Gateways** to **Yes**. To support multi-factor authentication (MFA), the GlobalProtect app must receive and acknowledge UDP authentication prompts that are inbound from the gateway. Select **Yes** to enable the GlobalProtect app to receive and acknowledge the prompt. By default, this value is set to **No**, meaning GlobalProtect will block UDP authentication prompts from the gateway.
   - In the **Network Port for Inbound Authentication Prompts (UDP)** field, specify the port number that the GlobalProtect app uses to receive inbound UDP authentication prompts from MFA gateways. The default port is 4501. To change the port, specify a number from 1 to 65535.
   - In the **Trusted MFA Gateways** field, specify the gateway address and port number (required only for non-default ports, such as 6082) of the redirect URL that the GlobalProtect app will trust for multi-factor authentication. When a GlobalProtect app receives a UDP authentication prompt with a redirect URL destined for the specified network port, GlobalProtect displays an authentication message only if the redirect URL is trusted.
   - Configure the **Default Message for Inbound Authentication Prompts**. When users try to access a resource that requires additional authentication, GlobalProtect receives a UDP packet containing the inbound authentication prompt and displays this message. The UDP packet also contains the URL for the Authentication Portal page you specified when you set up multi-factor authentication. GlobalProtect automatically appends the URL to the message. For example, to display the notification shown in the beginning of this topic enter the following message:

     ```
     You have attempted to access a protected resource that
     requires additional authentication. Proceed to authenticate
     at:
     ```
4. Save the agent configuration (click **OK** twice), and then **Commit** your changes.

Enable Delivery of VSAs to a RADIUS Server

When communicating with portals or gateways, GlobalProtect endpoints send information that includes the endpoint IP address, operating system (OS), hostname, user domain, and GlobalProtect app version. You can enable the firewall to send this information as Vendor-Specific Attributes (VSAs) to a RADIUS server during authentication (by default, the firewall does not send the VSAs). RADIUS administrators can then perform administrative tasks based on those VSAs. For example, RADIUS administrators might use the OS attribute to define a policy that mandates regular password authentication for Microsoft Windows users and one-time password (OTP) authentication for Google Android users.

The following are prerequisites for this procedure:

- Import the Palo Alto Networks RADIUS dictionary into your RADIUS server.
- Configure a RADIUS server profile and assign it to an authentication profile. See Set Up External Authentication for more details.
- Assign the authentication profile to a GlobalProtect portal or gateway. See Set Up Access to the GlobalProtect Portal or Configure a GlobalProtect Gateway for more details.

STEP 1 | Log in to the firewall CLI.

STEP 2 | Enter the command for each VSA you want to send:

```
username@hostname> set authentication radius-vsa-on client-source-
ip
username@hostname> set authentication radius-vsa-on client-os
username@hostname> set authentication radius-vsa-on client-
hostname
username@hostname> set authentication radius-vsa-on user-domain
username@hostname> set authentication radius-vsa-on client-gp-
version
```

If you later want to stop the firewall from sending particular VSAs, run the same commands but use the ***radius-vsa-off*** *option instead of* ***radius-vsa-on****.*

Enable Group Mapping

Because the agent or app running on your end-user systems requires the user to successfully authenticate before being granted access to GlobalProtect, the identity of each GlobalProtect user is known. However, if you want to be able to define GlobalProtect configurations and/or security policies based ongroup_membership, the firewall must retrieve the list of groups and the corresponding list of members from your directory server. This is known as *group mapping*.

To enable this functionality, you must create an LDAP server profile that instructs the firewall how to connect and authenticate to the directory server and how to search the directory for the user and group information. After the firewall connects to the LDAP server and retrieves the group mappings, you can select groups when you define the agent configurations and security policies. The firewall supports a variety of LDAP directory servers, including Microsoft Active Directory (AD), Novell eDirectory, and Sun ONE Directory Server.

Use the following procedure to connect to your LDAP directory to enable the firewall to retrieve user-to-group mapping information:

STEP 1 | Create an LDAP Server Profile that specifies how to connect to the directory servers to which the firewall should connect to obtain group mapping information.

1. Select **Device** > **Server Profiles** > **LDAP** and click **Add**.
2. Enter a **Profile Name** to identify the server profile.
3. If this profile is for a firewall with multiple virtual systems capability, select a virtual system or **Shared** as the **Location** where the profile is available.
4. For each LDAP server (up to four), **Add** and enter a **Name** (to identify the server), server IP address (**LDAP Server** field), and server **Port** (default 389).
5. Select the server **Type** from the drop-down: **active-directory**, **e-directory**, **sun**, or **other**.
6. If you want the device to use SSL or TLS for a more secure connection with the directory server, select the **Require SSL/TLS secured connection** check box (it is selected by default). The protocol that the device uses depends on the server **Port**:
   - 389 (default)—TLS (Specifically, the device uses the StartTLS operation, which upgrades the initial plaintext connection to TLS.)
   - 636—SSL
   - Any other port—The device first attempts to use TLS. If the directory server doesn't support TLS, the device falls back to SSL.
7. For additional security, you can select the **Verify Server Certificate for SSL sessions** check box (it is cleared by default) so that the device verifies the certificate that the directory server presents for SSL/TLS connections. To enable verification, you also have to select the **Require SSL/TLS secured connection** check box. For verification to succeed, the certificate must meet one of the following conditions:
   - It is in the list of device certificates: **Device** > **Certificate Management** > **Certificates** > **Device Certificates.** Import the certificate into the device, if necessary.
   - The certificate signer is in the list of trusted certificate authorities: **Device** > **Certificate Management** > **Certificates** > **Default Trusted Certificate Authorities**.
8. Click **OK**.

STEP 2 | Add the LDAP server profile to the User-ID Group Mapping configuration.

1. Select **Device** > **User Identification** > **Group Mapping Settings** and then **Add** a new group mapping configuration.
2. Select **Server Profile**.
3. Enter a **Name** for the group mapping configuration.
4. Select the **Server Profile** you just created.
5. Specify the **Update Interval** (in seconds) after which the firewall initiates a connection with the LDAP directory server to obtain any updates that are made to the groups that the firewall policies use (range of 60 to 86,400 seconds).
6. Make sure the server profile is **Enabled** for group mapping.

STEP 3 | (Optional) Enable GlobalProtect to retrieve serial numbers from the directory server.

GlobalProtect can identify the status of connecting endpoints and enforce Host Information-based security policies based on the presence of the endpoint serial number. If an endpoint is managed, you can bind the serial number of the endpoint to the machine account of the endpoint in your directory server. The firewall can then pre-fetch the serial numbers for these managed endpoints when it retrieves group mapping information from the directory server.

1. From your group mapping configuration, select **Server Profile**.
2. Enable the option to **Fetch list of managed devices**.

STEP 4 | (Optional) Specify attributes to identify users and user groups.

1. From your group mapping configuration, select **User and Group Attributes**.
2. In the User Attributes area, specify the **Primary Username**, **E-Mail**, and **Alternate Username 1-3** used to identify individual users.
3. In the Group Attributes area, specify the **Group Name**, **Group Member**, and **E-Mail** used to identify user groups.

STEP 5 | (Optional) Limit which groups can be selected in policy rules.

By default, if you don't specify groups, all groups are available in policy rules.

1. Add existing groups from the directory service:
   1. From your group mapping configuration, select **Group Include List**.
   2. In the Available Groups list, select the groups you want to appear in policy rules, and then click the Add (⊕) icon to move the group to the Included Groups list.
2. If you want to base policy rules on user attributes that don't match existing user groups, create custom groups based on LDAP filters:
   1. From your group mapping configuration, select **Custom Group**.
   2. **Add** a new custom group.
   3. Enter a group **Name** that is unique in the group mapping configuration for the current firewall or virtual system. If the **Name** has the same value as the Distinguished

Name (DN) of an existing AD group domain, the firewall uses the custom group in all references to that name (for example, in policies and logs).

4. Specify an **LDAP Filter** of up to 2,048 UTF-8 characters, then click **OK**. The firewall doesn't validate LDAP filters.

To optimize LDAP searches and minimize the performance impact on the LDAP directory server, use indexed attributes and reduce the search scope to include the user and group objects that you require for policy or visibility. Alternatively, you can create custom groups based on LDAP filters.

STEP 6 | Commit your changes.

Click **OK** and **Commit**.

GlobalProtect Gateways

GlobalProtect gateways provide security enforcement for traffic from the GlobalProtect apps. Additionally, if the Host Information Profile (HIP) feature is enabled, the gateway generates a HIP report from the raw host data that the endpoints submit, which it can use for policy enforcement.

Configure a GlobalProtect Gateway on any Palo Alto Networks NGFW or on Prisma Access. On the NGFW, you can run both a gateway and portal on the same firewall, or you can have multiple distributed gateways throughout your enterprise. On Prisma Access, all gateways in your Prisma Access locations are available to users. If you have additional GlobalProtect gateways that you'd like your users to be able to connect to, you can add those gateways

GlobalProtect supports the following gateway types:

- **Internal**—An internal gateway is an interface on the internal network that is configured as a GlobalProtect gateway and applies security policies for internal resource access. When used in conjunction with User-ID and/or HIP checks, an internal gateway can be used to provide a secure, accurate method of identifying and controlling traffic based on user and/or device state. Internal gateways are useful in sensitive environments where authenticated access to critical resources is required. You can configure an internal gateway in either tunnel mode or non-tunnel mode. The GlobalProtect app connects to the internal gateway after performing internal host detection to determine the location of the endpoint. If internal host detection is not configured, the GlobalProtect app first connects to the internal gateway followed by external gateway upon connection failure.
- **External gateway (auto discovery)**—An external gateway resides outside of the corporate network and provides security enforcement and/or virtual private network (VPN) access for your remote users. By default, the GlobalProtect app automatically connects to the **Best Available** external gateway, based on the priority you assign to the gateway, source region, and the response time (see Gateway Priority in a Multiple Gateway Configuration).
- **External gateway (manual)**—A manual external gateway also resides outside of the corporate network and provides security enforcement and/or VPN access for your remote users. The difference between the auto-discovery external gateway and the manual external gateway is that the GlobalProtect app only connects to a manual external gateway when the user initiates a connection. You can also configure different authentication requirements for manual external gateways. To configure a manual gateway, you must identify the gateway as **Manual** when you Define the GlobalProtect Agent Configurations.

Gateway Priority in a Multiple Gateway Configuration

To enable secure access for your mobile workforce no matter where they are located, you can strategically deploy additional Palo Alto Networks next-generation firewalls and configure them as GlobalProtect gateways. To determine the preferred gateway to which your apps connect, add the gateways to a portal agent configuration, and then assign each gateway a connection priority. See Define the GlobalProtect Agent Configurations.

If a GlobalProtect portal agent configuration contains more than one gateway, the app attempts to communicate with all gateways listed in its agent configuration. The app uses the priority and response time to determine the gateway to which to connect. With GlobalProtect app 4.0.2 and earlier releases, the app connects to a lower priority gateway only if the response time for the higher priority gateway is greater than the average response time across all gateways.

For example, consider the following response times for gw1 and gw2:

Name	Priority	Response Time
gw1	Highest	80 ms
gw2	High	25 ms

The app determines that the response time for the gateway with the highest priority (higher number) is greater than the average response time for both gateways (52.5 ms) and, as a result, connects to gw2. In this example, the app did not connect to gw1 even though it had a higher priority because a response time of 80 ms was higher than the average for both.

Now consider the following response times for gw1, gw2, and a third gateway, gw3:

Name	Priority	Response Time
gw1	Highest	30 ms
gw2	High	25 ms
gw3	Medium	50 ms

In this example, the average response time for all gateways is 35 ms. The app would then evaluate which gateways responded faster than the average response time and see that gw1 and gw2 both had faster response times. The app would then connect to whichever gateway had the highest priority. In this example, the app connects to gw1 because gw1 has the highest priority of all the gateways with response times below the average.

In addition to gateway priority, you can add one or more source regions to an external gateway configuration. GlobalProtect recognizes the source region and only allows uses to connect to gateways that are configured for that region. Regarding gateway selection, source region is considered first, then the gateway priority.

In GlobalProtect app 4.0.3 and later releases, the GlobalProtect app prioritizes the gateways assigned highest, high, and medium priority ahead of gateways assigned a low or lowest priority regardless of response time. The GlobalProtect app then appends any gateways assigned a low or lowest priority to the list of gateways. This ensures that the app first attempts to connect to the gateways that you configure with a higher priority.

Configure a GlobalProtect Gateway

Because the GlobalProtect portal configuration that is delivered to the apps includes the list of gateways to which the endpoint can connect, it is recommended that you configure the gateways before configuring the portal.

GlobalProtect Gateways are configured to provide two main functions:

- Enforce security policy for the GlobalProtect apps that connect to the gateways. You can also Configure HIP-Based Policy Enforcement on the gateway for enhanced security policy granularity.
- Provide virtual private network (VPN) access to the internal corporate network. VPN access is provided through an IPSec or SSL tunnel between the endpoint and the tunnel interface on the firewall hosting the gateway.

STEP 1 | Before you begin configuring the gateway make sure you have:

- ❑ Create Interfaces and Zones for GlobalProtect for the firewall on which you plan to configure each gateway. For gateways that require tunnel connections, you must configure both the physical interface and the virtual tunnel interface.
- ❑ Enable SSL Between GlobalProtect Components required for the GlobalProtect app to establish an SSL connection with the gateway.
- ❑ GlobalProtect User Authentication that will be used to authenticate GlobalProtect users.

STEP 2 | Add a gateway.

1. **Add** a new gateway (**Network** > **GlobalProtect** > **Gateways**).
2. **Name** the gateway.

   The gateway name cannot contain spaces and must be unique for each virtual system. As a best practice, include the location or other descriptive information to help users and administrators identify the gateway.
3. (Optional) Select the virtual system **Location** to which this gateway belongs.

STEP 3 | Specify the network information that enables endpoints to connect to the gateway.

If it does not already exist, Create Interfaces and Zones for GlobalProtect.

> *Do not attach an interface management profile that allows HTTP, HTTPS, Telnet, or SSH to the interface where you configure; doing so enables access to your management interface from the internet. Follow* Adminstrative Access Best Practices *to ensure that you are securing administrative access to your firewalls in a way that will prevent successful attacks.*

1. Select the **Interface** for the endpoints to use when communicating with the gateway.
2. Specify the **IP Address Type** and **IP Address** for the gateway web service:
   - Set the **IP Address Type** to **IPv4 Only**, **IPv6 Only**, or **IPv4 and IPv6.** Use **IPv4 and IPv6** if your network supports dual stack configurations, where IPv4 and IPv6 run at the same time.
   - The IP address must be compatible with the IP address type. For example, `172.16.1.0` for IPv4 addresses or `21DA:D3:0::2F3b` for IPv6 addresses. For dual stack configurations, enter both an IPv4 and IPv6 address.

STEP 4 | Configure Decryption log settings.

You can log successful and unsuccessful TLS/SSL handshakes and you can forward Decryption logs to Log Collectors, other storage devices, and to specific administrators.

- By default, the firewall logs only unsuccessful TLS handshakes. It is a best practice to log successful handshakes as well so that you gain visibility into as much decrypted traffic as available resources permit (but don't decrypt private or sensitive traffic; follow decryption best practices and decrypt as much traffic as you can).
- If you have not already done so, create a Log Forwarding profile to forward Decryption logs and specify it in the Gateway configuration.
- If you log successful TLS handshakes in addition to unsuccessful TLS handshakes, configure a larger log storage space quota for the Decryption log (**Device** > **Setup** > **Management** > **Logging and Reporting Settings** > **Log Storage**). The default quota (allocation) is one percent of the device's log storage capacity for Decryption logs and one percent for the general decryption summary. There is no default allocation for hourly, daily, or weekly decryption summaries. Configure Decryption Logging provides more information about how to allocate firewall log space to Decryption logs.

STEP 5 | Specify how the gateway authenticates users.

If an SSL/TLS service profile for the gateway does not already exist, Deploy Server Certificates to the GlobalProtect Components.

If authentication profiles or certificate profiles do not already exist, use the GlobalProtect User Authentication to configure these profiles for the gateway.

Configure any of the following gateway **Authentication** settings (**Network** > **GlobalProtect** > **Gateways** > ***<gateway-config>*** > **Authentication**):

- To secure communication between the gateway and the GlobalProtect app, select the **SSL/TLS Service Profile** for the gateway.

  *The **Max Version** of TLS in the **SSL/TLS Service Profile** is **TLSv1.2**. **TLSv1.3** is currently not supported for the GlobalProtect app and Clientless VPN connections.*

  *To provide the strongest security, set the **Min Version** of the SSL/TLS service profile to **TLSv1.2**.*

- To authenticate users with a local user database or an external authentication service, such as LDAP, Kerberos, TACACS+, SAML, or RADIUS (including OTP), **Add** a **Client Authentication** configuration with the following settings:
  - Specify a **Name** to identify the client authentication configuration.
  - Identify the type of **OS** (operating system) to which this configuration applies. By default, the configuration applies to **Any** operating system.
  - Select or add an **Authentication Profile** to authenticate endpoints seeking access to the gateway.
  - Enter a custom **Username Label** for gateway login (for example, **`Email Address (username@domain)`**.
  - Enter a custom **Password Label** for gateway login (for example, **`Passcode`** for two-factor, token-based authentication).
  - Enter an **Authentication Message** to help end-users understand which credentials to use during login. The message can be up to 256 characters in length (default is `Enter login credentials`).
  - Select one of the following options to define whether users can authenticate to the gateway using credentials and/or client certificates:
    - To require users to authenticate to the gateway using both user credentials AND a client certificate, set the **Allow Authentication with User Credentials OR Client Certificate** option to **No (User Credentials AND Client Certificate Required)** (default).
    - To allow users to authenticate to the gateway using either user credentials OR a client certificate, set the **Allow Authentication with User Credentials OR Client Certificate** option to **Yes (User Credentials OR Client Certificate Required)**.

      When you set this option to **Yes**, the gateway first checks the endpoint for a client certificate. If the endpoint does not have a client certificate or you do not configure a

certificate profile for your client authentication configuration, the endpoint user can then authenticate to the gateway using his or her user credentials.

- To authenticate users based on a client certificate or a smart card/CAC, select the corresponding **Certificate Profile**. You must pre-deploy the client certificate or Deploy User-Specific Client Certificates for Authentication using the Simple Certificate Enrollment Protocol (SCEP).
  - If you want to require users to authenticate to the gateway using both their user credentials and a client certificate, you must specify both a **Certificate Profile** and an authentication profile
  - If you want to allow users to authenticate to the gateway using either their user credentials or a client certificate and you specify an **Authentication Profile** for user authentication, then the **Certificate Profile** is optional.
  - If you want to allow users to authenticate to the gateway using either their user credentials or a client certificate and you don't select an **Authentication Profile** for user authentication, then the **Certificate Profile** is required.
  - If you do not configure any **Authentication Profile** that matches a specific OS, then the **Certificate Profile** is required.

  *If you allow users to authenticate to the gateway using either user credentials or a client certificate, do not select a **Certificate Profile** that has the **Username Field** configured as **None**.*

- To use two-factor authentication, select both an **Authentication Profile** and a **Certificate Profile**. This requires the user to authenticate successfully using both methods to gain access.

  (Chrome only) If you configure the gateway to use client certificates and LDAP for two-factor authentication, Chromebooks that run Chrome OS 47 or later versions encounter excessive prompts to select the client certificate. To prevent excessive prompts, configure a policy to specify the client certificate in the Google Admin console and then deploy that policy to your managed Chromebooks.

  1. *Log in to the Google Admin console and select **Device management** > **Chrome management** > **User settings**.*
  2. *In the Client Certificates section, enter the following URL pattern to **Automatically Select Client Certificate for These Sites**:*

     ```
     {"pattern": "https://[*.]","filter":{}}
     ```

  3. *Click **Save**. The Google Admin console deploys the policy to all devices within a few minutes.*
  4. *To block GlobalProtect users from logging in from quarantined devicesto the GlobalProtect gateway, select **Block login for quarantined devices.***

STEP 6 | Enable tunneling and then configure the tunnel parameters.

Tunnel parameters are required for an external gateway; they are optional for an internal gateway.

To force the use of SSL-VPN tunnel mode, disable (clear) the **Enable IPSec** option. By default, SSL-VPN is used only if the endpoint fails to establish an IPSec tunnel.

*Extended authentication (X-Auth) is supported only on IPSec tunnels. If you **Enable X-Auth Support**, GlobalProtect IPSec Crypto profiles are not used.*

GlobalProtect app is not able to connect to the GlobalProtect Gateway via IPSec tunnel if source NAT is configured on the same firewall for the GlobalProtect client's public IP address. In this case, the tunnel connection will fall back to SSL.

For more information on supported cryptographic algorithms, refer to Reference: GlobalProtect App Cryptographic Functions.

1. In the GlobalProtect Gateway Configuration dialog, select **Agent** > **Tunnel Settings**.
2. Enable **Tunnel Mode** to enable split tunneling.
3. Select the **Tunnel Interface** that you defined when you Create Interfaces and Zones for GlobalProtect.
4. (Optional) Specify the maximum number of users (**Max User**) that can access the gateway at the same time for authentication, HIP updates, and GlobalProtect app updates. The range of values is displayed when the field is empty and varies based on the platform.
5. **Enable IPSec** and then select a **GlobalProtect IPSec Crypto** profile to secure the VPN tunnels between the GlobalProtect app and the gateway. The **default** profile uses AES-128-CBC encryption and sha1 authentication.

   IPSec is not supported with Windows 10 UWP endpoints.

   You can also create a **New GlobalProtect IPSec Crypto** profile (**GlobalProtect IPSec Crypto** drop-down) and then configure the following settings:

   1. Specify a **Name** to identify the profile.
   2. **Add** the **Authentication** and **Encryption** algorithms that VPN peers can use to negotiate the keys for securing data in the tunnel:
      - **Encryption**—If you don't know what the VPN peers support, you can add multiple encryption algorithms in top-to-bottom order of most-to-least secure, as follows: **aes-256-gcm**, **aes-128-gcm**, **aes-128-cbc**. The peers will negotiate the strongest algorithm to establish the tunnel.
      - **Authentication**—Select the authentication algorithm (**sha1**) to provide data integrity and authenticity protection. Although the authentication algorithm is required for the profile, this setting only to the AES-CBC cipher (**aes-128-cbc**). If

you use an AES-GCM encryption algorithm (**aes-256-gcm** or **aes-128-gcm**), the setting is ignored because these ciphers provide native ESP integrity protection.

3. Click **OK** to save the profile.

6. (Optional) **Enable X-Auth Support** if any endpoint must connect to the gateway using a third-party VPN (for example, a VPNC client running on Linux). If you enable X-Auth, you must provide the **Group** name and **Group Password** (if the endpoint requires it). By default, the user is not required to re-authenticate if the key that establishes the IPSec tunnel expires. To require users to re-authenticate, disable the option to **Skip Auth on IKE Rekey**.

   Extended authentication (X-Auth) is not supported for Prisma Access deployments.

   *To **Enable X-Auth Support** for strongSwan endpoints, you must also disable the option to **Skip Auth on IKE Rekey** because these endpoints require re-authentication during IKE SA negotiation. In addition, you must add the `closeaction=restart` setting to the `conn %default` section of the strongSwan IPSec configuration file. (See Set Up Authentication for strongSwan Ubuntu and CentOS Endpoints for more information on the StrongSwan IPSec configuration.)*

   Although X-Auth access is supported on iOS and Android endpoints, it provides limited GlobalProtect functionality on these endpoints. Instead, use the GlobalProtect app for simplified access to all security features that GlobalProtect provides on iOS and Android endpoints. The GlobalProtect app for iOS is available in the Apple App Store. The GlobalProtect app for Android is available in Google Play.

STEP 7 | (Tunnel Mode Only) Specify selection criteria for your client settings configurations.

The gateway uses the selection criteria to determine which configuration to deliver to the GlobalProtect apps that connect. If you have multiple configurations, you must make sure to order them correctly. As soon as the gateway finds a match (based on the **Source User**, **OS**, and **Source Address**), it delivers the associated configuration to the user. Therefore, more specific configurations must precede more general ones. See step 13 for instructions on ordering the list of configurations for client settings.

*You cannot **Enable X-Auth Support** when you specify the selection criteria for your client settings configurations.*

1. In the GlobalProtect Gateway Configuration dialog, select **Agent** > **Client Settings**.
2. Select an existing client settings configuration or **Add** a new one. You can add up to 64 client configuration entries for a single gateway.
3. Configure the following **Config Selection Criteria**:
   - To deploy this configuration to specific users or user groups, **Add** the **Source User** (or user group). To deploy this configuration only to users with apps in pre-logon mode,

select **pre-logon** from the **Source User** drop-down; to deploy this configuration to all users, select **any**.

To deploy the configuration to specific groups, you must first map users to groups as described when you Enable Group Mapping.

- To deploy this configuration based on the endpoint operating system, **Add** an **OS** (such as Android or Chrome). To deploy this configuration to all operating systems, select **Any**.
- To deploy this configuration based on user location, **Add** a source **Region** or **IP address** (IPv4 and IPv6). To deploy this configuration to all user locations, do not specify the **Region** or **IP Address**.

4. Click **OK** to save your configuration selection criteria.

STEP 8 | (Tunnel Mode Only) Configure authentication override settings to enable the gateway to generate and accept secure, encrypted cookies for user authentication.

This capability allows the user to provide login credentials only once during the specified period of time (for example, every 24 hours).

By default, gateways authenticate users with an authentication profile and optional certificate profile. When authentication override is enabled, GlobalProtect caches the result of a successful login and uses the cookie to authenticate the user instead of prompting the user

for credentials. For more information, see Cookie Authentication on the Portal or Gateway. If client certificates are required, the endpoint must also provide a valid certificate to gain access.

If you must immediately block access to a device whose cookie has not expired (for example, if the device is lost or stolen), you can immediately Identification and Quarantine of Compromised Devices Overview and License Requirements by adding the device to a quarantine list.

1. On the GlobalProtect Gateway Configuration dialog, select **Agent** > **Client Settings**.
2. Select an existing client settings configuration or **Add** a new one.
3. Configure the following **Authentication Override** settings:
   - **Name**—Identifies the configuration.
   - **Generate cookie for authentication override**—Enables the gateway to generate encrypted, endpoint-specific cookies and issue authentication cookies to the endpoint.

     The authentication cookie includes the following fields:
     - `user`—Username that is used to authenticate the user.
     - `domain`—Domain name of the user.
     - `os`—Application name that is used on the device.
     - `hostID`—Unique ID that is assigned by GlobalProtect to identify the host.
     - `gen time`—Date and time that the authentication cookie was generated.
     - `ip`—IP address of the device that is used to successfully authenticate to GlobalProtect and to obtain the cookie.
   - **Accept cookie for authentication override**—Enables the gateway to authenticate users with a valid, encrypted cookie. When the app presents a valid cookie, the gateway verifies that the cookie was encrypted by the portal or gateway, decrypts the cookie, and then authenticates the user.

     The GlobalProtect app must know the username of the connecting user in order to match and retrieve the associated authentication cookies from the user's endpoint. After the app retrieves the cookies, it sends them to the portal or gateway for user authentication.

     *(Windows only) If you set the List item. option to **Yes** (SSO is enabled) in the portal agent configuration (**Network** > **GlobalProtect** > **Portals** > **<portal-config>** > **Agent** > **<agent-config>.** > **App**), the GlobalProtect app uses the Windows username to retrieve the local authentication cookie for the user. If you set the **Use Single Sign-On** option to **No** (SSO is disabled), you must enable the GlobalProtect app to List item. in order for the app to retrieve the authentication cookie for the user. Set the **Save User Credentials** option to **Yes** to save both the username and password or **Save Username Only** to save only the username.*
   - **Cookie Lifetime**—Specifies the hours, days, or weeks for which the cookie is valid (default is 24 hours). The range for hours is 1 to 72; for weeks is 1 to 52; and for days is 1 to 365. After the cookie expires, the user must re-enter their login credentials and

then the gateway subsequently encrypts a new cookie to send to the app. This value can be the same as or different from the **Cookie Lifetime** that you configure for the portal.

- **Certificate to Encrypt/Decrypt Cookie**—Selects the RSA certificate used to encrypt and decrypt the cookie. You must use the same certificate on the portal and gateway.

  As a best practice, configure the RSA certificate to use the strongest digest algorithm that your network supports.

  The portal and gateway use the RSA encrypt padding scheme PKCS#1 V1.5 to generate the cookie (using the public certificate key) and to decrypt the cookie (using the private certificate key).

STEP 9 | (Tunnel Mode only—Optional) Configure client level IP pools used to assign IPv4 or IPv6 addresses to the virtual network adapters on the endpoints that connect to the gateway.

*You must only either the client level (**Network** > **GlobalProtect** > **Gateways** > **<gateway-config>** > **GlobalProtect Gateway Configuration** > **Agent** > **Client Settings** > **<client-setting>** > **Configs** > **IP Pools**) or the gateway level (**Network** > **GlobalProtect** > **Gateways** > **<gateway-config>** > **GlobalProtect Gateway Configuration** > **Agent** > **Client IP Pool**).*

IP pools and split tunnel settings are not required for internal gateway configurations in non-tunnel mode because apps use the network settings assigned to the physical network adapter.

Using address objects when configuring gateway IP address pools is not supported.

1. On the GlobalProtect Gateway Configuration dialog, select **Agent** > **Client Settings**.
2. Select an existing client settings configuration or **Add** a new one.
3. Configure any of the following **IP Pools** settings:
   - To specify the authentication server IP address pool for endpoints that require static IP addresses, enable the option to **Retrieve Framed-IP-Address attribute from authentication server** and then **Add** the subnet or IP address range to the **Authentication Server IP Pool**. When the tunnel is established, an interface is created on the remote user's computer with an address in the subnet or IP range that matches the Framed-IP attribute of the authentication server.

     The authentication server IP address pool must be large enough to support all concurrent connections. IP address assignment is static and retained even after the user disconnects.
   - To specify the **IP Pool** used to assign IPv4 or IPv6 addresses to the endpoints that connect to the gateway, **Add** the IP address subnet/range. You can add IPv4 or IPv6 subnets or ranges, or a combination of the two.

     To ensure proper routing back to the gateway, you must use a different range of IP addresses from those assigned to existing IP pools on the gateway (if applicable) and

to the endpoints that are physically connected to your LAN. We recommend that you use a private IP addressing scheme.

4. Click **OK** to save the IP pool configuration.

STEP 10 | (Tunnel Mode only—Optional) Configure a Split Tunnel Based on the Access Route(including local subnet traffic) goes through the VPN tunnel for inspection and policy enforcement.

STEP 11 | (Tunnel Mode only—Optional) Configure a Split Tunnel Based on the Access Route.

STEP 12 | (Tunnel Mode only—Optional) Configure a Split Tunnel Based on the Domain and Application.

STEP 13 | (Tunnel Mode only—Optional) Configure a Split Tunnel Based on the Domain and Application.

STEP 14 | (Tunnel Mode only—Optional) Configure DNS settings for a client settings configuration.

*If you configure at least one DNS server or DNS suffix in the client settings configuration (**Network** > **GlobalProtect** > **Gateways** > **<gateway-config>** > **Agent** > **Client Settings** > **<client-settings-config>** > **Network Services**), the gateway sends the configuration for both the DNS server and DNS suffix to the endpoint. This occurs even when you configure global (gateway level) DNS servers and DNS suffixes.*

*If you do not configure any DNS servers or DNS suffixes in the client settings configuration, the gateway sends the global DNS servers and DNS suffixes to the endpoint, if configured (**Network** > **GlobalProtect** > **Gateways** > **<gateway-config>** > **Agent** > **Network Services**).*

1. In the GlobalProtect Gateway Configuration dialog, select **Agent** > **Client Settings**.
2. Select an existing client settings configuration or **Add** a new one.
3. Configure any of the following **Network Services** settings:
   - Specify the IP address of the **DNS Server** to which the GlobalProtect app with this client settings configuration sends DNS queries. You can add up to 10 DNS servers by separating each IP address with a comma.
   - Specify the **DNS Suffix** that the endpoint should use locally when encountering an unqualified hostname, which the endpoint cannot resolve.

STEP 15 | (Tunnel Mode Only) Arrange the gateway agent configurations so that the proper configuration is deployed to each GlobalProtect app.

When an app connects, the gateway compares the source information in the packet against the agent configurations you defined (**Agent** > **Client Settings**). As with security rule evaluation, the gateway looks for a match starting from the top of the list. When it finds a match, it delivers the corresponding configuration to the app.

- To move a gateway configuration up in the list of configurations, select the configuration and **Move Up**.
- To move a gateway configuration down in the list of configurations, select the configuration and **Move Down**.

STEP 16 | (Tunnel Mode Only—Optional) Configure the global IP address pools used to assign IPv4 or IPv6 addresses to the virtual network adapters on all endpoints that connect to the gateway.

This option enables you to simplify the configuration by defining IP pools at the gateway level instead of defining IP pools for each client setting in the gateway configuration.

*You must configure IP pools only at either the gateway level (**Network** > **GlobalProtect** > **Gateways** > **<gateway-config>** > **Agent** > **Client IP Pool**) or the client level (**Network** > **GlobalProtect** > **Gateways** > **<gateway-config>** > **Agent** > **Client Settings** > **<client-setting>** > **IP Pools**).*

Using address objects when configuring gateway IP address pools is not supported.

1. In the GlobalProtect Gateway Configuration dialog, select **Agent** > **Client IP Pool**.
2. **Add** the IP address subnet or range used to assign IPv4 or IPv6 addresses to all endpoints that connect to the gateway. You can add IPv4 or IPv6 subnets or ranges, or a combination of the two.

   To ensure proper routing back to the gateway, you must use a different range of IP addresses from those assigned to existing IP pools on the gateway (if applicable) and to the endpoints that are physically connected to your LAN. We recommend that you use a private IP addressing scheme.

STEP 17 | (Tunnel Mode Only) Specify the network configuration settings for the endpoint.

Network settings are not required for internal gateway configurations in non-tunnel mode because the GlobalProtect app uses the network settings assigned to the physical network adapter.

In the GlobalProtect Gateway Configuration dialog, select **Agent** > **Network Services** and then configure any of the following network configuration settings:

- If the firewall has an interface that is configured as a DHCP client, set the **Inheritance Source** to that interface so the GlobalProtect app is assigned the same settings as the DHCP client. You can also enable the option to **Inherit DNS Suffixes** from the inheritance source.
- Manually assign the **Primary DNS** server, **Secondary DNS** server, **Primary WINS** server, **Secondary WINS** server, and **DNS Suffix**. You can enter multiple DNS suffixes (up to 100) by separating each suffix with a comma.

  *The **DNS Suffix** cannot contain any non-ASCII characters.*

STEP 18 | (Optional) Modify the default timeout settings for endpoints.

In the GlobalProtect Gateway Configuration dialog, select **Agent** > **Connection Settings** and then configure the following in the Timeout Configuration area:

- Modify the endpoint session timeout settings for Modify Endpoint Session Timeout Settings.
- Set and schedule the display of Enable End-user Notifications about GlobalProtect Session Logout for login lifetime, inactivity logout, and administrator initiated logout.
- (Optional) Modify the default expiration notifcation and Enable End-user Notifications about GlobalProtect Session Logout that you want to display to users when their user sessions are about to expire.

STEP 19 | (Optional) Configure automatic restoration of SSL VPN tunnels.

If the GlobalProtect connection is lost due to network instability or a change in the endpoint state, you can allow or prevent the GlobalProtect app from automatically reestablishing the VPN tunnel for specific gateways by configuring automatic restoration of SSL VPN tunnels.

1. In the GlobalProtect Gateway Configuration dialog, select **Agent** > **Connection Settings**.
2. Configure one of the following options for Authentication Cookie Usage Restrictions:
   - To prevent the GlobalProtect app from automatically reestablishing the VPN tunnel for this gateway, **Disable Automatic Restoration of SSL VPN**.
   - To allow the GlobalProtect app to automatically reestablish the VPN tunnel for this gateway, disable (clear) the option to **Disable Automatic Restoration of SSL VPN** (default).

STEP 20 | (Optional) Configure source IP address enforcement for authentication cookies.

You can configure the GlobalProtect portal or gateway to accept cookies from endpoints only when the IP address of the endpoint matches the original source IP addresses for which the cookie was issued or when the IP address of the endpoint matches a specific network IP address range. You can define the network IP address range using a CIDR subnet mask, such as /24 or /32. For example, if an authentication cookie was originally issued to an endpoint with a public source IP address of 201.109.11.10, and the subnet mask of the network IP address range is set to /24, the authentication cookie is subsequently valid on endpoints with public source IP addresses within the 201.109.11.0/24 network IP address range.

1. In the GlobalProtect Gateway Configuration dialog, select **Agent** > **Connection Settings**.
2. In the Authentication Cookie Usage Restrictions section, **Restrict Authentication Cookie Usage (for Automatic Restoration of VPN tunnel or Authentication Override)** and then configure one of the following conditions:
   - If you select **The original Source IP for which the authentication cookie was issued**, the authentication cookie is valid only if the public source IP address of the endpoint that is attempting to use the cookie is the same public source IP address of the endpoint to which the cookie was originally issued.
   - If you select **The original Source IP network range**, the authentication cookie is valid only if the public source IP address of the endpoint attempting to use the cookie is within the designated network IP address range. Enter a **Source IPv4 Netmask** or

Source IPv6 Netmask to define the subnet mask of the network IP address range for which the authentication cookie is valid (for example, **32** or **128**).

STEP 21 | (Tunnel Mode Only) Exclude Video Traffic from the GlobalProtect VPN Tunnel.

STEP 22 | (Optional) Define the notification messages that end users see when a security rule with a host information profile (HIP) is enforced.

This step applies only if you created host information profiles and added them to your security policies. See Host Information for details on configuring the HIP feature and information about creating HIP notification messages.

1. On the GlobalProtect Gateway Configuration dialog, select **Agent** > **HIP Notification**.
2. Select an existing HIP notification configuration or **Add** a new one.
3. Configure the following settings:
   - Select the **Host Information** object or profile to which this message applies.
   - Depending on whether you want to display the message when the corresponding HIP profile is matched in policy or when the profile is not matched, select **Match Message** or **Not Match Message** and then **Enable** notifications. You can create messages for both a match and a non-match instance based on the objects on which you are matching and what your objectives are for the policy. For the **Match Message**, you can also enable the option to **Include Mobile App List** to indicate what applications can trigger the HIP match.
   - Select whether you want to display the message as a **System Tray Balloon** or as a **Pop Up Message**.
   - Enter and format the text of your message (**Template**) and then click **OK**.
   - Repeat these steps for each message you want to define.

STEP 23 | Save the gateway configuration.

1. Click **OK** to save the settings.
2. **Commit** the changes.

STEP 24 | (Optional) To configure the GlobalProtect app to display a label that identifies the location of this gateway when end users are connected, specify the physical location of the firewall on which you configured this gateway.

When end users experience unusual behavior, such as poor network performance, they can provide this location information to their support or Help Desk professionals to assist with troubleshooting. They can also use this location information to determine their proximity to

the gateway. Based on their proximity, they can evaluate whether they need to switch to a closer gateway.

If you do not specify a gateway location, the GlobalProtect app displays an empty location field.

- **In the CLI**—Use the following CLI command to specify the physical location of the firewall on which you configured the gateway:

```
<username@hostname> set deviceconfig setting global-protect
 location <location>
```

- **In the XML API**—Use the following XML API to specify the physical location of the firewall on which you configured the gateway:
  - **devices**—name of the firewall on which you configured the gateway
  - **location**—location of the firewall on which you configured the gateway

```
curl -k -F file=@filename.txt -g 'https://<firewall>/api/?
key=<apikey>&type=config&action=set&xpath=/config/devices/
entry[@name='<device-name>']/deviceconfig/setting/global-
protect&element=<location>location-string</location>'
```


Customize Endpoint Session Timeout Settings

Where Can I Use This?	What Do I Need?
• GlobalProtect Subscription • Prisma Access	❑ Prisma Access License ❑ GlobalProtect app version 6.2 or later and PAN-OS version 11.0.2 or later for Extend User Session OS Support: Windows and macOS Content release version: 8692-16961 ❑ GlobalProtect app version 6.1 or later and PAN-OS version 11.0 or later for End-user Notification about GlobalProtect Session Logout OS Support: Linux, Windows 10, ARM64-Based Windows 10, macOS 11 and later releases, and ARM-Based macOS 11 and later releases

GlobalProtect user sessions are created when a user connects to the GlobalProtect gateway and successfully authenticates. The session is then assigned to a specific gateway, that detemines which traffic to tunnel based on any defined split tunnel rules. The session can be customized in a number of ways, including the following:

- Set the Modify Endpoint Session Timeout Settings.
- Configure the types of applications that are allowed to be used during the session.
- Set the security policies that are applied to the session.
- Schedule the Enable End-user Notifications about GlobalProtect Session Logout about GlobalProtect session logout.
- Create Enable End-user Notifications about GlobalProtect Session Logout that you want to display to users when the sessions are about to expire.

By customizing the user sessions, you can ensure that users have the access they need to get their work done, while also protecting your network from unauthorized access.

Modify Endpoint Session Timeout Settings

Modify the **Timeout Configuration** as needed:

STEP 1 | Select **Network** > **GlobalProtect** > **Gateways** > **Agent** > **Connection Settings**

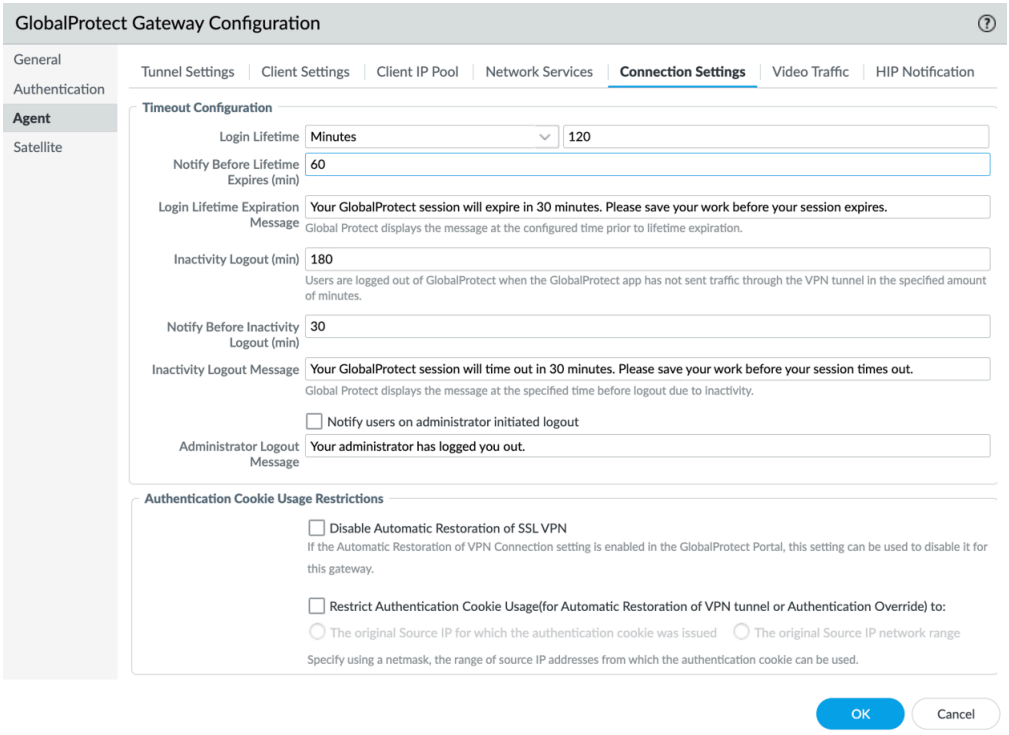
STEP 2 | In the Timeout Configuration area:

1. Modify the maximum **Login Lifetime** for a single gateway login session (default is 30 days). During the lifetime, the user stays logged in as long as the gateway receives a HIP

check from the endpoint within the **Inactivity Logout** period. After this time, the login session ends automatically.

2. Modify the **Inactivity Logout** period to specify the amount of time after which idle users are logged out of GlobalProtect. You can enforce a security policy to monitor traffic from endpoints while connected to GlobalProtect and to quickly log out inactive GlobalProtect sessions. You can enforce a shorter inactivity logout period. Users are logged out of GlobalProtect if the GlobalProtect app has not routed traffic through the VPN tunnel or if the gateway does not receive a HIP check from the endpoint within the configured time period.

   You must specify the **Inactivity Logout** period to be greater than the Automatic Restoration of VPN Connection Timeout to allow GlobalProtect to attempt to reestablish the connection after the tunnel is disconnected (range is 0 to 180 minutes; default is 30 minutes). When you configure an internal gateway in non-tunnel mode, the **Inactivity Logout** period must be greater than the current HIP check interval value that the GlobalProtect app waits before it sends the HIP report.



STEP 3 | (Optional) Enable end-user notifications about GlobalProtect session and create custom messages.

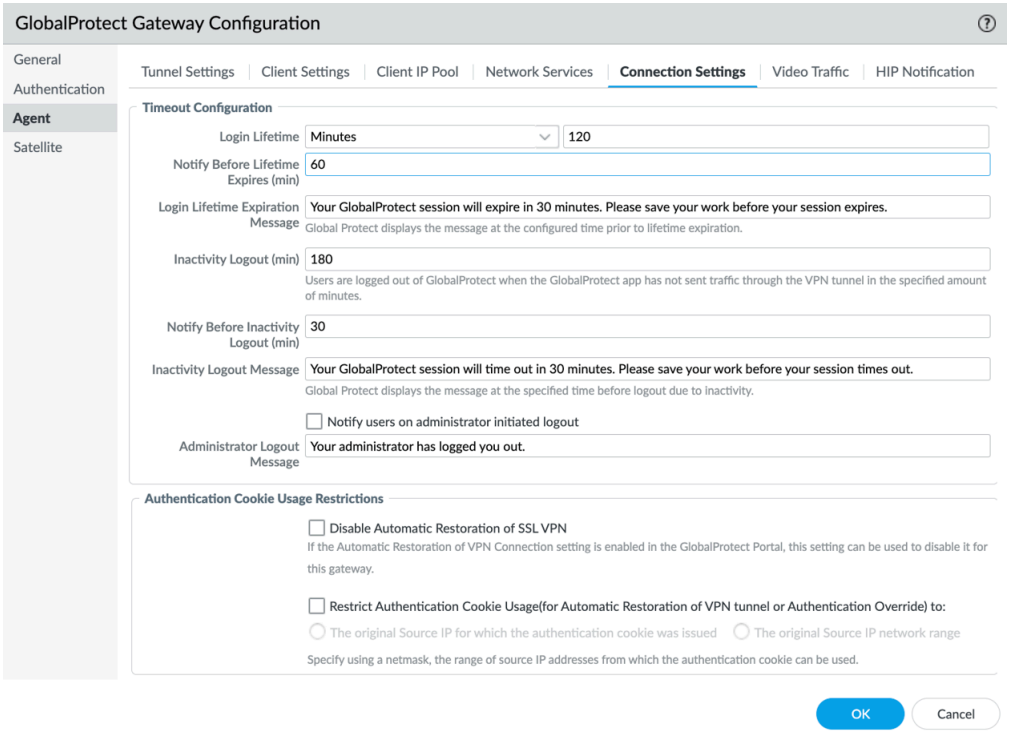
STEP 4 | Click **OK** to save the session timeout settings.

STEP 5 | **Commit** the changes.

Enable End-user Notifications about GlobalProtect Session Logout

To enable end-user notifications about GlobalProtect session logout and create custom messages:

STEP 1 | Select **Network** > **GlobalProtect** > **Gateways** > **Agent** > **Connection Settings**



STEP 2 | In the Timeout Configuration area, you can schedule the display of end-user notifications about GlobalProtect session logout and create custom messages:

1. Set the **Notify Before Lifetime Expires** time in minutes (default is 30 minutes) to schedule the display of login lifetime expiry notifications on the GlobalProtect app. The **Notify Before Lifetime Expires** must be lesser than the **Login Lifetime**. For example, if you set the **Notify Before Lifetime Expires** as 120 minutes, the app will display the notification to the user 2 hours before the expiry of the login lifetime. If you do not want the notification to be displayed, set the value to 0. If you configure the extend user session feature through the app settings of the GlobalProtect portal, the login lifetime expiry notification pop-up displays the option to extend the duration of user session so that users are not logged out of their session abruptly.
2. (Optional) Modify the default **Login Lifetime Expiration Message** to create a custom login lifetime expiration message. The maximum message length is 127 characters.
3. Set the **Notify Before Inactivity Logout** time in minutes (default is 30 minutes) to schedule the display of inactivity logout notification on the app. The **Notify Before Inactivity Logout** must be lesser than the **Inactivity Logout** period. For example, if you set the **Notify Before Inactivity Logout** as 20 minutes, the app will display the

notification to the user 20 minutes before the inactive session expires. If you do not want the notification to be displayed, set the value to 0.

4. (Optional) Modify the **Inactivity Logout Message** to create a custom message that you want to display to users when their inactive sessions are about to expire. The maximum message length is 127 characters.
5. Enable **Notify users on administrator initiated logout** if you want the app to display notification to users after the administrator initiated logout happens.
6. (Optional) Modify the **Administrator Logout Message** to create a custom message that you want to display to users after the administrator initiated logout happens. The maximum message length is 127 characters.
7. Click **OK** to save the notification settings.
8. **Commit** the changes.

Split Tunnel Traffic on GlobalProtect Gateways

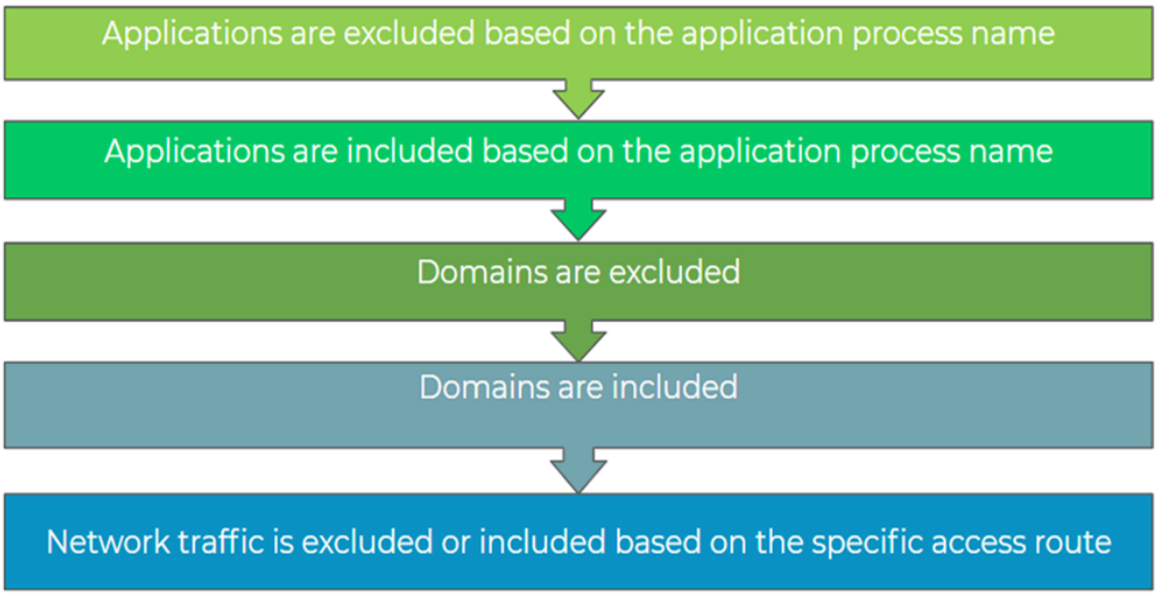
Where Can I Use This?	What Do I Need?
• macOS and Windows endpoints running any currently supported GlobalProtect app version. • Linux endpoints running GlobalProtect app 6.1 or later. Linux endpoints support domain and access route-based split tunneling only; application-based split tunneling not supported on Linux.	• GlobalProtect gateway subscription

You can configure split tunnel traffic based on an access route, destination domain, application, and HTTP/HTTPS video streaming application.

The split tunnel capability allows you to conserve bandwidth and route traffic to:

- Tunnel enterprise SaaS and public cloud applications for comprehensive SaaS application visibility and control to avoid risks associated with Shadow IT in environments where it is not feasible to tunnel all traffic.
- Send latency-sensitive traffic, such as VoIP, outside the VPN tunnel, while all other traffic goes through the VPN for inspection and policy enforcement by the GlobalProtect gateway.
- Exclude HTTP/HTTPS video streaming traffic from the VPN tunnel. Video streaming applications, such as YouTube and Netflix, consume large amounts of bandwidth. By excluding lower risk video streaming traffic from the VPN tunnel, you can decrease bandwidth consumption on the gateway.

The split tunnel rules are applied following order:



On Linux endpoints, only domain and access route rules are applied.

Refer to the following sections on how to configure split tunnel traffic on the gateways:

- Configure a Split Tunnel Based on the Access Route
- Configure a Split Tunnel Based on the Domain and Application
- Exclude Video Traffic from the GlobalProtect VPN Tunnel
- Host a Split Tunnel Configuration File on a Web Server

Configure a Split Tunnel Based on the Access Route

If you do not include or exclude routes, every request is routed through the VPN tunnel (without a split tunnel). You can include or exclude specific destination IP subnet traffic from being sent over the VPN tunnel. The routes that you send through the VPN tunnel can be defined either as the routes you include in the tunnel, or as routes that you exclude from the tunnel, or both. For example, you can set up a split tunnel to allow remote users to access the internet without going through the VPN tunnel. More specific routes take precedence over less-specific routes.

When you define split tunnel traffic to include access routes, these are the routes that the gateway pushes to the remote users' endpoints to specify what traffic the users' endpoints can send through the VPN tunnel. When you define split tunnel traffic to exclude access routes, these routes are sent through the physical adapter on the endpoint instead of sent through the GlobalProtect VPN tunnel through the virtual adapter (the tunnel). By excluding split tunnel traffic by access routes, you can send latency sensitive or high bandwidth consuming traffic outside of the VPN tunnel while all other traffic is routed through the VPN for inspection and policy enforcement by the GlobalProtect gateway.

Local routes take precedence over routes sent from the gateway. When you enable the split tunnel, users can reach proxies and local resources (such as local printers) directly without sending any local subnet traffic through the VPN tunnel. By disabling the split tunnel, you can force all traffic to go through the VPN tunnel for inspection and policy enforcement whenever users are connected to GlobalProtect. You can consider the following IPv4 and IPv6 traffic behavior based on whether you enable or disable direct access to local networks.

Table 1: IPv4 Traffic Behavior

IPv4 Traffic to Local Subnet	No Direct Access to Local Network is Enabled		No Direct Access to Local Network is Disabled	
	Before the tunnel is established	After the tunnel is established	Before the tunnel is established	After the tunnel is established
New Incoming Traffic	Traffic is allowed on the local subnet through the physical adapter.	(Windows 10 only) When split tunneling based on the	Traffic is allowed on the local subnet through the physical adapter.	Traffic is allowed on the local subnet through the physical adapter.

IPv4 Traffic to Local Subnet	No Direct Access to Local Network is Enabled		No Direct Access to Local Network is Disabled	
		destination domain and application is not enabled, traffic adhering to the routing table is sent through the VPN tunnel. Certain applications can still bind to a specific interface directly and route the traffic through physical interface ignoring the routing table. When you enable split tunneling based on the destination domain and application, traffic is allowed on the local subnet through the physical adapter. (macOS and Linux) Traffic is allowed on the local subnet through the physical adapter.		
New Outgoing Traffic	Traffic is allowed on the local subnet through the physical adapter.	Traffic is sent through the VPN tunnel.	Traffic is allowed on the local subnet through the physical adapter.	Traffic is allowed on the local subnet through the physical adapter.
Existing Traffic	Traffic is allowed on the local subnet through	(Windows) Traffic is terminated.	Traffic is allowed on the local subnet through	Traffic is allowed on the local subnet

IPv4 Traffic to Local Subnet	No Direct Access to Local Network is Enabled		No Direct Access to Local Network is Disabled	
	the physical adapter.	(macOS and Linux) Traffic is allowed on the local subnet through the physical adapter.	the physical adapter.	through the physical adapter.

Table 2: IPv6 Traffic Behavior

IPv6 Traffic to Local Subnet	No Direct Access to Local Network is Enabled		No Direct Access to Local Network is Disabled	
	Before the tunnel is established	After the tunnel is established	Before the tunnel is established	After the tunnel is established
New Incoming Traffic	Traffic is allowed on the local subnet through the physical adapter.	Traffic is allowed on the local subnet through the physical adapter.	Traffic is allowed on the local subnet through the physical adapter.	Traffic is allowed on the local subnet through the physical adapter.
New Outgoing Traffic	Traffic is allowed on the local subnet through the physical adapter.	Traffic (except fe80::/10 link-local addresses) is sent through the VPN tunnel.	Traffic is allowed on the local subnet through the physical adapter.	Traffic is allowed on the local subnet through the physical adapter.
Existing Traffic	Traffic is allowed on the local subnet through the physical adapter.	Traffic is allowed on the local subnet through the physical adapter.	Traffic is allowed on the local subnet through the physical adapter.	Traffic is allowed on the local subnet through the physical adapter.

Use the following steps to configure a split tunnel based on access routes.

STEP 1 | Before you begin:

1. Configure a GlobalProtect Gateway.
2. Select **Network** > **GlobalProtect** > **Gateways** > ***<gateway-config>*** to modify an existing gateway or add a new one.

STEP 2 | Enable a split tunnel.

1. In the **GlobalProtect Gateway Configuration** dialog, select **Agent** > **Tunnel Settings** to enable **Tunnel Mode**.
2. Configure a GlobalProtect Gateway for the GlobalProtect app.

STEP 3 | (Tunnel Mode only) Disable the split tunnel to ensure that all traffic (including local subnet traffic) goes through the VPN tunnel for inspection and policy enforcement.

1. In the **GlobalProtect Gateway Configuration** dialog, select **Agent** > **Client Settings** > ***<client-setting-config>*** to select an existing client settings configuration or add a new one.
2. Select **Split Tunnel** > **Access Route** and then enable the **No direct access to local network** option.

   If you enable this option, direct access to local network is disabled and users cannot send traffic directly to proxies or local resources while connected to GlobalProtect. Split tunnel traffic based on access route, destination domain, and application still works as expected.

STEP 4 | (Tunnel Mode only) Configure split tunnel settings based on the access route.

The split tunnel settings are assigned to the virtual network adapter on the endpoint when the GlobalProtect app establishes a tunnel with the gateway.

Avoid specifying the same access route as both an include and an exclude access route; doing so results in a misconfiguration.

You can route certain traffic to be included or excluded from the tunnel by specifying the destination subnets or address object (of type **IP Netmask**).

1. In the **GlobalProtect Gateway Configuration** dialog, select **Agent** > **Client Settings** > ***<client-setting-config>*** to select an existing client settings configuration or add a new one.
2. Configure any of the following access route-based **Split Tunnel** settings (**Split Tunnel** > **Access Route**):

   - (Optional) In the **Include** area, **Add** the destination subnets or address object (of type **IP Netmask**) to route only certain traffic destined for your LAN to GlobalProtect. You can include IPv6 or IPv4 subnets.

     On PAN-OS 8.0.2 and later releases, up to 100 access routes can be used to include traffic in a split tunnel gateway configuration. Unless combined with GlobalProtect app 4.1.x or a later release, up to 1,000 access routes can be used.

   - (Optional) In the **Exclude** area, **Add** the destination subnets or address object (of type **IP Netmask**) that you want the app to exclude. Excluded routes should be more specific than the included routes; otherwise, you may exclude more traffic than intended. You can exclude IPv6 or IPv4 subnets. The firewall supports up to 100 exclude access routes in a split tunnel gateway configuration. Unless combined with

GlobalProtect app 4.1 and later releases, then up to 200 exclude access routes can be used.

You cannot exclude access routes for endpoints running Android on Chromebooks. Only IPv4 routes are supported on Chromebooks.

3. Click **OK** to save the split tunnel configuration.

STEP 5 | Save the gateway configuration.

1. Click **OK** to save the settings.
2. **Commit** the changes.

Configure a Split Tunnel Based on the Domain and Application

When you configure a split tunnel to include all traffic—IPv4 and IPv6—based the destination domain and port (optional) or application, all traffic going to that specific domain or application is sent through the VPN tunnel for inspection and policy enforcement. For example, you can allow all Salesforce traffic to go through the VPN tunnel using the ***Salesforce.com** destination domain. By including all Salesforce traffic in the VPN tunnel, you can provide secure access to the entire Salesforce domain and subdomains. You can configure a split tunnel without specifying a destination IP address subnet, which extends the split tunnel capability to domains and applications with dynamic public IP addresses, such as SaaS and public cloud applications.

When you configure a split tunnel to exclude traffic—IPv4 and IPv6—based on the destination domain and port (optional) or application, all traffic for that specific application or domain is sent directly to the physical adapter on the endpoint without inspection. For example, you can exclude all Skype traffic from the VPN tunnel using the **C:\Program Files (x86)\Skype\Phone\Skype** application process name.

Follow these recommendations when configuring a split tunnel based on the destination domain and application:

- *With a GlobalProtect license, you can enforce or apply split tunnel rules based on the destination domain and application to Windows and macOS endpoints.*
- *On Linux endpoints running GlobalProtect app 6.1 or later you can apply split tunnel rules based on domain or access route only; split tunneling based on application is not supported on Linux endpoints.*
- *On Windows devices, domain-based tunneling supports TCP traffic only; UDP traffic is not supported in domain-based split tunneling on Windows.*
- *ICMP requests such as for latency, jitter, trace route tests are not supported for split tunneling based on the destination domain.*
- *Supported on endpoints with Windows 7 Service Pack 2 and later releases and macOS 10.10 and later releases.*

Use the following steps to configure a split tunnel to include or exclude traffic based on the destination domain or application process name.

STEP 1 | Before you begin:

1. Configure a GlobalProtect Gateway.
2. Select **Network** > **GlobalProtect** > **Gateways** > ***<gateway-config>*** to modify an existing gateway or add a new one.

STEP 2 | Enable a split tunnel.

1. In the **GlobalProtect Gateway Configuration** dialog, select **Agent** > **Tunnel Settings** to enable **Tunnel Mode**.
2. Configure a GlobalProtect Gateway for the GlobalProtect app.

STEP 3 | (Tunnel Mode only) Configure split tunnel settings based on the destination domain. These settings are assigned to the virtual network adapter on the endpoint when the GlobalProtect app establishes a tunnel with the gateway.

You can apply Customize the GlobalProtect App in addition to network traffic if you have already specified **Both Network Traffic and DNS** as the **Split-Tunnel Option** in the **App Configurations** area of your GlobalProtect portal.

1. In the GlobalProtect Gateway Configuration dialog, select **Agent** > **Client Settings** > ***<client-setting-config>*** to select an existing client settings configuration or add a new one.
2. (Optional) **Add** the SaaS or public cloud applications that you want to route to GlobalProtect through the VPN connection using the destination domain and port (**Split Tunnel** > **Domain and Application** > **Include Domain**). You can add up to 200 entries to the list. For example, add **`*.gmail.com`** to allow all Gmail traffic to go through the VPN tunnel.
3. (Optional) **Add** the SaaS or public cloud applications that you want to exclude from the VPN tunnel using the destination domain and port (**Split Tunnel** > **Domain and Application** > **Exclude Domain**). You can add up to 200 entries to the list. For example, add **`*.target.com`** to exclude all Target traffic from the VPN tunnel.
4. Click **OK** to save the split tunnel settings.

STEP 4 | (Tunnel Mode only) Configure split tunnel settings based on the application.

Safari traffic cannot be added to the application-based split tunnel rule on macOS endpoints.

You can use environment variables to configure a split tunnel based on the application on Windows and macOS endpoints.

1. In the GlobalProtect Gateway Configuration dialog, select **Agent** > **Client Settings** > ***<client-setting-config>*** to select an existing client settings configuration or add a new one.
2. (Optional) **Add** the SaaS or public cloud applications that you want to route to GlobalProtect through the VPN connection using the application process name (**Split Tunnel** > **Domain and Application** > **Include Client Application Process Name**. You can add up to 200 entries to the list. For example, add **`/Applications/RingCentral`**

`for Mac.app/Contents/MacOS/Softphone` to allow all RingCentral-based traffic to go through the VPN tunnel on macOS endpoints.

3. (Optional) **Add** the SaaS or public cloud applications that you want to exclude from the VPN tunnel using the application process name (**Split Tunnel** > **Domain and Application** > **Exclude Client Application Process Name**). You can add up to 200 entries to the list. For example, add **`/Applications/Microsoft Lync.app/Contents/MacOS/Microsoft Lync`** to exclude all Microsoft Lync application traffic from the VPN tunnel.
4. Click **OK** to save the split tunnel settings.

STEP 5 | Save the gateway configuration.

1. Click **OK** to save the gateway configuration.
2. **Commit** your changes.

Exclude Video Traffic from the GlobalProtect VPN Tunnel

You can configure a split tunnel to exclude HTTP/HTTPS video streaming traffic to a specific domain from being sent over the VPN tunnel. This allows video traffic to go directly from the physical interfaces on the endpoint. The App-ID functionality on the firewall identifies the video stream before traffic can be split tunneled. By excluding lower risk video streaming traffic (such as YouTube and Netflix) from the VPN tunnel, you can decrease bandwidth consumption on the gateway.

With a GlobalProtect license, you can enforce or apply split tunnel rules to exclude video streaming traffic from the VPN tunnel on Windows and macOS endpoints.

All video traffic types are redirected for the following video-streaming applications:

- YouTube
- Dailymotion
- Netflix

If you exclude any other video-streaming applications from the VPN tunnel, only the following video traffic types are redirected for those applications:

- MP4
- WebM
- MPEG

Use the following steps to configure a split tunnel to exclude video streaming traffic from the VPN tunnel.

STEP 1 | Before you begin:

1. Follow these prerequisites:
   - Supported only on endpoints with Windows 7 Service Pack 2 and later releases and macOS 10.10 and later releases.
   - You must ensure that the IP pools used to assign IP addresses to the virtual network adapters on these endpoints do not include any IPv6 addresses. If the physical adapter on a Windows or macOS endpoint supports only IPv4 addresses, the endpoint user

cannot access the video streaming applications that you exclude from the VPN tunnel when you configure the GlobalProtect gateway to assign IPv6 addresses to the virtual network adapters on the endpoints that connect to the gateway.

- If you exclude video streaming traffic from the VPN tunnel, do not include web browser applications, such as Firefox or Chrome, in the VPN tunnel. This ensures that there is no conflicting logic in the split tunnel configuration and that your users can stream videos from web browsers.
- To exclude Sling TV app traffic from the VPN tunnel, configure a split tunnel based on an application.

2. Configure a GlobalProtect Gateway.
3. Select **Network** > **GlobalProtect** > **Gateways** > ***<gateway-config>*** to modify an existing gateway or add a new one.

STEP 2 | Enable a split tunnel.

1. In the **GlobalProtect Gateway Configuration** dialog, select **Agent** > **Tunnel Settings** to enable **Tunnel Mode**.
2. Configure a GlobalProtect Gateway for the GlobalProtect app.

STEP 3 | (Tunnel Mode Only) Exclude HTTP/HTTPS video streaming traffic from the VPN tunnel.

1. In the **GlobalProtect Gateway Configuration** dialog, select **Agent** > **Video Traffic**.
2. Enable the option to **Exclude video applications from the tunnel**.

   If you enable this option but do not exclude specific video streaming applications from the VPN tunnel, all video streaming traffic is excluded.

3. (Optional) **Browse** the **Applications** list to view all of the video streaming applications that you can exclude from the VPN tunnel. Click the add (⊕) icon for the applications that you want to exclude. For example, click the add icon for **directv** to exclude DIRECTV video streaming traffic from the VPN tunnel.
4. **Add** the video streaming applications that you want to exclude from the VPN tunnel using the **Applications** drop-down—a shortened version of the **Applications** list. You can add up to 200 video application entries to the list. For example, select **youtube-streaming** to exclude all YouTube-based video streaming traffic from the VPN tunnel.

STEP 4 | Save the gateway configuration.

1. Click **OK** to save the gateway configuration.
2. **Commit** your changes.

Host a Split Tunnel Configuration File on a Web Server

Where Can I Use This?	What Do I Need?
• Prisma Access • GlobalProtect Subscription	• Prisma Access Mobile Users license (for use with Prisma Access) • GlobalProtect app version 6.2 or later for Windows and macOS • Content release version 8699-7991 or later

You can either Split Tunnel Traffic on GlobalProtect Gateways, or you can host it in a Split Tunnel configuration file that you host on a web server in your environment. In order to push the split tunnel configuration to the endpoint:

- Your split tunnel configuration file must parse as valid XML
- The web server must be reachable by all endpoints configured to fetch the split tunnel configuration file
- The server and the client must be able to mutually authenticate

If the GlobalProtect app cannot fetch the split tunnel configuration file, it falls back to the split tunnel configuration that you have configured on the gateway.

The following table shows the split tunnel configuration limits when the configuration is hosted on GlobalProtect vs. when it is hosted in a Split Tunnel Configuration file in your environment:

Split Tunnel By...		Configured on GlobalProtect Gateway	Hosted on a Web Server
Access Route	Include	1000	1000
	Exclude	200	1000
Domain	Include	200	1000
	Exclude	200	1000
Application	Include	200	200
	Exclude	200	200

STEP 1 | Create and sign the split tunnel configuration file.

1. Create your split tunnel configuration file in XML format, as in the following example.

```
File    Edit    View

    <access-routes>
        <member>0.0.0.0</member>
    </access-routes>
    <exclude-access-routes>
        <member>18.0.0.0/8</member>
    </exclude-access-routes>
    <include-split-tunneling-domain>
        <member>*.kohls.com</member>
        <member>*.target.com</member>
    </include-split-tunneling-domain>
    <exclude-split-tunneling-domain>
        <member>*.cnn.com</member>
        <member>*.barnesandnoble.com</member>
    </exclude-split-tunneling-domain>
    <exclude-split-tunneling-application>
        <member>C:\Users\admin\AppData\Roaming\Zoom\bin\Zoom.exe</member>
        <member>C:\Users\admin\AppData\Roaming\Zoom\bin\Zoom_launcher.exe</m
    </exclude-split-tunneling-application>
    <include-split-tunneling-application>
        <member>/Applications/TV.app/Contents/MacOS/TV</member>
    </include-split-tunneling-application>
```

2. Sign the configuration file.

   For example, if the signature file name is config_signature.sha256:

   openssl dgst -sha256 -sign private_key.pem -out config_signature.sha256 config.txt

   You can optionally verify the signature:

   openssl dgst -sha256 -verify public_key.pem -signature config_signature.sha256 config.txt

   Base64 encoding signature file (no wrapping):

   openssl base64 -A -in config_signature.sha256 -out encoded_signature.txt

3. Add the encoded digest to the configuration file.

   1. Add the encoded digest as the first line in the configuration file. It must be on a single line.
   2. Add the split tunnel configuration as the second line.
   3. If you want the traffic to be routed through GlobalProtect by default, add an <access-routes> section with the default route 0.0.0.0/0.

The content in the file must not be terminated with a NULL character (ASCII '\0', or ^@)").

```
YV8z+cr0f6qnjbRoptUuSiCsZeucNVdMCXdD4UrgQAX1faI3TwknO/Vuglo35mUi1RULuDyhuVq+
0HKI2DjHgqjiVCydFZqMFflMQY0Zng4VtmI9GYksXNtA5vtjQ0yBhEExNqfA7iS1b4os+BjGEoAXKQr
Gu1WOSpddGKnxS23DF84bR1ajrl75P6IRdoCMFZ0f4BJ7DQqPwtqOT4I3aBT8dxow0J6mCY5JPVLrRD
      <access-routes>
            <member>0.0.0.0</member>
      </access-routes>
      <exclude-access-routes>
            <member>18.0.0.0/8</member>
      </exclude-access-routes>
      <include-split-tunneling-domain>
            <member>*.kohls.com</member>
            <member>*.target.com</member>
      </include-split-tunneling-domain>
      <exclude-split-tunneling-domain>
            <member>*.cnn.com</member>
            <member>*.barnesandnoble.com</member>
      </exclude-split-tunneling-domain>
      <exclude-split-tunneling-application>
            <member>C:\Users\admin\AppData\Roaming\Zoom\bin\Zoom.exe</member>
            <member>C:\Users\admin\AppData\Roaming\Zoom\bin\Zoom_launcher.exe</
      </exclude-split-tunneling-application>
      <include-split-tunneling-application>
            <member>/Applications/TV.app/Contents/MacOS/TV</member>
      </include-split-tunneling-application>
```

4. Host the split tunnel configuration file you just created on a web server that your GlobalProtect endpoints can access.
5. Enable mutual authentication.

   You will need the public key certificate that you use for mutual authentication for the GlobalProtect configuration.

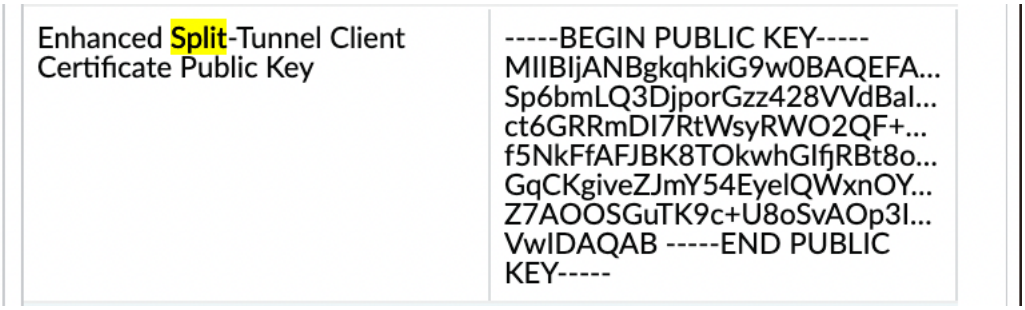
   For example, to host the split tunnel configuration file in AWS behind the network load balancers protected by the AWS network firewall, you would do the following:

   1. Provision EC2 instances to host servers.
   2. • Create network load balancers (NLB) and configure listeners on TCP port 443.

- Create Target Groups with port 443 and associate EC2 instances to the Target Groups.
- Configure the network firewall and two stateless rule groups and associate them with the configured firewalls that you have provisioned. Configure rule 1 to drop packets to all ports and protocols from a specific IP address or subnet. Configure rule 2 to allow packets to TCP port 443.
- Configure the VPC routing tables to forward traffic from the internet to the NLB via the network firewall.

STEP 2 | Add the public key certificate you used on your web server to the portal configuration.

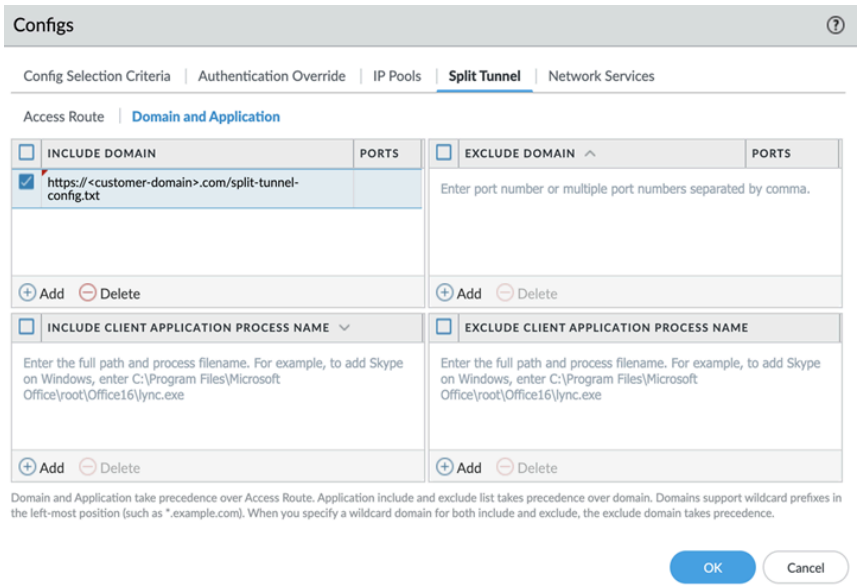
In the Customize the GlobalProtect App, paste the public key certificate in the **Enhanced Split Tunnel Client Certificate Public Key** field.



STEP 3 | Split Tunnel Traffic on GlobalProtect Gateways and add the URL for your split tunnel configuration file.

1. In the GlobalProtect Gateway Configuration dialog, select **Agent** > **Tunnel Settings** and enable **Tunnel Mode**
2. Configure the tunnel parameters for the GlobalProtect app.
3. In the GlobalProtect Gateway Configuration dialog, select **Agent** > **Client Settings** and select an existing client settings configuration or add a new one.
4. Select **Split Tunnel** and in the Include Domain section, add the URL of your split tunnel configuration file as the first entry in the Include Domain section.

   Only HTTPS URLs are supported.



5. Click **OK** and **Commit** the changes.

GlobalProtect MIB Support

Palo Alto Networks endpoints support standard and enterprise management information bases (MIBs) that enable you to monitor the endpoint's physical state, utilization statistics, traps, and other useful information. Most MIBs use object groups to describe characteristics of the endpoint using the Simple Network Management Protocol (SNMP) Framework. You must load these MIBs into your SNMP manager to monitor the objects (endpoint statistics and traps) that are defined in the MIBs (for details, see Use an SNMP Manager to ExploreMIBsand Objects).

The PAN-COMMON-MIB—which is included with the enterprise MIBs—uses the panGlobalProtect object group. The following table describes the objects that make up the panGlobalProtect object group.

Object	Description
panGPGWUtilizationPct	Utilization (as a percentage) of the GlobalProtect gateway
panGPGWUtilizationMaxTunnels	Maximum number of tunnels allowed
panGPGWUtilizationActiveTunnels	Number of active tunnels

Use these SNMP objects to monitor utilization of GlobalProtect gateways and make changes as needed. For example, if the number of active tunnels reaches 80% or is higher than the maximum number of tunnels allowed, you should consider adding additional gateways.

GlobalProtect Portals

The GlobalProtect portal provides the management functions for your GlobalProtect infrastructure. Every endpoint that participates in the GlobalProtect network receives configuration information from the portal, including information about available gateways and any client certificates that may be required to connect to the gateways. In addition, the portal controls the behavior and distribution of the GlobalProtect app software to both macOS and Windows endpoints.

The portal does not distribute the GlobalProtect app for use on mobile endpoints. To get the GlobalProtect app for mobile endpoints, end users must download the app from the device store: App Store for iOS, Google Play for Android, Chrome Web Store for Chromebooks, or Microsoft Store for Windows 10 UWP. However, the agent configurations that are deployed to mobile app users control the gateway(s) to which the mobile endpoints have access. See what endpoint OSes are supported on each GP app version.

In addition to distributing GlobalProtect app software, you can configure the GlobalProtect portal to provide secure remote access to common enterprise web applications that use HTML, HTML5, and JavaScript technologies using GlobalProtect Clientless VPN. Users have the advantage of secure access from SSL-enabled web browsers without installing the GlobalProtect app software. This is useful when you need to enable partner or contractor access to applications, and to safely enable unmanaged assets, including personal endpoints.

Set Up Access to the GlobalProtect Portal

Configure the GlobalProtect portal as follows:

STEP 1 | Before you begin configuring the portal make sure you have:

- Create Interfaces and Zones for GlobalProtect for the firewall where you plan to configure the portal.
- Set up the Enable SSL Between GlobalProtect Components, and, optionally, any client certificates to deploy to end users to enable SSL/TLS connections for the GlobalProtect™ services.
- GlobalProtect User Authentication that the portal can use to authenticate GlobalProtect users.
- Configure a GlobalProtect Gateway and understand Gateway Priority in a Multiple Gateway Configuration.

STEP 2 | Add the portal.

1. Select **Network** > **GlobalProtect** > **Portals**, and then **Add** a portal.
2. Enter a **Name** for the portal.

   The gateway name cannot contain spaces and must be unique for each virtual system.
3. (Optional) Select the virtual system to which this portal belongs from the **Location** field.

STEP 3 | Specify network settings to enable the GlobalProtect app to communicate with the portal.

If you have not yet created a network interface for the portal, see Create Interfaces and Zones for GlobalProtect. If you have not yet created an SSL/TLS service profile for the portal, see Deploy Server Certificates to the GlobalProtect Components.

Do not attach an interface management profile that allows HTTP, HTTPS, Telnet, or SSH on the interface where you have configured a GlobalProtect portal or gateway because this enables access to your management interface from the internet. Follow the Adminstrative Access Best Practices to ensure that you are securing administrative access to your firewalls in a way that will prevent successful attacks.

1. Select **General**.
2. In the Network Settings area, select an **Interface**.
3. Specify the **IP Address Type** and **IP address** for the portal web service:
   - The IP address type can be **IPv4 Only**, **IPv6 Only**, or **IPv4 and IPv6.** Use **IPv4 and IPv6** if your network supports dual stack configurations, where IPv4 and IPv6 run at the same time.
   - The IP address must be compatible with the IP address type. For example, `172.16.1.0` for IPv4 addresses or `21DA:D3:0::2F3b` for IPv6 addresses. For dual stack configurations, enter both an IPv4 and IPv6 address.
4. Select an **SSL/TLS Service Profile**.

STEP 4 | Select **General** and configure Decryption log settings.

You can log successful and unsuccessful TLS/SSL handshakes and you can forward Decryption logs to Log Collectors, other storage devices, and to specific administrators.

- By default, the firewall logs only unsuccessful TLS handshakes. It is a best practice to log successful handshakes as well so that you gain visibility into as much decrypted traffic as available resources permit (but don't decrypt private or sensitive traffic; follow decryption best practices and decrypt as much traffic as you can).
- If you have not already done so, create a Log Forwarding profile to forward Decryption logs and specify it in the Gateway configuration.
- If you log successful TLS handshakes in addition to unsuccessful TLS handshakes, configure a larger log storage space quota for the Decryption log (**Device** > **Setup** > **Management** > **Logging and Reporting Settings** > **Log Storage**). The default quota (allocation) is one percent of the device's log storage capacity for Decryption logs and one percent for the general decryption summary. There is no default allocation for hourly, daily, or weekly decryption summaries. Configure Decryption Logging provides more information about how to allocate firewall log space to Decryption logs.

STEP 5 | Select custom login and help pages or disable the login and help pages entirely. See Customize the GlobalProtect Portal Login, Welcome, and Help Pages for more details on creating a custom login page and help page.

1. Select **General**.
2. In the Appearance area, configure any of the following settings:
   - To set the **Portal Login Page** for user access to the portal, select the **factory-default** login page, **Import** a custom login page, or **Disable** access to the login page.
   - To set the **App Help Page** to provide assistance to users with the GlobalProtect app, select the **factory-default** help page, **Import** a custom help page, or select **None** to remove the **Help** option from the **Settings** menu of the GlobalProtect status panel.

STEP 6 | Specify how the portal authenticates users.

1. Select **Authentication**.
2. Configure any of the following portal authentication settings:

   If you have not yet created a server certificate for the portal and issued gateway certificates, see Deploy Server Certificates to the GlobalProtect Components.

   - To secure communication between the portal and the GlobalProtect app, select the **SSL/TLS Service Profile** that you configured for the portal.
   - To authenticate users through a local user database or an external authentication service, such as LDAP, Kerberos, TACACS+, SAML, or RADIUS (including OTP), Define the GlobalProtect Client Authentication Configurations.
   - To authenticate users based on a client certificate or a smart card/CAC, select the corresponding **Certificate Profile**. You must pre-deploy the client certificate

or Deploy User-Specific Client Certificates for Authentication using the Simple Certificate Enrollment Protocol (SCEP).

- If you want to require users to authenticate to the portal using both user credentials AND a client certificate, both a **Certificate Profile** and Authentication Profile are required.
- If you want to allow users to authenticate to the portal using either user credentials OR a client certificate, and you select an Authentication Profile for user authentication, the **Certificate Profile** is optional.
- If you want to allow users to authenticate to the portal using either user credentials OR a client certificate, and you do not select an Authentication Profile for user authentication, the **Certificate Profile** is required.
- If you do not configure any Authentication Profile that matches a specific OS, the **Certificate Profile** is required.

*If you allow users to authenticate to the portal using either user credentials OR a client certificate, select a **Certificate Profile** with the **Username Field** set to **Subject** or **Subject Alt**.*

STEP 7 | Define the data that the GlobalProtect app collects from connecting endpoints after users successfully authenticate to the portal.

The GlobalProtect app sends this data to the portal to match against the selection criteria that you define for each portal agent configuration. Based on this criteria, the portal delivers a specific agent configuration to the GlobalProtect apps that connect.

1. Select **Portal Data Collection**.
2. Configure any of the following data collection settings:
   - If you want the GlobalProtect app to collect machine certificates from connecting endpoints, select the **Certificate Profile** that specifies the machines certificates that you want to collect.
   - If you want the GlobalProtect app to collect custom host information from connecting endpoints, define the following registry, plist, or process list data in the Custom Checks area:
     - To collect registry data from Windows endpoints, select **Windows** and then **Add** the **Registry Key** and corresponding **Registry Value**.
     - To collect plist data from macOS endpoints, select **Mac** and then **Add** the **Plist** key and corresponding **Key** value.

STEP 8 | Save the portal configuration.

1. Click **OK** to save the settings.
2. **Commit** the changes.

Define the GlobalProtect Client Authentication Configurations

Each GlobalProtect client authentication configuration specifies the settings that enable the user to authenticate with the GlobalProtect portal. You can customize the settings for each OS or you can configure the settings to apply to all endpoints. For example, you can configure Android users to use RADIUS authentication and Windows users to use LDAP authentication. You can also customize client authentication for users who access the portal from a web browser (to download the GlobalProtect app) or for third-party IPsec VPN (X-Auth) access to GlobalProtect gateways.

STEP 1 | Set Up Access to the GlobalProtect Portal.

STEP 2 | Specify how the portal authenticates users.

You can configure the GlobalProtect portal to authenticate users through a local user database or an external authentication service, such as LDAP, Kerberos, TACACS+, SAML, or RADIUS (including OTP). If you have not yet set up the authentication profiles and/or certificate profiles, see GlobalProtect User Authentication for instructions.

On the GlobalProtect Portal Configuration dialog (**Network** > **GlobalProtect** > **Portals** > ***<portal-config>***), select **Authentication** to **Add** a new **Client Authentication** configuration with the following settings:

- Enter a **Name** to identify the client authentication configuration.
- Specify the endpoints to which you want to deploy this configuration. To apply this configuration to all endpoints, accept the default **OS** of **Any**. To apply this configuration to endpoints running a specific operating system, select an **OS** such as **Android**. Alternatively, you can apply this configuration to endpoints that connect to a GlobalProtect Clientless VPN from a web **Browser**.
- To enable users to authenticate to the portal or gateway using their user credentials, select or add an **Authentication Profile**.
  - If you want to require users to authenticate to the portal or gateway using both user credentials AND a client certificate, both the **Authentication Profile** and Certificate Profile are required.
  - If you want to allow users to authenticate to the portal or gateway using either user credentials OR a client certificate, and you select a Certificate Profile for user authentication, the **Authentication Profile** is optional.
  - If you want to allow users to authenticate to the portal or gateway using either user credentials OR a client certificate, but you do not select a Certificate Profile for user

authentication (or you set the **Certificate Profile** to **None**), the **Authentication Profile** is required.

- (Optional) Enter a custom **Username Label** for GlobalProtect portal login (for example, **Email Address (username@domain)**.
- (Optional) Enter a custom **Password Label** for GlobalProtect portal login (for example, **Passcode** for two-factor, token-based authentication).
- (Optional) Enter an **Authentication Message** to help end users understand which credentials to use when logging in. The message can be up to 256 characters in length (default is `Enter login credentials`).
- Select one of the following options to define whether users can authenticate to the portal using credentials and/or client certificates:
  - To require users to authenticate to the portal using both user credentials AND a client certificate, set the **Allow Authentication with User Credentials OR Client Certificate** option to **No (User Credentials AND Client Certificate Required)** (default).
  - To allow users to authenticate to the portal using either user credentials OR a client certificate, set the **Allow Authentication with User Credentials OR Client Certificate** option to **Yes (User Credentials OR Client Certificate Required)**.

    When you set this option to **Yes**, the GlobalProtect portal first searches the endpoint for a client certificate. If the endpoint does not have a client certificate or you do not configure a certificate profile for your client authentication configuration, the end user must then authenticate to the portal using his or her user credentials.

STEP 3 | Arrange the client authentication configurations with OS-specific configurations at the top of the list, and configurations that apply to **Any** OS at the bottom of the list (**Network** > **GlobalProtect** > **Portals** > **<portal-config>** > **Authentication**). As with security rule evaluation, the portal looks for a match starting from the top of the list. When it finds a match, it delivers the corresponding configuration to the app.

- To move a client authentication configuration up on the list of configurations, select the configuration and click **Move Up**.
- To move a client authentication configuration down on the list of configurations, select the configuration and click **Move Down**.

STEP 4 | (Optional) To enable two-factor authentication using an authentication profile and a certificate profile, configure both in this portal configuration.

The portal must authenticate the endpoint by using both methods before the user can gain access.

(Chrome only) If you configure the portal to use client certificates and LDAP for two-factor authentication, Chromebooks that run Chrome OS 47 or later versions encounter excessive prompts to select the client certificate. To prevent excessive prompts, configure a policy to specify the client certificate in the Google Admin console and then deploy that policy to your managed Chromebooks:

1. *Log in to the Google Admin console and select **Device management** > **Chrome management** > **User settings**.*
2. *In the Client Certificates section, enter the following URL pattern to **Automatically Select Client Certificate for These Sites**:*

   {"pattern": "https://[*.]","filter":{}}
3. *Click **Save**. The Google Admin console deploys the policy to all devices within a few minutes.*

On the GlobalProtect Portal Configuration dialog (**Network** > **GlobalProtect** > **Portals** > ***<portal-config>***), select **Authentication** to choose the **Certificate Profile** to authenticate users based on a client certificate or smart card.

The Common Name (CN) and, if applicable, the Subject Alternative Name (SAN) fields of the certificate must exactly match the IP address or FQDN of the interface where you configure the portal or HTTPS connections to the portal will fail.

STEP 5 | Save the portal configuration.

1. Click **OK** to save your configuration.
2. **Commit** the changes.

Define the GlobalProtect Agent Configurations

After a GlobalProtect user connects to the portal and is authenticated by the GlobalProtect portal, the portal sends the agent configuration to the app, based on the settings you define. If you have different roles for users or groups that need specific configurations, you can create a separate agent configuration for each user type or user group. The portal uses the OS of the endpoint and the username or group name to determine which agent configuration to deploy. As with other security rule evaluations, the portal starts to search for a match at the top of the list. When it finds a match, the portal sends the configuration to the app.

The configuration can include the following:

- A list of gateways to which the endpoint can connect.
- Among the external gateways, any gateway that the user can manually select for the session.
- The root CA certificate required to enable the app to establish an SSL connection with the GlobalProtect gateway(s).
- The root CA certificate for SSL forward proxy decryption.
- The client certificate that the endpoint should present to the gateway when it connects. This configuration is required only if mutual authentication between the app and the portal or gateway is required.
- A secure encrypted cookie that the endpoint should present to the portal or gateway when it connects. The cookie is included only if you enable the portal to generate one.
- The settings the endpoint uses to determine whether it is connected to the local network or to an external network.
- App behavior settings, such as what the end users can see in their display, whether users can save their GlobalProtect password, and whether users are prompted to upgrade their software.

If the portal is down or unreachable, the app uses the cached version of its agent configuration from its last successful portal connection to obtain settings, including the gateway(s) to which the app can connect, what root CA certificate(s) to use to establish secure communication with the gateway(s), and what connect method to use.

Use the following procedure to create an agent configuration.

STEP 1 | Add one or more trusted root CA certificates to the portal agent configuration to enable the GlobalProtect app to verify the identity of the portal and gateways.

The portal deploys the certificate in a certificate file which is read only by GlobalProtect.

1. Select **Network** > **GlobalProtect** > **Portals**.
2. Select the portal configuration to which you are adding the agent configuration, and then select the **Agent** tab.
3. In the **Trusted Root CA** field, **Add** and select the CA certificate that was used to issue the gateway and/or portal server certificates.

   The web interface presents a list of CA certificates that are imported on the firewall serving as the GlobalProtect portal. The web interface also excludes end-entity

certificates, sometimes referred to as leaf certificates, from the list of certificates you can select. You can also **Import** a new CA certificate.

Use the following best practices when creating and adding certificates:

- *Use the same certificate issuer to issue certificates for all of your gateways.*
- *Add the entire certificate chain (trusted root CA and intermediate CA certificates) to the portal agent configuration.*

4. (Optional) Deploy additional CA certificates for purposes other than GlobalProtect (for example, SSL forward proxy decryption).

   This option enables you to use the portal to deploy certificates to the endpoint and the agent to install them in the local root certificate store. This can be useful if you do not have another method for distributing these server certificates or prefer to use the portal for certificate distribution.

   For SSL forward proxy decryption, you specify the forward trust certificate that the firewall uses (on Windows and macOS endpoints only) to terminate the HTTPS connection, inspect the traffic for policy compliance, and re-establish the HTTPS connection to forward the encrypted traffic.

   1. Add the certificate as described in the previous step.
   2. Enable the option to **Install in Local Root Certificate Store**.

      The portal automatically sends the certificate when the user logs in to the portal and installs it in the endpoint's local store, thus eliminating the need for you to install the certificate manually.

STEP 2 | Add an agent configuration.

The agent configuration specifies the GlobalProtect configuration settings to deploy to the connecting apps. You must define at least one agent configuration. You can add up to 512 agent configuration entries for each portal.

1. From your portal configuration (**Network** > **GlobalProtect** > **Portals** > ***<portal-config>***), **Add** a new agent configuration.
2. Enter a **Name** to identify the configuration. If you plan on creating multiple configurations, make sure the name you define for each configuration is descriptive enough to distinguish them.

STEP 3 | (Optional) Configure settings to specify how users with this configuration authenticate with the portal.

If the gateway authenticates endpoints using a client certificate, you must select the source that distributes the certificate.

Configure any of the following **Authentication** settings:

- To enable users to authenticate with the portal using client certificates, select the **Client Certificate** source (**SCEP**, **Local**, or **None**) that distributes the certificate and its private key to an endpoint. If you use an internal CA to distribute certificates to endpoints, select **None** (default). To enable the portal to generate and send a machine certificate to the app for storage in the local certificate store and use the certificate for portal and gateway authentication, select **SCEP** and the associated SCEP profile. These certificates are device-

specific and can only be used on the endpoint to which it was issued. To use the same certificate for all endpoints, select a certificate that is **Local** to the portal. With **None**, the portal does not push a certificate to the endpoint, but you can use can other ways to get a certificate to the endpoint.

- Specify whether to **Save User Credentials**. Select **Yes** to save the username and password (default), **Save Username Only** to save only the username, **Only with User Fingerprint** to save the user's biometric (fingerprint) or, on iOS X endpoints only, face ID credentials, or **No** to never save credentials.

  *When you set **Save User Credentials** to **No**, and if the portal and the gateway are configured to use the same authentication methods, the GlobalProtect app can authenticate to the gateway transparently using the credentials provided by the user to authenticate to the portal. The user is not required to re-enter their credentials to authenticate to the gateway.*

  If you configure the portal or gateways to prompt for a dynamic password, such as a one-time password (OTP), the user must enter a new password at each login. In this case, the GlobalProtect app ignores the selection to save both the username and password, if specified, and saves only the username. For more information, see Enable Two-Factor Authentication Using One-Time Passwords (OTPs).

  If you select GlobalProtect to **Save User Credentials Only with User Fingerprint**, GlobalProtect can leverage the app's operating system capabilities for validating the user before allowing authentication with GlobalProtect. End users must supply a fingerprint that matches a trusted fingerprint template on the endpoint to use a saved password for authentication to GlobalProtect portal and gateways. On iOS X, GlobalProtect also supports facial recognition with Face ID. GlobalProtect does not store the fingerprint or facial template used for authentication, but relies on the operating system scanning capabilities to determine the validity of a scan match.

STEP 4 | If the GlobalProtect endpoint does not require tunnel connections when it is on the internal network, configure internal host detection.

1. Select **Internal**.
2. Enable **Internal Host Detection**(**IPv4** or **IPv6**).
3. Enter the **IP Address** of a host that can be reached from the internal network only. The IP address you specify must be compatible with the IP address type (**IPv4** or **IPv6**). For example, 172.16.1.0 for IPv4 or 21DA:D3:0:2F3b for IPv6.
4. Enter the DNS **Hostname** for the IP address you enter. Endpoints that try to connect to GlobalProtect attempt to do a reverse DNS lookup on the specified address. If the lookup fails, the endpoint determines that it is on the external network and then initiates a tunnel connection to a gateway on its list of external gateways.
5. (Optional) Enter a source address pool for endpoints. When users connect, GlobalProtect recognizes the source address of the device. Only GlobalProtect apps with IP addresses that are included in the source IP address pool can authenticate with the gateway and send HIP reports.

   IPv4 subnet must be /30 or larger. Otherwise, a specific IP range must be specified. For example, 192.168.1.0/30 or 192.168.2.6-192.168.2.7

STEP 5 | Set up access to a third-party mobile endpoint management system.

This step is required if the mobile endpoints using this configuration will be managed by a third-party mobile endpoint management system. All endpoints initially connect to the portal and, if a third-party mobile endpoint management system is configured on the corresponding portal agent configuration, the endpoint is redirected to it for enrollment.

1. Enter the IP address or FQDN of the endpoint check-in interface associated with your mobile endpoint management system. The value you enter here must exactly match the value of the server certificate associated with the endpoint check-in interface. You can specify an IPv6 or IPv4 address.
2. Specify the **Enrollment Port** on which the mobile endpoint management system listens for enrollment requests. This value must match the value set on the mobile endpoint management system (default=443).

STEP 6 | Specify the selection criteria for your portal agent configuration.

The portal uses the selection criteria that you specify to determine which configuration to deliver to the GlobalProtect apps that connect. Therefore, if you have multiple configurations, you must make sure to order them properly. As soon as the portal finds a match, it delivers the configuration. Therefore, more specific configurations must precede more general ones. See step 12 for instructions on ordering the list of agent configurations.

Select **Config Selection Criteria** and then configure any of the following options:

- To specify the user, user group, and/or operating system to which this configuration applies, select **User/User Group** and then configure any of the following options:
  - To deliver this configuration to apps running on a specific operating system, **Add** and select the **OS** (**Android**, **Chrome**, **iOS**, **Linux**, **Mac**, **Windows**, or **WindowsUWP**) to which this configuration applies. Set the **OS** to **Any** to deploy the configuration to all operating systems.
  - To restrict this configuration to a specific user and/or group, **Add** and then select the **User/User Group** you want to receive this configuration. Repeat this step for each user/group you want to add. To restrict the configuration to users who have not yet logged in to their endpoints, select **pre-logon** from the **User/User Group** drop-down. To deploy the configuration to any user regardless of login status (both pre-logon and logged in users), select **any** from the **User/User Group** drop-down.

    Before you can restrict the configuration to specific groups, you must map users to groups as described in Enable Group Mapping.
- To deliver this configuration to apps based on specific device attributes, select **Device Checks** and then configure any of the following options:
  - To deliver this configuration based on the presence of the endpoint serial number in the Active Directory or Azure AD, select an option from the **Machine account exists with device serial number** drop-down. If you set this option to **Yes**, the agent configuration applies only to endpoints with a serial number that exists (managed endpoints). If you set this option to **No**, the agent configuration applies only to endpoints for which a serial number does not exist (unmanaged endpoints). If you set this option to **None**,

the configuration is not delivered to apps based on the presence of the endpoint serial number.

- To deliver this configuration based on the endpoint's machine certificate, select a **Certificate Profile** to match against the machine certificate installed on the endpoint.

Device checks are supported on Windows and Mac operating systems.

- To deliver this configuration to apps based on custom host information, select **Custom Checks**. Enable **Custom Checks** and then define any of the following registry and plist data:
  - To verify whether Windows endpoints have a specific registry key, use the following steps:
    1. **Add** a new registry key (**Custom Checks** > **Registry Key**).
    2. When prompted, enter the **Registry Key** to match.
    3. (Optional) To deliver this configuration only if the endpoint does not have the specified registry key or key value, select **Key does not exist or match the specified value data**.
    4. (Optional) To deliver this configuration based on specific registry values, **Add** the **Registry Value** and corresponding **Value Data**. To deliver this configuration only endpoints that do not have the specified **Registry Value** or **Value Data**, select **Negate**.
  - To verify whether macOS endpoints have a specific entry in the plist, use the following steps:
    1. **Add** a new plist (**Custom Checks** > **Plist**).
    2. When prompted, enter the **Plist** name.
    3. (Optional) To deliver this configuration only if the endpoint does not have the specified plist, select **Plist does not exist**.
    4. (Optional) To deliver this configuration based on specific key-value pairs within the plist, click **Add** and then enter the **Key** and corresponding **Value**. To match only endpoints that do not have the specified key or value, select **Negate**.
  - To verify

STEP 7 | Specify the external gateways to which users with this configuration can connect.

Consider the following best practices when you configure the gateways:

- *If you are adding both internal and external gateways to the same configuration, make sure you enable **Internal Host Detection** (step 4).*
- *To learn more about how the GlobalProtect app determines the gateway to which it should connect, see* Gateway Priority in a Multiple Gateway Configuration.

1. Select **External**.
2. **Add** the **External Gateways** to which users can connect.
3. Enter a descriptive **Name** for the gateway. The name you enter here should match the name you defined when you configured the gateway and should be descriptive enough for users to know the location of the gateway to which they are connected.
4. Enter the FQDN or IP address of the interface where the gateway is configured in the **Address** field. You can configure an IPv4 or IPv6 address. The address you specify must exactly match the Common Name (CN) in the gateway server certificate.
5. **Add** one or more **Source Regions** for the gateway, or select **Any** to make the gateway available to all regions. When users connect, GlobalProtect recognizes the region and only allows users to connect to gateways that are configured for that region. For gateway selection, source region is considered first, then gateway priority.
6. Set the **Priority** of the gateway by clicking the field and selecting one of the following values:
   - If you have only one external gateway, you can leave the value set to **Highest** (the default).
   - If you have multiple external gateways, you can modify the priority values (ranging from **Highest** to **Lowest**) to indicate a preference for the specific user group to which this configuration applies. For example, if you prefer that the user group connects to a local gateway you would set the priority higher than that of more geographically distant gateways. The priority value is then used to weight the agent's gateway selection algorithm.
   - If you do not want apps to automatically establish connections with the gateway, select **Manual only**. This setting is useful in testing environments.
7. Select the **Manual** check box to allow users to manually switch to the gateway.

STEP 8 | Specify the internal gateways to which users with this configuration can connect.

Make sure you do not use on-demand as the connect method if your configuration includes internal gateways.

1. Select **Internal**.
2. **Add** the **Internal Gateways** to which users can connect.
3. Enter a descriptive **Name** for the gateway. The name you enter here should match the name you defined when you configured the gateway and should be descriptive enough for users to know the location of the gateway they are connected to.
4. Enter the FQDN or IP address of the interface where the gateway is configured in the **Address** field. You can configure an IPv4 or IPv6 address. The address you specify must exactly match the Common Name (CN) in the gateway server certificate.
5. (Optional) **Add** one or more **Source Addresses** to the gateway configuration. The source address can be an IP subnet, range, or predefined address. GlobalProtect supports both IPv6 and IPv4 addresses. When users connect, GlobalProtect recognizes the source address of the endpoint and only allows users to connect to gateways that are configured for that address.
6. Click **OK** to save your changes.
7. (Optional) **Add** a **DHCP Option 43 Code** to the gateway configuration. You can include one or more sub-option codes associated with the vendor-specific information (Option 43) that the DHCP server has been configured to offer the client. For example, you might have a sub-option code 100 that is associated with an IP address of 192.168.3.1.

   When a user connects, the GlobalProtect portal sends the list of option codes in the portal configuration to the GlobalProtect app, and the app selects gateways indicated by these options.

   When both the source address and DHCP options are configured, the list of available gateways presented to the endpoint is based on the combination (union) of the two configurations.

   DHCP options are supported on Windows and macOS endpoints only. DHCP options cannot be used to select gateways that use IPv6 addressing.
8. (Optional) Select **Internal Host Detection** to allow the GlobalProtect app to determine if it is inside the enterprise network. When a user attempts to log in, the app performs a reverse DNS lookup of the internal **Hostname** to the specified **IP Address**.

   The host serves as a reference point that is reachable if the endpoint is inside the enterprise network. If the app finds the host, the endpoint is inside the network and the app connects to an internal gateway; if the app fails to find the internal host, the endpoint is outside the network and the app connects to one of the external gateways.

   You can configure **IPv4** or **IPv6** addressing for **Internal Host Detection**. The IP address you specify must be compatible with the IP address type. For example, 172.16.1.0 for IPv4 or 21DA:D3:0:2F3b for IPv6.

STEP 9 | Customize the GlobalProtect app behavior for users with this configuration.

Modify the **App** settings as desired. For more details about each option, see Customize the GlobalProtect App.

STEP 10 | (Optional) Define any custom host information profile (HIP) data that you want the app to collect and/or exclude from collection.

This step applies only if you plan on using the HIP feature, there is information you want to collect that cannot be collected using the standard HIP objects, or if there is HIP information that you are not interested in collecting. See Host Information for details on setting up and using the HIP feature.

See Collect Application and Process Data From Endpoints for additional information on collecting custom HIP data.

1. Select **HIP Data Collection**.
2. Enable the GlobalProtect app to **Collect HIP Data**.
3. Specify the **Max Wait Time (sec)** that the app should search for HIP data before submitting the available data (range is 10-60 seconds; default is 20 seconds).
4. Select the **Certificate Profile** that the GlobalProtect portal uses to match the machine certificate send by the GlobalProtect app.
5. Select **Exclude Categories** to exclude specific categories and/or vendors, applications, or versions within a category. For more details, see Configure HIP-Based Policy Enforcement.
6. Select **Custom Checks** to define any custom data you want to collect from hosts running this agent configuration.

STEP 11 | Save the agent configuration.

Click **OK** to save the agent configuration.

STEP 12 | Arrange the agent configurations so that the proper configuration is deployed to each app.

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

- To move an agent configuration up on the list of configurations, select the configuration and click **Move Up**.
- To move an agent configuration down on the list of configurations, select the configuration and click **Move Down**.

STEP 13 | Save the portal configuration.

1. Click **OK** to save the portal configuration.
2. **Commit** the changes.

Customize the GlobalProtect App

The portal agent configuration allows you to customize how your end users interact with the GlobalProtect apps installed on their endpoints. You can customize the display and behavior of the app, and define different app settings for the different GlobalProtect agent configurations you create. For example, you can specify the following:

- What menus and views users can access.
- Whether users can uninstall or disable the app (user-logon connect method only).
- Whether to display a welcome page upon successful login. You can also configure whether or not the user can dismiss the welcome page, and you can Customize the GlobalProtect Portal Login, Welcome, and Help Pages to explain how to use GlobalProtect within your environment.
- Whether the GlobalProtect app upgrades automatically or prompts users to upgrade manually.
- Whether to prompt users if multi-factor authentication is required to access sensitive network resources.

You can also define app settings in the Windows Registry, Windows Installer (Msiexec), and global macOS plist. Settings that are defined in the web interface (portal agent configuration) take precedence over settings that are defined in the Windows Registry, Msiexec, and macOS plist. For more details, see Deploy App Settings Transparently.

Some settings do not have a corresponding portal configuration setting on the web interface and must be configured using the Windows Registry, Msiexec, or macOS plist. These settings are listed in the Customizable App Settings as "Not in portal."

The additional settings that are available only through the Windows Registry, Msiexec, or macOS plist enable you to customize options including, but not limited to, the following:

- Specify whether the app prompts the end user for credentials when Windows SSO fails.
- Specify the default portal IP address (or hostname).
- Enable GlobalProtect to initiate a connection before the user logs into the endpoint.
- Deploy scripts that run before or after GlobalProtect establishes a connection or after GlobalProtect disconnects.
- Configure the GlobalProtect app to wrap third-party credentials on Windows endpoints, enabling SSO when using a third-party credential provider.

STEP 1 | Select the agent configuration that you want to customize.

You can also configure most app settings from the Windows Registry, Windows Installer (Msiexec), and macOS plist. However, settings that are defined in the web interface take precedence over settings that are defined in the Windows Registry, Msiexec, and macOS plist. See Deploy App Settings Transparently for more details.

1. Select **Network** > **GlobalProtect** > **Portals**.
2. Select the portal on which you want to add the agent configuration, or **Add** a new one.
3. On the **Agent** tab, select the agent configuration that you want to modify, or **Add** a new one.
4. Select the **App** tab.

   The App Configurations area displays the app settings with default values that you can customize for each agent configuration. When you change the default behavior, the text color changes from gray to the default color.

STEP 2 | Specify the **Connect Method** that an app uses for its GlobalProtect connection.

*Use the **Pre-logon (Always On)**, **Pre-logon then On-demand**, or **User-log on (Always On)** connect method to access the network using an internal gateway.*

In the App Configurations area, select one of the following **Connect Method** options:

- **User-logon (Always On)**—The GlobalProtect app automatically connects to the portal as soon as the user logs in to the endpoint (or domain). When used in conjunction with SSO (Windows endpoints only), GlobalProtect login is transparent to the end user.

  On iOS endpoints, this setting prevents one-time password (OTP) applications from working because GlobalProtect forces all traffic to go through the tunnel.
- **Pre-logon (Always On)**—The GlobalProtect app authenticates the user and establishes a VPN tunnel to the GlobalProtect gateway before the user logs in to the endpoint. This option requires that you use an external PKI solution to pre-deploy a machine certificate to each endpoint that receives this configuration. See Remote Access VPN with Pre-Logon for details about pre-logon.
- **On-demand (Manual user initiated connection)**—Users must manually launch the app to connect to GlobalProtect. Use this connect method for external gateways only.
- **Pre-logon then On-demand**—Similar to the **Pre-logon (Always On)** connect method, this connect method (which requires Content Release version 590-3397 or later) enables the GlobalProtect app to authenticate the user and establish a VPN tunnel to the GlobalProtect gateway before the user logs in to the endpoint. Unlike the pre-logon connect method, after the user logs in to the endpoint, users must manually launch the app to connect to GlobalProtect if the connection is terminated for any reason. The benefit of this option is that you can allow users to specify a new password after their password expires or they forget their password, but still require users to manually initiate the connection after they log in.
- **Conditional Connect Method Based on Network Type (Using Windows Registry/macOS Plist)**—Using Windows Registry/macOS Plist, you can Configure Conditional Connect Method Based on Network Type from **Always-On** to **On-Demand** mode and vice-versa

based on the network type (internal or external) to which the end user is connected. To use this functionality you must enable internal host detection and set the connect method for endpoints to On-demand.

STEP 3 | (Windows 10, ARM64-Based Windows 10, macOS 11 and later releases, and ARM-Based macOS 11 and later releases; Content Release version 8450-6909 or later; Requires GlobalProtect app 6.0 or later) Configure endpoint traffic policy enforcement to block malicious inbound connections using the physical adapter on the remote endpoint.

By enforcing endpoint traffic policy on the GlobalProtect endpoint, you can perform the following functions:

- Block malicious inbound connections outside of the VPN tunnel to guard against data exfiltration.
- Restrict any applications from bypassing the GlobalProtect tunnel by binding their connections directly to the physical adapter on the remote endpoint.
- Prevent end users from tampering with the routing table to bypass the GlobalProtect tunnel.

When used in conjunction with the **No direct access to local network** option, you can also control access to the local network. By default, the endpoint traffic policy enforcement is disabled.

In the **App Configurations** area, select one of the following **Endpoint Traffic Policy Enforcement** options:

- **No**—Specifies that the Endpoint Traffic Policy Enforcement feature is disabled and that this feature is not applied. This is the default option.
- **TCP/UDP Traffic Based on Tunnel IP Address Type**—Enables endpoint traffic policy enforcement for TCP/UDP traffic. This feature is enabled for traffic based on the tunnel IP address type. If the tunnel is IPv4, this feature applies only to IPv4 traffic. If the tunnel is IPv6, this features applies only to IPv6 traffic.
- **All TCP/UDP Traffic**—Enables endpoint traffic policy enforcement for all TCP/UDP traffic regardless of the tunnel IP address type. If the tunnel IP address type is IPv4, endpoint traffic policy enforcement applies to all TCP/UDP (IPv4 or IPv6) traffic. If the tunnel IP address type is IPv6, endpoint traffic policy enforcement applies to all TCP/UDP (IPv4 or IPv6) traffic.
- **All Traffic**—Enables endpoint traffic policy enforcement for all TCP, UDP, ICMP, and all other protocols regardless of the tunnel IP address type.

STEP 4 | Specify whether to enforce GlobalProtect connections for network access.

(Windows 10 only) When **Enforce GlobalProtect Connection for Network Access** is enabled, the following application types are bypassed and all other outbound connections (not inbound connections) are blocked:

- GlobalProtect agent (**PanGPA.exe**), GlobalProtect service (**PanGPS.exe**), and Local Security Authority Subsystem Service (**lsass.exe**) processes
- DHCP, DNS, NetBIOS (Network Basic Input/Output System), and Link-Local Multicast Name Resolution (LLMNR) protocols
- Loopback interface traffic

(macOS only) When **Enforce GlobalProtect Connection for Network Access** is enabled, the following application types are bypassed and all other outbound and inbound connections are blocked:

- GlobalProtect application and GlobalProtect service (PanGPS)
- DHCP and DNS protocols
- Loopback interface traffic
- `ocspd`, `syspolicyd`, `ntpd`, `apsd`, and `trustd` processes

*To enforce GlobalProtect for network access, we recommend that you enable this feature only for users that connect in **User-logon** or **Pre-logon** modes. Users that connect in **On-demand** mode may not be able to establish a connection within the permitted grace periods.*

In the App Configurations area, configure any of the following options:

- To force all network traffic to traverse a GlobalProtect tunnel, set **Enforce GlobalProtect Connection for Network Access** to **Yes**. By default, GlobalProtect is not required for network access, meaning users can still access the internet when GlobalProtect is disabled or disconnected. To provide instructions to users before traffic is blocked, configure GlobalProtect to **Displays Traffic Blocking Notification Message**, and optionally specify when to display the message (**Traffic Blocking Notification Delay**).

  *When **Enforce GlobalProtect Connection for Network Access** is enabled, you may want to consider allowing users to disable the GlobalProtect app with a passcode. The **Enforce GlobalProtect Connection for Network Access** feature enhances the network security by requiring a GlobalProtect connection for network access. On rare occasions, endpoints may fail to connect to the VPN and require remote administrative login for troubleshooting. By disabling the GlobalProtect app (for Windows or macOS) using the passcode provided by the administrator during the troubleshooting session, you can allow administrators to connect to your endpoint remotely.*
- Configure exclusions for specific local IP addresses or network segments for network access by entering these IP addresses to **Allow traffic to specified hosts/networks when Enforce GlobalProtect Connection for Network Access is enabled and GlobalProtect Connection is not established**. Specify up to twenty IP addresses or network segments for

which you want to allow access when you enforce GlobalProtect for network access and GlobalProtect cannot establish a connection.

This option requires a Content Release version of 8196-5685 or later.

If you are using Deploy Connect Before Logon Settings in the Windows Registry *in conjunction with the enforcer for smart card authentication or username/password-based authentication for user login using an authentication service such as LDAP, RADIUS, or OTP, you must configure exclusions for specific IP addresses or network segments for the portal and gateway by entering them to* ***Allow traffic to specified FQDN when Enforce GlobalProtect Connection for Network Access is enabled and GlobalProtect Connection is not established****.*

By configuring exclusions, you can improve the user experience by allowing users to access local resources when GlobalProtect is disconnected. For example, when GlobalProtect is not connected, GlobalProtect can allow access to link-local addresses. This allows a user to access a local network segment or broadcast domain.

- (Windows 10 and macOS running macOS Catalina 10.15.4 or later only; Requires GlobalProtect™ app 5.2 or later) Configure exclusions for specific fully qualified domain names for which you want to allow access when you enforce GlobalProtect connections for network access by entering these fully qualified domain names to **Allow traffic to specified FQDN when Enforce GlobalProtect Connection for Network Access is enabled and GlobalProtect Connection is not established**.

  Specify up to 40 fully qualified domain names for which you want to allow access when you enforce GlobalProtect connections for network access and GlobalProtect cannot establish a connection.

  If you are using Deploy Connect Before Logon Settings in the Windows Registry *in conjunction with the enforcer for smart card authentication or username/password-based authentication for user login using an authentication service such as LDAP, RADIUS, or OTP, you must configure exclusions for specific fully qualified domain names for the portal and gateway by entering them to* ***Allow traffic to specified FQDN when Enforce GlobalProtect Connection for Network Access is enabled and GlobalProtect Connection is not established****.*

  The fully qualified domain names that you provide are used only when **Enforce GlobalProtect Connection for Network Access** is set to **Yes**. Use commas to separate multiple fully qualified domain names (for example, google.com, gmail.com). Use the wildcard character (*) for domain names (for example, *.gmail.com). The maximum length is 1,024 characters.

  This option requires a Content Release version of 8284-6139 or later.

  By configuring FQDN exclusions, you can improve the user experience by allowing users to access specific resources when GlobalProtect is disconnected. For example, the endpoint can communicate with a cloud-hosted identity provider (IdP) for authentication purposes

or a remote device management server even when the Enforce GlobalProtect for Network Access feature is enabled.

- If your users must log in to a captive portal to access the internet, specify a **Captive Portal Exception Timeout (sec)** to indicate the amount of time (in seconds) within which users can log in to the captive portal (range is 0 to 3600 seconds; default is 0 seconds). If users do not log in within this time period, the captive portal login page times out and users will be blocked from using the network.

  To enable the GlobalProtect app to display a notification message when it detects a captive portal, set the **Display Captive Portal Detection Message** to **Yes**. In the **Captive Portal Notification Delay (sec)** field, enter the amount of time (in seconds) after which the GlobalProtect app displays this message (range is 1 to 120 seconds; default is 5 seconds). GlobalProtect initiates this timer after the captive portal has been detected but before the internet becomes reachable. You can also provide additional instructions by configuring a **Captive Portal Detection Message**.

  To automatically launch your default web browser upon captive portal detection so that users can log in to the captive portal seamlessly, in the **Automatically Launch Webpage in Default Browser Upon Captive Portal Detection** field, enter the fully qualified domain name (FQDN) or IP address of the website that you want to use for the initial connection attempt that initiates web traffic when the default web browser launches (maximum length is 256 characters). The captive portal then intercepts this website connection attempt and redirects the default web browser to the captive portal login page. If this field is empty (default), GlobalProtect does not launch the default web browser automatically upon captive portal detection.

*These options require Content Release version 607-3486 or later. The **Captive Portal Notification Delay** requires Content Release version 8118-5277 or later. The **Automatically Launch Webpage in Default Browser Upon Captive Portal Detection** option requires Content Release version released on July 8th, 2019 or later.*

STEP 5 | Specify additional GlobalProtect connection settings.

When single sign-on (SSO) is enabled (default), the GlobalProtect app uses the user's Windows login credentials to automatically authenticate and connect to the GlobalProtect portal and gateway. This also allows the GlobalProtect app to wrap third-party credentials to ensure that Windows users can authenticate and connect even with a third-party credential provider.

In the App Configurations area, configure any of the following options:

- (Windows and macOS only; macOS support requires Content Release version 8196-5685 or later) Set **Use Single Sign-On (Windows)** or **Use Single Sign-On (macOS)** to **No** to disable single sign-on.

  *If you configure the GlobalProtect gateway to authenticate users through SAML authentication and also generate and accept cookies for authentication override, you must set the **Use Single Sign-On** option to **No** when the user's Windows username is different from his or her SAML username (for example, the Windows username is "user" and the SAML username is "user123") or if one username contains a fully qualified domain name (for example, the Windows username is "user" and the SAML username is "user@example.com").*

- (Windows 10 only; Content Release version 8451-6911 or later; Requires GlobalProtect app 6.0 or later) Set **Use Single Sign-On for Smart Card PIN (Windows)** to **Yes** to enable the GlobalProtect app to use SSO for smart card PIN. The default is **No**.

  If you have configured the GlobalProtect portal to authenticate end users through single sign-on (SSO) using smart card authentication, end users can connect without having to re-enter their smart card Personal Identification Number (PIN) in the GlobalProtect app for a seamless SSO experience. End users can leverage the same smart card PIN for GlobalProtect with their Windows endpoint. This improves the user experience by reducing the number of times end users must enter their smart card PIN when they log in. After the end user successfully logs in to the Windows endpoint, the GlobalProtect app acquires and remembers their smart card PIN to authenticate with the GlobalProtect portal and gateway.

  You must set the pre-deployed setting on the end user endpoints before you can enable SSO for smart card PIN. GlobalProtect retrieves this entry only once, when the GlobalProtect app initializes.

  If the **USESSOPIN** value is set to **yes** in the pre-deployed setting of the client machine and the **Use Single Sign-On for Smart Card PIN (Windows)** option is set to **no** in the portal configuration, end users will not have the best user experience. The **Use Single Sign-On for Smart Card PIN (Windows)** option of the GlobalProtect portal and the pre-deployed setting in the end user machine must have the same value to provide the best user experience.

  *If you set both **Use Single Sign-On (Windows)** and **Use Single Sign-On for Smart Card PIN (Windows)** options to **yes** in the portal configuration, the **Use Single Sign-On for Smart Card PIN (Windows)** option takes precedence over the **Use Single Sign-On (Windows)** option.*

- (Content Release version 8284-6139 or later; Requires GlobalProtect app 5.2 or later) Set **Use Default Browser for SAML Authentication** to **Yes** to enable the GlobalProtect app to

open the default system browser for SAML authentication. The default is **No**. The app will open an embedded browser.

If you have configured the GlobalProtect portal to authenticate users through Security Assertion Markup Language (SAML) authentication, end users can connect to the app or other SAML-enabled applications without having to re-enter their credentials, for a seamless single sign-on (SSO) experience. You can enable the GlobalProtect app so that end users can leverage the same login for GlobalProtect and use their Use the Default System Browser for SAML Authentication such as Chrome, Firefox, or Safari.

- Specify the amount of time (in hours) during which you want the GlobalProtect app to **Automatically Use SSL When IPSec Is Unreliable** (range is 0-168 hours). If you configure this option, the GlobalProtect app does not attempt to establish an IPSec tunnel during the specified time period. This timer initiates each time an IPSec tunnel goes down due to a tunnel keepalive timeout.

  If you accept the default value of **0**, the app does not fall back to establishing an SSL tunnel if it can establish an IPSec tunnel successfully. It falls back to establishing an SSL tunnel only when the IPSec tunnel cannot be established.

  This option requires Content Release version released on July 8th, 2019 or later.

- (Content Release version 8387-6595 or later; Requires GlobalProtect app 5.2.6 or later) Set **Display IPSec to SSL Fallback Notification** to **Yes** to enable the GlobalProtect app to display an SSL fallback notification only when GlobalProtect falls back to using SSL after attempting IPSec. Set **Display IPSec to SSL Fallback Notification** to **No** to disable the app from displaying the notification. By default, this option is set to **Yes**. If you specify the amount of time (in hours) during which you want the GlobalProtect app to **Automatically Use SSL When IPSec Is Unreliable**, for example 5 hours, the app will not display this notification during the specified time period because it will not attempt to establish an IPSec tunnel and instead establish an SSL tunnel.
- Choose the SSL connection options for the GlobalProtect app. You can opt to enforce SSL connections only, disallow SSL connections, or allow the user to choose SSL or IPSec (default) depending on geo-location and network performance to provide the best user experience.

  In the App Configuration area, choose the **Connect with SSL Only** options you want to allow.

  This option requires Content Release version 8207-5750 or later.

  - **Yes**—Require that all GlobalProtect clients connect using SSL only.
  - **No**—Connect with the protocol configured on the gateway for the VPN connection. If the gateway configuration has enabled IPSec, then it will use IPSec for the VPN

connection. If the gateway has SSL configured, then it will use SSL for the VPN connection.

- **User can Change**—Allow the user to change, whether they want to use SSL or stay with IPSec, on the GlobalProtect app.

  On the app, the user can select **Settings** > **General** to enable **Connect with SSL Only** and **Settings** > **Connection** to verify that the **Protocol** is **SSL**.

- (Content Release version 8346-6423 or later; Requires GlobalProtect app 5.2.4 or later) Enter the **GlobalProtect Connection MTU (bytes)** value that is used by the app for gateway connections. You can specify the MTU range from 1000 to 1420 bytes instead of the preset default MTU value of 1400 bytes. The default value is 1400 bytes.

  (Windows UWP only) After you manually configure the **GlobalProtect Connection MTU (bytes)** value using the **`netsh`** command, the GlobalProtect client is unable to set the **GlobalProtect Connection MTU (bytes)** value in the portal configuration greater than the manually configured value.

  If the MTU value is less than 1280 bytes and IPv6 is enabled, the GlobalProtect adapter automatically changes the value to 1280 bytes as per the minimum supported MTU requirement for IPv6.

  You can optimize the connection experience for end users connecting over networks that require maximum transmission unit (MTU) values lower than the standard of 1500 bytes by configuring the MTU value that is used by the GlobalProtect app to connect to the gateway. By reducing the MTU size, you can eliminate performance and connectivity issues that occur due to fragmentation when the VPN tunnel connections go through multiple Internet Service Providers (ISPs) and network paths with MTU lower than 1500 bytes. For example, you can adjust the MTU value for a specific group of users from a region to a lower MTU value by using a different portal configuration with a lower MTU value requirement. The MTU value that you configured for a specific portal applies to all the gateway tunnel connections listed for that portal for both IPSec and SSL tunnel protocols.

  *In Pre-Logon (Always On) deployments, GlobalProtect must recreate the user tunnel in order for the new configured MTU value in the user's portal configuration to take effect. This deployment requires the **Pre-logon Tunnel Rename Timeout** value be set to **0** in the GlobalProtect portal configuration.*

- Enter the **Maximum Internal Gateway Connection Attempts** to specify the number of times the GlobalProtect app can retry the connection to an internal gateway after the first attempt fails (range is 0-100; 4 or 5 is recommended; the default value of 0 indicates that the GlobalProtect app does not retry the connection). By increasing this value, you can enable the app to connect to an internal gateway that is temporarily down or unreachable but comes back up before the specified number of retries are exhausted. Increasing the value also ensures that the internal gateway receives the most up-to-date user and host information.
- Enter the **GlobalProtect App Config Refresh Interval** to specify the number of hours that the GlobalProtect portal waits before it initiates the next refresh of a client's configuration (range is 1-168; default is 24).
- (Windows only) Depending on your security requirements, specify whether to **Retain Connection on Smart Card Removal**. By default, this option is set to **Yes**, meaning

GlobalProtect retains the tunnel when a user removes a smart card containing a client certificate. To terminate the tunnel, set this option to **No**.

This feature requires Content Release version 590-3397 or later.

- Configure an **Automatic Restoration of VPN Connection Timeout** to specify the action GlobalProtect takes when the tunnel is disconnected. Set this option to a non-zero value to allow GlobalProtect to attempt to reestablish the connection after the tunnel is disconnected. If the tunnel downtime exceeds the configured timeout value (range is 0 to 180 minutes; default is 30), tunnel restoration will not be performed, and the result is the same as if you set this option to **0**. Set this option to **0** to prevent GlobalProtect from attempting to reconnect after the tunnel is disconnected. If you configure the connection setting as **Always-On**, GlobalProtect will perform network discovery again. If you configure the connection setting as **On-Demand**, the user must manually connect again. Configure the **Wait Time Between VPN Connection Restore Attempts** to adjust the amount of time (in seconds) that GlobalProtect waits between attempts to restore the connection (range is 1 to 60 seconds; default is 5). The GlobalProtect client tries several times to restore the connection, and uses this wait time as the connection timeout value.

  *With the Always On connect method, if a user switches from an external network to an internal network before the timeout value expires, GlobalProtect does not perform network discovery. As a result, GlobalProtect restores the connection to the last known external gateway. To trigger internal host detection, the user must select **Refresh Connection** from the settings menu on the GlobalProtect status panel.*

STEP 6 | Configure the menus and UI views that are available to users who have this agent configuration.

In the App Configurations area, configure any of the following options:

- If you want users to see only basic status information within the application, set **Enable Advanced View** to **No**. When you disable this option, users can view information from the following tabs:
  - **General**—Displays the username and portal(s) associated with the GlobalProtect account.
  - **Notification**—Displays any GlobalProtect notifications.

  The default is **Yes**. When you enable this option, users can view the following additional tabs:
  - **Connection**—Lists the gateways configured for the GlobalProtect app and information about each gateway.
  - **Host Profile**—Displays the endpoint data that GlobalProtect uses to monitor and enforce security policies using Host Information.
  - **Troubleshooting**—Displays information about the network configuration, route settings, active connections, and logs. You can also collect logs generated by GlobalProtect and set the logging level.

    In order for the GlobalProtect app to send troubleshooting logs, diagnostic logs, or both to Cortex Data Lake for further analysis, you must configure the GlobalProtect portal to enable the Configure the App Log Collection Settings on the GlobalProtect Portal. Additionally, you can Configure the App Log Collection Settings on the GlobalProtect Portal that can contain IP addresses or fully qualified domain names of the web servers/resources that you want to probe, and to determine issues such as latency or network performance on the end user's endpoint.
- If you want hide the GlobalProtect system tray icon on endpoints, set **Display GlobalProtect Icon** to **No**. When the icon is hidden, users cannot perform tasks such as changing saved passwords, rediscovering the network, resubmitting host information, viewing troubleshooting information, or initiating on-demand connections. However, HIP notification messages, login prompts, and certificate dialogs still display as necessary.
- To prevent users from performing network discovery, set the **Enable Rediscover Network Option** to **No**. When you disable this option, the **Refresh Connection** option is grayed out in the settings menu of the GlobalProtect status panel.
- To prevent users from manually resubmitting HIP data to the gateway, set **Enable Resubmit Host Profile Option** to **No**. This option, which is enabled by default, is useful in cases where

HIP-based security policy prevents users from accessing resources because it allows the user to fix the compliance issue on the computer before resubmitting the HIP data.

- (Windows only) To allow GlobalProtect to display notifications in the system tray, set **Show System Tray Notifications** to **Yes**.
- To create a custom message to display to users when their passwords are about to expire, enter a **Custom Password Expiration Message (LDAP Authentication Only)**. The maximum message length is 200 characters.
- To create a custom message to specify password policies or requirements when users change their Active Directory (AD) password, enter a **Change Password Message**. The maximum message length is 255 characters.

STEP 7 | Define what end users with this configuration can do in their app.

- Set **Allow User to Change Portal Address** to **No** to disable the **Portal** field on the status panel of the GlobalProtect app. Because the user will not be able to specify the portal to which to connect, you must supply the default portal address in the Windows Registry (`HKEY_LOCAL_MACHINE\SOFTWARE\PaloAlto Networks\GlobalProtect\PanSetup` with key `Portal`) or the macOS plist (`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist` with key `Portal` under dictionary `PanSetup`). For more information, see Deploy App Settings Transparently.
- To prevent users from dismissing the welcome page, set **Allow User to Dismiss Welcome Page** to **No**. When this option is set to **Yes**, the user can dismiss the welcome page and prevent GlobalProtect from displaying the page after subsequent logins.
- To require the end user to accept terms of use to comply with corporate policies and to see a page to review your company's terms of service before connecting to GlobalProtect, set **Have User Accept Terms of Use Before Creating Tunnel** to **Yes**. When this option is set to **No**, the end user is not required to accept terms of use to comply with corporate policies before connecting to GlobalProtect.

STEP 8 | Specify whether users can disable the GlobalProtect app.

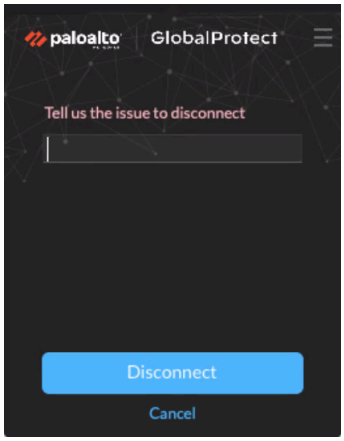
The **Allow User to Disable GlobalProtect** option applies to agent configurations with the **User-Logon (Always On) Connect Method**. In user-logon mode, the app automatically connects as soon as the user logs in to the endpoint. This mode is sometimes referred to as "always on", which is why the user must override this behavior to disable the GlobalProtect app.

By default, this option is set to **Allow**, which permits users to disable GlobalProtect without providing a comment, passcode, or ticket number. However,

If the GlobalProtect system tray icon is not visible, users cannot disable the GlobalProtect app. See Step 6 for more details.

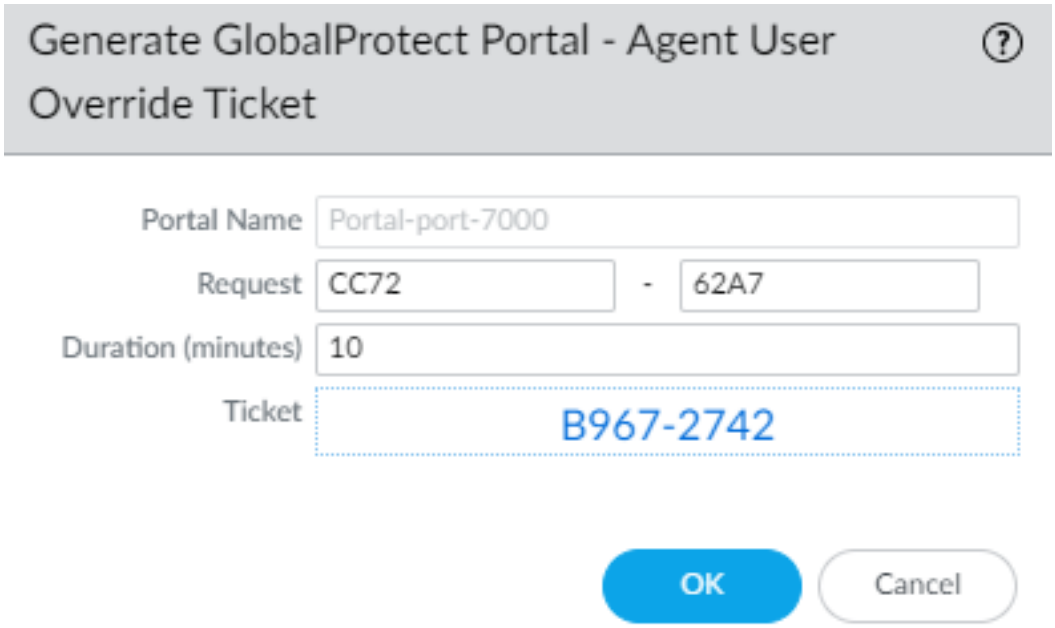
- To prevent users with the user-logon connect method from disabling GlobalProtect, set **Allow User to Disable GlobalProtect App** to **Disallow**.
- To allow users to disable GlobalProtect only if they need to respond to one or more reasons such as **Internet speed slow** or **App not working** (if required). The reasons for disconnecting are displayed only if you configure **Display the following reasons to disconnect GlobalProtect (Always-on mode)**. If you did not configure the GlobalProtect app

to display the reasons for disconnecting, end users are prompted to provide a reason for disconnecting from the app.



- To allow end users to provide a reason a reason for disconnecting, set **Allow User to Disable GlobalProtect App** to **Allow with Comment**. With this option, end users can select **Other reason** in the GlobalProtect app to supply a reason for disconnecting.
- To allow users to disable GlobalProtect only if they provide a passcode, set **Allow User to Disable GlobalProtect App** to **Allow with Passcode**. Then, in the Disable GlobalProtect App area, enter (and confirm) the **Passcode** that the end users must supply.
- To allow users to disable GlobalProtect only if they provide a ticket, set **Allow User to Disable GlobalProtect** to **Allow with Ticket**. With this option, the disable action triggers the app to generate a Request Number, which the end user must communicate to the administrator. The administrator then clicks **Generate Ticket** on the **Network** > **GlobalProtect** > **Portals** page and enters the request number from the user to generate the

ticket. The administrator provides the ticket to the end user, who enters it into the Disable GlobalProtect dialog to disable the app.



- To limit the number of times users can disable the GlobalProtect app, specify the **Max Times User Can Disable** value in the Disable GlobalProtect App area. A value of 0 (default) indicates that users are not limited in the number of times they can disable the app.

  *This setting is applicable only with the **Allow**, **Allow with Comment**, and **Allow with Passcode** disable options.*

  If your users disable the GlobalProtect app the maximum number of times and must continue to have the ability to disable the app thereafter:

  - You can increase the **Max Times User Can Disable** value in the GlobalProtect portal agent configuration (**Network** > **GlobalProtect** > **Portals** > ***<portal-config>*** > **Agent** > ***<agent-config>*** > **App**). The user must then select **Refresh Connection** from the settings menu of the GlobalProtect status panel or establish a new GlobalProtect connection in order for the new value to take effect.
  - Users can reset the counter by reinstalling the app.
- To restrict the amount of time for which the app can be disabled, enter a **Disable Timeout (min)** value in the Disable GlobalProtect App area. A value of 0 (default) indicates that there is no restriction for how long the user can keep the app disabled.

  *This setting is applicable only with the **Allow**, **Allow with Comment**, and **Allow with Passcode** disable options.*

STEP 9 | Specify whether users can uninstall the GlobalProtect app.

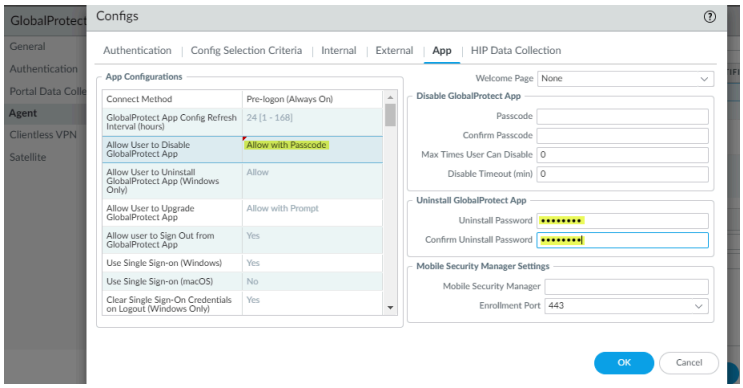
Use the **Allow User to Uninstall GlobalProtect App** option to allow users to uninstall the GlobalProtect app, prevent them from uninstalling the GlobalProtect app, or allow them to uninstall if they specify a password you create.

This setting gets pushed to the endpoint device registry when it connects to portal for the first time, and is saved for each portal to which it connects.

This option requires Content Release version 8207-5750 or later.

- To allow users to uninstall the GlobalProtect app with no restrictions, select **Allow**.
- To prevent users from uninstalling the GlobalProtect app, select **Disallow**.

  When you set it to **Disallow** in the Windows registry, the value for that portal is set to 1 under `Computer\\HKEY_LOCAL_MACHINE\\SOFTWARE\\Palo Alto Networks\\GlobalProtect\\Settings\\ 'Uninstall = 1'`.
- To allow users to uninstall the GlobalProtect app with a password, select **Allow with Passcode**; then, in the Uninstall GlobalProtect App section, enter an **Uninstall Password** and **Confirm Uninstall Password**.



STEP 10 | Specify whether users can sign out of the GlobalProtect app.

In the App Configurations area, set **Allow user to Sign Out from GlobalProtect App** to **No** to prevent users from logging out of the GlobalProtect app; set **Allow user to Sign Out from GlobalProtect App** to **Yes** to allow users to log out.

This option requires a Content Release version of 8196-5685 or later.

STEP 11 | Configure the certificate settings and behavior for the users that receive this configuration.

In the App Configurations area, configure any of the following options:

- **Client Certificate Store Lookup**—Select which store the app should use to look up client certificates. **User** certificates are stored in the Current User certificate store on Windows and in the Personal Keychain on macOS. **Machine** certificates are stored in the Local

Computer certificate store on Windows and in the System Keychain on macOS. By default, the app looks for **User and machine** certificates in both places.

- **SCEP Certificate Renewal Period (days)**—With SCEP, the portal can request a new client certificate before the certificate expires. This time before the certificate expires is the optional *SCEP certificate renewal period*. During a configurable number of days before a client certificate expires, the portal can request a new certificate from the SCEP server in your enterprise PKI (range is 0-30; default is 7). A value of 0 means the portal does not automatically renew the client certificate when it refreshes the agent configuration.

  For the GlobalProtect app to obtain the new certificate during the renewal period, the user must log in to the app. For example, if a client certificate has a lifespan of 90 days, the certificate renewal period is 7 days, and the user logs in during the final 7 days of the certificate lifespan, the portal acquires a new certificate and deploys it along with a fresh agent configuration. For more information, see Deploy User-Specific Client Certificates for Authentication.
- **Extended Key Usage OID for Client Certificate** (Windows and macOS endpoints only)—Use this option only if you enabled client authentication, expect multiple client certificates to be present on the endpoint, and have identified a secondary purpose by which you can filter the client certificates. This option enables you to specify a secondary purpose for a client certificate using the associated object identifier (OID). For example, to display only client certificates that also have a purpose of Server Authentication, enter the OID 1.3.6.1.5.5.7.3.1. When the GlobalProtect app finds only one client certificate that matches the secondary purpose, GlobalProtect automatically selects and authenticates using that certificate. Otherwise, GlobalProtect prompts the user to select the client certificate from the list of filtered client certificates that match the criteria. For more information, including a list of common certificate purposes and OIDs, see Enable Certificate Selection Based on OID.
- If you do not want the app to establish a connection with the portal when the portal certificate is not valid, set **Allow User to Continue with Invalid Portal Server Certificate** to **No**. Keep in mind that the portal provides the agent configuration only; it does not provide network access. Therefore, security to the portal is less critical than security to the gateway. However, if you have deployed a trusted server certificate for the portal, disabling this option can help prevent man-in-the-middle (MITM) attacks.

STEP 12 | Specify whether users receive login prompts when multi-factor authentication is required to access sensitive network resources.

For internal gateway connections, sensitive network resources (such as financial applications or software development applications) may require additional authentication. You can Configure GlobalProtect to Facilitate Multi-Factor Authentication Notifications that are required to access these resources.

In the App Configurations area, configure any of the following options:

- Set **Enable Inbound Authentication Prompts from MFA Gateways** to **Yes**. To support multi-factor authentication (MFA), the GlobalProtect app must receive and acknowledge UDP prompts that are inbound from the gateway. Select **Yes** to enable GlobalProtect

apps to receive and acknowledge the prompt. By default, the value is set to **No**, meaning GlobalProtect will block UDP prompts from the gateway.

- Specify the **Network Port for Inbound Authentication Prompts (UDP)** that the GlobalProtect app uses to receive inbound authentication prompts from MFA gateways. The default port is 4501. To change the port, specify a number from 1 to 65535.
- Specify the **Trusted MFA Gateways** that the GlobalProtect app can trust for multi-factor authentication. When a GlobalProtect app receives a UDP message on the specified network port, GlobalProtect displays an authentication message only if the UDP prompt comes from a trusted gateway.
- Configure the **Inbound Authentication Message**; for example, `You have attempted to access a protected resource that requires additional authentication. Proceed to authenticate at:`. When users attempt to access a resource that requires additional authentication, GlobalProtect receives and displays an inbound authentication message. GlobalProtect automatically appends the URL for the Authentication Portal page that you specify when you configure multi-factor authentication to the inbound authentication message.

STEP 13 | (Windows only) Configure settings for Windows endpoints that receive this configuration.

- **Resolve All FQDNs Using DNS Servers Assigned by the Tunnel (Windows Only)**—Configure the DNS resolution preferences for the GlobalProtect tunnel. Select **No** to allow Windows endpoints to send DNS queries to the DNS server set on the physical adapter if the initial query to the DNS server configured on the gateway is not resolved. This option retains the native Windows behavior to query all DNS servers on all adapters recursively but can result in long wait times to resolve some DNS queries. Select **Yes** (default) to allow Windows endpoints to resolve all DNS queries with the DNS servers you configure on the gateway instead of allowing the endpoint to send some DNS queries to the DNS servers set on the physical adapter.

  This feature does not support DNS over TCP.

- **Send HIP Report Immediately if Windows Security Center (WSC) State Changes**—Select **No** to prevent the GlobalProtect app from sending HIP data when the status of the Windows Security Center (WSC) changes. Select **Yes** (default) to immediately send HIP data when the status of the WSC changes.
- **Clear Single Sign-On Credentials on Logout**—Select **No** to keep single sign-on credentials when the user logs out. Select **Yes** (default) to clear them and force users to enter credentials upon the next login.
- **Use Default Authentication on Kerberos Authentication Failure**—Select **No** to use only Kerberos authentication. Select **Yes** (default) to retry using the default authentication method after Kerberos authentication fails.

STEP 14 | (Starting with GlobalProtect™ app 6.1) Specify the **Proxy Auto-Configuration (PAC) File URL** that you want to push to the endpoint to configure proxy settings via the GlobalProtect portal. You can deploy different PAC URLs to different endpoints based username or group membership. Once the endpoint has the proxy settings, it uses the proxy server to

access the internet.The maximum URL length is 256 characters. The following Proxy Auto-Configuration (PAC) File URL methods are supported:

- Proxy Auto-Config (PAC) standard (for example, http://pac.<hostname or IP>/proxy.pac).
- Web Proxy Auto-Discovery Protocol (WPAD) standard (for example, http://wpad.<hostname or IP>/wpad.dat).

STEP 15 | (Windows only) Configure the GlobalProtect app for Windows endpoints to **Detect Proxy for Each Connection**.

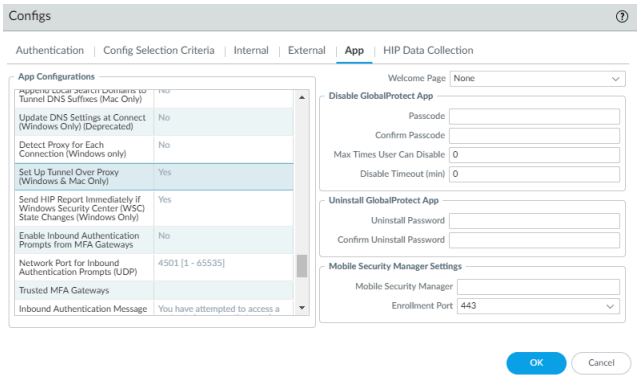
For more details about network traffic behavior based on proxy use, see Tunnel Connections Over Proxies.

- Select **No** to auto-detect the proxy for the portal connection and use that proxy for subsequent connections.
- Select **Yes** (default) to auto-detect the proxy for every connection.

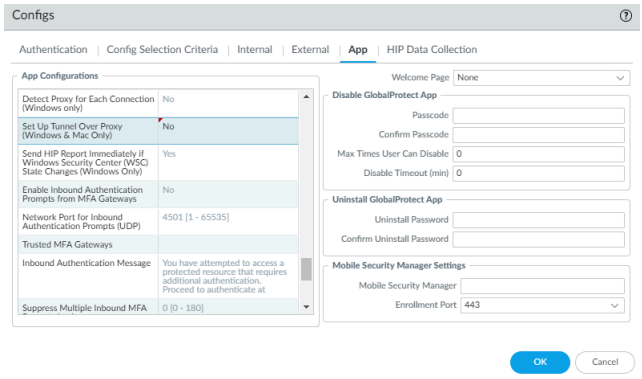
STEP 16 | (Windows and macOS only) Specify whether GlobalProtect must use proxies or bypass proxies.

With this setting, you can configure network traffic behavior based on GlobalProtect proxy use. See Tunnel Connections Over Proxies for more details.

- To require GlobalProtect to use proxies, set the **Set Up Tunnel Over Proxy (Windows & Mac only)** option to **Yes**.



- To require GlobalProtect to bypass proxies, set the **Set Up Tunnel Over Proxy (Windows & Mac only)** option to **No**.



STEP 17 | (Starting with GlobalProtect™ app 6.1) Set **Enable Advance Host Detection** to **Yes** to add an additional security layer during the internal host detection by the app. With the advanced internal host detection, the app validates the server certificate of the internal gateways in addition to performing a reverse DNS lookup of the internal host to determine whether the app is inside the enterprise network. Select **No** (default) for GlobalProtect app to perform internal host detection without validating the server certificate of the internal gateways.

STEP 18 | If your endpoints frequently experience latency or slowness when connecting to the GlobalProtect portal or gateways, consider adjusting the portal and TCP timeout values.

To allow more time for your endpoints to connect to or receive data from the portal or gateway, increase the timeout values as needed. Keep in mind that increasing the values can result in longer wait times if the GlobalProtect app is unable to establish the connection. In contrast, decreasing the values can prevent the GlobalProtect app from establishing a connection when the portal or gateway does not respond before the timeout expires.

In the App Configurations area, configure any of the following timeout options:

- **Portal Connection Timeout (sec)**—The number of seconds (between 1 and 600) before a connection request to the portal times out due to no response from the portal. When your firewall is running Applications and Threats content versions earlier than 777-4484, the default is 30. Starting with content version 777-4484, the default is 5.
- **TCP Connection Timeout (sec)**—The number of seconds (between 1 and 600) before a TCP connection request times out due to unresponsiveness from either end of the connection. When your firewall is running Applications and Threats content versions earlier than 777-4484, the default is 60. Starting with content version 777-4484, the default is 5.
- **TCP Receive Timeout (sec)**—The number of seconds before a TCP connection times out due to the absence of some partial response of a TCP request (range is 1-600; default is 30).

STEP 19 | (Windows 10 and macOS running macOS Catalina 10.15.4 or later; Requires GlobalProtect™ app 5.2 or later) Specify whether to enable split DNS to allow users to direct their DNS queries for applications and resources over the VPN tunnel or outside the VPN tunnel in addition to network traffic by specifying the **Split-Tunnel Option**.

Select **Network Traffic Only** to include and exclude rules that are applied only to network application traffic and not to DNS traffic. All DNS traffic goes through the VPN tunnel irrespective of the split tunnel based on the Configure a Split Tunnel Based on the Domain and Application that you specified for inclusions and exclusions. When you select **Both Network Traffic and DNS**, the split tunnel based on the Configure a Split Tunnel Based on the Domain and Application that you specified for inclusions and exclusions are applied to the DNS traffic and the associated network application traffic for that domain.

- (GlobalProtect app 6.2 and later) You can optionally push Host a Split Tunnel Configuration File on a Web Server to endpoints through the gateway using a split tunnel configuration file hosted on a web server, which allows you to add more excluded/included domains,

applications, or routes to split tunnel functionality without manually modifying the gateway configuration.

*If you selected **Both Network Traffic and DNS**, you must add at least one fake domain to the exclude list.*

With Split DNS, you can configure which domains are resolved by the VPN assigned DNS servers and which domains are resolved by the local DNS servers.

This option requires a Content Release version of 8284-6139 or later.

STEP 20 | (Optional—Requires GlobalProtect app 6.2) Set the **HIP Remediation Process Timeout (sec)** within which the GlobalProtect app will run a script to complete the HIP remediation process. After you Configure HIP Process Remediation the GlobalProtect app provides a specified timeout period in which the endpoint can run a remediation script if an endpoint fails a process check. After the timeout period expires, the GlobalProtect app resubmits the HIP report.

STEP 21 | Specify whether remote desktop connections are permitted over existing VPN tunnels by specifying the **User Switch Tunnel Rename Timeout**. When a new user connects to a Windows machine using Remote Desktop Protocol (RDP), the gateway reassigns the VPN tunnel to the new user. The gateway can then enforce security policies on the new user.

Allowing remote desktop connections over VPN tunnels can be useful in situations where an IT administrator needs to access a remote end-user system using RDP.

By default, the **User Switch Tunnel Rename Timeout** value is set to 0, meaning the GlobalProtect gateway terminates the connection if a new user authenticates over the VPN tunnel. To modify this behavior, configure a timeout value from 1 to 600 seconds. If the new user does not log in to the gateway before the timeout value expires, the GlobalProtect gateway terminates the VPN tunnel assigned to the first user.

*Changing the **User Switch Tunnel Rename Timeout** value only affects the RDP tunnel and does not rename a pre-logon tunnel when configured.*

STEP 22 | To enable GlobalProtect to preserve the existing VPN tunnel after users log out of their endpoint, specify a **Preserve Tunnel on User Logoff Timeout** value (range is 0 to 600 seconds; default is 0 seconds). If you accept the default value of **0**, GlobalProtect does not preserve the tunnel following user logout.

This option requires Content Release version released on July 8th, 2019 or later.

Consider the following GlobalProtect connection behaviors when you configure GlobalProtect to preserve the VPN tunnel:

- If the same user logs out and then logs back in to an endpoint within the specified timeout period in either Always On or On-Demand mode, GlobalProtect remains connected without requiring any user interaction (including portal and gateway authentication). If the user does

not log back in within the specified timeout period, the tunnel disconnects and he or she must reestablish the GlobalProtect connection.

- If a user logs out of an endpoint and then a different user logs in to the same endpoint in either Always On or On-Demand mode, the existing tunnel is renamed for the new user only if the new user authenticates to GlobalProtect successfully within the specified timeout period. If the new user does not log in and authenticate successfully within the specified timeout period, the existing tunnel disconnects and a new GlobalProtect connection must be established. If the new user is in Always On mode, GlobalProtect attempts to establish a new connection automatically. If the new user is in On-Demand mode, he or she must establish a new GlobalProtect connection manually.

STEP 23 | Specify how GlobalProtect app upgrades occur.

If you want to control when users can upgrade, you can customize the app upgrade on a per-configuration basis. For example, if you want to test a release on a small group of users before deploying it to your entire user base, you can create a configuration that applies to users in your IT group only, thus allowing them to upgrade and test while disabling upgrades in all other user/group configurations. After you have thoroughly tested the new version, you can modify the agent configurations for the rest of your users to allow the upgrade.

By default, the **Allow User to Upgrade GlobalProtect App** option is set to **Allow with Prompt**, which means end users are prompted to upgrade when a new version of the app is activated on the firewall. To modify this behavior, select one of the following options:

- **Allow Transparently**—Upgrades occur automatically without user interaction. Upgrades can occur when the user is working remotely or connected within the corporate network.
- **Internal**—Upgrades occur automatically without user interaction, provided the user is connected within the corporate network. This setting is recommended to prevent slow upgrades in low-bandwidth situations. When a user connects outside the corporate network, the upgrade is postponed and re-activated when the user connects within the corporate network. You must configure internal gateways and internal host detection to use this option.
- **Disallow**—This option prevents app upgrades.
- **Allow Manually**—End users initiate app upgrades. In this case, the user must select **Check Version** from the settings menu on the GlobalProtect status panel to determine if there is a new app version available, and then upgrade if desired. Note that this option will not work if the GlobalProtect app is hidden from the user. See Step 6 for details on the **Display GlobalProtect Icon** settings.

*Upgrades for **Allow Transparently** and **Internal** occur only if the GlobalProtect software version on the portal is more recent than the GlobalProtect software version on the endpoint. For example, a GlobalProtect 6.0.3 agent connecting to a GlobalProtect 6.0.1 portal is not upgraded.*

*Starting with GlobalProtect app 6.0, configurations set to **Allow with Prompt** do not prompt users to downgrade their app version when the app version that is activated on the portal is an earlier version. To see the prompt to downgrade, users must **Check for Updates** on the **About** tab.*

STEP 24 | Add a **Change Password Message** to specify password policies or requirements your users must follow when they change their passwords (for example, passwords must contain at least one number and one uppercase letter).

STEP 25 | Specify whether you want the GlobalProtect app to send gateway selection criteria logs to the firewall by specifying the **Log Gateway Selection Criteria** option.

Select **Yes** to enable the GlobalProtect app to send the enhanced logs for the gateway selection criteria to the firewall. The default is **No**. The app does not send the enhanced logs to the firewall.

To help you to identify details as to why the GlobalProtect app chose to connect to a specific gateway, the GlobalProtect app collects and reports information to identify gateway selection criteria and latency between the gateway and the endpoint. Information about the gateway selection criteria can help you to identify the priority and response time of the selected gateway, the list of gateway connection attempts, and statistics about the pre-tunnel and post-tunnel network latency. The enhanced log fields for the gateway selection criteria have been added to the GlobalProtect logs in **Monitor** > **Logs** > **GlobalProtect**.

STEP 26 | Specify whether to display a welcome page upon successful login.

A welcome page can be a useful way to direct users to internal resources that they can only access when connected to GlobalProtect, such as your Intranet or other internal servers.

By default, the only indication that the app has successfully connected is a balloon message that displays in the system tray/menubar.

To display a welcome page after a successful login, select **factory-default** from the **Welcome Page** drop-down. GlobalProtect displays the welcome page in the GlobalProtect app. You can also select a custom welcome page that provides information specific to your users, or to a specific group of users (based on which portal configuration gets deployed). For details on creating custom pages, see Customize the GlobalProtect Portal Login, Welcome, and Help Pages.

STEP 27 | Configure the GlobalProtect app log collection settings.

You can configure the GlobalProtect app to send troubleshooting logs, diagnostic logs, or both to Cortex Data Lake. See Checklist for GlobalProtect App Log Collection for Troubleshooting for details on setting up the components to enable the GlobalProtect app log collection for troubleshooting and to view the Details Within the GlobalProtect App Troubleshooting and Diagnostic Logs on the Explore app.

- (Content Release version 8350-14191 or later; Requires GlobalProtect app 5.2.5) Set **Enable Autonomous DEM and GlobalProtect App Log Collection for Troubleshooting** to **Yes** to enable the GlobalProtect app to display the **Report an Issue** option on the GlobalProtect app to allow end users to send the troubleshooting and diagnostic logs directly to Cortex Data Lake. You must configure the Cortex Data Lake certificate that is pushed from the portal as a client certificate to display the **Report an Issue** option. This certificate is used for the client to authenticate to Cortex Data Lake when sending the logs. When this setting is set to **No** (default), the GlobalProtect app will not display the **Report an**

Issue option and end users cannot send the troubleshooting and diagnostic logs to Cortex Data Lake.

- (Content Release version 8350-14191 or later; Requires GlobalProtect app 5.2.5) Enter up to ten HTTPS-based destination URLs that can contain IP addresses or fully qualified domain names (for example, https://10.10.10.10/resource.html, https://webserver/file.pdf, or https://google.com) to **Run Diagnostics Tests for These Destination Web Servers** on the GlobalProtect portal. To help you accurately identify download speed results, you can specify a download file location that has the relevant size. For example, the size of the file can range from 10 MB to 50 MB to calculate the sufficient download speed. However, this calculation is not true for the size limitation of the web page to fetch and download the file that can take less than a second, which is not a sufficient sample size to determine strong download speed results. This field is empty by default.

  The HTTPS-based destination URLs that can contain IP addresses or fully qualified domain names that you provide are used only when **Enable Autonomous DEM and GlobalProtect App Log Collection for Troubleshooting** is set to **Yes** and when diagnostics are performed. These HTTPS-based destination URLs are not used when the GlobalProtect app creates troubleshooting reports when encountering an issue. Use commas, semi-colons, or separate lines to separate multiple fully qualified domain names (for example, google.com, gmail.com).

STEP 28 | (Windows 10 and macOS only; Content Release version 8393-6628 or later; Requires GlobalProtect app 5.2.6) Specify whether you want to install the Autonomous DEM (ADEM) endpoint agent during the GlobalProtect app installation and allow end users to enable or disable user experience tests from the app.

Select **Install and user can enable/disable agent from GlobalProtect** to install the ADEM endpoint agent during the GlobalProtect app installation, and allow end users to enable or disable user experience tests from the GlobalProtect app. Select **Install and user cannot enable/disable agent from GlobalProtect** to install the ADEM endpoint agent during the GlobalProtect app installation, and not allow end users to enable or disable user experience tests from the GlobalProtect app. Select **Do Not Install** (default) to not install the ADEM endpoint agent during the GlobalProtect app installation.

For details about getting started with ADEM on Panorama Managed Prisma Access, see Get Started with Autonomous DEM. For details about getting started with ADEM on Cloud Managed Prisma Access, see Get Started with Autonomous DEM.

STEP 29 | (Windows only) Specify whether you want the GlobalProtect app to **Display Status Panel at Startup**.

- To suppress the status panel when users establish a GlobalProtect connection for the first time, select **No**.
- To automatically display the status panel when users establish a GlobalProtect connection for the first time, select **Yes**. With this option, users must click outside the status panel to close it manually.

STEP 30 | (Windows 10 and macOS only; Content Release version 8450-6909 or later; Requires GlobalProtect app 6.0) Set **Allow GlobalProtect UI to Persist for User Input** to **Yes** to allow the status panel to continue to be displayed on the screen while the end user is entering their credentials when logging in or cancels the request. When this setting is set to **No**

(default) and the end user must enter their credentials, they must click outside the status panel to minimize it manually.

STEP 31 | Save the agent configuration.

1. If you are done customizing your agent configurations, click **OK** to save your agent configuration. Otherwise, return to Define the GlobalProtect Agent Configurations to complete the agent configuration.
2. Click **OK** to save your portal configuration.
3. **Commit** the changes.

Customize the GlobalProtect Portal Login, Welcome, and Help Pages

GlobalProtect provides default login, welcome, and/or help pages. However, you can create your own custom pages with your corporate branding, acceptable use policies, and links to your internal resources.

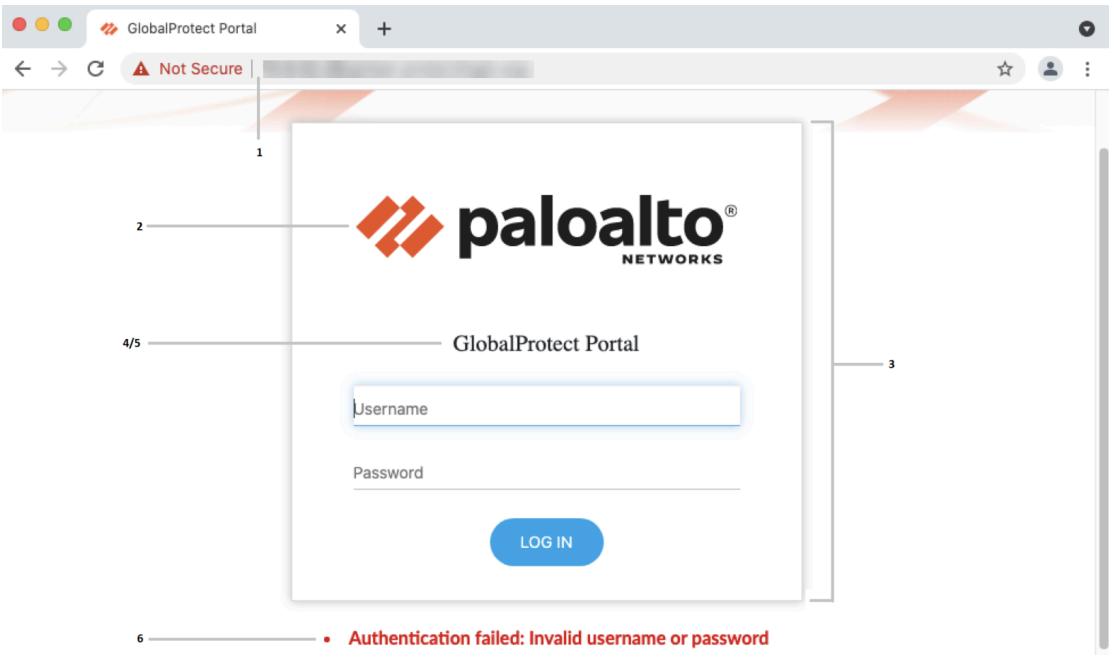
*You can alternatively disable browser access to the portal login page in order to prevent unauthorized attempts to authenticate to the GlobalProtect portal (configure the **Portal Login Page** > **Disable** option from **Network** > **GlobalProtect** > **Portals** > **<portal_config** > **General)**. With the portal login page disabled, you can instead use a software distribution tool, such as Microsoft's System Center Configuration Manager (SCCM), to allow your users to download and install the GlobalProtect app.*

STEP 1 | Export the default portal login, home, welcome, or help page.

1. Select **Device** > **Response Pages**.
2. Select the link for the corresponding GlobalProtect portal page, such as **GlobalProtect Portal Login Page**.
3. Select the predefined **Default** page and click **Export**.

STEP 2 | Edit the exported page.

1. Use the HTML text editor of your choice to open and edit the page.
2. To edit the login or home page, configure any of the following variables:
   - **GlobalProtect Portal Login Page**:

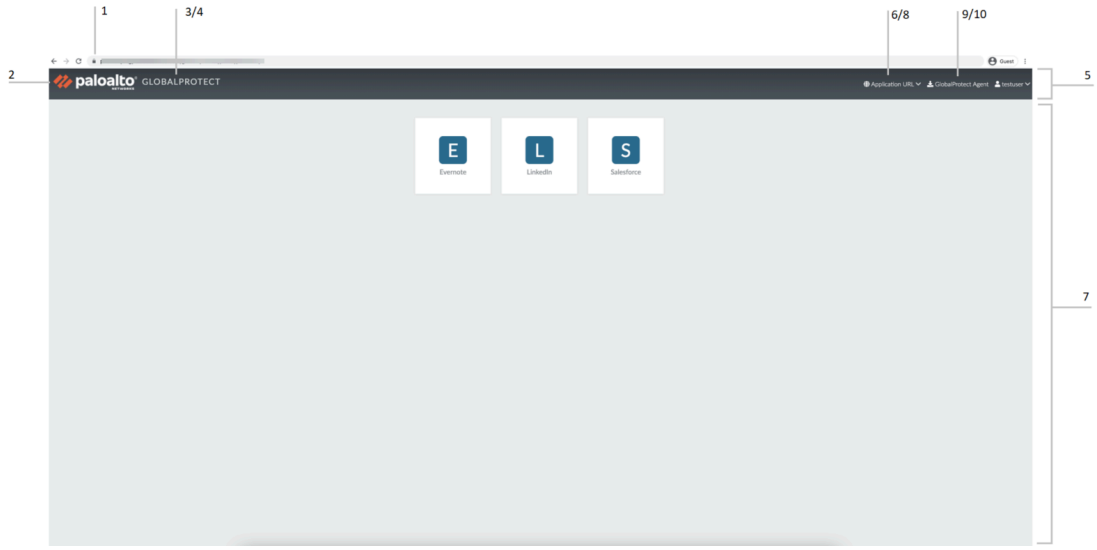


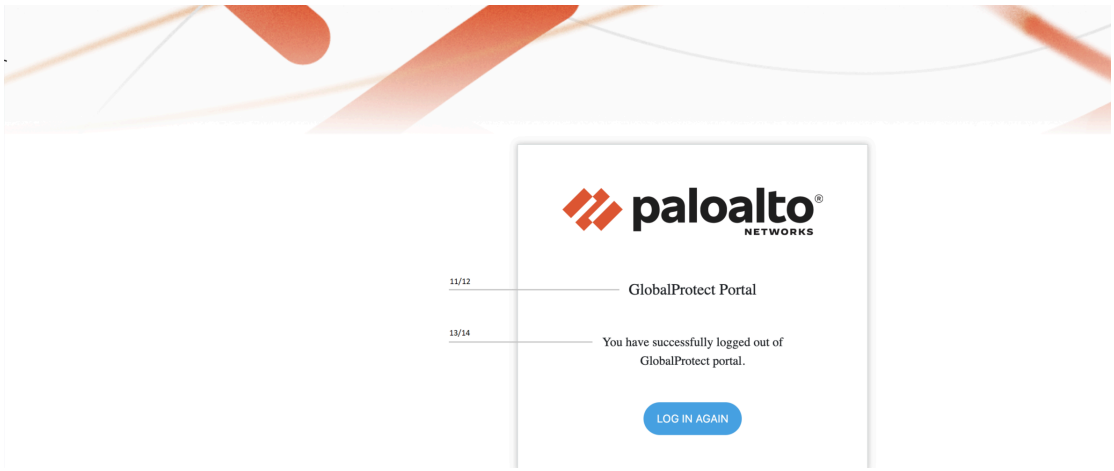
Label Number	Variable	Description	Example
1	`favicon`	URL of the icon displayed in the address bar of the web browser.	`var favicon = 'http://cdn.slidesharecdn.com/logo-24x24.jpg?3975762018';`
2	`logo`	URL of the company logo.	`var logo = 'http://cdn.slidesharecdn.com/logo-96x96.jpg?1382722588';`
3	`bg_color`	Login page background color.	`var bg_color = '#D3D3D3';`

Label Number	Variable	Description	Example
4	gp_portal_name	Text displayed under the company logo.	`var gp_portal_name = 'GlobalProtect Portal';`
5	gp_portal_name_color	Color of the text displayed under the company logo.	`var gp_portal_name_color = '#000000';`
6	error_text_color	Text color for logon failure messages.	`var error_text_`

Label Number	Variable	Description	Example
			`color = '#196390' ;`

- **GlobalProtect Portal Home Page:**





Label Number	Variable	Description	Example
1	`favicon`	URL of the icon displayed in the address bar of the web browser.	`var favicon = 'http://cdn.slidesharecdn.com/logo-24x24.`

Label Number	Variable	Description	Example
			`jpg?3975762018';`
2	`logo`	URL of the company logo.	`var logo = 'http://cdn.slidesharecdn.com/logo-96x96.jpg?1382722588';`
3	`navbar_text`	Navigation bar text.	`var navbar_text = 'GlobalProtect';`
4	`navbar_text_color`	Navigation bar text color.	`var navbar_text_color = '#D3D3D3';`
5	`navbar_bg_color`	Navigation bar background color.	`var navbar_bg_color = '#A9A9A9';`
6	`dropdown_bg_color`	Drop-down menu background color.	`var dropdown_bg_color = '#FFFFFF';`
7	`bg_color`	Home page background color.	`var bg_color = '#D3D3D3';`
8	`label_custom_app_url`	Label for custom/internal application URLs.	`var label_custom_app_url = 'Application URL';`
9	`display_globalprotect_agent`	Option to display or hide the GlobalProtect app download button. Enter **1** to display the download	`var display_globalprotect_agent`

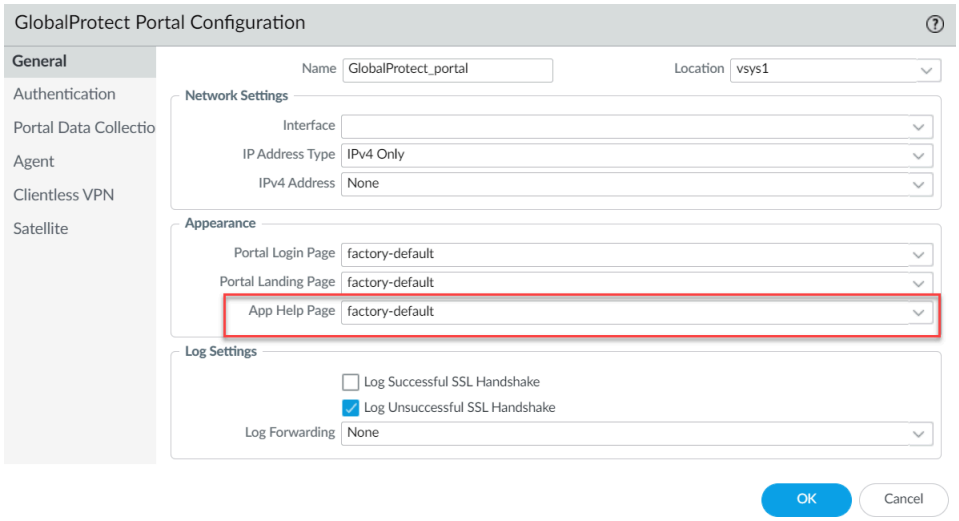
Label Number	Variable	Description	Example
		button. Enter **0** to hide the download button.	`= 1;`
10	`label_globalprotect_agent`	Label for the GlobalProtect app download button.	`var label_globalprotect_agent = 'GlobalProtect Agent';`
11	`gp_portal_name`	Text displayed under the company logo on the portal logout page.	`var gp_portal_name = 'GlobalProtect Portal';`
12	`gp_portal_name_color`	Color of the text displayed under the company logo on the portal logout page.	`var gp_portal_name_color = '#000000';`
13	`logout_text_array`	Messages displayed on the portal logout page after users log out of the portal. *You can only modify the existing messages; you cannot add new messages or delete any existing messages.*	`var logout_text_array = ["You have successfully logged out of GlobalProtect portal.", "GlobalProtect Gateway is not licensed. Contact system administrator.", "User not authenticated to GlobalProtect portal.", "System error, contact system administrator.", "System error, failed to delete user session. Contact system administrator.", "Can not create user session. Max-capacity`

Label Number	Variable	Description	Example
			`reached. Contact system administrator.");`
14	`logout_text_color`	Text color for messages displayed on the portal logout page after users log out of the portal.	`var logout_text_color = '#000000';`

3. Save the edited page with a new filename. Make sure that the page retains its UTF-8 encoding.

To set the **GlobalProtect App Help Page** to provide assistance to users with the GlobalProtect app:

1. Select **Network** > **GlobalProtect** > **Portals**, and then **Add** a portal.
2. Select **General**.
3. In the Appearance area, select the **factory-default** help page, **Import** a custom help page, or select **None** to remove the **Help** option from the **Settings** menu of the GlobalProtect status panel.



4. Click **OK** and **Commit** the changes.

STEP 3 | Import the new page(s).

1. Select **Device** > **Response Pages**.
2. Select the link for the corresponding GlobalProtect portal page.
3. **Import** the new portal page. Enter the path and filename in the **Import File** field or **Browse** to locate and select the file.
4. (Optional) Select the virtual system on which this page will be used from the **Destination** drop-down or select **shared** (default) to make it available to all virtual systems.
5. Click **OK** to import the file.

STEP 4 | Configure the portal to use the new page(s).

- **Portal Login Page**, **Portal Landing Page**, and **App Help Page**:
  1. Select **Network** > **GlobalProtect** > **Portals**.
  2. Select the portal to which you want to add the login, landing (home), or app help page.
  3. In the Appearance area of the **General** tab, select the new page from the relevant drop-down.
- **Custom Welcome Page**:
  1. Select **Network** > **GlobalProtect** > **Portals**.
  2. Select the portal to which you want to add the welcome page.
  3. On the **Agent** tab, select the agent configuration to which you want to add the welcome page.
  4. On the **App** tab, select the new page from the **Welcome Page** drop-down.
  5. Click **OK** to save the agent configuration.

STEP 5 | Save the portal configuration.

Click **OK** to save the portal configuration, and then **Commit** your changes.

STEP 6 | Verify that the new page displays.

- **Test the login page**—Open a web browser and go to the URL for your portal (do not add the :4443 port number to the end of the URL or you will be directed to the web interface for the firewall). For example, enter **`https://myportal`** rather than **`https://myportal:4443`**. The new portal login page will display.
- **Test the home page**—Open a web browser and go to the URL for your portal (do not add the :4443 port number to the end of the URL or you will be directed to the web interface for the firewall). For example, enter **`https://myportal`** rather than **`https://myportal:4443`**. Enter your **Username** and **Password**, and then **LOG IN** to the portal. The new portal home page will display.
- **Test the help page**—Click the GlobalProtect system tray icon to launch the GlobalProtect app. When the status panel opens, click the settings icon ( ) to open the settings menu. Select **Help** to view the new help page.
- **Test the welcome page**—Click the GlobalProtect system tray icon to launch the GlobalProtect app. When the status panel opens, click the settings icon ( ) to open the settings menu. Select **Welcome Page** to view the new welcome page.

Enforce GlobalProtect for Network Access

To reduce the security risk of exposing your enterprise when a user is off-premise, you can force users on endpoints running Windows 7 or Mac OS 10.9 and later releases to connect to GlobalProtect to access the network.

When this feature is enabled, GlobalProtect blocks all traffic until the agent is internal or connects to an external gateway. After the agent establishes a connection, GlobalProtect permits internal and external network traffic according to your security policy thus subjecting the traffic to inspection by the firewall and security policy enforcement. This feature also prevents the use of proxies as a means to bypass the firewall and access the internet.

If users must connect to the network using a captive portal (such as at a hotel or airport), you can also configure a grace period that provides users enough time to connect to the captive portal and then connect to GlobalProtect.

Because GlobalProtect blocks traffic unless the GlobalProtect agent can connect to a gateway, we recommend that you enable this feature only for users that connect in User-logon mode. Keep in mind that if you configure the app to use User-logon mode and the user disables or disconnects from GlobalProtect they will be able to connect to the network because the enforcement feature only works when GlobalProtect is enabled. To prevent users from accessing the network without a GlobalProtect connection make sure you do not enable the users in User-logon mode to disable or disconnect GlobalProtect.

STEP 1 | GlobalProtect Portals.

STEP 2 | Create or modify an agent configuration.

1. Select **Network** > **GlobalProtect** > **Portals** and select the portal configuration for which you want to add a client configuration or **Add** a new one.
2. From the **Agent** tab, select the agent configuration you want to modify or **Add** a new one.
3. Select the **App** tab.

STEP 3 | Configure GlobalProtect to force all network traffic to traverse a GlobalProtect tunnel.

In the App Configuration area, set **Enforce GlobalProtect Connection for Network access** to **Yes**. By default this option is set to **No** meaning that users can still access the internet if GlobalProtect is disabled or disconnected.

STEP 4 | (Optional) To provide additional information, configure a traffic blocking notification message.

The message can indicate the reason for blocking the traffic and provide instructions on how to connect, such as `To access the network, you must first connect to`

`GlobalProtect`. If you enable a message, GlobalProtect will display the message when GlobalProtect is disconnected but detects the network is reachable.

1. In the App Configuration area, make sure **Display Captive Portal Detection Message** is set to **Yes**. The default is **No**.
2. Specify the message text in the **Captive Portal Detection Message** field. The message must be 512 or fewer characters.
3. To specify the amount of time in which the user has to authenticate with a captive portal, enter the **Captive Portal Exception Timeout** in seconds (default is 0; range is 0 to 3600). For example, a value of 60 means that the user must log in to the captive portal within one minute after GlobalProtect detects the captive portal. A value of 0 means GlobalProtect does not allow users to connect to a captive portal and immediately blocks access.
4. If you have a **Captive Portal Detection Message** enabled, the message appears 85 seconds before the **Captive Portal Exception Timeout** occurs. If the **Capture Portal Exception Timeout** is 90 seconds or less, the message appears 5 seconds after a captive portal is detected.

STEP 5 | Click **OK** twice to save the configuration and then **Commit** your changes.

GlobalProtect Apps

The GlobalProtect™ app runs on your users' endpoints (desktop computer, laptop, tablet, or smart phone) to extend the security policy you use on your corporate network to your mobile users to ensure that their traffic is secured, whether they are accessing resources in your data center, private cloud, public cloud, or on the internet.

In addition to providing secure connectivity and remote access like traditional VPN products, the GlobalProtect app also:

- Protects your internal networks
- Provides app- and service-level control
- Secures IoT devices
- Protects against data loss and credential theft
- Provides advanced threat prevention
- Enables automatic quarantine of compromised devices

To see what endpoint OSes are supported on each GlobalProtect app version, refer to the Compatibility Matrix. After you decide what app versions you want to support for your users, you can Deploy the GlobalProtect App to End Users. You can also customize the app behavior when you Configure a GlobalProtect Gateway, or you can Deploy App Settings Transparently.

Deploy the GlobalProtect App to End Users

In order to connect to GlobalProtect™, an endpoint must be running the GlobalProtect app. Use the GlobalProtect app compatibility matrix to determine what version of the GlobalProtect app you want your users to run on their endpoints. Because the version that an end user must download and install to enable successful connectivity to your network depends on your environment, there is no direct download link for the GlobalProtect app on the Palo Alto Networks site.

After you decide what version of the GlobalProtect app you want your end users to run, you can deploy the app. The software deployment method depends on the type of endpoint as follows:

Platform	Deployment Options
macOS and Windows endpoints	There are several options you can use to distribute and install the software on macOS and Windows endpoints: • **Directly from the portal**—Download the app software to the firewall hosting the portal, and then activate it so that end users can install the updates when they connect to the portal. This option provides flexibility by allowing you to control how and when end users receive updates based on the agent configuration settings you define for each user, group, and/or operating system. However, if you have a large number of apps that require updates, it could put extra load on your portal. See Host App Updates on the Portal for instructions. • **From a web server**—If you have a large number of endpoints that need to upgrade the app simultaneously, consider hosting the app updates on a web server to reduce the load on the firewall. See Host App Updates on a Web Server for instructions. • **Transparently from the command line**—For Windows endpoints, you can deploy app settings automatically using the Windows Installer (Msiexec). However, to upgrade to a later app version using Msiexec, you must first uninstall the existing app. In addition, Msiexec allows for deployment of app settings directly on the endpoints by setting values in the Windows registry. Similarly, you can also deploy app settings to macOS endpoints, by configuring settings in the macOS plist. See Deploy App Settings Transparently. • **Using group policy rules**—In Active Directory environments, the GlobalProtect app can also be distributed to end users through an Active Directory group policy. AD Group policies allow for automated modification of Windows endpoint settings and software. Refer to the article at http://support.microsoft.com/kb/816102 for more information on how to use Group Policy to automatically distribute programs to endpoints or users. • **From a mobile endpoint management system**—If you use a mobile management system, such as an MDM or EMM, to

Platform	Deployment Options
	manage your mobile endpoints, you can use the system to deploy and configure the GlobalProtect app. See Mobile Device Management.
Windows 10 phone and Windows 10 UWP	• **From a mobile endpoint management system**—If you use a mobile management system, such as an MDM or EMM, that supports Windows 10 endpoints, you can use the system to deploy and configure the GlobalProtect app. See Mobile Device Management. • **From the Microft Store**—The end user can also download and install the GlobalProtect app directly from the Microsoft Store. For instructions on how to download and test the GlobalProtect app installation, see Download and Install the GlobalProtect Mobile App.
iOS and Android endpoints	• **From a mobile endpoint management system**—If you use a mobile management system, such as an MDM or EMM, you can use the system to deploy and configure the GlobalProtect app. See Mobile Device Management. • **From an app store**—The end user can also download and install the GlobalProtect app directly from the Apple App Store (iOS endpoints) or from Google Play (Android endpoints). For instructions on how to download and test the GlobalProtect app installation, see Download and Install the GlobalProtect Mobile App.
Chromebooks	• **From the Google Admin console**—The Google Admin console enables you to manage Chromebook settings and apps from a central, web-based location. To deploy the GlobalProtect app for Android on managed Chromebooks using the Google Admin console, see Deploy the GlobalProtect App for Android on Managed Chromebooks Using the Google Admin Console. *The GlobalProtect app for Android is supported only on certain Chromebooks. Chromebooks that do not support Android applications must continue to run the GlobalProtect app for Chrome, which is not supported starting with GlobalProtect app 5.0 and later.* • **From Workspace ONE**—You can deploy the GlobalProtect app for Android on managed Chromebooks that are enrolled with Workspace ONE. After you deploy the app, configure and deploy a VPN profile to set up the GlobalProtect app for end users automatically. To deploy the GlobalProtect app for Android on managed Chromebooks using Workspace ONE, see Deploy the GlobalProtect App for Android on Managed Chromebooks Using Workspace ONE.

Platform	Deployment Options
Linux	After you download the GlobalProtect app for Linux from the Support Site, you can distribute and install the app: • **Using Linux app distribution tools**—Linux app distribution is typically managed using third-party tools (such as Chef and Puppet), or using a local repository for the Linux operating system (for example, Ubuntu repositories and RHELrepositories). See the documentation for your Linux operating system for more information. • **Manual installation**—If you make the software available to your end users, they can manually install the software using Linux tools such as **apt** or **dpkg**. For instructions on how to install the GlobalProtect app for Linux, see the GlobalProtect App User Guide.

As an alternative to deploying the GlobalProtect app software, you can configure the GlobalProtect portal to provide 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 the GlobalProtect app software. Refer to GlobalProtect Clientless VPN.

GlobalProtect App Minimum Hardware Requirements

The GlobalProtect app runs on a variety of operating systems. To determine the minimum GlobalProtect app version required for a specific operating system, refer to the Compatibility Matrix. The hardware requirements for each endpoint OS are detailed in the following sections:

- Minimum Hardware Requirements for GlobalProtect App on Windows
- Minimum Hardware Requirements for GlobalProtect App on macOS
- Minimum Hardware Requirements for GlobalProtect App on Linux

Minimum Hardware Requirements for GlobalProtect App on Windows

You can install the GlobalProtect app on Windows endpoints that meet the following hardware requirements:

Requirement	Specification
Processor	• Intel Pentium 4 or later with SSE2 instruction set support • AMD Opteron/Athlon 64 or later with SSE2 instruction set support • Dual core processor (minimum)
RAM	2GB minimum
Hard disk space	200 MB minimum (for log storage)

Minimum Hardware Requirements for GlobalProtect App on macOS

You can install the GlobalProtect app on macOS endpoints that meet the following hardware requirements:

Requirement	Specification
Processor	• Intel Pentium 4 or later with SSE2 instruction set support • AMD Opteron/Athlon 64 or later with SSE2 instruction set support • macOS based devices with Apple Silicon M1
RAM	512 MB minimum; 2 GB recommended
Hard disk space	200 MB minimum (for log storage)

Minimum Hardware Requirements for GlobalProtect App on Linux

You can install the GlobalProtect app on macOS endpoints that meet the following hardware requirements:

Support for Linux endpoints also requires a About GlobalProtect Licenses.

Requirement	Specification
Processor	x86 instruction set with 64-bit processor
RAM	256 MB minimum
Hard disk space	100 MB minimum

Download the GlobalProtect App Software Package for Hosting on the Portal

Palo Alto Networks does not provide a direct download link for the GlobalProtect app for end users. To successfully connect to your network, end users must be running an app version that is compatible with your environment. *After you decide what version of the app you are going to support for each OS, you can* Deploy the GlobalProtect App to End Users. *If you are an end user, please contact your IT Administrator for the latest supported GlobalProtect software.*

Before you can deploy the GlobalProtect app for your end users, you must upload the new app installation package to the firewall that is hosting your portal, and then activate the software for download to the apps connecting to the portal. This deployment method is available for all non-mobile app versions. To download the mobile version of the GlobalProtect app see the app store for your mobile device (for more information, see Download and Install the GlobalProtect Mobile App).

To download the latest app directly to the firewall, the firewall must have a service route that enables it to access the Palo Alto Networks Update Server (see Deploy the GlobalProtect App to End Users). If the firewall does not have internet access, you can download the app software package from the Palo Alto Networks Software Updates support site using an internet-connected computer, and then manually Host App Updates on the Portal.

To manually download the app software package:

STEP 1 | Log in to the Palo Alto Networks Customer Support Portal (https://support.paloaltonetworks.com/).

You must have a valid Palo Alto Networks Customer Support Portal account to log in to and download software from the Software Updates page.

STEP 2 | Select **Updates** > **Software Updates**.

STEP 3 | Select the GlobalProtect app version by operating system.

STEP 4 | Review the Release Notes for the app version, and then select the download link to proceed with the download.

STEP 5 | Deploy the GlobalProtect App to End Users.

See the Palo Alto Networks Compatibility Matrix for the operating systems on which you can install each release of the GlobalProtect app.

Host App Updates on the Portal

The simplest way to deploy the GlobalProtect app software is to download the new app installation package to the firewall that is hosting your portal, and then activate the software for download to the apps connecting to the portal. To do this automatically, the firewall must have a service route that enables it to access the Palo Alto Networks Update Server. If the firewall does not have internet access, you can Download the GlobalProtect App Software Package for Hosting on the Portal software package from the Palo Alto Networks Software Updates support site using an internet-connected computer, and then manually upload it to the firewall.

You define how the app software updates are deployed in the portal agent configurations—whether they occur automatically when the app connects to the portal, whether the user is prompted to upgrade the app, or whether the end user can manually check for and download a new app version. For details on creating an agent configuration, see Define the GlobalProtect Agent Configurations.

STEP 1 | On the firewall hosting the GlobalProtect portal, check for new app software images.

Select **Device** > **GlobalProtect Client** to view the list of available app software images.

- If the firewall has access to the Update Server, click **Check Now** for the latest updates. If the value in the **Action** column is **Download**, it indicates that a new version of the app is available.
- If the firewall does not have access to the Update Server, you must manually download the software image from the Palo Alto Networks Software Updates support site, as described in step 2.

STEP 2 | Download the app software image.

- If the firewall has access to the Update Server, locate the app version you want, and then click **Download**. When the download completes, the value in the **Action** column changes to **Activate**.
- If the firewall does not have access to the Update Server, Download the GlobalProtect App Software Package for Hosting on the Portal. After you download the software image, go back to the **Device** > **GlobalProtect Client** page of the firewall to **Upload** it.

STEP 3 | Activate the app software image so that end users can download it from the portal.

Only one version of the app software image can be activated at a time. If you activate a new version, but have some apps that require a previously activated version, you must activate the required version again to enable it for download.

- If the software image was automatically downloaded from the Update Server, click **Activate**.
- If you manually uploaded the software image to the firewall, click **Activate From File**, and then select the **GlobalProtect Client File** you uploaded from the drop-down. Click **OK** to activate the selected image. You may need to refresh the page before the version displays as **Currently Activated**.

Host App Updates on a Web Server

If a large number of your endpoints must install and/or update the GlobalProtect app software, consider hosting the GlobalProtect app software images on an external web server. This helps reduce the load on the firewall when users connect to and download the app.

STEP 1 | Download and activate the version of the GlobalProtect app that you plan to host on the web server to the firewall.

Follow the steps for downloading and activating the app software on the firewall, as described in Host App Updates on the Portal.

STEP 2 | Download the GlobalProtect app software image that you want to host on your web server.

Download the same image that you activated on the portal.

From a web browser, Download the GlobalProtect App Software Package for Hosting on the Portal.

STEP 3 | Publish the software image files to your web server.

STEP 4 | Redirect end users to the web server.

On the firewall hosting the portal, enter the following CLI commands in operational mode:

```
> set global-protect redirect on
```



```
> set global-protect redirect location <path>
```

where *<path>* is the path is the URL to the folder hosting the image (for example, **https://acme/GP**).

STEP 5 | Test the redirect.

1. From a web browser, go to the following URL:

   ```
   https://<portal address or name>
   ```

   For example, **https://gp.acme.com**.
2. On the portal login page, enter your user **Name** and **Password**, and then click **LOGIN**. After successful login, the portal should redirect you to the download.

Test the App Installation

Use the following procedure to test the GlobalProtect app installation.

STEP 1 | Create an agent configuration for testing the app installation.

When initially installing the GlobalProtect app software on the endpoint, the end user must be logged in to the system using an account that has administrative privileges. Subsequent app software updates do not require administrative privileges.

As a best practice, create an agent configuration that is limited to a small group of users, such as administrators in the IT department responsible for administering the firewall:

1. Select **Network** > **GlobalProtect** > **Portals**.
2. Select an existing portal configuration that you want to modify or **Add** a new one
3. On the **Agent** tab, select an existing configuration or **Add** a new one to deploy to the test users/group.
4. On the **User/User Group** tab, **Add** the **User/User Group** who will be testing the app.
5. On the **App** tab, set **Allow User to Upgrade GlobalProtect App** to **Allow with Prompt**. Click **OK** to save the configuration.
6. (Optional) On the **Agent** tab, select the agent configuration that you just created or modified, and then click **Move Up** so that it is higher on the list than the more generic configurations you have created.

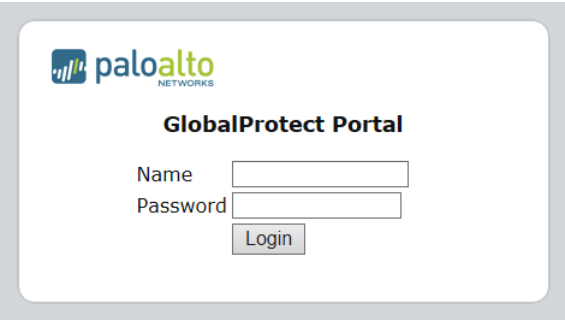
   When a GlobalProtect app connects, the portal compares the source information in the packet against the agent configurations you have defined. As with security rule evaluation, the portals looks for a match starting from the top of the list. When it finds a match, it delivers the corresponding configuration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

STEP 2 | Log in to the GlobalProtect portal.

1. Launch your web browser and go to the following URL:

   ```
   https://<portal address or name>
   ```

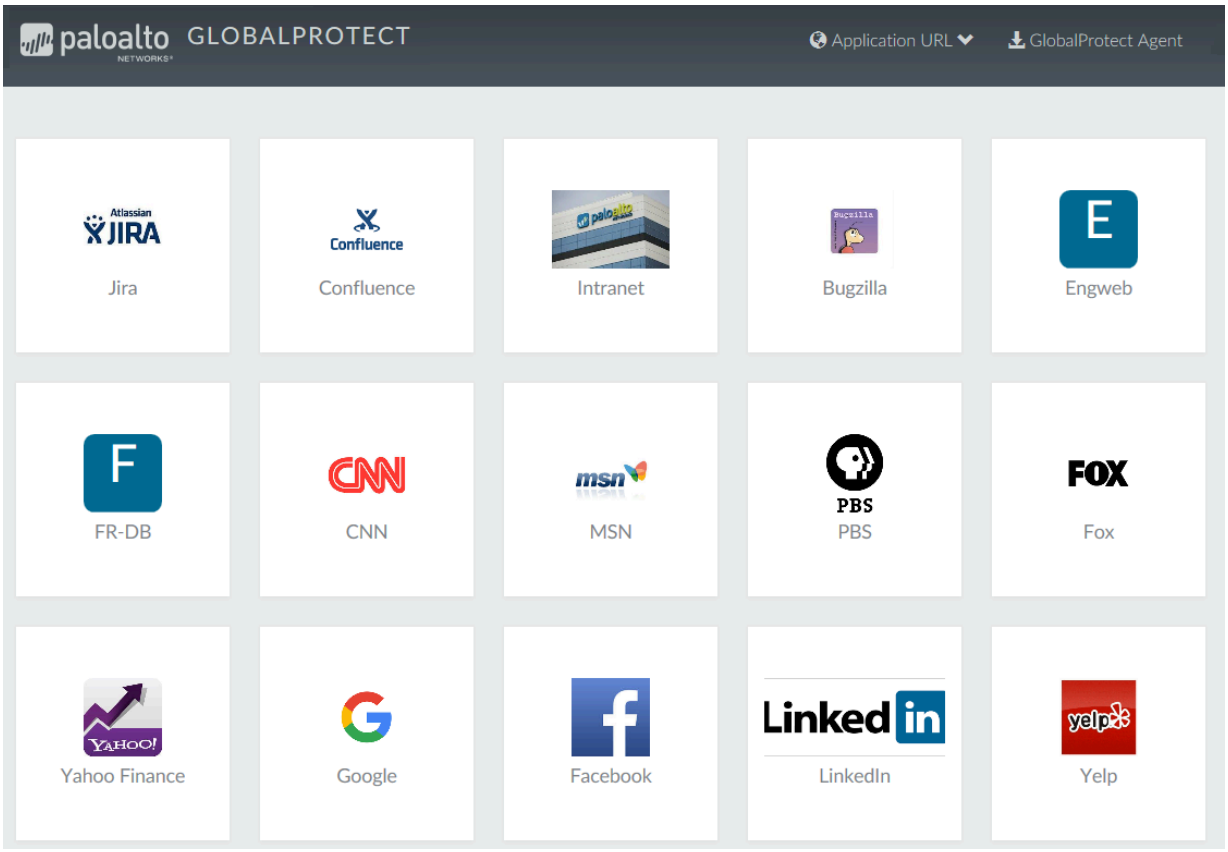
   For example, **`https://gp.acme.com`**.
2. On the portal login page, enter your user **Name** and **Password**, and then click **LOG IN**.



STEP 3 | Navigate to the app download page.

In most cases, the app download page appears immediately after you log in to the portal. Use this page to download the latest app software package.

If you have enabled GlobalProtect Clientless VPN access, the applications page opens after you log in to the portal (instead of the agent download page) when you log in to the portal. Select **GlobalProtect Agent** to open the download page.



STEP 4 | Download the app.

1. To begin the download, click the link that corresponds to the operating system running on your computer.

2. Open the software installation file.
3. When prompted to run or save the software, click **Run**.
4. When prompted, click **Run** to launch the GlobalProtect Setup Wizard.

When initially installing the GlobalProtect app software on the endpoint, the end user must be logged in to the system using an account that has administrative privileges. Subsequent app software updates do not require administrative privileges.

STEP 5 | Complete the GlobalProtect app setup.

1. From the GlobalProtect Setup Wizard, click **Next**.
2. Click **Next** to accept the default installation folder (C:\Program Files\Palo Alto Networks \GlobalProtect) and then click **Next** twice.

*Although you can **Browse** to select a different location in which to install the GlobalProtect app, the best practice is to install it in the default location. The default installation location is read-only for non-privileged users and therefore installing to this location protects against malicious access to the app.*

3. After the installation is complete, **Close** the wizard.

STEP 6 | Log in to GlobalProtect.

1. Launch the GlobalProtect app by clicking the system tray icon. The status panel opens.
2. Enter the FQDN or IP address of the portal, and then click **Connect**.
3. (Optional) By default, you are automatically connected to the **Best Available** gateway, based on the configuration that the administrator defines and the response times of the available gateways. To connect to a different gateway, select the gateway from the **Gateway** drop-down (for external gateways only).

   This option is only available if you enable manual gateway selection.

4. (Optional) Depending on the connection mode, click **Connect** to initiate the connection.
5. (Optional) If prompted, enter your **Username** and **Password**, and then click **Sign In**.

If authentication is successful, you are connected to your corporate network, and the status panel displays the **Connected** or **Connected - Internal** status. If you set up a GlobalProtect welcome page, it displays after you log in successfully.

Download and Install the GlobalProtect Mobile App

The GlobalProtect app provides a simple way to extend the enterprise security policies out to mobile endpoints. As with other remote endpoints running the GlobalProtect app, the mobile app provides secure access to your corporate network over an IPsec or SSL VPN tunnel. The app automatically connects to the gateway that is closest to the end user's current location. In addition, traffic to and from the endpoint is automatically subject to the same security policy enforcement as other hosts on your corporate network. The mobile app also collects information about the host configuration and can use this information for enhanced HIP-based security policy enforcement.

There are two primary methods for installing the GlobalProtect app: You can deploy the app from your third-party MDM and transparently push the app to your managed endpoints; or, you can install the app directly from the official store for your endpoint:

- iOS endpoints—App Store
- Android endpoints and Chromebooks—Google Play

  Starting with GlobalProtect app 5.0, the GlobalProtect app for Chrome OS is not supported; use the GlobalProtect app for Android instead.
- Windows 10 phones and Windows 10 UWP endpoints—Microsoft Store

This workflow describes how to install the GlobalProtect app directly on the mobile endpoint. For instructions on how to deploy the GlobalProtect app from Workspace ONE, see Deploy the GlobalProtect Mobile App Using Workspace ONE.

STEP 1 | Create an agent configuration for testing the app installation.

As a best practice, create an agent configuration that is limited to a small group of users, such as administrators in the IT department responsible for administering the firewall:

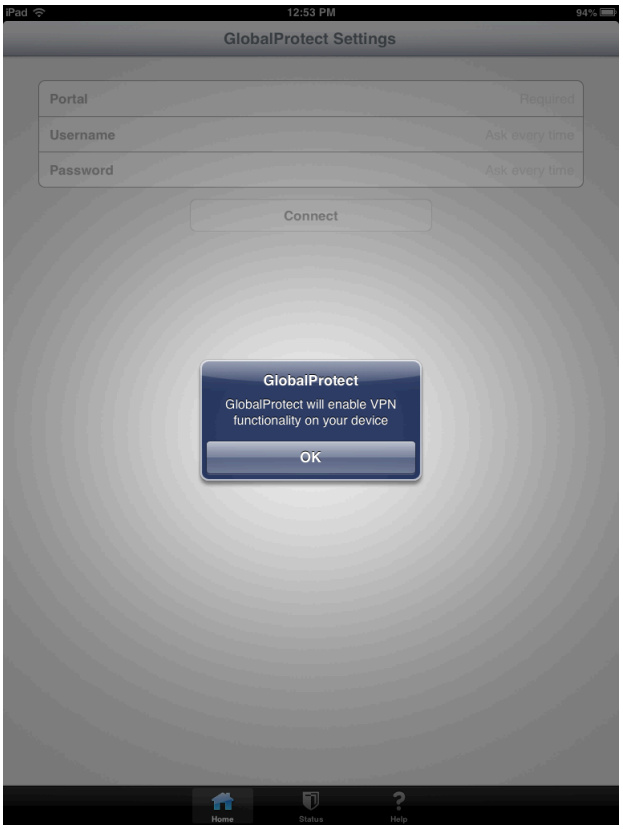
1. Select **Network** > **GlobalProtect** > **Portals**.
2. Select an existing portal configuration to modify or **Add** a new one.
3. On the **Agent** tab, either select an existing configuration or **Add** a new configuration to deploy to the test users/group.
4. On the **User/User Group** tab, **Add** the **User/User Group** who will be testing the app.
5. Select the **OS** for the app you are testing (**iOS**, **Android**, or **WindowsUWP**).
6. (Optional) Select the agent configuration that you just created/modified, and then click **Move Up** so that it is higher on the list than the more generic configurations you have created.
7. **Commit** the changes.

STEP 2 | From the endpoint, follow the prompts to download and install the app.

- On Android endpoints, search for the app on Google Play.
- On iOS endpoints, search for the app at the App Store.
- On Windows 10 UWP endpoints, search for the app at the Microsoft Store.

STEP 3 | Launch the app.

When successfully installed, the GlobalProtect app icon displays on the endpoint's Home screen. To launch the app, tap the icon. When prompted to enable GlobalProtect VPN functionality, tap **OK**.



STEP 4 | Connect to the portal.

1. When prompted, enter the **Portal** name or address, User **Name**, and **Password**. The portal name must be an FQDN and it should not include the https:// at the beginning.

2. Tap **Connect** and verify that the app successfully establishes a connection to GlobalProtect.

   If a third-party mobile endpoint management system is configured, the app prompts you to enroll.

View and Collect GlobalProtect App Logs

You have two options for collecting GlobalProtect™ app logs from the end users' endpoints:

- Collect logs—End users must manually collect the GlobalProtect app logs.
- Report an issue—End users report an issue directly to Cortex Data Lake to which the administrator can access when they experience unusual behavior such as poor network performance or a connection is not established with the portal and gateway.

> *In order for the GlobalProtect app to send troubleshooting logs, diagnostic logs, or both to Cortex Data Lake for further analysis, you must configure the GlobalProtect portal to enable the Configure the App Log Collection Settings on the GlobalProtect Portal. Additionally, you can Configure the App Log Collection Settings on the GlobalProtect Portal that can contain IP addresses or fully qualified domain names of the web servers/resources that you want to probe, and to determine issues such as latency or network performance on the end user's endpoint.*

Use the following steps to view or collect GlobalProtect logs:

STEP 1 | Launch the GlobalProtect app.

STEP 2 | From the status panel, open the settings dialog ( ).

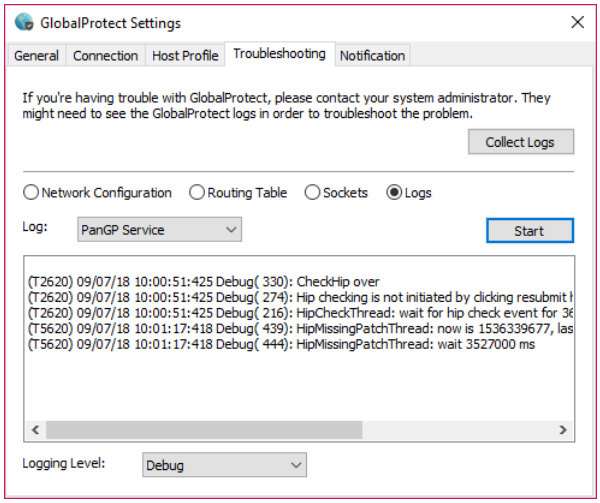
STEP 3 | Select **Settings**.

STEP 4 | From the GlobalProtect Settings panel, select **Troubleshooting**.

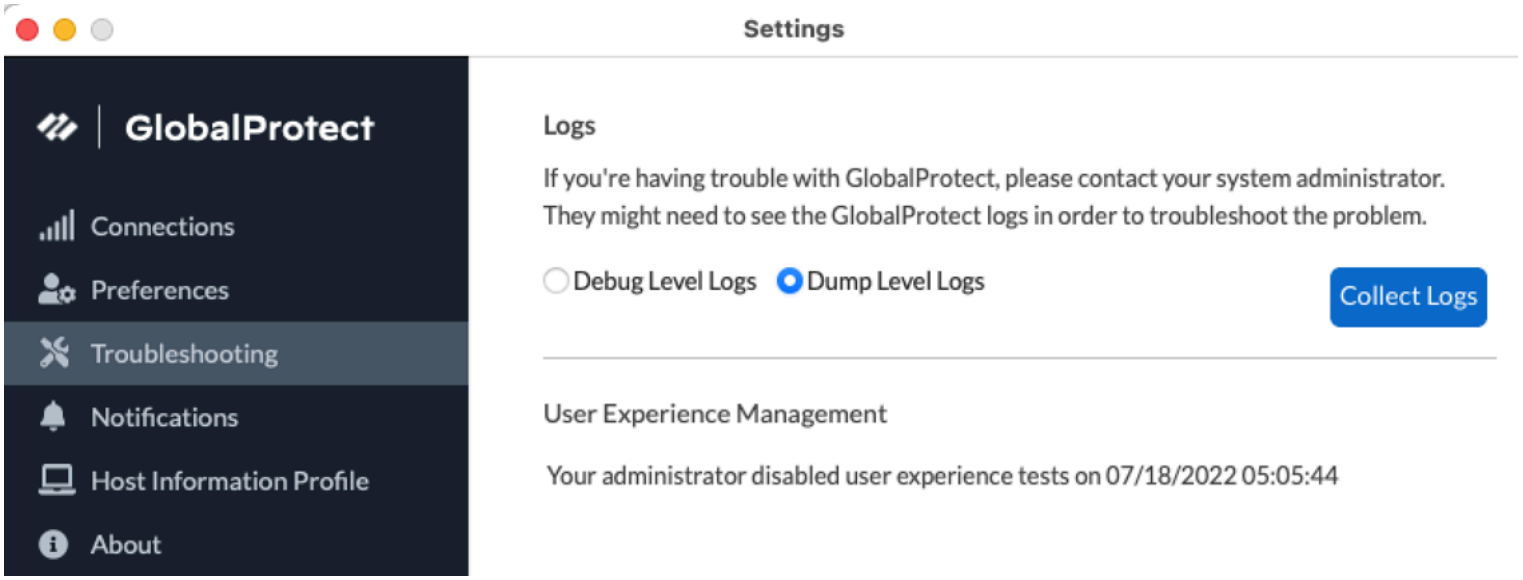
STEP 5 | Select either **Debug** or **Dump** from the **Logging Level** drop-down.

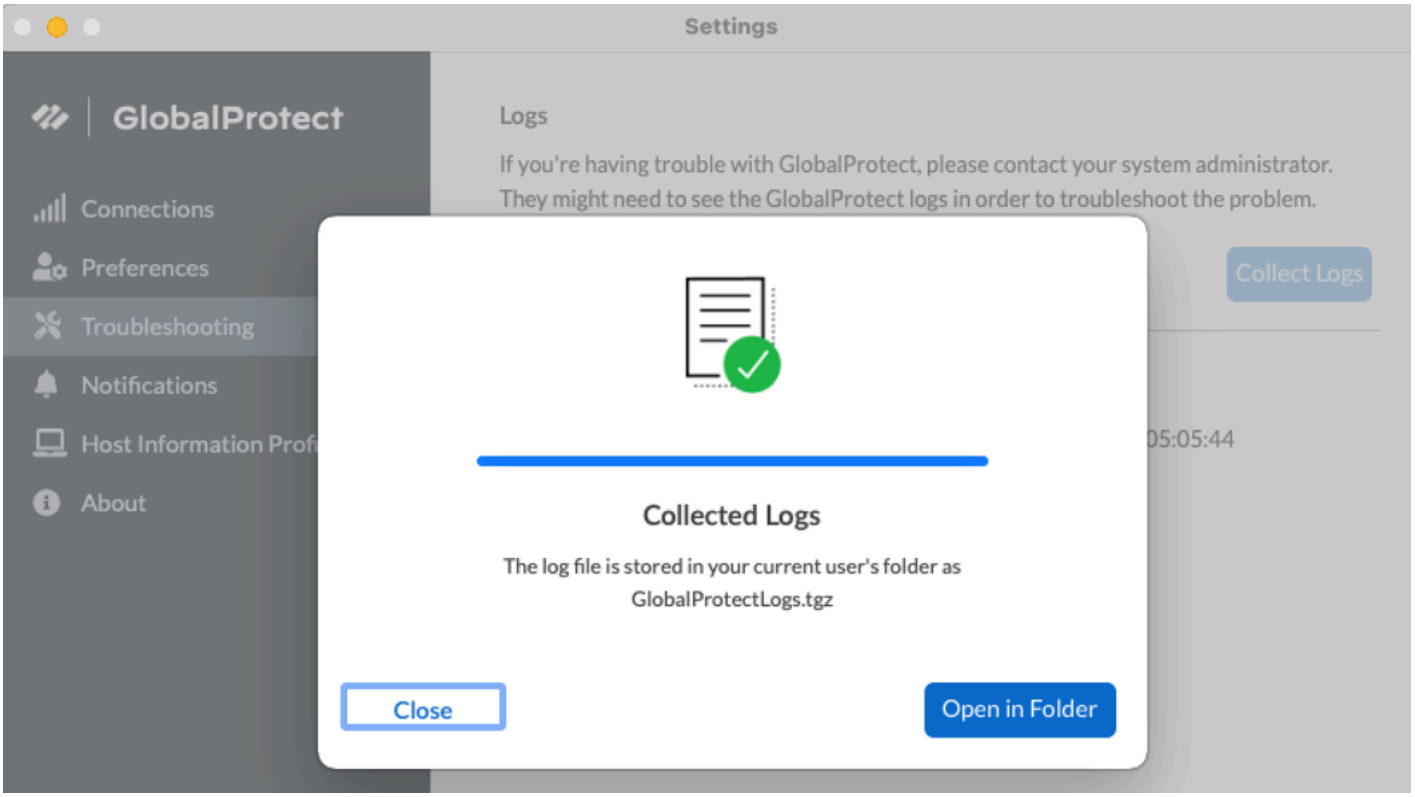
STEP 6 | (Optional—Windows only) View your GlobalProtect logs:

1. Select **Logs**.
2. Choose a **Log** type.
3. **Start** viewing logs.



STEP 7 | (Optional) **Collect Logs** to send to your GlobalProtect administrator for troubleshooting.





Deploy App Settings Transparently

As an alternative to deploying app settings from the portal configuration, you can define them directly from the following endpoints:

- Windows—Registry or Windows Installer (Msiexec)
- macOS—global macOS plist
- Linux—pre-deployment configuration file (`pangps.xml`)

The benefit of this alternative is that you can enable deployment of GlobalProtect app settings to endpoints prior to their first connection to the GlobalProtect portal.

Some settings do not have a corresponding portal configuration setting on the web interface and must be configured using the Windows Registry, Msiexec, or macOS plist. These settings are listed in the Customizable App Settings as "Not in portal."

Settings defined in the portal configuration always override settings defined in the Windows Registry, macOS plist, or pre-deployment configuration file (`pangps.xml`) for Linux. If you define settings in the registry, plist, or `pangps.xml`, but the portal configuration specifies different settings, the settings that the app receives from the portal overrides the settings defined on the endpoint. This override also applies to login-related settings, such as whether to connect on-demand, whether to use single sign-on (SSO), and whether the app can connect if the portal certificate is invalid. Therefore, you should avoid conflicting settings. In addition, the portal configuration is cached on the endpoint, and that cached configuration is used anytime the GlobalProtect app restarts or the endpoint reboots.

The following sections describe what customizable app settings are available and how to deploy these settings transparently to Windows, macOS, and Linux endpoints:

- Customizable App Settings
- Deploy App Settings to Windows Endpoints
- Deploy App Settings to macOS Endpoints
- Deploy App Settings to Linux Endpoints

In addition to using the Windows Registry, macOS plist, or Linux pre-deployment configuration to deploy GlobalProtect app settings, you can enable the GlobalProtect app to collect specific Windows Registry or macOS plist information from the endpoints, including data on applications installed on the endpoints, processes running on the endpoints, and attributes or properties of those applications and processes. You can then monitor the data and add it to a security rule to use as matching criteria. Endpoint traffic that matches the registry settings you define can be enforced according to the security rule. Additionally, you can set up custom checks to Collect Application and Process Data From Endpoints.

Customizable App Settings

In addition to pre-deploying the portal address, you can also define the app settings. To Deploy App Settings to Windows Endpoints you define keys in the Windows Registry (path `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect`

\Settings\ unless otherwise stated). To Deploy App Settings to macOS Endpoints you define entries in the Settings dictionary of the macOS plist (/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist). To Deploy App Settings to Linux Endpoints you define entries under <Settings> of the /opt/paloaltonetworks/globalprotect/pangps.xml pre-deployment configuration file. On Windows endpoints only, you can also use the Windows Installer to Deploy App Settings from Msiexec.

The following topics describe each customizable app setting. Settings defined in the GlobalProtect portal agent configuration take precedence over settings defined in the Windows Registry or the macOS plist.

Some settings do not have a corresponding portal configuration setting on the web interface and must be configured using the Windows Registry or Msiexec. These include, but are not limited to, settings such as the following: `can-prompt-user-credential`, `wrap-cp-guid`, and `filter-non-gpcp`. They are listed in the following options as "Not in portal."

- App Display Options
- User Behavior Options
- App Behavior Options
- Script Deployment Options

App Display Options

The following table lists the options that you can configure in the Windows Registry or macOS plist to customize the display of the GlobalProtect app.

Table 3: Table: Customizable App Settings

Portal Agent Configuration	Windows Registry/ macOS Plist	Msiexec Parameter	Default
Enable Advanced View	`enable-advanced-view yes | no`	`ENABLEADVANCEDVIEW="yes | no"`	yes
Display GlobalProtect Icon	`show-agent-icon yes | no`	`SHOWAGENTICON="yes | no"`	yes
Enable Rediscover Network Option	`rediscover-network yes | no`	`REDISCOVERNETWORK="yes | no"`	yes
Enable Resubmit Host Profile Option	`resubmit-host-info yes | no`	n/a	yes
Show System Tray Notifications	`show-system-tray-notifications yes | no`	`SHOWSYSTEMTRAYNOTIFICATIONS="yes | no"`	yes

User Behavior Options

The following table lists the options that you can configure in the Windows registry and macOS plist to customize how the user interacts with the GlobalProtect app.

Some settings do not have a corresponding portal configuration setting on the web interface and must be configured using the Windows Registry, Msiexec, or macOS plist. These settings are listed in the table as "Not in portal." They include, but are not limited to, settings such as the following: `ShowPrelogonButton` *and* `can-save-password`.

Table 4: Table: Customizable User Behavior Options

Portal Agent Configuration	Windows Registry/macOS Plist	Msiexec Parameter	Default
Allow User to Change Portal Address	**`can-change-portal yes | no`**	**`CANCHANGEPORTAL="yes | no"`**	**yes**
Allow User to Dismiss Welcome Page	**`enable-hide-welcome-page yes | no`**	**`ENABLEHIDEWELCOMEPAGE= "yes | no"`**	**yes**
Allow User to Continue with Invalid Portal Server Certificate	**`can-continue-if-portal-cert-invalid yes | no`**	**`CANCONTINUEIFPORTALCERTINVALID= "yes | no"`**	**yes**
Allow User to Disable GlobalProtect App	**`disable-allowed yes | no`**	**`DISABLEALLOWED="yes | no"`**	**no**
Save User Credentials Specify a 0 to prevent GlobalProtect from saving credentials, a 1 to save both username and password, or a 2 to save the username only.	**`save-user-credentials 0 | 1 | 2`**	n/a	n/a
Not in portal The **Allow user to save password** setting is deprecated	**`can-save-password yes | no`**	**`CANSAVEPASSWORD="yes | no"`**	**yes**

Portal Agent Configuration	Windows Registry/macOS Plist	Msiexec Parameter	Default
in the web interface in PAN-OS 7.1 and later releases but is configurable from the Windows registry and macOS plist. Any value specified in the **Save User Credentials** field overwrites a value specified here.			
Windows only/Not in portal This setting enables the GlobalProtect credential provider to display the **Start GlobalProtect Connection** button, which allows users to initiate the GlobalProtect pre-logon connection manually.	**`ShowPrelogonButton yes | no`**	n/a	**`no`**
Windows 10 only/ Not in portal This setting is used in conjunction with GlobalProtect SSO and enables the GlobalProtect credential provider to be set as the default sign-in option at the next Windows login and for subsequent logins. See Deploy GlobalProtect Credential Provider Settings in the Windows Registry for details.	**`MakeGPCPDefault yes | no`**	**`MAKEGPCPDEFAULT="yes | no"`**	n/a

Portal Agent Configuration	Windows Registry/macOS Plist	Msiexec Parameter	Default
Windows only/ Not in portal This setting is used in conjunction with GlobalProtect SSO and sets the number of seconds for users to wait to log in to Windows before establishing a tunnel connection. See Deploy GlobalProtect Credential Provider Settings in the Windows Registryfor details.	**LogonWaitTime <5-30 seconds>**	n/a	n/a
Windows only/ Not in portal This setting is used in conjunction with GlobalProtect SSO and sets the number of seconds to delay users from logging in to Windows after establishing a tunnel connection. See Deploy GlobalProtect Credential Provider Settings in the Windows Registryfor details.	**LogonPostWaitTime <3-10 seconds>**	n/a	n/a

App Behavior Options

The following table lists the options that you can configure in the Windows Registry and macOS plist to customize the behavior of the GlobalProtect app.

Some settings do not have a corresponding portal configuration setting on the web interface and must be configured using the Windows Registry, Msiexec, or macOS plist. These settings are listed in the table as "Not in portal." They include, but are not limited to, settings such as the following: `portal <IPaddress>`, `prelogon 1`, *and* `can-prompt-user-credential`.

Table 5: Table: Customizable App Behavior Options

Portal Agent Configuration	Windows Registry/macOS Plist	Msiexec Parameter	Default
Connect Method	**connect-method on-demand | pre-logon | user-logon**	**CONNECTMETHOD="on-demand | pre-logon | user-logon"**	**user-logon**
Conditional Connect Method Based on Network Type	**conditional-connect yes | no**	n/a	**no**
GlobalProtect App Config Refresh Interval (hours)	**refresh-config-interval** <**hours**>	**REFRESHCONFIGINTERVAL= "<hours>"**	**24**
Send HIP Report Immediately if Windows Security Center (WSC) State Changes (Windows Only)	**wsc-autodetect yes | no**	n/a	**no**
Detect Proxy for Each Connection (Windows Only)	**proxy-multiple-autodetect yes | no**	n/a	**no**
Clear Single Sign-On Credentials on Logout (Windows Only)	**logout-remove-sso yes | no**	**LOGOUTREMOVESSO="yes | no"**	**yes**
Disable Single Sign-On on local machines This setting allows you to disable the SSO feature even if it is configured on the portal. It overwrites the portal configuration when you manually add the key to the Windows registry	For Windows endpoints, you must manually add this setting to the Windows registry: **Windows Path:** **HKEY_LOCAL_MACHINE \SOFTWARE\Palo Alto Networks \GlobalProtect \Settings** **Key Name/Value:** **force-sso-disable yes | no**	This setting is not supported in msiexec.	n/a

Portal Agent Configuration	Windows Registry/macOS Plist	Msiexec Parameter	Default
or macOS plist and set the value as **Yes**.	For macOS endpoints, you must manually add this setting to the macOS plist: **macOS Path:** **`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`** Add the setting under **`Palo Alto Networks > GlobalProtect > Settings`** **Key Name/Value:** **`force-sso-disable yes | no`**		
Use Default Authentication on Kerberos Authentication Failure (Windows Only)	**`krb-auth-fail-fallback yes | no`**	**`KRBAUTHFAILFALLBACK= ”yes | no”`**	**`no`**
Use Default Browser for SAML Authentication	(macOS plist) **`default-browser yes | no`**	**`DEFAULTBROWSER= “yes | no”`**	**`no`**
Custom Password Expiration Message (LDAP Authentication Only)	(Deprecated) **`PasswordExpiryMessage <message>`**	n/a	**`Password expires in <number> days`**
Portal Connection Timeout (sec)	**`portal-timeout <portaltimeout>`**	n/a	**`5`**
TCP Connection Timeout (sec)	**`connect-timeout <connect-timeout>`**	n/a	**`5`**
TCP Receive Timeout (sec)	**`receive-timeout <receive-timeout>`**	n/a	**`30`**

Portal Agent Configuration	Windows Registry/macOS Plist	Msiexec Parameter	Default
Client Certificate Store Lookup	**certificate-store-lookup user | machine | user and machine | invalid**	**CERTIFICATESTORELOOKUP="user | machine | user and machine | invalid"**	**user and machine**
SCEP Certificate Renewal Period (days)	**scep-certificate-renewal-period <renewalPeriod>**	n/a	**7**
Maximum Internal Gateway Connection Attempts	**max-internal-gateway-connection-attempts <maxValue>**	**MIGCA="<maxValue>"**	**0**
Extended Key Usage OID for Client Certificate	**ext-key-usage-oid-for-client-cert <oidValue>**	**EXTCERTOID="<oidValue>"**	n/a
User Switch Tunnel Rename Timeout (sec)	**user-switch-tunnel-rename-timeout <renameTimeout>**	n/a	**0**
Use Single Sign-On (Windows Only)	**use-sso yes | no**	**USESSO="yes | no"**	**yes**
Use Single Sign-On for Smart Card (Windows Only)	**use-sso-pin yes | no**	**USESSOPIN="yes | no"**	**no**
Inbound Authentication Message	**authentication-message**	n/a	n/a
Allow Overriding Username from Client Certificate	**override-cc-username yes | no**	n/a	**no**
Not in portal This setting specifies the default portal IP address (or hostname).	**portal <IPaddress>**	**PORTAL="<IPaddress>"**	n/a

Portal Agent Configuration	Windows Registry/macOS Plist	Msiexec Parameter	Default
Not in portal This setting enables GlobalProtect to initiate a VPN tunnel before a user logs in to the device and connects to the GlobalProtect portal.	`prelogon 1`	`PRELOGON="1"`	`1`
Not in portal This setting is used in conjunction with single sign-on (SSO) and indicates whether or not to prompt the user for credentials if SSO fails.	(Windows) `can-prompt-user-credential yes | no`	`CANPROMPTUSERCREDENTIAL=”yes | no”`	`yes`
Windows only/Not in portal This setting filters the third-party credential provider's tile from the Windows login page so that only the native Windows tile is displayed.*	`wrap-cp-guid {third party credential provider guid}`	`WRAPCPGUID=”{guid_value}” FILTERNONGPCP=”yes | no”`	`no” ]`
Windows only/Not in portal This setting is an additional option for the setting wrap-cp-guid, and allows the third-party credential provider tile to be displayed on the	`filter-non-gpcp no`	n/a	n/a

Portal Agent Configuration	Windows Registry/macOS Plist	Msiexec Parameter	Default
Windows login page, in addition to the native Windows logon tile.*			
Windows only/Not in portal This setting allows you to assign static IP addresses to Windows endpoints.	**reserved-ipv4** <reserved-ipv4> **reserved-ipv6** <reserved-ipv6>	**RESERVEDIPV4=”**<reserved-ipv4>**”** **RESERVEDIPV6=”**<reserved-ipv6>**”**	n/a
(Windows Only) This setting allows you to set a valid default gateway on GlobalProtect virtual adapter when you configure GlobalProtect app in Full-Tunnel mode.	**fake-default-gateway yes | no**	**fake-default-gateway yes | no**	n/a
(Windows Only) This setting allows you to collect HIP data on Windows endpoints.	**collect-hip-data yes | no**	**COLLECTHIPDATA= ”yes | no”**	n/a
(Windows Only) This setting allows you to save gateway passwords on Windows endpoints.	**save-gateway-password yes | no**	**SAVEGATEWAYPASSWORD= ”yes | no”**	n/a
Windows Only/ Not in portal This setting allows you to press the **Enter**	Windows Registry Path: **HKEY_CURRENT_USER \SOFTWARE\Palo Alto Networks**	**TRANSLATEENTERKEY= "yes | no"**	**yes**

Portal Agent Configuration	Windows Registry/macOS Plist	Msiexec Parameter	Default
key to log in to GlobalProtect from the embedded browser on Windows endpoints during SAML authentication. In some cases, enabling this setting will prevent the **Enter** key press from being accepted during sign on. If this occurs, change the setting to **no**.	**\GlobalProtect\Settings** **Key Name/Value** **translate-enter-key** **yes | no**		

For detailed steps to enable these settings using the Windows registry or Windows Installer (Msiexec), see SSO Wrapping for Third-Party Credential Providers on Windows Endpoints.

Script Deployment Options

The following table displays options that enable GlobalProtect to initiate scripts before and after establishing a connection and before disconnecting. Because these options are not available in the portal, you must define the values for the relevant key—either pre-vpn-connect, post-vpn-connect, or pre-vpn-disconnect—from the Windows registry or macOS plist. For detailed steps to deploy scripts, see Deploy Scripts Using the Windows Registry, Deploy Scripts Using Msiexec, or Deploy Scripts Using the macOS Plist.

If you are allowing end users to establish the VPN connection to the corporate network before logging in to the Windows endpoint by using Connect Before Logon, you must run VPN connect scripts with the ***context admin*** *value specified the Windows registry. You cannot specify the default* ***context user*** *value because there is no user prior to Windows logon.*

Table: Customizable Script Deployment Options

Portal Agent Configuration	Windows Registry/macOS Plist	Msiexec Parameter	Default
Execute the script specified in the command setting	**command** <**parameter1**> <**parameter2**> **[...]**	**PREVPNCONNECTCOMMAND=** **”**<**parameter1**> <**parameter2**> **[...]”**	**n/a**

Portal Agent Configuration	Windows Registry/macOS Plist	Msiexec Parameter	Default
(including any parameters passed to the script). *Environmental variables are supported.* *Specify the full path in commands.*	Windows example: **command %userprofile%\vpn_script.bat c:test_user** macOS example: **command $HOME/vpn_script.sh /Users/test_user test_user**	**POSTVPNCONNECTCOMMAND=”<parameter1> <parameter2> [...]”** **PREVPNDISCONNECTCOMMAND=”<parameter1> <parameter2> [...]”**	
(Optional) Specify the privileges under which the command(s) can run (default is user: if you do not specify the context, the command runs as the current active user).	**context admin | user**	**PREVPNCONNECTCONTEXT=”admin | user”** **POSTVPNCONNECTCONTEXT=”admin | user”** **PREVPNDISCONNECTCONTEXT=”admin | user”**	**user**
(Optional) Specify the number of seconds the GlobalProtect app waits for the command to execute (range is 0-120). If the command does not complete before the timeout, the app proceeds to establish a connection or disconnect. A value of 0 (the default) means the app does not wait to execute the command. *Not supported for post-vpn-connect.*	**timeout <value>** Example: **timeout 60**	**PREVPNCONNECTTIMEOUT=”<value>”** **PREVPNDISCONNECTTIMEOUT=”<value>”**	**0**
(Optional) Specify the full path of a file used in a command.	**file <path_file>**	**PREVPNCONNECTFILE=”<path_file>”**	**n/a**

Portal Agent Configuration	Windows Registry/macOS Plist	Msiexec Parameter	Default
The GlobalProtect app verifies the integrity of the file by checking it against the value specified in the checksum key. *Environmental variables are supported.*		**POSTVPNCONNECTFILE= ”<path_file>”** **PREVPNDISCONNECTFILE= ”<path_file>”**	
(Optional) Specify the sha256 checksum of the file referred to in the file key. If the checksum is specified, the GlobalProtect app executes the command(s) only if the checksum generated by the GlobalProtect app matches the checksum value specified here.	**checksum <value>**	**PREVPNCONNECTCHECKSUM= ”<value>”** **POSTVPNCONNECTCHECKSUM= ”<value>”** **PREVPNDISCONNECTCHECKSUM =”<value>”**	n/a
(Optional) Specify an error message to inform the user that either the command(s) cannot be executed or the command(s) exited with a non-zero return code. *The message must be 1,024 or fewer ANSI characters.*	**error-msg <message>** Example: **error-msg Failed executing pre-vpn-connect action!**	**PREVPNCONNECTERRORMSG= ”<message>”** **POSTVPNCONNECTERRORMSG= ”<message>”** **PREVPNDISCONNECTERRORMSG =”<message>”**	n/a

Configure Conditional Connect Method Based on Network Type

Where Can I Use This?	What Do I Need?
• Prisma Access • GlobalProtect Subscription	• Prisma Access Mobile Users license (for use with Prisma Access) • GlobalProtect app version 6.2 or later for Windows and macOS

Configure Conditional Connect to enable the GlobalProtect app to change the connect method dynamically based on whether the internal host detection determines that the user is on the internal network or working from a remote location. You Deploy App Settings Transparently from the macOS plist or the Windows Registry. Before enabling Conditional Connect, make sure that you have:

- ☐ Enabled internal host detection
- ☐ Configured the endpoints to use the on-demand connect method

- Deploy Conditional Connect to Windows endpoints.
  1. In the Windows Registry, go to: **\HKEY_LOCAL_MACHINE > SOFTWARE> Palo Alto Networks > GlobalProtect > Settings** .
  2. Set the key as **conditional-connect** and the value to **Yes**.

- Deploy Conditional Connect to macOS endpoints.
  1. In the plist file (/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist), go to **/Palo Alto Networks/GlobalProtect/Settings**.
  2. Set **conditional-connect** to **Yes**.

Deploy App Settings to Windows Endpoints

Use the Windows Registry or Windows Installer (Msiexec) to transparently deploy the GlobalProtect app and settings to Windows endpoints.

- Deploy App Settings in the Windows Registry
- Deploy App Settings from Msiexec
- Deploy Scripts Using the Windows Registry
- Deploy Scripts Using Msiexec
- Deploy Connect Before Logon Settings in the Windows Registry
- Deploy GlobalProtect Credential Provider Settings in the Windows Registry
- SSO Wrapping for Third-Party Credential Providers on Windows Endpoints
- Enable SSO Wrapping for Third-Party Credentials with the Windows Registry
- Enable SSO Wrapping for Third-Party Credentials with the Windows Installer

Deploy App Settings in the Windows Registry

You can enable deployment of GlobalProtect app settings to Windows endpoints prior to their first connection to the GlobalProtect portal by using the Windows Registry. Use the options described in the following table to use the Windows Registry to customize app settings for Windows endpoints.

In addition to using the Windows Registry to deploy GlobalProtect app settings, you can enable the GlobalProtect app to collect specific Windows Registry information from Windows endpoints. You can then monitor the data and add it to a security rule to use as matching criteria. Endpoint traffic that matches registry settings you define can be enforced according to the security rule. Additionally, you can set up custom checks to Collect Application and Process Data From Endpoints.

STEP 1 | Locate the GlobalProtect app customization settings in the Windows Registry.

Open the Windows Registry (enter **regedit** on the command prompt) and go to:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings
\
```

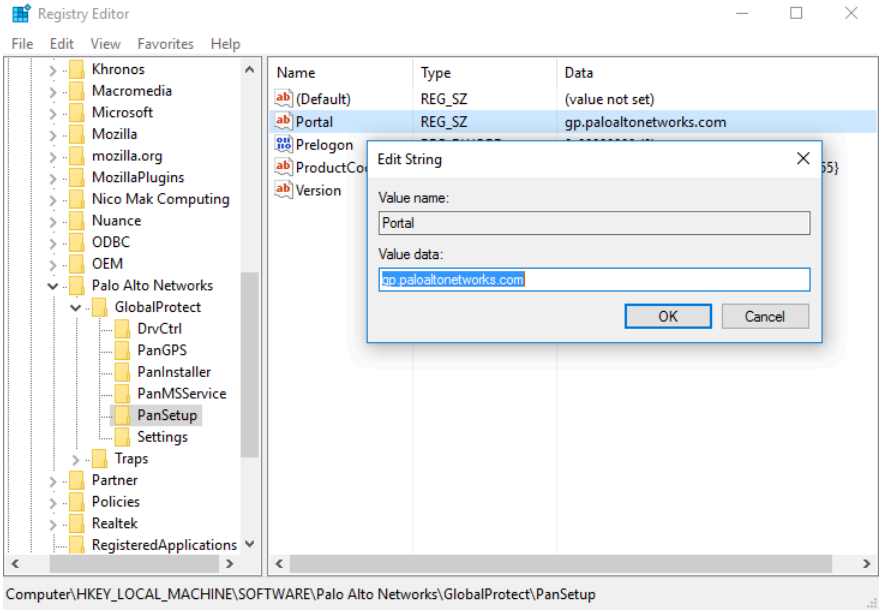

STEP 2 | Set the portal name.

If you do not want the end user to manually enter the portal address even for the first connection, you can pre-deploy the portal address through the Windows Registry.

If you want to define all other app settings, you can define keys in the Windows Registry (`HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\`

1. In the Window Registry, go to:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup`
2. Right-click **Portal** and then select **Modify**.
3. Enter the portal name in the **Value data** field, and then click **OK**.



STEP 3 | Deploy various settings to the Windows endpoint, including the connect method for the GlobalProtect app and SSO.

View Customizable App Settings for a full list of the commands and values you can set up using the Windows Registry.

You have the option to Deploy Connect Before Logon Settings in the Windows Registry to the Windows endpoints prior to enabling end users to log in to the VPN before logging into the endpoint.

You have the option to Deploy GlobalProtect Credential Provider Settings in the Windows Registry to the Windows endpoints to delay the GlobalProtect credential provider Windows sign-in request or enforce the GlobalProtect credential provider as the default sign-in option.

STEP 4 | Enable the GlobalProtect app to wrap third-party credentials on the Windows endpoint, allowing for SSO when using a third-party credential provider.

Enable SSO Wrapping for Third-Party Credentials with the Windows Registry.

Deploy App Settings from Msiexec

On Windows endpoints, you have the option of automatically deploying the GlobalProtect app and the app settings from the Windows Installer (Msiexec) by using the following syntax:

```
msiexec.exe /i GlobalProtect.msi <SETTING>="<value>"
```

Msiexec is an executable program that installs or configures a product from the command line. On endpoints running Microsoft Windows XP or a later OS, the maximum string length that you can use at the command prompt is 8,191 characters.

Msiexec Example	Description
`msiexec.exe /i GlobalProtect.msi /quiet PORTAL="portal.acme.com"`	Install GlobalProtect in quiet mode (no user interaction) and configure the portal address.
`msiexec.exe /i GlobalProtect.msi CANCONTINUEIFPORTALCERTINVALID= "no"`	Install GlobalProtect with the option to prevent users from connecting to the portal if the certificate is not valid.

For a complete list of settings and the corresponding default values, see Customizable App Settings.

You can also Enable SSO Wrapping for Third-Party Credentials with the Windows Installer.

Deploy Scripts Using the Windows Registry

You can enable deployment of custom scripts to Windows endpoints using the Windows Registry.

You can configure the GlobalProtect app to initiate and run a script for any or all of the following events: before and after establishing the tunnel, and before disconnecting the tunnel. To run the script at a particular event, reference the batch script from a command registry entry for that event.

Depending on the configuration settings, the GlobalProtect app can run a script before and after the app establishes a connection to the gateway, and before the app disconnects. Use the following workflow to use the Windows Registry to customize app settings for Windows endpoints.

The registry settings that enable you to deploy scripts are supported on endpoints running GlobalProtect App 2.3 and later releases.

STEP 1 | Open the Windows registry, and locate the GlobalProtect app customization settings.

Open the Windows registry (enter **regedit** in the command prompt) and go to one of the following key locations, depending on when you want to execute scripts (pre/post connect or pre disconnect):

`HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\pre-vpn-connect`

`HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\post-vpn-connect`

`HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\pre-vpn-disconnect`

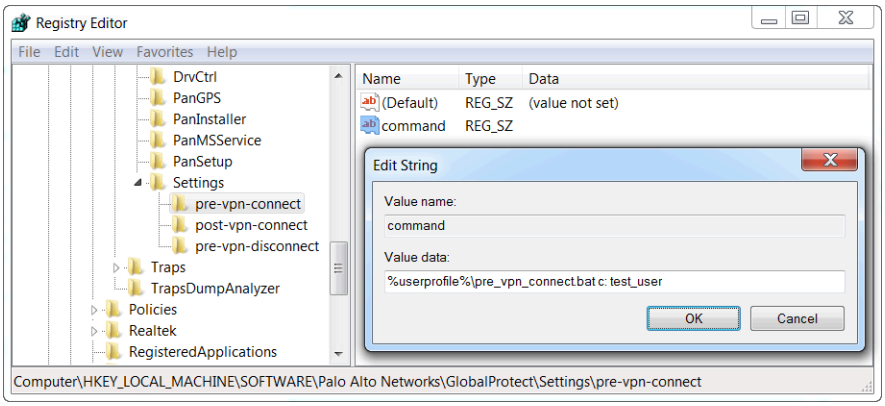
*If the key does not exist within the **Settings** key, create it by right-clicking **Settings** and selecting **New** > **Key**).*

STEP 2 | Enable the GlobalProtect app to run scripts by creating a new String Value named `command`.

The batch file specified here should contain the specific script (including any parameters passed to the script) that you want run on the device.

1. If the `command` string does not already exist, create it by right-clicking the `pre-vpn-connect`, `post-vpn-connect`, or `pre-vpn-disconnect` key, selecting **New** > **String Value**, and naming it **command**).
2. Right click `command`, and then select **Modify**.
3. Enter the commands or script that the GlobalProtect app should run. For example:

```
%userprofile%\pre_vpn_connect.bat c:test_user
```



STEP 3 | (Optional) Add additional registry entries as needed for each command.

Create or modify registry strings and their corresponding values, including `context`, `timeout`, `file`, `checksum`, or `error-msg`. For additional information, see Customizable App Settings.

Deploy Scripts Using Msiexec

On Windows endpoints, you can use the Windows Installer (Msiexec) to deploy the GlobalProtect app, app settings, and scripts that the app will run automatically (see Customizable App Settings). To do so, use the following syntax:

```
msiexec.exe /i GlobalProtect.msi <SETTING>="<value>"
```

Msiexec is an executable program that installs or configures a product from a command line. On systems running Microsoft Windows XP or later releases, the maximum string length that you can use at the command prompt is 8,191 characters.

This limitation applies to the command line, individual environment variables (such as the USERPROFILE variable) that are inherited by other processes, and all environment variable expansions. If you run batch files from the command line, this limitation also applies to batch file processing.

For example, to deploy scripts that run at specific connect or disconnect events, you can use syntax similar to the following examples:

Example: Use Msiexec to Deploy Scripts that Run Before a Connect Event

For a script that you can copy and paste, go here.

```
msiexec.exe /i GlobalProtect.msi
PREVPNCONNECTCOMMAND="%userprofile%\pre_vpn_connect.bat c:
 test_user"
PREVPNCONNECTCONTEXT="user"
PREVPNCONNECTTIMEOUT="60"
PREVPNCONNECTFILE="C:\Users\test_user\pre_vpn_connect.bat"
PREVPNCONNECTCHECKSUM="a48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b011
8647ccf599"
PREVPNCONNECTERRORMSG="Failed executing pre-vpn-connect action."
```

For a complete list of settings and the corresponding default values, see Customizable App Settings.

Example: Use Msiexec to Deploy Scripts that Run at Pre-Connect, Post-Connect, and Pre-Disconnect Events

For a script that you can copy and paste, go here.

```
msiexec.exe /i GlobalProtect.msi
PREVPNCONNECTCOMMAND="%userprofile%\pre_vpn_connect.bat c:
 test_user"
PREVPNCONNECTCONTEXT="user"
PREVPNCONNECTTIMEOUT="60"
PREVPNCONNECTFILE="C:\Users\test_user\pre_vpn_connect.bat"
PREVPNCONNECTCHECKSUM="a48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b011
```



```
8647ccf599"
PREVPNCONNECTERRORMSG="Failed executing pre-vpn-connect action."
POSTVPNCONNECTCOMMAND="c:\users\test_user\post_vpn_connect.bat c:
 test_user"
POSTVPNCONNECTCONTEXT="admin"
POSTVPNCONNECTFILE="%userprofile%\post_vpn_connect.bat"
POSTVPNCONNECTCHECKSUM="b48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b011
8647ccf598"
POSTVPNCONNECTERRORMSG="Failed executing post-vpn-connect action."
PREVPNDISCONNECTCOMMAND="%userprofile%\pre_vpn_disconnect.bat c:
 test_user"
PREVPNDISCONNECTCONTEXT="admin"
PREVPNDISCONNECTTIMEOUT="0"
PREVPNDISCONNECTFILE="C:\Users\test_user\pre_vpn_disconnect.bat"
PREVPNDISCONNECTCHECKSUM="c48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b0
118647ccf597"
PREVPNDISCONNECTERRORMSG="Failed executing pre-vpn-disconnect
 action."
```

For a complete list of settings and the corresponding default values, see Customizable App Settings.

Deploy Connect Before Logon Settings in the Windows Registry

You can deploy Connect Before Logon settings to Windows 10 endpoints prior to enabling end users to log in to the VPN before logging into the endpoint by using the Windows Registry. GlobalProtect retrieves the registry keys only once, when the GlobalProtect app initializes.

Follow these guidelines when deploying the Connect Before Logon settings:

- *The Pre-logon and Pre-logon then On-demand connection methods are not supported simultaneously with Connect Before Logon.*
- *If you are using smart card authentication or username/password-based authentication for user login using an authentication service such as LDAP, RADIUS, or OTP, you must configure exclusions for specific fully qualified domain names for the portal and gateway by entering them to* ***Allow traffic to specified FQDN when Enforce GlobalProtect Connection for Network Access is enabled and GlobalProtect Connection is not established*** *as an* Customize the GlobalProtect App *in the* ***App Configurations*** *area of the GlobalProtect portal. If you are using SAML authentication for user login and using the configured SAML identity providers (IdPs) such as Okta, you must also configure exclusions for *okta.com and *oktacdn.com. For other IdPs, you must configure exclusions for the URLs that contain IP addresses or fully qualified domain names only if the Enforcer status is enabled.*

STEP 1 | Configure the registry keys on the end user Windows endpoints.

You must change the Windows registry on the end users' Windows endpoints before you can enable Connect Before Logon. You can automatically add the registry keys or manually add the keys.

- To automatically add the registry keys for `PanPlapProvider` and `PanPlapProvider.dll` in **PanGPS.exe** (`C:\Program Files\Palo Alto Networks`

\GlobalProtect), use the -registerplap command to run as an administrator by using the following syntax:

```
PanGPS.exe -registerplap
```

- To automatically unregister the keys for PanPlapProvider and PanPlapProvider.dll in **PanGPS.exe** (C:\Program Files\Palo Alto Networks\GlobalProtect), use the -unregisterplap command to run as an administrator by using the following syntax:

```
PanGPS.exe -unregisterplap
```

To manually add the registry keys, open the Windows Registry Editor and enter **regedit** on the command prompt.

You must create the CLSID folder.

1. In the Windows Registry, go to HKEY_CLASSES_ROOT\CLSID\{20A29589-E76A-488B-A520-63582302A285}.

   Add the PanPlapProvider value in the format **@=PanPlapProvider**.
2. In the Windows Registry, go to HKEY_CLASSES_ROOT\CLSID\{20A29589-E76A-488B-A520-63582302A285}\InprocServer32@="PanPlapProvider.dll".

   Verify that the **ThreadingModel** value is set to **Apartment**. This is the default value.
3. In the Windows Registry, go to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\PLAP Providers\{20A29589-E76A-488B-A520-63582302A285}@="PanPlapProvider".

   Add the PanPlapProvider value in the format **@=PanPlapProvider**.

STEP 2 | (Optional) Configure additional portal addresses or names to display.

If configured, Connect Before Logon will use the default portal address or name in the Windows Registry (HKEY_LOCAL_MACHINE\SOFTWARE\PaloAlto Networks\GlobalProtect\PanSetup with key Portal).

You can configure additional portal addresses or names that you want to display in the Portal drop-down by changing the registry keys on the end user Windows endpoints. You can add up

to five portal addresses or names. You must change the Windows registry on the end users' Windows endpoints before you can define the portal addresses or names.

Open the Windows Registry Editor and enter **regedit** on the command prompt.

1. In the Windows Registry, create the CBL folder under `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect`.
2. In the Windows Registry, go to `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\CBL`.
3. Select **Edit** > **New** > **String Value** to create a registry entry for each portal that you want to add.

   You must specify each entry as *Portal1*, *Portal2*, *Portal3*, *Portal4*, and *Portal5*. Each entry cannot contain spaces.
4. Right-click the *portal* registry value, and then select **Modify**.
5. Enter the IP address or name of the GlobalProtect portal in the **Value Data** field, and then click **OK**.
6. Repeat steps 3 and 4 for each portal that you want to add.

STEP 3 | (Optional) Display the predefined portal addresses or names.

You must change the Windows registry on the end users' Windows endpoints before you can display the portal addresses or names.

Open the Windows Registry Editor and enter **regedit** on the command prompt.

1. In the Windows Registry, create the CBL folder under `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect`.
2. In the Windows Registry, go to `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\CBL`.
3. Select **Edit** > **New** > **String Value** to create a registry entry for *AlwaysShowPortal*.
4. Enter the value as *yes* in the **Value Data** field, and then click **OK**.

   By default, Connect Before Logon does not display the portal address or name if only one portal is defined.

STEP 4 | (Optional) Enable end users to authenticate using a smart card.

You must change the Windows registry on the end users' Windows endpoints before you can enable smart card authentication.

Open the Windows Registry Editor and enter **regedit** on the command prompt.

1. In the Windows Registry, create the CBL folder under `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect`.
2. In the Windows Registry, go to `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\CBL`.
3. Select **Edit** > **New** > **String Value** to create a registry entry for *UseSmartCard*.
4. Enter the value as *yes* in the **Value Data** field, and then click **OK**.

STEP 5 | Reboot the endpoint.

You must reboot the endpoint in order for the PLAP and Connect Before Logon registry keys to take effect.

STEP 6 | Verify the configuration.

After you have configured the settings in the Windows registry and to use Connect Before Logon starting with GlobalProtect™ app 5.2, choose the authentication method:

- Connect Before Logon Using Smart Card Authentication
- Connect Before Logon Using SAML Authentication
- Connect Before Logon Using Username/Password-Based Authentication

Deploy GlobalProtect Credential Provider Settings in the Windows Registry

You can deploy the GlobalProtect credential provider settings to delay the GlobalProtect credential provider Windows sign-in request or to enforce the GlobalProtect credential provider as the default sign-in option for Windows 10 by using the Windows Registry.

STEP 1 | Delay the GlobalProtect credential provider Windows sign-in request.

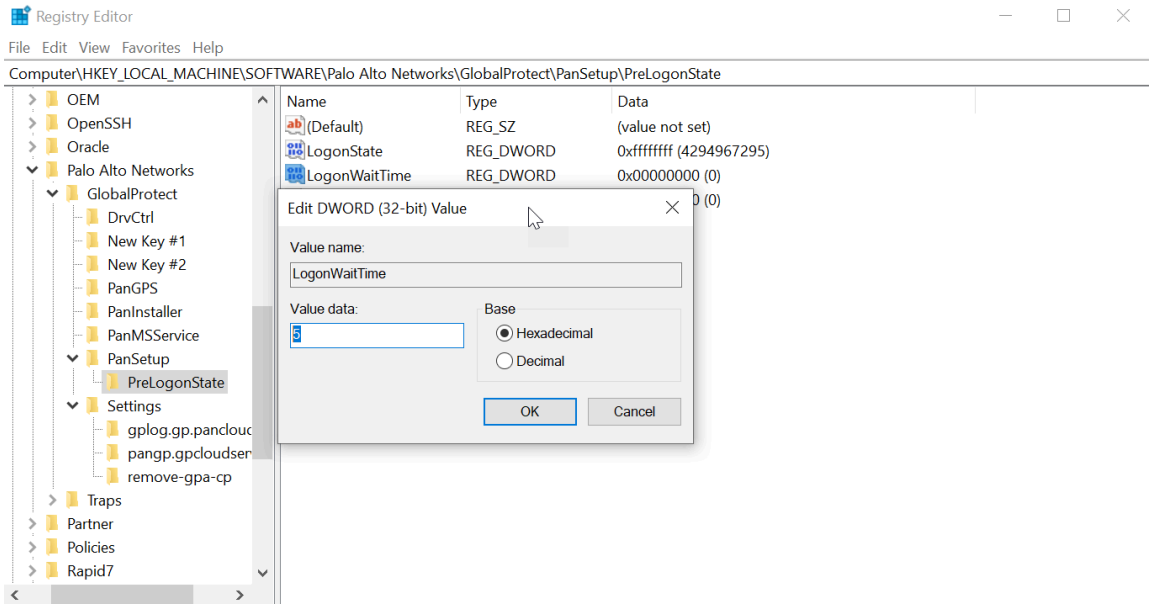
Establishing the GlobalProtect tunnel before Windows login can be useful in certain situations. For example, you may want to enforce the Windows device to synchronize data with the Active Directory or want to delay the GlobalProtect credential provider Windows sign-in request.

You can configure the amount of time (in seconds) that the GlobalProtect credential provider waits for the tunnel to be established before submitting a Windows sign-in request when single sign on (SSO) is enabled. By default, the GlobalProtect Credential Provider Support to

Delay Windows Login Before Establishing the Tunnel Connection feature is disabled and the GlobalProtect credential provider submits the sign-in requests without any delay.

1. From the command prompt, enter the **`regedit`** command to open the Windows Registry Editor.
2. In the Windows Registry, go to `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup`
3. Right-click **PreLogonState** and then select **New** > **DWORD (32-bit) Value**.
4. Right-click **New Value #1** and then select **Rename**.

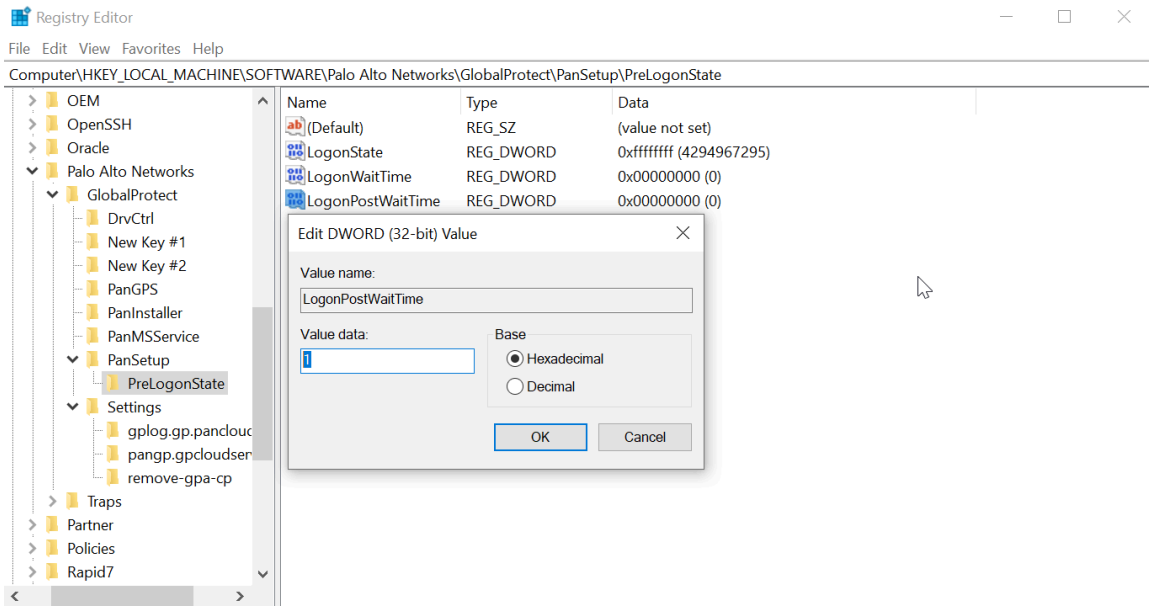
   Enter **LogonWaitTime**. Right-click **LogonWaitTime** and then select **Modify**. In the **Value Data** field, set the number of seconds (range is 5-30) for end users to wait to log in to Windows before establishing a tunnel connection. Click **OK**.



5. Repeat substeps 1, 2, and 3 to delay the GlobalProtect credential provider from submitting the Windows sign-in request after the tunnel is established.

   Enter **LogonPostWaitTime**. Right-click **LogonPostWaitTime** and then select **Modify**. In the **Value Data** field, set the number of seconds (range is 3-10) for end users to wait to log in to Windows. Click **OK**.

   *You are required to first enter the amount of time (in seconds) for **LogonWaitTime**, and then enter the amount of time (in seconds) for **LogonPostWaitTime**.*



STEP 2 | Enforce GlobalProtect credential provider as the default sign-in option for Windows 10.

When GlobalProtect SSO is enabled on Windows devices, users can have more than one sign-in option in addition to using the GlobalProtect credential provider options such as a third-party credential, smart card, Windows Hello PIN, Windows Hello Password, or Windows Hello Fingerprint. Users can use any of these sign-in options to sign in to their Windows device and set it as the default sign-in option at the next Windows login making GlobalProtect SSO unavailable. Users must manually switch to the GlobalProtect credential provider again to enable GlobalProtect SSO. When the GlobalProtect credential provider is enabled as the default sign-in option even when users can login with any other sign-in option, the

GlobalProtect credential provider sign-in option is selected at the next Windows login and for subsequent logins.

*When GlobalProtect is installed on Windows devices, users cannot log in to the device using the User Principal Name (UPN)- for example, **username@domain**- when the GlobalProtect credential provider is selected and the device is offline.*

Follow these guidelines when you are enforcing the GlobalProtect credential provider to be the default-sign option on Windows devices:

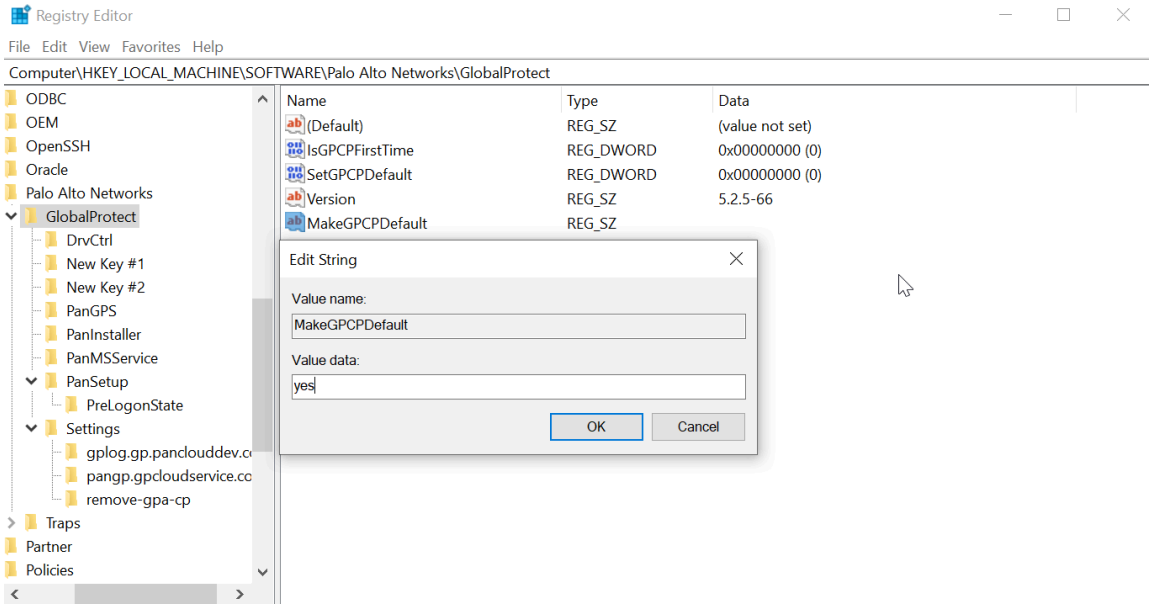
- *While the GlobalProtect app is installed or SSO is enabled, the GlobalProtect credential provider is set as the default sign-in option for all users even when the **MakeGPCPDefault** setting is disabled.*
- *When SSO is enabled and the **MakeGPCPDefault** setting is enabled, users can use any sign-in options such as a third-party credential provider, smart card, Windows Hello PIN, Windows Hello password, or Windows Fingerprint to sign in to their Windows device. Regardless of the sign-in option selected, the GlobalProtect credential provider will be used as the default sign-in option at the next Windows login.*
- *When SSO is enabled and the **MakeGPCPDefault** setting is disabled or empty, the user selected sign-in option will be used as the default at the next Windows login.*
- *When SSO is disabled, the GlobalProtect credential provider is unavailable. The Windows default sign-in option will work as expected.*
- *The Enforce GlobalProtect Credential Provider as the Default Sign-In for Windows 10 feature does not support the Other user login option. You can configure the Other user login option by using the Group Policy Object (GPO) on the Windows device.*

1. From the command prompt, enter the **regedit** command to open the Windows Registry Editor.
2. In the Window Registry, go to:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect`
3. Right-click the **GlobalProtect** folder, then select **New** > **String Value** to add a new string value.
4. Enter the **MakeGPCPDefault** string value. Right-click **MakeGPCPDefault** and then select **Modify**.

   In the **Value data** field, enter **yes** to enable the GlobalProtect credential provider to be the default sign-in option at the next Windows login. If you set the **Value data** to **no**, the

`MakeGPCPDefault` setting is disabled and the user selected sign-in option will be used as the default at the next Windows login. Click **OK**.



SSO Wrapping for Third-Party Credential Providers on Windows Endpoints

On Windows 7 endpoints, the GlobalProtect app utilizes the Microsoft credential provider framework to support single sign-on (SSO). With SSO, the GlobalProtect credential provider wraps the Windows native credential provider, enabling GlobalProtect to use Windows login credentials to automatically authenticate and connect to the GlobalProtect portal and gateway. In addition, SSO wrapping enables Windows 10 users to update their Active Directory (AD) password using the GlobalProtect credential provider when their password expires or an administrator requires a password change at the next login.

When other third-party credential providers also exist on the endpoint, the GlobalProtect credential provider is unable to gather the user's Windows login credentials. As a result, GlobalProtect fails to connect to the GlobalProtect portal and gateway automatically. If SSO fails, you can identify the third-party credential provider and configure the GlobalProtect app to wrap those third-party credentials, which enables users to successfully authenticate to Windows, GlobalProtect, and the third-party credential provider using only their Windows login credentials.

Optionally, you can configure Windows to display separate login tiles: one for each third-party credential provider and another for the native Windows login. This is useful when a third-party credential provider adds additional functionality that does not apply to GlobalProtect.

*If you want to remove the GlobalProtect credential provider from your Windows endpoint, execute the **`GlobalProtectPanGPS.exe -u`** command in the Command Prompt.*

Use the Windows registry or the Windows Installer (`msiexec`) to allow GlobalProtect to wrap third-party credentials:

- Enable SSO Wrapping for Third-Party Credentials with the Windows Registry

- Enable SSO Wrapping for Third-Party Credentials with the Windows Installer

> *GlobalProtect SSO wrapping for third-party credential providers (CPs) is dependent on the third-party CP settings. In some cases, GlobalProtect SSO wrapping might not work correctly if the third-party CP implementation does not allow GlobalProtect to successfully wrap their CP.*

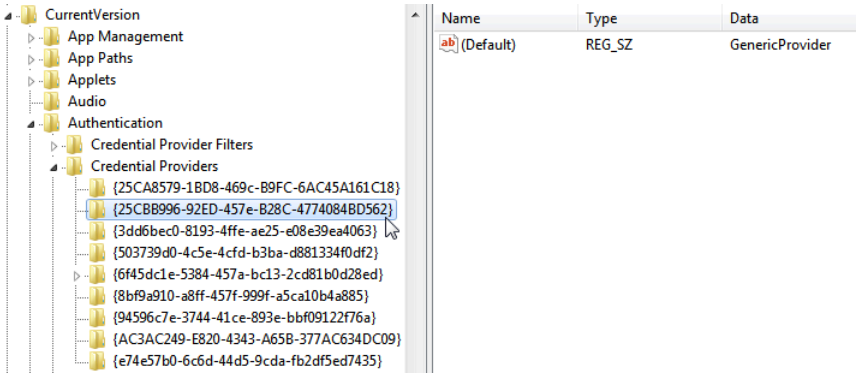
Enable SSO Wrapping for Third-Party Credentials with the Windows Registry

Use the following steps in the Windows Registry to enable SSO to wrap third-party credentials on Windows 7 endpoints.

STEP 1 | Open the Windows Registry and locate the globally unique identifier (GUID) for the third-party credential provider that you want to wrap.

1. From the command prompt, enter the **`regedit`** command to open the Windows Registry Editor.
2. Go to the following Windows Registry location to view the list of currently installed credential providers:

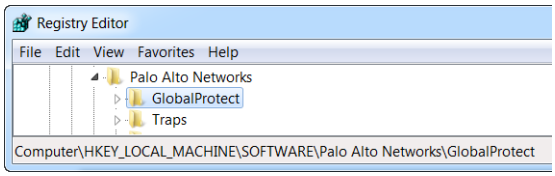
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion \Authentication\Credential Providers.`
3. Copy the GUID key for the credential provider that you want to wrap (including the curly brackets — { and } — on either end of the GUID):



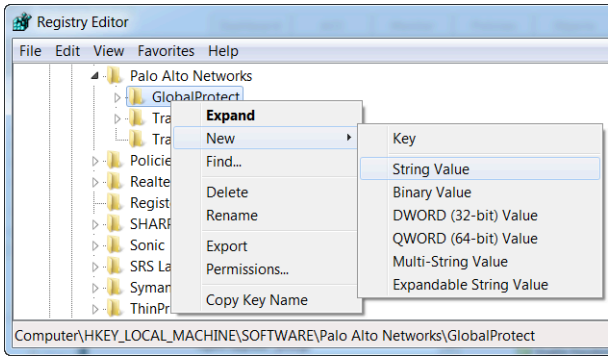
STEP 2 | Enable SSO wrapping for third-party credential providers by adding the **`wrap-cp-guid`** setting to the GlobalProtect Registry.

1. Go to the following Windows Registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\ GlobalProtect:
```



2. Right-click the **GlobalProtect** folder, and then select **New** > **String Value** to add a new string value:



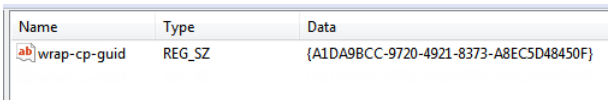
3. Configure the following **String Value** fields:
   - **Name**: **`wrap-cp-guid`**
   - **Value data**: {<**`third-party credential provider GUID`**>}

   > *For the **Value data** field, the GUID value that you enter must be enclosed with curly brackets: { and }.*

   The following is an example of what a third-party credential provider GUID in the **Value data** field might look like:

```
{A1DA9BCC-9720-4921-8373-A8EC5D48450F}
```

   For the new **String Value**, `wrap-cp-guid` is displayed as the string value's **Name** and the GUID is displayed as the **Value Data**.



STEP 3 | Next Steps:

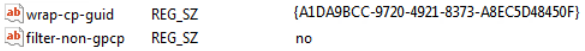
- With this setup, the native Windows logon tile is displayed to users on the logon screen. When users click the tile and log in to the system with their Windows credentials, that

single login authenticates the users to Windows, GlobalProtect, and the third-party credential provider.

- (Optional) If you want to display multiple tiles on the logon screen (for example, the native Windows tile and the tile for the third-party credential provider), continue to step 4.
- (Optional) If you want to assign a default credential provider for users, continue to step 5.
- (Optional) If you want to hide a third-party credential provider tile from the logon screen, continue to step 6.

STEP 4 | (Optional) Allow the third-party credential provider tile to be displayed to users at login.

Add a second **String Value** with the **Name** **`filter-non-gpcp`** and enter **`no`** for the string's **Value data**:



After you add this string value to the GlobalProtect settings, two login options are presented to users on the Windows logon screen: the native Windows tile and the third-party credential provider's tile.

STEP 5 | Assign a default credential provider for user login.

1. Open the Windows Registry to locate the globally unique identifier (GUID) for the third-party credential provider that you want to assign as the default credential provider.
   1. From the command prompt, enter the `regedit` command to open the Windows Registry Editor.
   2. Go to the following Windows Registry location to view the list of currently installed credential providers:

      `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion \Authentication\Credential Providers.`
   3. Copy the complete GUID key for the credential provider (including the curly brackets — { and } —on either end of the GUID).
2. Open the Local Group Policy Editor to enable and assign a default credential provider.
   1. From the command prompt, enter the `gpedit.msc` command to open the Local Group Policy Editor.
   2. Select **Computer Configuration** > **Administrative Templates** > **System** > **Logon**.
   3. Under **Setting**, double-click **Assign a default credential provider** to open the **Assign a default credential provider** window.
   4. Set the policy to **Enabled**.
   5. Under **Assign the following credential provider as the default credential provider**, enter the GUID of the credential provider (copied from the Windows Registry).
   6. Click **Apply**, and the click **OK** to save your changes.

STEP 6 | (Optional) Hide a third-party credential provider tile from the Windows logon screen.

1. Open the Windows Registry to locate the globally unique identifier (GUID) for the third-party credential provider that you want to hide.
   1. From the command prompt, enter the `regedit` command to open the Windows Registry Editor.
   2. Go to the following Windows Registry location to view the list of currently installed credential providers:

      ```
      HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion
      \Authentication\Credential Providers.
      ```
   3. Copy the complete GUID key for the credential provider that you want to hide (including the curly brackets — { and } — on either end of the GUID).
2. Open the Local Group Policy Editor to hide the third-party credential provider.
   1. From the command prompt, enter the `gpedit.msc` command to open the Local Group Policy Editor.
   2. Select **Computer Configuration** > **Administrative Templates** > **System** > **Logon**.
   3. Under **Setting**, double-click **Exclude credential providers** to open the **Exclude credential providers** window.
   4. Set the policy to **Enabled**.
   5. Under **Exclude the following credential providers**, enter the GUID of the credential provider you want to hide (copied from the Windows Registry).

      To hide multiple credential providers, separate each GUID with a comma.
   6. Click **Apply**, and then click **OK** to save your changes.

STEP 7 | Finalize your changes.

Once your changes are finalized, reboot your system for the changes to take effect.

Enable SSO Wrapping for Third-Party Credentials with the Windows Installer

Use the following options in the Windows Installer (Msiexec) to enable SSO to wrap third-party credential providers on Windows 7 endpoints.

- Wrap third-party credentials and display the native tile to users at login. Users can click the tile to log in to the endpoint using their native Windows credentials. With that single login, users can authenticate to Windows, GlobalProtect, and the third-party credential provider.

  Use the following syntax from the Windows Installer (Msiexec):

  ```
  msiexec.exe /i GlobalProtect.msi WRAPCPGUID=”{guid_value}”
   FILTERNONGPCP=”yes”
  ```

  In the syntax above, the **FILTERNONGPCP** parameter simplifies authentication for the user by filtering the option to log in to the system using the third-party credentials.

- If you would like users to have the option of logging in using the third-party credentials, use the following syntax from the Windows Installer (Msiexec):

```
msiexec.exe /i GlobalProtect.msi WRAPCPGUID="{guid_value}"
FILTERNONGPCP="no"
```

In the syntax above, the **FILTERNONGPCP** parameter is set to **"no"**, which filters out the third-party credential provider's logon tile so that only the native tile displays. In this case, both the native Windows tile and the third-party credential provider tile are displayed to users when logging in to the Windows endpoint.

Deploy App Settings to macOS Endpoints

Use the macOS global plist (property list) file to set the GlobalProtect app customization settings or to deploy scripts to macOS endpoints.

- Deploy App Settings in the macOS Plist
- Deploy Scripts Using the macOS Plist

Deploy App Settings in the macOS Plist

You can set the GlobalProtect app customization settings in the macOS global plist (Property list) file. This enables deployment of GlobalProtect app settings to macOS endpoints prior to their first connection to the GlobalProtect portal.

On macOS endpoints, plist files are either located in `/Library/Preferences` or in `~/Library/Preferences`. The tilde (~) symbol indicates that the location is in the current user's home folder. The GlobalProtect app on a macOS endpoint first checks for the GlobalProtect plist settings. If the plist does not exist at that location, the GlobalProtect app searches for plist settings in `~/Library/Preferences`.

In addition to using the macOS plist to deploy GlobalProtect app settings, you can enable the GlobalProtect app to collect specific macOS plist information from the endpoints. You can then monitor the data and add it to a security rule to use as matching criteria. Endpoint traffic that matches registry settings you define can be enforced according to the security rule. Additionally, you can set up custom checks to Collect Application and Process Data From Endpoints.

STEP 1 | Open the GlobalProtect plist file and locate the GlobalProtect app customization settings.

Use Xcode or an alternate plist editor to open the plist file:

`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`

Then go to:

`/Palo Alto Networks/GlobalProtect/Settings`

If the `Settings` dictionary does not exist, create it. Add each key to the `Settings` dictionary as a string.

STEP 2 | Set the portal name.

If you do not want the end user to manually enter the portal address even for the first connection, you can pre-deploy the portal address through the plist. In the `PanSetup` dictionary, configure an entry for `Portal`.

STEP 3 | Deploy various settings to the macOS endpoint, including the connect method for the GlobalProtect app.

View Customizable App Settings for a full list of the keys and values that you can configure using the macOS plist.

STEP 4 | (Optional) If you are using Enable System Extensions in the GlobalProtect App for macOS Endpoints and need to switch to Enable Kernel Extensions in the GlobalProtect App for macOS Endpoints, set the **key** value to **UseKextAnyway** in the macOS plist (`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`) for the GlobalProtect app.

Follow these guidelines when you are using system extensions and need to switch to kernel extensions:

- *After you have enabled system extensions, you must first uninstall the existing app to use the **UseKextAnyway** plist key to enable kernel extensions on macOS.*
- *You later have the option to revert to use system extensions. You must delete the **UseKextAnyway** plist key in the macOS plist. After you have deleted this plist key, you must restart the GobalProtect app in order for the change to take effect.*
- *By switching to kernel extensions, you can no longer use the Split DNS and Enforce GlobalProtect Connections with FQDN Exclusions features.*
- *If you have configured split tunnel settings based on the application on macOS endpoints, all Safari-based traffic, Microsoft Teams-based traffic, or Slack-based traffic that are defined in the split tunnel configuration would be dropped. We recommend that you use Chrome instead of Safari so that traffic defined in the split tunnel configuration will not be dropped. All traffic that was created based on the WebKit framework such as Safari, Microsoft Teams, or Slack might have problems using kernel extensions.*

You must specify **UseKextAnyway** as the plist key before installing GlobalProtect app 5.2.6 or later releases or upgrading from an earlier release to GlobalProtect app 5.2.6 or later releases running Catalina 10.15.4 or later. However, if you are upgrading from an earlier release to GlobalProtect app 5.2.6 or later releases running macOS Big Sur 11 or later, you must enable system extensions.

Deploy Scripts Using the macOS Plist

When a user connects to the GlobalProtect gateway for the first time, the GlobalProtect app downloads the configuration file and stores app settings in a GlobalProtect macOS property file (plist). In addition to making changes to the app settings, you use the plist to deploy scripts at any or all of the following events: before and after establishing the tunnel, and before disconnecting the tunnel. Use the following workflow to use the plist to deploy scripts to macOS endpoints.

The macOS plist settings that enable you to deploy scripts are supported on endpoints running GlobalProtect App 2.3 and later releases.

STEP 1 | (Endpoints running Mac OS X 10.9 or a later OS) Flush the settings cache. This prevents the OS from using the cached preferences after making changes to the plist.

To clear the default preferences cache, run the **`killall cfprefsd`** command from a macOS terminal.

STEP 2 | Open the GlobalProtect plist file, and locate or create the GlobalProtect dictionary associated with the connect or disconnect event. The dictionary under which you will add the settings determines when the GlobalProtect app runs the script(s).

Use Xcode or an alternate plist editor to open the plist file (`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`) and go to one of the following dictionary locations:

- `/PaloAlto Networks/GlobalProtect/Settings/pre-vpn-connect`
- `/Palo Alto Networks/GlobalProtect/Settings/post-vpn-connect`
- `/Palo Alto Networks/GlobalProtect/Settings/pre-vpn-disconnect`

If `Settings` dictionary does not exist, create it. Then, in `Settings`, create a new dictionary for the event or events at which you want to run scripts.

STEP 3 | Enable the GlobalProtect app to run scripts by creating a new `String` named **`command`**.

The value specified here should reference the shell script (and the parameters to pass to the script) that you want run on your endpoints.

If the `command` string does not already exist, add it to the dictionary and specify the script and parameters in the **Value** field. For example:

```
$HOME\pre_vpn_connect.sh
/Users/username username
```

Environmental variables are supported.

As a best practice, specify the full path in commands.

STEP 4 | (Optional) Add additional settings related to the command, including administrator privileges, a timeout value for the script, checksum value for the batch file, and an error message to display if the command fails to execute successfully.

Create or modify additional strings in the plist (`context`, `timeout`, `file`, `checksum`, and/or `error-msg`) and enter their corresponding values. For additional information, see Customizable App Settings.

STEP 5 | Save the changes to the plist file.

Save the plist.

Deploy App Settings to Linux Endpoints

You can set the GlobalProtect app customization settings in the pre-deployment configuration file (`pangps.xml`). This enables deployment of GlobalProtect app settings to Linux endpoints prior to their first connection to the GlobalProtect portal.

On Linux endpoints, the pre-deployment configuration file (`pangps.xml`) is located in `/opt/paloaltonetworks/globalprotect`.

The following table lists the pre-deployment settings for Linux endpoints that you can add to the `pangps.xml` file to customize the behavior of the GlobalProtect app and how the user interacts with the GlobalProtect app.

Portal Agent Configuration	Linux	Default
Connect Method	**connect-method on-demand | user-logon**	**user-logon**
Allow User to Change Portal Address	**can-change-portal yes | no**	**yes**
Allow User to Continue with Invalid Portal Server Certificate	**can-continue-if-portal-cert-invalid yes | no**	**yes**
Use Default Browser for SAML Authentication	**default-browser yes | no**	**no**
Portal Connection Timeout (sec)	**portal-timeout <portaltimeout>**	**5**
TCP Connection Timeout (sec)	**connect-timeout <connect-timeout>**	**5**
TCP Receive Timeout (sec)	**receive-timeout <receive-timeout>**	**30**
Not in portal This setting specifies the default portal IP address (or hostname).	**Portal <IPaddress>**	n/a

If you have already installed the GlobalProtect app on the Linux endpoint, follow these instructions:

1. *Stop the GlobalProtect VPN daemon. Use the* ***`sudo systemctl stop gpd.service`*** *command.*

   ```
   user@linuxhost:~$ sudo systemctl stop gpd.service
   ```

2. *Add the pre-deployment settings to the* `pangps.xml` *file in* `/opt/paloaltonetworks/globalprotect`.
3. *Modify the pre-deployment setting you want to edit for the* `pangps.xml` *file in* `/opt/paloaltonetworks/globalprotect`.
4. *Reboot the Linux endpoint in order for the pre-deployment configuration changes to take effect.*

If you are installing the GlobalProtect app for the first time, follow these instructions to deploy various settings to the Linux endpoint.

STEP 1 | Create the `/opt/paloaltonetworks/globalprotect/pangps.xml` pre-deployment configuration file.

STEP 2 | Add the pre-deployment settings to the `pangps.xml` file, including the connect method for the GlobalProtect app and the default browser for SAML authentication.

The following example shows the XML configuration of the pre-deployment changes that you deployed on the Linux endpoint, including the portal IP address (or hostname) under `<PanSetup>`.

```
<?xml version="1.0" encoding="UTF-8"?>
<GlobalProtect>
      <Settings>
          <connect-method>on-demand</connect-method>
          <can-continue-if-portal-cert-invalid>yes</can-continue-
if-portal-cert-invalid>
          <can-change-portal>no</can-change-portal>
          <portal-timeout>100</portal-timeout>
          <connect-timeout>100</connect-timeout>
          <receive-timeout>100</receive-timeout>
          <default-browser>yes</default-browser>
      </Settings>
      <PanSetup>
          <Portal>portal.acme.com</Portal>
      </PanSetup>
      <PanGPS>
      </PanGPS>
</GlobalProtect>
```

STEP 3 | Install the GlobalProtect app for Linux.

GlobalProtect Clientless VPN

GlobalProtect Clientless VPN provides secure remote access to common enterprise web applications. Users have the advantage of secure access from SSL-enabled web browsers without installing the GlobalProtect software. This is useful when you need to enable partner or contractor access to applications, and safely enable unmanaged assets, including personal endpoints. You can configure the GlobalProtect portal landing page to provide access to web applications based on users and user groups and also allow single-sign on to SAML-enabled applications. The following topics provide information on how to configure and troubleshoot Clientless VPN.

Clientless VPN Overview

When you configure GlobalProtect Clientless VPN, remote users can log in to the GlobalProtect portal using a web browser and launch the web applications you publish for the users. Based on users or user groups, you can allow users to access a set of applications that you make available to them or allow them to access additional corporate applications by entering a custom application URL.

Clientless VPN is not supported on firewalls with multiple virtual systems if the Clientless VPN traffic must traverse multiple virtual systems.

After logging in to the portal, users see a published applications page with the list of web applications that they can launch. You can use the default applications landing page on the GlobalProtect portal or create a custom landing page for your enterprise.

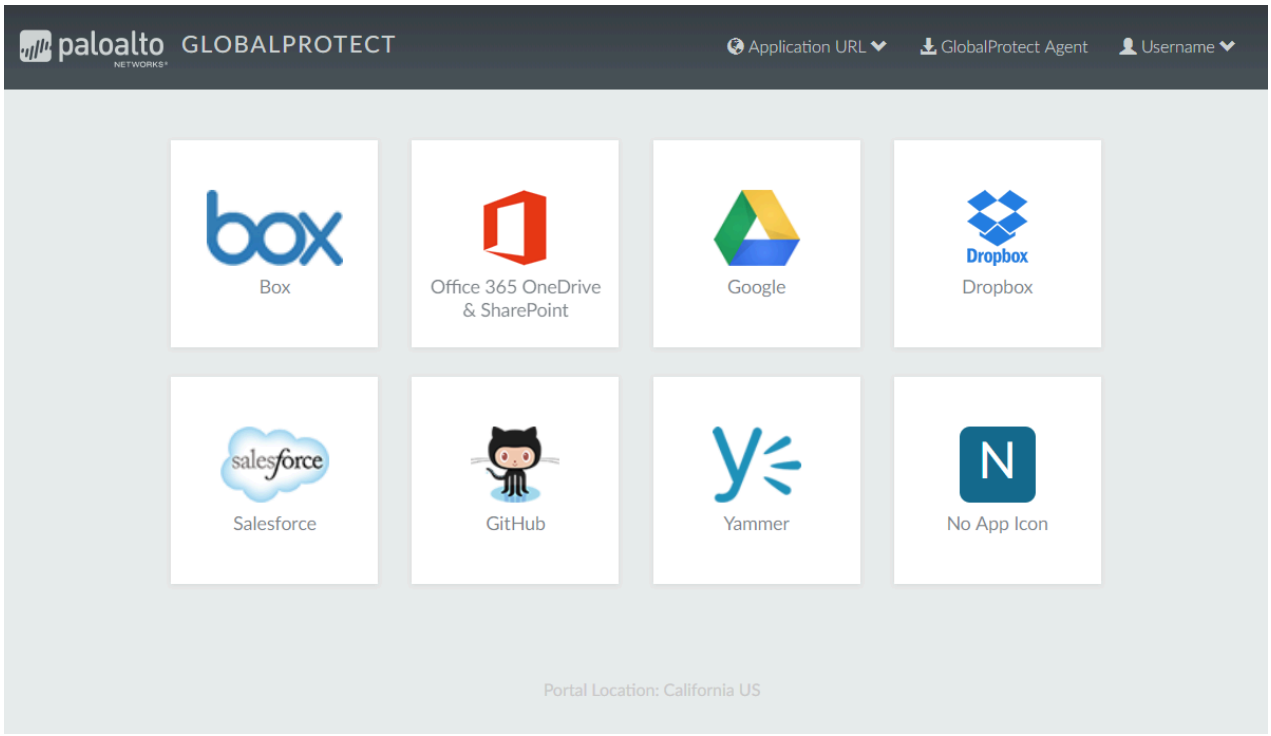


Figure 3: Applications Landing Page for Clientless VPN

Because this page replaces the default portal landing page, it includes a link to the GlobalProtect app download page. If configured, users can also select **Application URL** and enter URLs to launch additional unpublished corporate web applications.

When you configure only one web application (and disable access to unpublished applications), instead of taking the user to the published applications page, the application will launch automatically as soon as the user logs in. If you do not configure GlobalProtect Clientless VPN, users will see the app software download page when they log in to the portal.

When you configure GlobalProtect Clientless VPN, you need security policies to allow traffic from GlobalProtect endpoints to the security zone associated with the GlobalProtect portal that hosts the published applications landing page and security policies to allow user-based traffic from the GlobalProtect portal zone to the security zone where the published application servers are hosted. The security policies you define control which users have permission to use each published application.

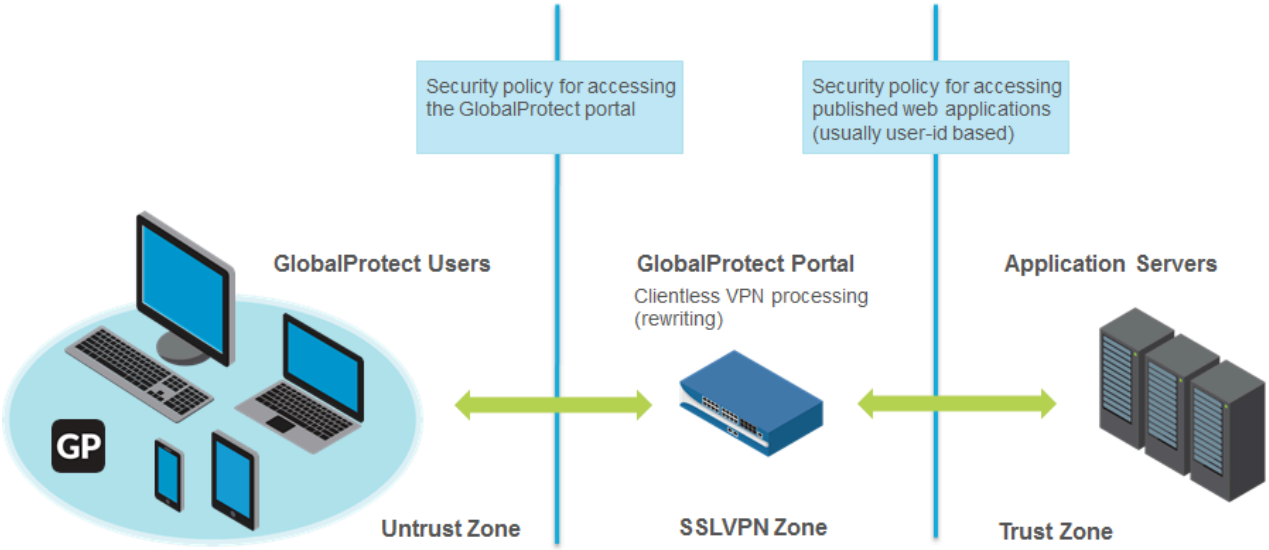


Figure 4: Zones and Security Policy for Clientless VPN

Supported Technologies

You can configure the GlobalProtect portal to provide secure remote access to common enterprise web applications. For best results, make sure you thoroughly test your Clientless VPN applications in a controlled environment before deploying them or making them available to a large number of users.

The following Web application technologies are not supported:

- *Non-Web applications such as SSH, FTP, SMTP, Remote desktop protocol (RDP), and so forth*
- *HTTP 2.0*
- *Non-UTF-8 encodings*
- *IPv6 deployment*
- *Multiple transactions in HTTP such as NT LAN Manager (NTLM) authentication*
- *Javascript ES6*
- *Files are not rewritten other than HTML, Javascript, and CSS (for example, Flash, Java Applet, Microsoft Silverlight, PDF, XML, and so forth)*
- *Other technologies (for example, Microsoft Silverlight or XML/XSLT)*
- *Any content encodings (for example, `Accept-Encoding: defalte, br`)*

Technology	Supported Version

Web application technologies	• HTML
	• HTML5
	• HTML5-Web-Sockets
	• Javascript ES5 or earlier
	• RDP, VNC, or SSH
	  • Virtual Desktop Infrastructure (VDI) and Virtual Machine (VM) environments, such as Citrix XenApp and XenDesktop, VMWare Horizon and vCenter support access natively through HTML5. You can RDP, VNC, or SSH to these machines through Clientless VPN without requiring additional third-party middleware.
	  • In environments that do not include native support for HTML5 or other web application technologies supported by Clientless VPN, you can use third-party vendors, such as Thinfinity, to RDP through Clientless VPN.
	• Adobe Flash—With Clientless VPN, browsers can serve content that uses Adobe Flash, Microsoft Word documents, or Adobe PDFs. However, Clientless VPN cannot rewrite HTML URLs or links within Adobe Flash, Microsoft Word documents, or Adobe PDFs, which can prevent the content from rendering correctly.

Technology	Supported Version
	• Content encodings (for example, `Accept-Encoding: gzip`)
Operating systems	• Windows • macOS • iOS • Android • Chrome • Linux
Supported browsers	• Chrome • Edge • Internet Explorer • Safari • Firefox

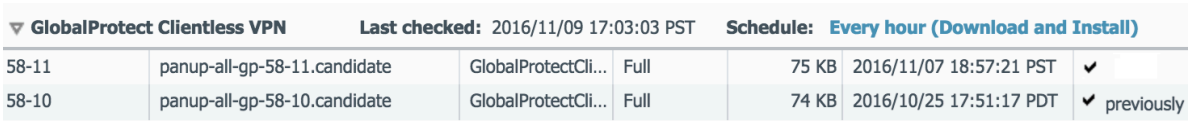
Supported authentication methods	• Local Authentication
	• External Authentication
	  • LDAP
	  • SAML
	  • Kerberos
	  • RADIUS or TACACS+
	• Client Certificate Authentication
	• Two-Factor Authentication

Configure Clientless VPN

To configure GlobalProtect Clientless VPN:

STEP 1 | Before you begin:

- Install a GlobalProtect subscription on the firewall that hosts the Clientless VPN from the GlobalProtect portal. Refer to Active Licenses and Subscriptions.
- Install the latest GlobalProtect Clientless VPN dynamic update (see Install Content and Software Updates) and set a schedule for installing new dynamic content updates. As a best practice, it is recommended to always install the latest content updates for GlobalProtect Clientless VPN.



GlobalProtect Clientless VPN	Last checked: 2016/11/09 17:03:03 PST		Schedule: Every hour (Download and Install)			
58-11	panup-all-gp-58-11.candidate	GlobalProtectCli...	Full	75 KB	2016/11/07 18:57:21 PST	✔
58-10	panup-all-gp-58-10.candidate	GlobalProtectCli...	Full	74 KB	2016/10/25 17:51:17 PDT	✔ previously

- As a best practice, configure a separate FQDN for the GlobalProtect portal that hosts Clientless VPN. Do not use the same FQDN as the PAN-OS Web Interface.
- Host the GlobalProtect portal on the standard SSL port (TCP port 443). Non-standard ports are not supported.

STEP 2 | Configure the applications that are available using GlobalProtect Clientless VPN. The GlobalProtect portal displays these applications on the landing page that users see when they log in (the applications landing page).

1. Select **Network** > **GlobalProtect** > **Clientless Apps** and **Add** one or more applications. For each application, specify the following:
   - **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.
   - **Location** (for a firewall that is in multiple virtual system mode)—the virtual system (vsys) where the Clientless VPN applications are available. For a firewall that is not in multi-vsys mode, the **Location** field does not display.
   - **Application Home URL**—The URL where the web application is located (up to 4,095 characters).
   - **Application Description** (Optional)—A brief description of the application (up to 255 characters).
   - **Application Icon** (Optional)—An icon to identify the application on the published application page. You can browse to upload the icon.
2. Click **OK**.

STEP 3 | (Optional) Create groups to manage sets of web applications.

Clientless App Groups are useful if you want to manage multiple collections of applications and provide access based on user groups. For example, financial applications for the G&A team or developer applications for the Engineering team.

1. Select **Network** > **GlobalProtect** > **Clientless App Groups**. **Add** a new Clientless VPN application group, and specify the following:
   - **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.
   - **Location** (for a firewall that is in multiple virtual system mode)—the virtual system (vsys) where the Clientless VPN application group is available. For a firewall that is not in multi-vsys mode, the **Location** field does not display.
2. In the **Applications** section, **Add** applications to the group. You can select from the list of existing Clientless VPN applications or define a **New Clientless App**.
3. Click **OK**.

STEP 4 | Configure the GlobalProtect portal to provide the Clientless VPN service.

1. Select **Network** > **GlobalProtect** > **Portal** and select an existing portal configuration or **Add** a new one. Refer to Set Up Access to the GlobalProtect Portal.
2. In the **Authentication** tab, you can:
   - (Optional) Create a new client authentication specifically for Clientless VPN. In this case, choose **Browser** as the **OS** for **Client Authentication**.
   - Use an existing client authentication.
3. In **Clientless** > **General**, select **Clientless VPN** to enable the portal service and configure the following:
   - Specify a **Hostname** (IP address or FQDN) for the GlobalProtect portal that hosts the applications landing page. This hostname is used for rewriting application URLs. (For more information on URL rewriting, refer to step 8).

     If you use Network Address Translation (NAT) to provide access to the GlobalProtect portal, the IP address or FQDN you enter must match (or resolve to) the NAT IP address for the GlobalProtect portal (the public IP address). Because users cannot access the GlobalProtect portal on a custom port, the pre-NAT port must also be TCP port 443.

   - Specify a **Security Zone**. This zone is used as a source zone for the traffic between the firewall and the applications. Security rules defined from this zone to the application zone determine which applications users can access.
   - Select a **DNS Proxy** server or configure a **New DNS Proxy**. GlobalProtect will use this proxy to resolve application names. Refer to DNS Proxy Object.
   - **Login Lifetime**—Specify the maximum length of time (in hours or minutes) that a Clientless VPN session is valid. The typical session time is 3 hours. The range for

hours is 1 to 24; the range for minutes is 60 to 1,440. After the session expires, users must re-authenticate and start a new Clientless VPN session.

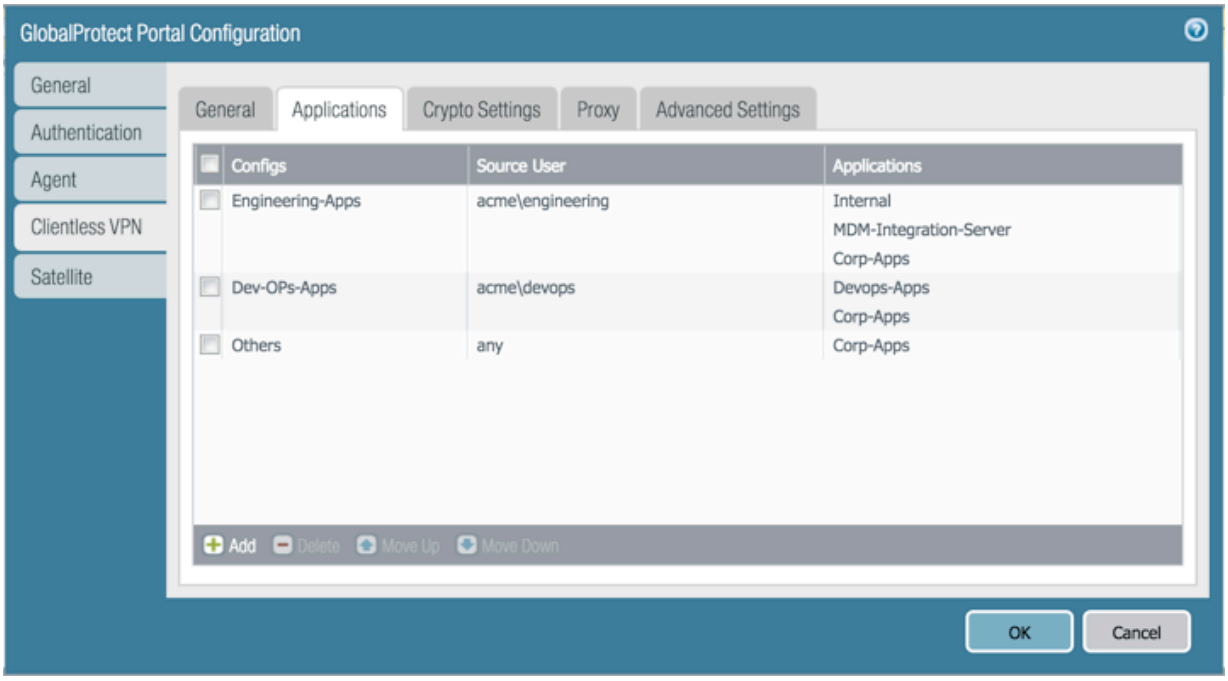
- **Inactivity Timeout**—Specify the length of time (in hours or minutes) that a Clientless VPN session can remain idle. The typical inactivity timeout is 30 minutes. The range for hours is 1 to 24; the range for minutes is 5 to 1,440. If there is no user activity during the specified length of time, users must re-authenticate and start a new Clientless VPN session.
- **Max User**—Specify the maximum number of users who can be logged in to the portal at the same time. If no value is specified, then endpoint capacity is assumed. If the endpoint capacity is unknown, then a capacity of 50 users is assumed. When the maximum number of users is reached, additional Clientless VPN users cannot log in to the portal.

STEP 5 | Map users and user groups to applications.

This mapping controls which applications users or user groups can launch from a GlobalProtect Clientless VPN session.

The GlobalProtect portal uses the user/user group settings that you specify to determine which configuration to deliver to the GlobalProtect Clientless VPN user that connects. If you have multiple configurations, make sure they are ordered correctly and map to all of the required applications; the portal looks for a configuration match starting from the top of

the list. As soon as the portal finds a match, it delivers the associated configuration to the GlobalProtect Clientless VPN user.



Publishing an application to a user/user group or allowing them to launch unpublished applications does not imply that they can access those applications. You use security policies to control access to applications (published or not).

*You must configure group mapping (**Device** > **User Identification** > **Group Mapping Settings**) before you can select the groups.*

1. On the **Applications** tab, **Add** an **Applications to User Mapping** to match users with published applications.
   - **Name**—Enter a name for the mapping (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
   - **Display application URL address bar**—Select this option to display an application URL address bar from which users can launch applications that are not published on the applications landing page. When enabled, users can select the **Application URL**.

     When this option is disabled:
     - Application URL will not appear in the Clientless VPN landing page.
     - The application will launch automatically as soon as the user logs in when only one web application is published. If the option is not disabled, user must click on the application to launch.

2. Specify the **Source Users**. You can **Add** individual users or user groups to which the current application configuration applies. These users have permission to launch the configured applications using a GlobalProtect Clientless VPN. In addition to users and groups, you can specify when these settings apply to the users or groups:
   - **any**—The application configuration applies to all users (no need to **Add** users or user groups).
   - **select**—The application configuration applies only to users and user groups you **Add** to this list.
3. **Add** individual applications or application groups to the mapping. The **Source Users** you included in the configuration can use GlobalProtect Clientless VPN to link to the applications you add.

STEP 6 | Specify the security settings for a Clientless VPN session.

1. On the **Crypto Settings** tab, specify the authentication and encryption algorithms for the SSL sessions between the firewall and the published applications.
   - **Protocol Versions**—Select the required minimum and maximum TLS/SSL versions. The higher the TLS version, the more secure the connection. Choices include **SSLv3**, **TLSv1.0**, **TLSv1.1**, or **TLSv1.2**.

     *The **Max Version** of TLS supported for Clientless VPN is TLSv1.2. **TLSv1.3** is currently not supported for Clientless VPN connections.*
   - **Key Exchange Algorithms**—Select the supported algorithm types for key exchange. Choices are: **RSA**, Diffie-Hellman (**DHE**), or Elliptic Curve Ephemeral Diffie-Hellman (**ECDHE**).
   - **Encryption Algorithms**—Select the supported encryption algorithms. We recommend **AES128** or higher.
   - **Authentication Algorithms**—Select the supported authentication algorithms. Choices are: **MD5**, **SHA1**, **SHA256**, or **SHA384**. We recommend **SHA256** or higher.
2. Select the action to take when the following issues occur with a server certificate presented by an application:
   - **Block sessions with expired certificate**—If the server certificate has expired, block access to the application.
   - **Block sessions with untrusted issuers**—If the server certificate is issued from an untrusted certificate authority, block access to the application.
   - **Block sessions with unknown certificate status**—If the OCSP or CRL service returns a certificate revocation status of `unknown`, block access to the application.
   - **Block sessions on certificate status check timeout**—If the certificate status check times out before receiving a response from any certificate status service, block access to the application.

STEP 7 | (Optional) Specify one or more proxy server configurations to access the applications.

Only basic authentication to the proxy is supported (username and password).

If users need to reach the applications through a proxy server, specify a **Proxy Server**. You can add multiple proxy server configurations, one for each set of domains.

- **Name**—A label (up to 31 characters) to identify the proxy server configuration. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
- **Domains**—Add the domains served by the proxy server. You can use a wild card character (*) at the beginning of the domain name to indicate multiple domains.
- **Use Proxy**—Select to assign a proxy server to provide access to the domains.
- **Server**—Specify the IP address or hostname of the proxy server.
- **Port**—Specify a port for communication with the proxy server.
- **User** and **Password**—Specify the **User** and **Password** credentials needed to log in to the proxy server. Specify the password again for verification.

STEP 8 | (Optional) Specify any special treatment for application domains.

The Clientless VPN acts as a reverse proxy and modifies web pages returned by the published web applications. It rewrites all URLs and presents a rewritten page to remote users such that when they access any of those URLs, the requests go through the GlobalProtect portal.

In some cases, the application may have pages that do not need to be accessed through the portal (for example, the application may include a stock ticker from yahoo.finance.com). You can exclude these pages.

On the **Advanced Settings** tab, **Add** domain names, hostnames, or IP addresses to the **Rewrite Exclude Domain List.** These domains are excluded from rewrite rules and cannot be rewritten.

Paths are not supported in hostnames and domain names. The wildcard character (*) for hostnames and domain names can appear only at the beginning of the name (for example, *.etrade.com).

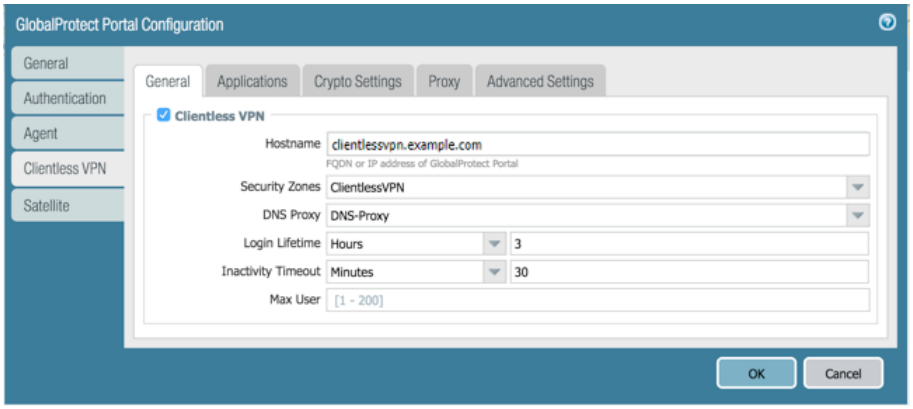
STEP 9 | Save the portal configuration.

1. Click **OK** twice.
2. **Commit** your changes.

STEP 10 | Configure a Security policy rule to enable users to access the published applications.

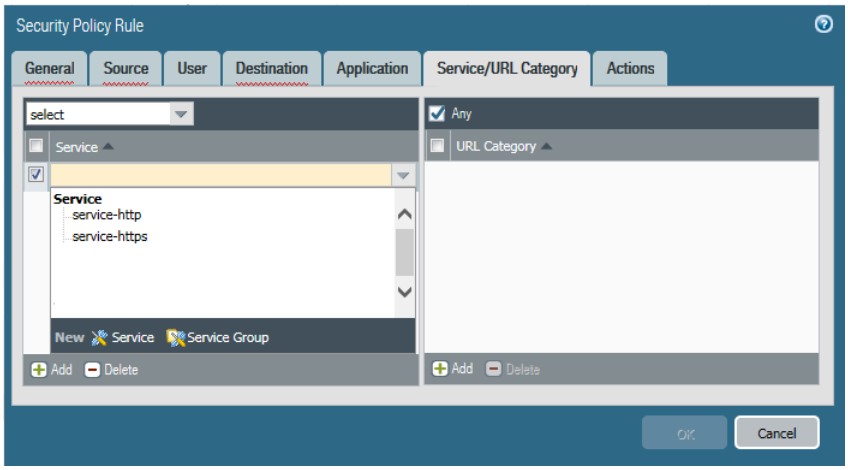
You need security policies for the following:

- Make the GlobalProtect portal that hosts Clientless VPN reachable from the internet. This is traffic from the Untrust or Internet Zone to the zone where you host the Clientless VPN portal.
- Allow Clientless VPN users to reach the internet. This is traffic from the Clientless VPN zone to the Untrust or Internet Zone.



- Allow Clientless VPN users to reach corporate resources. This is traffic from the Clientless VPN zone to the Trust or Corp Zone. The security policies you define control which users have permission to use each published application. For the security zone where the published application servers are hosted, make sure to **Enable User Identification**

  By default, **Service/URL** in **Security Policy Rule** is set to **application-default**. Clientless VPN will not work for HTTPS sites with this default setting. Change **Service/URL** to include both **service-http** and **service-https**.



- When you configure a proxy server to access Clientless VPN applications, make sure you include the proxy IP address and port in the security policy definition. When applications are accessed through a proxy server, only Security policies defined for the proxy IP address and port are applied.

STEP 11 | (Optional) To configure the Clientless VPN portal landing page to display the location of the portal to which Clientless VPN users are connected, specify the physical location of the firewall on which you configured the portal.

When Clientless VPN users experience unusual behavior, such as poor network performance, they can provide this location information to their support or Help Desk professionals to assist with troubleshooting. They can also use this location information to determine their proximity to the portal. Based on their proximity, they can evaluate whether they need to switch to a closer portal.

If you do not specify a portal location, the Clientless VPN portal landing page displays an empty location field.

- **In the CLI**—Use the following CLI command to specify the physical location of the firewall on which you configured the portal:

```
<username@hostname> set deviceconfig setting global-protect
 location <location>
```

- **In the XML API**—Use the following XML API to specify the physical location of the firewall on which you configured the portal:
  - **devices**—name of the firewall on which you configured the portal
  - **location**—location of the firewall on which you configured the portal

```
curl -k -F file=@filename.txt -g 'https://<firewall>/api/?
key=<apikey>&type=config&action=set&xpath=/config/devices/
entry[@name='<device-name>']/deviceconfig/setting/global-
protect&element=<location>location-string</location>'
```

The source IP address of Clientless VPN traffic (as seen by the application) will be either the IP address of the egress interface through which the portal can reach the application or the translated IP address when source NAT is in use.

Troubleshoot Clientless VPN

Because this feature involves dynamic re-writing of HTML applications, the HTML content for some applications may not re-write correctly and break the application. If issues occur, use the commands in the following table to help you identify the likely cause:

Table 6: Table: Rewrite Engine Statistics

Action	Command
CLI Commands	
List the version of Clientless VPN dynamic content being used You can also view the dynamic update version from the **Device** > **Dynamic Updates** > **GlobalProtect Clientless VPN**.	**show system setting ssl-decrypt memory** proxy uses shared allocator SSL certificate cache: Current Entries: 1 Allocated 1, Freed 0 Current CRE (61-62) : 3456 KB (Actual 3343 KB) Last CRE (60-47) : 3328 KB (Actual 3283 KB) In this example, the current dynamic update is version 61-62, and the last installed dynamic update is version 60-47.
List active (current) users of Clientless VPN	**show global-protect-portal current-user portal GP ClientlessPortal filter-user all-users** GlobalProtect Portal : GPClientlessPortal Vsys-Id : 1 User : paloaltonetworks.com\johndoe Session-id : 1SU2vrPIDfdopGf-7gahMTCiX8PuL0S0 Client-IP : 5.5.5.5 Inactivity Timeout : 1800 Seconds before inactivity timeout : 1750 Login Lifetime : 10800 Seconds before login lifetime : 10748 Total number of user sessions: 1
Show DNS resolution results This can be useful to determine if there are	**show system setting ssl-decrypt dns-cache** Total DNS cache entries: 89

Action	Command
DNS issues. If there is a DNS issue, you will notice querying against an FQDN that was not resolvable in the CLI output.	Site IP Expire(secs) Interface bugzilla.panw.local 10.0.2.15 querying 0 www.google.com 216.58.216.4 Expired 0 stats.g.doubleclick.net 74.125.199.154 Expired 0
Show all Clientless VPN user sessions and cookies stored	**show system setting ssl-decrypt gp-cookie-cache** User: johndoe, Session-id: 1SU2vrPIDfdopGf-7gahMTCiX8PuL0S0, Client-ip: 199.167.55.50
Show rewrite-stats This is useful to identify the health of the Clientless VPN rewrite engine. Refer to Troubleshoot Clientless VPN for information on rewrite statistics and their meaning or purpose.	**show system setting ssl-decrypt rewrite-stats** Rewrite Statistics initiate_connection : 11938 setup_connection : 11909 session_notify_mismatch : 1 reuse_connection : 37 file_end : 4719 packet : 174257 packet_mismatch_session : 1 peer_queue_update_rcvd : 167305 peer_queue_update_sent : 167305 peer_queue_update_rcvd_failure: 66 setup_connection_r : 11910 packet_mismatch_session_r : 22 pkt_no_dest : 23 cookie_suspend : 2826 cookie_resume : 2826 decompress : 26 decompress_freed : 26 dns_resolve_timeout : 27 stop_openend_response : 43 received_fin_for_pending_req : 26 Destination Statistics To mp : 4015 To site : 12018 To dp : 17276 Return Codes Statistics ABORT : 18 RESET : 30 PROTOCOL_UNSUPPORTED : 7 DEST_UNKNOWN : 10 CODE_DONE : 52656 DATA_GONE : 120359

Action	Command
	SWITCH_PARSER : 48 INSERT_PARSER : 591 SUSPEND : 2826 Total Rewrite Bytes : 611111955 Total Rewrite Useconds : 6902825 Total Rewrite Calls : 176545
Debug Commands	
Enable debug logs on the firewall running Clientless VPN Portal	**debug dataplane packet-diag set log feature ssl all** **debug dataplane packet-diag set log feature misc all** **debug dataplane packet-diag set log feature proxy all** **debug dataplane packet-diag set log feature flow basic** **debug dataplane packet-diag set log on**
Enable packet capture on the firewall running the Clientless VPN Portal	**debug dataplane packet-diag set capture username <*portal-username*>** **debug dataplane packet-diag set capture stage clientless-vpn-client file <*clientless-vpn-client-file*>** **debug dataplane packet-diag set capture stage clientless-vpn-server file <*clientless-vpn-server-file*>** **debug dataplane packet-diag set capture stage firewall file <*firewall-file*>** **debug dataplane packet-diag set capture stage receive file <*receive-file*>** **debug dataplane packet-diag set capture stage transmit file <*transmit-file*>** **debug dataplane packet-diag set capture on**

Action	Command
	When you execute packet capture commands, a consent page appears after end users log in to the Clientless VPN portal, informing them that the packets captured during their user session will contain unencrypted (clear-text) data. If users consent to the packet capture session, they then proceed to the applications landing page, where packet capture begins. If users do not consent to the packet capture session, they are logged out of the Clientless VPN portal and must contact an administrator to proceed with a regular user session (without packet capture). *If you execute packet capture commands for user sessions that are already in progress, those users are automatically logged out of the Clientless VPN portal and must log back in to accept or decline the packet capture session.*
Show packet capture files	**debug dataplane packet-diag show setting** -- --------- Packet diagnosis setting: -- --------- Packet filter Enabled: no Match pre-parsed packet: no -- --------- Logging Enabled: no Log-throttle: no Sync-log-by-ticks: yes Features: Counters: -- --------- Packet capture Enabled: yes Snaplen: 0 Username: test1 Stage clientless-vpn-client: file client.pcap Captured: packets - 3558 bytes - 11366322 Maximum: packets - 0 bytes - 0 Stage clientless-vpn-server: file server.pcap Captured: packets - 1779 bytes - 5651923 Maximum: packets - 0 bytes - 0 -- ---------
Export packet capture files to a	**scp export filter-pcap**

Action	Command
Secure Copy (SCP) server	+ remote-port SSH port number on remote host + source-ip Set source address to specified inter face address * from from * to Destination (username@host:path) **scp export filter-pcap from <*source-file*> to <*scp -server*> Destination (username@host:path)**

Table 7: Table: Rewrite Engine Statistics

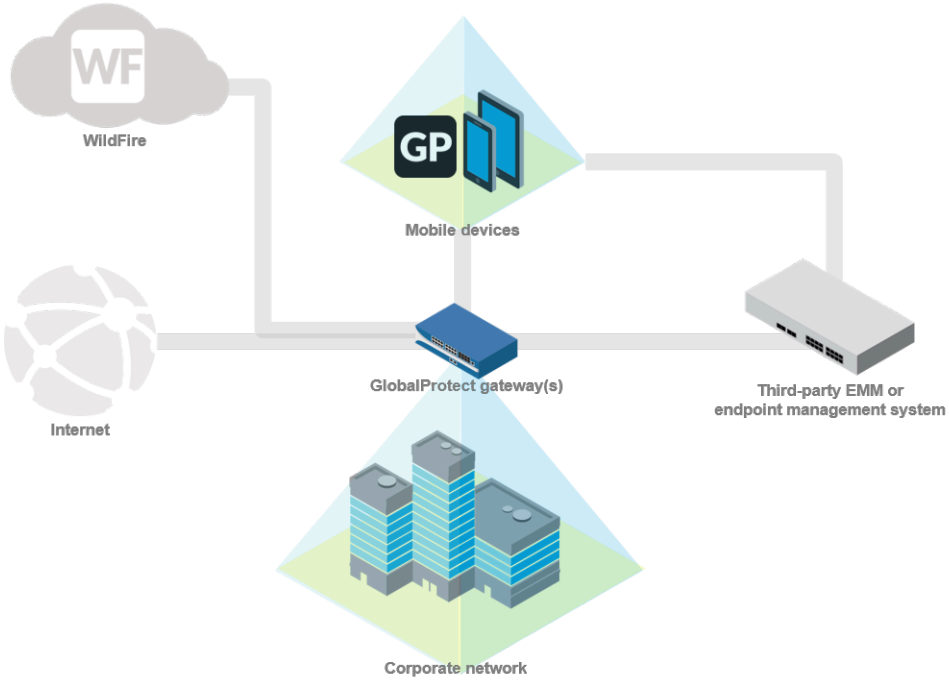
Statistic	Description
initiate_connection_failure	Connection initiation failed to back-end host
setup_connection_failure	Connection setup failed
setup_connection_duplicate	Duplicate peer session exists
session_notify_mismatch	Mostly invalid session
packet_mismatch_session	Failed to find right session for incoming packet
peer_queue_update_rcvd_failure	Session was invalid when packet update received by peer
peer_queue_update_sent_failure	Failed to send packet updates to peer or failed to send packet queue length updates to peer
exceed_pkt_queue_limit	Too many packets queued
proxy_connection_failure	Proxy connection failed
setup_connection_r	Installing the peer session to the application server. This value should match the values for **initiate_connection** and **setup_connection**.
setup_connection_duplicate_r	Duplicate sessions already in proxy
setup_connection_failure_r	Failed to set up the peer session
session_notify_mismatch_r	Peer session not found
packet_mismatch_session_r	Peer session not found when trying to get the packet
exceed_pkt_queue_limit_r	Too many packets held

Statistic	Description
unknown_dest	Failed to find destination host
pkt_no_dest	No destination for this packet
cookie_suspend	Suspended session to fetch cookies
cookie_resume	Received response from MP with updated cookies. This value generally matches the value of cookie_suspend.
decompress_failure	Failed to decompress
memory_alloc_failure	Failed to allocate memory
wait_for_dns_resolve	Suspended session to resolve DNS requests
dns_resolve_reschedule	Rescheduled DNS query due to no response (retry before timeout)
dns_resolve_timeout	DNS query timeout
setup_site_conn_failure	Failed to setup connection to site (proxy, DNS)
site_dns_invalid	DNS resolve failed
multiple_multipart	Multi-part content-type processed
site_from_referer	Received the back-end host from referrer. This can indicate failed rewrite links from flash or other content which Clientless VPN does not rewrite.
received_fin_for_pending_req	Received FIN from server for pending request from client
unmatched_http_state	Unexpected HTTP content. This can indicate an issue parsing the http headers or body.

Mobile Device Management

Mobile Device Management Overview

As mobile endpoints become more powerful, end users increasingly rely on them to perform business tasks. However, these same endpoints that access your corporate network also connect to the internet without protection against threats and vulnerabilities.



A mobile device management (MDM) system or enterprise mobility management (EMM) system simplifies the administration of mobile endpoints by enabling you to automatically deploy your corporate account configuration and VPN settings to compliant endpoints. You can also use your mobile device management system for remediation of security breaches by interacting with an endpoint that has been compromised. This protects both corporate data as well as personal end user data. For example, if an end user loses an endpoint, you can remotely lock the endpoint from the mobile device management system or even wipe the endpoint (either completely or selectively).

In addition to the account provisioning and remote device management functions that a mobile device management system can provide, when integrated with your existing GlobalProtect™ VPN infrastructure, you can use host information that the endpoint reports to enforce security policies for access to apps through the GlobalProtect gateway. You can also use the monitoring tools that are built into the Palo Alto next-generation firewall to monitor mobile endpoint traffic.

GlobalProtect Integration With an MDM or EMM System

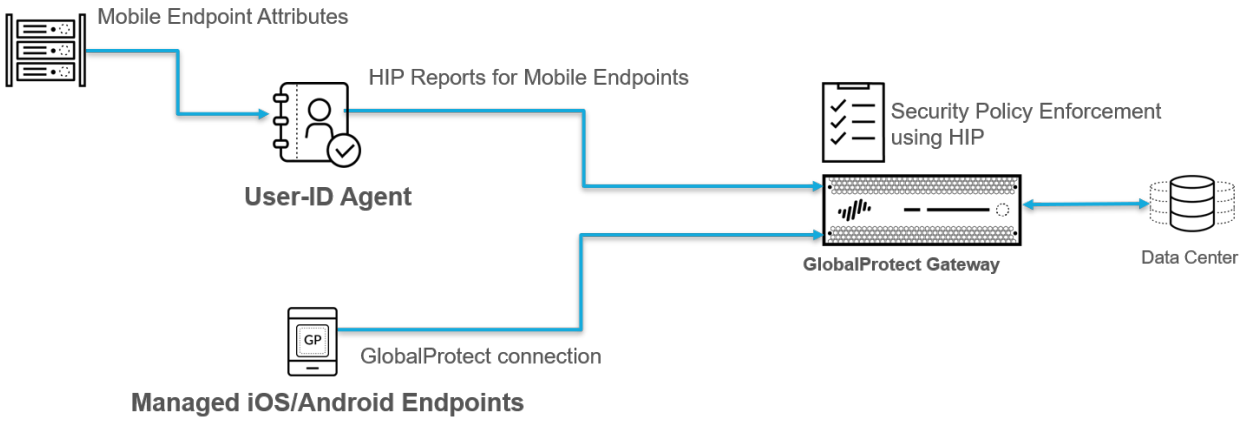
You can integrate your GlobalProtect deployment with an MDM or EMM system using one of the following methods:

Firewall Integration With an MDM or EMM System (Workspace ONE only)

You can Configure Windows User-ID Agent to Collect Host Information to communicate with the Workspace ONE MDM server to collect host information from connecting endpoints. The User-ID agent sends this host information to the GlobalProtect gateway as part of the HIP report for use in HIP-based policy enforcement.

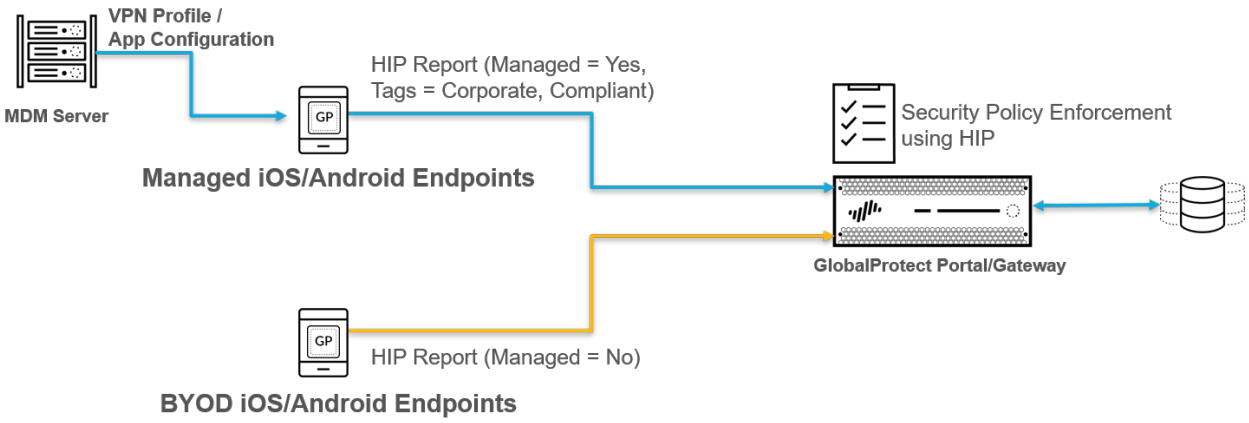
Firewall integration is supported with PAN-OS 8.0 and later releases.

Firewall integration is supported only with VMware Workspace ONE.



GlobalProtect App Integration With an MDM or EMM System

Starting with version 5.0, the GlobalProtect app for iOS and Android endpoints can obtain vendor data attributes and tags from MDM systems. For iOS endpoints, MDM systems send these attributes to the GlobalProtect app as part of the VPN profile. For Android endpoints, MDM systems send these attributes as part of the App Restrictions configuration. The GlobalProtect app can then send these attributes and tags to the GlobalProtect gateway as part of the HIP report for use in HIP-based policy enforcement.



GlobalProtect app integration is qualified with VMware Workspace ONE, MobileIron, and Microsoft Intune. However, this integration method is also supported with any MDM or EMM system that supports vendor data attributes in the VPN profile.

The following table describes the supported vendor data attributes:

MDM Attribute	HIP Report Attribute	HIP Report Category	Description
`mobile_id`	**Host ID**	**General**	Unique device identifier (UDID) of the endpoint.
`managed`	**Managed**	**General**	Value that indicates whether the endpoint is managed. If this value is **Yes**, the endpoint is managed. If this value is **No**, the endpoint is unmanaged.
`compliance`	**Tag**	**Mobile Device**	Compliance status that indicates whether the endpoint is compliant with the MDM compliance policies that you have defined (for example, **Compliant**). This value is appended to the **Tag** attribute in the HIP report.
`ownership`	**Tag**	**Mobile Device**	Ownership category of the endpoint (for example, **Employee Owned**).

MDM Attribute	HIP Report Attribute	HIP Report Category	Description
			This value is appended to the **Tag** attribute in the HIP report.
`tag`	**Tag**	**Mobile Device**	Tags to match against other MDM-based attributes.

Set Up the MDM Integration With GlobalProtect

To set up the MDM integration with GlobalProtect, use the following workflow:

STEP 1 | Set up the GlobalProtect Infrastructure.

1. Create Interfaces and Zones for GlobalProtect.
2. Enable SSL Between GlobalProtect Components.
3. Set up GlobalProtect User Authentication. Refer to GlobalProtect User Authentication.
4. Enable Group Mapping.
5. Configure a GlobalProtect Gateway.
6. Activate Licenses for each firewall running a gateway(s) that supports the GlobalProtect app on mobile endpoints.
7. Set Up Access to the GlobalProtect Portal.

STEP 2 | Set up the mobile device management system and decide whether to support only corporate-issued endpoints or both corporate-issued and personal endpoints.

See the instructions for your mobile device management (MDM) system or enterprise mobility management (EMM) system.

STEP 3 | Obtain the GlobalProtect app for mobile endpoints.

You can install the app directly from the app store on your endpoint (see Download and Install the GlobalProtect Mobile App) or deploy the app from a mobile device management system (such as Workspace ONE) and transparently push the app to your managed endpoints.

- App store— Download and Install the GlobalProtect Mobile App
- Supported mobile device management systems—See the following instructions on how to deploy apps to managed endpoints:
  - Deploy the GlobalProtect Mobile App Using Workspace ONE
  - Deploy the GlobalProtect App for Android on Managed Chromebooks Using Workspace ONE
  - Deploy the GlobalProtect Mobile App Using Microsoft Intune
  - Deploy the GlobalProtect Mobile App Using MobileIron
  - Deploy the GlobalProtect App for Android on Managed Chromebooks Using the Google Admin Console
- Other third-party mobile device management system—See the instructions from your vendor on how to deploy apps to managed endpoints.

STEP 4 | Configure the MDM integration.

Use one of the following methods to configure the MDM integration:

- Firewall integration with an MDM or EMM system:
  - Configure Windows User-ID Agent to Collect Host Information
- GlobalProtect app integration with an MDM or EMM system:
  - Manage the GlobalProtect App Using Workspace ONE
  - Manage the GlobalProtect App Using Microsoft Intune
  - Manage the GlobalProtect App Using MobileIron
  - Manage the GlobalProtect App Using Google Admin Console
  - Manage the GlobalProtect App Using Other Third-Party MDMs

STEP 5 | Configure polices that target mobile endpoints using host information.

Configure HIP-Based Policy Enforcement for managed endpoints.

Qualified MDM Vendors

The following table lists the qualified MDM vendors that you can use to configure, deploy, and manage the GlobalProtect app by OS. A — indicates that the OS is not supported.

If you want to use an MDM vendor that has not been qualified, Manage the GlobalProtect App Using Other Third-Party MDMs.

Supported MDM Vendor	Android	iOS	Chrome	Windows	Windows 10 UWP	macOS	Linux
Workspace ONE (formerly AirWatch)	√ (Per-App VPN only)	√	—	—	√	—	—
Microsoft Intune	√ (Always On, Remote Access, and Per-App VPN only)	√	—	—	√ (Always On and Per-App VPN only)	—	—
MobileIron	√ (Always On VPN only)	√	—	—	—	—	—
Google Admin console	√ (for Android app support on Chromebooks; app deployment only)	—	√ (app deployment only)	—	—	—	—

Supported MDM Vendor	Android	iOS	Chrome	Windows	Windows 10 UWP	macOS	Linux
	You can use the Google Admin console only to deploy the GlobalProtect app; you cannot use the console to configure VPN configurations. You must configure the VPN configuration through the Customize the GlobalProtect App before you can deploy the app using the Google Admin console.						
Jamf Pro	–	–	–	–	–	√ (app deployment and configuration profile deployment only)	–
	You can use Jamf Pro only to deploy the GlobalProtect app and configuration profiles; you cannot use the Jamf to configure VPN configurations. You must configure the VPN configuration through the Customize the GlobalProtect App before you can deploy the app using Jamf.						

Manage the GlobalProtect App Using Workspace ONE

Workspace ONE is an Enterprise Mobility Management Platform that enables you to manage mobile endpoints from a central console. The GlobalProtect app provides a secure connection between the firewall and the mobile endpoints that are managed by Workspace ONE at either the device or application level. Using GlobalProtect as the secure connection allows consistent inspection of traffic and enforcement of network security policy for threat prevention on mobile endpoints.

Refer to the following sections for information on how to deploy, configure, and manage the GlobalProtect app for mobile endpoints using Workspace ONE:

- Deploy the GlobalProtect Mobile App Using Workspace ONE
- Deploy the GlobalProtect App for Android on Managed Chromebooks Using Workspace ONE
- Configure Workspace ONE for iOS Endpoints
- Configure Workspace ONE for Windows 10 UWP Endpoints
- Configure Workspace ONE for Android Endpoints
- Enable App Scan Integration with WildFire

If you are not using a Qualified MDM Vendors, you can Manage the GlobalProtect App Using Other Third-Party MDMs.

Deploy the GlobalProtect Mobile App Using Workspace ONE

You can deploy the GlobalProtect app to managed endpoints that are enrolled with Workspace ONE. Endpoints running iOS or Android must download the Workspace ONE agent to enroll with the Workspace ONE MDM. Windows 10 endpoints do not require the Workspace ONE agent but require you to configure enrollment on the endpoint. After you deploy the app, configure and deploy a VPN profile to set up the GlobalProtect app for end users automatically.

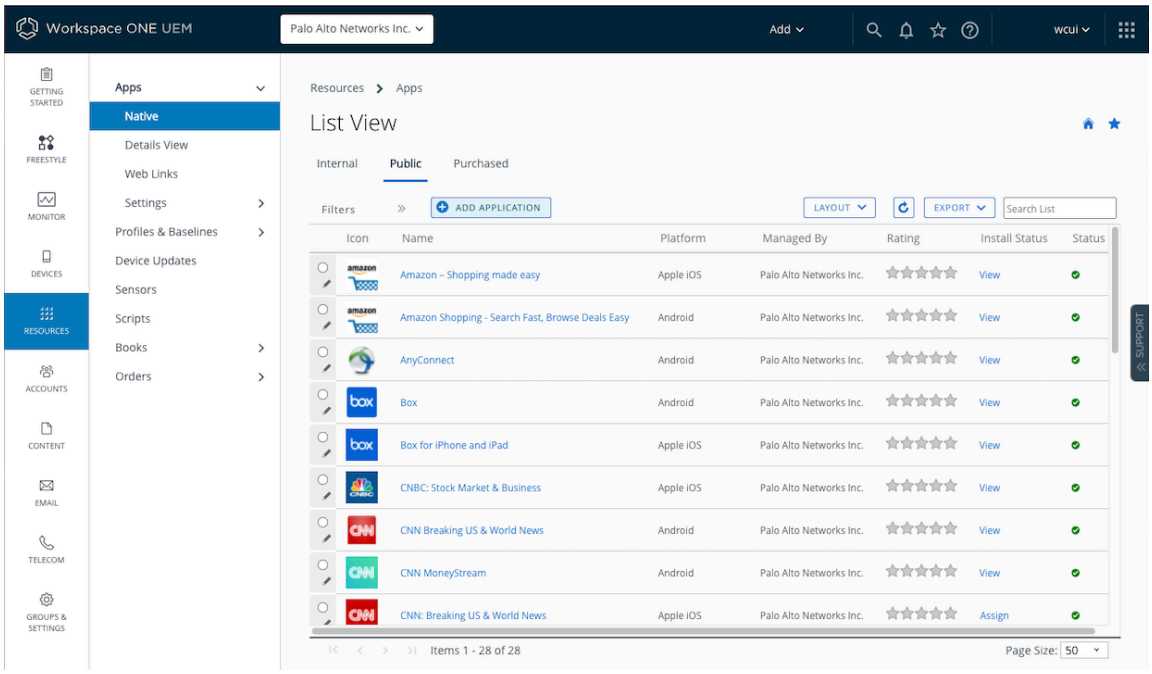
If you want to run the GlobalProtect app for Android on managed Chromebooks, you can Deploy the GlobalProtect App for Android on Managed Chromebooks Using Workspace ONE.

STEP 1 | Before you begin, ensure that the endpoints to which you want to deploy the GlobalProtect app are enrolled with Workspace ONE:

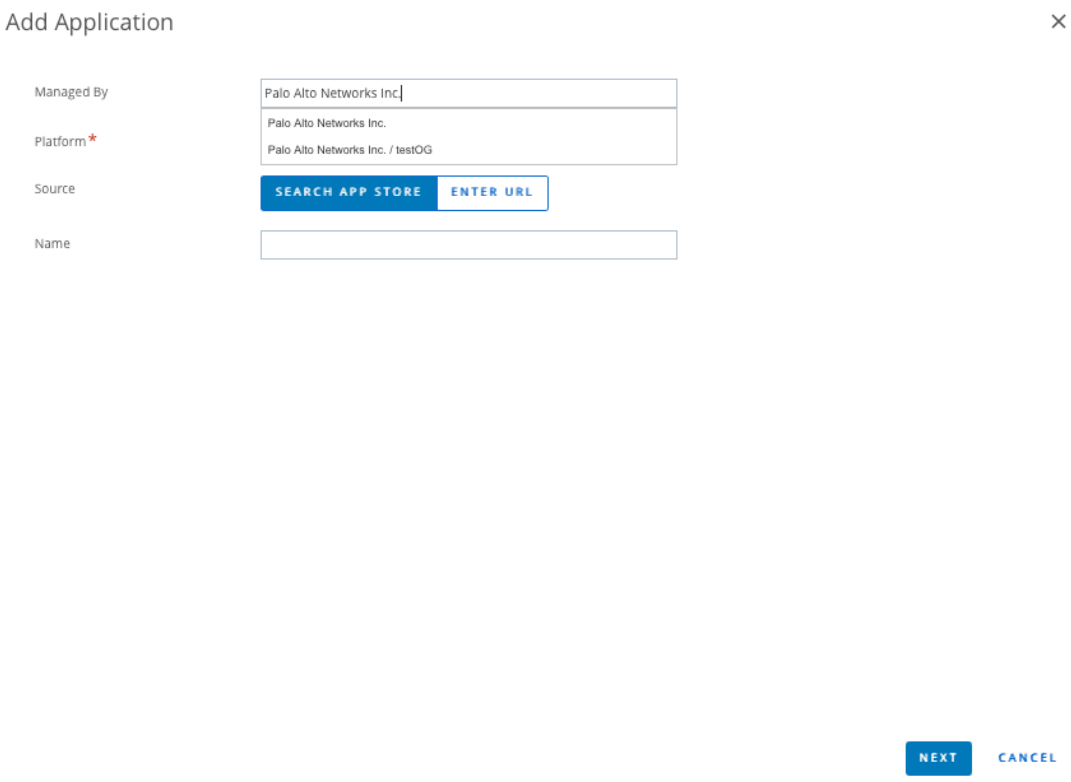
- **Android and iOS**—Download the Workspace ONE agent and follow the prompts to enroll.
- **Windows Phone and Windows 10 UWP**—Configure the Windows 10 UWP endpoint to enroll with Workspace ONE (from the endpoint, select **Settings** > **Accounts** > **Work access** > **Connect**).

STEP 2 | Add the GlobalProtect app to Workspace ONE:

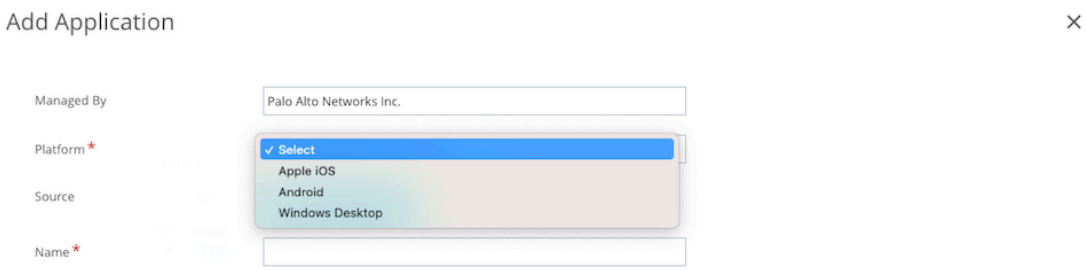
1. From Workspace ONE, select **Resources** > **Apps** > **Native** > **Public** > **Add Application**.



2. In the **Managed by** field, select the organization group by which this app will be managed.



3. Select the **Platform** (**Apple iOS**, **Android**, or **Windows Desktop**).



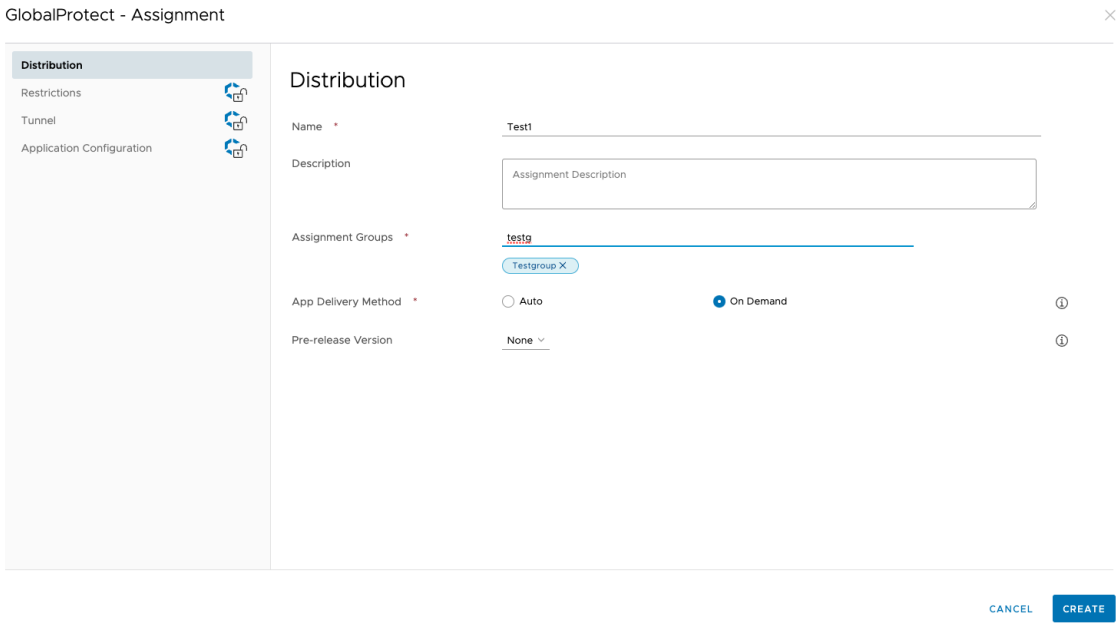
4. Search for the GlobalProtect app in the endpoint app store, or enter one of the following URLs for the GlobalProtect app page:
   - **Apple iOS**—https://apps.apple.com/us/app/globalprotect/id1400555706
   - **Android**—https://play.google.com/store/apps/details?id=com.paloaltonetworks.globalprotect
   - **Windows Phone and Windows 10 UWP**—https://www.microsoft.com/en-us/p/globalprotect/9nblggh6bzl3
5. Click **Next**. If you searched for the app in the endpoint app store, you must also **Select** the app from a list of search results, and then **SAVE & ASSIGN** to configure deployment options.

   If you searched for the GlobalProtect app for Android and did not see the app in the list, contact your Android for Work administrator to add GlobalProtect to the list of approved company apps or use the app URL in the Google Play Store.

STEP 3 | Configure deployment options for the GlobalProtect app:

*If you added the app previously but did not assign the app to any Smart Groups, select the GlobalProtect link from the list of apps (**Resources** > **Apps** > **Native** > **Public**). In the Details View, select **Assign** > **Add Assignment**.*

1. On the **Distribution** tab, specify the following information:
   1. Enter a **Name** for the assignment.
   2. Select one or more **Assignment Groups** that will have access to the GlobalProtect app.
   3. Choose the **App Delivery Method**, either **Auto**, which pushes the app to the device automatically, or **On Demand**, which deploys the app when needed.

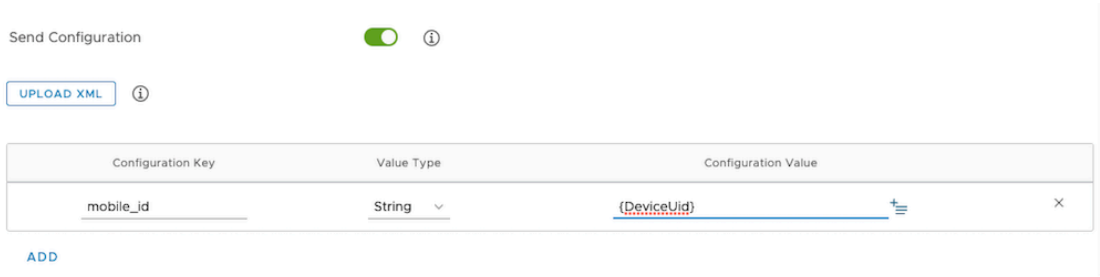


2. (GlobalProtect App for iOS or Android only) On the **Application Configuration** tab, enable the application configuration to use the UDID to identify the endpoint.
   - **iOS**—To use Configure Windows User-ID Agent to Collect Host Information for your GlobalProtect deployment on iOS devices, you can specify the unique

device identifier (UDID) attribute. For details, see Configure an Always On VPN Configuration for iOS Endpoints Using Workspace ONE.

Toggle on **Send Configuration** and add the following key-value pairs:

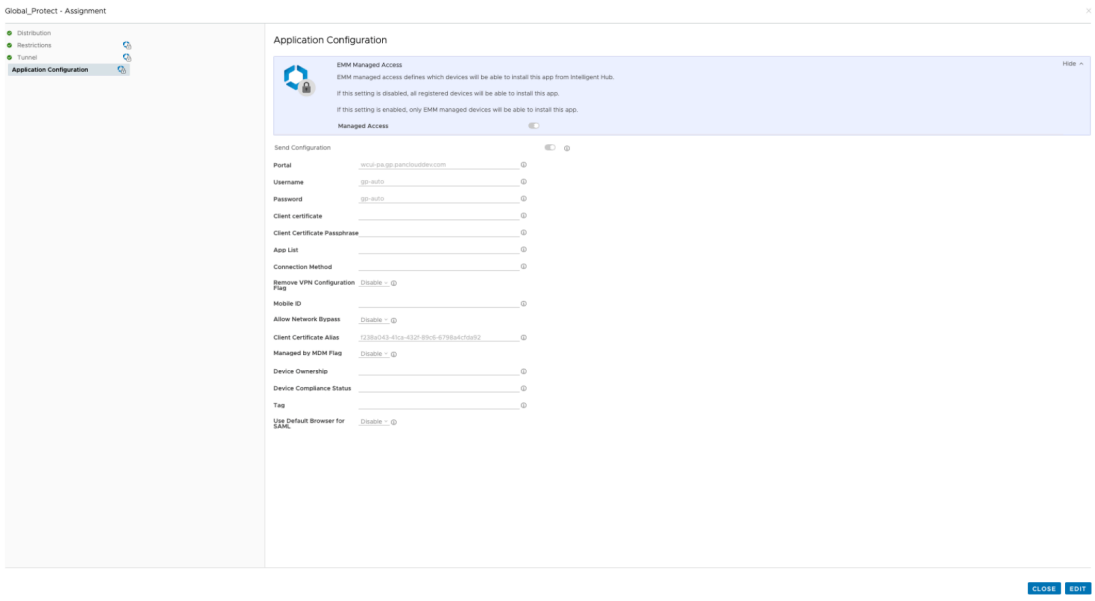
- **Configuration Key**—**`mobile_id`**
- **Value Type**—**`String`**
- **Configuration Value**—**`{DeviceUid}`**



- **Android**—Toggle on **Send Configuration** and specify the settings in the application configuration that are relevant for your company:
  - **Portal**—IP address or fully qualified domain name (FQDN) of the portal.
  - **Username**—Username for portal authentication.
  - **Password**—Password for portal authentication.
  - **Client Certificate**—Client certificate for portal authentication.
  - **Client Certificate Passphrase**—Passphrase for the client certificate.
  - **App List**—Begin the string with either the **allowlist** keyword or **blocklist** keyword followed by a colon, and follow it with an array of app names separated by semicolons. The block list or allow list enables you to control which application traffic can go through the VPN tunnel in a per-app VPN configuration

(for example, **allowlist| blocklist: com.google.calendar; com.android.email; com.android.chrome**).

- **Connection Method**—VPN connection method (for example, **user-logon | on-demand**).
- **Remove VPN Configuration Flag**—Flag to remove the VPN configuration.
- **Mobile ID**—Unique identifier used to identify mobile endpoints, as configured in a third-party MDM system.
- **Allow Network Bypass**—Flag to allow application traffic to bypass the VPN tunnel.
- **Client Certificate Alias**—Unique name to identify the client certificate during portal or gateway authentication.
- Specify the **Managed by MDM Flag** to indicate whether the device is enrolled with an MDM server.
- **Device Ownership**—Ownership category of the device (for example, **Employee Owned**).
- **Device Compliance Status**—Compliance status that indicates whether the device is compliant with the compliance policies that you have defined.
- **Tag**—Tags to enable you to identify devices. Each tag must be separated by a comma.
- **Use Default Browser for SAML**—Whether to enable or disable the default system browser for SAML authentication.

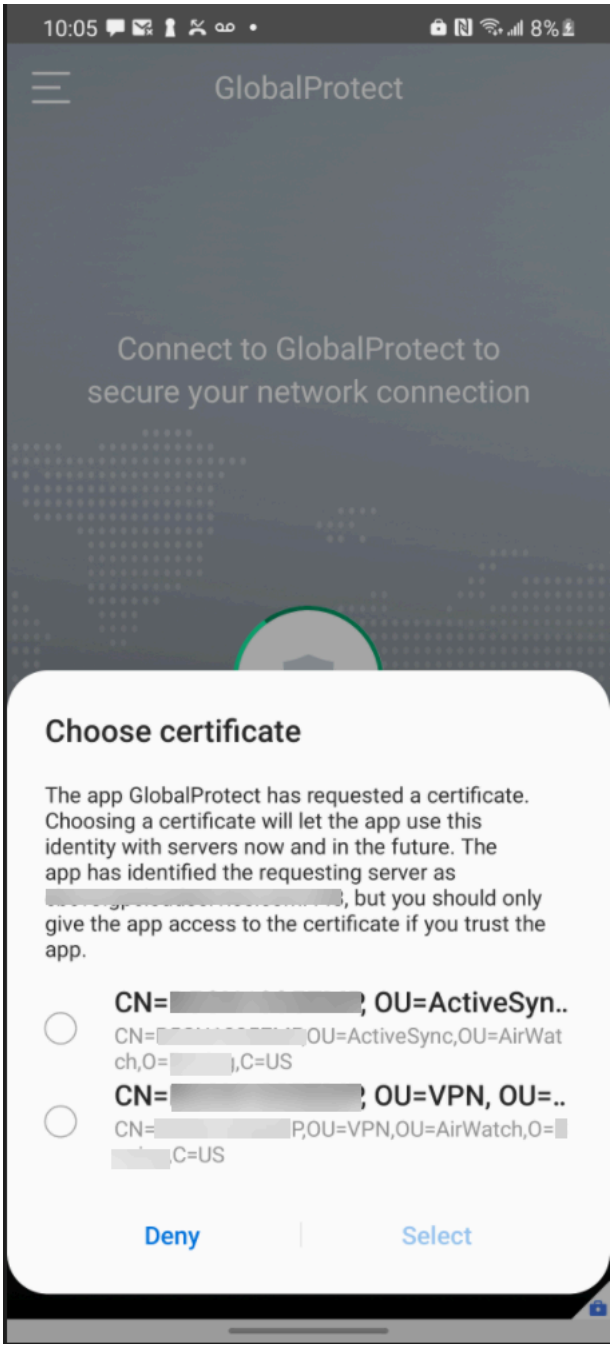


STEP 4 | Click **Create** and then **Save** to preview the assigned devices.

STEP 5 | Click **Publish** to push the App Catalog to the endpoints in the Smart Groups that you assigned.

Delegate GlobalProtect Certificates for Android Endpoints Using Workspace ONE

When you have more than one client certificate available for GlobalProtect client authentication on Android endpoints, the Choose Certificate pop-up prompt appears, prompting GlobalProtect app users to manually select a specific client certificate.



Starting with Android 8 or a later release, you can delegate certificate selection to GlobalProtect app 5.2.5 or a later release. You can use Workspace ONE to grant permission to the GlobalProtect app for certificate delegation as part of the VPN profile that is pushed from the mobile device management (MDM) server. This enables the GlobalProtect app to select a client certificate based on the client certificate alias without first prompting GlobalProtect app users to manually select a certificate on their Android endpoint. As a result, the Choose Certificate pop-up prompt does not

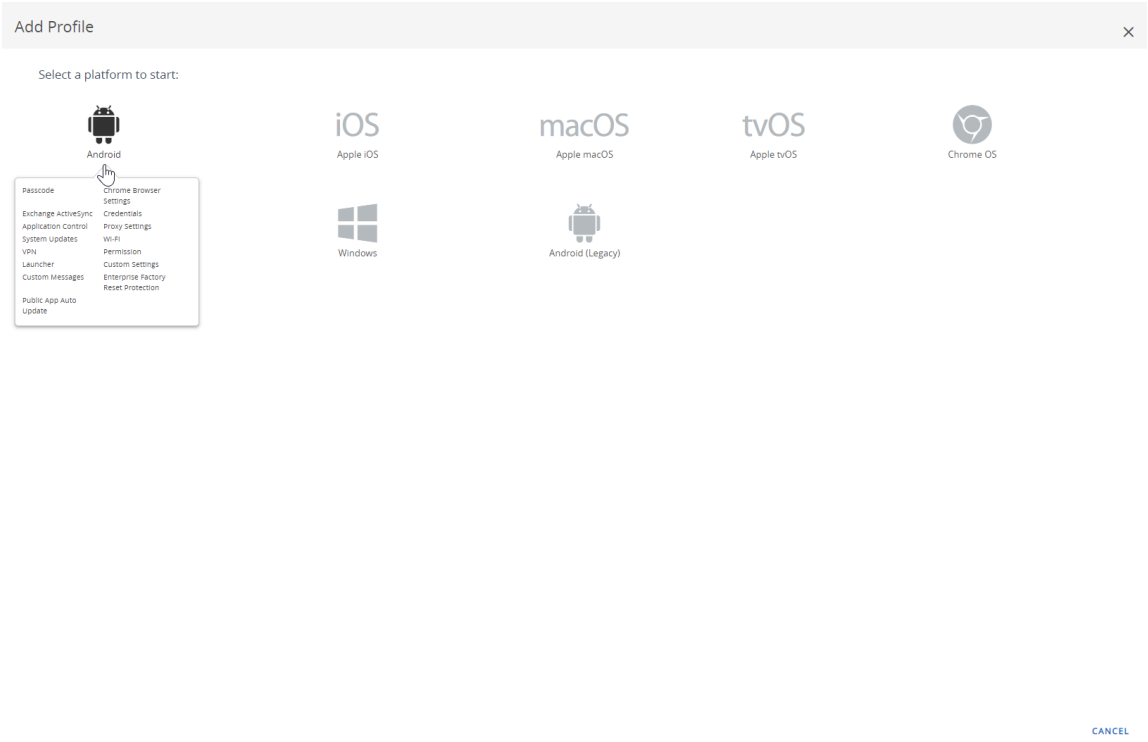
appear on the Android endpoint. If you delegate certificate selection from the MDM server using any other method, the certificates cannot be used by the GlobalProtect app.

STEP 1 | Download the GlobalProtect app for Android.

- Deploy the GlobalProtect Mobile App Using Workspace ONE.
- Download the GlobalProtect app directly from Google Play.

STEP 2 | From the Workspace ONE console, modify an existing Android profile or add a new one.

1. Select **Resources** > **Profiles & Baselines** > **Profiles**, and then **ADD** a new profile.
2. Select **Android** from the platform list.

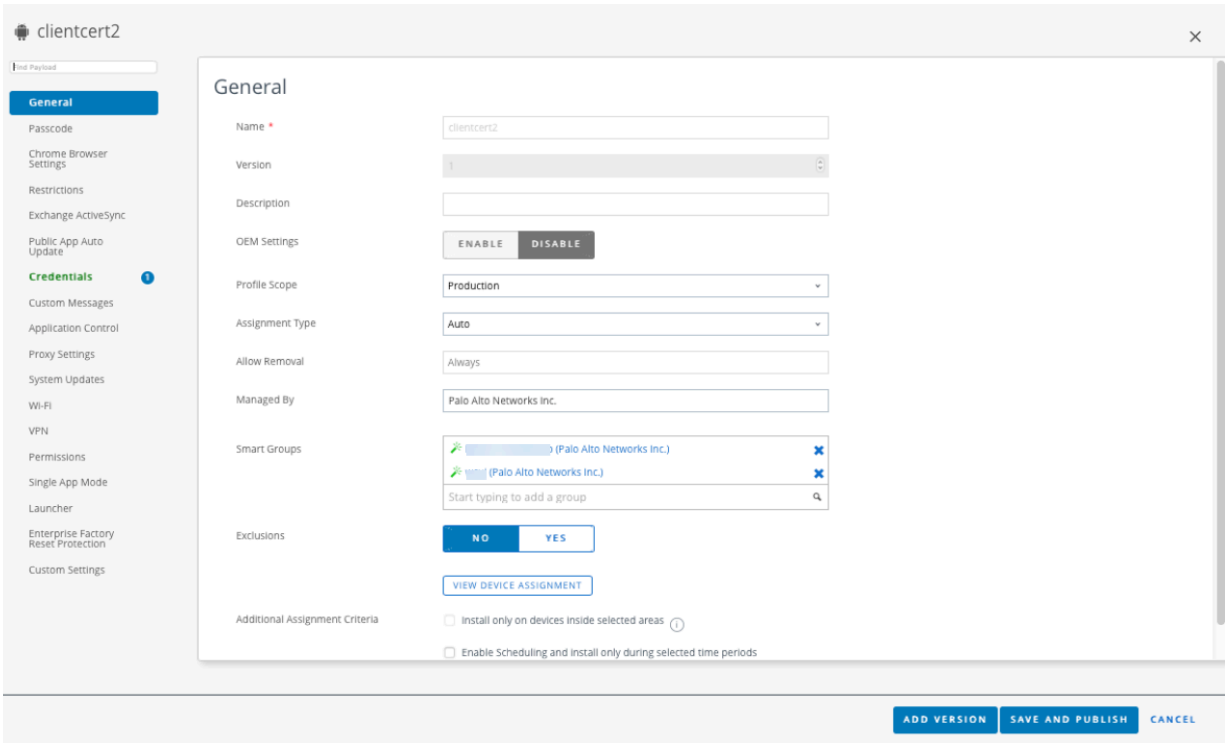


STEP 3 | Configure any of the **General** settings that are appropriate for your company.

Setting	Description
Name	Enter the name of the profile.
Description	Enter a brief description of the profile that indicates its purpose.
OEM Settings	Specify whether to enable or disable the **OEM Settings**.
Profile Scope	Select either **Production**, **Staging**, or **Both**.
Assignment Type	Determine how the profile is deployed to endpoints. Select **Auto** to deploy the profile to

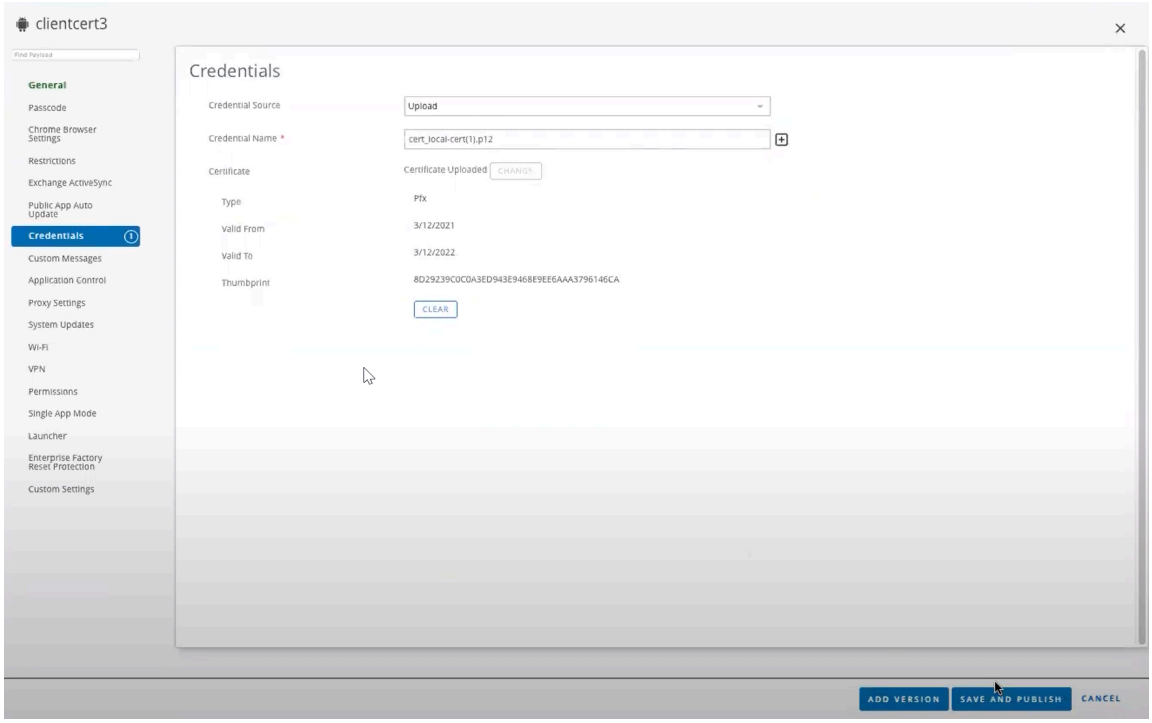
Setting	Description
	all endpoints automatically, **Optional** to enable the end user to install the profile from the Self-Service Portal (SSP) or to manually deploy the profile to individual endpoints, or **Compliance** to deploy the profile when an end user violates a compliance policy applicable to the endpoint.
Allow Removal	Determine whether to remove the profile of the end user. Select **Always** to enable the end user to manually remove the profile at any time, **Never** to prevent the end user from removing the profile, or **With Authorization** to enable the end user to remove the profile with the authorization of the administrator. Choosing **With Authorization** adds a required Password to enter.
Managed By	Enter the Organization Group with administrative access to the profile.
Smart Groups	Add the Smart Groups to which you want the profile added. This field includes an option to create a new Smart Group, which can be configured with specs for minimum OS, device models, ownership categories, organization groups, and more.
Exclusions	Indicate whether you want to include any exclusions. If you select **Yes**, the **Excluded Groups** field displays, enabling you to select the

Setting	Description
	Smart Groups that you wish to exclude from the assignment of this profile.

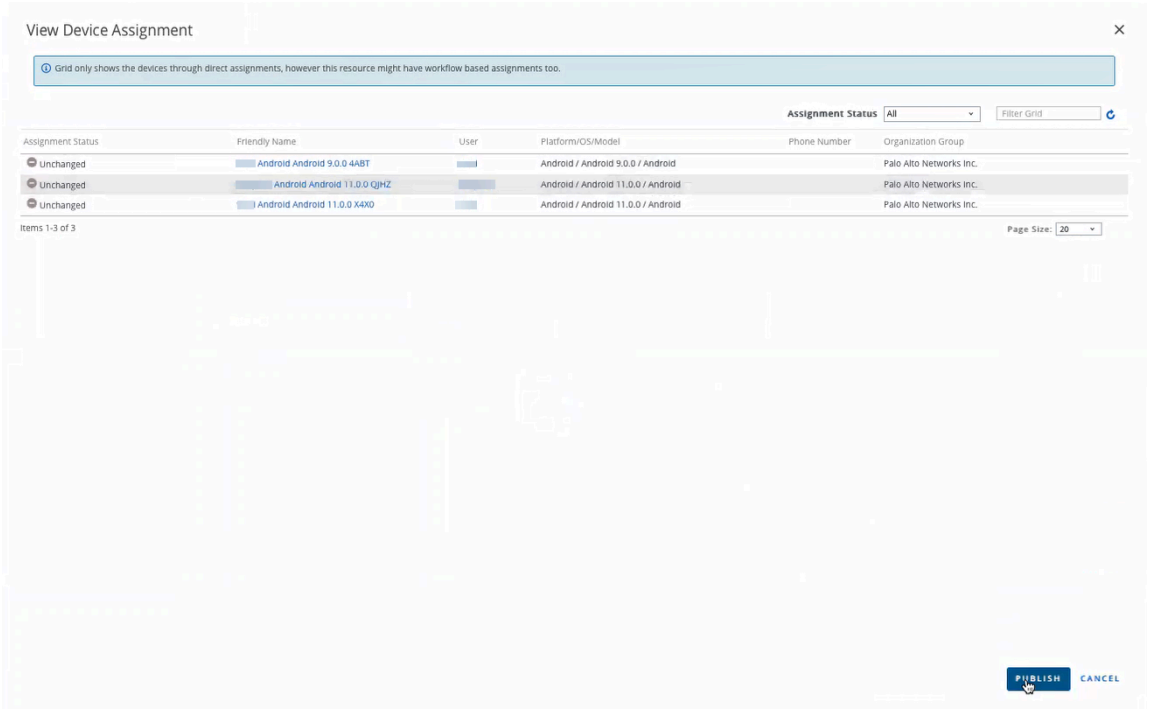


STEP 4 | For your GlobalProtect deployment, configure the **Credentials** settings to upload a client certificate manually and to create a credentials profile:

1. Select **Resources** > **Profiles & Baselines** > **Profiles** > **Add Profile**.
2. Select the **Platform**(**Android**).
3. Select **Credentials**, and then **Configure**.
4. Set the **Credential Source** to **Upload**.
5. Enter a **Credential Name**.
6. Click **UPLOAD** to locate and select the certificate that you want to upload.
7. After you select a certificate, click **SAVE**.
8. Click **SAVE AND PUBLISH** to save your changes.



9. Click **PUBLISH** to push the endpoint to the **Assigned Smart Groups** that will have access to this app.



STEP 5 | Verify the credentials profile and universally unique identifier (UUID) attribute.

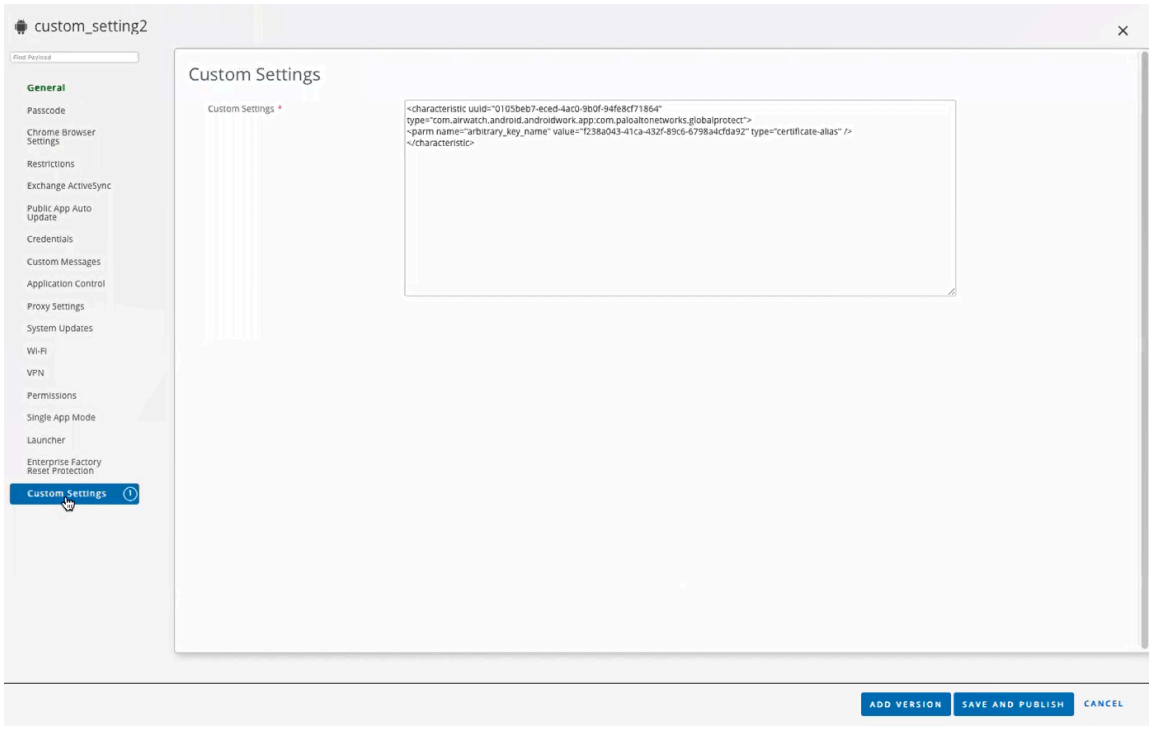
1. Select **Resources** > **Profiles & Baselines** > **Profiles**.
2. Select the radio button next to the new credentials profile you added from the previous step, and then select **</>XML** at the top of the table.

   You can modify the `arbitrary_key_name` and `UUID_from_profile` elements to avoid conflicting parameter and key name settings with existing key value pairs (KVPs) that you applied to a managed configuration file of the GlobalProtect app, as shown in the following sample configuration.

```
<characteristicuuid="0105beb7-eced-4ac0-9b0f-94fe8cf71864"
 type="com.airwatch.android.androidwork.app:your_package_id">
<parm name="arbitrary_key_name" value="UUID_from_profile"
 type="certificate-alias" />
</characteristic>
```


STEP 6 | Create a custom settings profile to suppress certificate selection notifications on the GlobalProtect app for Android endpoints.

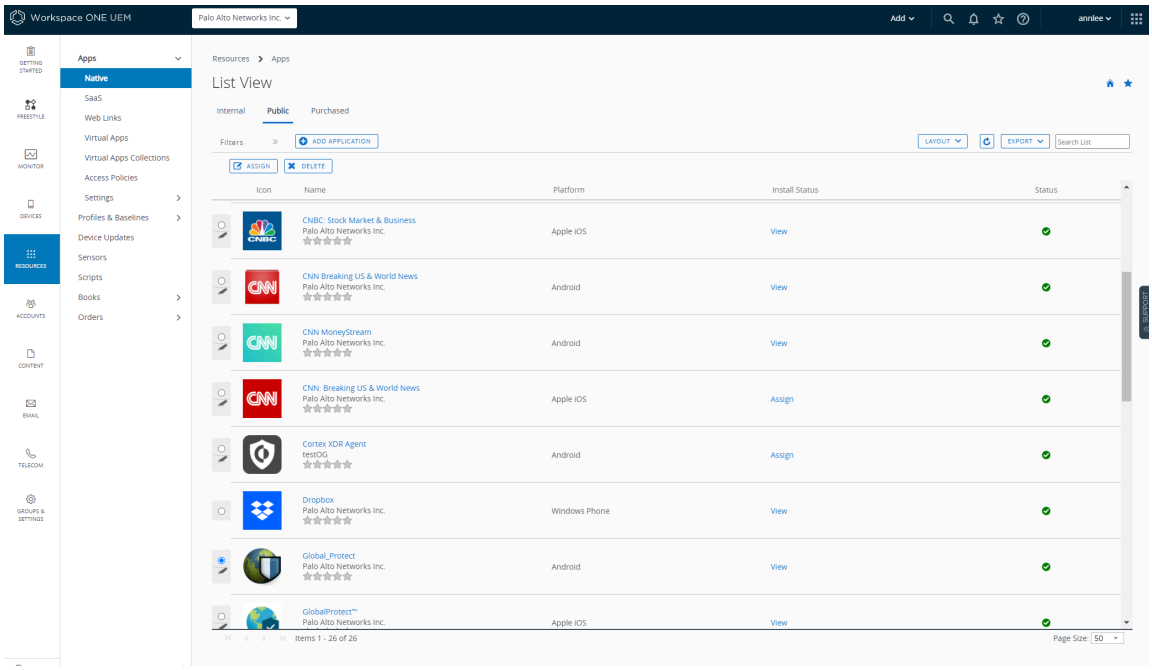
1. Select **Resources** > **Profiles & Baselines** > **Profiles** > **Add Profile**.
2. Select the **Platform** (**Android**).
3. Select **Custom Settings** > **Configure**, and then copy and paste the edited configuration.
4. Click **SAVE AND PUBLISH** to save your changes.



STEP 7 | Configure the VPN profile settings to modify the settings for an existing managed app.

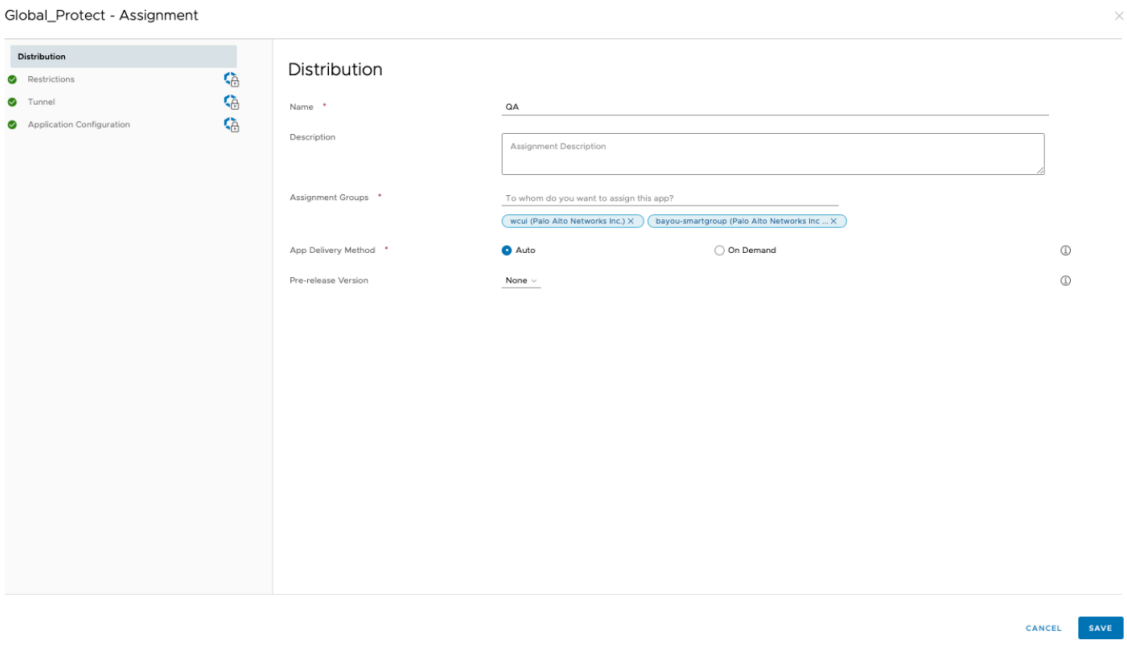
After configuring the settings for the app, you can publish the app to a group of users and Workspace ONE can intercept the certificate selection request to provide the correct certificate to GlobalProtect.

1. Select **Apps** > **Native** > **Public**.
2. To modify the settings for an existing app, locate the app in the list of Public apps (List View) and then select the edit (✎) icon in the actions menu next to the row.

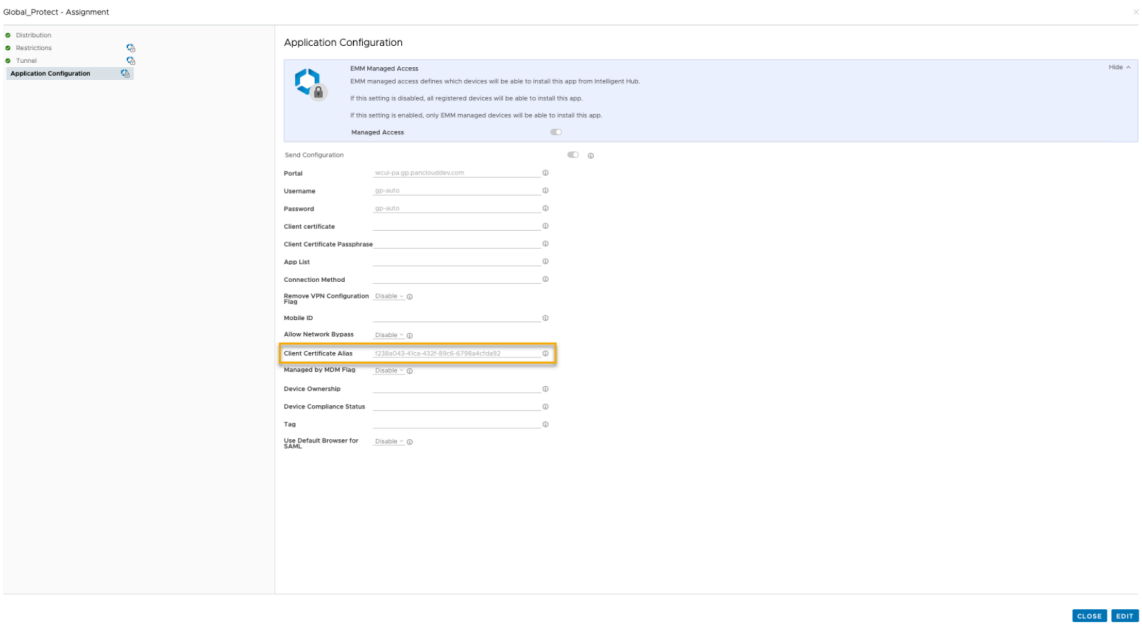


3. Select the existing app from the list of Public apps (List View).
4. Select **Assignment**, and then an existing assignment.

   The **Distribution** window displays the **Assigned Smart Groups** that have access to the GlobalProtect app.



5. Select **Application Configuration**. For details about the other relevant settings in the application configuration that are relevant for your company, see Deploy the GlobalProtect Mobile App Using Workspace ONE.
6. In the **Client Certificate Alias** field, specify the same UUID value that you used for the credential profile. The **Client Certificate Alias** is the unique UUID value used to identify the client certificate during portal or gateway authentication.
7. Click **Edit** to modify the settings.



Deploy the GlobalProtect App for Android on Managed Chromebooks Using Workspace ONE

Starting with GlobalProtect app 5.0, you can deploy the GlobalProtect app for Android on managed Chromebooks that are enrolled with Workspace ONE. After you deploy the app, configure and deploy a VPN profile to set up the GlobalProtect app for end users automatically.

The GlobalProtect app for Android is supported only on certain Chromebooks. Chromebooks that do not support Android applications must continue to run the GlobalProtect app for Chrome, which is not supported starting with GlobalProtect app 5.0 and later.

Do not deploy both the GlobalProtect app for Android and GlobalProtect app for Chrome on the same Chromebook.

Use the following steps to deploy the GlobalProtect app for Android on managed Chromebooks using Workspace ONE:

STEP 1 | Set up the Google Admin console.

The Google Admin console enables you to manage Google services for users in your organization. Workspace ONE uses the Google Admin console for integration with Chromebooks.

1. Log in to the Google Admin console as an administrator.
2. From the console, select **Security** > **Advanced Settings** > **Manage API client access**.
3. In the **Client Name** field, enter the Client ID that was provided to you by Workspace ONE.
4. In the **One or More API Scopes** field, enter the following Google API scopes to which you want to control application access:

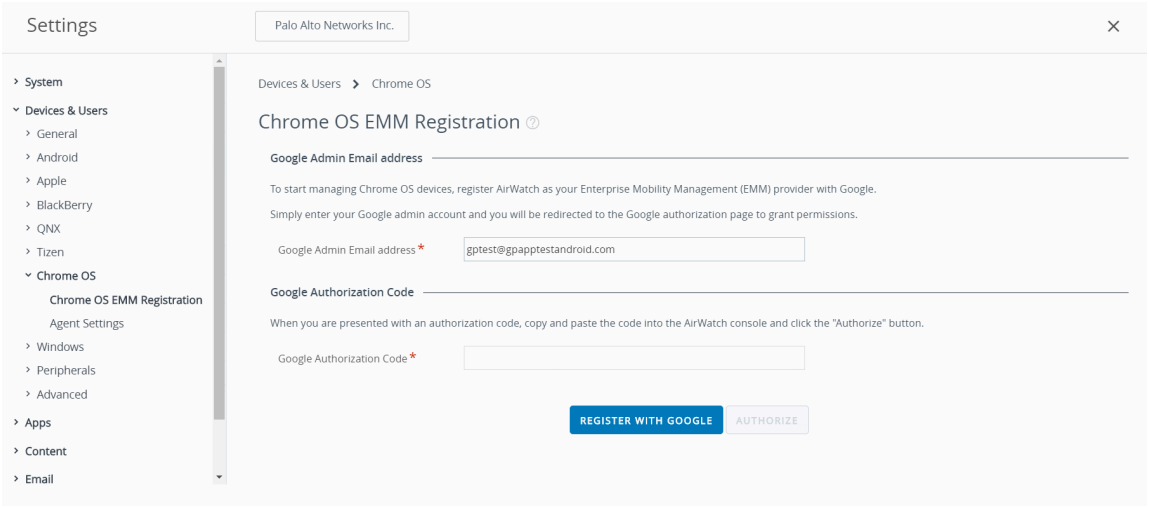
   Each API scope must be separated by a comma.

   - https://www.googleapis.com/auth/chromedevicemanagementapi
   - https://www.googleapis.com/auth/admin.directory.user
   - https://www.googleapis.com/auth/admin.directory.device.chromeos
5. Click **Authorize**.
6. Enable **Chrome Management - Partner Access** for device policies (**Device Management** > **Device Settings** > **Chrome Management** > **Device Settings**) and user policies (**Device Management** > **Device Settings** > **Chrome Management** > **User Settings**).

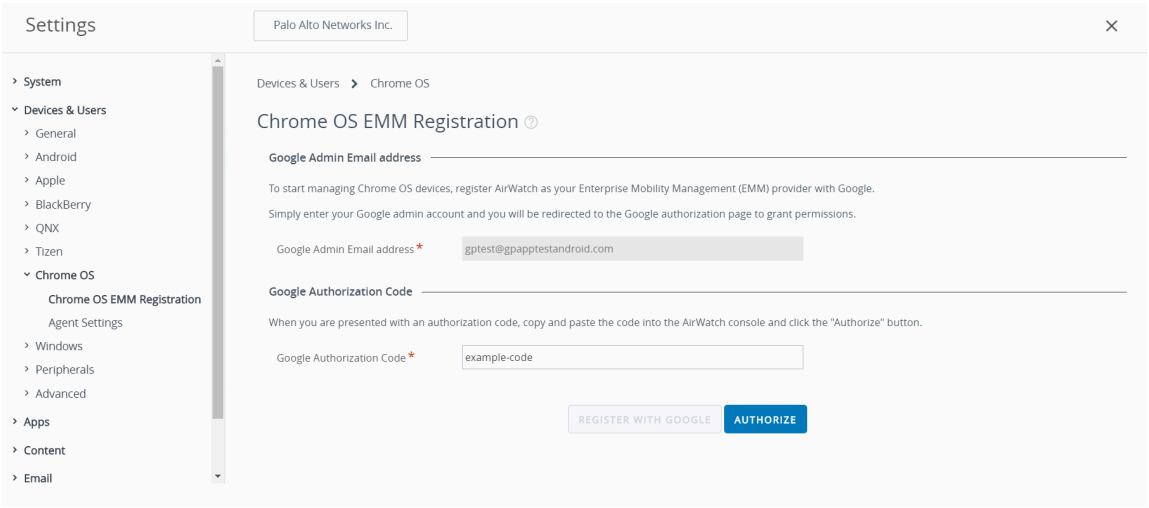
STEP 2 | Register Workspace ONE as your Enterprise Mobility Management (EMM) provider for Google.

To manage Chromebooks using Workspace ONE, you must register Workspace ONE with the Google Admin console.

1. Log in to your Workspace ONE console.
2. Select **Devices** > **Devices Settings** > **Devices & Users** > **Chrome OS** > **Chrome OS EMM Registration**.
3. Enter the **Google Admin Email address** that you used to access the Google Admin console.
4. Click **REGISTER WITH GOOGLE**. You will be redirected to the Google authorization page, where you can obtain a Google authorization code.



5. Enter the **Google Authorization Code** that you obtained from the Google authorization page.
6. Click **AUTHORIZE** to complete the registration.



STEP 3 | Enroll Chromebooks with Workspace ONE.

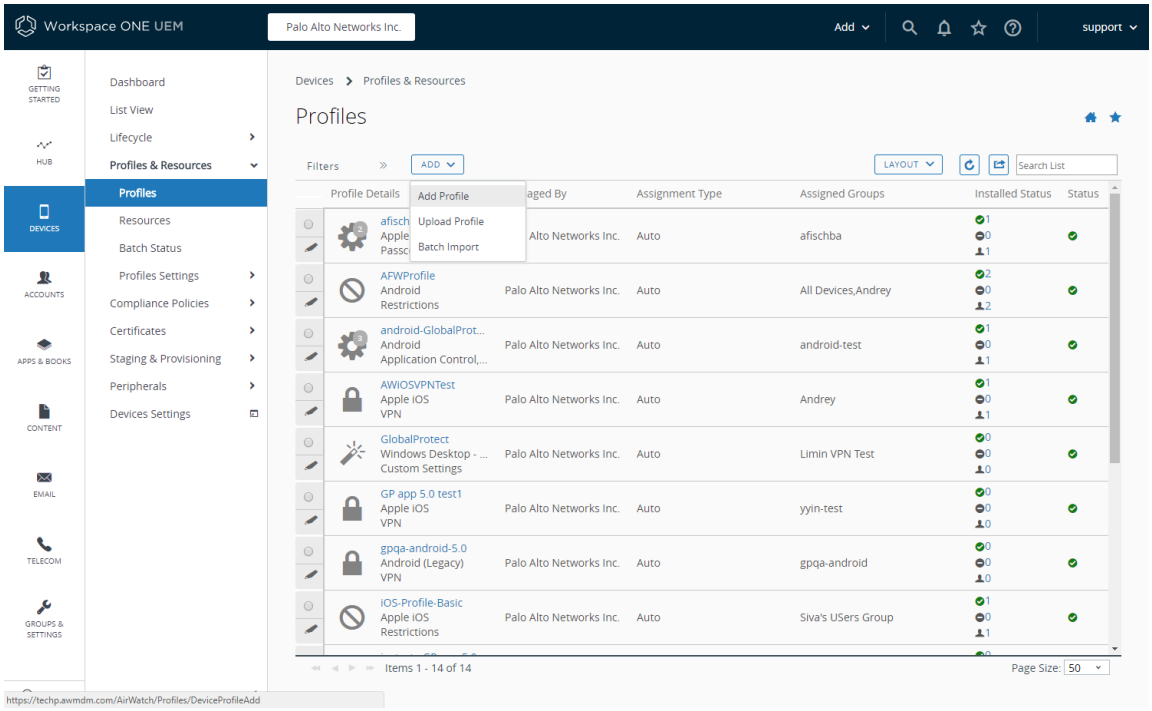
Before you can begin managing Chromebooks using Workspace ONE, you must enroll and sync your Chromebooks to Workspace ONE.

1. From your Chromebook, press **CTRL+ALT+E** to open the enterprise enrollment screen.
2. Enter the username and password from your Google Admin welcome letter or enter your existing G Suite user credentials.
3. Click **Enroll device**. You will receive a confirmation message when the Chromebook is successfully enrolled.
4. Log in to your Workspace ONE console.
5. Select **Devices** > **Devices Settings & Users** > **Chrome OS** > .
6. Click **Device Sync** to sync all enrolled Chromebooks to Workspace ONE.

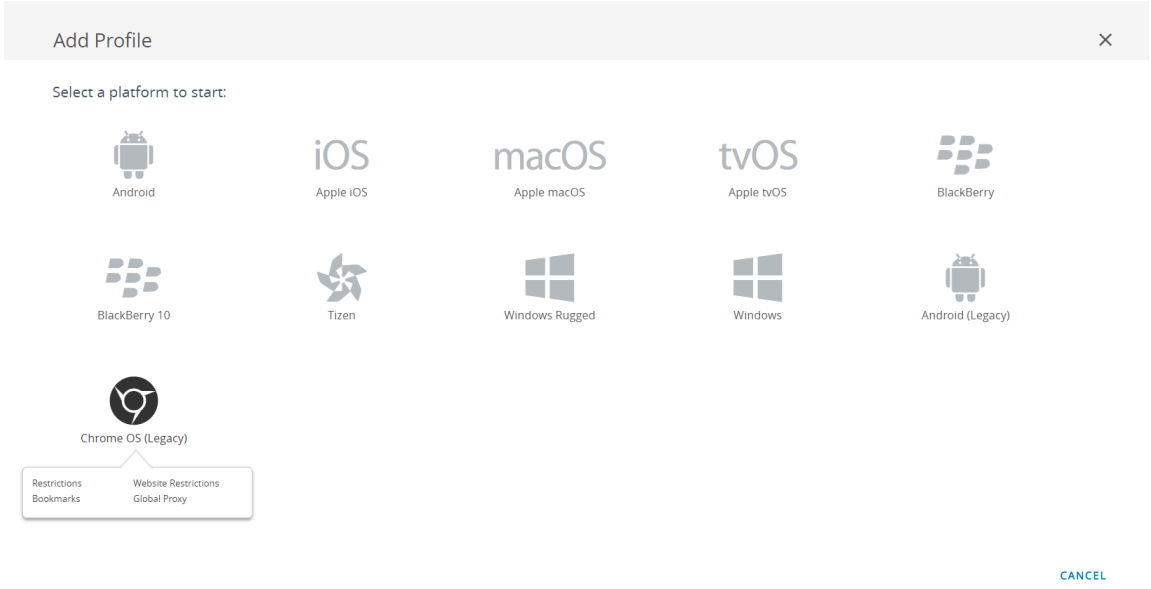
STEP 4 | Add the GlobalProtect app for Android to a Chrome OS profile on Workspace ONE.

The **Application Control** profile enables you to add apps from Google Play and the Chrome Web Store.

1. Log in to your Workspace ONE console.
2. Select **Devices** > **Profiles & Resources** > **Profiles** to **ADD** a new Chrome OS profile.

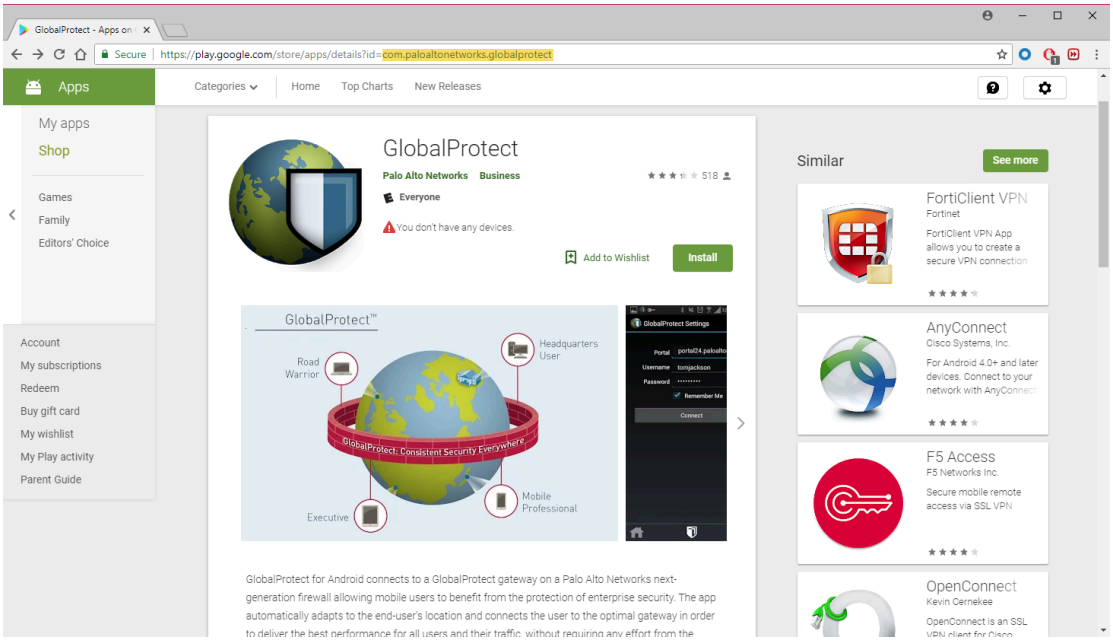


3. Select **Chrome OS (Legacy)** from the platform list.



4. Configure the **General** settings.
5. Configure the **Application Control** settings.

1. Enter the GlobalProtect **App ID** displayed in the Google Play URL (com.paloaltonetworks.globalprotect).



2. Enter the app **Name**.
3. Specify whether you want to **Pin App to Shelf**. Enter **Y** to pin the app to the Chromebook app shelf.
4. **SAVE & PUBLISH** your changes.

Configure Workspace ONE for iOS Endpoints

Refer to the following sections for information on how to set up VPN configurations for iOS endpoints using Workspace ONE:

- Configure an Always On VPN Configuration for iOS Endpoints Using Workspace ONE
- Configure a User-Initiated Remote Access VPN Configuration for iOS Endpoints Using Workspace ONE
- Configure a Per-App VPN Configuration for iOS Endpoints Using Workspace ONE

Configure an Always On VPN Configuration for iOS Endpoints Using Workspace ONE

In an Always On VPN configuration, the secure GlobalProtect connection is always on. Traffic that matches specific filters (such as port and IP address) configured on the GlobalProtect gateway is always routed through the VPN tunnel.

Use the following steps to configure an Always On VPN configuration for iOS endpoints using Workspace ONE:

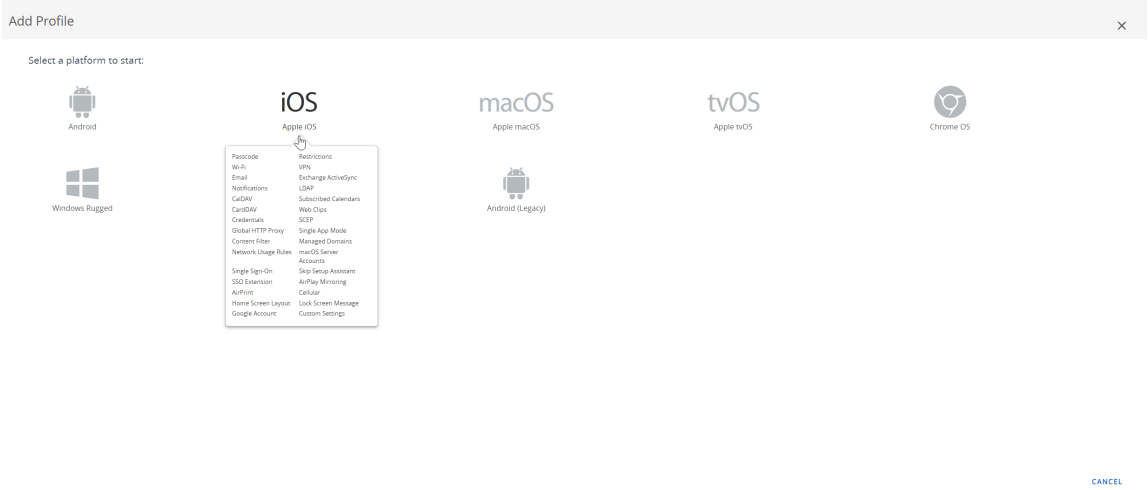
STEP 1 | Download the GlobalProtect app for iOS.

- Deploy the GlobalProtect Mobile App Using Workspace ONE.
- Download the GlobalProtect app directly from the App Store.

The GlobalProtect app for iOS is also available in the Apple App Store in China.

STEP 2 | From the Workspace ONE console, modify an existing Apple iOS profile or add a new one.

1. Select **Resources** > **Profiles & Baselines** > **Profiles** > **ADD**, and then **Add Profile**.
2. Select **iOS** from the platform list.



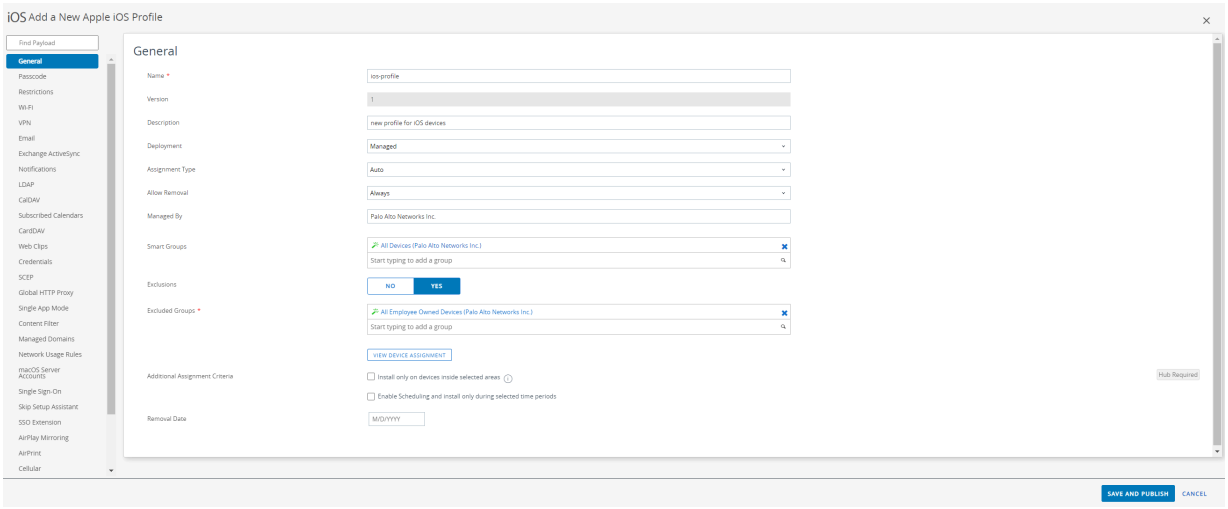
3. Select **Device Profile** from the **Select Context** window.

STEP 3 | Configure the **General** settings:

1. Enter a **Name** for the profile.
2. (Optional) Enter a brief **Description** of the profile that indicates its purpose.
3. (Optional) Select the **Deployment** method, which indicates whether the profile will be removed automatically upon unenrollment—either **Managed** (the profile is removed) or **Manual** (the profile remains installed until it is removed by the end user).
4. (Optional) Select an **Assignment Type** to determine how the profile is deployed to endpoints. Select **Auto** to deploy the profile to all endpoints automatically, **Optional** to enable the end user to install the profile from the Self-Service Portal (SSP) or to manually deploy the profile to individual endpoints, or **Compliance** to deploy the profile when an end user violates a compliance policy applicable to the endpoint.
5. (Optional) Select whether or not you want to **Allow Removal** of the profile by the end user. Select **Always** to enable the end user to manually remove the profile at any time, **Never** to prevent the end user from removing the profile, or **With Authorization** to enable the end user to remove the profile with the authorization of the administrator. Choosing **With Authorization** adds a required Password.
6. (Optional) In the **Managed By** field, enter the Organization Group with administrative access to the profile.
7. (Optional) In the **Assigned Groups** field, add the Smart Groups to which you want the profile added. This field includes an option to create a new Smart Group, which can be

configured with specs for minimum OS, device models, ownership categories, organization groups, and more.

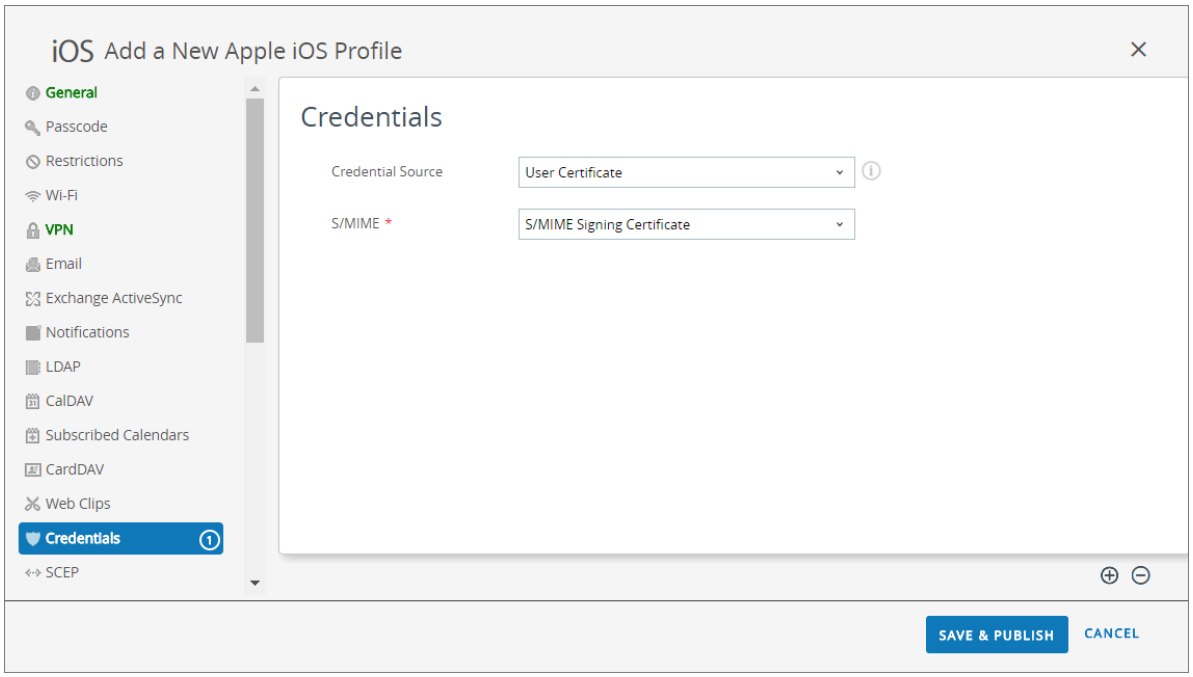
8. (Optional) Indicate whether you want to include any **Exclusions** to the assignment of this profile. If you select **Yes**, the **Excluded Groups** field displays, enabling you to select the Smart Groups that you wish to exclude from the assignment of this profile.
9. (Optional) If you enable the option to **Install only on devices inside selected areas**, the profile can be installed only on endpoints in specified geofence or iBeacon regions. When prompted, add the geofence or iBeacon regions in the **Assigned Geofence Areas** field.
10. (Optional) If you **Enable Scheduling and install only during selected time periods**, you can apply a time schedule (**Devices** > **Profiles & Resources** > **Profiles Settings** > **Time Schedules**) to the profile installation, which limits the periods of time during which the profile can be installed on endpoints. When prompted, enter the schedule name in the **Assigned Schedules** field.
11. (Optional) Select the **Removal Date** on which you want the profile to be removed from all endpoints.



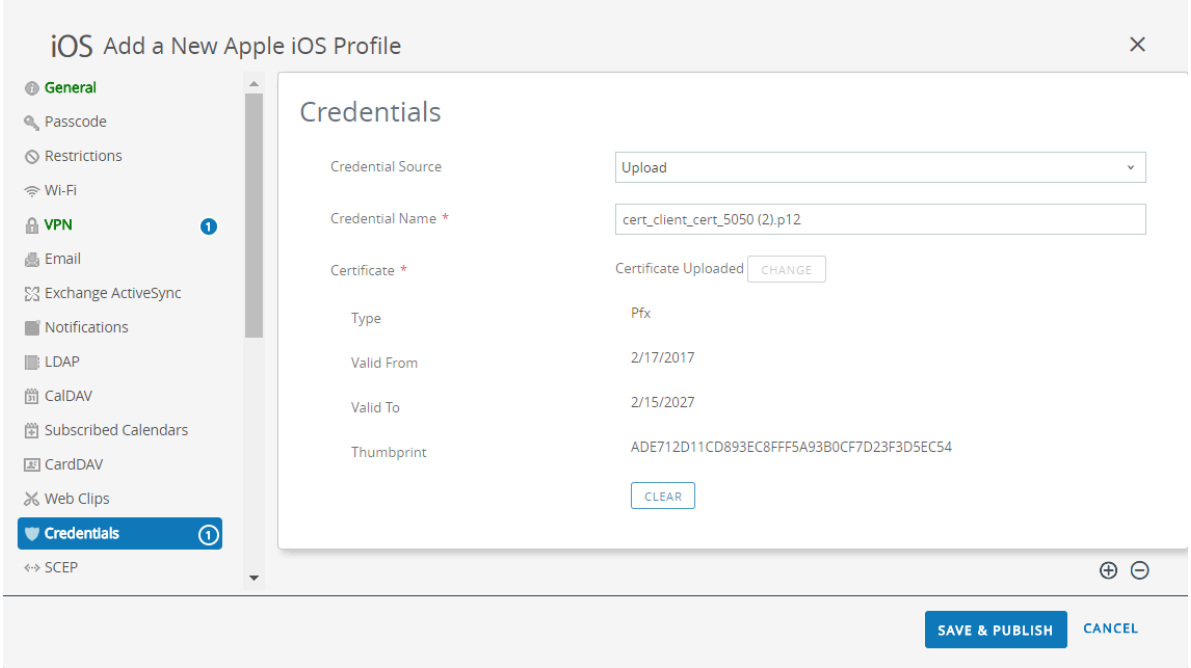
STEP 4 | (Optional) If your GlobalProtect deployment requires client certificate authentication, configure the **Credentials** settings:

Starting with iOS 12, if you want to use client certificates for GlobalProtect client authentication, you must deploy the client certificates as part of the VPN profile that is pushed from the MDM server. If you deploy client certificates from the MDM server using any other method, the certificates cannot be used by the GlobalProtect app.

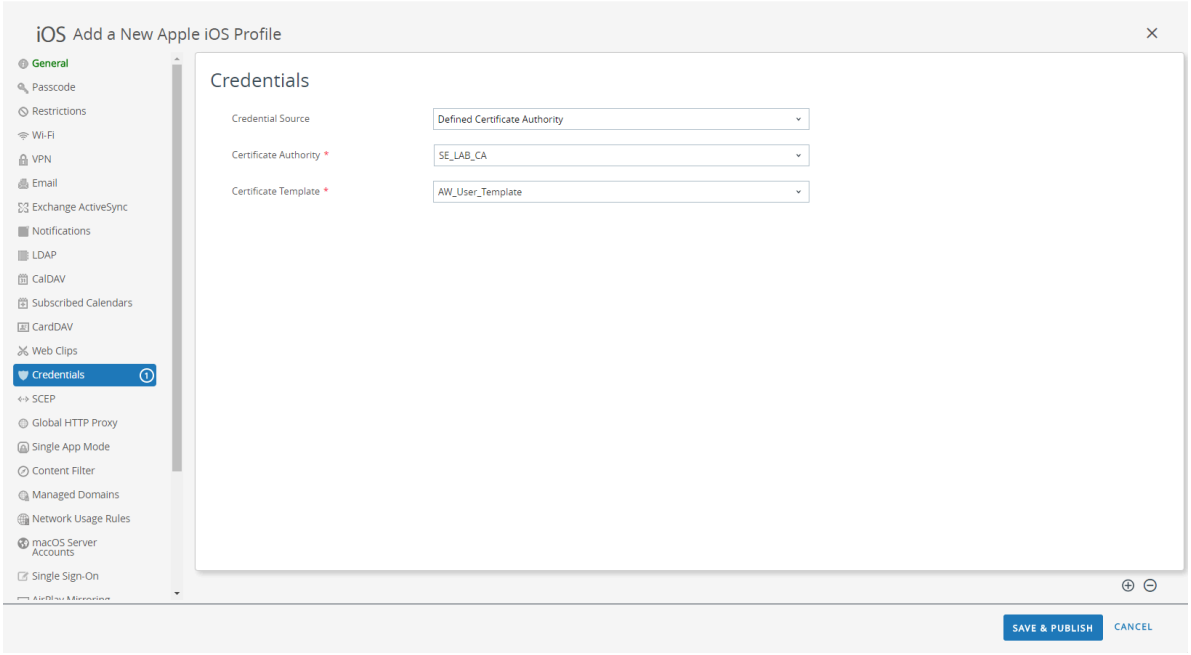
- To pull client certificates from Workspace ONE users:
  1. Set the **Credential Source** to **User Certificate**.
  2. Select the **S/MIME Signing Certificate** (default).



- To upload a client certificate manually:
  1. Set the **Credential Source** to **Upload**.
  2. Enter a **Credential Name**.
  3. Click **UPLOAD** to locate and select the certificate that you want to upload.
  4. After you select a certificate, click **SAVE**.



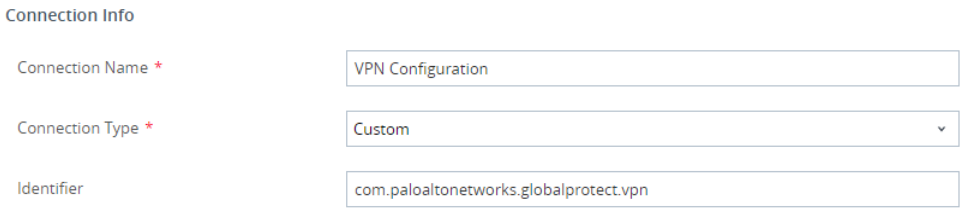
- To use a predefined certificate authority and template:
  1. Set the **Credential Source** to **Defined Certificate Authority**.
  2. Select the **Certificate Authority** from which you want obtain certificates.
  3. Select the **Certificate Template** for the certificate authority.



STEP 5 | Configure the **VPN** settings:

1. Enter the **Connection Name** that the endpoint displays.
2. Select the network **Connection Type**:
   - For GlobalProtect app 4.1.x and earlier releases, select **Palo Alto Networks GlobalProtect**.
   - For GlobalProtect app 5.0 and later releases, select **Custom**.
3. (Optional) If you set the **Connection Type** to **Custom**, enter the bundle ID (**com.paloaltonetworks.globalprotect.vpn**) in the **Identifier** field to identify the GlobalProtect app.

   *If you downloaded the GlobalProtect app directly from the Apple App Store in China, enter the bundle ID (**com.paloaltonetworks.globalprotect.vpncn**) in the **Identifier** field.*



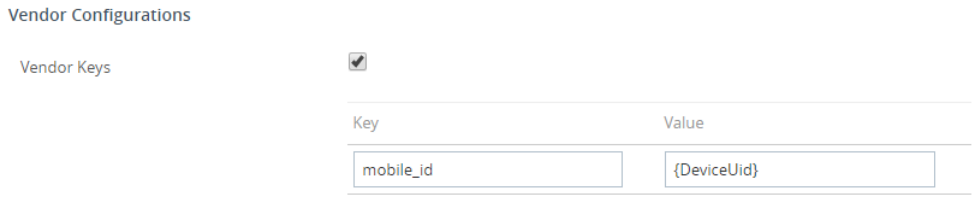
4. In the **Server** field, enter the hostname or IP address of the GlobalProtect portal to which users connect.
5. (Optional) Enter the username of the VPN **Account** or click the add (**+**) button to view supported lookup values that you can insert.
6. (Optional) In the **Disconnect on idle** field, specify the amount of time (in seconds) at which an endpoint logs out of the GlobalProtect app after the app stops routing traffic through the VPN tunnel.
7. In the Authentication area, select a user **Authentication** method: **Password**, **Certificate**, **Password + Certificate**.
8. When prompted, enter a **Password** and/or select the **Identity Certificate** that GlobalProtect will use to authenticate users. The **Identity Certificate** is the same certificate that you configured in the **Credentials** settings.
9. **Enable VPN On Demand** and **Use new on demand keys** .
10. Configure an on-demand rule with **Action: Connect**.
11. (Optional) Select the **Proxy** type and configure the relevant settings.

STEP 6 | (Optional) (starting with GlobalProtect app 5.0) If your GlobalProtect deployment requires Configure Windows User-ID Agent to Collect Host Information, specify the unique device identifier (UDID) attribute.

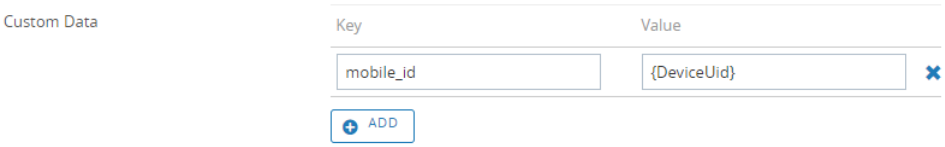
GlobalProtect supports integration with MDM to obtain mobile device attributes from the MDM server for use in HIP-based policy enforcement. In order for the MDM integration to work, the GlobalProtect app must present the UDID of the endpoint to the GlobalProtect gateway. The UDID attribute enables the GlobalProtect app to retrieve and use UDID information in MDM-based deployments. If you remove the UDID attribute from the profile,

you can no longer use the MDM integration. The GlobalProtect app generates a new UDID, but it cannot be used for the integration.

- If you are using the **Palo Alto Networks GlobalProtect** network **Connection Type**, go to the **VPN** settings and enable **Vendor Keys** in the Vendor Configurations area. Set the **Key** to **`mobile_id`** and the **Value** to **`{DeviceUid}`**.



- If you are using the **Custom** network **Connection Type**, go to the **VPN** settings and **ADD Custom Data** in the Connection Info area. Set the **Key** to **`mobile_id`** and the **Value** to **`{DeviceUid}`**.



STEP 7 | **SAVE & PUBLISH** your changes.

Configure a User-Initiated Remote Access VPN Configuration for iOS Endpoints Using Workspace ONE

In a remote access (On-Demand) VPN configuration, users must manually launch the app to establish the secure GlobalProtect connection. Traffic that matches specific filters (such as port and IP address) configured on the GlobalProtect gateway is routed through the VPN tunnel only after users initiate and establish the connection.

Use the following steps to configure a user-initiated remote access VPN configuration for iOS endpoints using Workspace ONE:

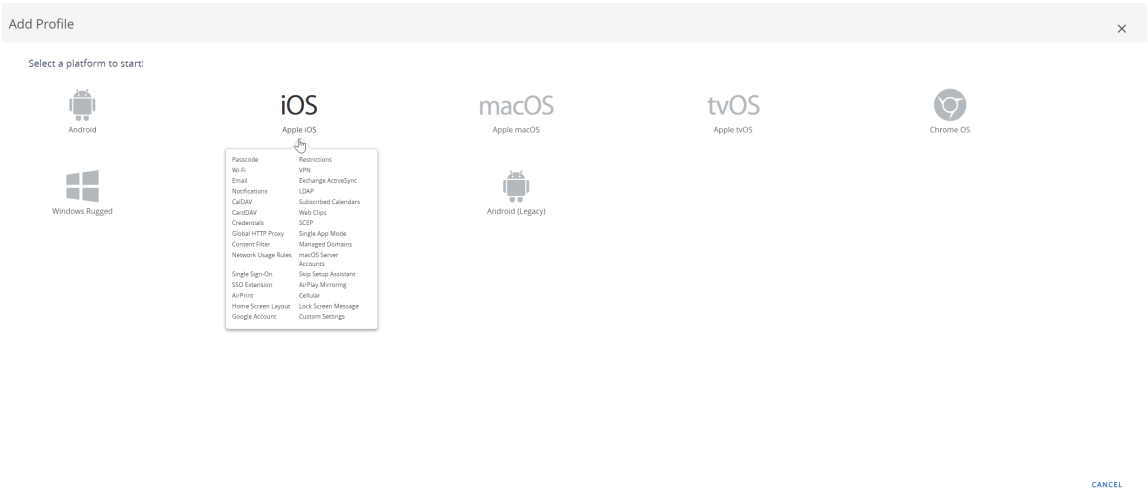
STEP 1 | Download the GlobalProtect app for iOS.

- Deploy the GlobalProtect Mobile App Using Workspace ONE.
- Download the GlobalProtect app directly from the App Store.

The GlobalProtect app for iOS is also available in the Apple App Store in China.

STEP 2 | From the Workspace ONE console, modify an existing Apple iOS profile or add a new one.

1. Select **Devices** > **Profiles & Resources** > **Profiles**, and then **ADD** a new profile.
2. Select **iOS** from the platform list.

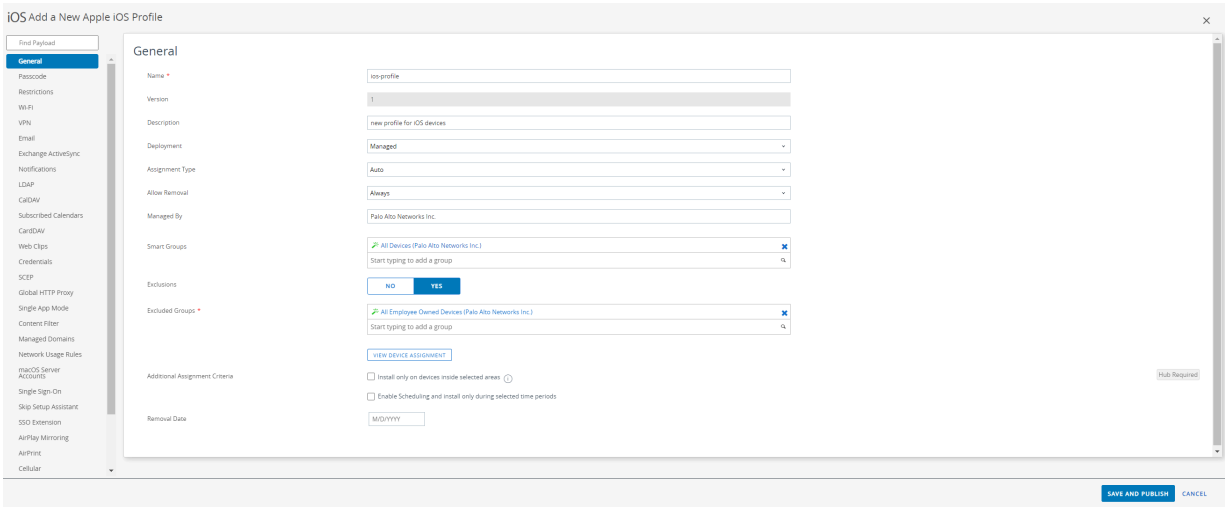


STEP 3 | Configure the **General** settings:

1. Enter a **Name** for the profile.
2. (Optional) Enter a brief **Description** of the profile that indicates its purpose.
3. (Optional) Select the **Deployment** method, which indicates whether the profile will be removed automatically upon unenrollment—either **Managed** (the profile is removed) or **Manual** (the profile remains installed until it is removed by the end user).
4. (Optional) Select an **Assignment Type** to determine how the profile is deployed to endpoints. Select **Auto** to deploy the profile to all endpoints automatically, **Optional** to enable the end user to install the profile from the Self-Service Portal (SSP) or to manually deploy the profile to individual endpoints, or **Compliance** to deploy the profile when an end user violates a compliance policy applicable to the endpoint.
5. (Optional) Select whether or not you want to **Allow Removal** of the profile by the end user. Select **Always** to enable the end user to manually remove the profile at any time, **Never** to prevent the end user from removing the profile, or **With Authorization** to enable the end user to remove the profile with the authorization of the administrator. Choosing **With Authorization** adds a required Password.
6. (Optional) In the **Managed By** field, enter the Organization Group with administrative access to the profile.
7. (Optional) In the **Assigned Groups** field, add the Smart Groups to which you want the profile added. This field includes an option to create a new Smart Group, which can be

configured with specs for minimum OS, device models, ownership categories, organization groups, and more.

8. (Optional) Indicate whether you want to include any **Exclusions** to the assignment of this profile. If you select **Yes**, the **Excluded Groups** field displays, enabling you to select the Smart Groups that you wish to exclude from the assignment of this profile.
9. (Optional) If you enable the option to **Install only on devices inside selected areas**, the profile can be installed only on endpoints in specified geofence or iBeacon regions. When prompted, add the geofence or iBeacon regions in the **Assigned Geofence Areas** field.
10. (Optional) If you **Enable Scheduling and install only during selected time periods**, you can apply a time schedule (**Devices** > **Profiles & Resources** > **Profiles Settings** > **Time Schedules**) to the profile installation, which limits the periods of time during which the profile can be installed on endpoints. When prompted, enter the schedule name in the **Assigned Schedules** field.
11. (Optional) Select the **Removal Date** on which you want the profile to be removed from all endpoints.

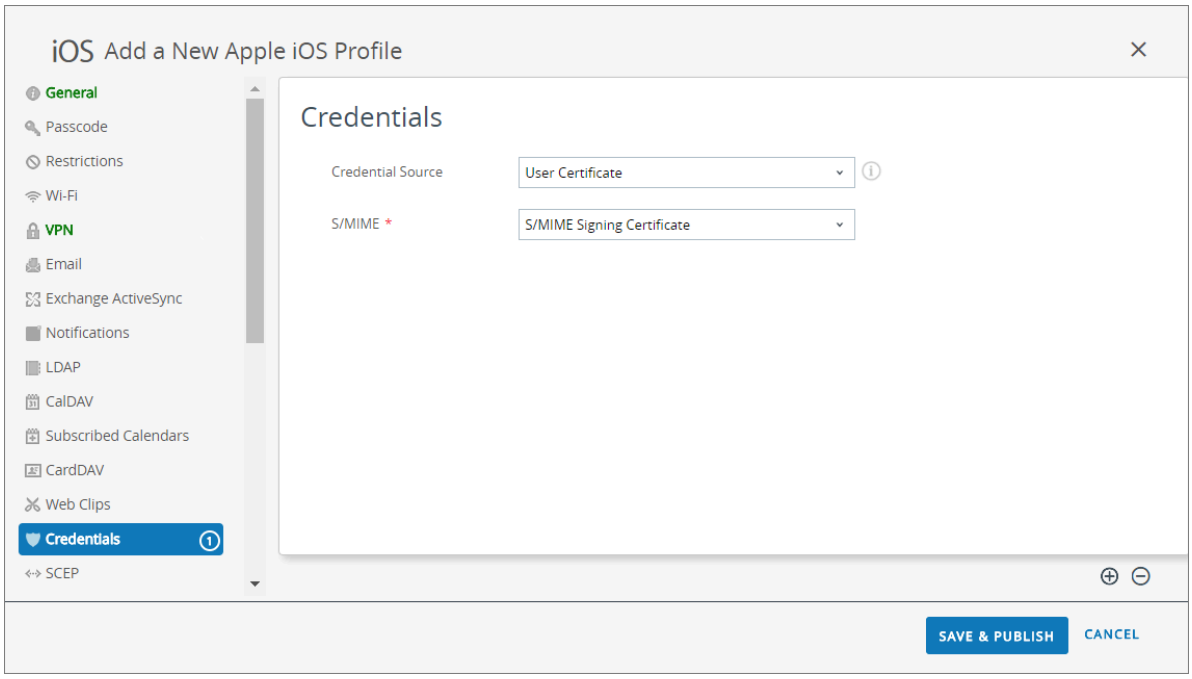


STEP 4 | Configure the **Credentials** settings:

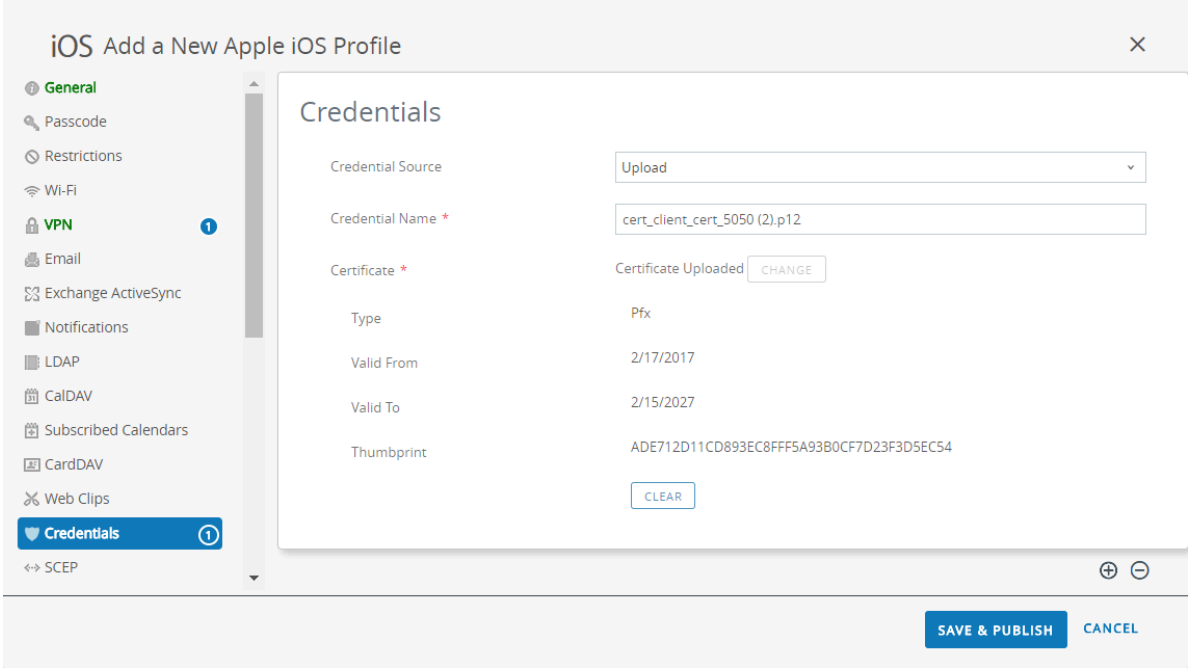
All remote access VPN configurations for iOS endpoints require certificate-based authentication.

Starting with iOS 12, if you want to use client certificates for GlobalProtect client authentication, you must deploy the client certificates as part of the VPN profile that is pushed from the MDM server. If you deploy client certificates from the MDM server using any other method, the certificates cannot be used by the GlobalProtect app.

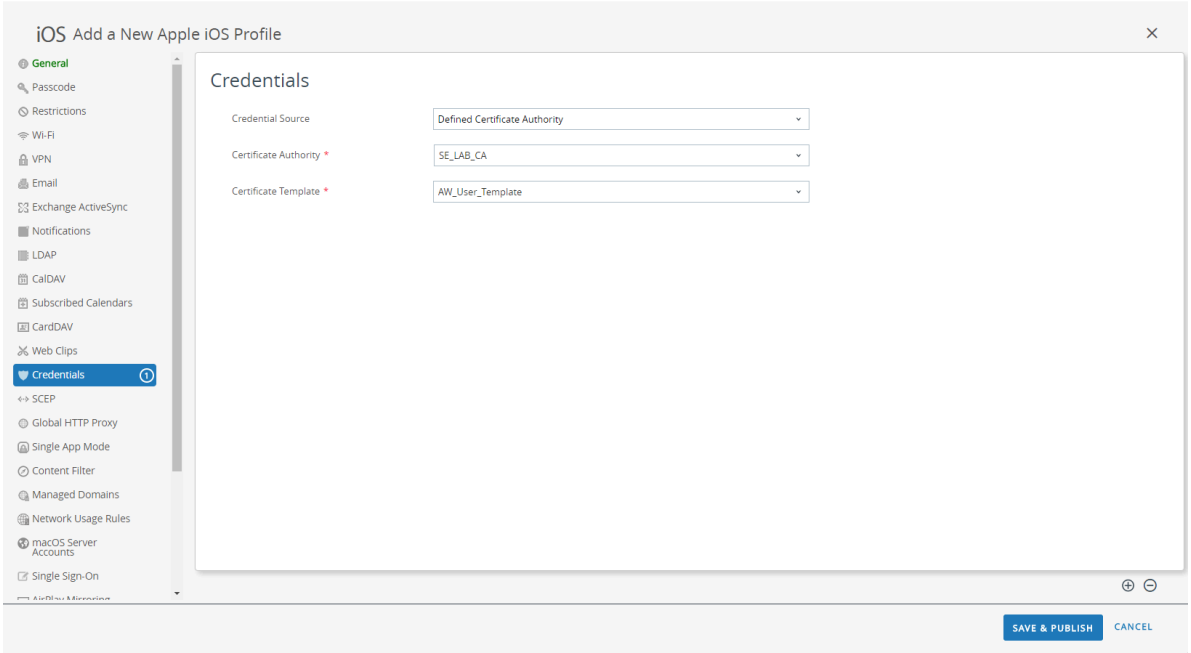
- To pull client certificates from Workspace ONE users:
  1. Set the **Credential Source** to **User Certificate**.
  2. Select the **S/MIME Signing Certificate** (default).



- To upload a client certificate manually:
  1. Set the **Credential Source** to **Upload**.
  2. Enter a **Credential Name**.
  3. Click **UPLOAD** to locate and select the certificate that you want to upload.
  4. After you select a certificate, click **SAVE**.



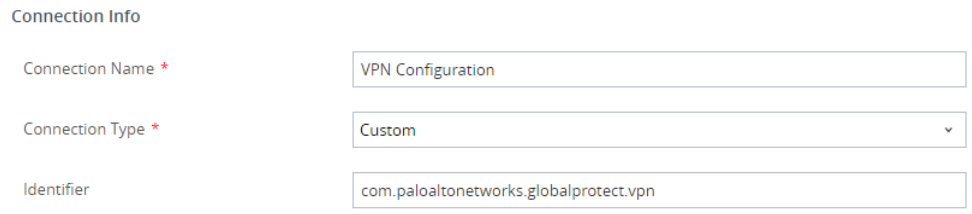
- To use a predefined certificate authority and template:
  1. Set the **Credential Source** to **Defined Certificate Authority**.
  2. Select the **Certificate Authority** from which you want obtain certificates.
  3. Select the **Certificate Template** for the certificate authority.



STEP 5 | Configure the **VPN** settings:

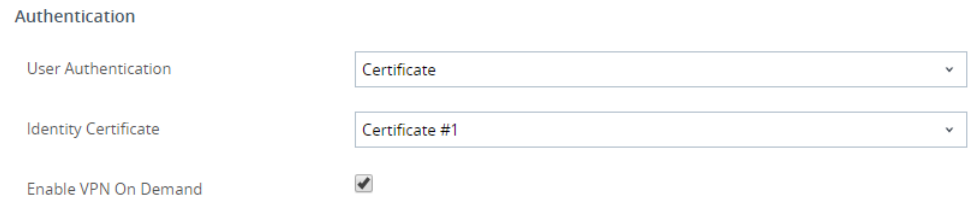
1. Enter the **Connection Name** that the endpoint displays.
2. Select the network **Connection Type**:
   - For GlobalProtect app 4.1.x and earlier releases, select **Palo Alto Networks GlobalProtect**.
   - For GlobalProtect app 5.0 and later releases, select **Custom**.
3. (Optional) If you set the **Connection Type** to **Custom**, enter the bundle ID (**com.paloaltonetworks.globalprotect.vpn**) in the **Identifier** field to identify the GlobalProtect app.

   *If you downloaded the GlobalProtect app directly from the Apple App Store in China, enter the bundle ID (**com.paloaltonetworks.globalprotect.vpncn**) in the **Identifier** field.*



4. In the **Server** field, enter the hostname or IP address of the GlobalProtect portal to which users connect.
5. (Optional) Enter the username of the VPN **Account** or click the add (**+**) button to view supported lookup values that you can insert.
6. (Optional) In the **Disconnect on idle** field, specify the amount of time (in seconds) at which an endpoint logs out of the GlobalProtect app after the app stops routing traffic through the VPN tunnel.
7. In the Authentication area, set the user **Authentication** method to **Certificate**.

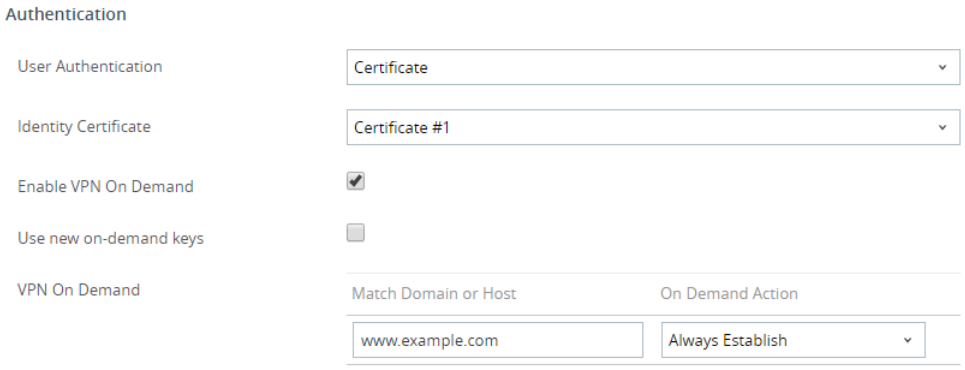
   All remote access VPN configurations for iOS endpoints require certificate-based authentication.
8. When prompted, select the **Identity Certificate** that GlobalProtect will use to authenticate users. The **Identity Certificate** is the same certificate that you configured in the **Credentials** settings.
9. Ensure that the **Enable VPN On Demand** option is enabled (default setting).



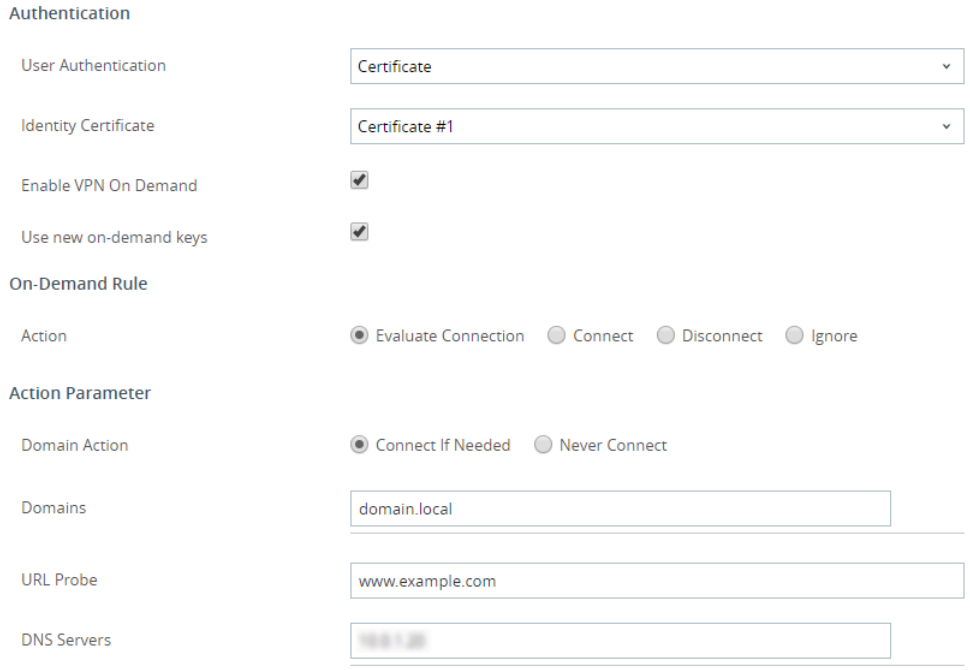
10. (Optional) Configure legacy **VPN On-Demand** connection rules:

- **Match Domain or Host**—Enter the domain or hostname that triggers the GlobalProtect connection to establish when accessed by users.
- **On Demand Action**—Set the **On Demand Action** to **Establish if Needed** or **Always Establish** to establish the GlobalProtect connection only if users cannot reach the specified domain or hostname directly. Set the **On Demand Action** to **Never Establish** to

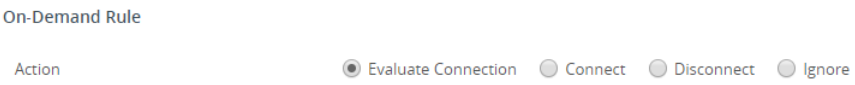
prevent the GlobalProtect connection from establishing when users access the specified domain or hostname. If the connection is already established, it can continue to be used.



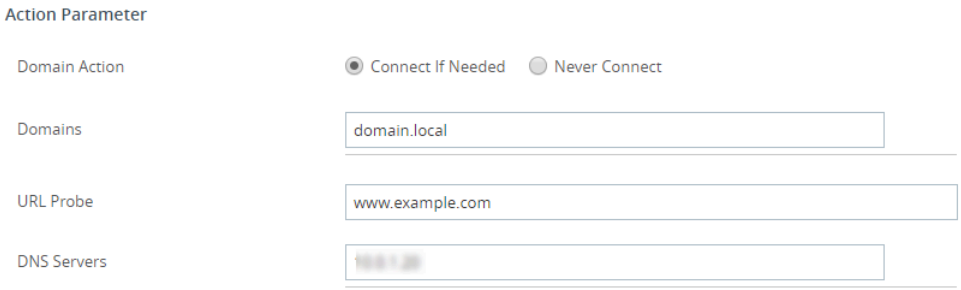
11. (Optional) Set more granular On-Demand connection rules by enabling the GlobalProtect app to **Use new on-demand keys**. You can add multiple rules by clicking **ADD RULE**.



- In the On-Demand Rule area, select an **Action** to apply to the GlobalProtect connection based on the Criteria that you define:
  - **Evaluate Connection**—Automatically establish the GlobalProtect connection based on the network and connection settings. This evaluation occurs each time a user attempts to connect to a domain.
  - **Connect**—Automatically establish the GlobalProtect connection.
  - **Disconnect**—Automatically disable GlobalProtect and prevent GlobalProtect from reconnecting.
  - **Ignore**—Leave the existing GlobalProtect connection as is and prevent GlobalProtect from reconnecting if it disconnects.

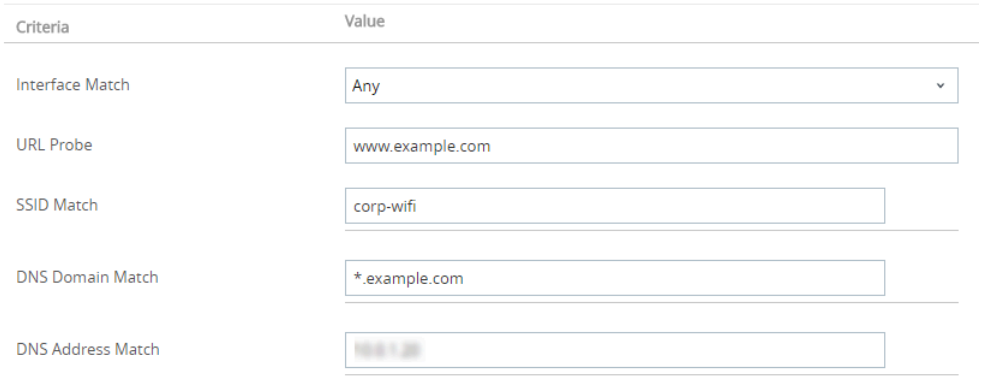


- (Optional) If you set the **Action** for your On-Demand connection rule to **Evaluate Connection**, you must also configure an Action Parameter to specify whether or not GlobalProtect can attempt to reconnect if domain name resolution fails during the connection evaluation (for example, if the DNS server fails to respond due to a timeout). You can add multiple parameters by clicking **ADD ACTION PARAMETERS**.
  - Set the **Domain Action** to **Connect if Needed** to enable GlobalProtect to reconnect or to **Never Connect** to prevent GlobalProtect from reconnecting.
  - Enter the **Domains** for which this **Action Parameter** applies.
  - (Optional) If you set the **Domain Action** to **Connect if Needed**, enter the HTTP or HTTPS URL that you want to probe in the **URL Probe** field. If the hostname of the URL cannot be resolved, the server is unreachable, or the server does not respond with a 200 HTTP status code, the GlobalProtect connection establishes.
  - (Optional) If you set the **Domain Action** to **Connect if Needed**, enter the IP addresses of the **DNS Servers** (internal or trusted external) used to resolve the specified **Domains**. If the DNS servers are not reachable, the GlobalProtect connection establishes.



- Configure the following Criteria to match against for your On-Demand connection rule. If an endpoint matches all specified criteria, the On-Demand connection rule is applied to that endpoint.
  - **Interface Match**—Specify the connection type to match against the endpoint's network adapter: **Any**, **Ethernet**, **Wi-Fi**, **Cellular**.
  - **URL Probe**—Enter the HTTP or HTTPS URL to match against. If the match is successful, a 200 HTTP status code is returned.
  - **SSID Match**—Enter the network SSID to match against. You can add multiple network SSIDs by clicking the add (**+**) button. For a successful match, the endpoint must match at least one specified network SSID.
  - **DNS Domain Match**—Enter the DNS search domain to match against. You can also match with a Wildcard record (such as **`*.example.com`**) to include all subdomains.
  - **DNS Address Match**—Enter the DNS server IP address to match against. You can add multiple DNS server IP addresses by clicking the add (**+**) button. You can also match with a single Wildcard record (such as **`17.*`**) that includes all DNS servers without IP

addresses. For a successful match, all DNS server IP addresses listed on the endpoint must match the specified DNS server IP addresses.

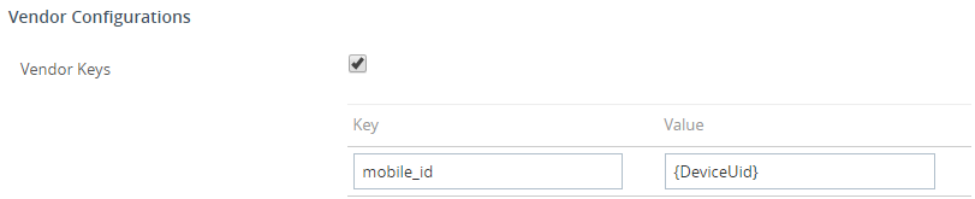


12. (Optional) Select the **Proxy** type and configure the relevant settings.

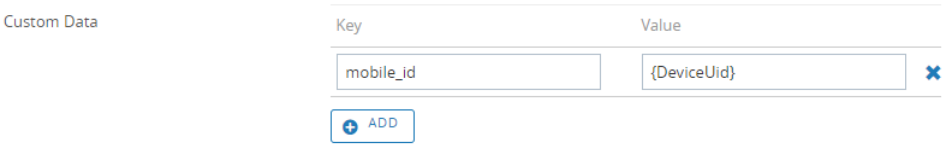
STEP 6 | (Optional) (starting with GlobalProtect app 5.0) If your GlobalProtect deployment requires Configure Windows User-ID Agent to Collect Host Information, specify the unique device identifier (UDID) attribute.

GlobalProtect supports integration with MDM to obtain mobile device attributes from the MDM server for use in HIP-based policy enforcement. In order for the MDM integration to work, the GlobalProtect app must present the UDID of the endpoint to the GlobalProtect gateway. The UDID attribute enables the GlobalProtect app to retrieve and use UDID information in MDM-based deployments. If you remove the UDID attribute from the profile, you can no longer use the MDM integration. The GlobalProtect app generates a new UDID, but it cannot be used for the integration.

- If you are using the **Palo Alto Networks GlobalProtect** network **Connection Type**, go to the **VPN** settings and enable **Vendor Keys** in the Vendor Configuration area. Set the **Key** to **`mobile_id`** and the **Value** to **`{DeviceUid}`**.



- If you are using the **Custom** network **Connection Type**, go to the **VPN** settings and **ADD Custom Data** in the Connection Info area. Set the **Key** to **`mobile_id`** and the **Value** to **`{DeviceUid}`**.



STEP 7 | **SAVE & PUBLISH** your changes.

Configure a Per-App VPN Configuration for iOS Endpoints Using Workspace ONE

You can enable access to internal resources from your managed mobile endpoints by configuring GlobalProtect VPN access using Workspace ONE. In a per-app VPN configuration, you can specify which managed apps can route traffic through the VPN tunnel. Unmanaged apps will continue to connect directly to the internet instead of through the VPN tunnel.

Use the following steps to configure a per-app VPN configuration for iOS endpoints using Workspace ONE:

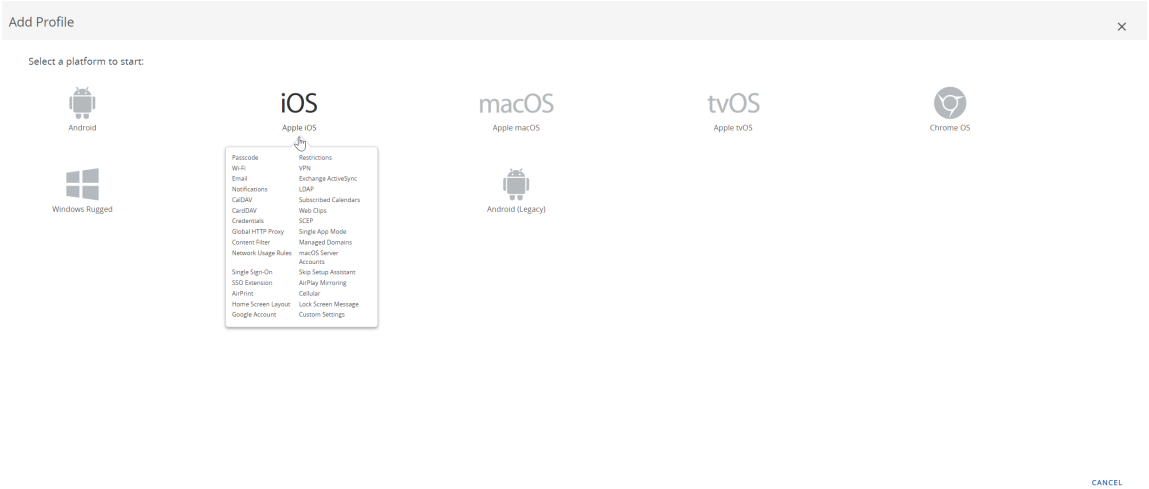
STEP 1 | Download the GlobalProtect app for iOS:

- Deploy the GlobalProtect Mobile App Using Workspace ONE.
- Download the GlobalProtect app directly from the App Store.

The GlobalProtect app for iOS is also available in the Apple App Store in China.

STEP 2 | From the Workspace ONE console, modify an existing Apple iOS profile or add a new one.

1. Select **Devices** > **Profiles & Resources** > **Profiles**, and then **ADD** a new profile.
2. Select **iOS** from the platform list.

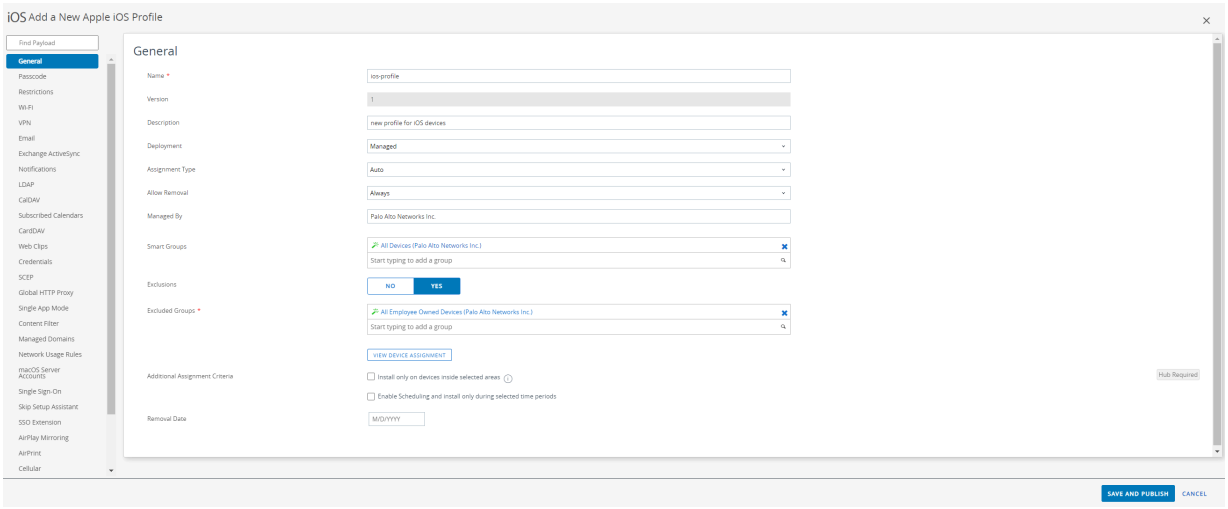


STEP 3 | Configure the **General** settings:

1. Enter a **Name** for the profile.
2. (Optional) Enter a brief **Description** of the profile that indicates its purpose.
3. (Optional) Select the **Deployment** method, which indicates whether the profile will be removed automatically upon unenrollment—either **Managed** (the profile is removed) or **Manual** (the profile remains installed until it is removed by the end user).
4. (Optional) Select an **Assignment Type** to determine how the profile is deployed to endpoints. Select **Auto** to deploy the profile to all endpoints automatically, **Optional** to enable the end user to install the profile from the Self-Service Portal (SSP) or to manually deploy the profile to individual endpoints, or **Compliance** to deploy the profile when an end user violates a compliance policy applicable to the endpoint.
5. (Optional) Select whether or not you want to **Allow Removal** of the profile by the end user. Select **Always** to enable the end user to manually remove the profile at any time, **Never**

to prevent the end user from removing the profile, or **With Authorization** to enable the end user to remove the profile with the authorization of the administrator. Choosing **With Authorization** adds a required Password.

6. (Optional) In the **Managed By** field, enter the Organization Group with administrative access to the profile.
7. (Optional) In the **Assigned Groups** field, add the Smart Groups to which you want the profile added. This field includes an option to create a new Smart Group, which can be configured with specs for minimum OS, device models, ownership categories, organization groups, and more.
8. (Optional) Indicate whether you want to include any **Exclusions** to the assignment of this profile. If you select **Yes**, the **Excluded Groups** field displays, enabling you to select the Smart Groups that you wish to exclude from the assignment of this profile.

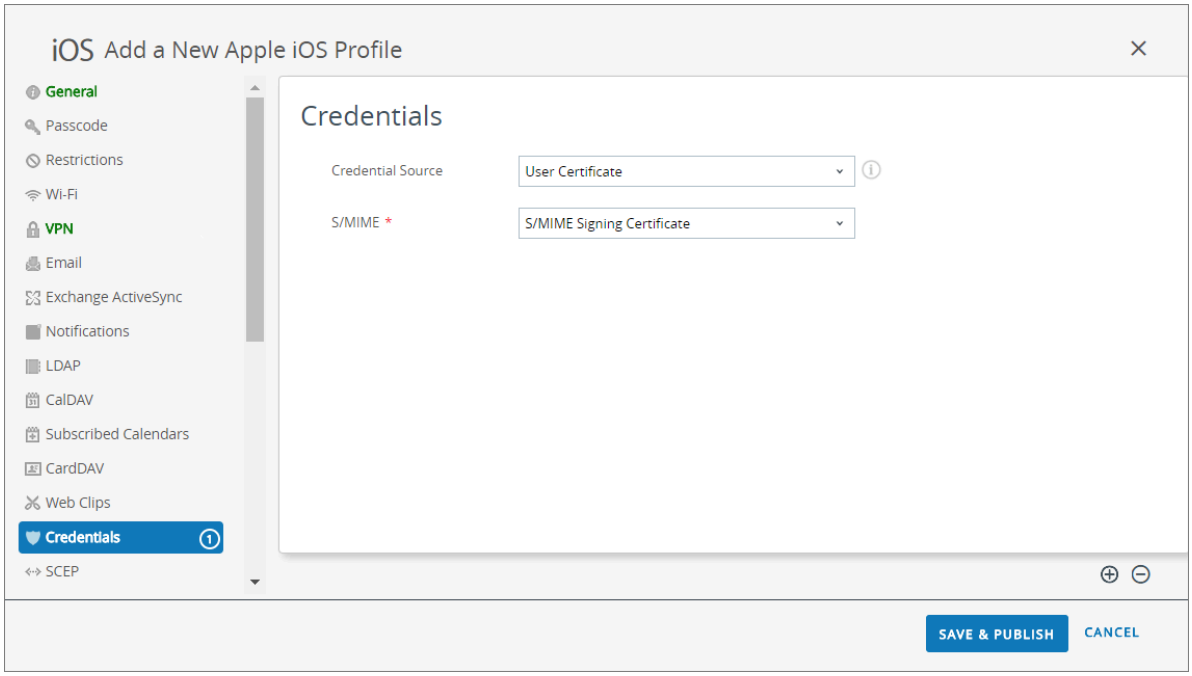


STEP 4 | Configure the **Credentials** settings:

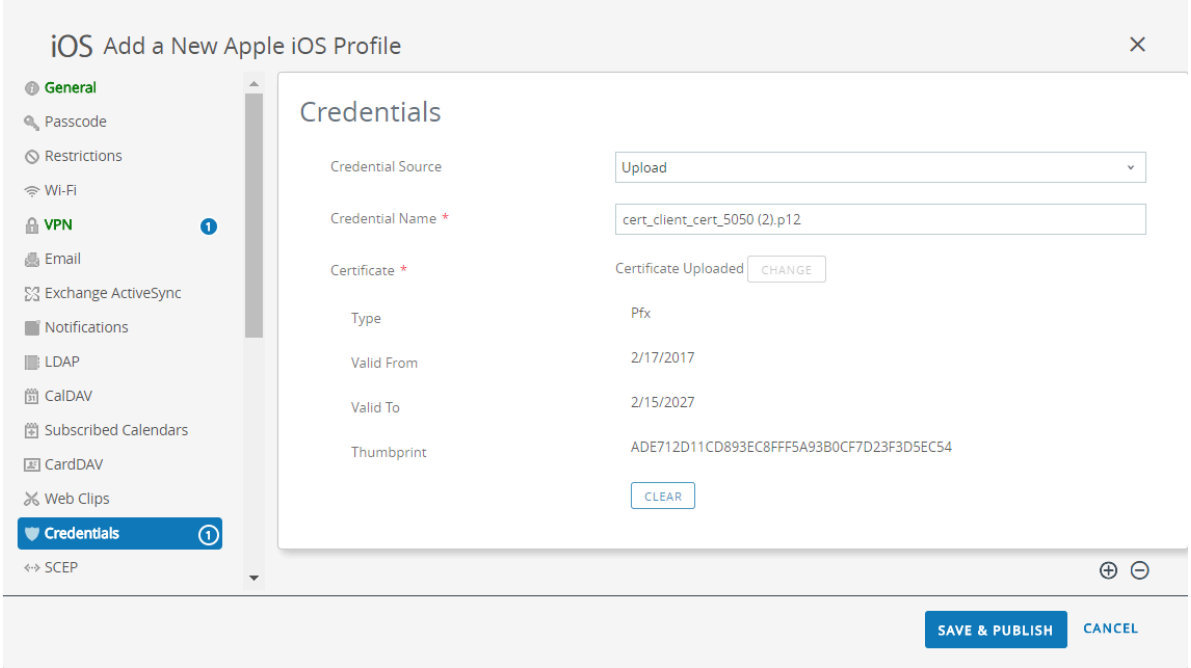
All per-app VPN configurations require certificate-based authentication.

Starting with iOS 12, if you want to use client certificates for GlobalProtect client authentication, you must deploy the client certificates as part of the VPN profile that is pushed from the MDM server. If you deploy client certificates from the MDM server using any other method, the certificates cannot be used by the GlobalProtect app.

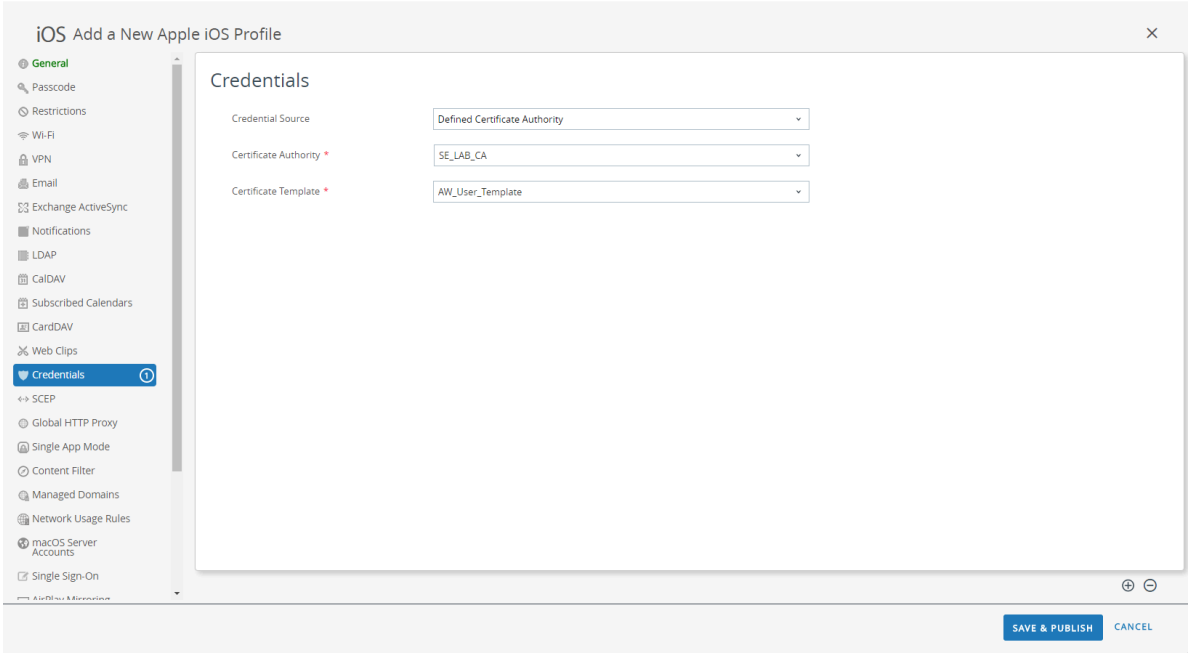
- To pull client certificates from Workspace ONE users:
  1. Set the **Credential Source** to **User Certificate**.
  2. Select the **S/MIME Signing Certificate** (default).



- To upload a client certificate manually:
  1. Set the **Credential Source** to **Upload**.
  2. Enter a **Credential Name**.
  3. Click **UPLOAD** to locate and select the certificate that you want to upload.
  4. After you select a certificate, click **SAVE**.



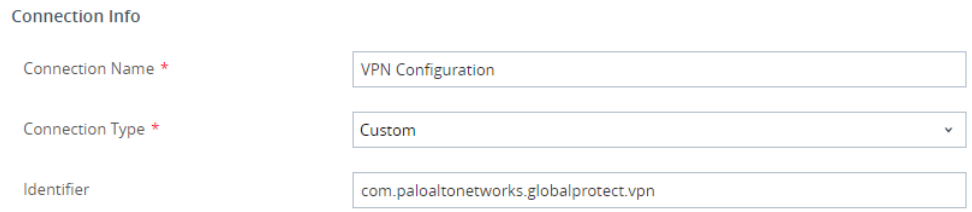
- To use a predefined certificate authority and template:
  1. Set the **Credential Source** to **Defined Certificate Authority**.
  2. Select the **Certificate Authority** from which you want obtain certificates.
  3. Select the **Certificate Template** for the certificate authority.



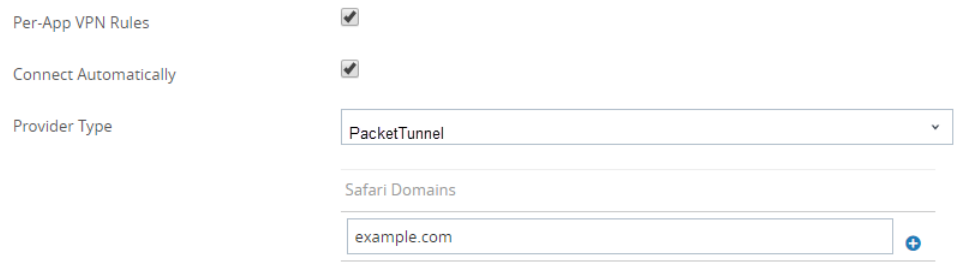
STEP 5 | Configure the **VPN** settings:

1. Enter the **Connection Name** that the endpoint displays.
2. Select the network **Connection Type**:
   - For GlobalProtect app 4.1.x and earlier releases, select **Palo Alto Networks GlobalProtect**.
   - For GlobalProtect app 5.0 and later releases, select **Custom**.
3. (Optional) If you set the **Connection Type** to **Custom**, enter the bundle ID (**com.paloaltonetworks.globalprotect.vpn**) in the **Identifier** field to identify the GlobalProtect app.

   *If you downloaded the GlobalProtect app directly from the Apple App Store in China, enter the bundle ID (**com.paloaltonetworks.globalprotect.vpncn**) in the **Identifier** field.*



4. In the **Server** field, enter the hostname or IP address of the GlobalProtect portal to which users connect.
5. (Optional) Enter the username of the VPN **Account** or click the add (**+**) button to view supported lookup values that you can insert.
6. (Optional) In the **Disconnect on idle** field, specify the amount of time (in seconds) at which an endpoint logs out of the GlobalProtect app after the app stops routing traffic through the VPN tunnel.
7. Enable **Per App VPN Rules** to route all traffic for managed apps through the GlobalProtect VPN tunnel.
   - Enable GlobalProtect to **Connect Automatically** to specified **Safari Domains**. You can add multiple **Safari Domains** by clicking the add (**+**) button.
   - Set the **Provider Type** to indicate how traffic will be tunneled—either at the application layer or the IP layer. Use PacketTunnel.



8. In the Authentication area, set the user **Authentication** method to **Certificate**.

All per-app VPN configurations require certificate-based authentication.

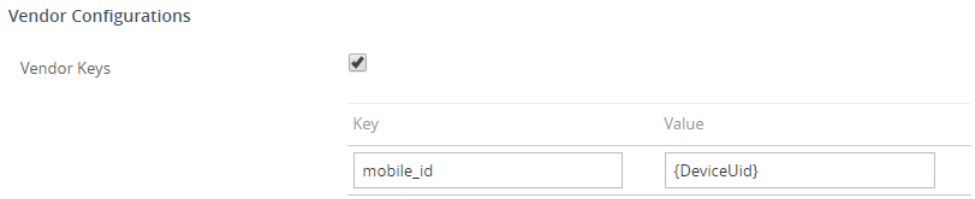
9. When prompted, select the **Identity Certificate** that GlobalProtect will use to authenticate users. The **Identity Certificate** is the same certificate that you configured in the **Credentials** settings.

10. (Optional) Select the **Proxy** type and configure the relevant settings.

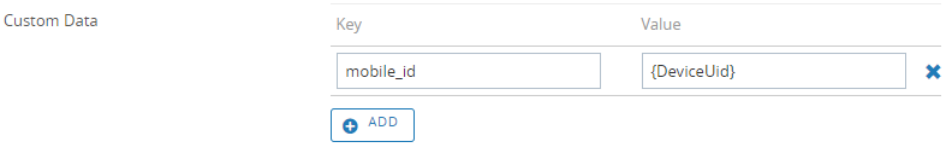
STEP 6 | (Optional) (starting with GlobalProtect app 5.0) If your GlobalProtect deployment requires Configure Windows User-ID Agent to Collect Host Information, specify the unique device identifier (UDID) attribute.

GlobalProtect supports integration with MDM to obtain mobile device attributes from the MDM server for use in HIP-based policy enforcement. In order for the MDM integration to work, the GlobalProtect app must present the UDID of the endpoint to the GlobalProtect gateway. The UDID attribute enables the GlobalProtect app to retrieve and use UDID information in MDM-based deployments. If you remove the UDID attribute from the profile, you can no longer use the MDM integration. The GlobalProtect app generates a new UDID, but it cannot be used for the integration.

- If you are using the **Palo Alto Networks GlobalProtect** network **Connection Type**, go to the **VPN** settings and enable **Vendor Keys** in the Vendor Configuration area. Set the **Key** to **`mobile_id`** and the **Value** to **`{DeviceUid}`**.



- If you are using the **Custom** network **Connection Type**, go to the **VPN** settings and **ADD Custom Data** in the Connection Info area. Set the **Key** to **`mobile_id`** and the **Value** to **`{DeviceUid}`**.

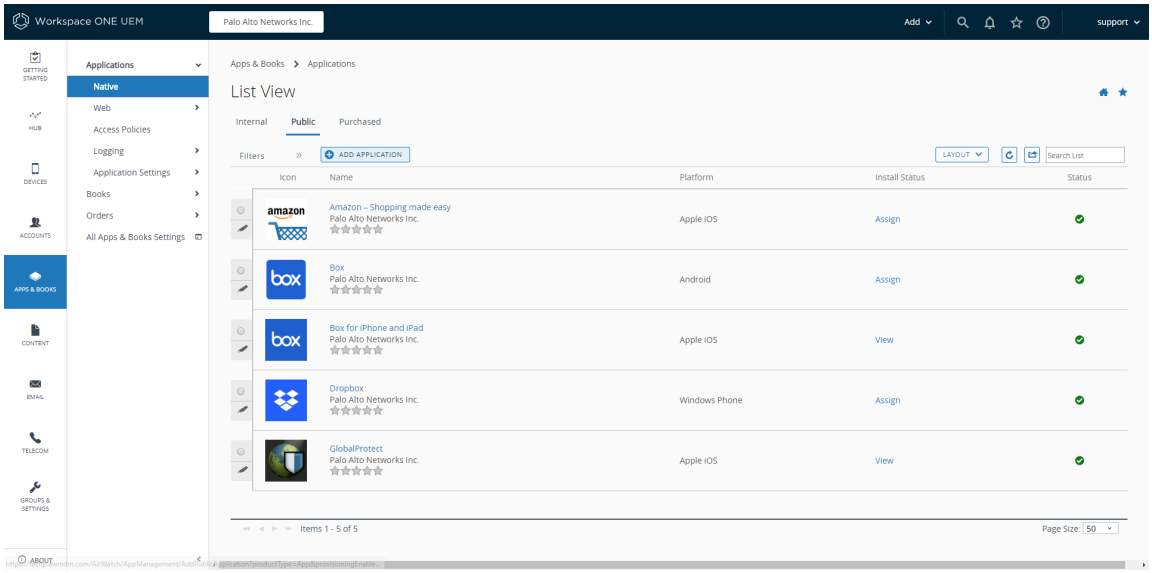


STEP 7 | **SAVE & PUBLISH** your changes.

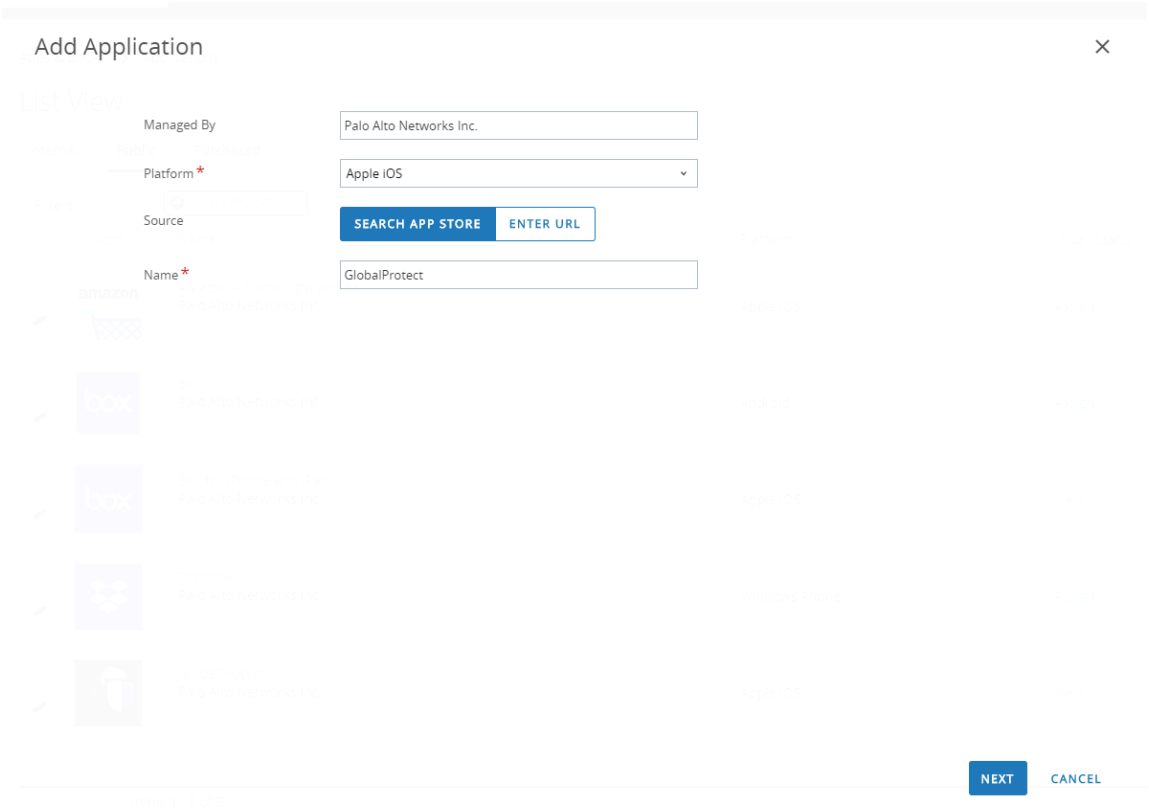
STEP 8 | Configure per-app VPN settings for a new managed app or modify the settings for an existing managed app.

After configuring the settings for the app and enabling per-app VPN, you can publish the app to a group of users and enable the app to send traffic through the GlobalProtect VPN tunnel.

1. Select **APPS & BOOKS** > **Applications** > **Native** > **Public**.
2. To add a new app, select **ADD APPLICATION**. To modify the settings for an existing app, locate the app in the list of Public apps (List View) and then select the edit (✎) icon in the actions menu next to the row.

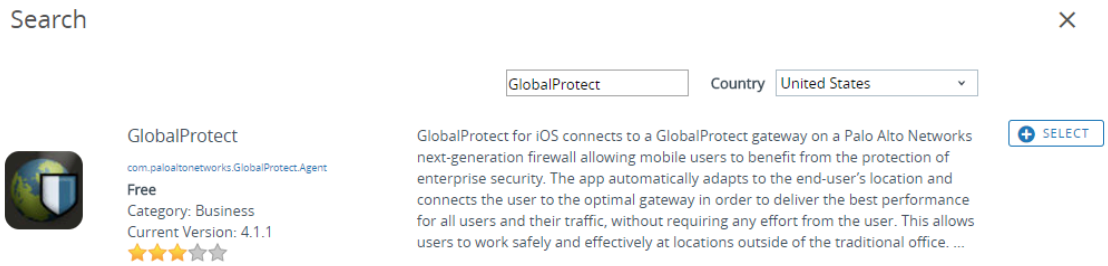


3. In the **Managed By** field, select the organization group that will manage this app.
4. Set the **Platform** to **Apple iOS**.
5. Select your preferred **Source** for locating the app:
   - **SEARCH APP STORE**—Enter the **Name** of the app.
   - **ENTER URL**—Enter the App Store URL for the app (for example, to add the Box app, enter https://itunes.apple.com/us/app/box-for-iphone-and-ipad/id290853822?mt=8&uo=4).

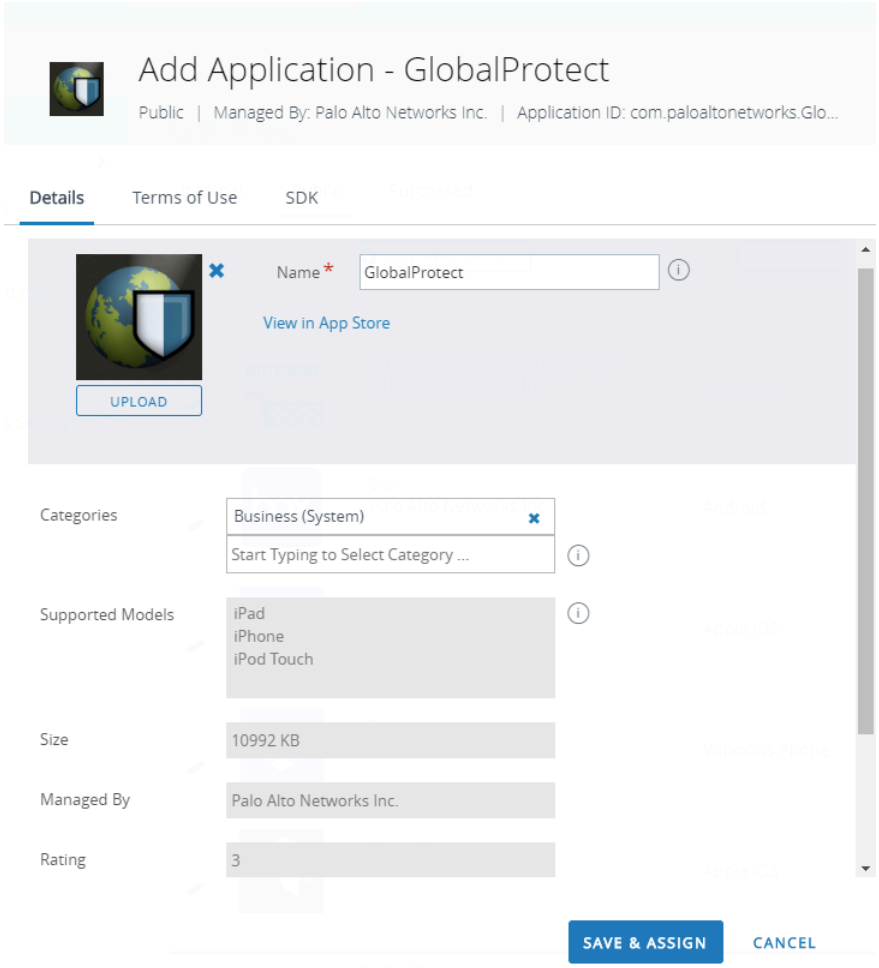


6. Click **NEXT**.

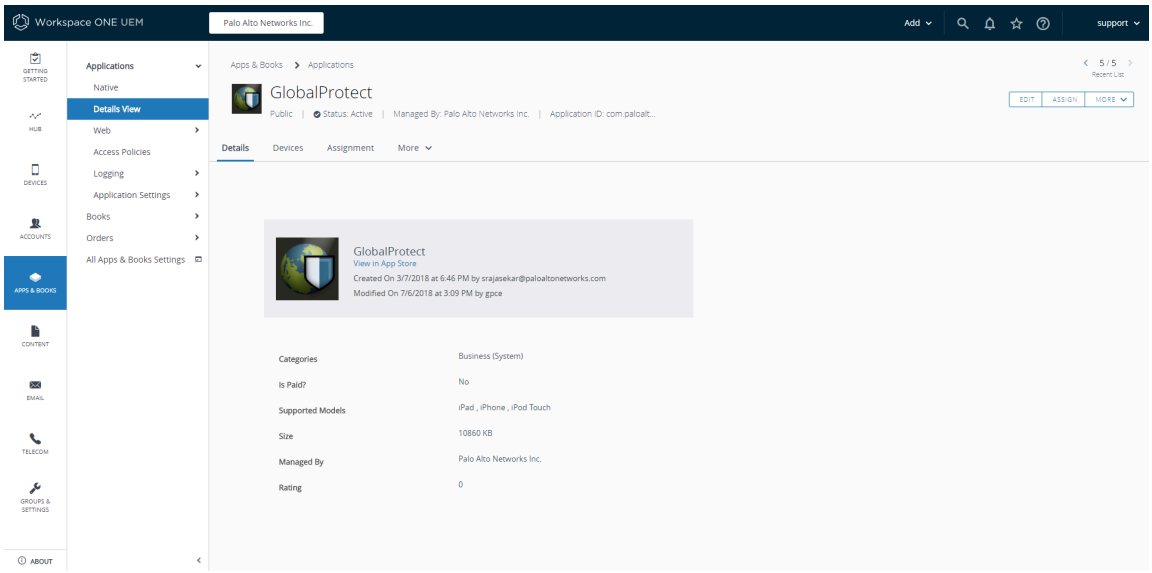
   If you chose to search the App Store, you must also **SELECT** the app from the list of search results.



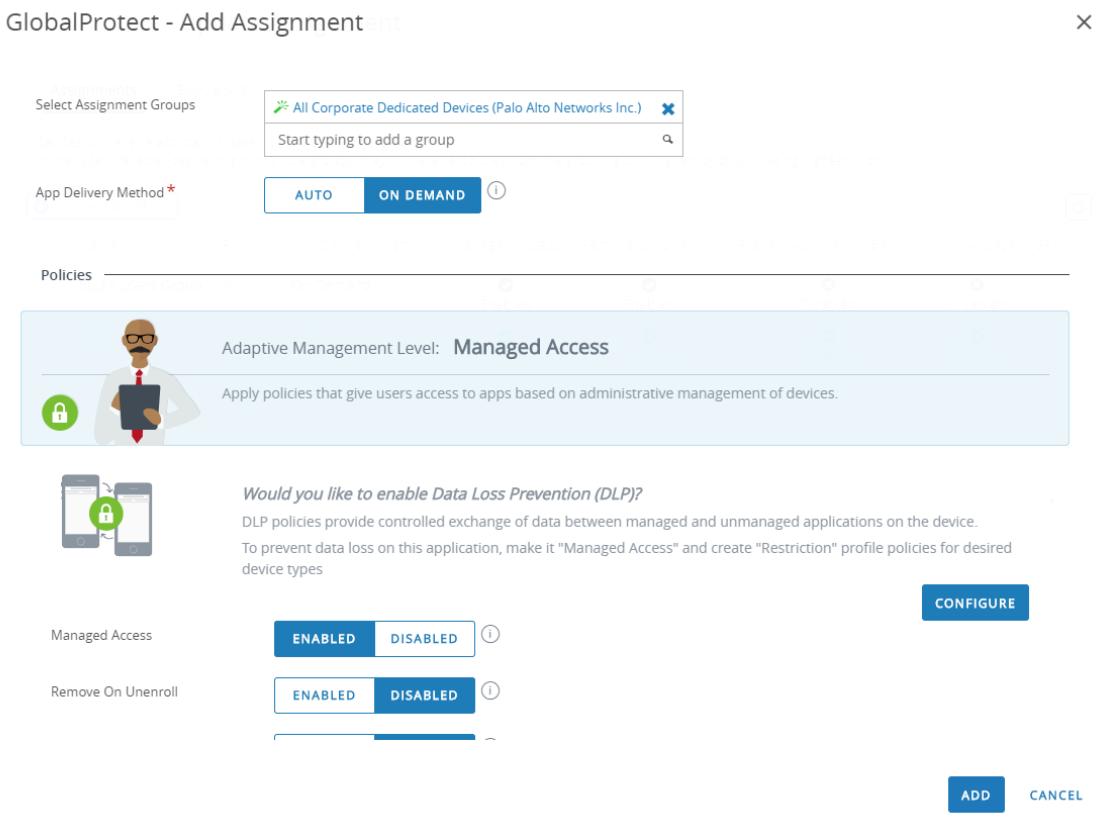
7. On the Add Application dialog, ensure that the app **Name** is correct. This is the name that will appear in the Workspace ONE App Catalog.
8. (Optional) Assign the app to pre-defined or custom **Categories** for ease-of-access in the Workspace ONE App Catalog.



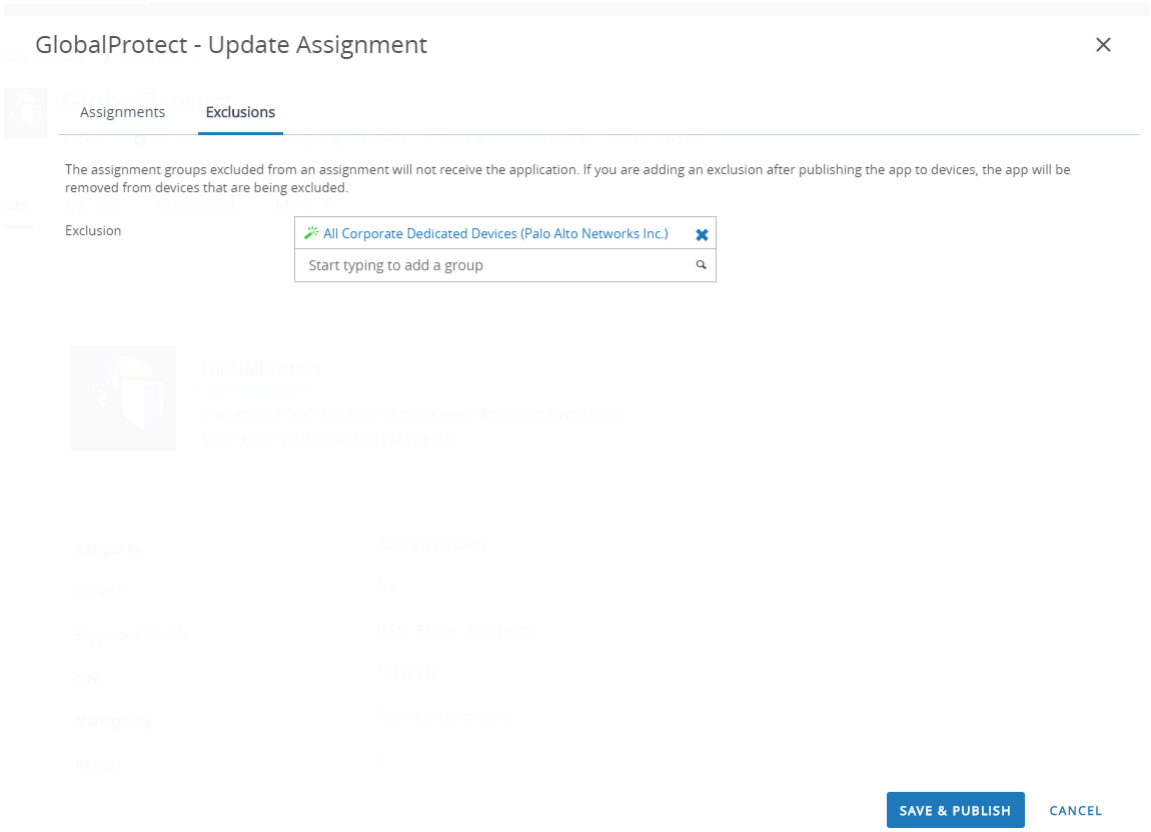
9. **SAVE & ASSIGN** the new app.
10. Select the newly added app from the list of Public apps (List View).
11. From the **Applications** > **Details View**, click **ASSIGN** at the top-right corner of the screen.



12. Select **Assignments** and then click **ADD ASSIGNMENT** to add the Smart Groups that will have access to this app.
    1. In the **Select Assignment Groups** field, select the Smart Groups that you want to grant access to this app.
    2. Select the **App Delivery Method**. If you select **AUTO**, the app is automatically deployed to the specified Smart Groups. If you select **ON DEMAND**, the app must be deployed manually.
    3. Set the **Managed Access** option to **ENABLED**. This option gives users access to the app based on the management policies that you apply.
    4. Configure the remaining settings as needed.
    5. **ADD** the new assignment.



13. (Optional) To exclude certain Smart Groups from accessing the app, select **Exclusions** and then select the Smart Groups that you want to exclude from the **Exclusion** field.



14. **SAVE & PUBLISH** the configuration to the assigned Smart Groups.

Configure Workspace ONE for Windows 10 UWP Endpoints

Refer to the following sections for information on how to set up VPN configurations for Windows 10 UWP endpoints using Workspace ONE:

- Configure an Always On VPN Configuration for Windows 10 UWP Endpoints Using Workspace ONE
- Configure a User-Initiated Remote Access VPN Configuration for Windows 10 UWP Endpoints Using Workspace ONE
- Configure a Per-App VPN Configuration for Windows 10 UWP Endpoints Using Workspace ONE

Configure an Always On VPN Configuration for Windows 10 UWP Endpoints Using Workspace ONE

In an Always On VPN configuration, the secure GlobalProtect connection is always on. Traffic that matches specific filters (such as port and IP address) configured on the GlobalProtect gateway is always routed through the VPN tunnel. For even tighter security requirements, you can enable VPN lockdown, which forces the secure connection to always be on and connected in addition to disabling network access when the app is not connected. This configuration is similar to the **Enforce GlobalProtect for Network Access** option that you would typically configure in a GlobalProtect portal configuration.

Because Workspace ONE does not yet list GlobalProtect as an official connection provider for Windows endpoints, you must select an alternate VPN provider, edit the settings for the GlobalProtect app, and import the configuration back into the VPN profile as described in the following workflow.

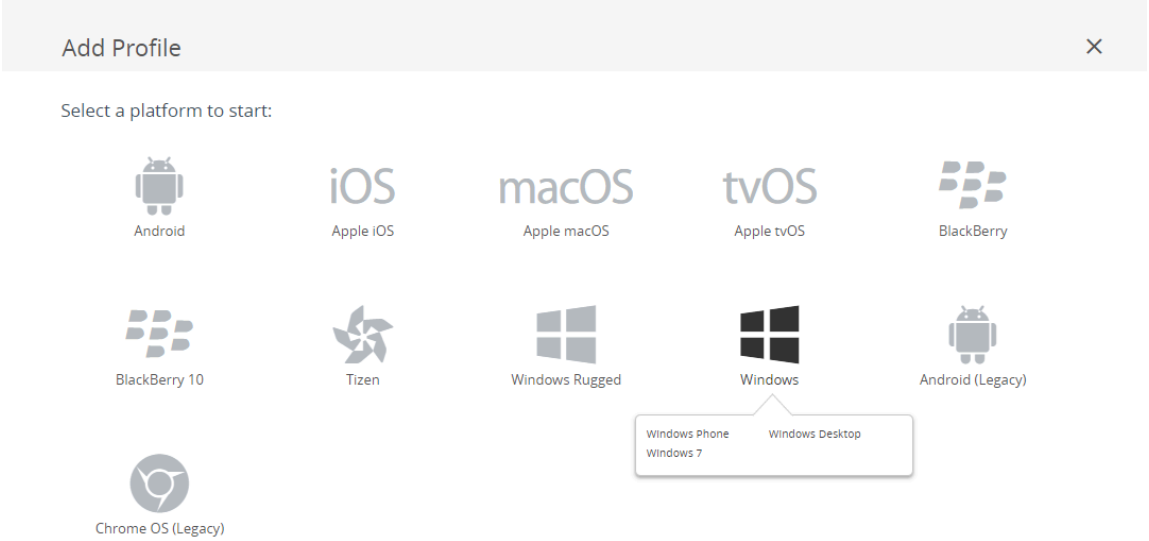
Use the following steps to configure an Always On VPN configuration for Windows 10 UWP endpoints using Workspace ONE:

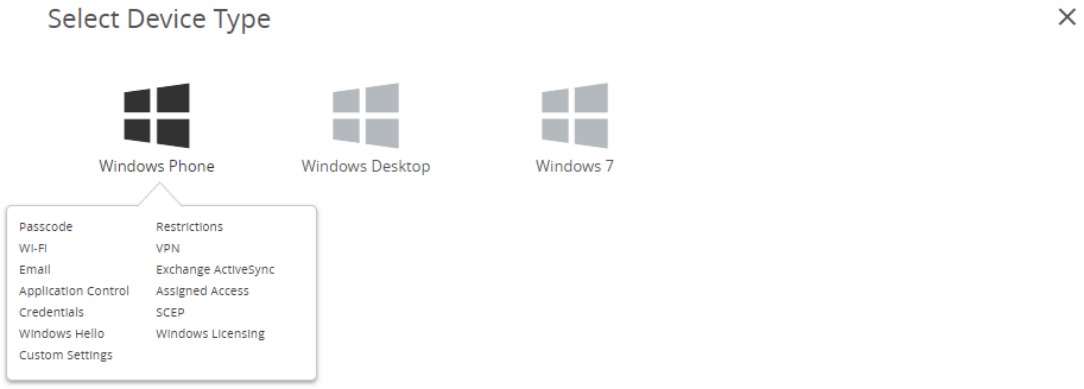
STEP 1 | Download the GlobalProtect app for Windows 10 UWP:

- Deploy the GlobalProtect Mobile App Using Workspace ONE.
- Download the GlobalProtect app directly from the Microsoft Store.

STEP 2 | From the Workspace ONE console, modify an existing Windows 10 UWP profile add a new one.

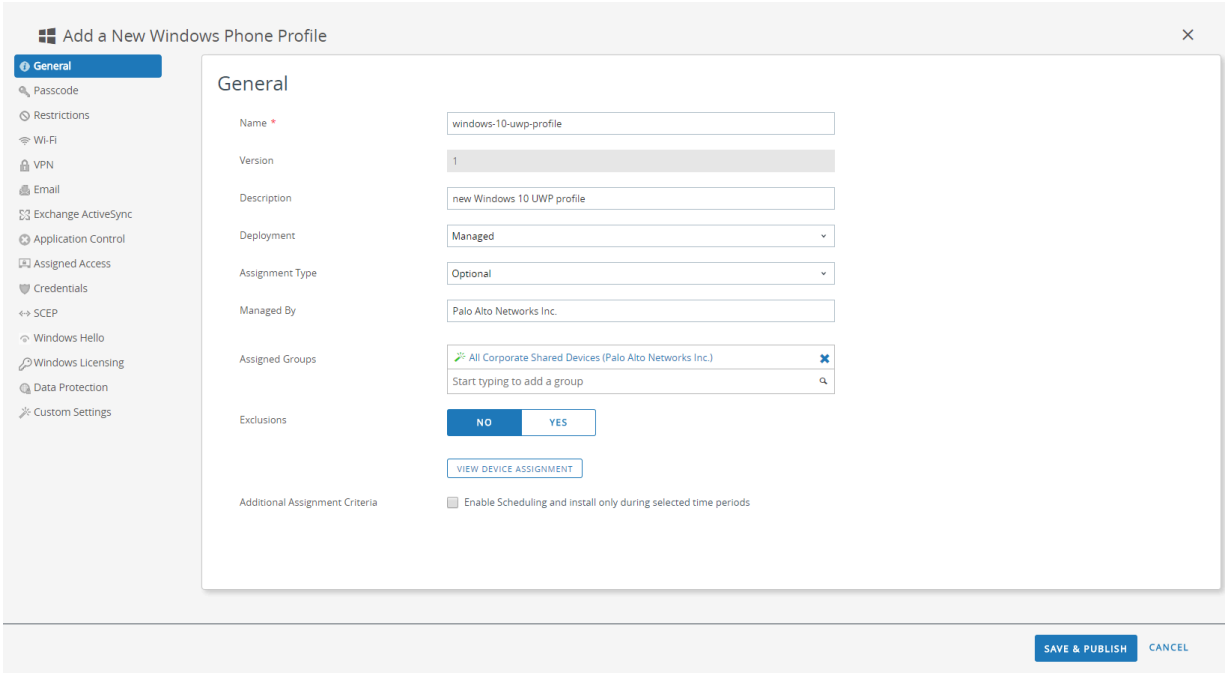
1. Select **Devices** > **Profiles & Resources** > **Profiles**, and then **ADD** a new profile.
2. Select **Windows** as the platform and **Windows Phone** as the device type.





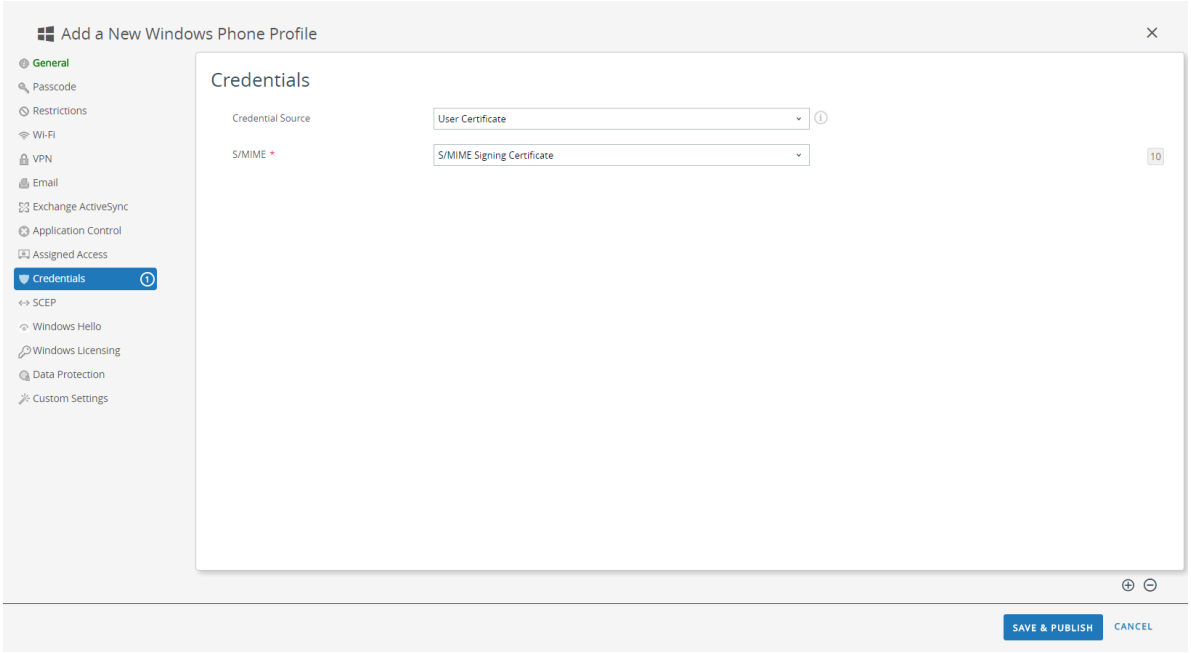
STEP 3 | Configure the **General** settings:

1. Enter a **Name** for the profile.
2. (Optional) Enter a brief **Description** of the profile that indicates its purpose.
3. (Optional) Set the **Deployment** method to **Managed** to enable the profile to be removed automatically upon unenrollment
4. (Optional) Select an **Assignment Type** to determine how the profile is deployed to endpoints. Select **Auto** to deploy the profile to all endpoints automatically, **Optional** to enable the end user to install the profile from the Self-Service Portal (SSP) or to manually deploy the profile to individual endpoints, or **Compliance** to deploy the profile when an end user violates a compliance policy applicable to the endpoint.
5. (Optional) In the **Managed By** field, enter the Organization Group with administrative access to the profile.
6. (Optional) In the **Assigned Groups** field, add the Smart Groups to which you want the profile added. This field includes an option to create a new Smart Group, which can be configured with specs for minimum OS, device models, ownership categories, organization groups, and more.
7. (Optional) Indicate whether you want to include any **Exclusions** to the assignment of this profile. If you select **Yes**, the **Excluded Groups** field displays, enabling you to select the Smart Groups that you wish to exclude from the assignment of this profile.
8. (Optional) If you **Enable Scheduling and install only during selected time periods**, you can apply a time schedule (**Devices** > **Profiles & Resources** > **Profiles Settings** > **Time Schedules**) to the profile installation, which limits the periods of time during which the profile can be installed on endpoints. When prompted, enter the schedule name in the **Assigned Schedules** field.

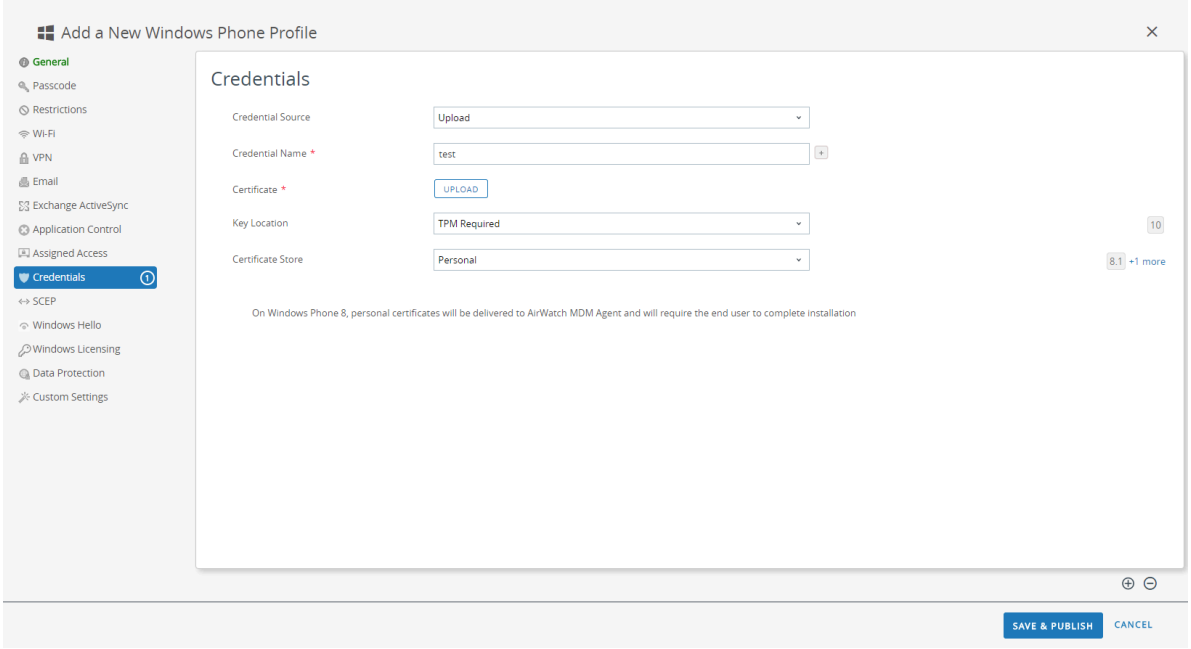


STEP 4 | (Optional) If your GlobalProtect deployment requires client certificate authentication, configure the **Credentials** settings:

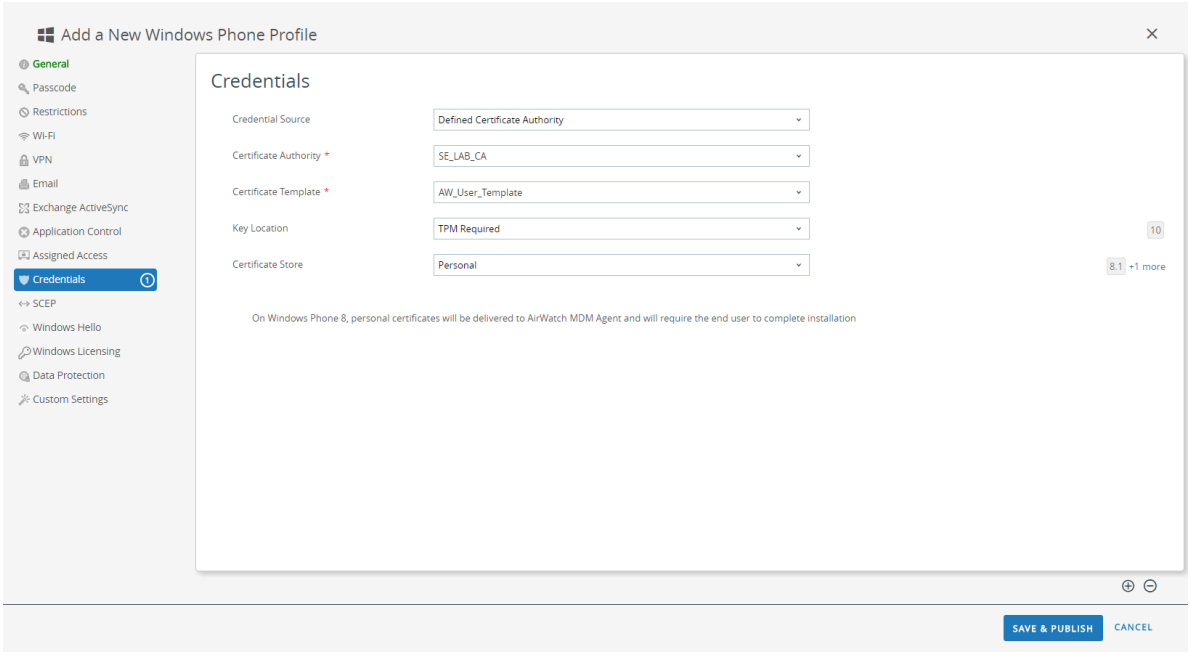
- To pull client certificates from Workspace ONE users:
  1. Set the **Credential Source** to **User Certificate**.
  2. Select the **S/MIME Signing Certificate** (default).



- To upload a client certificate manually:
  1. Set the **Credential Source** to **Upload**.
  2. Enter a **Credential Name**.
  3. Click **UPLOAD** to locate and select the certificate that you want to upload.
  4. After you select a certificate, click **SAVE**.
  5. Select the **Key Location** where you want to store the certificate's private key:
     - **TPM Required**—Store the private key on a Trusted Platform Module. If a Trusted Platform Module is not available on the endpoint, the private key cannot be installed.
     - **TPM If Present**—Store the private key on a Trusted Platform Module if one is available on the endpoint. If a Trusted Platform Module is not available on the endpoint, the private key is stored in the endpoint software.
     - **Software**—Store the private key in the endpoint software.
     - **Passport**—Save the private key to Microsoft Passport. To use this option, Workspace ONE Protection Agent must be installed on the endpoint.
  6. Set the **Certificate Store** to **Personal**.



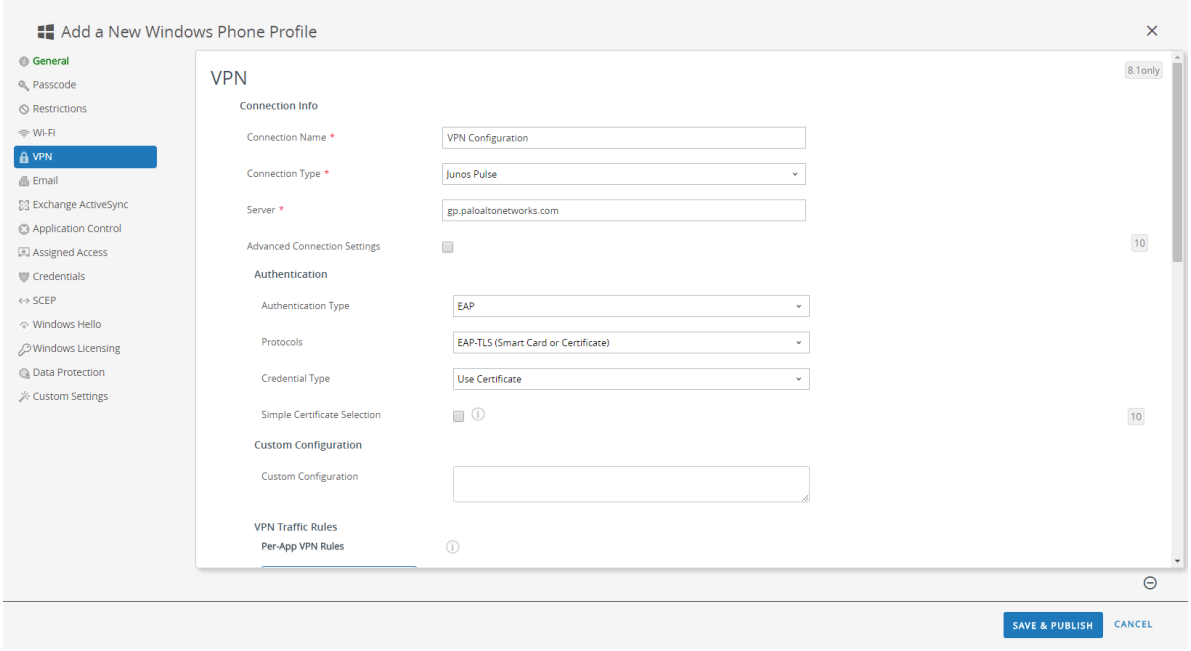
- To use a predefined certificate authority and template:
  1. Set the **Credential Source** to **Defined Certificate Authority**.
  2. Select the **Certificate Authority** from which you want obtain certificates.
  3. Select the **Certificate Template** for the certificate authority.
  4. Select the **Key Location** where you want to store the certificate's private key:
     - **TPM Required**—Store the private key on a Trusted Platform Module. If a Trusted Platform Module is not available on the endpoint, the private key cannot be installed.
     - **TPM If Present**—Store the private key on a Trusted Platform Module if one is available on the endpoint. If a Trusted Platform Module is not available on the endpoint, the private key is stored in the endpoint software.
     - **Software**—Store the private key in the endpoint software.
     - **Passport**—Save the private key to Microsoft Passport. To use this option, Workspace ONE Protection Agent must be installed on the endpoint.
  5. Set the **Certificate Store** to **Personal**.



STEP 5 | Configure the **VPN** settings:

1. Enter the **Connection Name** that the endpoint displays.
2. Select an alternate **Connection Type** provider (do not select **IKEv2**, **L2TP**, **PPTP**, or **Automatic**, as these do not have the associated vendor settings required for the GlobalProtect VPN profile).

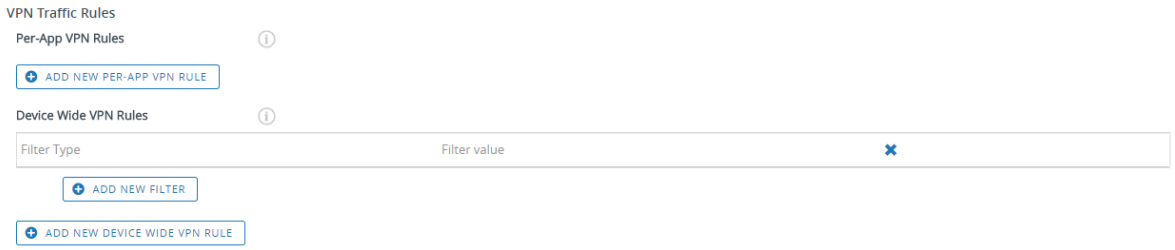
   You must select an alternate vendor because Workspace ONE has not yet listed GlobalProtect as an official connection provider for Windows endpoints.
3. In the **Server** field, enter the hostname or IP address of the GlobalProtect portal to which users connect.
4. In the Authentication area, select an **Authentication Type** to specify the method authenticate end users.



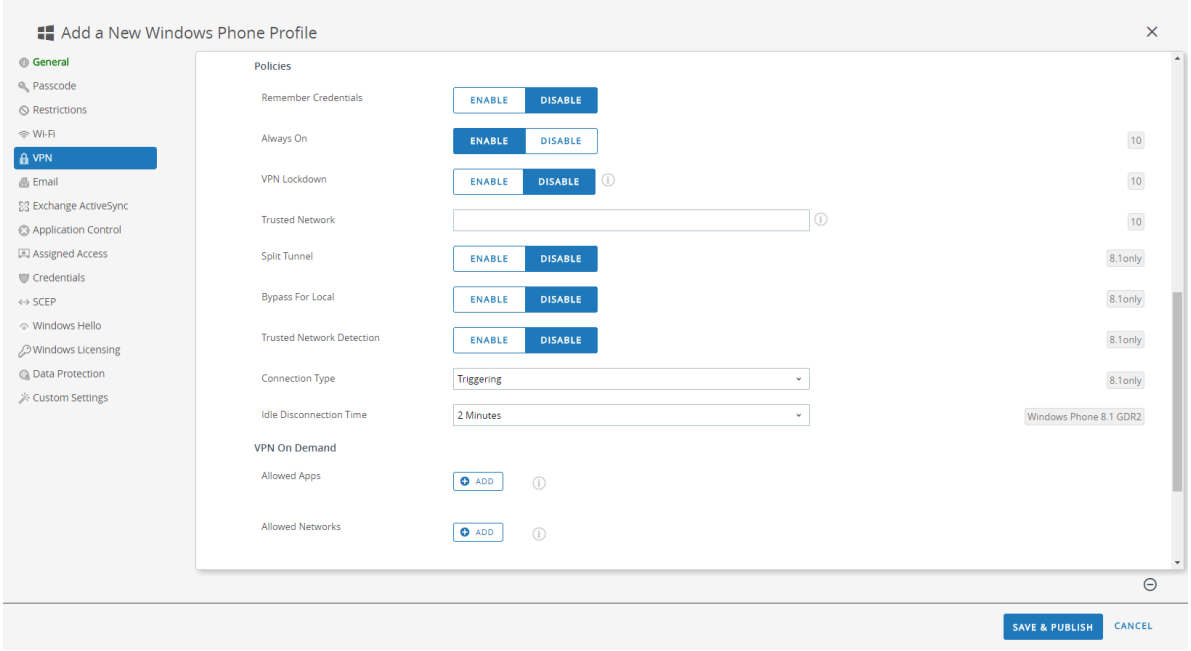
5. (Optional) To permit GlobalProtect to save user credentials, **ENABLE** the option to **Remember Credentials** in the Policies area.
6. (Optional) In the VPN Traffic Rules area, **ADD NEW DEVICE WIDE VPN RULE** to send traffic matching a specific route through the VPN tunnel. These rules are not bound by

application but are evaluated across the endpoint. If the traffic matches the specified match criteria, it is routed through the VPN tunnel.

Add match criteria by clicking **ADD NEW FILTER** and then entering a **Filter Type** and corresponding **Filter Value**.



7. To maintain the GlobalProtect connection always, configure either of the following options in the Policies area:
   - **ENABLE Always On** to force the secure connection to be always on.
   - **ENABLE VPN Lockdown** to force the secure connection to be always on and connected, and to disable network access when the app is not connected. The **VPN Lockdown** option in Workspace ONE is similar to the **Enforce GlobalProtect for Network Access** option that you would configure in a GlobalProtect portal configuration.



8. (Optional) Specify **Trusted Network** addresses if you want GlobalProtect to connect only when it detects a trusted network connection.

STEP 6 | **SAVE & PUBLISH** your changes.

STEP 7 | To set the connection type provider to GlobalProtect, edit the VPN profile in XML.

To minimize additional edits in the raw XML, review the settings in your VPN profile before you export the configuration. If you need to change a setting after you export the VPN profile, you can make the changes in the raw XML or, you can update the setting in the VPN profile and perform this step again.

1. In the **Devices** > **Profiles** > **List View**, select the radio button next to the new profile you added in the previous steps, and then select **</>XML** at the top of the table. Workspace ONE opens the XML view of the profile.
2. **Export** the profile and then open it in a text editor of your choice.
3. Edit the following settings for GlobalProtect:

- In the `LoclURI` element that specifies the `PluginPackageFamilyName`, change the element to:

  `<LocURI>./Vendor/MSFT/VPNv2/PaloAltoNetworks/PluginProfile/PluginPackageFamilyName</LocURI>`

- In the `Data` element that follows, change the value to:

  `<Data>PaloAltoNetworks.GlobalProtect_rn9aeerfb38dg</Data>`

1. Save your changes to the exported profile.
2. Return to Workspace ONE and select **Devices** > **Profiles** > **List View**.
3. Create and name a new profile (select **ADD** > **Add Profile** > **Windows** > **Windows Phone**).
4. Select **Custom Settings** > **Configure**, and then copy and paste the edited configuration.
5. **SAVE & PUBLISH** your changes.

STEP 8 | Clean up the original profile by selecting the original profile from **Devices** > **Profiles** > **List View**, and then selecting **More Actions** > **Deactivate**. Workspace ONE moves the profile to the Inactive list.

STEP 9 | Test the configuration.

Configure a User-Initiated Remote Access VPN Configuration for Windows 10 UWP Endpoints Using Workspace ONE

In a remote access (On-Demand) VPN configuration, users must manually launch the app to establish the secure GlobalProtect connection. Traffic that matches specific filters (such as port and IP address) configured on the GlobalProtect gateway is routed through the VPN tunnel only after users initiate and establish the connection.

Because Workspace ONE does not yet list GlobalProtect as an official connection provider for Windows endpoints, you must select an alternate VPN provider, edit the settings for the GlobalProtect app, and import the configuration back into the VPN profile as described in the following workflow.

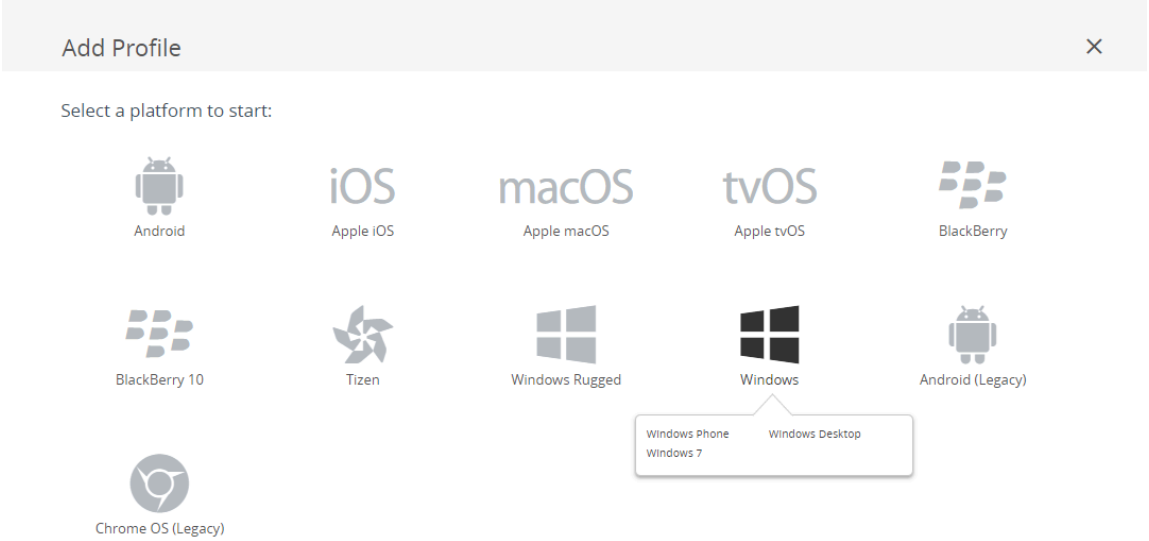
Use the following steps to configure a user-initiated remote access VPN configuration for Windows 10 UWP endpoints using Workspace ONE:

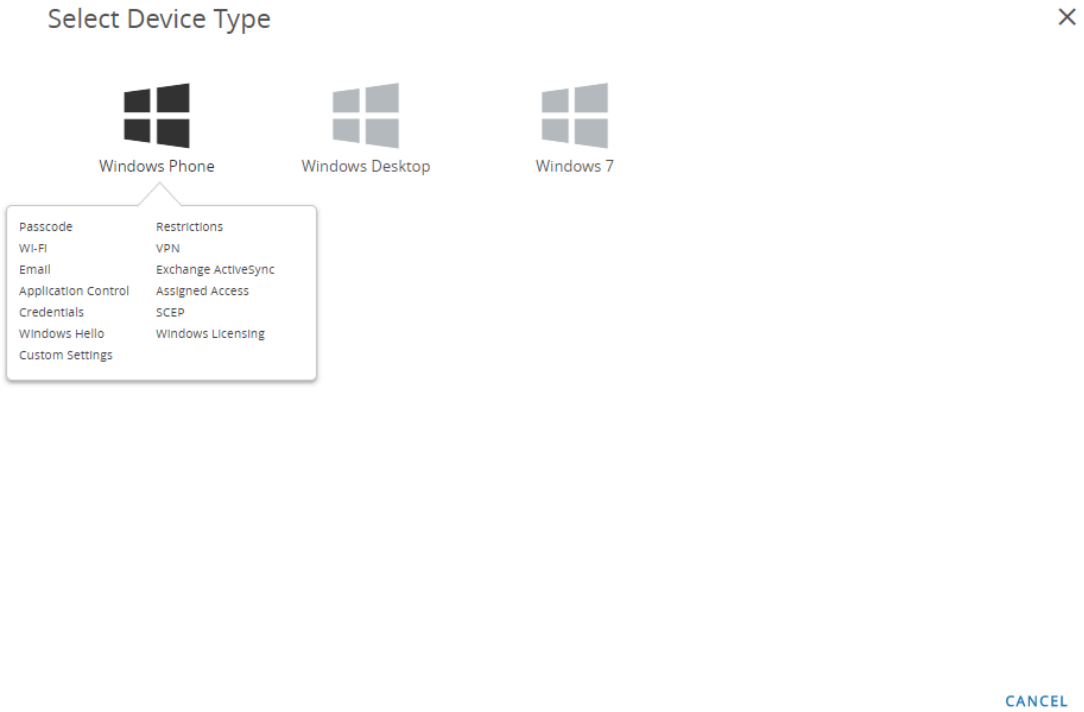
STEP 1 | Download the GlobalProtect app for Windows 10 UWP:

- Deploy the GlobalProtect Mobile App Using Workspace ONE.
- Download the GlobalProtect app directly from the Microsoft Store.

STEP 2 | From the Workspace ONE console, modify an existing Windows 10 UWP profile add a new one.

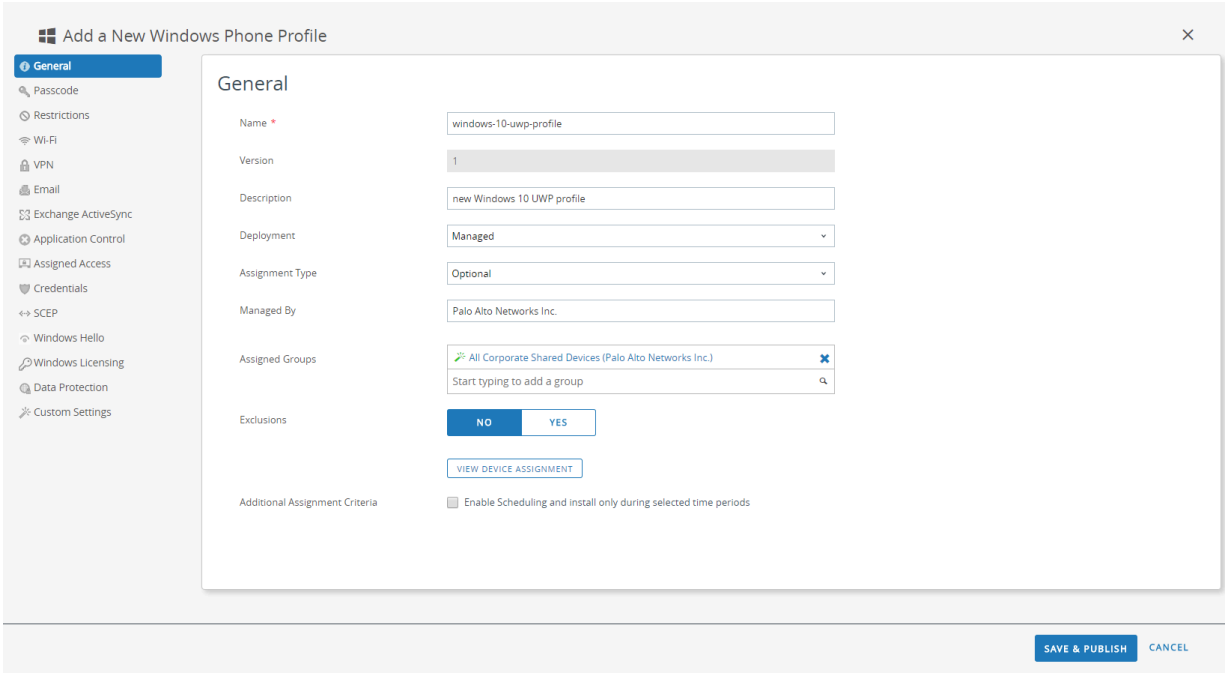
1. Select **Devices** > **Profiles & Resources** > **Profiles**, and then **ADD** a new profile.
2. Select **Windows** as the platform and **Windows Phone** as the device type.





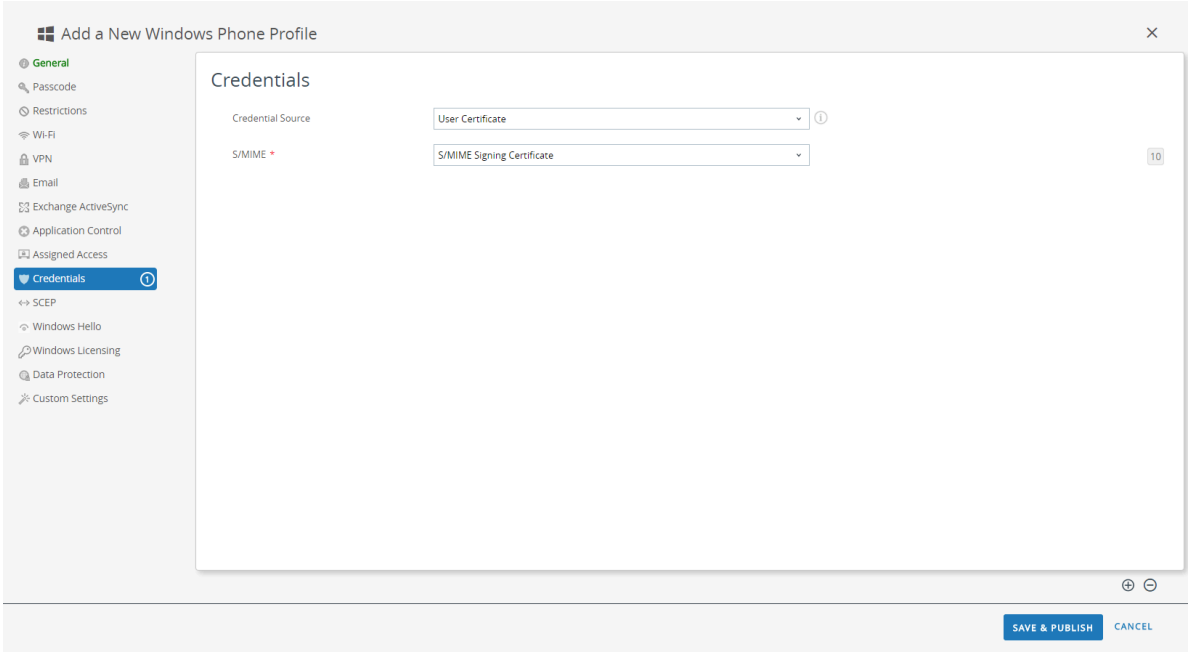
STEP 3 | Configure the **General** settings:

1. Enter a **Name** for the profile.
2. (Optional) Enter a brief **Description** of the profile that indicates its purpose.
3. (Optional) Set the **Deployment** method to **Managed** to enable the profile to be removed automatically upon unenrollment
4. (Optional) Select an **Assignment Type** to determine how the profile is deployed to endpoints. Select **Auto** to deploy the profile to all endpoints automatically, **Optional** to enable the end user to install the profile from the Self-Service Portal (SSP) or to manually deploy the profile to individual endpoints, or **Compliance** to deploy the profile when an end user violates a compliance policy applicable to the endpoint.
5. (Optional) In the **Managed By** field, enter the Organization Group with administrative access to the profile.
6. (Optional) In the **Assigned Groups** field, add the Smart Groups to which you want the profile added. This field includes an option to create a new Smart Group, which can be configured with specs for minimum OS, device models, ownership categories, organization groups, and more.
7. (Optional) Indicate whether you want to include any **Exclusions** to the assignment of this profile. If you select **Yes**, the **Excluded Groups** field displays, enabling you to select the Smart Groups that you wish to exclude from the assignment of this profile.
8. (Optional) If you **Enable Scheduling and install only during selected time periods**, you can apply a time schedule (**Devices** > **Profiles & Resources** > **Profiles Settings** > **Time Schedules**) to the profile installation, which limits the periods of time during which the profile can be installed on endpoints. When prompted, enter the schedule name in the **Assigned Schedules** field.

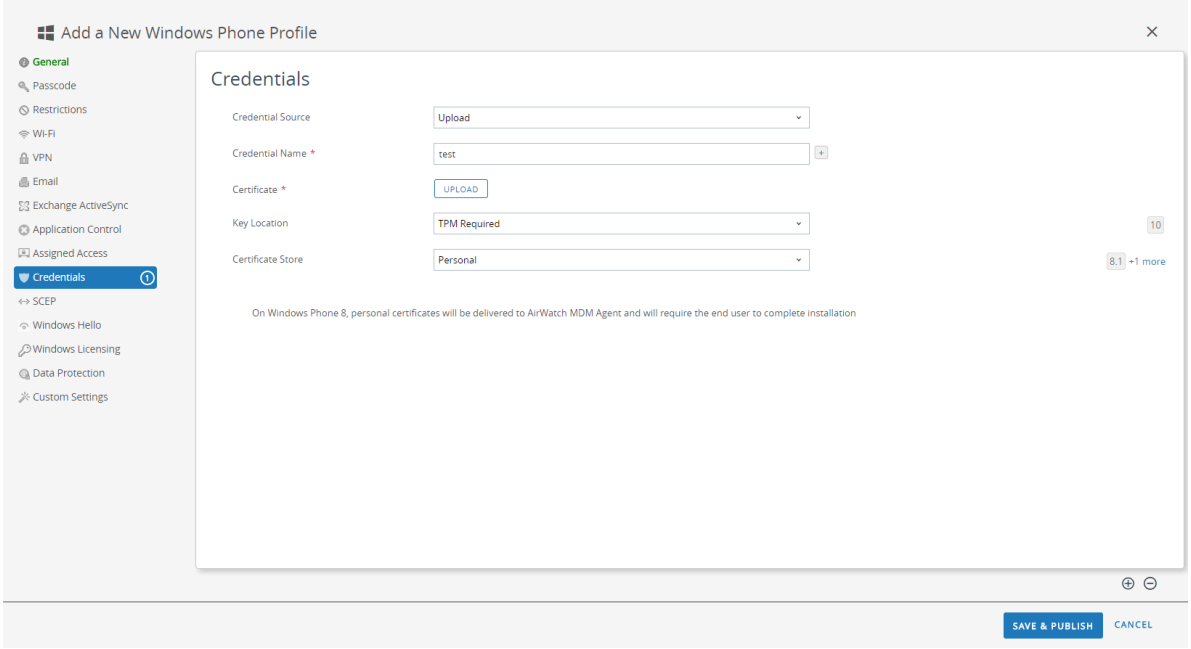


STEP 4 | (Optional) If your GlobalProtect deployment requires client certificate authentication, configure the **Credentials** settings:

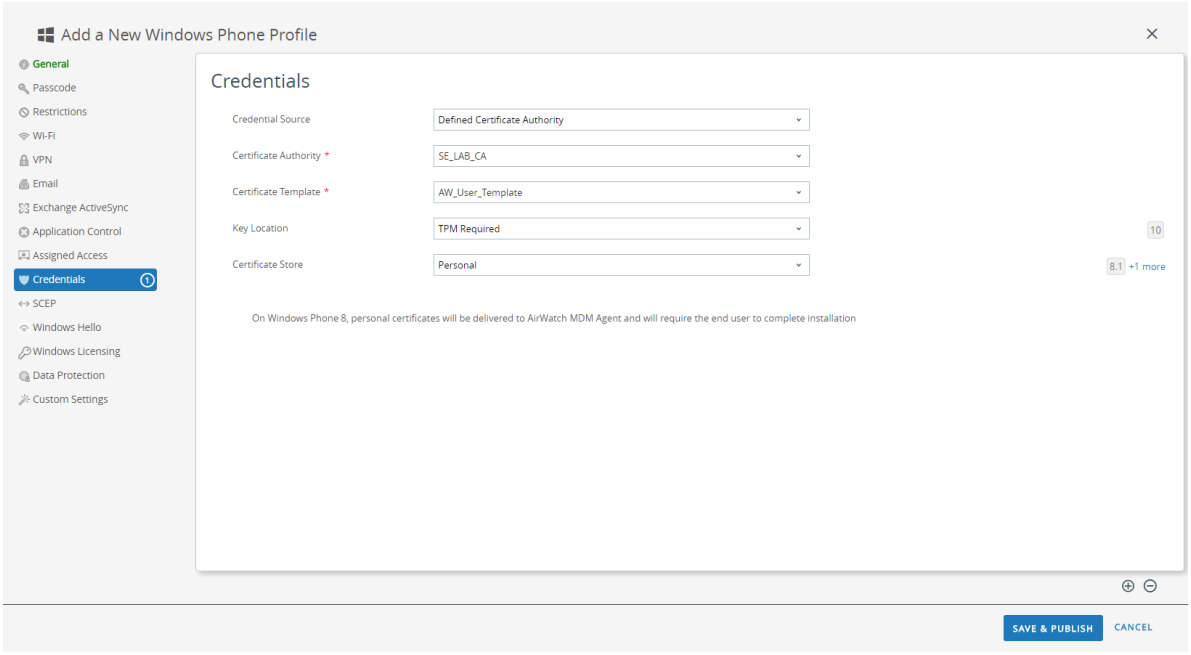
- To pull client certificates from Workspace ONE users:
  1. Set the **Credential Source** to **User Certificate**.
  2. Select the **S/MIME Signing Certificate** (default).



- To upload a client certificate manually:
  1. Set the **Credential Source** to **Upload**.
  2. Enter a **Credential Name**.
  3. Click **UPLOAD** to locate and select the certificate that you want to upload.
  4. After you select a certificate, click **SAVE**.
  5. Select the **Key Location** where you want to store the certificate's private key:
     - **TPM Required**—Store the private key on a Trusted Platform Module. If a Trusted Platform Module is not available on the endpoint, the private key cannot be installed.
     - **TPM If Present**—Store the private key on a Trusted Platform Module if one is available on the endpoint. If a Trusted Platform Module is not available on the endpoint, the private key is stored in the endpoint software.
     - **Software**—Store the private key in the endpoint software.
     - **Passport**—Save the private key to Microsoft Passport. To use this option, Workspace ONE Protection Agent must be installed on the endpoint.
  6. Set the **Certificate Store** to **Personal**.



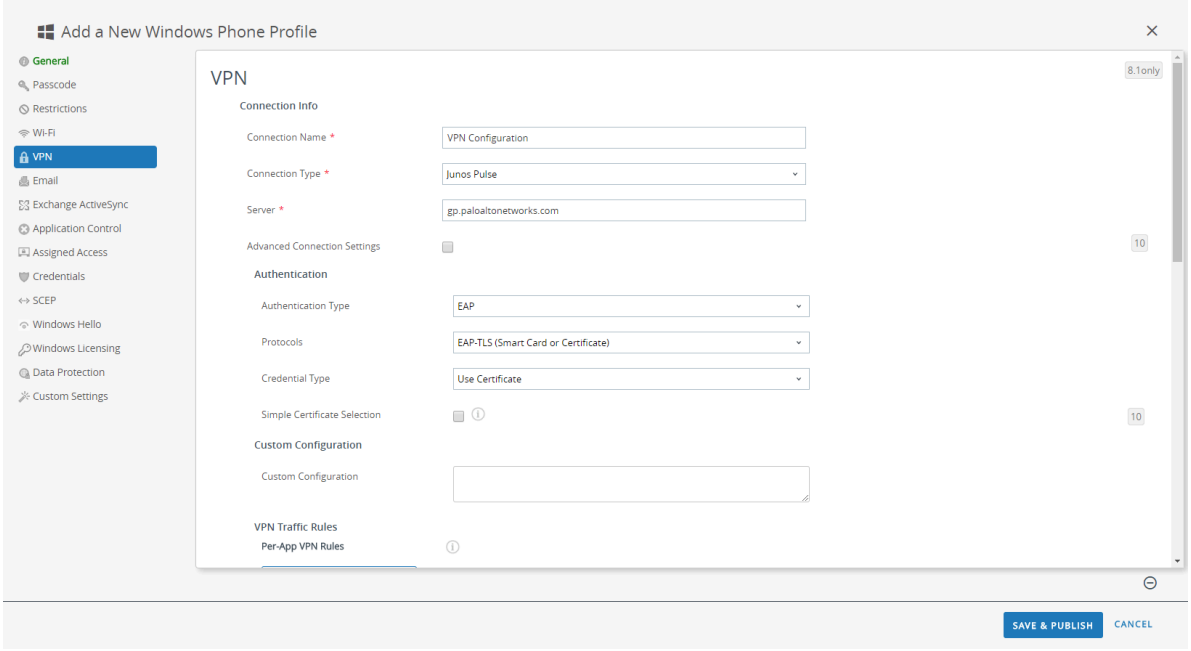
- To use a predefined certificate authority and template:
  1. Set the **Credential Source** to **Defined Certificate Authority**.
  2. Select the **Certificate Authority** from which you want obtain certificates.
  3. Select the **Certificate Template** for the certificate authority.
  4. Select the **Key Location** where you want to store the certificate's private key:
     - **TPM Required**—Store the private key on a Trusted Platform Module. If a Trusted Platform Module is not available on the endpoint, the private key cannot be installed.
     - **TPM If Present**—Store the private key on a Trusted Platform Module if one is available on the endpoint. If a Trusted Platform Module is not available on the endpoint, the private key is stored in the endpoint software.
     - **Software**—Store the private key in the endpoint software.
     - **Passport**—Save the private key to Microsoft Passport. To use this option, Workspace ONE Protection Agent must be installed on the endpoint.
  5. Set the **Certificate Store** to **Personal**.



STEP 5 | Configure the **VPN** settings:

1. Enter the **Connection Name** that the endpoint displays.
2. Select an alternate **Connection Type** provider (do not select **IKEv2**, **L2TP**, **PPTP**, or **Automatic**, as these do not have the associated vendor settings required for the GlobalProtect VPN profile).

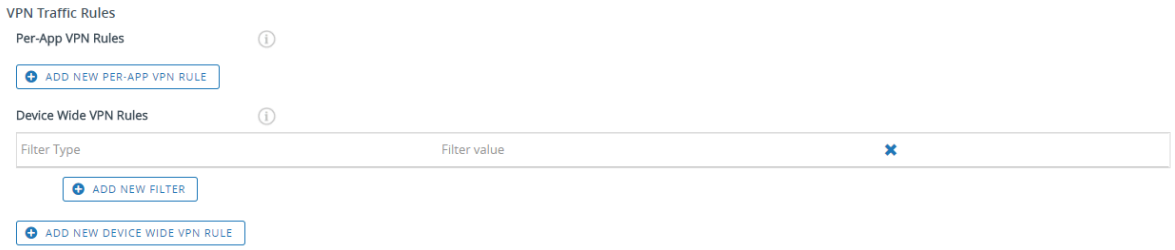
   You must select an alternate vendor because Workspace ONE has not yet listed GlobalProtect as an official connection provider for Windows endpoints.
3. In the **Server** field, enter the hostname or IP address of the GlobalProtect portal to which users connect.
4. In the Authentication area, select an **Authentication Type** to specify the method to authenticate end users.



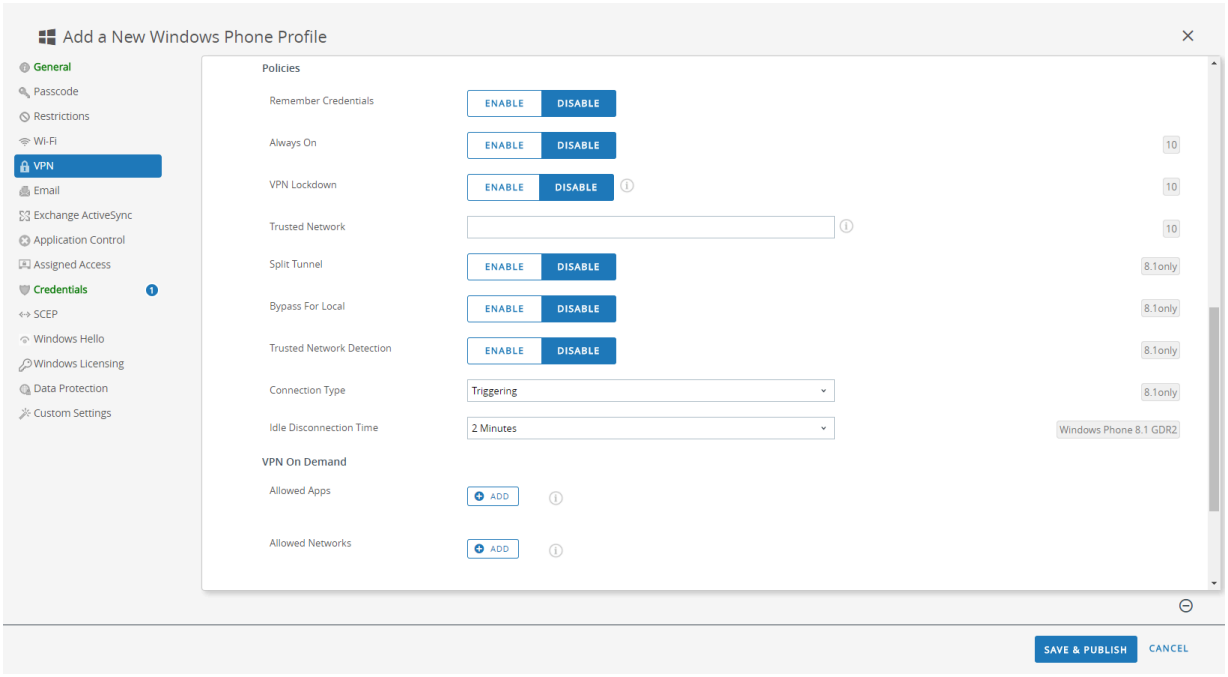
5. (Optional) To permit GlobalProtect to save user credentials, **ENABLE** the option to **Remember Credentials** in the Policies area.
6. (Optional) In the VPN Traffic Rules area, **ADD NEW DEVICE WIDE VPN RULE** to send traffic matching a specific route through the VPN tunnel. These rules are not bound by

application but are evaluated across the endpoint. If the traffic matches the specified match criteria, it is routed through the VPN tunnel.

Add match criteria by clicking **ADD NEW FILTER**. When prompted, enter a **Filter Type** and corresponding **Filter Value**.



7. To ensure that this profile uses the On-Demand connect method, configure the following settings in the Policies area:
   - **DISABLE Always On**. If this field is **ENABLED**, the secure connection is always on.
   - **DISABLE VPN Lockdown**. If this field is **ENABLED**, the secure connection is always on and connected, and network access is disabled when the app is not connected. The **VPN Lockdown** option in Workspace ONE is similar to the **Enforce GlobalProtect for Network Access** option that you would configure in a GlobalProtect portal configuration.



STEP 6 | **SAVE & PUBLISH** your changes.

STEP 7 | To set the connection type provider to GlobalProtect, edit the VPN profile in XML.

To minimize additional edits in the raw XML, review the settings in your VPN profile before you export the configuration. If you need to change a setting after you export the VPN profile, you can make the changes in the raw XML or, you can update the setting in the VPN profile and perform this step again.

1. In the **Devices** > **Profiles** > **List View**, select the radio button next to the new profile you added in the previous steps, and then select **</>XML** at the top of the table. Workspace ONE opens the XML view of the profile.
2. **Export** the profile and then open it in a text editor of your choice.
3. Edit the following settings for GlobalProtect:

- In the `LoclURI` element that specifies the `PluginPackageFamilyName`, change the element to:

  `<LocURI>./Vendor/MSFT/VPNv2/PaloAltoNetworks/PluginProfile/PluginPackageFamilyName</LocURI>`

- In the `Data` element that follows, change the value to:

  `<Data>PaloAltoNetworks.GlobalProtect_rn9aeerfb38dg</Data>`

1. Save your changes to the exported profile.
2. Return to Workspace ONE and select **Devices** > **Profiles** > **List View**.
3. Create (select **Add** > **Add Profile** > **Windows** > **Windows Phone**) and name a new profile.
4. Select **Custom Settings** > **Configure**, and then copy and paste the edited configuration.
5. **Save & Publish** your changes.

STEP 8 | Clean up the original profile by selecting the original profile from **Devices** > **Profiles** > **List View**, and then selecting **More Actions** > **Deactivate**. Workspace ONE moves the profile to the Inactive list.

STEP 9 | Test the configuration.

Configure a Per-App VPN Configuration for Windows 10 UWP Endpoints Using Workspace ONE

You can enable access to internal resources from your managed mobile endpoints by configuring GlobalProtect VPN access using Workspace ONE. In a per-app VPN configuration, you can specify which managed apps can send traffic through the GlobalProtect VPN tunnel. Unmanaged apps will continue to connect directly to the internet instead of through the GlobalProtect VPN tunnel.

Because Workspace ONE does not yet list GlobalProtect as an official connection provider for Windows endpoints, you must select an alternate VPN provider, edit the settings for the GlobalProtect app, and import the configuration back into the VPN profile as described in the following workflow.

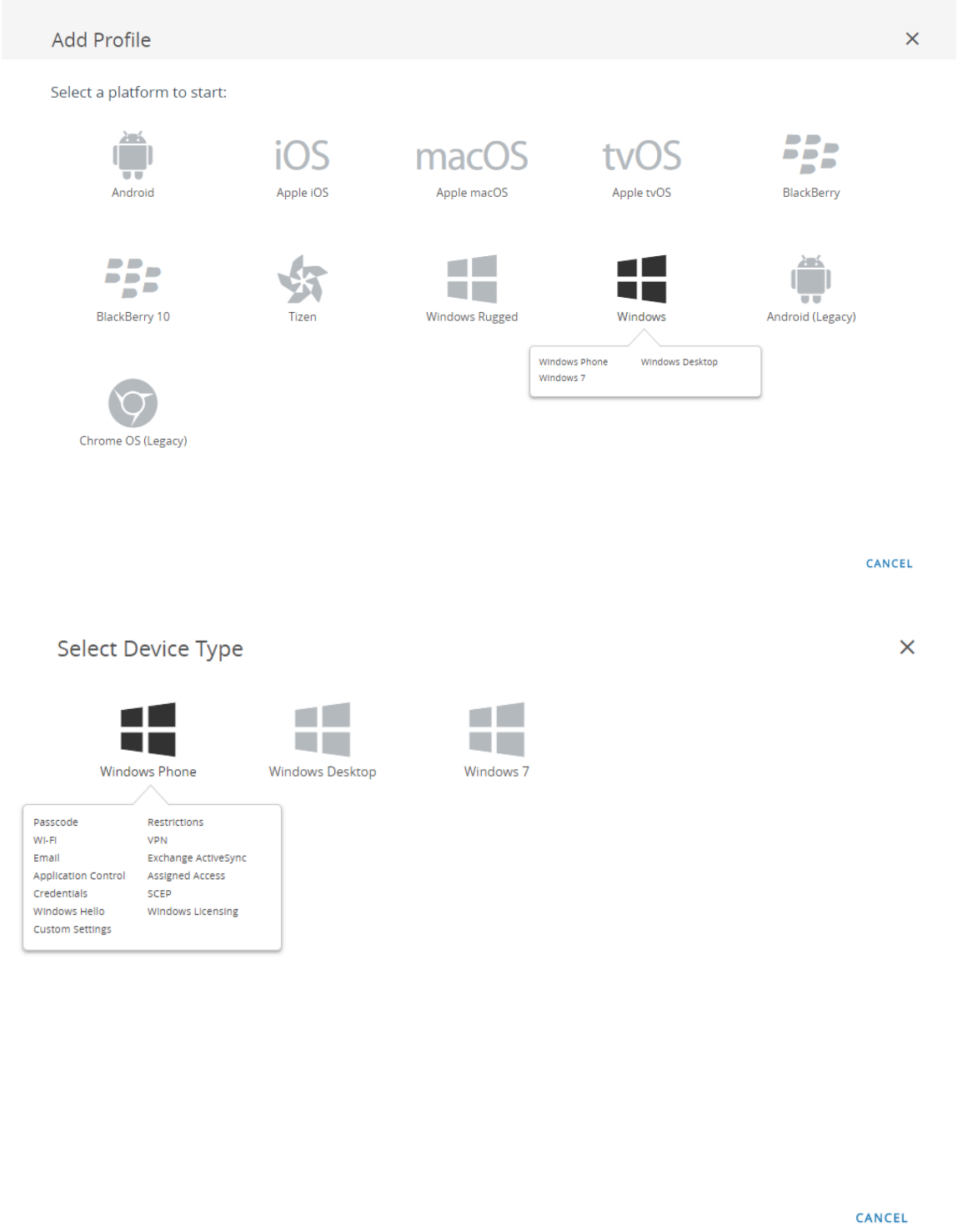
Use the following steps to configure a per-app VPN configuration for Windows 10 UWP endpoints using Workspace ONE:

STEP 1 | Download the GlobalProtect app for Windows 10 UWP:

- Deploy the GlobalProtect Mobile App Using Workspace ONE.
- Download the GlobalProtect app directly from the Microsoft Store.

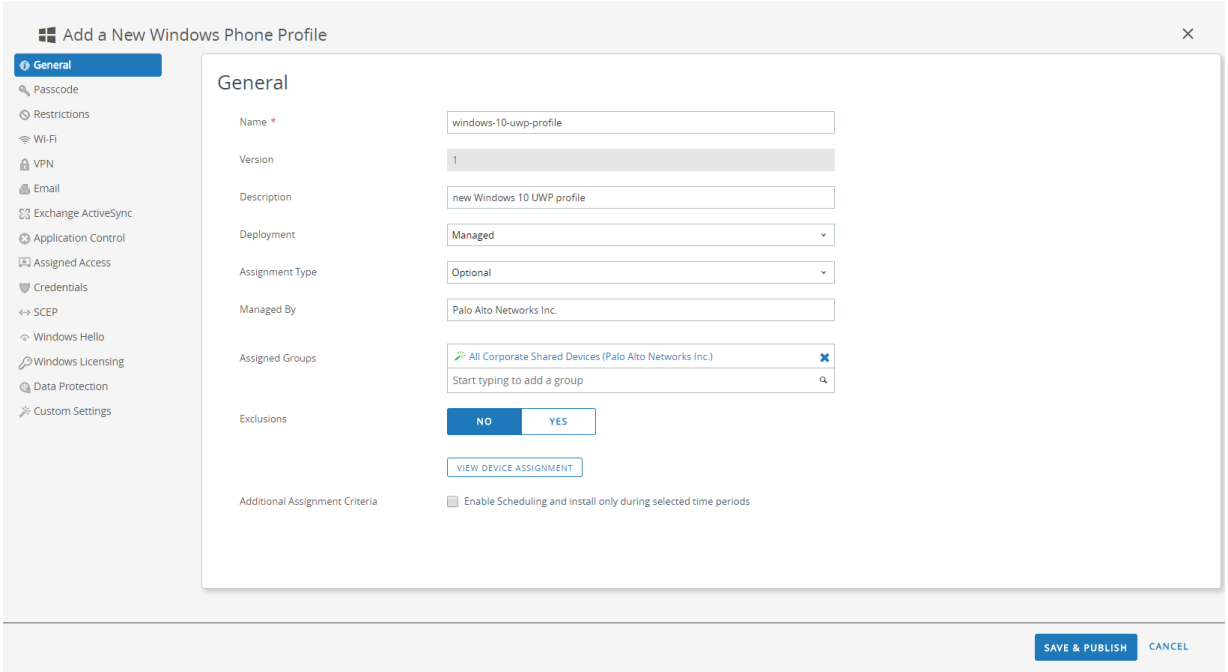
STEP 2 | From the Workspace ONE console, modify an existing Windows 10 UWP profile add a new one.

1. Select **Devices** > **Profiles & Resources** > **Profiles**, and then **ADD** a new profile.
2. Select **Windows** as the platform and **Windows Phone** as the device type.



STEP 3 | Configure the **General** settings:

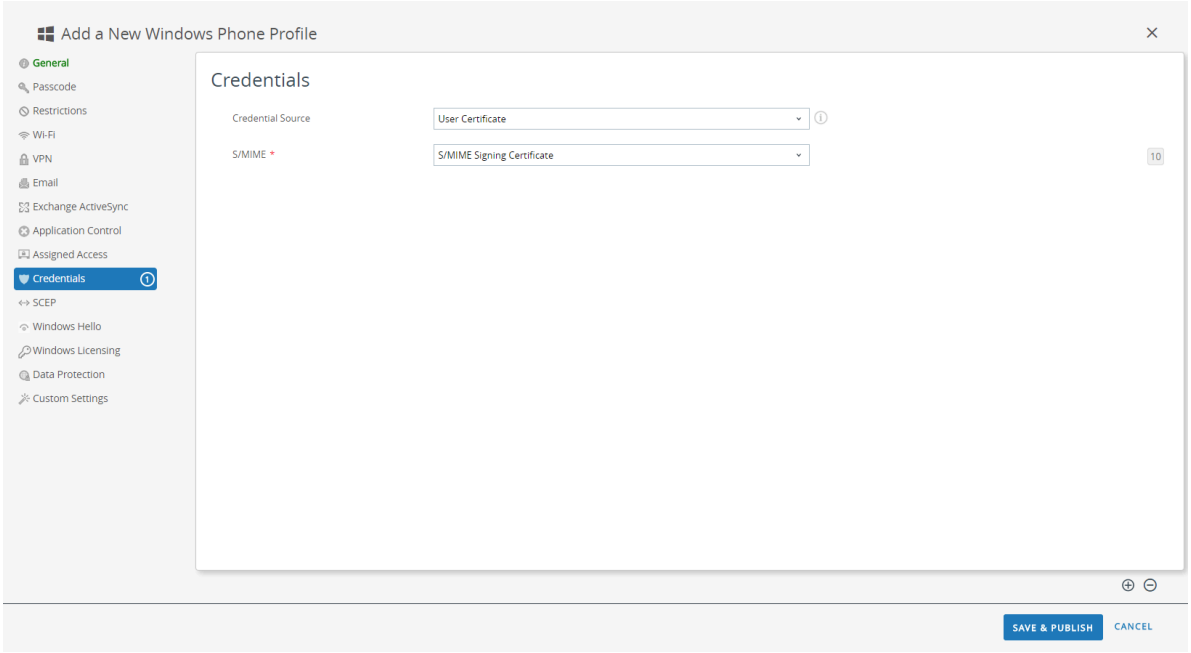
- Enter a **Name** for the profile.
- (Optional) Enter a brief **Description** of the profile that indicates its purpose.
- (Optional) Set the **Deployment** method to **Managed** to enable the profile to be removed automatically upon unenrollment
- (Optional) Select an **Assignment Type** to determine how the profile is deployed to endpoints. Select **Auto** to deploy the profile to all endpoints automatically, **Optional** to enable the end user to install the profile from the Self-Service Portal (SSP) or to manually deploy the profile to individual endpoints, or **Compliance** to deploy the profile when an end user violates a compliance policy applicable to the endpoint.
- (Optional) In the **Managed By** field, enter the Organization Group with administrative access to the profile.
- (Optional) In the **Assigned Groups** field, add the Smart Groups to which you want the profile added. This field includes an option to create a new Smart Group, which can be configured with specs for minimum OS, device models, ownership categories, organization groups, and more.
- (Optional) Indicate whether you want to include any **Exclusions** to the assignment of this profile. If you select **Yes**, the **Excluded Groups** field displays, enabling you to select the Smart Groups that you wish to exclude from the assignment of this profile.



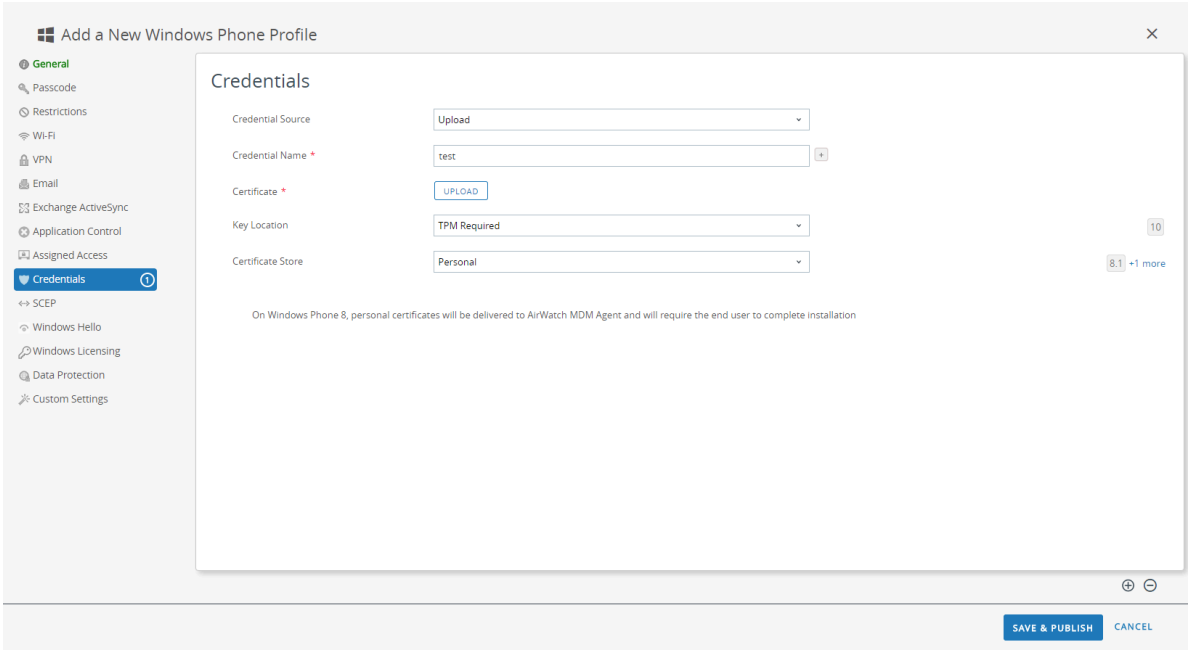
STEP 4 | Configure the **Credentials** settings:

All per-app VPN configurations require certificate-based authentication.

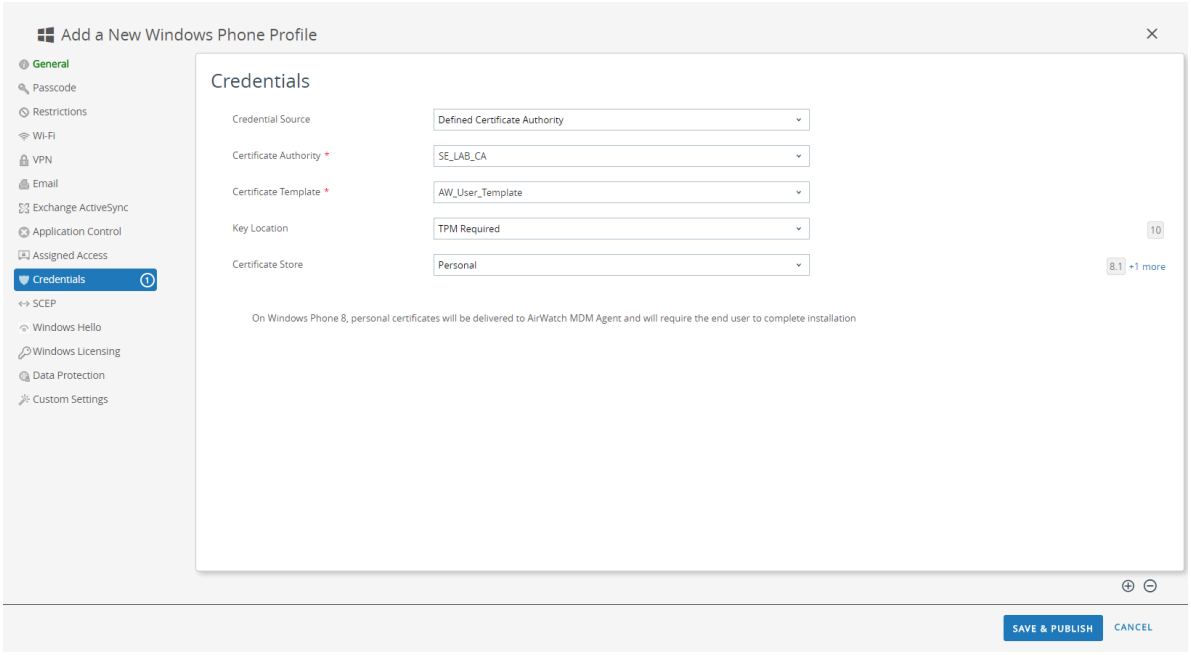
- To pull client certificates from Workspace ONE users:
  1. Set the **Credential Source** to **User Certificate**.
  2. Select the **S/MIME Signing Certificate** (default).



- To upload a client certificate manually:
  1. Set the **Credential Source** to **Upload**.
  2. Enter a **Credential Name**.
  3. Click **UPLOAD** to locate and select the certificate that you want to upload.
  4. After you select a certificate, click **SAVE**.
  5. Select the **Key Location** where you want to store the certificate's private key:
     - **TPM Required**—Store the private key on a Trusted Platform Module. If a Trusted Platform Module is not available on the endpoint, the private key cannot be installed.
     - **TPM If Present**—Store the private key on a Trusted Platform Module if one is available on the endpoint. If a Trusted Platform Module is not available on the endpoint, the private key is stored in the endpoint software.
     - **Software**—Store the private key in the endpoint software.
     - **Passport**—Save the private key to Microsoft Passport. To use this option, Workspace ONE Protection Agent must be installed on the endpoint.
  6. Set the **Certificate Store** to **Personal**.



- To use a predefined certificate authority and template:
  1. Set the **Credential Source** to **Defined Certificate Authority**.
  2. Select the **Certificate Authority** from which you want obtain certificates.
  3. Select the **Certificate Template** for the certificate authority.
  4. Select the **Key Location** where you want to store the certificate's private key:
     - **TPM Required**—Store the private key on a Trusted Platform Module. If a Trusted Platform Module is not available on the endpoint, the private key cannot be installed.
     - **TPM If Present**—Store the private key on a Trusted Platform Module if one is available on the endpoint. If a Trusted Platform Module is not available on the endpoint, the private key is stored in the endpoint software.
     - **Software**—Store the private key in the endpoint software.
     - **Passport**—Save the private key to Microsoft Passport. To use this option, Workspace ONE Protection Agent must be installed on the endpoint.
  5. Set the **Certificate Store** to **Personal**.

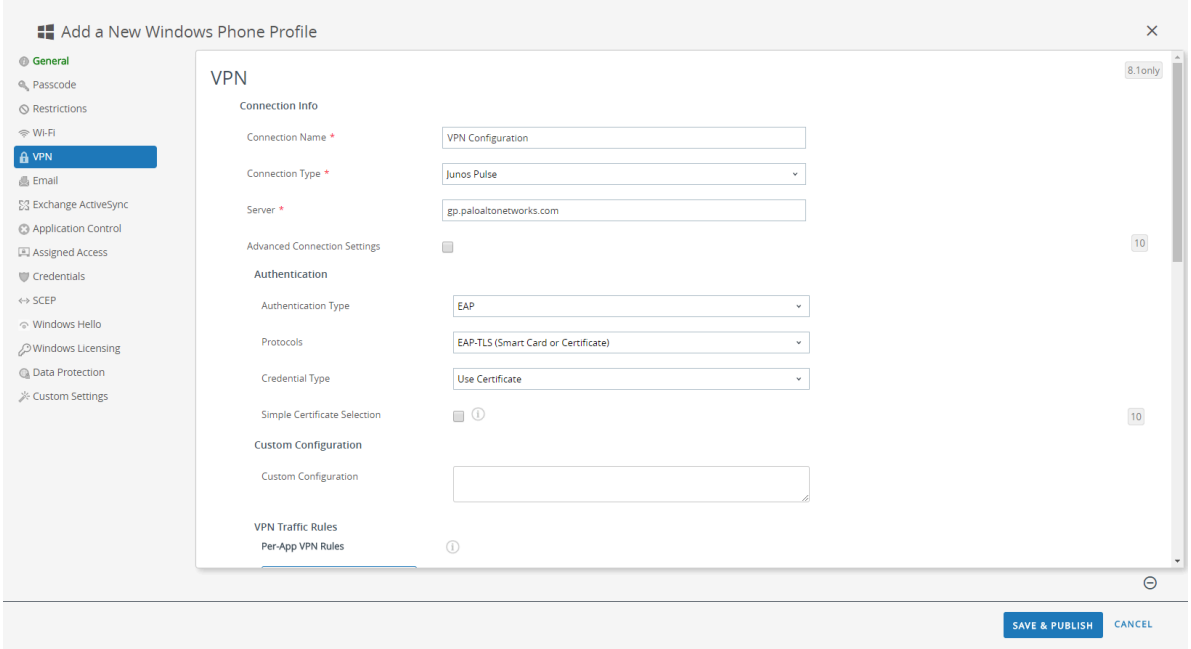


STEP 5 | Configure the **VPN** settings:

1. Enter the **Connection Name** that the endpoint displays.
2. Select an alternate **Connection Type** provider (do not select **IKEv2**, **L2TP**, **PPTP**, or **Automatic**, as these do not have the associated vendor settings required for the GlobalProtect VPN profile).

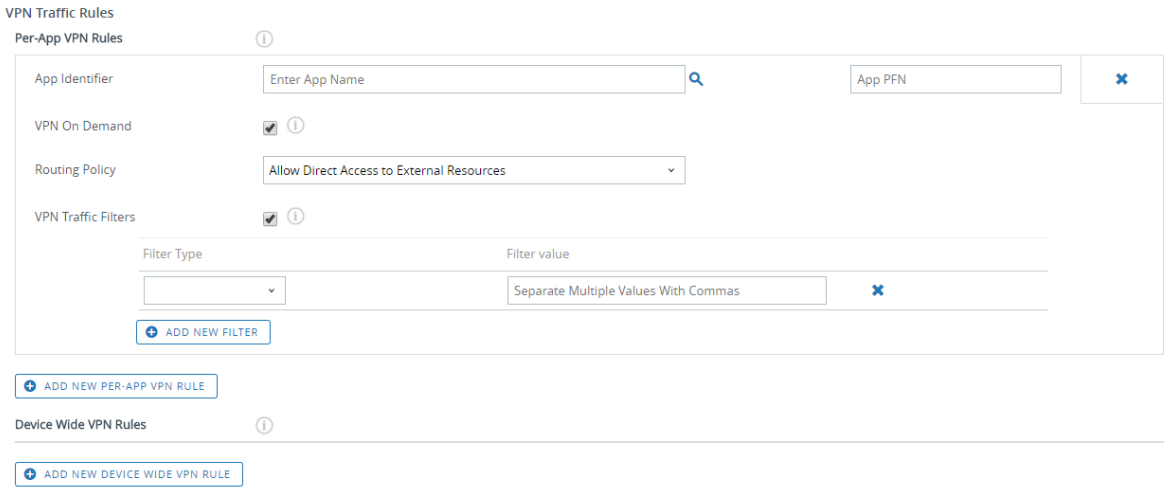
   You must select an alternate vendor because Workspace ONE has not yet listed GlobalProtect as an official connection provider for Windows endpoints.
3. In the **Server** field, enter the hostname or IP address of the GlobalProtect portal to which users connect.
4. In the Authentication area, select a certificate-based **Authentication Type** to specify the method to authenticate end users.

   All per-app VPN configurations require certificate-based authentication.



5. (Optional) To permit GlobalProtect to save user credentials, **ENABLE** the option to **Remember Credentials** in the Policies area.
6. In the VPN Traffic Rules area, **ADD NEW PER-APP VPN RULE** to specify rules for specific legacy apps (typically .exe files) or modern apps (typically downloaded from the Microsoft Store):
   1. (Optional) Enable **VPN On Demand** to allow the GlobalProtect connection to establish automatically when the app is launched.
   2. Select a **Routing Policy** to specify whether to send app traffic through the VPN tunnel.
   3. (Optional) Configure specific **VPN Traffic Filters** to route app traffic through the VPN tunnel only if it matches specific match criteria that you define, such as IP address and port.

Add match criteria by clicking **ADD NEW FILTER**. When prompted, enter a **Filter Name** and corresponding **Filter Value**.

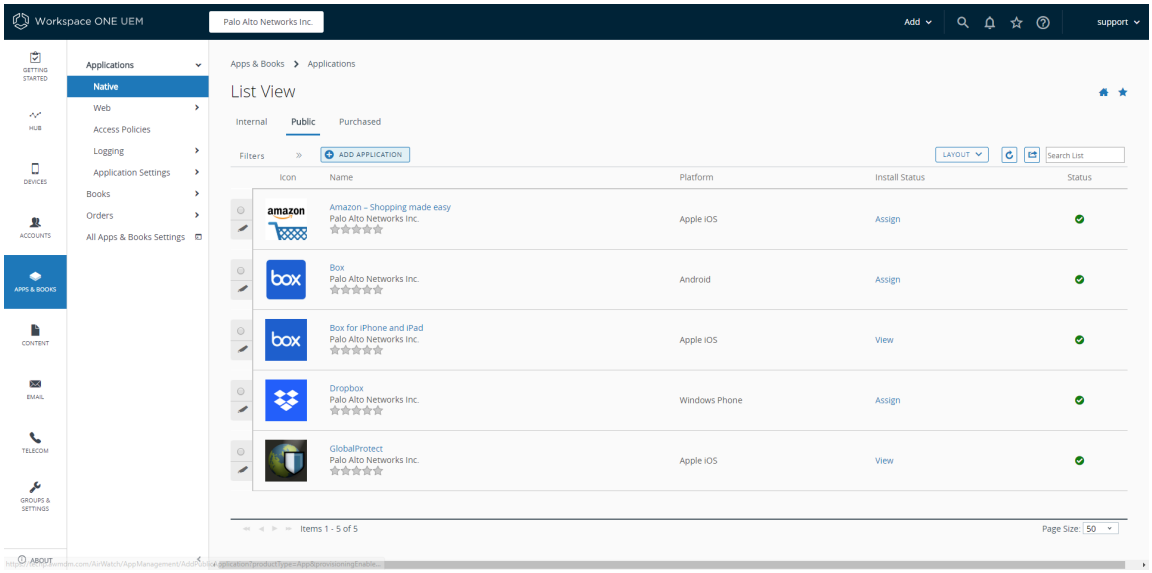


STEP 6 | **SAVE & PUBLISH** your changes.

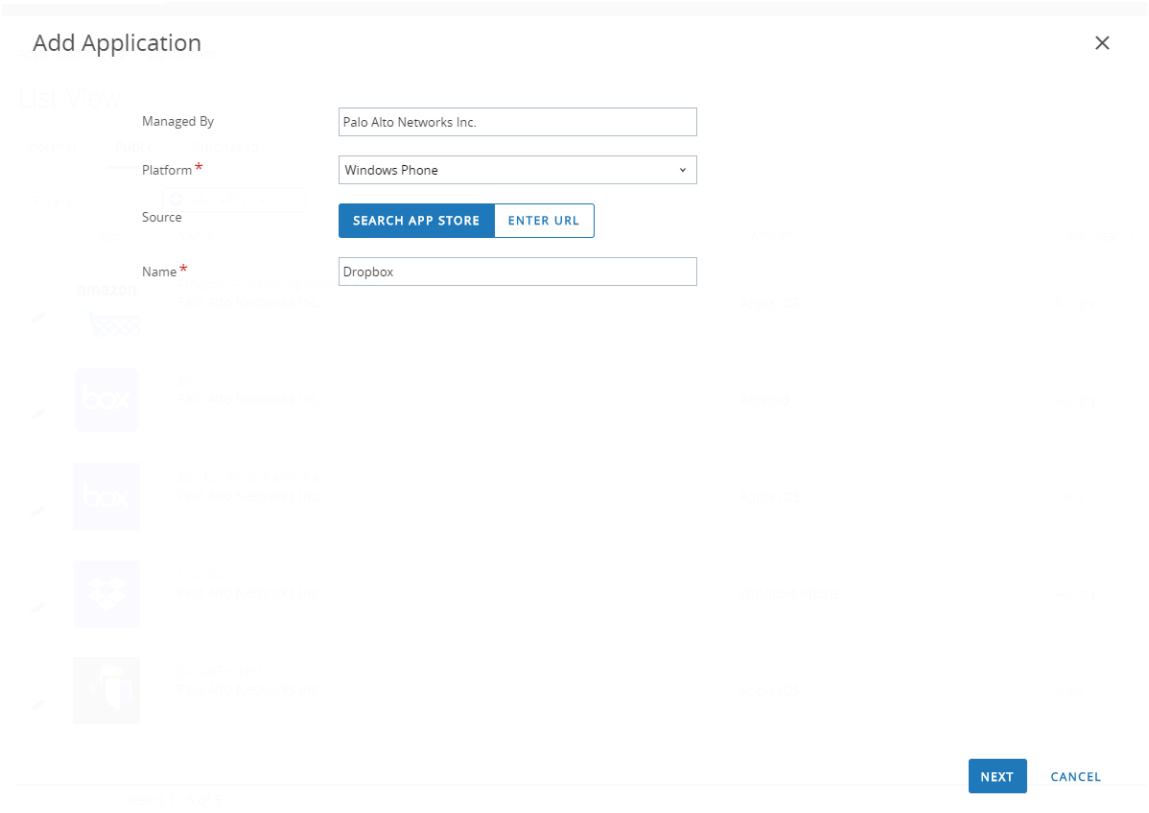
STEP 7 | Configure per-app VPN settings for a new managed app or modify the settings for an existing managed app.

After configuring the settings for the app and enabling per-app VPN, you can publish the app to a group of users and enable the app to send traffic through the GlobalProtect VPN tunnel.

1. Select **APPS & BOOKS** > **Applications** > **Native** > **Public**.
2. To add a new app, select **ADD APPLICATION**. To modify the settings for an existing app, locate the app in the list of Public apps and then select the edit (✎) icon in the actions menu next to the row.

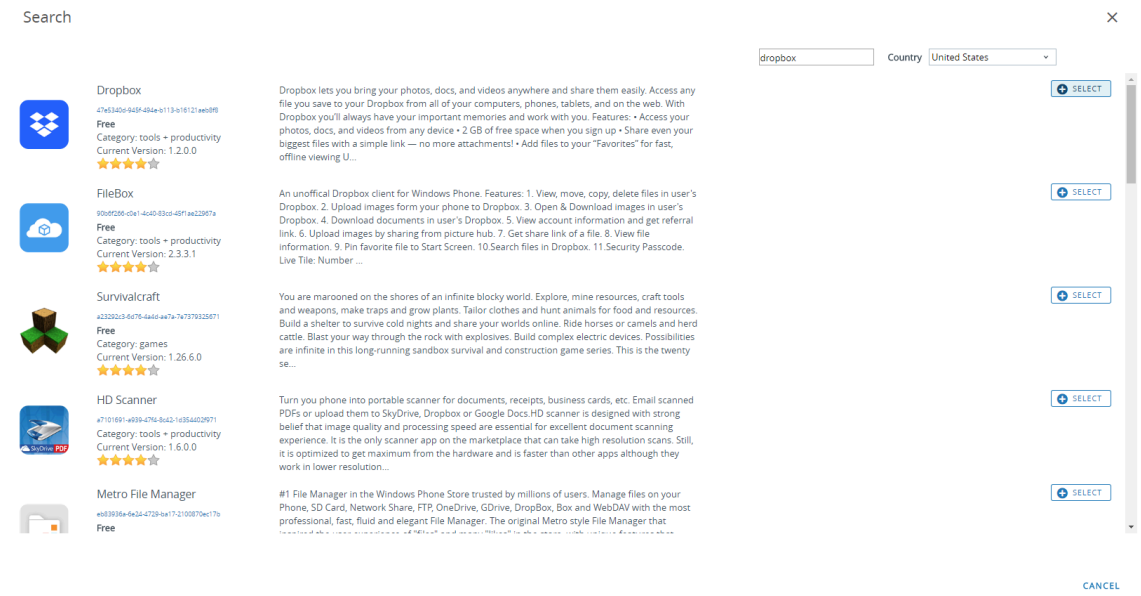


3. In the **Managed By** field, select the organization group that will manage this app.
4. Set the **Platform** to **Windows Phone**.
5. Select your preferred **Source** for locating the app:
   - **SEARCH APP STORE**—Enter the **Name** of the app.
   - **ENTER URL**—Enter the Microsoft Store URL for the app (for example, to search for the Dropbox mobile app by URL, enter https://www.microsoft.com/en-us/p/dropbox-mobile/9wzdncrfj0pk).



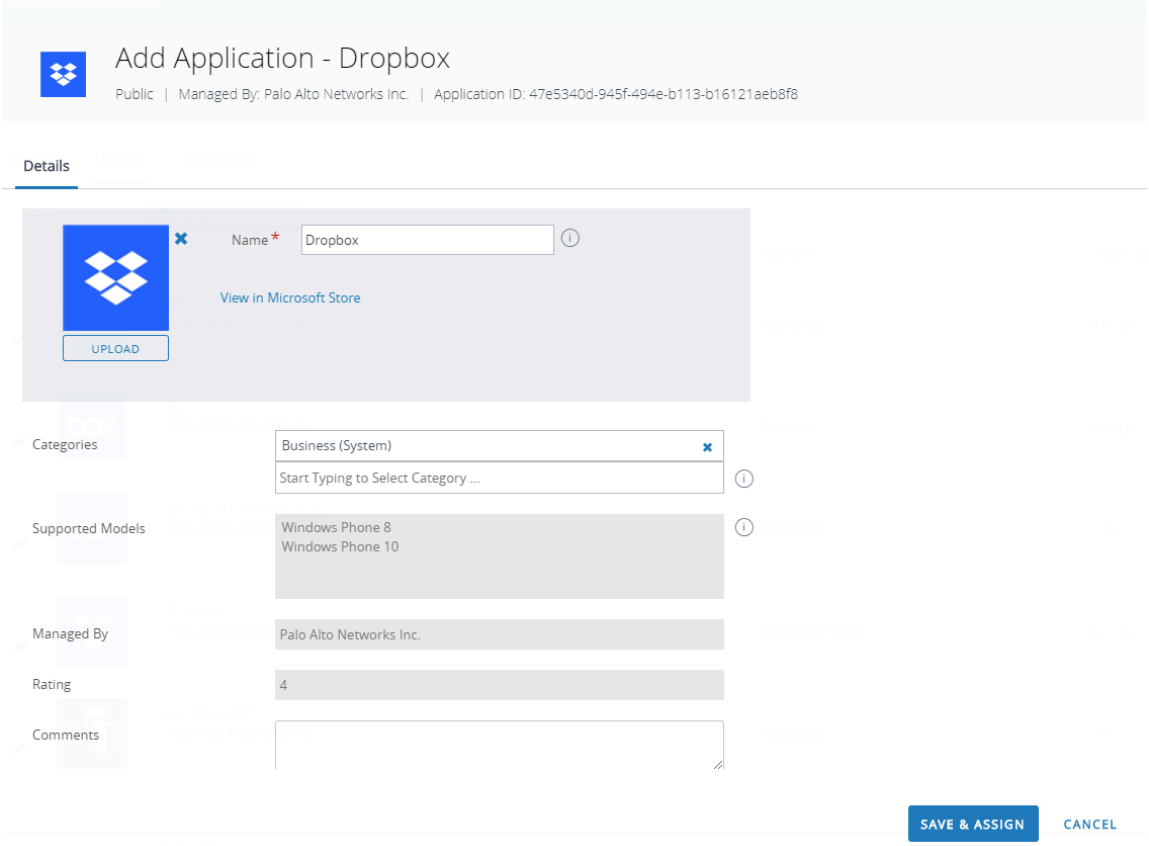
6. Click **NEXT**.

   If you chose to search the Microsoft Store, **SELECT** the app from the list of search results.

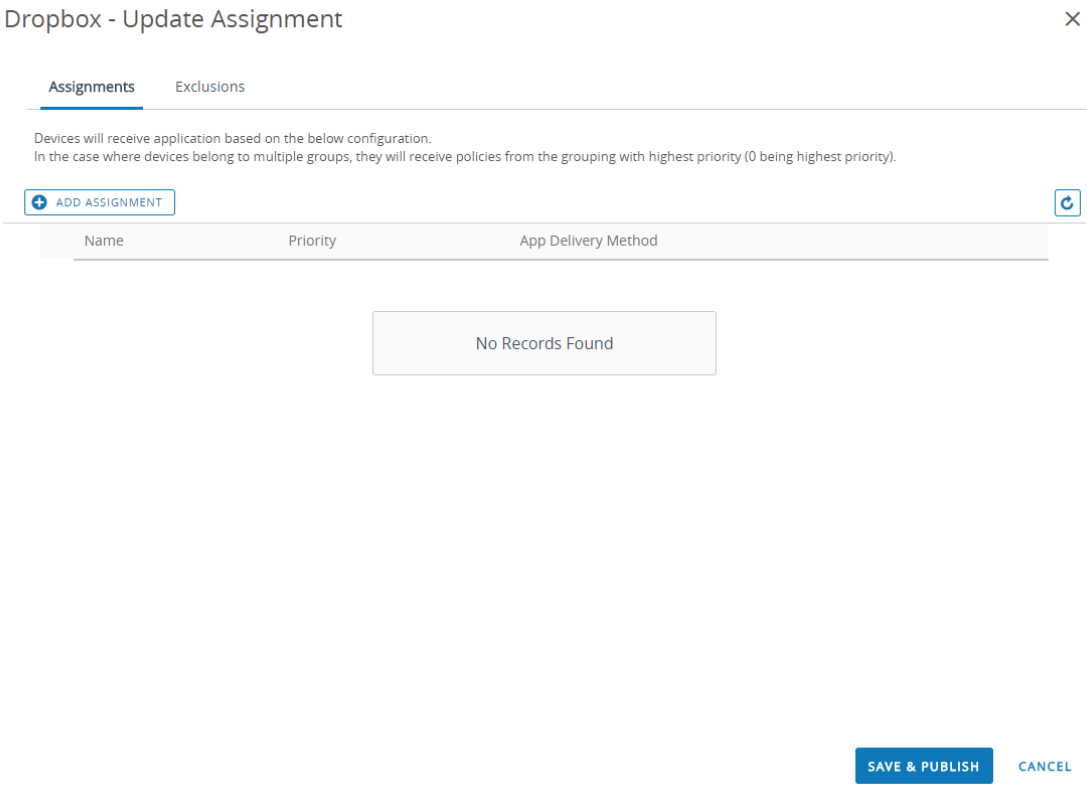


7. On the Add Application dialog, ensure that the app **Name** is correct. This is the name that will appear in the Workspace ONE App Catalog.

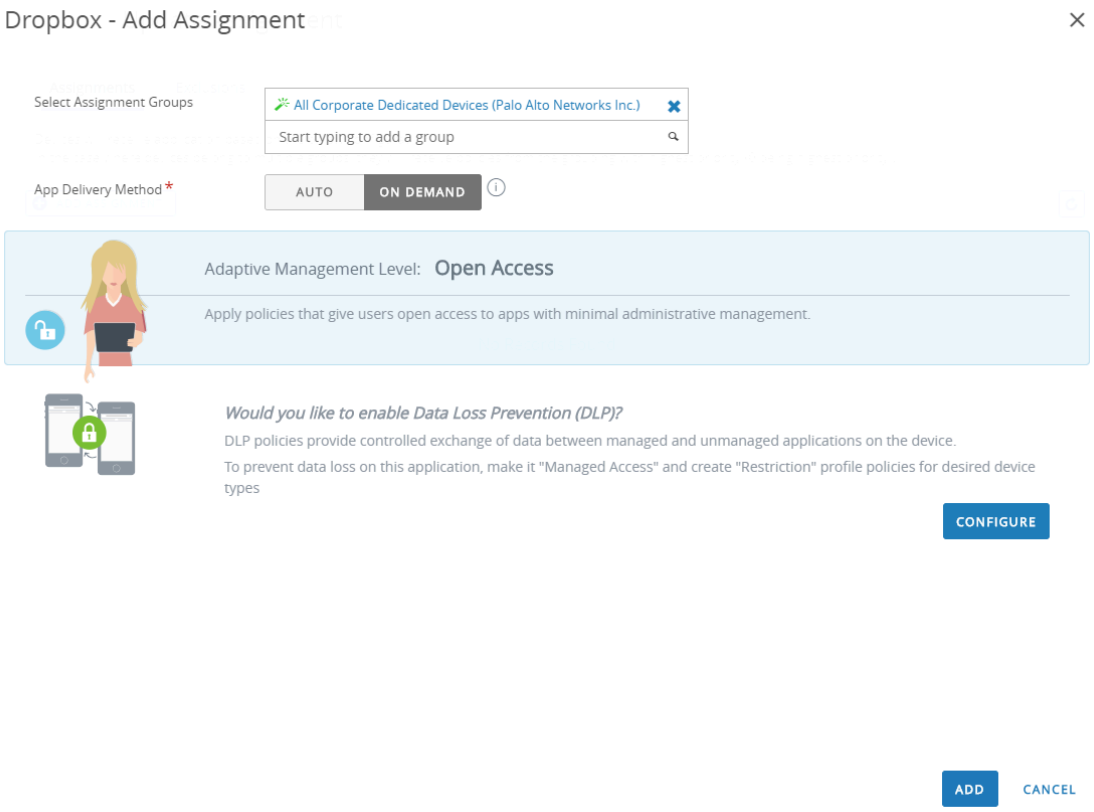
8. (Optional) Assign the app to pre-defined or custom **Categories** for ease-of-access in the Workspace ONE App Catalog.



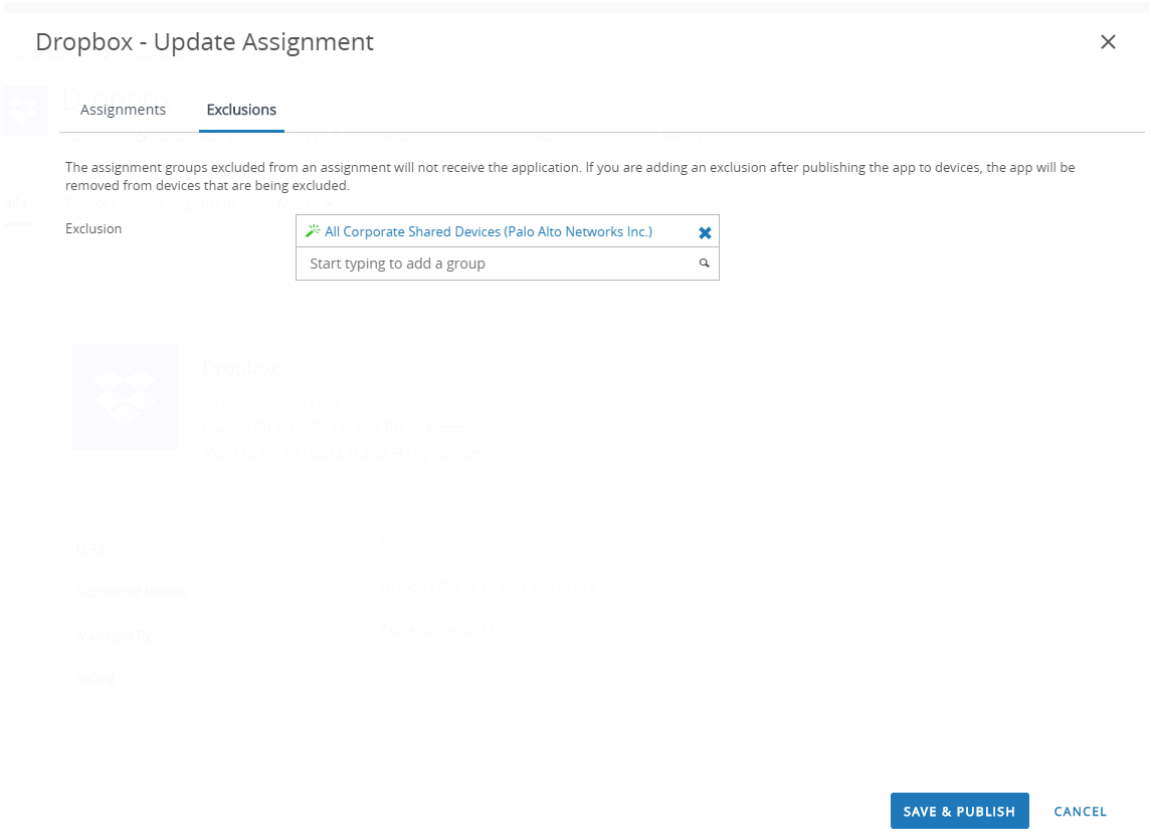
9. **SAVE & ASSIGN** the new app.
10. On the Update Assignment dialog, select **Assignments** and then click **ADD ASSIGNMENT** to add the Smart Groups that will have access to this app.



1. In the **Select Assignment Groups** field, select the Smart Groups that you want to grant access to this app.
2. Select the **App Delivery Method**. If you select **AUTO**, the app is automatically deployed to the specified Smart Groups. If you select **ON DEMAND**, the app must be deployed manually.
3. **ADD** the new assignment.



11. (Optional) To exclude certain Smart Groups from accessing the app, select **Exclusions** and then select the Smart Groups that you want to exclude from the **Exclusion** field.



12. **SAVE & PUBLISH** the configuration to the assigned Smart Groups.

STEP 8 | To set the connection type provider to GlobalProtect, edit the VPN profile in XML.

To minimize additional edits in the raw XML, review the settings in your VPN profile before you export the configuration. If you need to change a setting after you export the VPN profile, you can make the changes in the raw XML or, you can update the setting in the VPN profile and perform this step again.

1. In the **Devices** > **Profiles** > **List View**, select the radio button next to the new profile you added in the previous steps, and then select **</>XML** at the top of the table. Workspace ONE opens the XML view of the profile.
2. **Export** the profile and then open it in a text editor of your choice.
3. Edit the following settings for GlobalProtect:

- In the `LoclURI` element that specifies the `PluginPackageFamilyName`, change the element to:

  `<LocURI>./Vendor/MSFT/VPNv2/PaloAltoNetworks/PluginProfile/PluginPackageFamilyName</LocURI>`

- In the `Data` element that follows, change the value to:

  `<Data>PaloAltoNetworks.GlobalProtect_rn9aeerfb38dg</Data>`

1. Save your changes to the exported profile.
2. Return to Workspace ONE and select **Devices** > **Profiles** > **List View**.
3. Create (select **Add** > **Add Profile** > **Windows** > **Windows Phone**) and name a new profile.
4. Select **Custom Settings** > **Configure**, and then copy and paste the edited configuration.
5. **Save & Publish** your changes.

STEP 9 | Clean up the original profile by selecting the original profile from **Devices** > **Profiles** > **List View**, and then selecting **More Actions** > **Deactivate**. Workspace ONE moves the profile to the Inactive list.

STEP 10 | Test the configuration.

Configure Workspace ONE for Android Endpoints

Refer to the following sections for information on how to set up VPN configurations for Android endpoints using Workspace ONE:

- Configure a Per-App VPN Configuration for Android Endpoints Using Workspace ONE

Configure a Per-App VPN Configuration for Android Endpoints Using Workspace ONE

You can enable access to internal resources from your managed mobile endpoints by configuring GlobalProtect VPN access using Workspace ONE. In a per-app VPN configuration, you can specify which managed apps can send traffic through the GlobalProtect VPN tunnel. Unmanaged apps will continue to connect directly to the internet instead of through the GlobalProtect VPN tunnel.

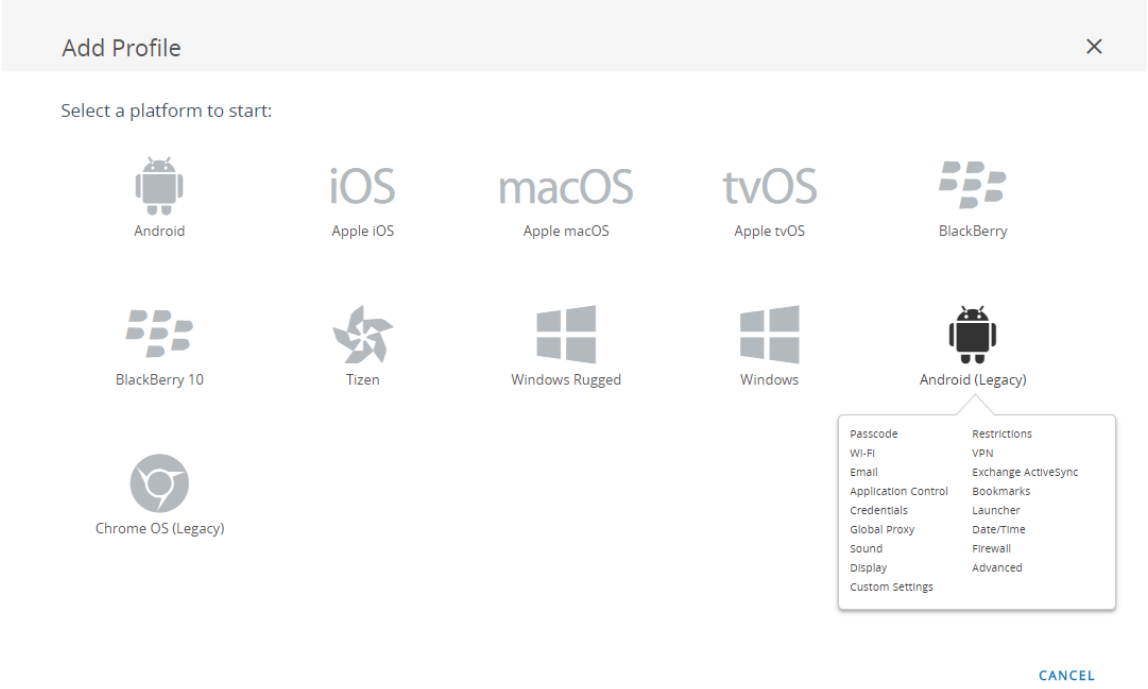
Use the following steps to configure a per-app VPN configuration for Android endpoints using Workspace ONE:

STEP 1 | Download the GlobalProtect app for Android:

- Deploy the GlobalProtect Mobile App Using Workspace ONE.
- Download the GlobalProtect app directly from Google Play.

STEP 2 | From the Workspace ONE console, modify an existing Android profile or add a new one.

1. Select **Devices** > **Profiles & Resources** > **Profiles**, and then **ADD** a new profile.
2. Select **Android (Legacy)** from the platform list.

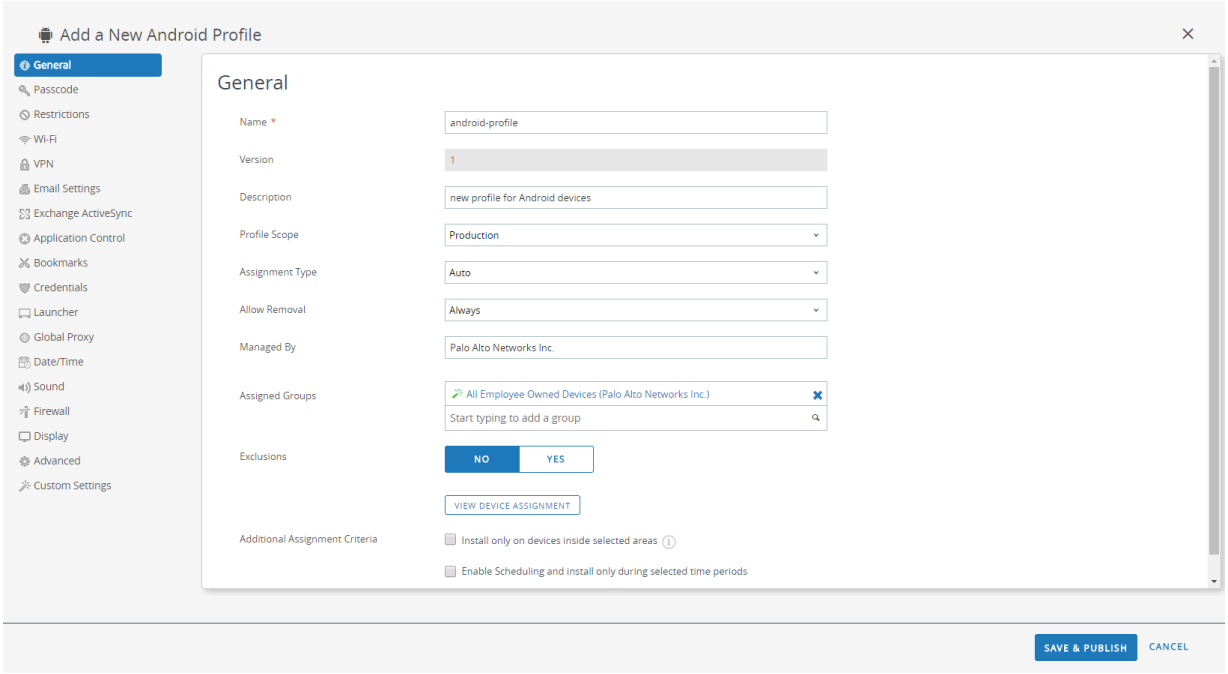


STEP 3 | Configure the **General** settings:

1. Enter a **Name** for the profile.
2. (Optional) Enter a brief **Description** of the profile that indicates its purpose.
3. (Optional) Select the **Profile Scope**, either **Production, Staging**, or **Both**.
4. (Optional) Select an **Assignment Type** to determine how the profile is deployed to endpoints. Select **Auto** to deploy the profile to all endpoints automatically, **Optional** to enable the end user to install the profile from the Self-Service Portal (SSP) or to manually deploy the profile to individual endpoints, or **Compliance** to deploy the profile when an end user violates a compliance policy applicable to the endpoint.
5. (Optional) Select whether or not you want to **Allow Removal** of the profile by the end user. Select **Always** to enable the end user to manually remove the profile at any time, **Never** to prevent the end user from removing the profile, or **With Authorization** to enable the

end user to remove the profile with the authorization of the administrator. Choosing **With Authorization** adds a required Password.

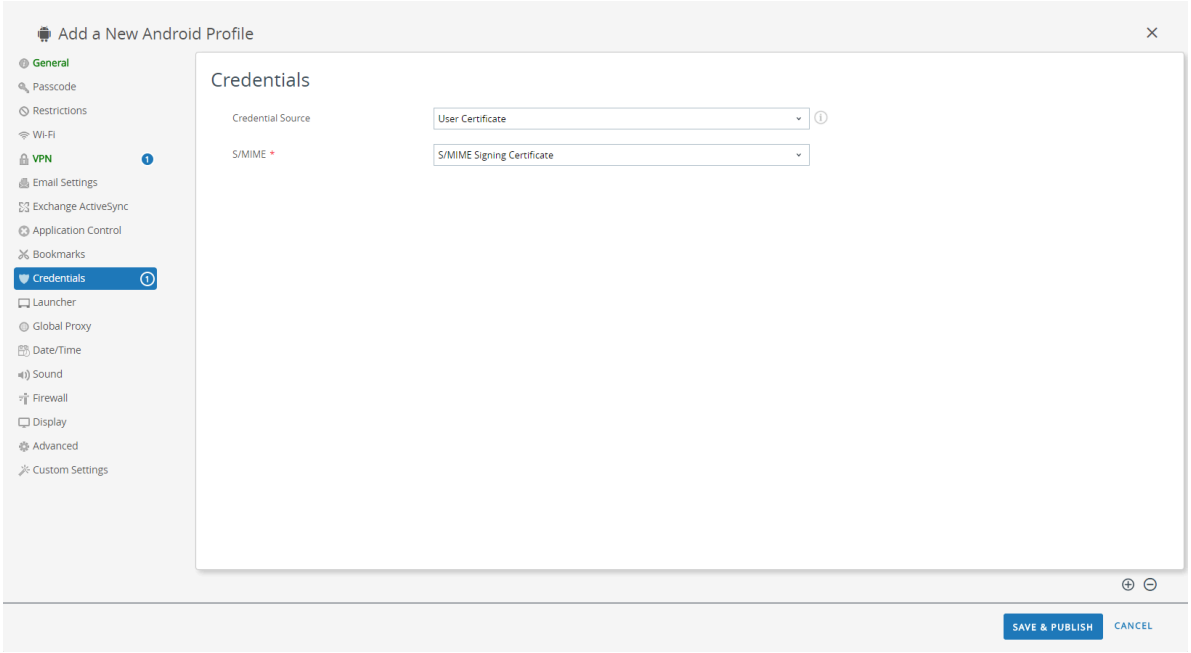
6. (Optional) In the **Managed By** field, enter the Organization Group with administrative access to the profile.
7. (Optional) In the **Assigned Groups** field, add the Smart Groups to which you want the profile added. This field includes an option to create a new Smart Group, which can be configured with specs for minimum OS, device models, ownership categories, organization groups, and more.
8. (Optional) Indicate whether you want to include any **Exclusions** to the assignment of this profile. If you select **Yes**, the **Excluded Groups** field displays, enabling you to select the Smart Groups that you wish to exclude from the assignment of this profile.



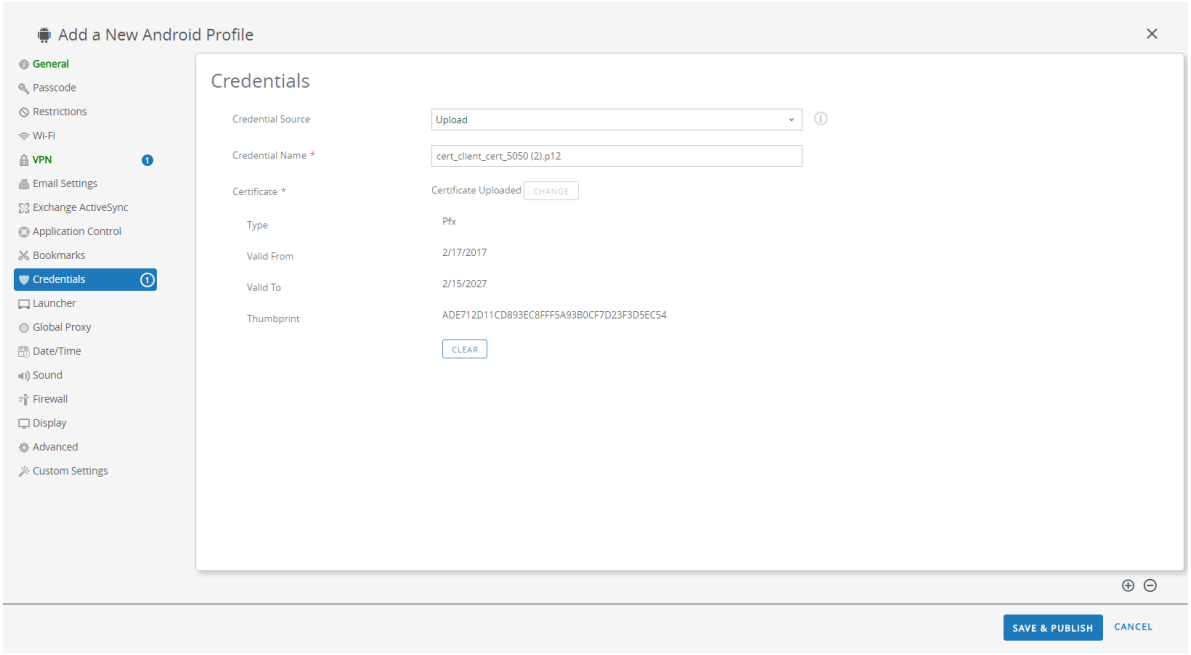
STEP 4 | Configure the **Credentials** settings:

All per-app VPN configurations require certificate-based authentication.

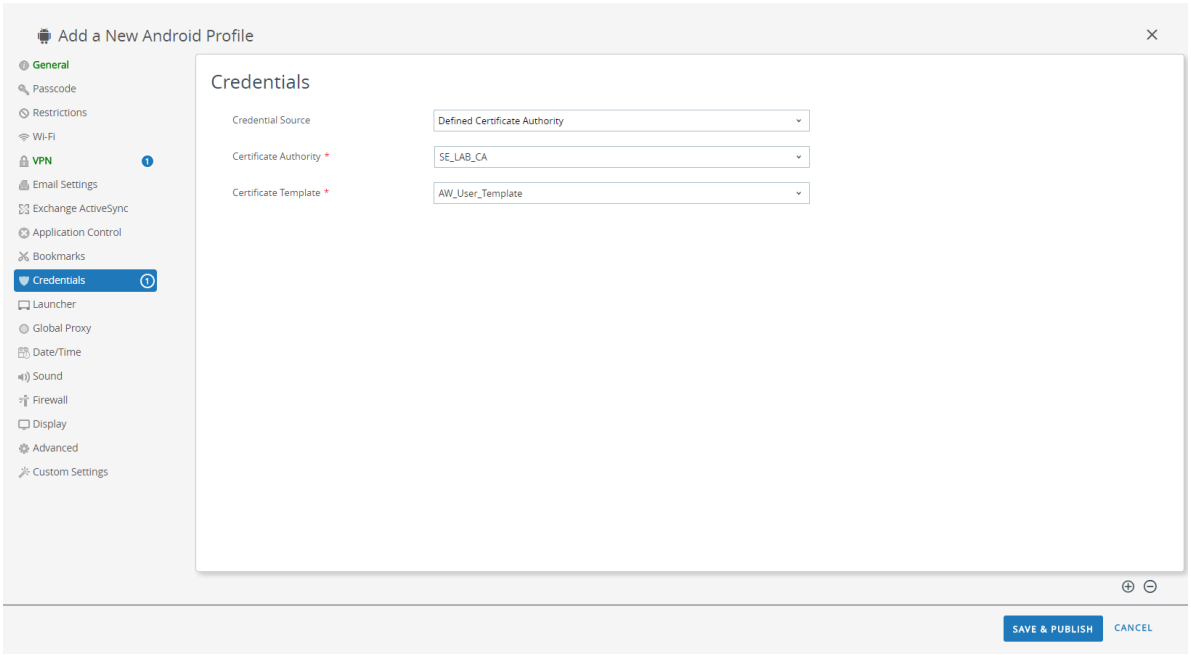
- To pull client certificates from Workspace ONE users:
  1. Set the **Credential Source** to **User Certificate**.
  2. Select the **S/MIME Signing Certificate** (default).



- To upload a client certificate manually:
  1. Set the **Credential Source** to **Upload**.
  2. Enter a **Credential Name**.
  3. Click **UPLOAD** to locate and select the certificate that you want to upload.
  4. After you select a certificate, click **SAVE**.



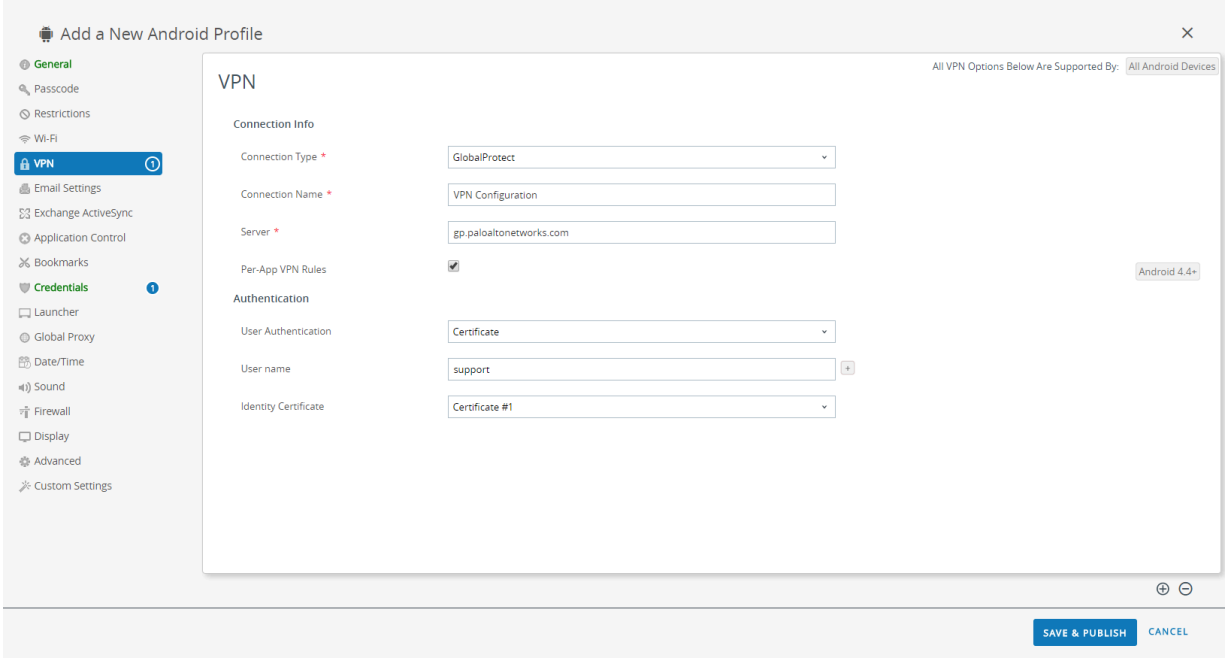
- To use a predefined certificate authority and template:
  1. Set the **Credential Source** to **Defined Certificate Authority**.
  2. Select the **Certificate Authority** from which you want obtain certificates.
  3. Select the **Certificate Template** for the certificate authority.



STEP 5 | Configure the **VPN** settings:

1. Set the network **Connection Type** to **GlobalProtect**.
2. Enter the **Connection Name** that the endpoint displays.
3. In the **Server** field, enter the hostname or IP address of the GlobalProtect portal to which users connect.
4. Enable **Per-App VPN Rules** to route all traffic for managed apps through the GlobalProtect VPN tunnel.
5. In the Authentication area, set the **User Authentication** method to **Certificate**.

   All per-app VPN configurations require certificate-based authentication.
6. Enter the **User name** for the VPN account or click the add (**+**) button to view supported lookup values that you can insert.
7. When prompted, select the **Identity Certificate** that GlobalProtect will use to authenticate users. The **Identity Certificate** is the same certificate that you configured in the **Credentials** settings.

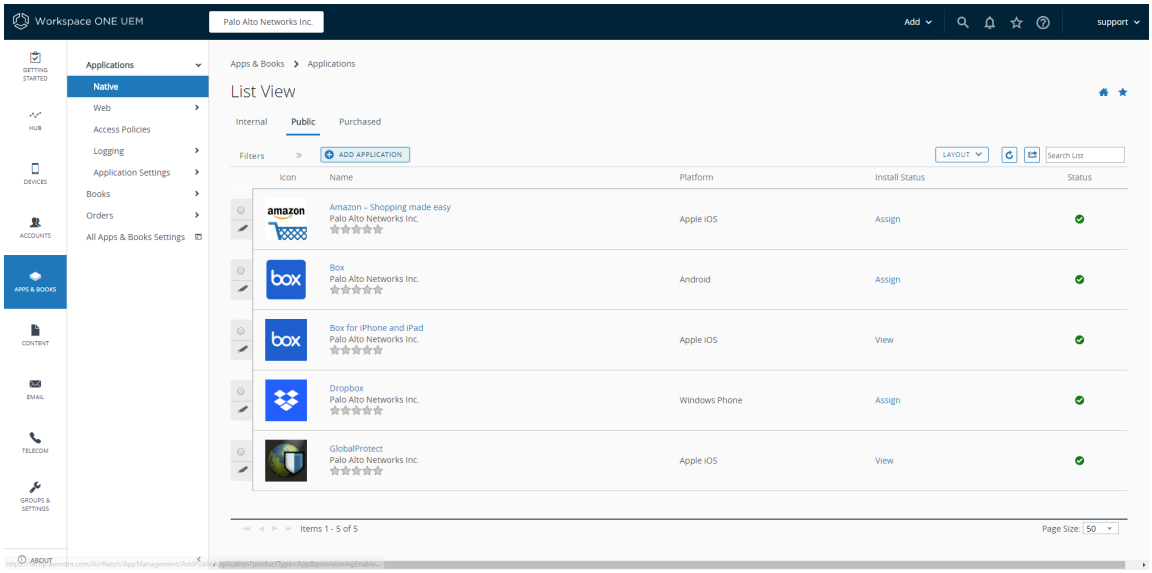


STEP 6 | **SAVE & PUBLISH** your changes.

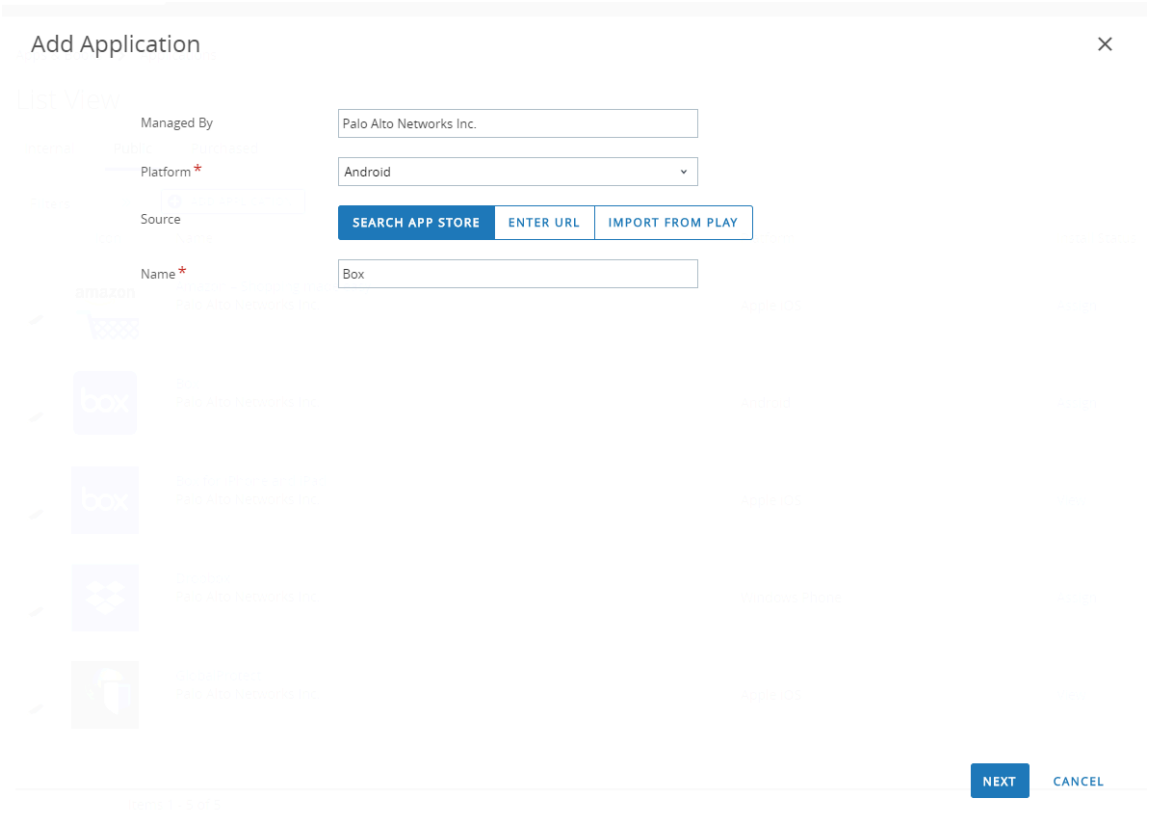
STEP 7 | Configure per-app VPN settings for a new managed app or modify the settings for an existing managed app.

After configuring the settings for the app and enabling per-app VPN, you can publish the app to a group of users and enable the app to send traffic through the GlobalProtect VPN tunnel.

1. Select **APPS & BOOKS** > **Applications** > **Native** > **Public**.
2. To add a new app, select **ADD APPLICATION**. To modify the settings for an existing app, locate the app in the list of Public apps (List View) and then select the edit (✎) icon in the actions menu next to the row.

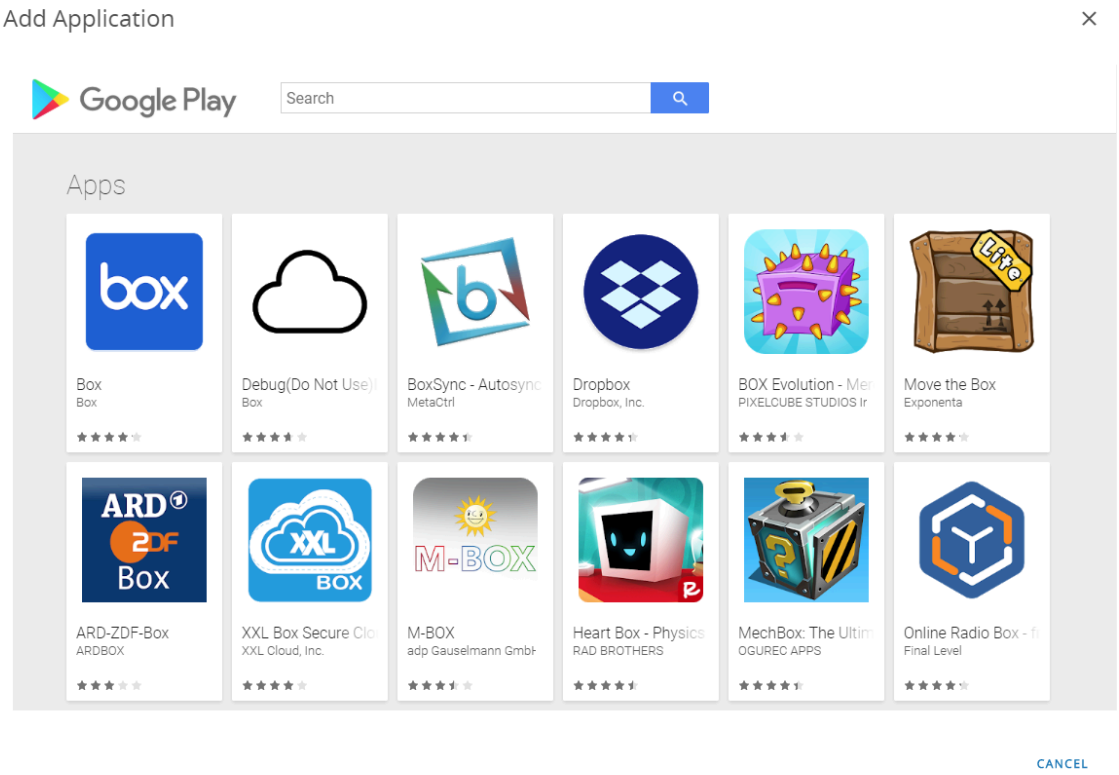


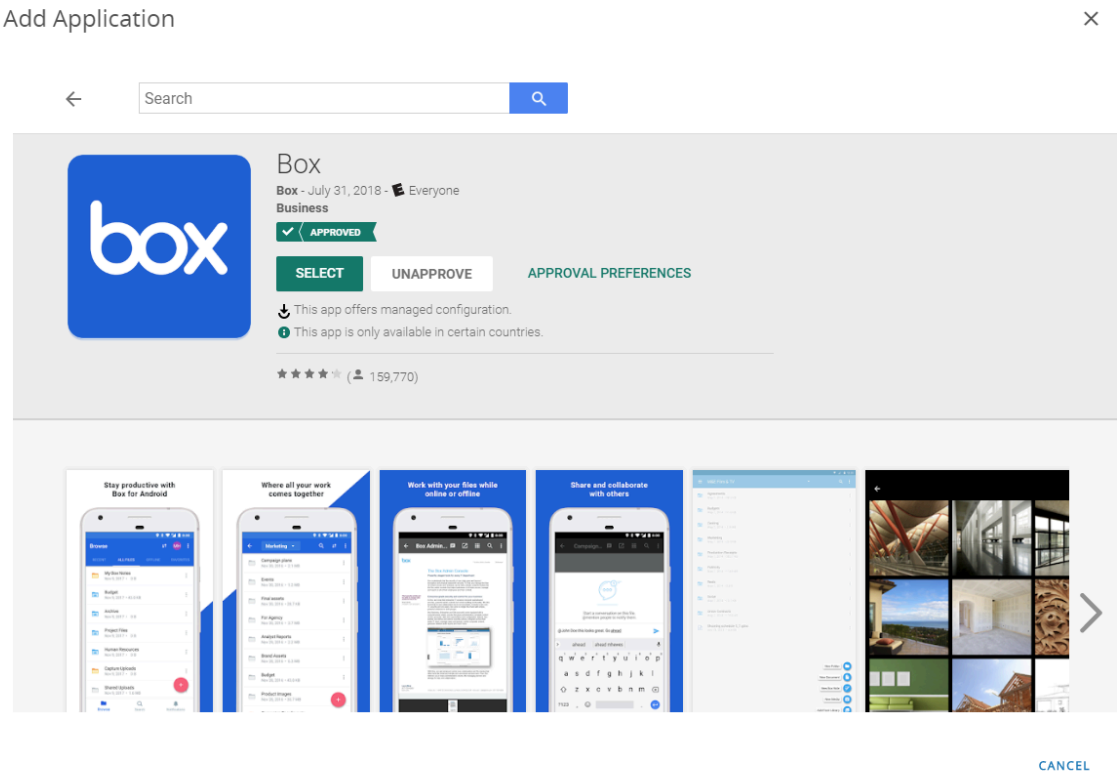
3. In the **Managed By** field, select the organization group that will manage this app.
4. Set the **Platform** to **Android**.
5. Select your preferred **Source** for locating the app:
   - **SEARCH APP STORE**—Enter the **Name** of the app.
   - **ENTER URL**—Enter the Google Play URL for the app (for example, to search for the Box app by URL, enter https://play.google.com/store/apps/details?id=com.box.android).
   - **IMPORT FROM PLAY**—Import a company-approved app from Google Play.



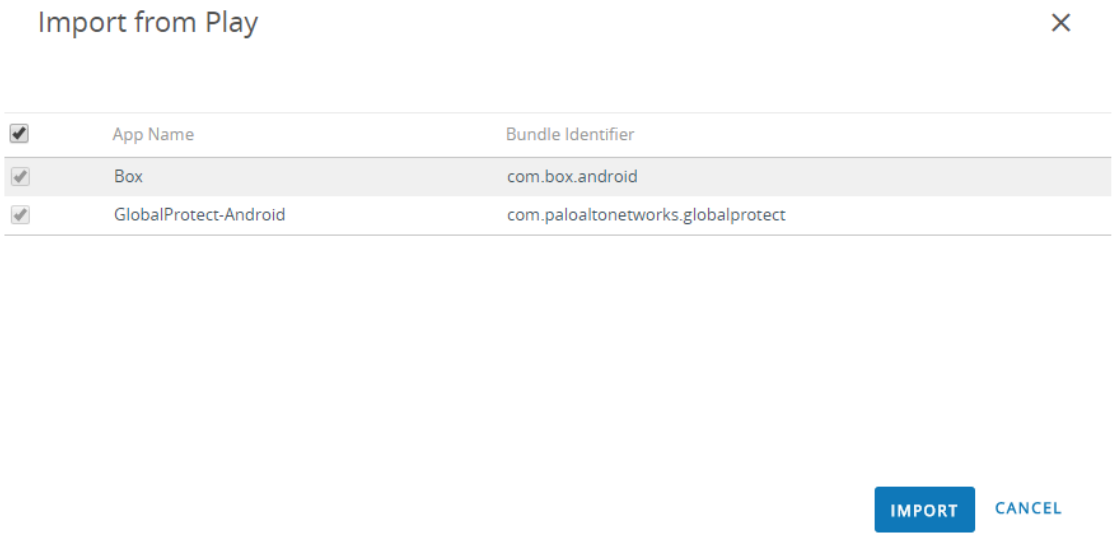
6. Click **NEXT**.

   If you chose to search Google Play, click the app icon from the list of search results. If the app has not already been approved for your company, you must **APPROVE** the app. After the app is approved, **SELECT** the app.

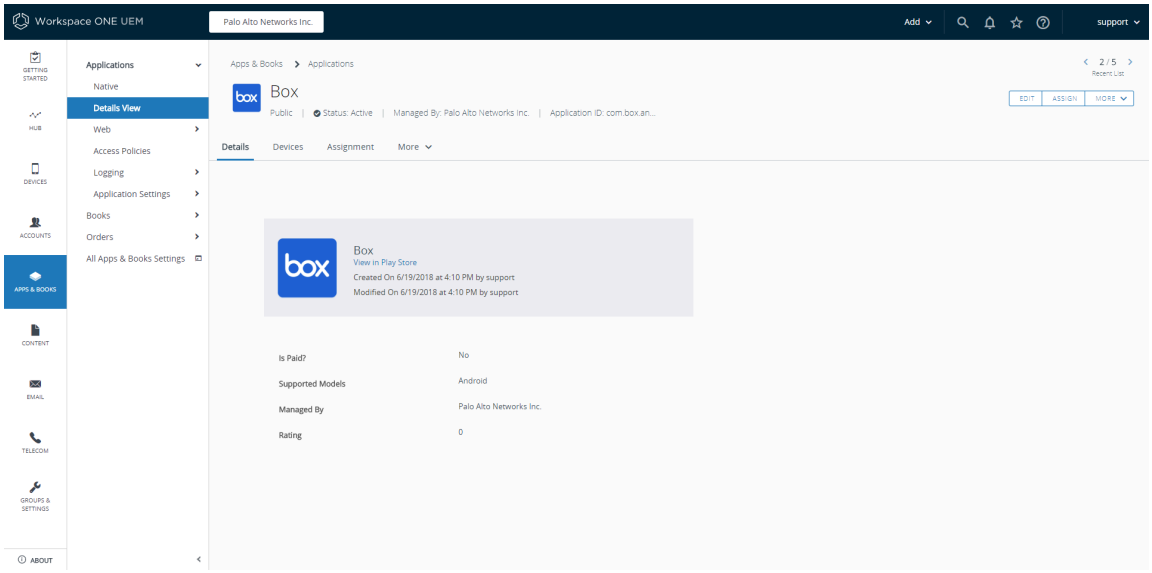




If you chose to import the app from Google Play, select the app from the list of approved company apps and then click **IMPORT**. If you do not see the app in the list, contact your Android for Work administrator to approve the app.

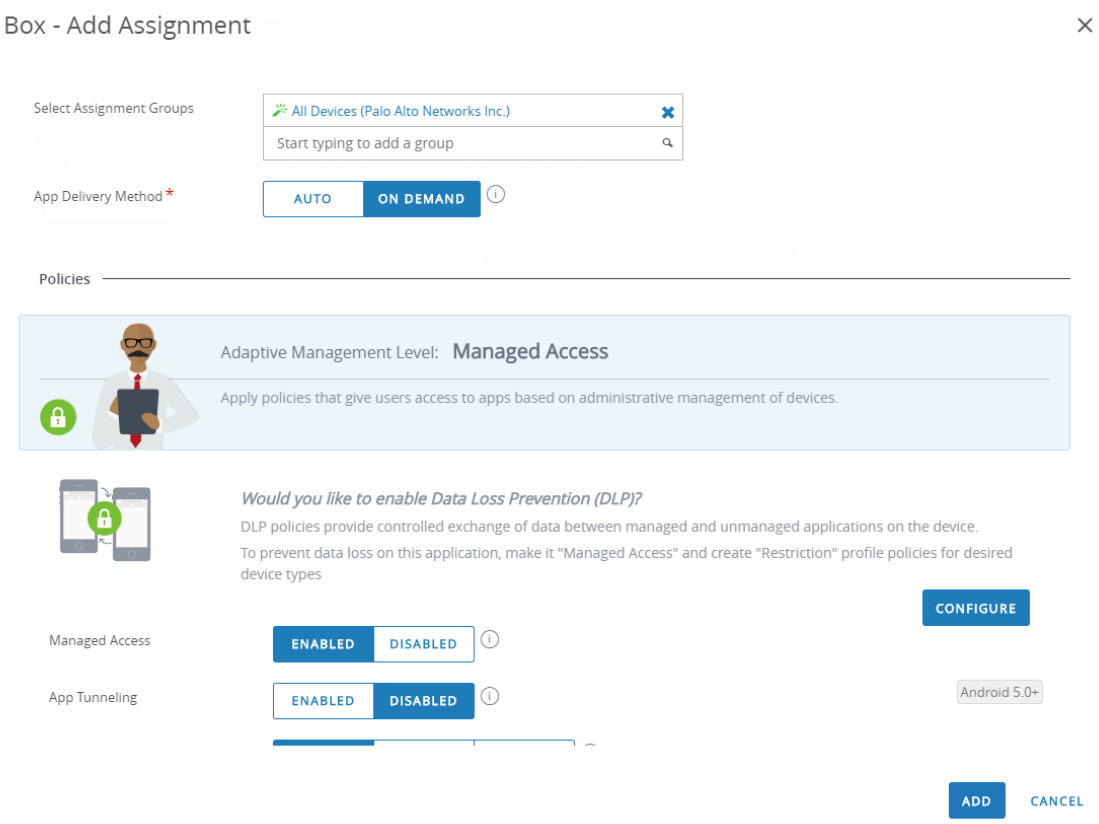


7. Select the newly added app from the list of Public apps (List View).
8. From the **Applications** > **Details View**, click **ASSIGN** at the top-right corner of the screen.

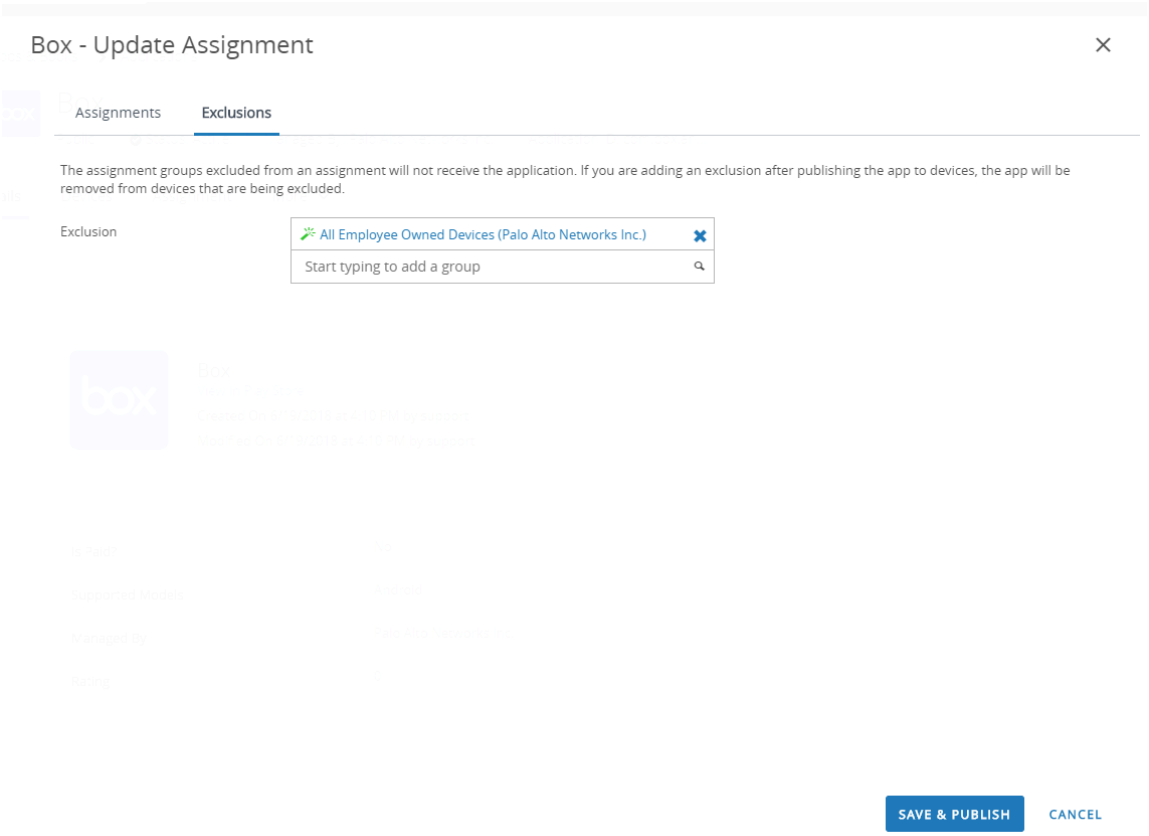


9. Select **Assignments** and then click **ADD ASSIGNMENT** to add the Smart Groups that will have access to this app.
   1. In the **Select Assignment Groups** field, select the Smart Groups that you want to grant access to this app.
   2. Select the **App Delivery Method**. If you select **AUTO**, the app is automatically deployed to the specified Smart Groups. If you select **ON DEMAND**, the app must be deployed manually.

3. Set the **Managed Access** option to **ENABLED**. This option gives users access to the app based on the management policies that you apply.
4. Configure the remaining settings as needed.
5. **ADD** the new assignment.



10. (Optional) To exclude certain Smart Groups from accessing the app, select **Exclusions** and then select the Smart Groups that you want to exclude from the **Exclusion** field.



11. **SAVE & PUBLISH** the configuration to the assigned Smart Groups.

Enable App Scan Integration with WildFire

By enabling App Scan in Workspace ONE, you can leverage WildFire® threat intelligence about apps to detect malware on Android endpoints. When enabled, the Workspace ONE agent sends the list of apps that are installed on the Android endpoint to Workspace ONE. This occurs during enrollment and subsequently on any endpoint check-in. Workspace ONE then periodically queries WildFire for verdicts and can take compliance action on the endpoint based on the verdict.

STEP 1 | Before you begin, obtain a WildFire API key. If you do not already have an API key, contact Support.

STEP 2 | From Workspace ONE, select **Groups & Settings** > **All Settings** > **Apps** > **App Scan** > **Third Party Integration**.

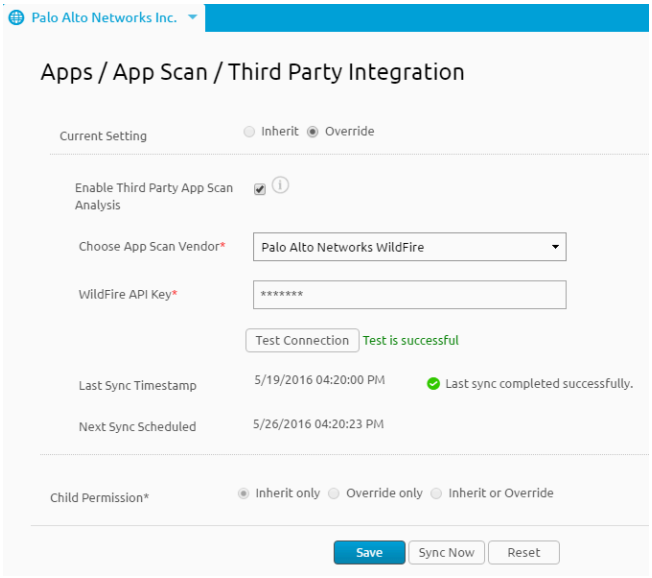
STEP 3 | Select **Current Setting: Override**.

STEP 4 | Select **Enable Third Party App Scan Analysis** to enable communication between Workspace ONE and WildFire.

STEP 5 | Select **Palo Alto Networks WildFire** from the **Choose App Scan Vendor** drop-down.

STEP 6 | Enter your WildFire API key.

STEP 7 | Click **Test Connection** to ensure that Workspace ONE can communicate with WildFire. If the test is not successful, verify connectivity to the internet, re-enter the API key, and then try again.



STEP 8 | **Save** your changes. Workspace ONE schedules a synchronization task to communicate with WildFire to obtain the latest verdicts for application hashes and runs the task at regular intervals. Click **Sync Now** to initiate a manual sync with WildFire.

Manage the GlobalProtect App Using Microsoft Intune

Microsoft Intune is a cloud-based Enterprise Mobility Management Platform that enables you to manage mobile endpoints from a central location. The GlobalProtect app provides a secure connection between the firewall and the mobile endpoints that are managed by Microsoft Intune at either the device or application level. Using GlobalProtect as the secure connection allows consistent inspection of traffic and enforcement of network security policy for threat prevention on mobile endpoints.

Refer to the following sections for information on how to deploy, configure, and manage the GlobalProtect app using Microsoft Intune:

- Deploy the GlobalProtect Mobile App Using Microsoft Intune
- Configure Microsoft Intune for iOS Endpoints
- Configure Microsoft Intune for Windows 10 UWP Endpoints

If you are not using a Qualified MDM Vendors, you can Manage the GlobalProtect App Using Other Third-Party MDMs.

Deploy the GlobalProtect Mobile App Using Microsoft Intune

You can deploy the GlobalProtect app to managed endpoints that are enrolled with Microsoft Intune or to users whose endpoints are not enrolled with Microsoft Intune (iOS only). After you deploy the app, configure and deploy a VPN profile to managed endpoints to set up the GlobalProtect app for end users automatically.

STEP 1 | Enroll endpoints with Microsoft Intune.

To deploy the GlobalProtect app to your endpoints, ensure that the endpoints are enrolled with Microsoft Intune.

STEP 2 | Add the GlobalProtect app to Microsoft Intune.

Before you can assign the GlobalProtect app to any users or endpoints, you must add the app to Microsoft Intune.

STEP 3 | Set the app assignment type for the GlobalProtect app.

You can determine who has access to the GlobalProtect app by assigning the app to users or endpoints. Before you can assign the app, you must set the assignment type for the app. The assignment type makes the app available, required, or uninstalls the app.

STEP 4 | Assign the GlobalProtect app to specific users or endpoints.

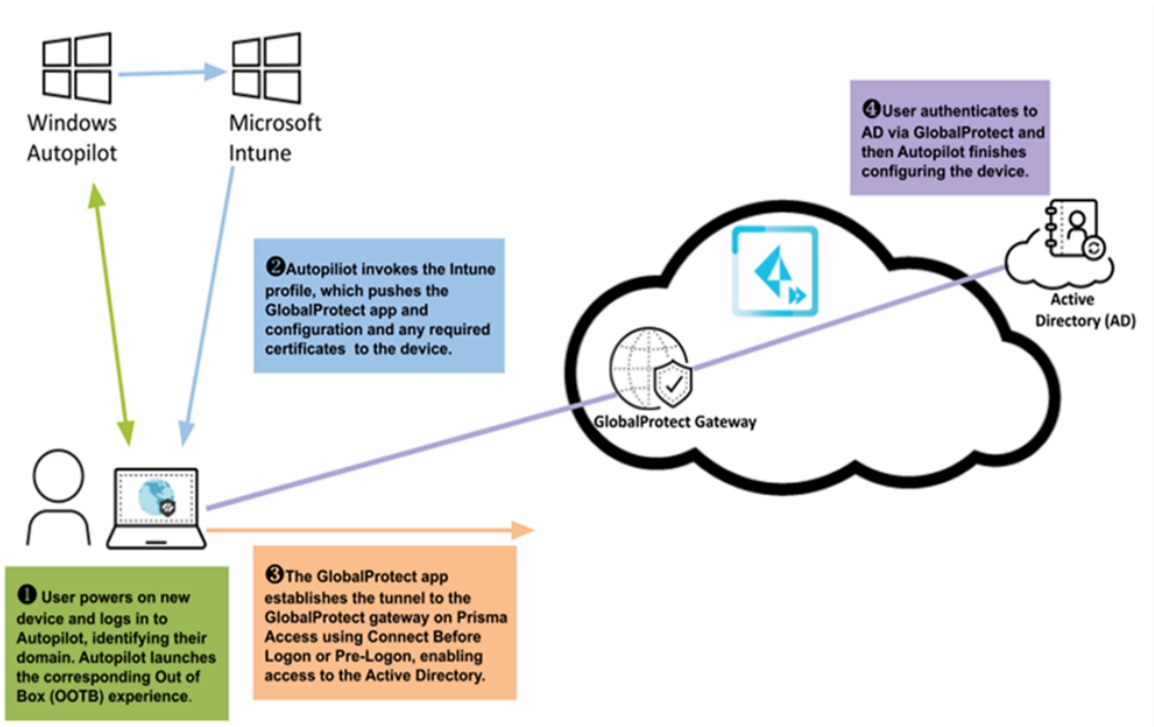
After you set the assignment type for the GlobalProtect app, you can assign the app to specific users or endpoints.

(iOS only) You can assign the GlobalProtect app to users whose endpoints are not enrolled with Microsoft Intune.

Deploy a New Device Using Windows Autopilot and Microsoft Intune

Where Can I Use This?	What Do I Need?
• Prisma Access • GlobalProtect Subscription	• Prisma Access Mobile Users license (for use with Prisma Access) • Supported with GlobalProtect app for Windows (version 5.2 or later is required for the Use Autopilot to Deploy GlobalProtect in Connect Before Logon Mode) • Endpoints must be running Windows 10 (64-bit)

You can ship a new Windows device to an end user and automatically deploy the GlobalProtect app and any required PKI or authentication settings automatically by leveraging Microsoft Intune and Windows Autopilot. This is useful in environments where you want to ship the device directly from a supplier or warehouse without having to do any configuration, such as PKI and certificate deployment, GlobalProtect app deployment prior to delivery to the end user.



Use Autopilot to Deploy GlobalProtect in Connect Before Logon Mode

In Connect Before Logon mode, the GlobalProtect app acts as a Pre-Login Access Provider (PLAP) credential provider to provide access to your corporate network before the user logs in to the Windows device, allowing users on an endpoint that is not yet set up with a local profile,

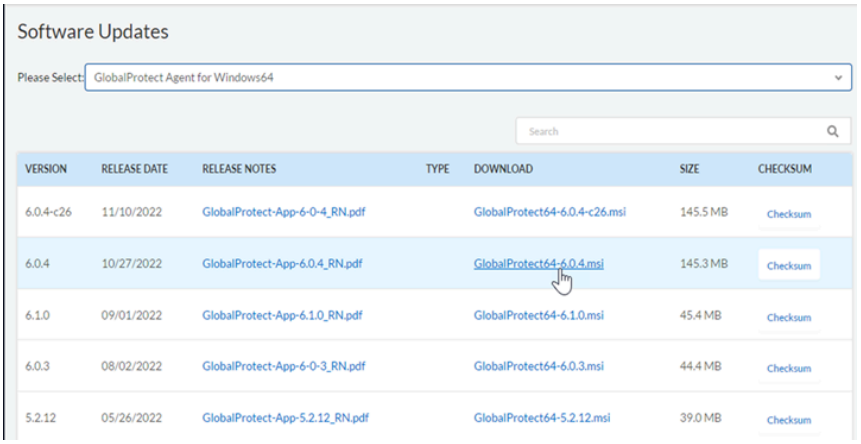
certificates, or user accounts to gain the access needed to reach the domain controller and join the domain. This deployment does not require a PKI environment and instead uses a user-based logon sequence (LDAP, RADIUS, SAML, username/password-based authentication, smart cards, or OTP authentication are supported). In this deployment, the end user device is provisioned as follows:

1. The end user logs in to Autopilot, identifying their domain.
2. Autopilot then connects to Intune, which has been configured to deploy the GlobalProtect app with the default portal address, the Connect Before Logon settings, and the domain join configuration.
3. The end user clicks the Pre-Login Access Provider (PLAP) button to log in to GlobalProtect and establish the tunnel to the GlobalProtect gateway (on premises or Prisma Access), enabling access to the domain controller.
4. GlobalProtect prompts the user to log in to the credential provider, after which Windows Autopilot can finish configuring the device.

To use this deployment, you will need to create a package for Microsoft Intune to deploy to Windows Autopilot. This package will contain the GlobalProtect MSI file along with a couple of wrapper scripts you will create to install the MSI and set the configuration parameters needed to deploy the app in Connect Before Logon mode, and a second script to launch the installer in 64-bit mode (Intune launches in 32-bit mode by default). You will then upload the package to Intune to create the application and add it to the group targeted for Autopilot.

STEP 1 | Download the GlobalProtect app MSI file from the Palo Alto Networks Customer Support Portal.

For this deployment to work you must use GlobalProtect App version 5.2.x or later (which is when Connect Before Logon was introduced).



STEP 2 | Create a PowerShell wrapper script to instruct Microsoft Intune how to install GlobalProtect.

The script must include the instructions to:

- Set the portal address so the user doesn't have to enter it (**PORTAL="portal_name"**)
- Set the app to use the default browser after the initial logon (**DEFAULTBROWSER="yes"**)
- Set the connect method to Connect Before Logon (**CONNECTMETHOD="user-logon"**)
- Register GlobalProtect with the Windows credential provider to allow for Connect Before Logon at the login screen

You can also use Customizable App Settings. Here is an example of a wrapper script that you can copy and edit with your own values for the portal address and MSI file name:

```
$PortalAddress = 'myportal.gpcloudservice.com'
$MSIFileName = 'GlobalProtect64-6.0.4.msi'
$MSISwitches = '/quiet /norestart'

$ScriptPath = Split-Path -Path $MyInvocation.MyCommand.Path

$InstallProcess = Start-Process -FilePath "msiexec" -ArgumentList
 ("/i " + [char]34 + $ScriptPath + "\" + $MSIFileName + [char]34
PORTAL="myportal.gpcloudservice.com"" DEFAULTBROWSER=""yes""
 CONNECTMETHOD=""user-logon""

#Register PLAP provider
Start-Process -FilePath "$env:ProgramFiles\Palo Alto Networks
\GlobalProtect\PanGPS.exe" -ArgumentList "-registerplap" -Wait
Write-Host ("Installation completed, exiting with last return code
 (" + $InstallProcess.ExitCode + ")")
Exit $InstallProcess.ExitCode
```

STEP 3 | (Hybrid Azure AD only) Install the Intune Connector for Active Directory and the AzureAD Connector.

STEP 4 | Register the end user devices with Autopilot and create the group for the Out of Box Experience (OOBE) you are creating to deploy the GlobalProtect app.

Refer to the Microsoft Windows Autopilot documentation for instructions.

STEP 5 | Create the GlobalProtect app installation package (the MSI file and the scripts) and upload it to Microsoft Intune.

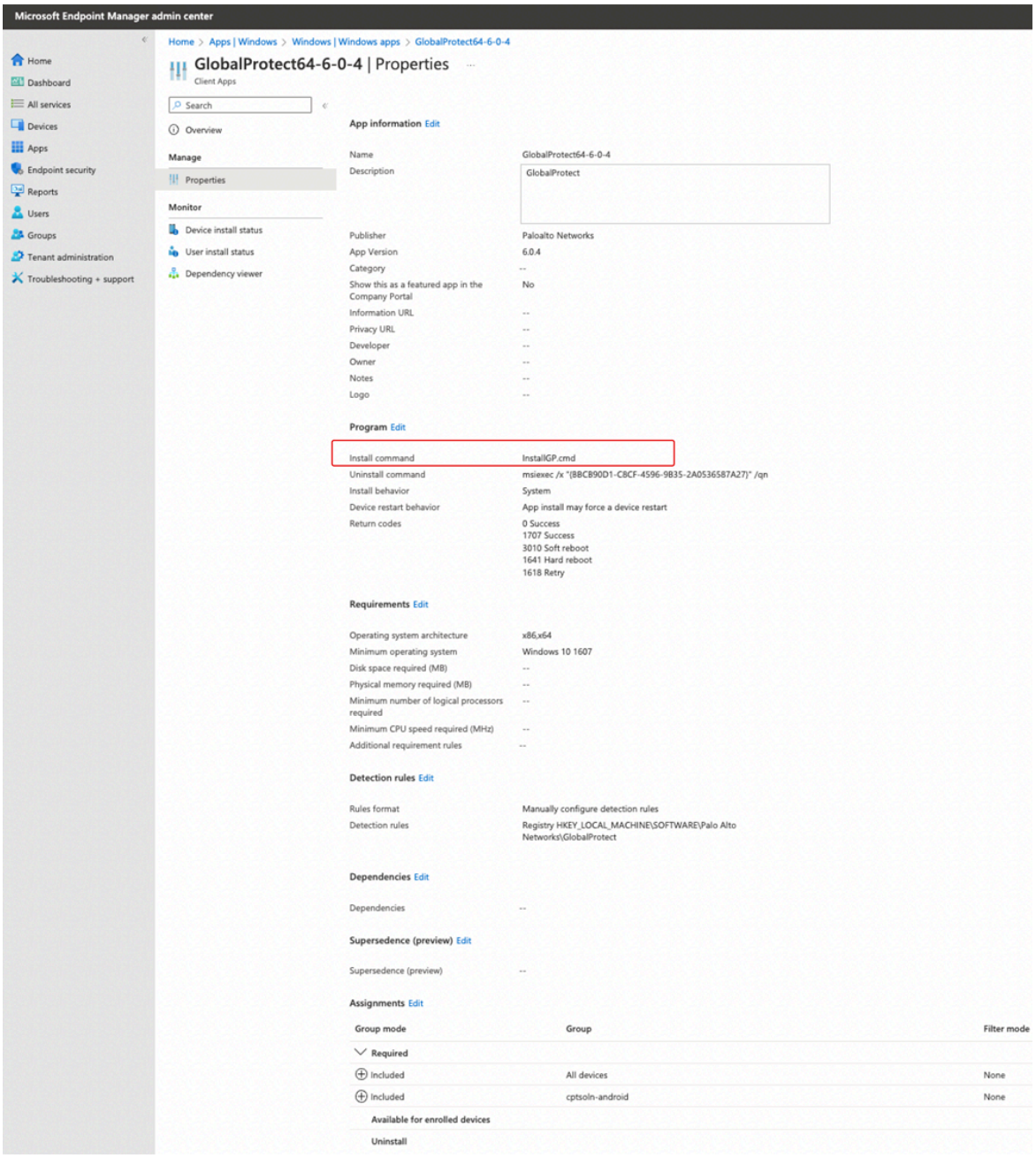
1. Use the Microsoft Win32 Content Prep Tool to create the app package.

   By default, the installer launches in 32-bit mode. Use the script to convert it to 64-bit mode as in the following example:

   ```
   IntuneWinAppUtil.exe -c C:\Temp\GlobalProtectPackage\Install -s
   GlobalProtect64-6.0.4.msi -o C:\Temp\GlobalProtectPackage\Output
   ```

2. Upload the app package to Microsoft Intune.

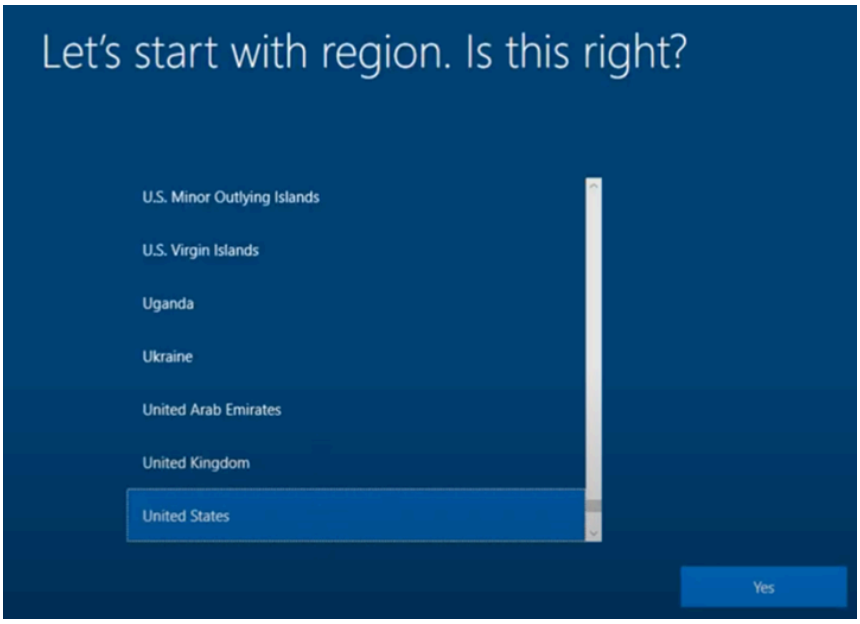
   Make sure the **Install command** points to the batch file you created to launch the MSI in 64-bit mode.



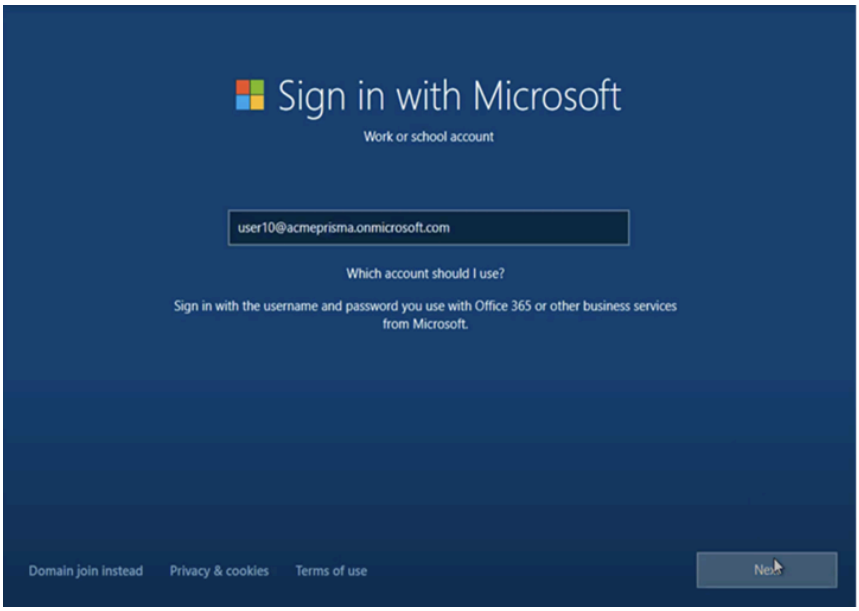
3. Assign the app to the group you created for Autopilot.

STEP 6 | Test the deployment process.

1. Power on the device, which will automatically connect to Autopilot and launch the OOBE experience you customized.

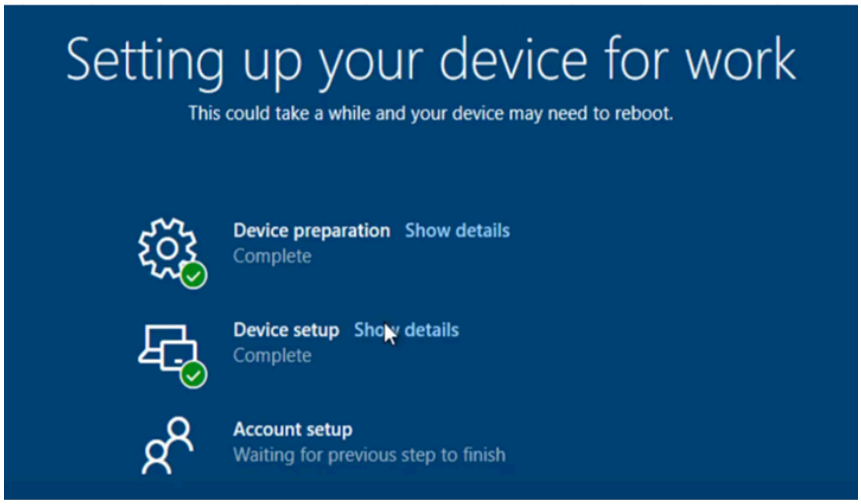


2. When prompted, provide your username to identify the organization you belong to so that you can complete Autopilot registration.

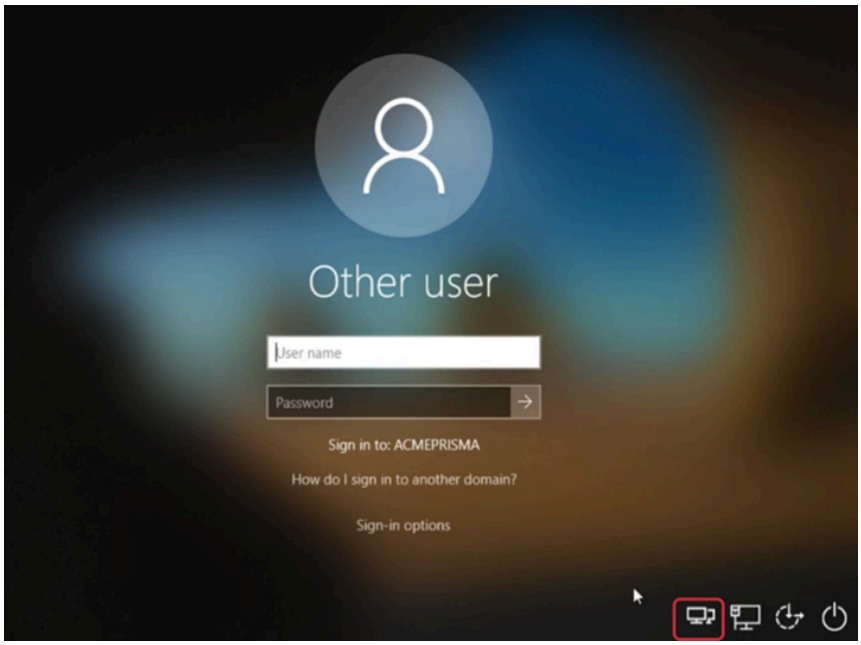


This initiates the Autopilot registration. Autopilot then reboots the system and invokes the Intune profile you created and assigned to the device, which begins the process of pushing the GlobalProtect app and the settings you defined to specify the portal, set the Connect Before Logon mode, and the command flags to register GlobalProtect with

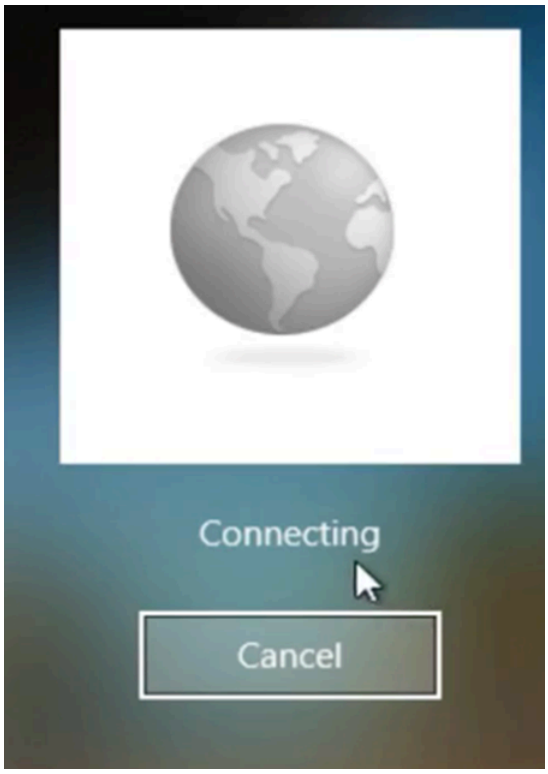
the credential provider to the device, along with any other apps and configurations you defined in the Intune profile.



3. After the configurations and apps are pushed to the endpoint, click the Pre-Login Access Provider (PLAP) button to log in to GlobalProtect and establish the tunnel.

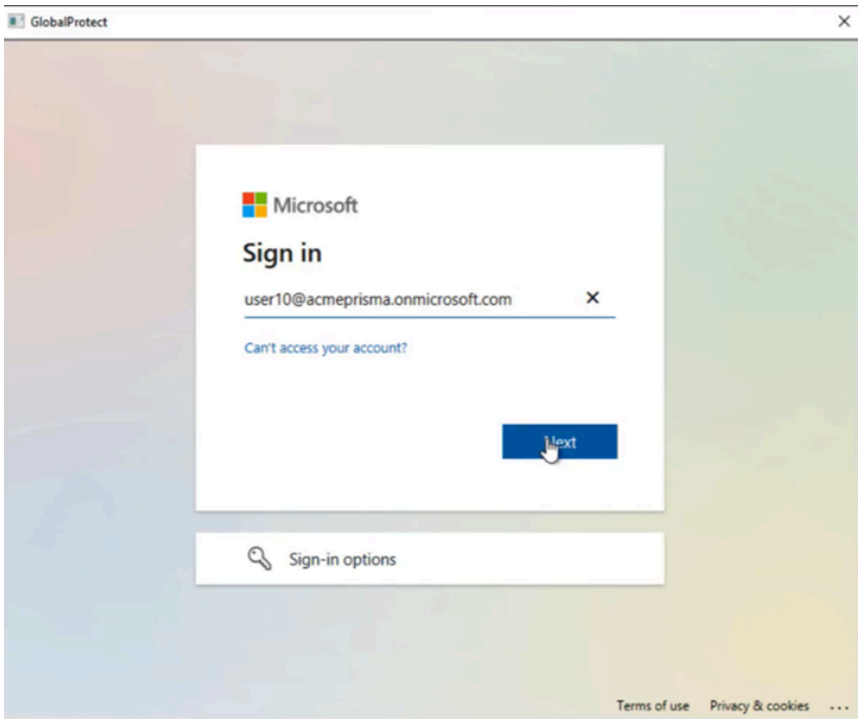


GlobalProtect begins connecting using the portal name you supplied in your wrapper script.

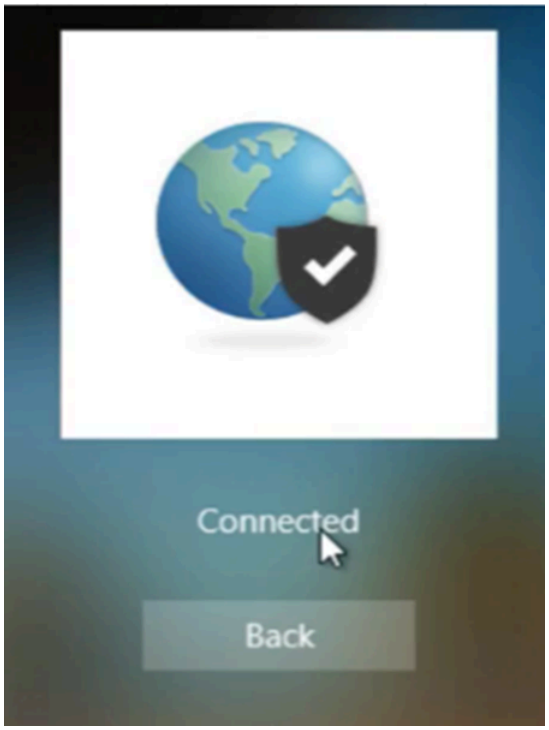


4. After successfully establishing the tunnel, GlobalProtect prompts you to log in to the credential provider. Enter your domain credentials.

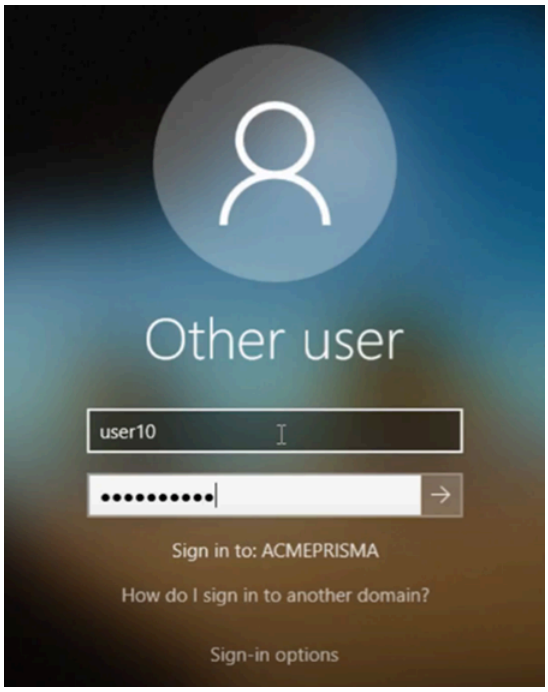
   If you are using SAML, GlobalProtect presents the embedded browser even if you have pushed settings to use the default browser. This is because the user is not yet logged in.



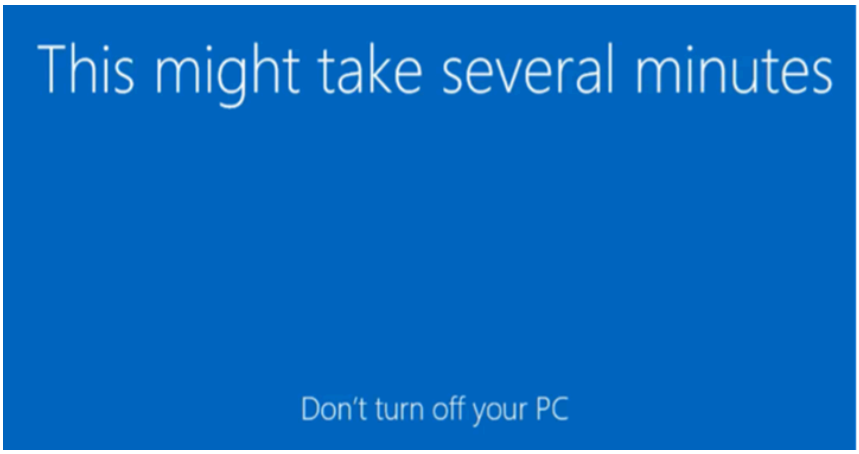
5. After successful authentication, the GlobalProtect Connected screen displays. The device now has the connectivity required to reach the domain controller and join the domain. Click **Back**.



6. Enter your Windows domain login credentials to log in to the device and join the domain.



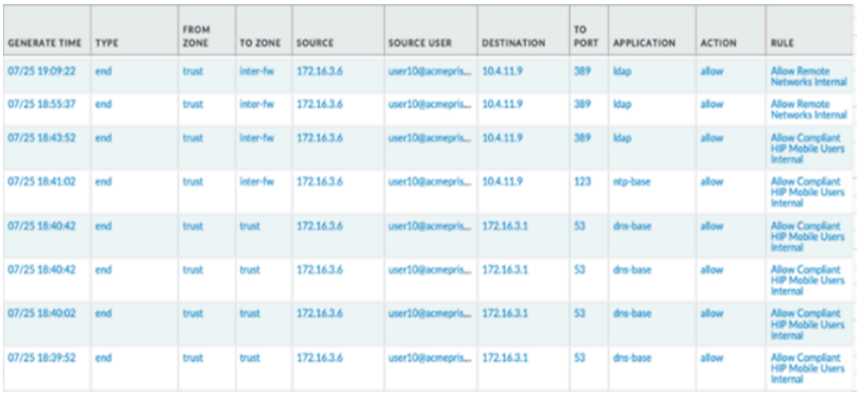
7. After you successfully authenticate using the domain credentials, Autopilot finishes configuring the user profile.



8. Verify that GlobalProtect has been successfully installed and that policy is being enforced as expected.

   Review the traffic logs to ensure that the device is hitting the security policy you have configured for your GlobalProtect users. For example, in the logs below we can see that

user10@acmeprismaaccess.com is hitting the rule that allows mobile users that pass the HIP check can access the internal network.



GENERATE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	TO PORT	APPLICATION	ACTION	RULE
07/25 19:09:22	end	trust	inter-fw	172.16.3.6	user10@acmepris...	10.4.11.9	389	ldap	allow	Allow Remote Networks Internal
07/25 18:55:37	end	trust	inter-fw	172.16.3.6	user10@acmepris...	10.4.11.9	389	ldap	allow	Allow Remote Networks Internal
07/25 18:43:52	end	trust	inter-fw	172.16.3.6	user10@acmepris...	10.4.11.9	389	ldap	allow	Allow Compliant HIP Mobile Users Internal
07/25 18:41:02	end	trust	inter-fw	172.16.3.6	user10@acmepris...	10.4.11.9	123	ntp-base	allow	Allow Compliant HIP Mobile Users Internal
07/25 18:40:42	end	trust	trust	172.16.3.6	user10@acmepris...	172.16.3.1	53	dns-base	allow	Allow Compliant HIP Mobile Users Internal
07/25 18:40:42	end	trust	trust	172.16.3.6	user10@acmepris...	172.16.3.1	53	dns-base	allow	Allow Compliant HIP Mobile Users Internal
07/25 18:40:02	end	trust	trust	172.16.3.6	user10@acmepris...	172.16.3.1	53	dns-base	allow	Allow Compliant HIP Mobile Users Internal
07/25 18:39:52	end	trust	trust	172.16.3.6	user10@acmepris...	172.16.3.1	53	dns-base	allow	Allow Compliant HIP Mobile Users Internal

Configure Microsoft Intune for iOS Endpoints

Refer to the following sections for information on how to set up VPN configurations for iOS endpoints using Microsoft Intune:

- Configure an Always On VPN Configuration for iOS Endpoints Using Microsoft Intune
- Configure a User-Initiated Remote Access VPN Configuration for iOS Endpoints Using Microsoft Intune
- Configure a Per-App VPN Configuration for iOS Endpoints Using Microsoft Intune

Configure an Always On VPN Configuration for iOS Endpoints Using Microsoft Intune

In an Always On VPN configuration, the secure GlobalProtect connection is always on. Traffic that matches specific filters (such as port and IP address) configured on the GlobalProtect gateway is always routed through the VPN tunnel.

Use the following steps to configure an Always On VPN configuration for iOS endpoints using Microsoft Intune:

STEP 1 | Download the GlobalProtect app for iOS.

- Deploy the GlobalProtect Mobile App Using Microsoft Intune.
- Download the GlobalProtect app directly from the App Store.

STEP 2 | (Optional) If your deployment requires certificate-based authentication, configure a certificate profile.

STEP 3 | Create a new iOS VPN profile.

- Set the **Platform** to **iOS**.

STEP 4 | Configure always on VPN settings for iOS endpoints.

- Set the **Connection type** to **Palo Alto Networks GlobalProtect**.

Configure a User-Initiated Remote Access VPN Configuration for iOS Endpoints Using Microsoft Intune

In a remote access (On-Demand) VPN configuration, users must manually launch the app to establish the secure GlobalProtect connection. Traffic that matches specific filters (such as port and IP address) configured on the GlobalProtect gateway is routed through the VPN tunnel only after users initiate and establish the connection.

Use the following steps to configure a user-initiated remote access VPN configuration for iOS endpoints using Microsoft Intune:

STEP 1 | Download the GlobalProtect app for iOS.

- Deploy the GlobalProtect Mobile App Using Microsoft Intune.
- Download the GlobalProtect app directly from the App Store.

STEP 2 | (Optional) If your deployment requires certificate-based authentication, configure a certificate profile.

STEP 3 | Create a new iOS VPN profile.

- Set the **Platform** to **iOS**.

STEP 4 | Configure on-demand (remote access) VPN settings for iOS endpoints.

- Set the **Connection type** to **Palo Alto Networks GlobalProtect**.
- In the Automatic VPN settings area, enable **On-demand VPN** to configure conditional rules that control when the VPN connection is initiated.

Configure a Per-App VPN Configuration for iOS Endpoints Using Microsoft Intune

You can enable access to internal resources from your managed mobile endpoints by configuring GlobalProtect VPN access using Microsoft Intune. In a per-app VPN configuration, you can specify which managed apps can route traffic through the VPN tunnel. Unmanaged apps will continue to connect directly to the internet instead of through the VPN tunnel.

Use the following steps to configure a per-app VPN configuration for iOS endpoints using Microsoft Intune:

STEP 1 | Download the GlobalProtect app for iOS.

- Deploy the GlobalProtect Mobile App Using Microsoft Intune.
- Download the GlobalProtect app directly from the App Store.

STEP 2 | Add apps to Microsoft Intune.

Before you can assign, monitor, configure, or protect apps, you must add them to Microsoft Intune.

- Set the **App type** to **iOS**.
- Add iOS store apps to Microsoft Intune.

STEP 3 | Set up a per-app VPN configuration for iOS.

- When you create a per-app VPN profile, set the **Platform** to **iOS** and the **Connection type** to **Palo Alto Networks GlobalProtect**.
- When you associate an app with the VPN profile, select your per-app VPN profile from the **VPNS** drop-down.

Configure Microsoft Intune for Windows 10 UWP Endpoints

Refer to the following sections for information on how to set up VPN configurations for Windows 10 UWP endpoints using Microsoft Intune:

- Configure an Always On VPN Configuration for Windows 10 UWP Endpoints Using Microsoft Intune
- Configure a Per-App VPN Configuration for Windows 10 UWP Endpoints Using Microsoft Intune

Configure an Always On VPN Configuration for Windows 10 UWP Endpoints Using Microsoft Intune

In an Always On VPN configuration, the secure GlobalProtect connection is always on. Traffic that matches specific filters (such as port and IP address) configured on the GlobalProtect gateway is always routed through the VPN tunnel.

Use the following steps to configure an Always On VPN configuration for Windows 10 UWP endpoints using Microsoft Intune:

STEP 1 | Download the GlobalProtect app for Windows 10 UWP:

- Deploy the GlobalProtect Mobile App Using Microsoft Intune.
- Download the GlobalProtect app directly from the Microsoft Store.

STEP 2 | (Optional) If your deployment requires certificate-based authentication, configure a certificate profile.

STEP 3 | Create a new Windows 10 UWP VPN profile.

- Set the **Platform** to **Windows 10 and later**.

STEP 4 | Configure always on VPN settings for Windows 10 UWP endpoints.

- Set the **Connection type** to **Palo Alto Networks GlobalProtect**.
- Enable **Always On** VPN.

Configure a Per-App VPN Configuration for Windows 10 UWP Endpoints Using Microsoft Intune

You can enable access to internal resources from your managed mobile endpoints by configuring GlobalProtect VPN access using Microsoft Intune. In a per-app VPN configuration, you can specify which managed apps can route traffic through the VPN tunnel. Unmanaged apps will continue to connect directly to the internet instead of through the VPN tunnel.

Use the following steps to configure a per-app VPN configuration for Windows 10 UWP endpoints using Microsoft Intune:

STEP 1 | Download the GlobalProtect app for Windows 10 UWP:

- Deploy the GlobalProtect Mobile App Using Microsoft Intune.
- Download the GlobalProtect app directly from the Microsoft Store.

STEP 2 | Configure a certificate profile.

All per-app VPN configurations require certificate-based authentication.

STEP 3 | Create a new Windows 10 UWP VPN profile.

- Set the **Platform** to **Windows 10 and later**.

STEP 4 | Configure per-app VPN settings for Windows 10 UWP endpoints.

- Set the **Connection type** to **Palo Alto Networks GlobalProtect**.
- In the Apps and Traffic rules area, set the **Associate WIP or apps with this VPN** option to **Associate apps with this connection**. **Enable** the option to **Restrict VPN connection to these apps**, and then **Add** the associated apps that you want to use the VPN connection.

Manage the GlobalProtect App Using MobileIron

MobileIron is an Enterprise Mobility Management Platform that enables you to manage mobile endpoints from a central console. The GlobalProtect app provides a secure connection between the firewall and the mobile endpoints that are managed by MobileIron at either the device or application level. Using GlobalProtect as the secure connection allows consistent inspection of traffic and enforcement of network security policy for threat prevention on mobile endpoints.

Refer to the following sections for information on how to deploy, configure, and manage the GlobalProtect app using MobileIron:

- Deploy the GlobalProtect Mobile App Using MobileIron
- Configure MobileIron for iOS Endpoints
- Configure MobileIron for Android Endpoints

If you are not using a Qualified MDM Vendors, you can Manage the GlobalProtect App Using Other Third-Party MDMs.

Deploy the GlobalProtect Mobile App Using MobileIron

You can deploy the GlobalProtect app to managed endpoints that have enrolled with MobileIron. After you deploy the app, configure and deploy a VPN profile to set up the GlobalProtect app for the end user automatically.

STEP 1 | Add users to MobileIron.

Before users can register their endpoints to MobileIron, you must create a user entry for each user.

STEP 2 | (Optional) Assign users to user groups.

To deploy the GlobalProtect app based on group membership instead of individual users, you can assign users to different user groups.

STEP 3 | Invite users to register their endpoints with MobileIron.

After you add users to MobileIron, you can invite them to register their endpoints.

STEP 4 | Add the GlobalProtect app to the MobileIron app catalog.

The app catalog lists the mobile apps that are available to your users. You can either search for and add the GlobalProtect app from a public store (such as the Apple App Store) or upload the app directly to MobileIron as an in-house app. You must then configure the app distribution settings to indicate how the GlobalProtect app will be installed and configured on registered endpoints.

Configure MobileIron for iOS Endpoints

Refer to the following sections for information on how to configure VPN configurations for iOS endpoints using MobileIron:

- Configure an Always On VPN Configuration for iOS Endpoints Using MobileIron

- Configure a User-Initiated Remote Access VPN Configuration for iOS Endpoints Using MobileIron
- Configure a Per-App VPN Configuration for iOS Endpoints Using MobileIron

Configure an Always On VPN Configuration for iOS Endpoints Using MobileIron

In an Always On VPN configuration, the secure GlobalProtect connection is always on. Traffic that matches specific filters (such as port and IP address) configured on the GlobalProtect gateway is always routed through the VPN tunnel.

Use the following steps to configure an Always On VPN configuration for iOS endpoints using MobileIron:

STEP 1 | Download the GlobalProtect app for iOS.

- Deploy the GlobalProtect Mobile App Using MobileIron.
- Download the GlobalProtect app directly from the App Store.

STEP 2 | (Optional) If your deployment requires certificate-based authentication, add a certificate configuration and then configure the certificate settings.

STEP 3 | Add an always on VPN configuration.

- Set the configuration type to **Always On VPN**.

STEP 4 | Configure always on VPN settings for iOS.

Configure a User-Initiated Remote Access VPN Configuration for iOS Endpoints Using MobileIron

In a remote access (On-Demand) VPN configuration, users must manually launch the app to establish the secure GlobalProtect connection. Traffic that matches specific filters (such as port and IP address) configured on the GlobalProtect gateway is routed through the VPN tunnel only after users initiate and establish the connection.

Use the following steps to configure a user-initiated remote access VPN configuration for iOS endpoints using MobileIron:

STEP 1 | Download the GlobalProtect app for iOS.

- Deploy the GlobalProtect Mobile App Using MobileIron.
- Download the GlobalProtect app directly from the App Store.

STEP 2 | Add a certificate configuration and then configure the certificate settings.

All on-demand VPN configurations require certificate-based authentication.

STEP 3 | Add an on-demand (remote access) VPN configuration.

- Set the configuration type to **VPN On Demand**.

STEP 4 | Configure VPN on-demand settings for iOS.

- Set the **Connection Type** to **Palo Alto Networks GlobalProtect**, and then configure the associated settings.

Configure a Per-App VPN Configuration for iOS Endpoints Using MobileIron

You can enable access to internal resources from your managed mobile endpoints by configuring GlobalProtect VPN access using MobileIron. In a per-app VPN configuration, you can specify which managed apps can route traffic through the VPN tunnel. Unmanaged apps will continue to connect directly to the internet instead of through the VPN tunnel.

Use the following steps to configure a per-app VPN configuration for iOS endpoints using MobileIron:

STEP 1 | Download the GlobalProtect app for iOS.

- Deploy the GlobalProtect Mobile App Using MobileIron.
- Download the GlobalProtect app directly from the App Store.

STEP 2 | Add a certificate configuration and then configure the certificate settings.

All per-app VPN configurations require certificate-based authentication.

STEP 3 | Add a per-app VPN configuration.

- Set the configuration type to **Per-app VPN**.

STEP 4 | Configure per-app VPN settings for iOS.

- Set the **Connection Type** to **Palo Alto Networks GlobalProtect**, and then configure the associated settings.

Configure MobileIron for Android Endpoints

Refer to the following sections for information on how to configure a VPN configuration for Android endpoints using MobileIron:

- Configure an Always On VPN Configuration for Android Endpoints Using MobileIron

Configure an Always On VPN Configuration for Android Endpoints Using MobileIron

In an Always On VPN configuration, the secure GlobalProtect connection is always on. Traffic that matches specific filters (such as port and IP address) configured on the GlobalProtect gateway is always routed through the VPN tunnel.

Use the following steps to configure an Always On VPN configuration for Android endpoints using MobileIron:

STEP 1 | Download the GlobalProtect app for Android.

- Deploy the GlobalProtect Mobile App Using MobileIron.
- Download the GlobalProtect app directly from Google Play.

STEP 2 | (Optional) If your deployment requires certificate-based authentication, add a certificate configuration and then configure the certificate settings.

STEP 3 | Add an always on VPN configuration.

- Set the configuration type to **Always On VPN**.

STEP 4 | Configure always on VPN settings for Android.

Manage the GlobalProtect App Using Google Admin Console

The Google Admin console is a cloud-based Enterprise Mobility Management Platform that enables you to manage Chromebooks from a central console. The GlobalProtect app provides a secure connection between the firewall and the Chromebooks that are managed by the Google Admin console at either the device or application level. Using GlobalProtect as the secure connection allows consistent inspection of traffic and enforcement of network security policy for threat prevention on mobile endpoints.

Refer to the following sections for information on how to deploy, configure, and manage the GlobalProtect app using Google Admin console:

- Deploy the GlobalProtect App for Android on Managed Chromebooks Using the Google Admin Console
- Configure Google Admin Console for Android Endpoints

If you are not using a Qualified MDM Vendors, you can Manage the GlobalProtect App Using Other Third-Party MDMs.

Deploy the GlobalProtect App for Android on Managed Chromebooks Using the Google Admin Console

The Google Admin console enables you to manage Chromebook settings and apps from a central, web-based location. You can deploy the GlobalProtect app for Android on managed Chromebooks and configure the associated VPN settings from the console.

To set up the app for the user automatically, you can optionally use the Google Chromebook Management Console to configure and deploy settings to managed Chrome OS devices. You can use the Google Admin console to manage Chromebook settings and apps.

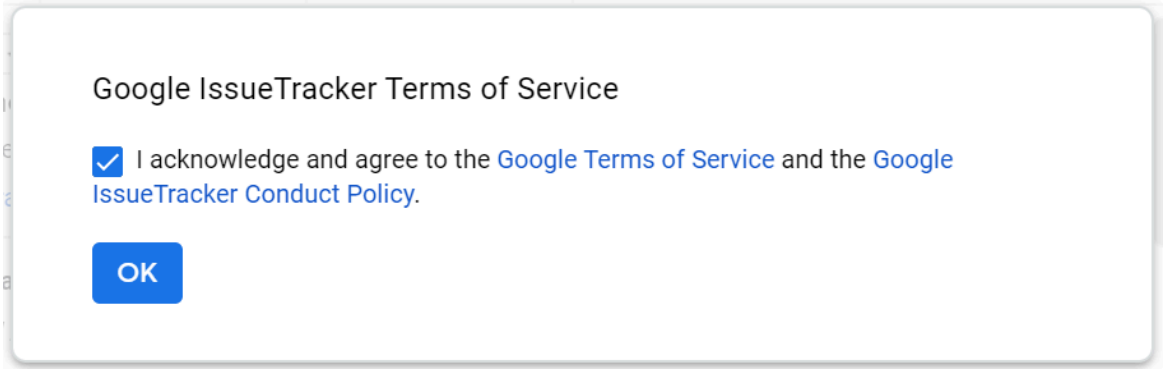
Follow these recommendations to deploy the GlobalProtect app for Android on managed Chromebooks:

- *You cannot push a unique certificate for authentication to the device using the Google Admin console.*
- *From your Chromebook, press **CTRL+ALT+T** to open the terminal command line. Use the `route` command to display the routes that are installed on the device. You can determine whether to include the access routes for split tunneling.*
- *Because applications often use different file formats, you can use OpenSSL to convert the certificates from PKCS #12 format to Base64 format. Use the `openssl base64 -A -in` <certificate-in-p12-format> `-out` <cert.txt> command.*

Use the following steps to deploy the GlobalProtect app for Android on managed Chromebooks using the Google Admin console:

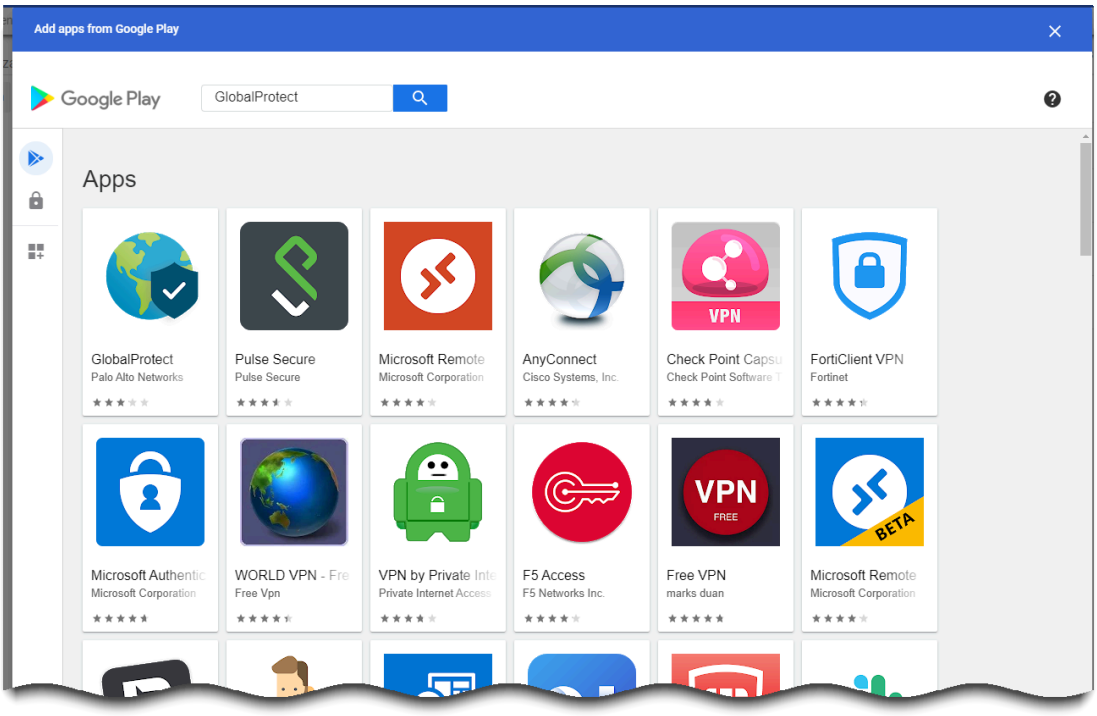
STEP 1 | Before you begin:

- Configure the GlobalProtect gateways to support the GlobalProtect app for Android on managed Chromebooks. Refer to Configure a GlobalProtect Gateway.
- Configure the portal and customize the GlobalProtect app for Android on managed Chromebooks. You must configure one or more gateways to which the GlobalProtect app can connect. Refer to Set Up Access to the GlobalProtect Portal. Refer to the Palo Alto Networks Compatibility Matrix for a list of features supported for Android on Chrome OS.
- (Recommended) Enable SAML SSO for the GlobalProtect app for Android on Chromebooks for seamless authentication. We recommend that you set up SAML SSO to allow users to connect automatically after they log in to Chromebook without having to re-enter their credentials on the GlobalProtect app. This ensures that users have access to Configure an Always On VPN Configuration for Chromebooks Using the Google Admin Console. Refer to Set Up SAML Authentication.
- When users connect to GlobalProtect for the first time on Android on managed Chromebooks, the following suppress VPN notification message must be acknowledged before the tunnel is set up:



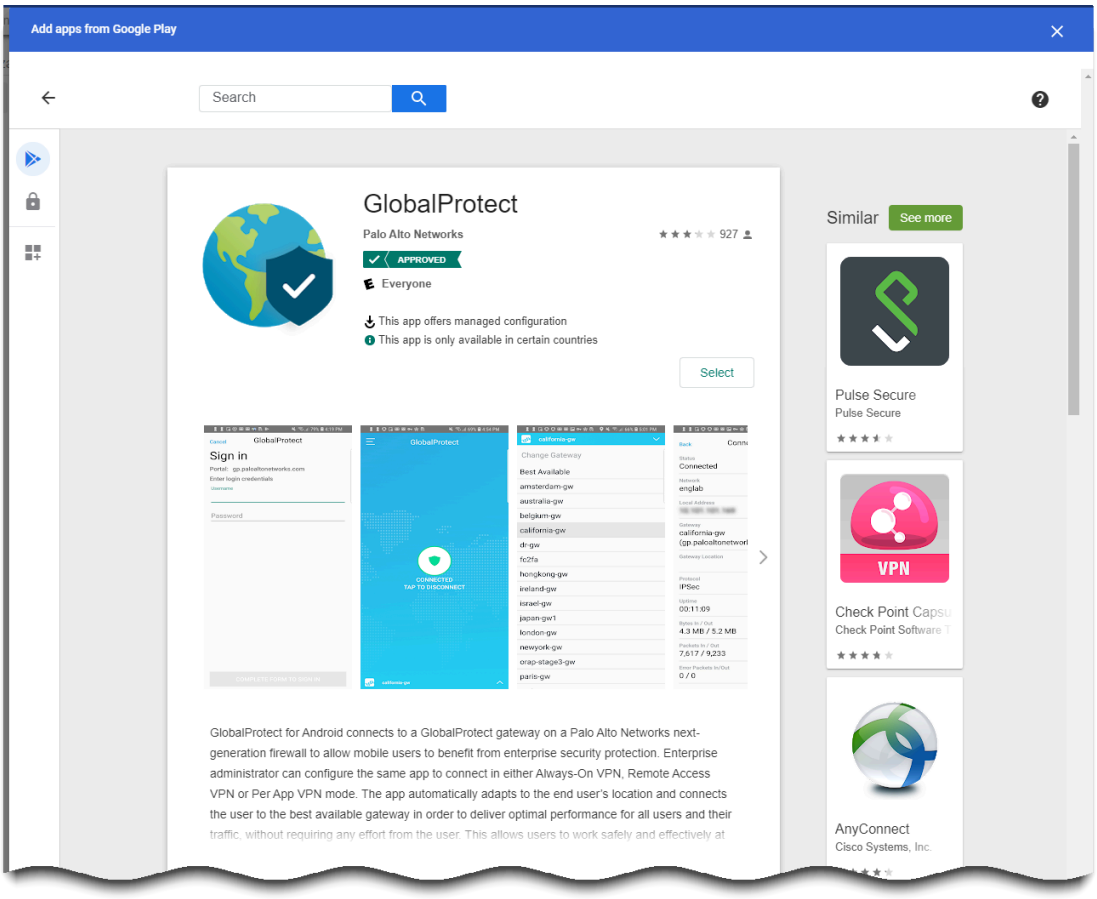
STEP 2 | Approve the GlobalProtect app for Chromebook users.

1. Log in to the Google Admin console as an administrator.
2. From the Admin console, select **Devices** > **Chrome management** to view and modify the Chrome management settings.
3. Select **Apps & extensions**.
4. In the Apps and extensions area, click the **application settings page** link.
5. Click the add ( ) button to add GlobalProtect to the list of approved Android apps from the Google Playstore.
6. When the Google Play store launches, search for **`GlobalProtect`** and then click the GlobalProtect app icon.



7. Click **Select** to add the GlobalProtect app.

   A message appears if the GlobalProtect app is successfully added as a result.



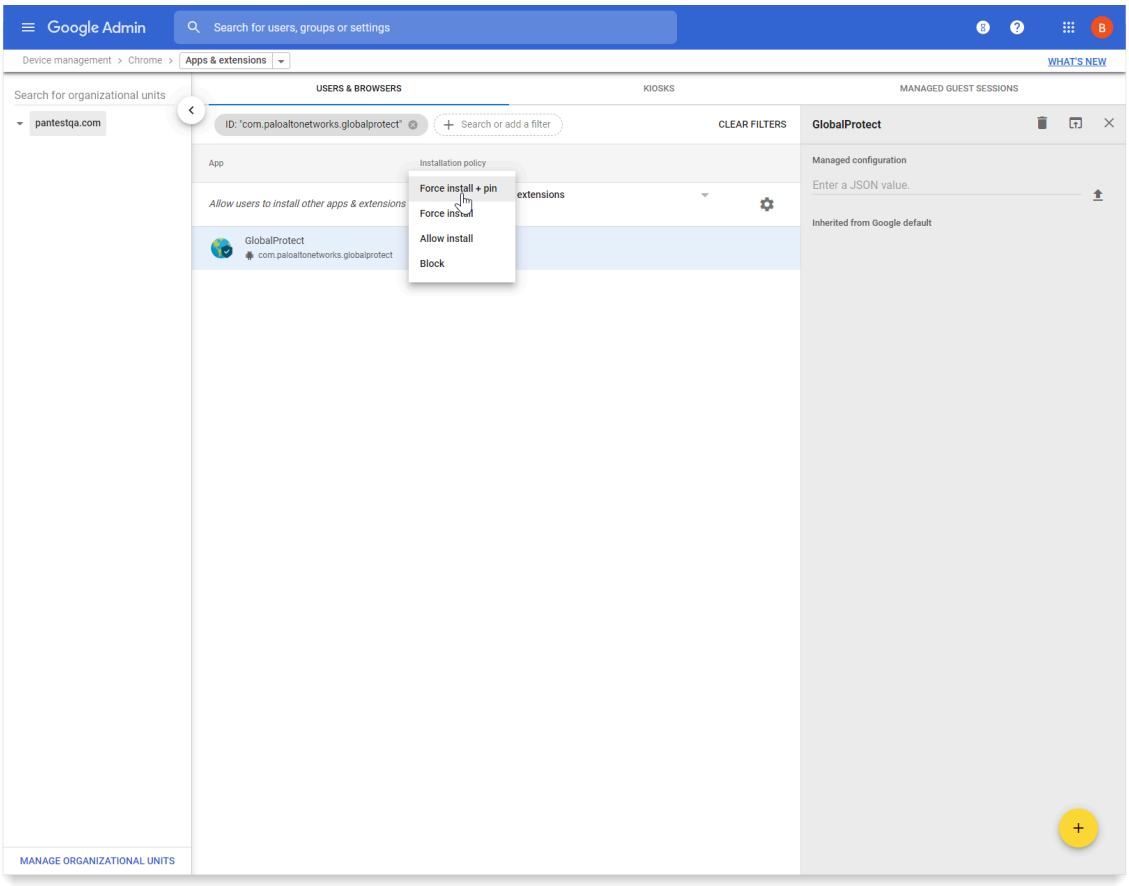
STEP 3 | Determine how the GlobalProtect app is installed on Chromebooks.

After you approve the GlobalProtect app, you must specify how the app is installed on Chromebooks. To prevent users from bypassing GlobalProtect by uninstalling the app, force all Chromebooks to install the GlobalProtect app automatically when users log in to their Chromebook.

1. From the app extension management settings (**Device management** > **Chrome** > **Apps & extensions**), select **GlobalProtect** from the Apps list.
2. Select your organizational unit from the list on the left edge of the page.
3. Select any of the following options:
   - (Recommended) **Force install + pin**—Enable and pin the force-installed GlobalProtect app to the taskbar. If you selected this option, users will not have the option to Sign Out of the app.
   - **Force install**—Use this option if you want to ensure that the GlobalProtect app is automatically installed on each Chromebook when users log in to their Chromebooks. To prevent users from uninstalling the GlobalProtect app and getting around the

security and compliance requirements you want to enforce the **Force install** option. If you selected this option, users will not have the option to Sign Out of the app.

- **Allow install**—Install this app manually from the Google Playstore. This option also allows users to uninstall the GlobalProtect app from their Chromebooks.
- **Block**—Block users from installing this app.



4. **SAVE** your changes.

STEP 4 | Apply a managed configuration to the GlobalProtect app.

If you have enabled the GlobalProtect app to force install, you can apply a managed configuration file to the app. The managed configuration file contains values for configurable app settings.

1. From the App Management settings (**Device Management** > **Chrome management** > **Apps & Extensions**), select **GlobalProtect** from the Apps list.
2. Select your organizational unit from the list on the left edge of the page.
3. Click the **Upload from file** icon on the right edge of the page to select and upload your managed configuration file. Or enter the name of the key value in JSON format, as shown in the following sample configuration.

```
{
 "portal": "acme.portal.com",
 "username": "user123"
```



```
}
```

The following table displays an example of the settings in the managed configuration file. For the settings that are relevant for your company, please contact your IT administrator.

Setting	Description	Value Type	Example
portal	IP address or fully qualified domain name (FQDN) of the portal.	String	**acme.portal.com**
username	Username for portal authentication.	String	**user123**
password	Password for portal authentication.	String	**password123**
client_certificate	Client certificate for portal authentication.	String (in Base64)	**DAFDSaweEWQ23wDSAFD…**
client_certificate _passphrase	Client certificate passphrase for portal authentication.	String	**PA$$W0RD$123**
app_list	Begin the string with either the **allowlist** keyword or **blocklist** keyword followed by a colon, and follow it with an array of app names separated by semicolons. The block list or allow list enables you to control which application traffic can go through the VPN tunnel in a per-app VPN configuration.	String	**allowlist| blocklist: com.google.calendar; com.android.email; com.android.chrome**
connect_method	VPN connection method.	String	**user-logon | on-demand**
mobile_id	Unique identifier used to identify mobile endpoints, as configured in a third-party MDM system.	String	**5188a8193be43f42d332 dde5cb2c941e**

Setting	Description	Value Type	Example
remove_vpn_config _via_restriction	Flag to remove the VPN configuration.	Boolean	**true | false**
allow_vpn_bypass	Flag to allow application traffic to bypass the VPN tunnel.	Boolean	**true | false**
cert_alias	Unique name used to identify the client certificate during portal or gateway authentication.	String	**Company User client**
managed	Flag to indicate whether the device is enrolled with an MDM server.	Boolean	**true | false**
ownership	Ownership category of the device (for example, **Employee Owned**).	String	**byod**
compliance	Compliance status that indicates whether the device is compliant with the compliance policies that you have defined.	String	**yes**
tag	Tags to enable you to identify devices. Each tag must be separated by a comma.	String	**GuestAccount,SatelliteOffi**

4. **SAVE** your changes.

STEP 5 | Enforce policies on the GlobalProtect app for Android on managed Chromebooks.

- Configure HIP-Based Policy Enforcement using **Host Info** that is specific to Android on managed Chromebooks. Then use it as match conditions in any Host Information Profile (HIP) profiles.
- Configure HIP-Based Policy Enforcement using a HIP profile as a match condition in a policy rule. By default, the app What Data Does the GlobalProtect App Collect? of information to help identify the security state of the host.

Configure Google Admin Console for Android Endpoints

Refer to the following sections for information on how to configure VPN configurations for Android endpoints using the Google Admin console:

- Configure an Always On VPN Configuration for Chromebooks Using the Google Admin Console

Configure an Always On VPN Configuration for Chromebooks Using the Google Admin Console

Chromebooks support Always On VPN through extended support for the GlobalProtect app for Android. In an Always On VPN configuration, the secure GlobalProtect connection is always on. Traffic that matches specific filters (such as port and IP address) configured on the GlobalProtect gateway is always routed through the VPN tunnel. By enabling your end users to run the GlobalProtect app for Android on their Chromebooks, you can ensure that they are always connected to GlobalProtect and have access to always on security.

- *The GlobalProtect app for Android is supported only on* certain Chromebooks.
- *Chromebooks that do not support Android applications must continue to use the GlobalProtect app for Chrome. However, these Chromebooks will not support Always On VPN.*
- *If the GlobalProtect app for Android is installed on a Chromebook for Always On VPN capability, the GlobalProtect app for Chrome should not be installed on the same Chromebook.*

Use the following steps to configure an Always On VPN configuration for Chromebooks using the Google Admin console.

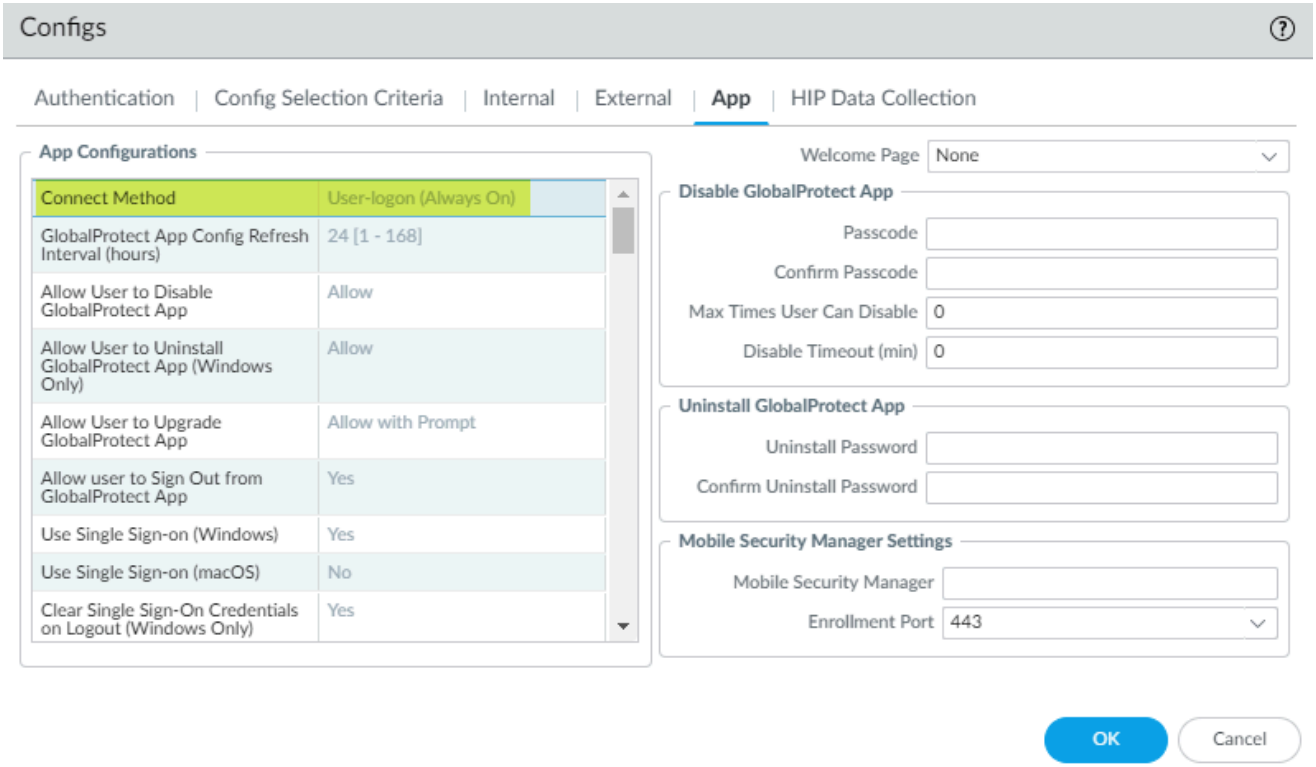
The following steps are applicable only if you Deploy the GlobalProtect App for Android on Managed Chromebooks Using the Google Admin Console. Deploy the GlobalProtect App for Android on Managed Chromebooks Using Workspace ONE does not currently support Always On VPN configurations for the GlobalProtect app for Android on managed Chromebooks.

STEP 1 | From your Palo Alto Networks firewall, Set Up Access to the GlobalProtect Portal.

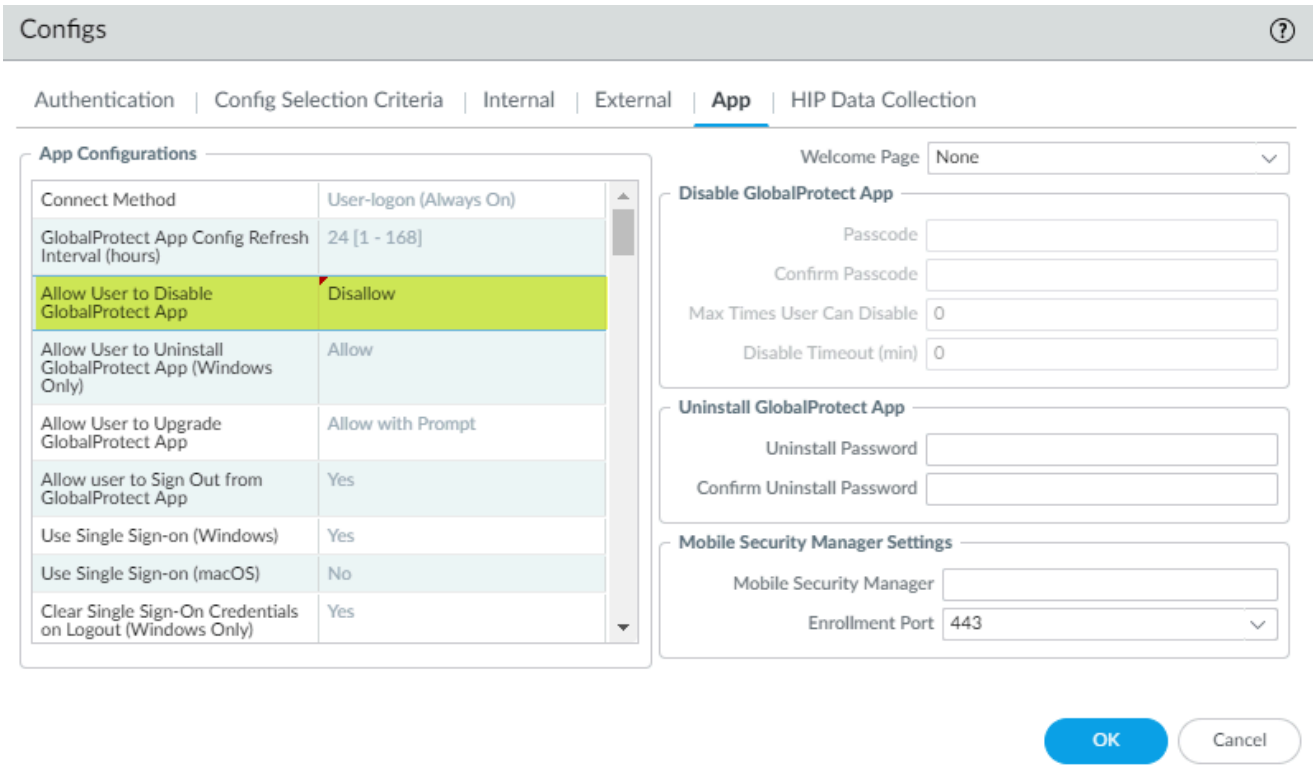
STEP 2 | Define the GlobalProtect Agent Configurations.

STEP 3 | Customize the GlobalProtect App.

- To configure the GlobalProtect connection to be always on, set the **Connect Method** to **User-logon (Always On)**.



- To prevent users from disabling the GlobalProtect app, set the **Allow User to Disable GlobalProtect App** option to **Disallow**.

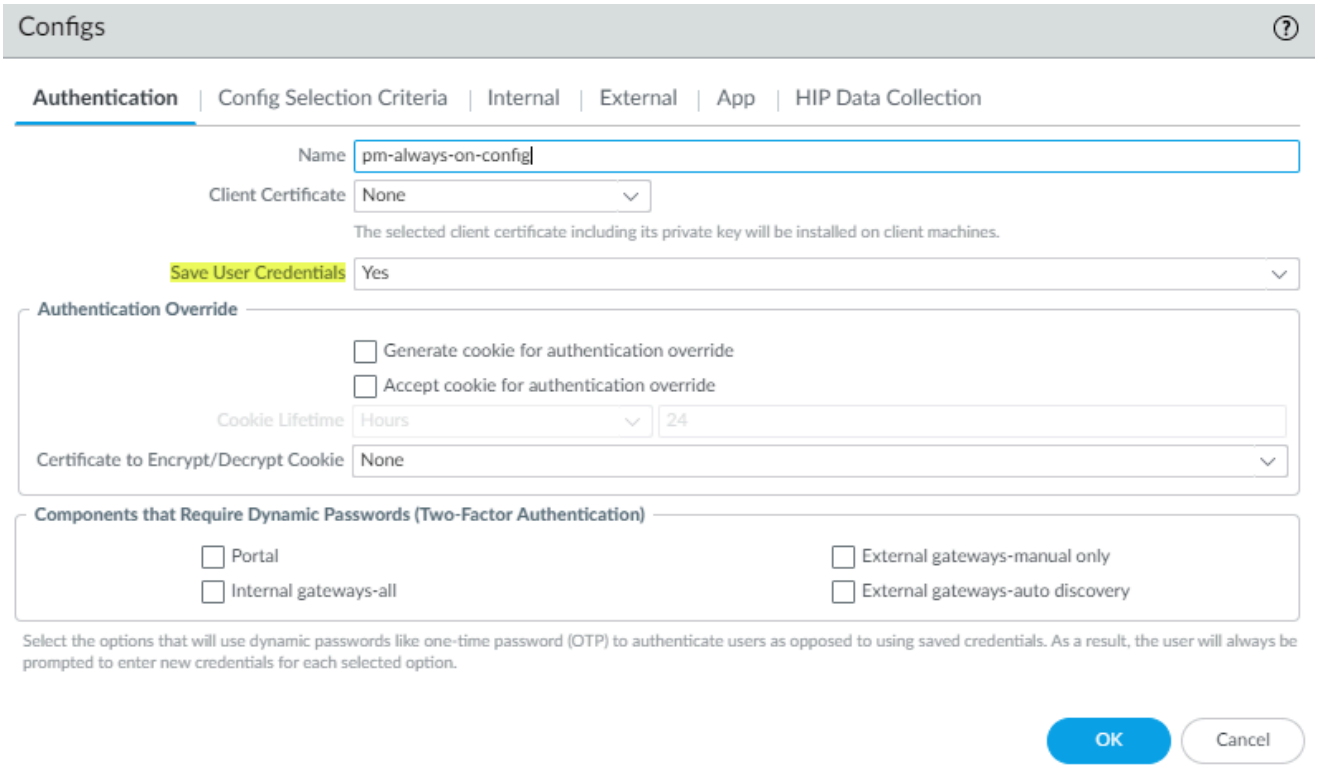


STEP 4 | Enable transparent authentication for GlobalProtect.

To prevent users from skipping GlobalProtect authentication prompts and thereby bypass the GlobalProtect connection upon disconnecting from GlobalProtect, configure one of the following options for transparent authentication:

- Enable users to authenticate to GlobalProtect transparently using Remote Access VPN (Certificate Profile).
- Enable the GlobalProtect app to save both the username and password for transparent login.

  1. From your portal agent configuration (**Network** > **GlobalProtect** > **Portals** > ***<portal-config>*** > **Agent** > ***<agent-config>***), select **Authentication**.
  2. Set the **Save User Credentials** option to **Yes**.

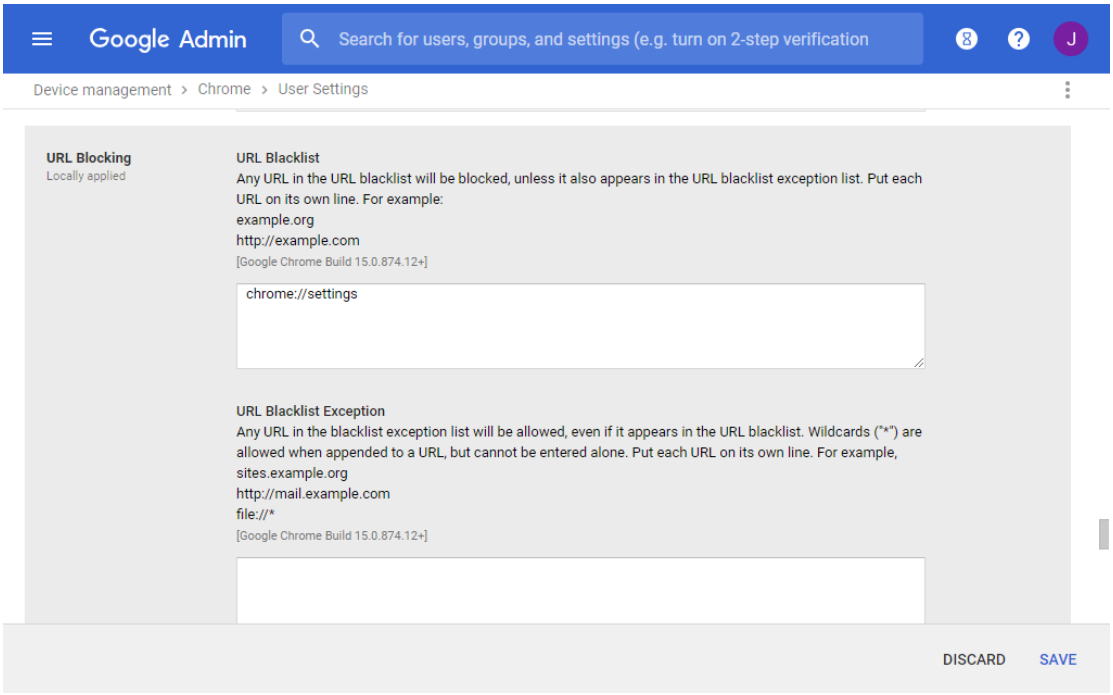


  3. Click **OK** twice to save the portal agent configuration.

STEP 5 | **Commit** your changes on the firewall.

STEP 6 | Prevent Chromebook users from bypassing GlobalProtect using Chrome OS VPN settings.

1. Log in to the Google Admin console as an administrator.
2. Deploy the GlobalProtect App for Android on Managed Chromebooks Using the Google Admin Console on all managed Chromebooks.
3. Blocklist the Chrome settings (**`chrome://settings`**) to prevent users from modifying any VPN settings:
   1. Select **Device Management** > **Chrome management** > **User Settings**.
   2. In the Content > URL Blocking area, enter **`chrome://settings`** in the **URL Blocklist** text box.



4. **SAVE** your changes.

Manage the GlobalProtect App Using Jamf Pro

Where Can I Use This?	What Do I Need?
• Prisma Access • GlobalProtect Subscription	❑ Prisma Access Mobile Users license (for use with Prisma Access) ❑ PAN-OS 10.1 and later ❑ GlobalProtect Gateway license (for use with PAN-OS) ❑ GlobalProtect app for macOS 6.0.4 and later and 6.1 and later releases ❑ Endpoints on macOS 10.15.4 (Catalina) and later, macOS 11 (Big Sur), macOS 12 (Monterey), or macOS 13 (Ventura)

Starting with GlobalProtect App 6.0.4 and later and 6.1 releases, Jamf Pro is officially qualified for deployment of the GlobalProtect app to macOS endpionts.

Jamf Pro is an Enterprise Mobility Management Platform that enables you to manage macOS endpoints from a central console. The GlobalProtect app provides a secure connection between the firewall and the macOS endpoints that Jamf Pro manages at either the device or application level. Using GlobalProtect as the secure connection allows consistent inspection of traffic and enforcement of network security policy for threat prevention on mobile endpoints.

You can use Jamf Pro to deploy the GlobalProtect app with a custom script that contains Deploy App Settings in the macOS Plist, which can be run before or after the GlobalProtect client installation. You can also use Jamf Pro configuration profiles to prevent end user notifications by automatically loading system and network extensions related to features such as split tunnel, split DNS, and enforcer.

The Jamf Pro configuration profile method for deploying VPN settings is not supported. You can configure the VPN settings through the Customize the GlobalProtect App or by using Deploy App Settings in the macOS Plist before you can deploy the app using Jamf Pro.

Refer to the following sections for information on how to deploy the GlobalProtect using Jamf Pro and manage GlobalProtect app notifications:

- Create a Smart Computer Group for GlobalProtect App Deployment
- Create a Single Configuration Profile for the GlobalProtect App for macOS
- Deploy the GlobalProtect Mobile App Using Jamf Pro
- Enable System and Network Extensions on macOS Endpoints Using Multiple Configuration Profiles
- Uninstall the GlobalProtect Mobile App Using Jamf Pro

If you are not using a Qualified MDM Vendors, you can Manage the GlobalProtect App Using Other Third-Party MDMs.

Create a Smart Computer Group for GlobalProtect App Deployment

Where Can I Use This?	What Do I Need?
• Prisma Access • GlobalProtect Subscription	❑ Prisma Access Mobile Users license (for use with Prisma Access) ❑ PAN-OS 10.1 and later ❑ GlobalProtect Gateway license (for use with PAN-OS) ❑ GlobalProtect app for macOS 6.0.4 and later and 6.1 and later releases ❑ Endpoints on macOS 10.15.4 (Catalina) and later, macOS 11 (Big Sur), macOS 12 (Monterey), or macOS 13 (Ventura)

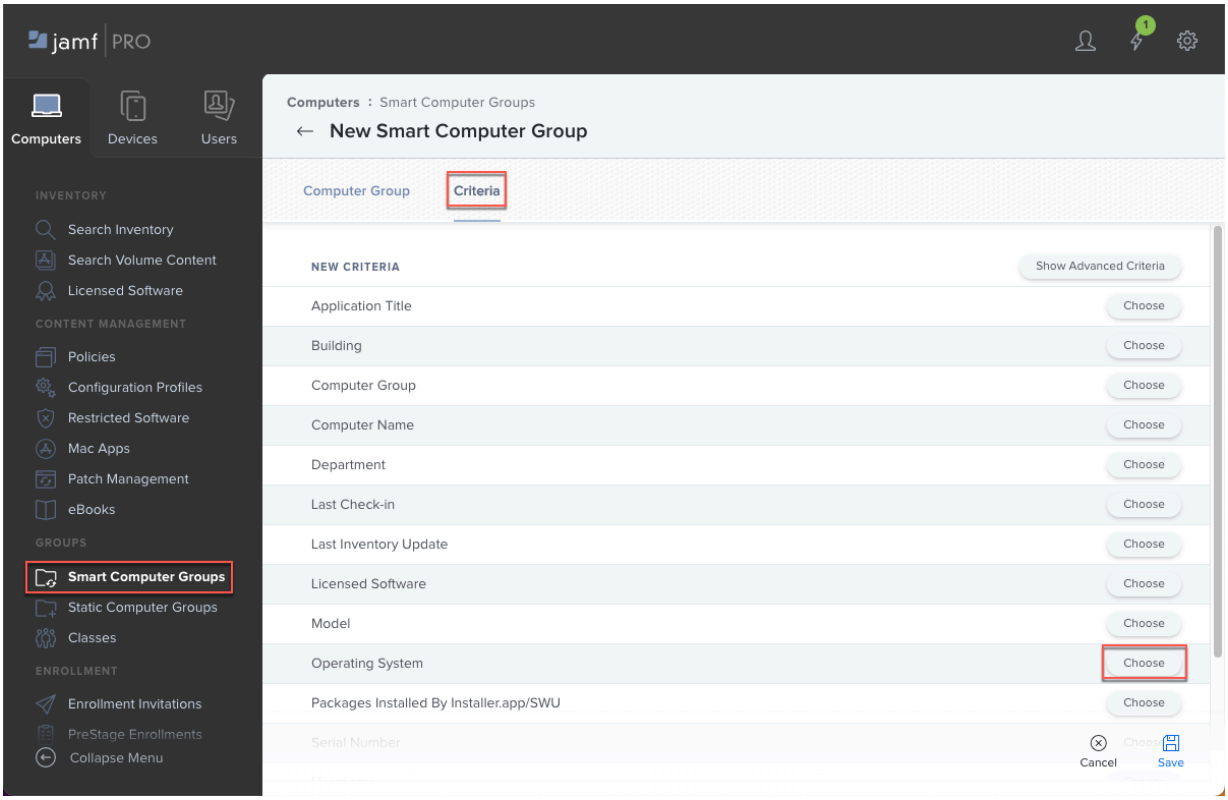
You can create a Jamf Smart Computer Group in Jamf Pro to target managed macOS devices for the installation of the GlobalProtect app. When you set up configuration profiles or Jamf policies for GlobalProtect app deployment, you can set the scope to the Smart Computer Group that you created.

STEP 1 | In Jamf Pro, select **Computers** > **Smart Computer Groups** > **New**.

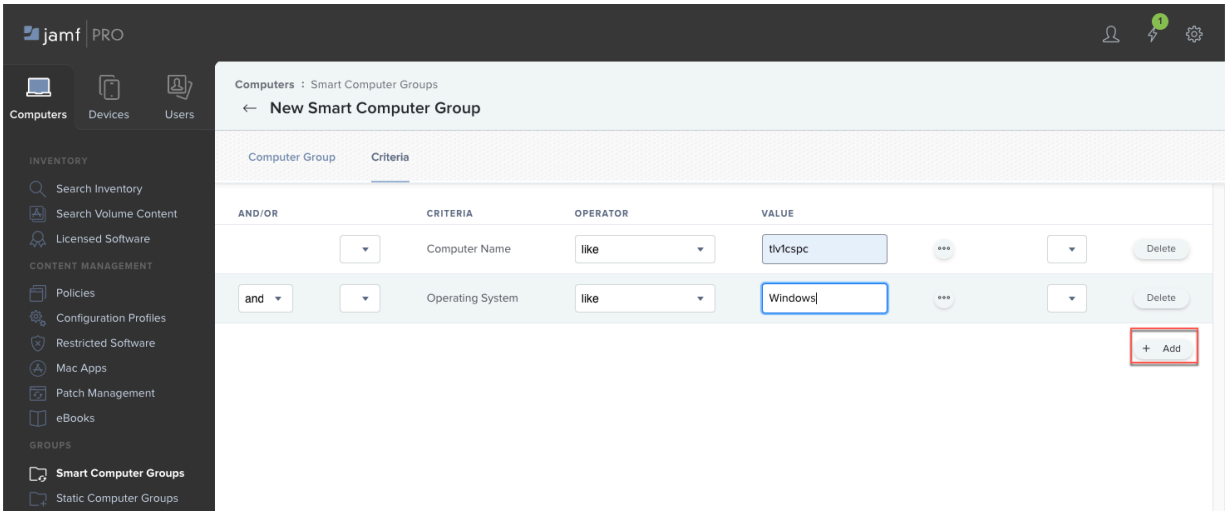
STEP 2 | Enter a **Display Name** for the group.

STEP 3 | Select **Criteria** and **Add** a criteria for the group.

STEP 4 | **Choose** a criteria from the list.



STEP 5 | Select the **Operator** and **Value** for the criteria. If necessary, you can **Add** more criteria.



STEP 6 | **Save** your settings.

Create a Single Configuration Profile for the GlobalProtect App for macOS

Where Can I Use This?	What Do I Need?
• Prisma Access • GlobalProtect Subscription	❑ Prisma Access Mobile Users license (for use with Prisma Access) ❑ PAN-OS 10.1 and later ❑ GlobalProtect Gateway license (for use with PAN-OS) ❑ GlobalProtect app for macOS 6.0.4 and later and 6.1 and later releases ❑ Endpoints on macOS 10.15.4 (Catalina) and later, macOS 11 (Big Sur), macOS 12 (Monterey), or macOS 13 (Ventura)

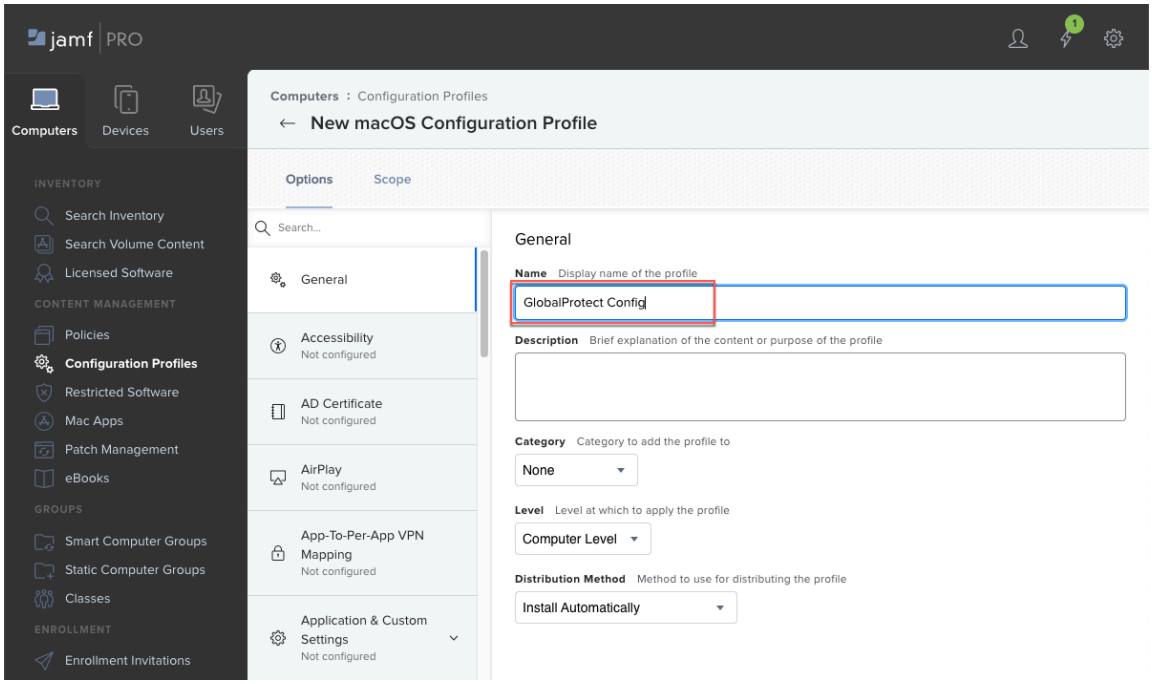
Before you Deploy the GlobalProtect Mobile App Using Jamf Pro, you can create and deploy a single configuration profile that defines the configuration of GlobalProtect app 6.0.4 and later and 6.1 and later releases on managed macOS devices. For example, you can set up the configuration profile to load system extensions to provide a seamless experience when users run the GlobalProtect app to access the internet, SaaS applications, private applications, and resources in your organization.

If you want to use multiple configuration profiles instead of a single configuration profile, skip this procedure and Enable System and Network Extensions on macOS Endpoints Using Multiple Configuration Profiles.

Before you begin, Create a Smart Computer Group for GlobalProtect App Deployment so that you can deploy this configuration profile to the computers in the Smart Computer Group.

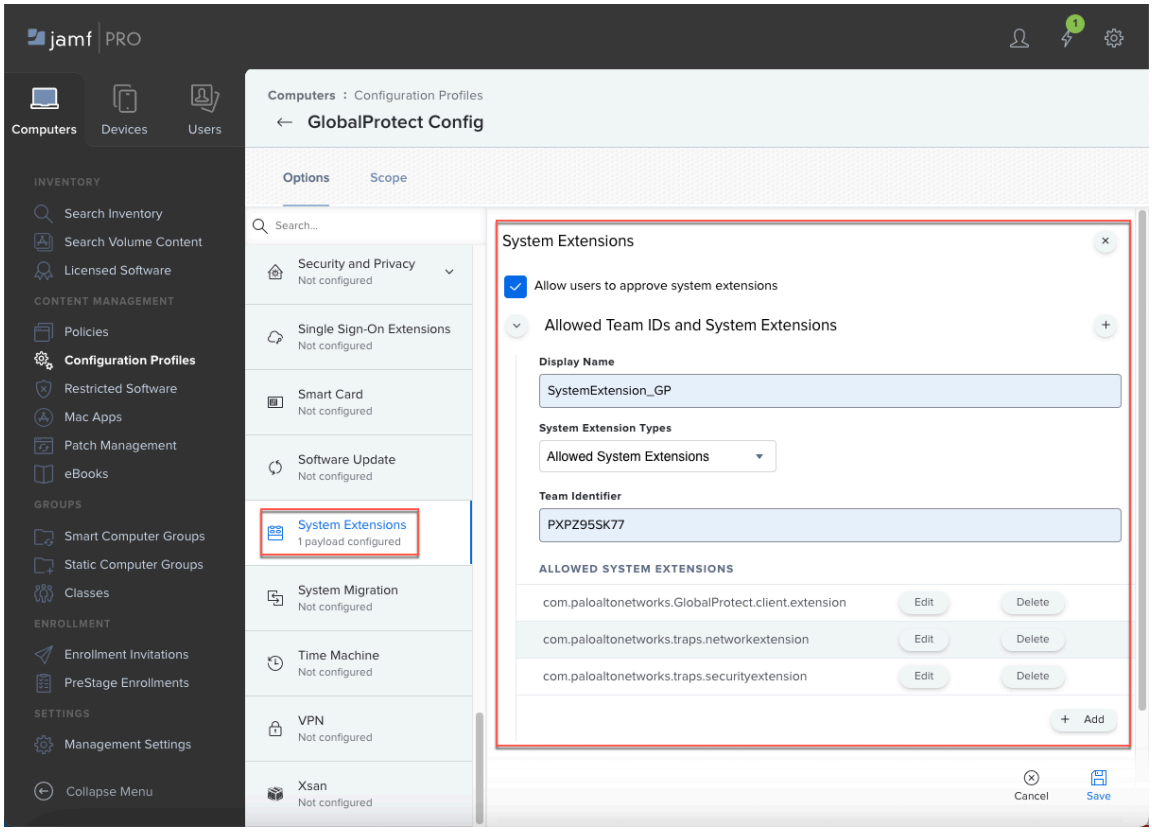
STEP 1 | Create a configuration profile for the GlobalProtect app and specify general settings.

1. In Jamf Pro, select **Computers** > **Configuration Profiles** > **New**.
2. Enter a **Display Name** for the configuration profile.



STEP 2 | Create a payload to automatically load GlobalProtect system extensions. This configuration suppresses notification pop-ups and enables the GlobalProtect app to run without prompting users to accept the extensions.

1. If you saved your settings in the previous step, click **Edit**.
2. Select **System Extensions** > **Configure**.
3. Specify the following settings:
   - **Display Name**—Enter a name for the system extensions payload, such as **`SystemExtension_GP`**
   - **System Extension Types**—Select **Allowed System Extensions**
   - **Team Identifier**—Enter **PXPZ95SK77**
   - **ALLOWED SYSTEM EXTENSIONS**—**Add** and **Save** the following system extensions:
     - **`com.paloaltonetworks.GlobalProtect.client.extension`**—Enables system extensions, which are used for the split tunnel and enforce GlobalProtect connections for network access features
     - **`com.paloaltonetworks.traps.networkextension`**—Enables network extensions for Cortex XDR (required only if you are using Cortex XDR)
     - **`com.paloaltonetworks.traps.securityextension`**—Enables security extensions for Cortex XDR (required only if you are using Cortex XDR)



4. **Save** your settings.

STEP 3 | If you configured the GlobalProtect app with the Customize the GlobalProtect App feature on macOS endpoints, create a payload to filter network content.

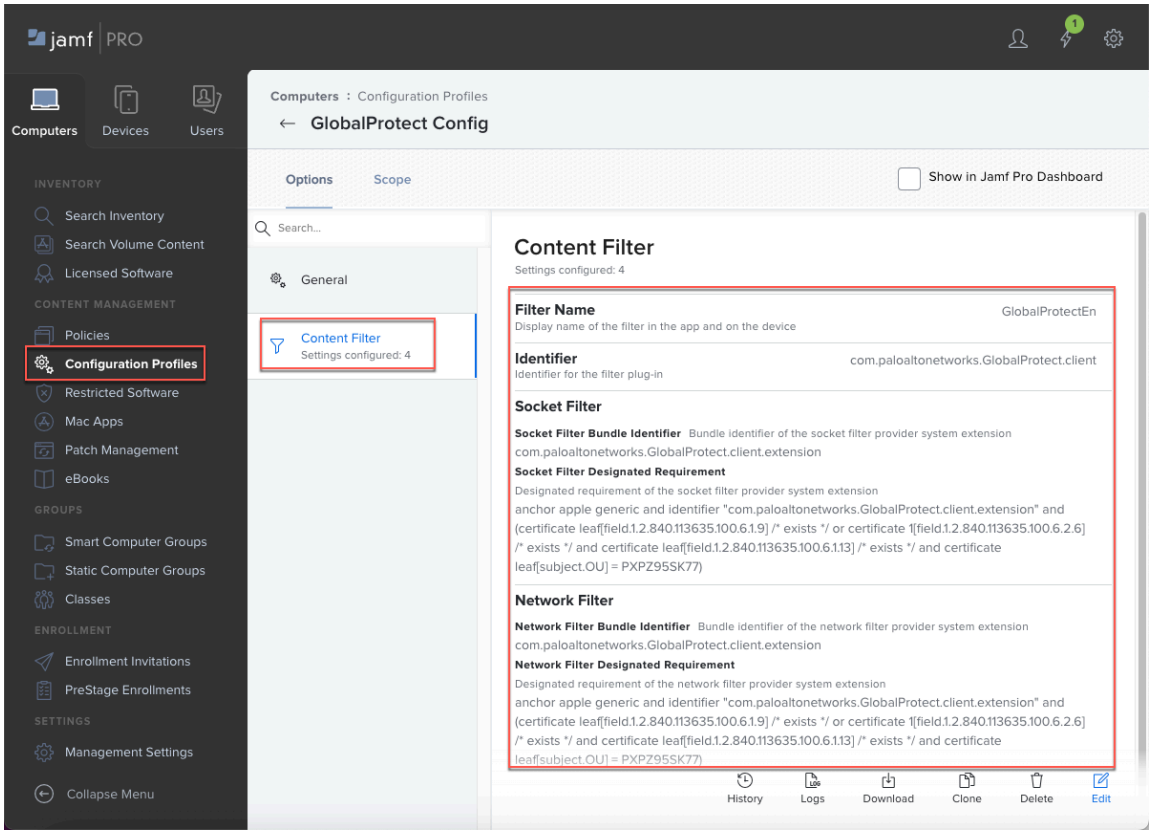
1. If you saved your settings in the previous step, click **Edit**.
2. Select **Content Filter**.
3. Specify the following settings:
   - **Filter Name**—Enter the name of the filter, such as **`GlobalProtectEn`**
   - **Identifier**—Enter **`com.paloaltonetworks.GlobalProtect.client`**
   - **Socket Filter Bundle Identifier**—Enter **`com.paloaltonetworks.GlobalProtect.client.extension`**
   - **Socket Filter Designated Requirement**—Enter the following requirement:

     ```
     anchor apple generic and identifier
     "com.paloaltonetworks.GlobalProtect.client.extension" and
     (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists
     */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists
     */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /*
     exists */ and certificate leaf[subject.OU] = PXPZ95SK77)
     ```
   - **Network Filter Bundle Identifier**—Enter **`com.paloaltonetworks.GlobalProtect.client.extension`**
   - **Network Filter Designated Requirement**—Enter the following requirement:

     ```
     anchor apple generic and identifier
     "com.paloaltonetworks.GlobalProtect.client.extension" and
     (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists
     */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists
     ```



```
*/ and certificate leaf[field.1.2.840.113635.100.6.1.13] /*
exists */ and certificate leaf[subject.OU] = PXPZ95SK77)
```



4. **Save** your settings.

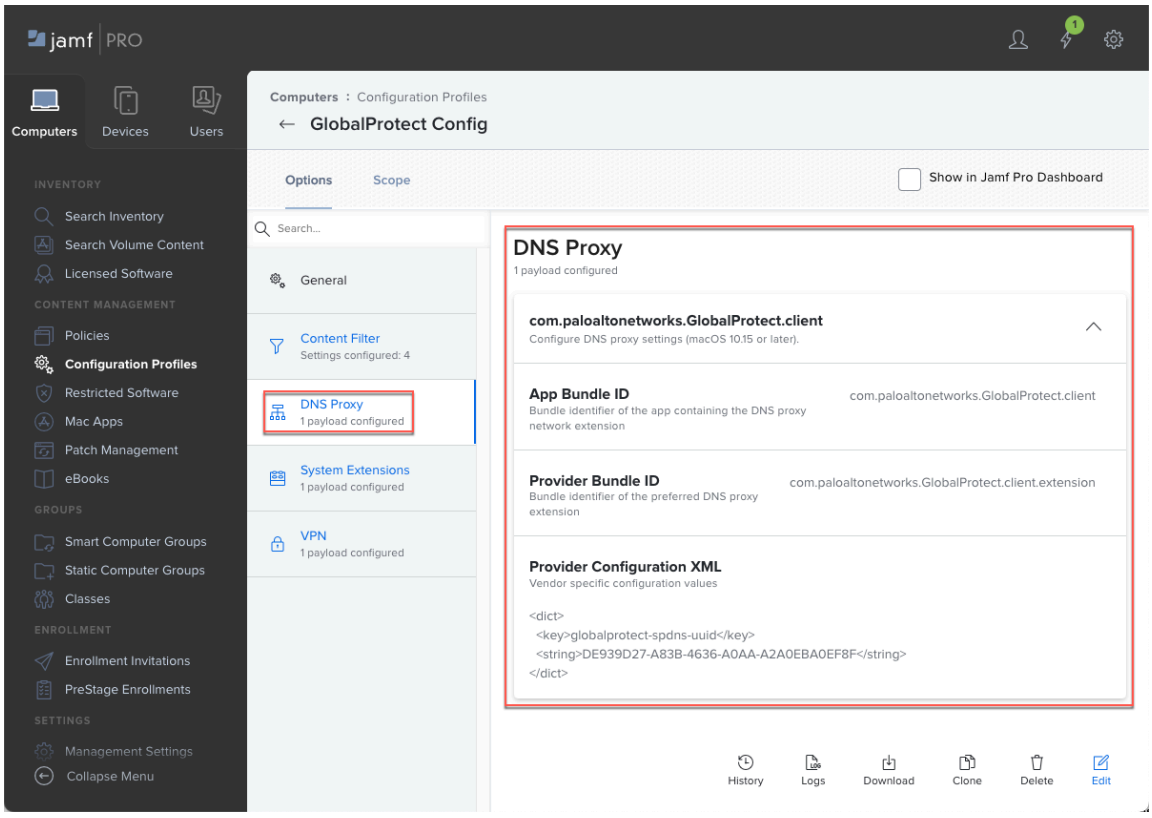
STEP 4 | Optional: Create a DNS Proxy payload if you configured the split DNS feature.

1. If you saved your settings in the previous step, click **Edit**.
2. Select **DNS Proxy** > **Add**.
3. Specify the following settings:
   - **App Bundle ID**—Enter **`com.paloaltonetworks.GlobalProtect.client`**
   - **Provider Bundle ID**—Enter **`com.paloaltonetworks.GlobalProtect.client.extension`**
   - **Provider Configuration XML**—Enter the following text:

```
<dict>
  <key>globalprotect-spdns-uuid</key>
  <string>DE939D27-A83B-4636-A0AA-A2A0EBA0EF8F</string>
```



```
</dict>
```



STEP 5 | Optional: If you Configure a Split Tunnel Based on the Domain and Application, create a VPN payload.

There can only be one VPN payload per configuration profile. If you need more than one VPN payload, you must create a separate configuration profile with the additional payload.

1. If you saved your settings in the previous step, click **Edit**.
2. Select **VPN** > **Configure**.
3. Specify the following settings:
   - **Connection Name**—Enter a name for the connection, such as **`GP_split_tunnel_app`**
   - **VPN Type**—Select **Per-App VPN**
   - **Per-App VPN Connection Type**—Select **Custom SSL**
   - **Identifier**—Enter **`com.paloaltonetworks.GlobalProtect.client`**
   - **Server**—Enter the hostname or IP address of the GlobalProtect portal that users will connect to
   - **Custom Data**—**Add** and **Save** the following key and value:
     - **KEY**—Enter **`globalprotect-spapp-uuid`**
     - **VALUE**—Enter **`B078FC83-11E5-4559-AA53-E24D2A63B0F9`**
   - **Provider Type**—Select **App-proxy**
4. **Save** your settings.

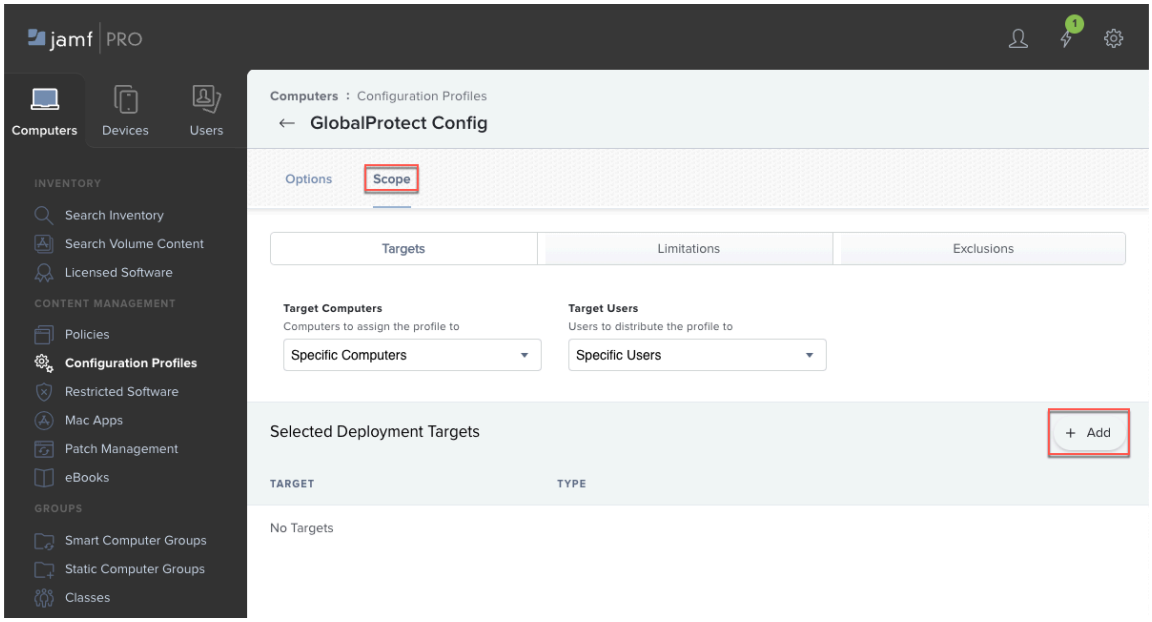
STEP 6 | Optional: If you Configure a Split Tunnel Based on the Domain and Application, create a VPN payload.

There can only be one VPN payload per configuration profile. If you need more than one VPN payload, you must create a separate configuration profile with the additional payload.

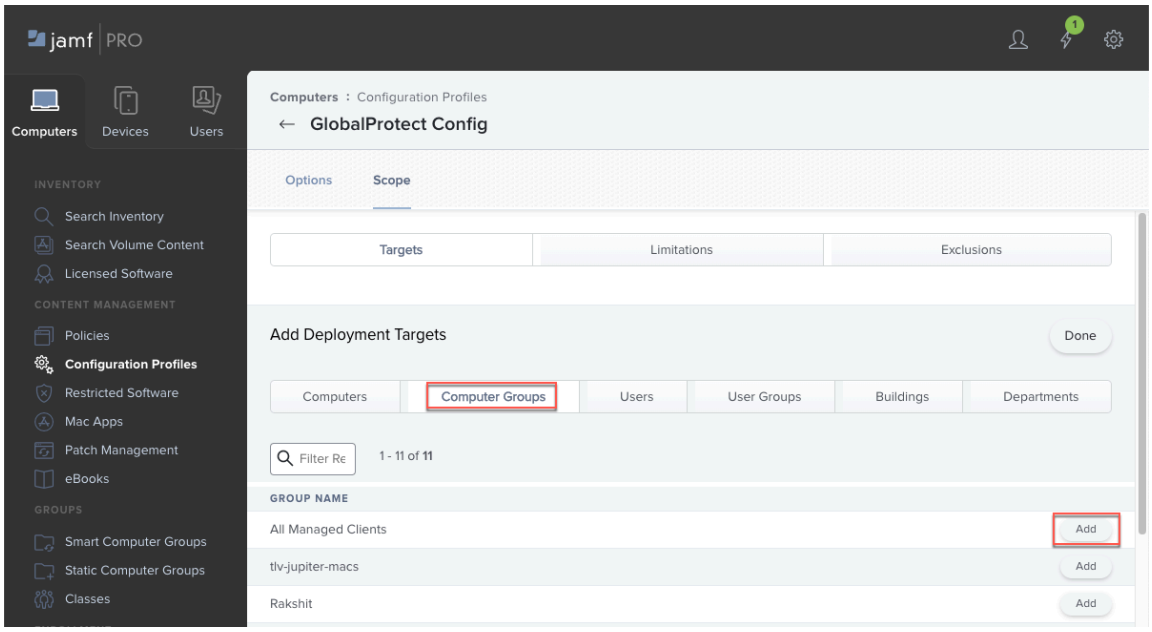
1. If you saved your settings in the previous step, click **Edit**.
2. Select **VPN** > **Configure**.
3. Specify the following settings:
   - **Connection Name**—Enter a name for the connection, such as **`GP_split_tunnel_domain`**
   - **VPN Type**—Select **VPN**
   - **Per-App VPN Connection Type**—Select **Custom SSL**
   - **Identifier**—Enter **`com.paloaltonetworks.GlobalProtect.client`**
   - **Server**—Enter the hostname or IP address of the GlobalProtect portal that users will connect to
   - **Custom Data**—**Add** and **Save** the following key and value:
     - **KEY**—Enter **`globalprotect-spdomain-uuid`**
     - **VALUE**—Enter **`0894A92D-70D2-475A-B5B6-FB07F2DEAA77`**
   - **Provider Type**—Select **App-proxy**
4. **Save** your settings.

STEP 7 | Set the scope for the configuration profile.

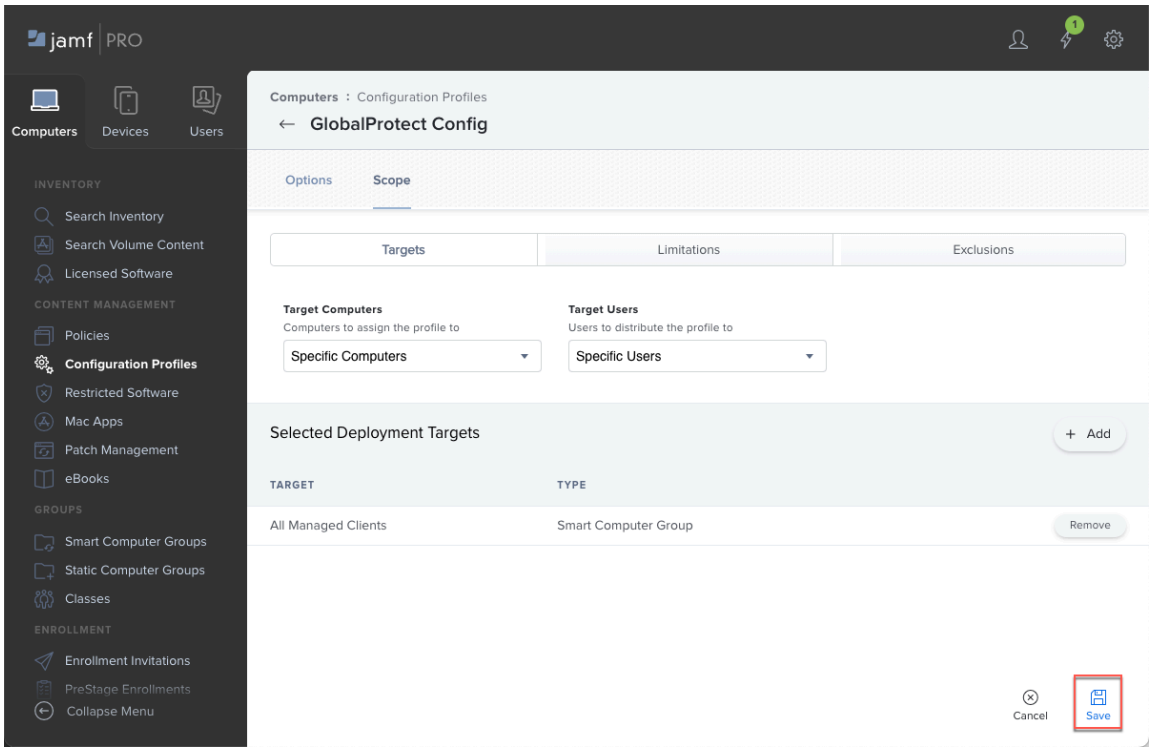
1. **Edit** the configuration profile.
2. Select **Scope** and **Add** a deployment target.



3. Click **Computer Groups** and **Add** the Smart Computer Group that you created. Then, click **Done**.



4. **Save** the scope of the profile. Jamf will distribute the profile to the devices in the selected computer group the next time they contact Jamf Pro.



Deploy the GlobalProtect Mobile App Using Jamf Pro

Where Can I Use This?	What Do I Need?
• Prisma Access • GlobalProtect Subscription	❑ Prisma Access Mobile Users license (for use with Prisma Access) ❑ PAN-OS 10.1 and later ❑ GlobalProtect Gateway license (for use with PAN-OS) ❑ GlobalProtect app for macOS 6.0.4 and later and 6.1 and later releases ❑ Endpoints on macOS 10.15.4 (Catalina) and later, macOS 11 (Big Sur), macOS 12 (Monterey), or macOS 13 (Ventura)

Starting with GlobalProtect app 6.0.4 and later and 6.1 releases, you can deploy the GlobalProtect app to managed macOS endpoints that have enrolled with Jamf Pro by using a script that prepopulates GlobalProtect app settings such as the default portal address and connection method. As a best practice, you can also target the app installation or upgrade to a smaller group of endpoints before rolling out the installation to the rest of your organization.

For a demonstration on how to deploy the GlobalProtect app by using Jamf Pro, watch this video.

Before you begin, Create a Single Configuration Profile for the GlobalProtect App for macOS or Enable System and Network Extensions on macOS Endpoints Using Multiple Configuration Profiles.

For step-by-step instructions, refer to the following procedure:

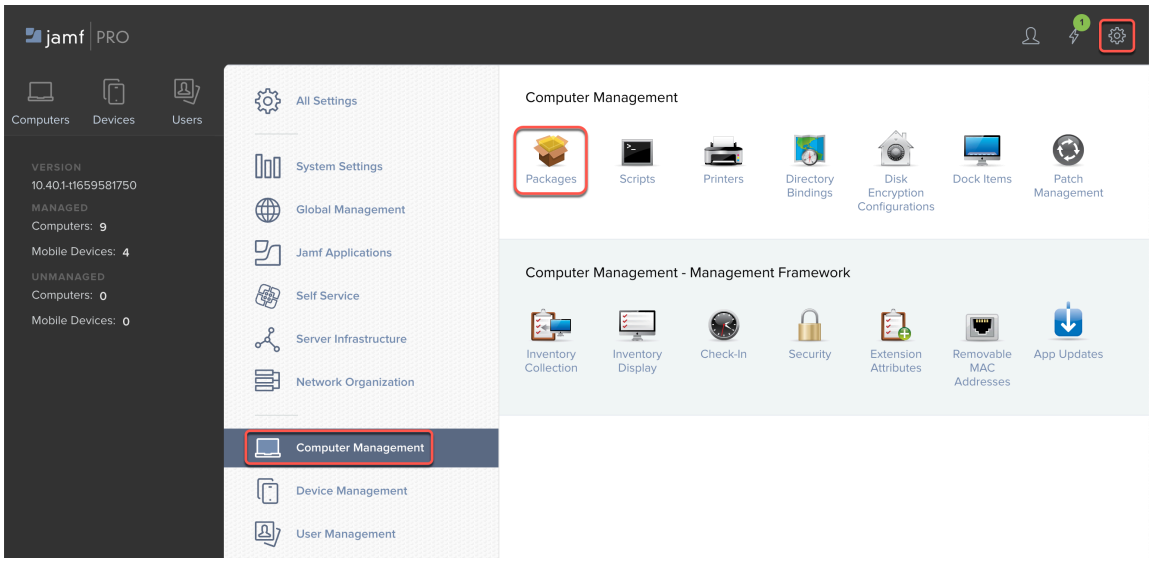
STEP 1 | Download the GlobalProtect app package for macOS from the Customer Support Portal (CSP).

1. Log in to the Palo Alto Networks Customer Support Portal (https://support.paloaltonetworks.com/).

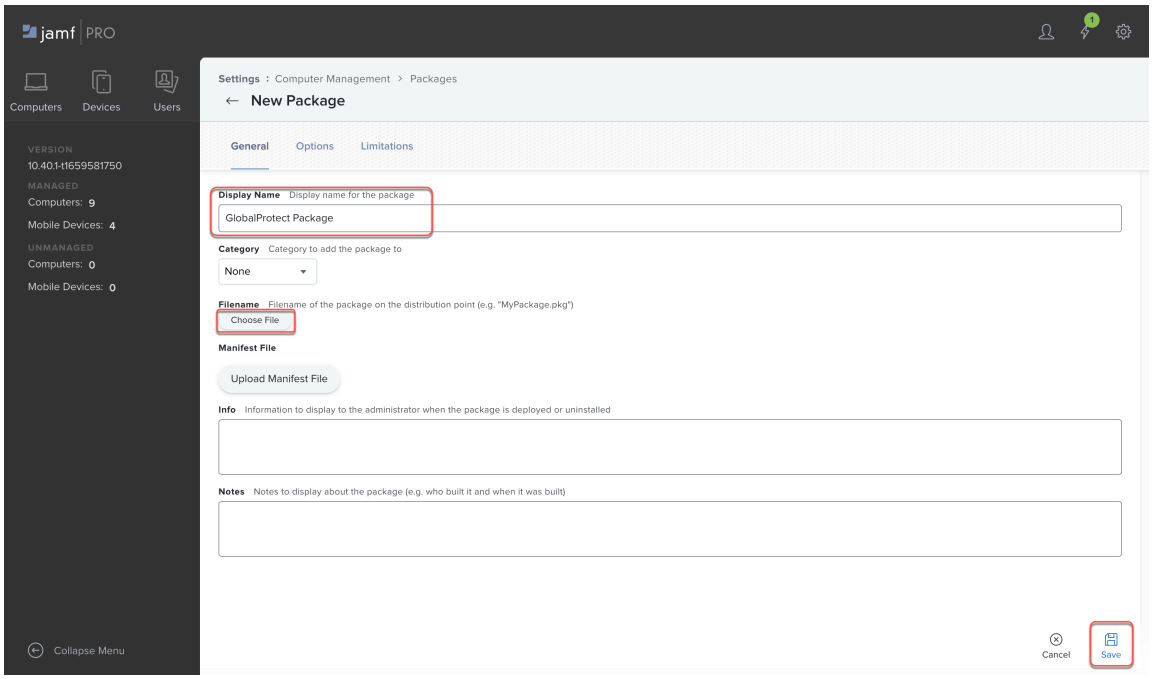
   You must have a valid Palo Alto Networks Customer Support Portal account to log in to and download software from the Software Updates page.
2. Select **Updates** > **Software Updates**.
3. Select the GlobalProtect app version for macOS.
4. Review the Release Notes for the app version, and then select the download link.

STEP 2 | Upload the GlobalProtect app PKG file to Jamf Pro:

1. Select **Settings** > **Computer Management** > **Packages**.



2. Click **New**.
3. Configure general settings for the package, including the display name and category (optional).
4. Click **Choose File** and select the GlobalProtect app package to upload.
5. **Save** your settings.



STEP 3 | Create a script that will be added to Jamf Pro to prepopulate default settings, such as the default GlobalProtect portal and connection method.

The following example is provided as a reference. Customize the script and Customizable App Settings as needed for your environment.

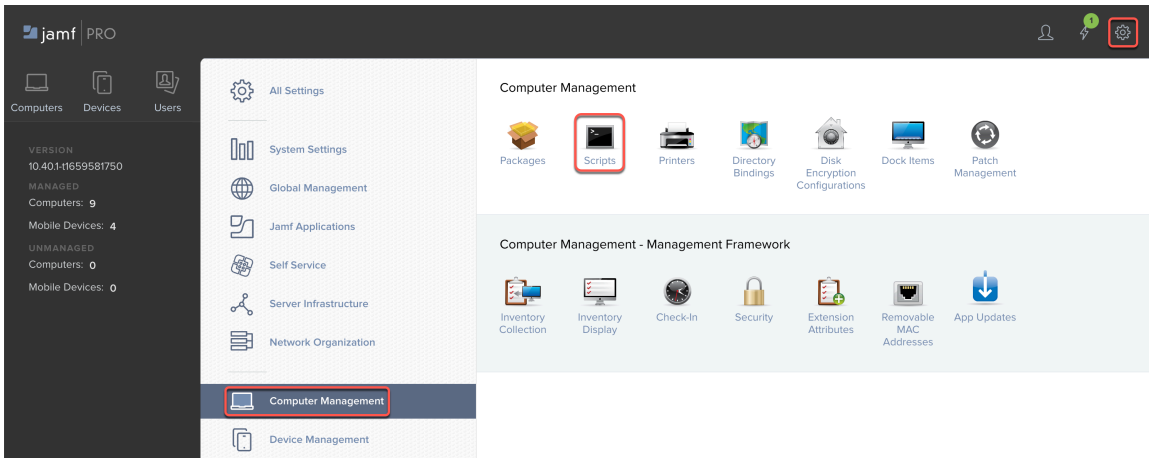
```
#!/bin/bash
## Description: Checks for global preferences file and populates
## it with the default portal if needed.
## Body ##########################################################
## Declare Variables #############################################

# Get current Console user
active_user=$( stat -f "%Su" /dev/console )

# Global Prefs File
gPrefs=/Library/Preferences/
com.paloaltonetworks.GlobalProtect.settings.plist

## Logic #########################################################

# Check to see if the global preference file already exists...
if [[ -e $gPrefs ]]; then
 echo "Default global portal already exists. Skipping."
else
 echo "Setting default global portal to: your.portal.here.com"
     # If it does not already exist, create it and populate the
 default portal using the echo command
       echo '<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://
www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>Palo Alto Networks</key>
    <dict>
        <key>GlobalProtect</key>
        <dict>
            <key>PanSetup</key>
            <dict>
                <key>Portal</key>
                <string>your.portal.here.com</string>
                <key>Prelogon</key>
                <string>0</string>
            </dict>
            <key>Settings</key>
            <dict>
                <key>connect-method</key>
                <string>on-demand</string>
            </dict>
        </dict>
    </dict>
</dict>
</plist>
' > $gPrefs
echo $?
```



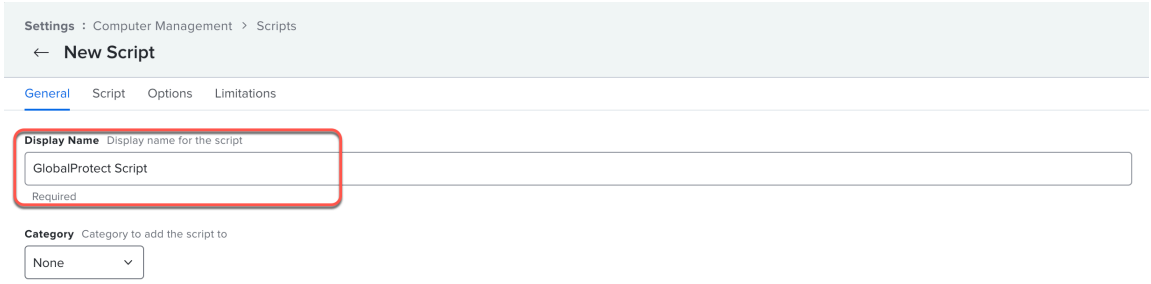
```
 # Kill the Preference caching daemon to prevent it from
 overwriting any changes
 killall cfprefsd
 echo $?
fi
# Check exit code.
exit $?
```


STEP 4 | Add the script to Jamf Pro.

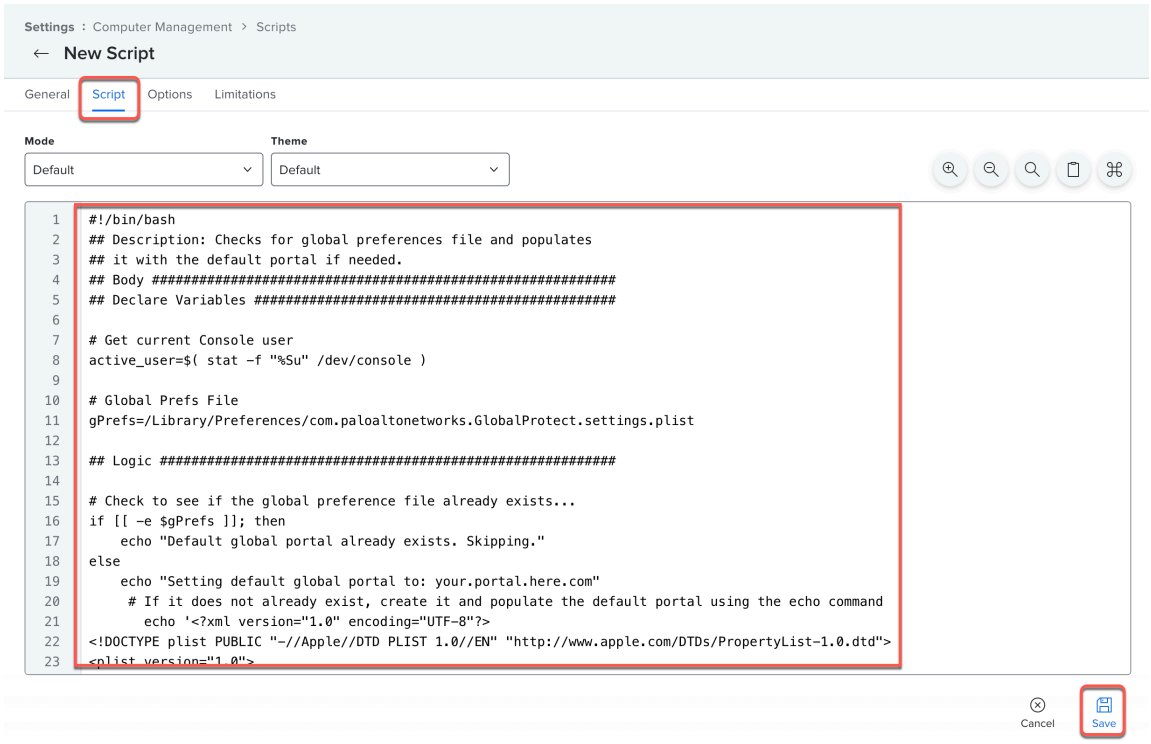
1. Select **Settings** > **Computer Management** > **Scripts**.



2. Click **New**.
3. Enter a **Display Name** for the script.



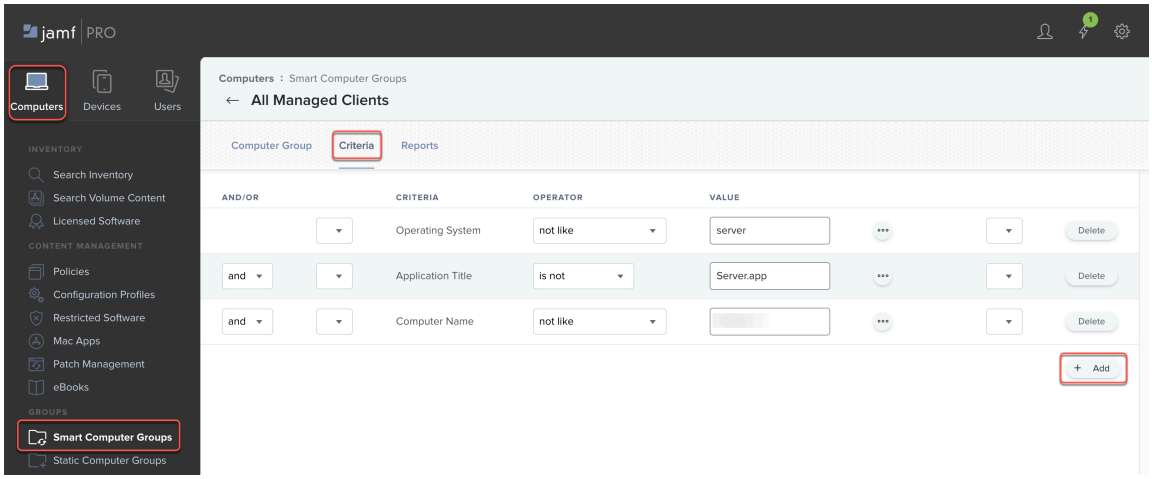
4. Select **Script** and copy and paste your script to the editor.



5. **Save** the script.

STEP 5 | If you have not done so already, create a Jamf Smart Computer Group to target specific macOS devices for installation of the GlobalProtect app.

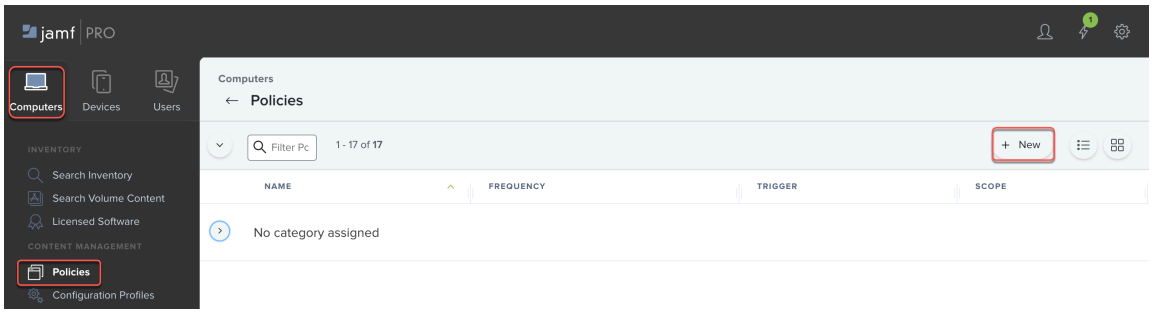
1. Select **Computers** > **Smart Computer Groups** > **New**.
2. Enter a **Display Name** for the group.
3. Select **Criteria** and **Add** the criteria for the group.



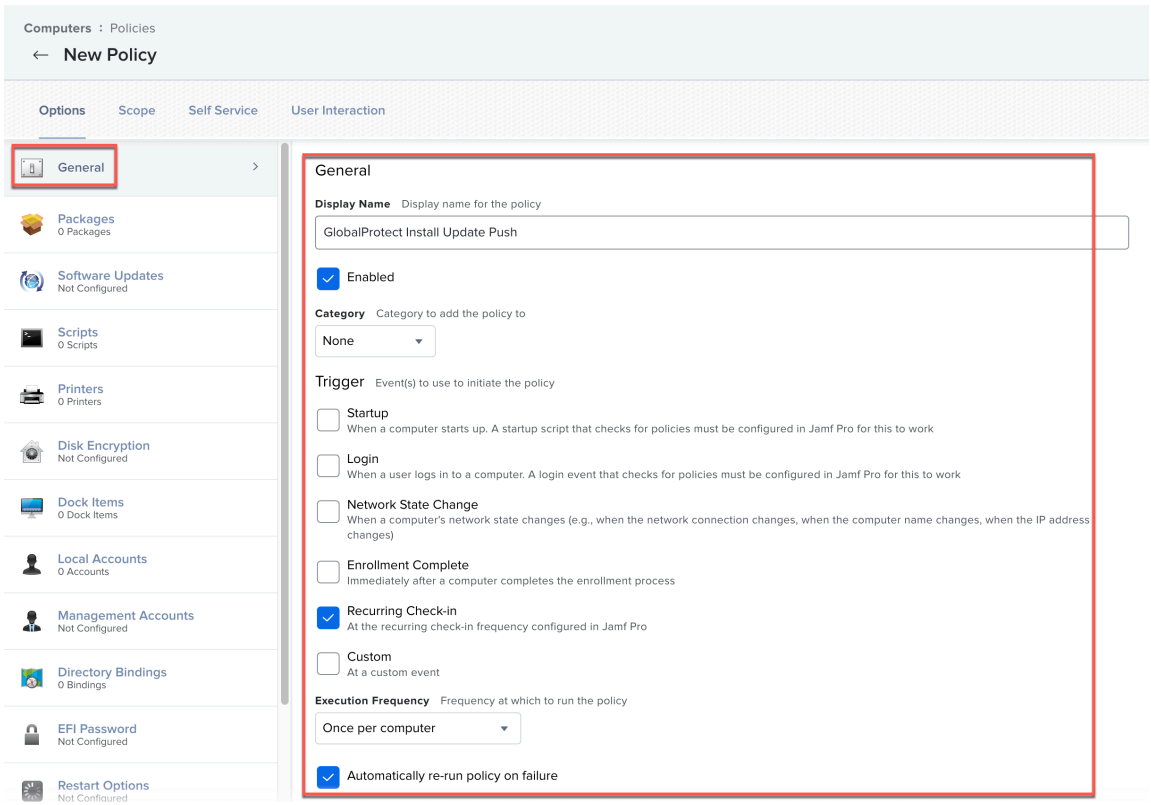
4. **Save** your settings.

STEP 6 | Create a Jamf Policy by adding the GlobalProtect package and script to the policy, and setting the scope to the Smart Computer Group that you created for your macOS devices in step 5.

1. In Jamf Pro, select **Computers** > **Policies** > **New**.

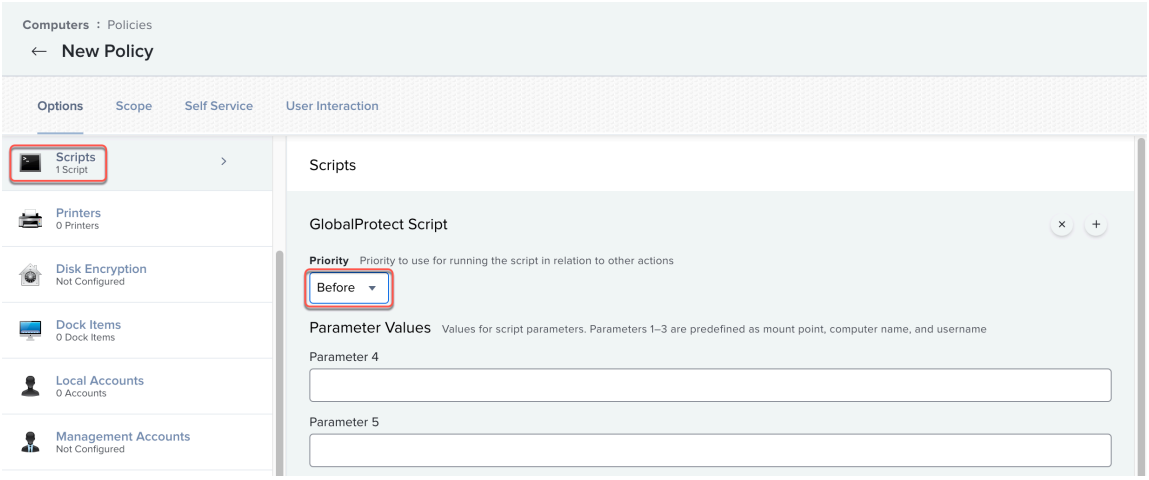


2. In the **General** payload, configure the basic settings for the policy:
   - Enter a **Display Name** for the policy and **Enable** the policy.
   - (Optional) Select a **Category**.
   - Specify a **Trigger** that will initiate a policy, such as **Recurring Check-in**.
   - Select an **Execution Frequency**, such as **Once per computer** and **Automatically re-run the policy on failure**.

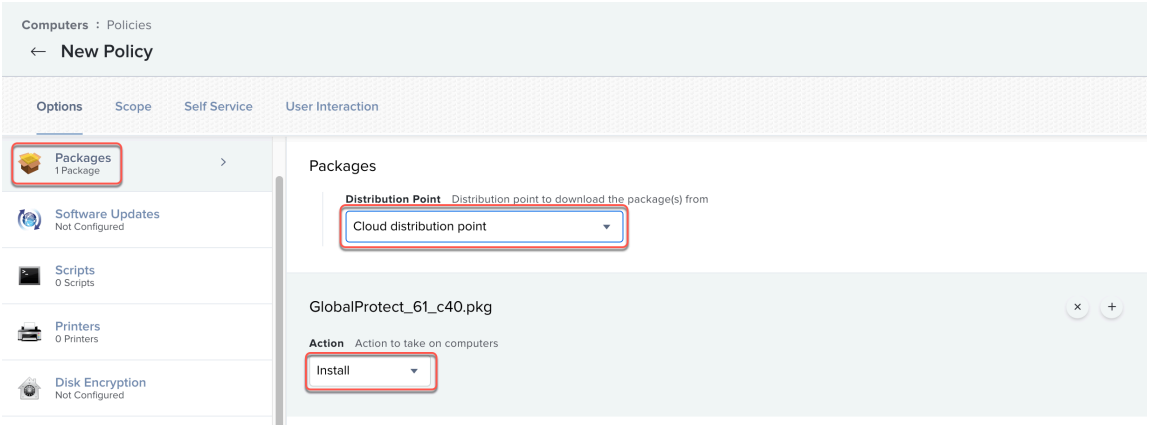


3. Configure the Scripts payload by selecting **Scripts** > **Configure**.

   Add the script that you created in step 4 and select the **Priority** for running the script.

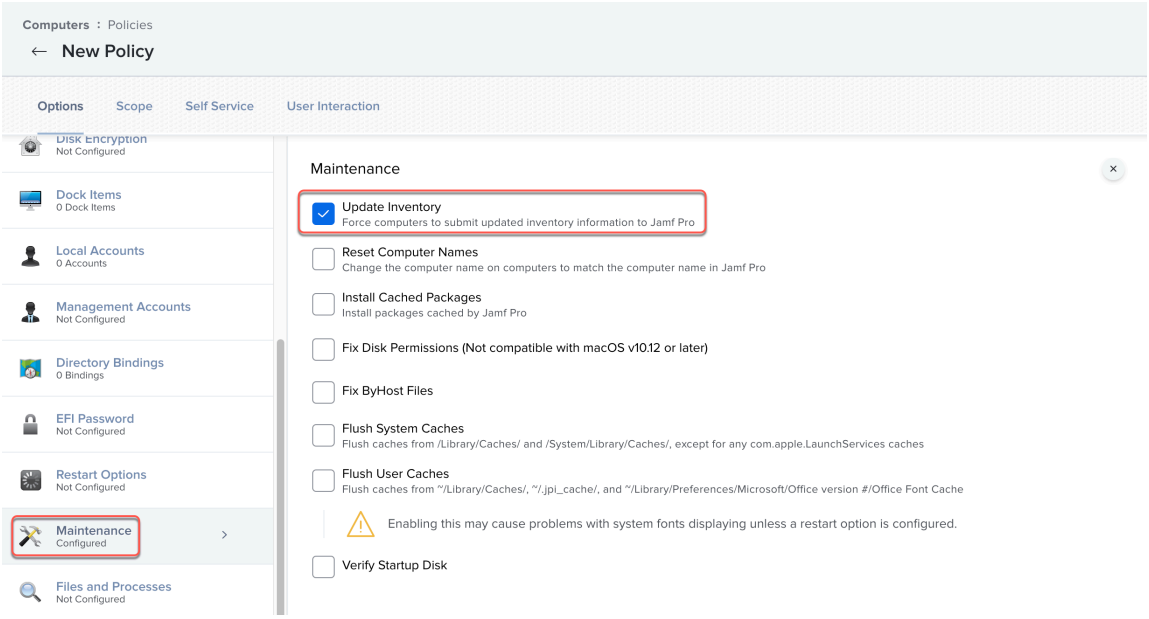


4. Configure the Packages payload by selecting **Packages** > **Configure**.
   1. **Add** the GlobalProtect app package that you uploaded in step 2.
   2. Select a **Distribution Point**.
   3. Select **Install** in the **Action** menu.



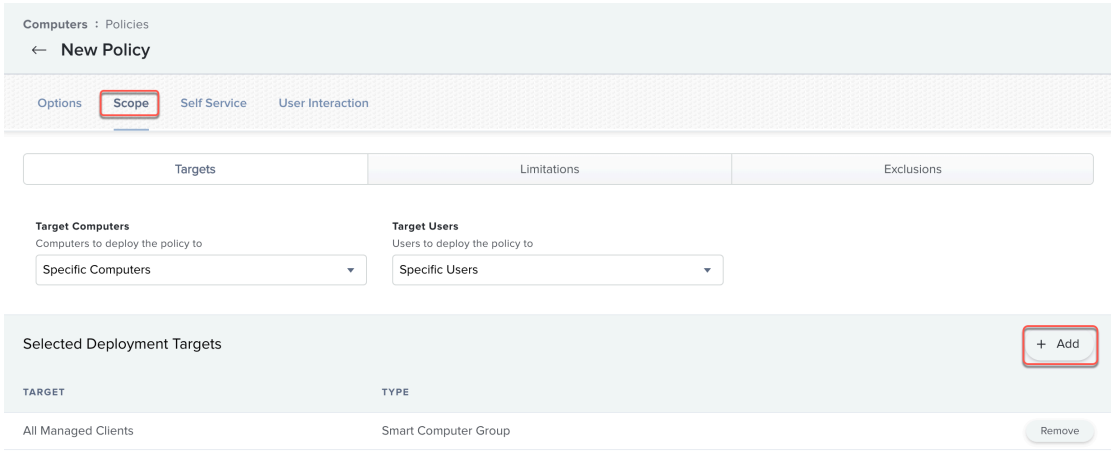
5. Configure the Maintenance payload by selecting **Maintenance** > **Configure**.

   Select **Update Inventory**.



6. Configure the scope of the policy.

   1. Select **Scope** and **Add** a deployment target.



   2. Click **Computer Groups** and **Add** the Smart Computer Group that you created in step 5.
   3. Click **Done**. The computers in the selected computer group will be targeted for deployment of the GlobalProtect app.

7. **Save** the policy.

   The next time macOS endpoints in the Smart Computer Group that is scoped to the policy check in with Jamf Pro and meet the trigger in the General payload, the policy will run and deploy the GlobalProtect app to the endpoints.

Enable System and Network Extensions on macOS Endpoints Using Multiple Configuration Profiles

Where Can I Use This?	What Do I Need?
• Prisma Access • GlobalProtect Subscription	❑ Prisma Access Mobile Users license (for use with Prisma Access) ❑ PAN-OS 10.1 and later ❑ GlobalProtect Gateway license (for use with PAN-OS) ❑ GlobalProtect app for macOS 6.0.4 and later and 6.1 and later releases ❑ Endpoints on macOS 10.15.4 (Catalina) and later, macOS 11 (Big Sur), macOS 12 (Monterey), or macOS 13 (Ventura)

End users must enable system and network extensions on macOS endpoints if the GlobalProtect app is configured with any of the following features:

- Configure a Split Tunnel Based on the Domain and Application
- Enforce GlobalProtect connections for network access (see Customize the GlobalProtect App) without requiring Enable Kernel Extensions in the GlobalProtect App for macOS Endpoints
- Split DNS

After the installation or upgrade of the GlobalProtect app on a macOS device, notification messages appear that prompt users to load the GlobalProtect system extension and network extensions that were blocked from loading.

To allow the GlobalProtect app to run seamlessly without disruption on macOS endpoints, you can create GlobalProtect signed configuration profiles and deploy them using Jamf Pro to load the system and network extensions, and suppress the notification pop-ups automatically.

The following procedures assume that the macOS endpoints do not have network extensions enabled manually. If users already enabled network extensions when they were notified by GlobalProtect pop-ups, deploying configuration profiles using Jamf Pro to enable network extensions will create duplicate network extension entries on the macOS endpoints.

Refer to the following sections for information on how to enable system and network extensions on the GlobalProtect app for macOS endpoints:

- Enable GlobalProtect System Extensions on macOS Endpoints Using Jamf Pro
- Enable GlobalProtect Network Extensions on macOS Catalina Endpoints Using Jamf Pro
- Enable GlobalProtect Network Extensions on macOS Big Sur Endpoints Using Jamf Pro
- Add a Configuration Profile for the GlobalProtect Enforcer by Using Jamf Pro 10.26.0
- Verify Configuration Profiles Deployed by Jamf Pro

- Remove System Extensions on macOS Monterey Endpoints Using Jamf Pro

If you want to use a single configuration profile to configure your managed macOS devices, you can Create a Single Configuration Profile for the GlobalProtect App for macOS.

For GlobalProtect app 6.0.3 and earlier users, you can Suppress Notifications on the GlobalProtect App for macOS Endpoints using a Qualified MDM Vendors such as Workspace ONE.

Enable GlobalProtect System Extensions on macOS Endpoints Using Jamf Pro

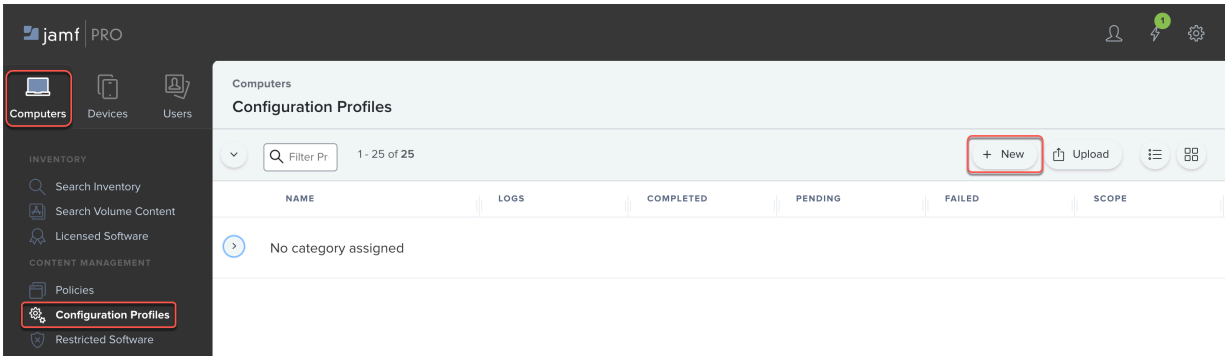
Where Can I Use This?	What Do I Need?
• Prisma Access • GlobalProtect Subscription	☐ Prisma Access Mobile Users license (for use with Prisma Access) ☐ PAN-OS 10.1 and later ☐ GlobalProtect Gateway license (for use with PAN-OS) ☐ GlobalProtect app for macOS 6.0.4 and later and 6.1 and later releases ☐ Endpoints on macOS 10.15.4 (Catalina) and later, macOS 11 (Big Sur), macOS 12 (Monterey), or macOS 13 (Ventura)

On the GlobalProtect app 6.0.4 and later and 6.1 releases running on macOS Catalina 10.15.4 and later or macOS Big Sur 11, you can use Jamf Pro to configure a GlobalProtect signed configuration profile to automatically load system extensions that are required for the split tunnel, enforce GlobalProtect connections for network access, and split DNS features.

For GlobalProtect app 6.0.3 and earlier users, you can Suppress Notifications on the GlobalProtect App for macOS Endpoints *using a* Qualified MDM Vendors *such as Workspace ONE.*

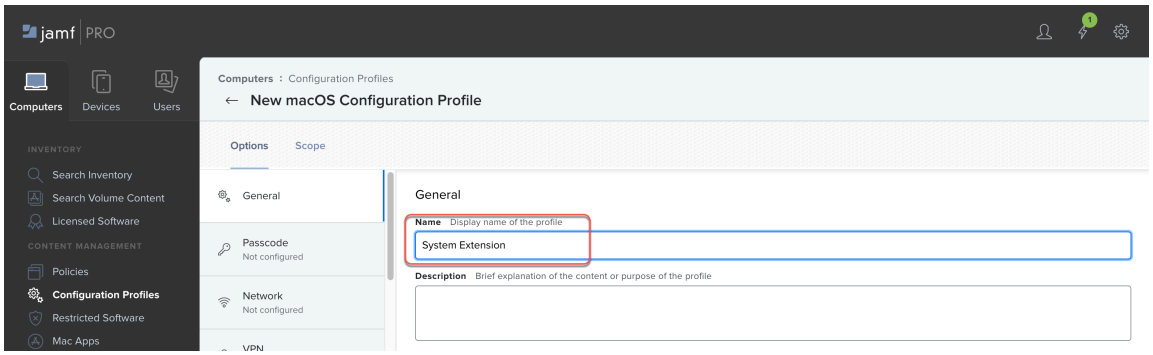
To enable the GlobalProtect system extension on macOS endpoints using Jamf Pro:

STEP 1 | In Jamf Pro, select **Computers** > **Configuration Profiles** > **New**.

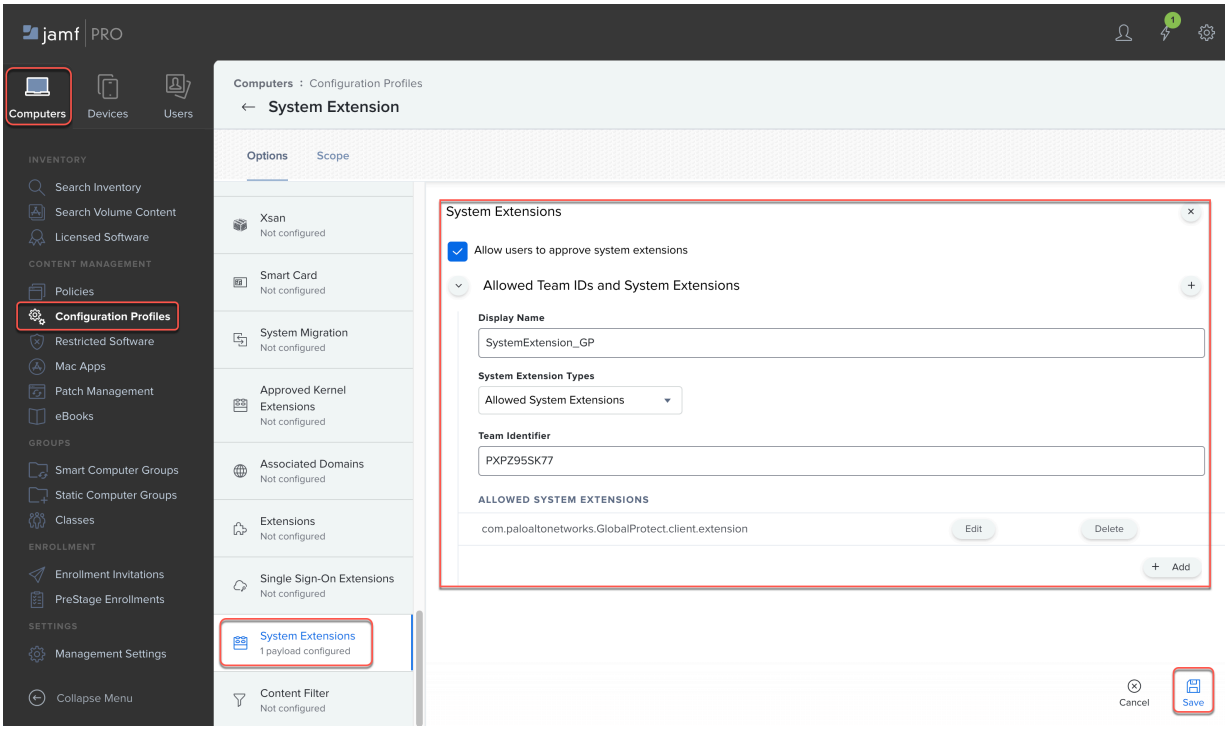


STEP 2 | Create a configuration profile to enable GlobalProtect system extensions.

1. Enter a **Display Name** for the configuration profile.



2. Select **System Extensions** > **Configure**.
3. (Optional) Enter a **Display Name**.
4. In **System Extension Types**, select **Allowed System Extensions**.
5. Enter the **Team Identifier** for the GlobalProtect app (**PXPZ95SK77**).
6. In the **ALLOWED SYSTEM EXTENSIONS** section, **Add** the Bundle Identifier for GlobalProtect system extensions (**`com.paloaltonetworks.GlobalProtect.client.extension`**) and **Save** the allowed system extension.
7. **Save** the configuration profile.



STEP 3 | Deploy the GlobalProtect app package and enable system extensions immediately after installation of the GlobalProtect app.

1. Create an settings file called `install_system_extensions.xml` with the following content:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://
www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<array>
            <dict>
                  <key>attributeSetting</key>
                  <integer>1</integer>
                  <key>choiceAttribute</key>
                  <string>selected</string>
                  <key>choiceIdentifier</key>
                  <string>third</string>
            </dict>
            <dict>
                  <key>attributeSetting</key>
                  <integer>1</integer>
                  <key>choiceAttribute</key>
                  <string>selected</string>
                  <key>choiceIdentifier</key>

 <string>com.paloaltonetworks.globalprotect.systemext.pkg</
string>
             </dict>
</array>
</plist>
```

2. Deploy the GlobalProtect app package by running the following command:

   `sudo installer -pkg GlobalProtect.pkg -applyChoiceChangesXML install_system_extensions.xml -target /`

Enable GlobalProtect Network Extensions on macOS Catalina Endpoints Using Jamf Pro

Where Can I Use This?	What Do I Need?
• Prisma Access • GlobalProtect Subscription	❑ Prisma Access Mobile Users license (for use with Prisma Access) ❑ PAN-OS 10.1 and later ❑ GlobalProtect Gateway license (for use with PAN-OS) ❑ GlobalProtect app for macOS 6.0.4 and later and 6.1 and later releases ❑ Endpoints on macOS 10.15.4 (Catalina) and later

On the GlobalProtect app 6.0.4 and later or 6.1 releases running on macOS Catalina 10.15.4 and later, you can use Jamf Pro to configure a GlobalProtect signed configuration profile. This profile will automatically allow network extensions that are required for the split tunnel, split DNS, and enforce GlobalProtect connections for network access features.

Upon installation or upgrade of the GlobalProtect app, the following messages for network extension notifications appear:

- For the split tunnel based on application and domain and split DNS features, the following pop-up is displayed:

- For the enforce GlobalProtect connections for network access feature, the following pop-up is displayed:

Palo Alto Networks provides the following configuration profiles that you can deploy to macOS endpoints using Jamf Pro to allow these network extensions automatically and suppress the pop-ups:

- `GlobalProtectSplitApp.mobileconfig` (**MD5 Hash** = d3d9940daadd91cb8b727db28026910c)
  - A configuration profile file specific to the GlobalProtect split-tunnel based on application feature
  - Suppresses network extension pop-ups related to VPN configurations
- `GlobalProtectSplitDomain.mobileconfig` (**MD5 Hash** = 235bda0a10eed7ca2b1efe7892439389)
  - A configuration profile file specific to the GlobalProtect split-tunnel based on domain feature
  - Suppresses network extension pop-ups related to VPN configurations
- `GlobalProtectSplitDNS.mobileconfig` (**MD5 Hash** = 020c721f6fed19cac436e0205eb0bedb)
  - A configuration profile file specific to the GlobalProtect split DNS feature
  - Suppresses network extension pop-up related to adding VPN configurations

- `GlobalProtectEnforcer.mobileconfig` (**MD5 Hash** = f1e1a501fc70b3a69e29fb5e722983ff)
  - A configuration profile file specific to the enforce GlobalProtect connections for network access feature
  - Suppresses network extension pop-ups related to filtering network content

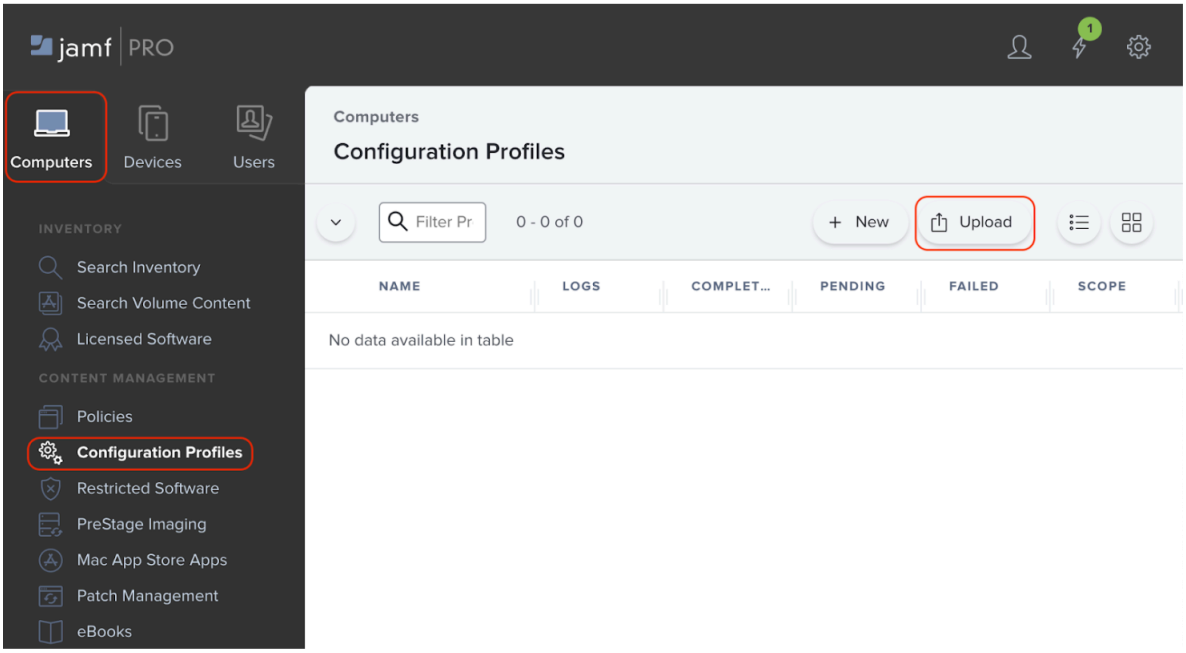
The mobileconfig for the enforcer feature works for all Jamf Pro versions except for Jamf Pro 10.26.0. If you are using Jamf Pro v10.26.0, you must Add a Configuration Profile for the GlobalProtect Enforcer by Using Jamf Pro 10.26.0 instead of uploading the enforcer mobileconfig.

You can download the configuration profile that applies to your GlobalProtect app configuration from this Knowledge Base article.

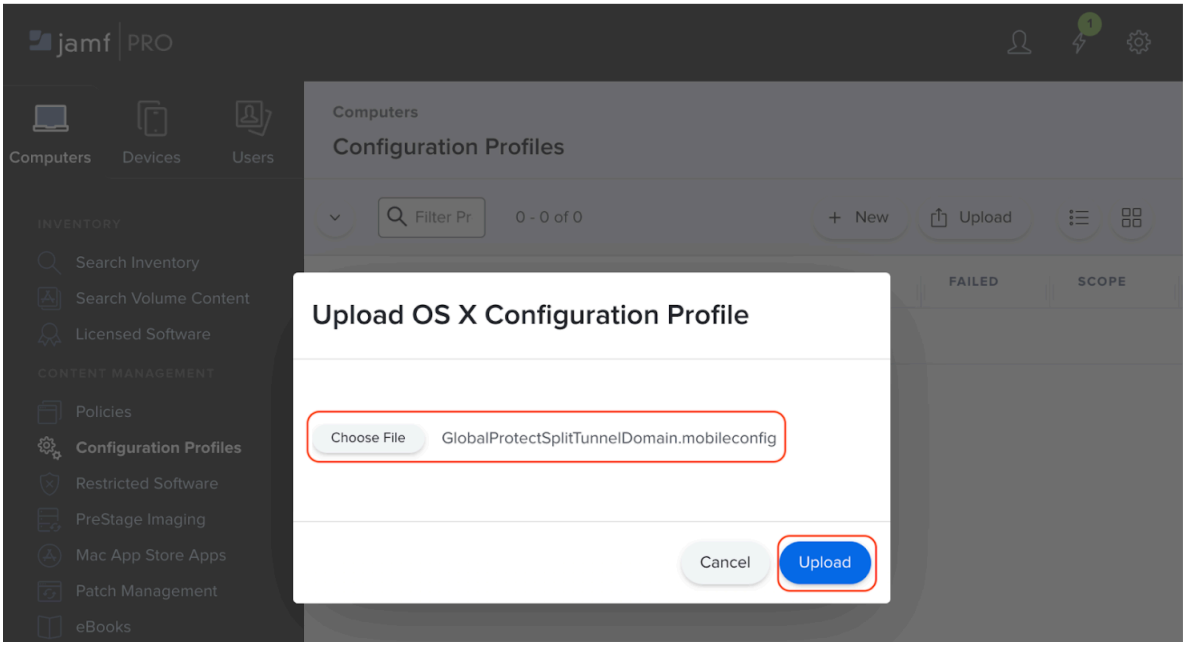
Before using the configuration profile files, ensure that the files are not corrupted by verifying that the hashes of the downloaded files match the hashes provided for the files as listed above. If the hash for a configuration profile does not match, download the file again.

Complete the following steps to upload and deploy the configuration profiles to Jamf Pro and deploy them to your macOS Catalina endpoints:

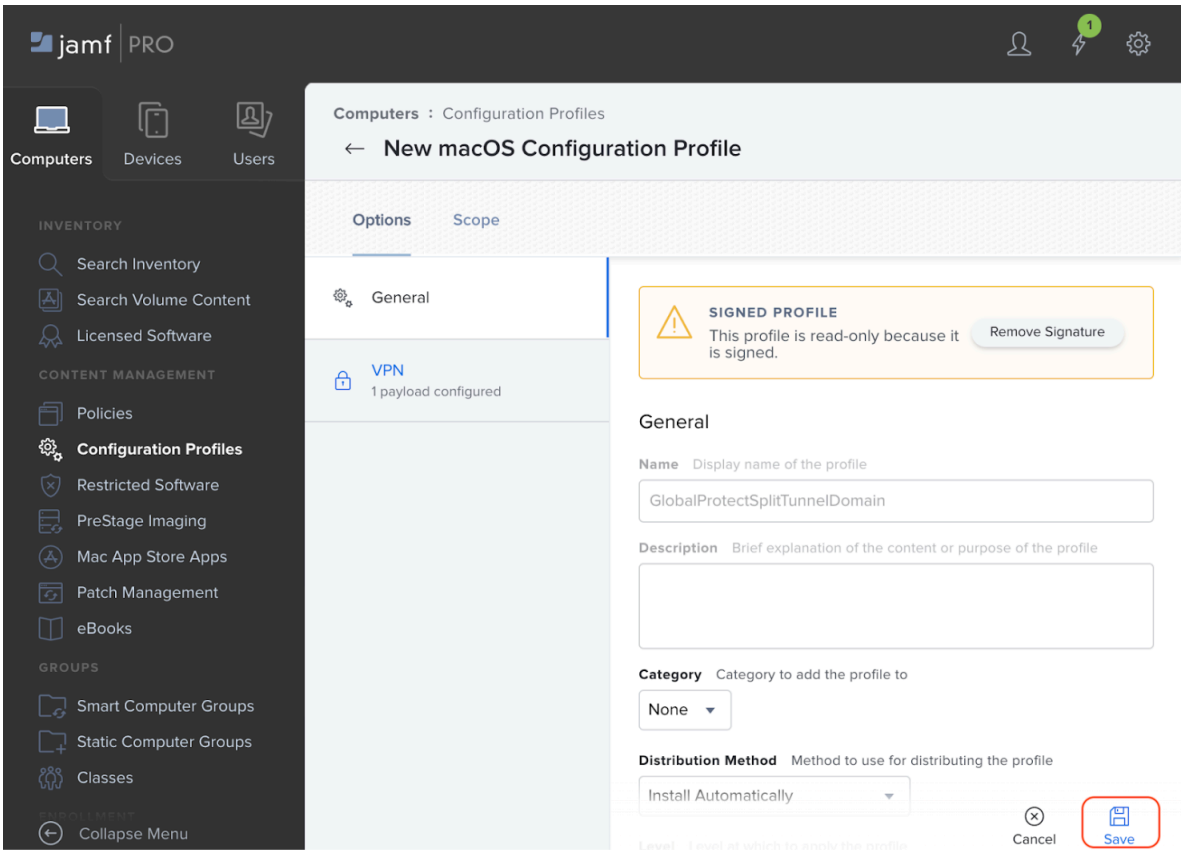
STEP 1 | From Jamf Pro, select **Computers** > **Configuration Profiles** > **Upload**.



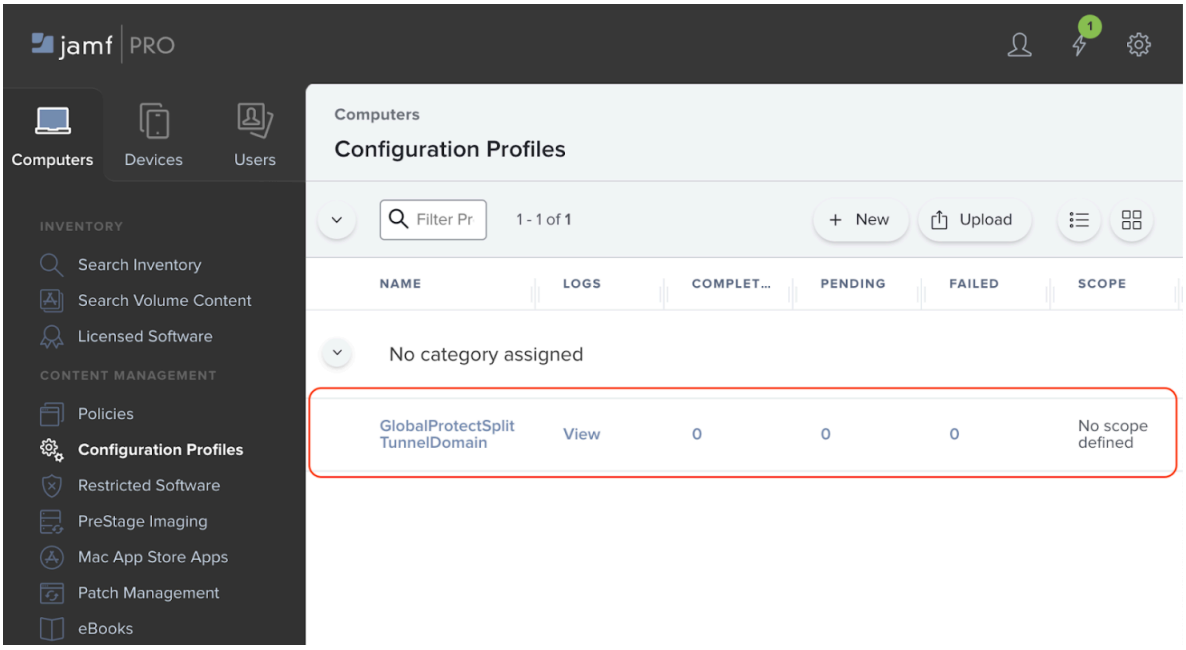
STEP 2 | Select the configuration file that you want to **Upload**.



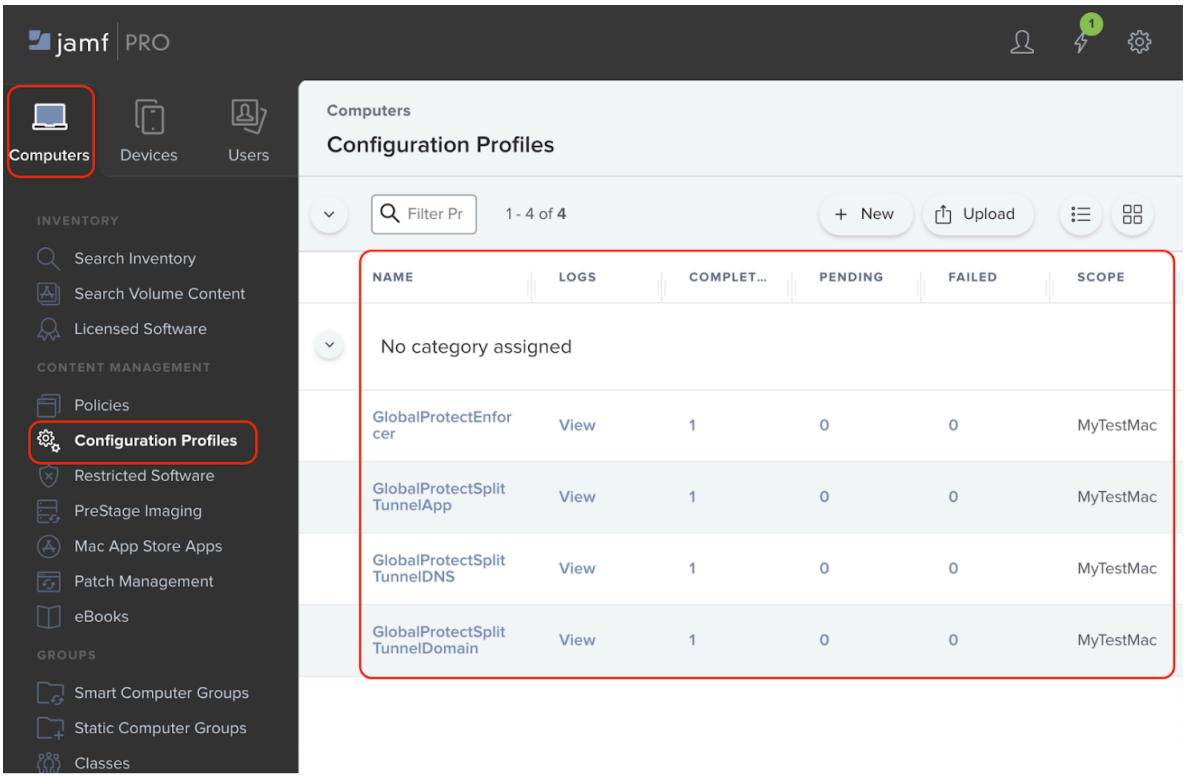
STEP 3 | After the configuration profile has been uploaded, **Save** it.



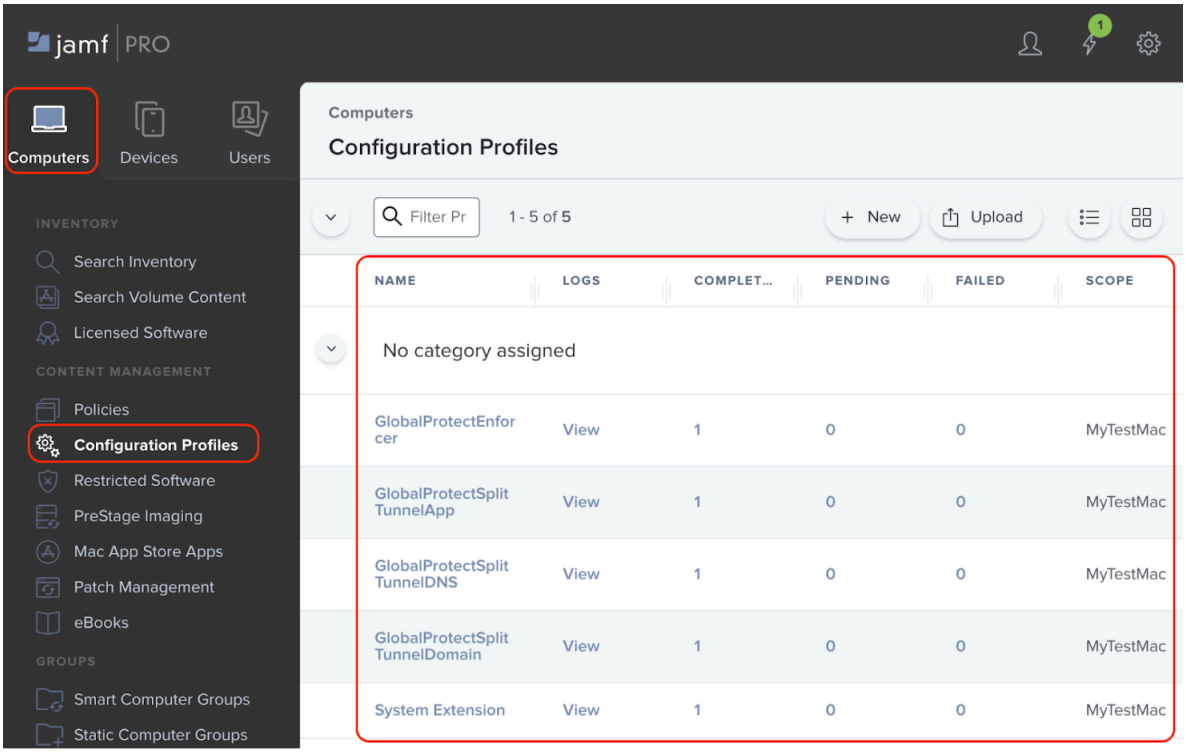
STEP 4 | Verify that the configuration profile has been uploaded successfully.



STEP 5 | Repeat steps 1 to 4 to upload any additional configuration profiles.



STEP 6 | Deploy one or more configuration profiles to your macOS Catalina endpoints.



Enable GlobalProtect Network Extensions on macOS Big Sur Endpoints Using Jamf Pro

Where Can I Use This?	What Do I Need?
• Prisma Access • GlobalProtect Subscription	❑ Prisma Access Mobile Users license (for use with Prisma Access) ❑ PAN-OS 10.1 and later ❑ GlobalProtect Gateway license (for use with PAN-OS) ❑ GlobalProtect app for macOS 6.0.4 and later and 6.1 and later releases ❑ Endpoints on macOS 11 (Big Sur), macOS 12 (Monterey), or macOS 13 (Ventura)

On the GlobalProtect app 6.0.4 and later or 6.1 releases running on macOS Big Sur 11, you can use Jamf Pro to configure a GlobalProtect signed configuration profile to automatically allow network extensions required for the split tunnel, split DNS, and enforce GlobalProtect connections for network access features.

After the installation or upgrade of the GlobalProtect app on macOS endpoints, a pop-up appears to prompt the user to allow network content filtering for GlobalProtect.

To allow this network extension automatically and suppress the pop-up, use the same procedure as Add a Configuration Profile for the GlobalProtect Enforcer by Using Jamf Pro 10.26.0.

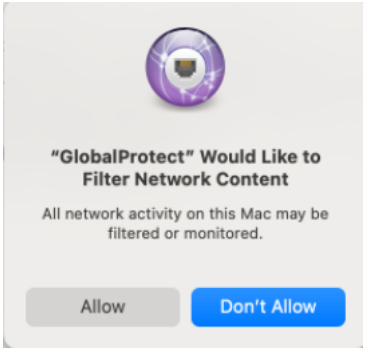
Add a Configuration Profile for the GlobalProtect Enforcer by Using Jamf Pro 10.26.0

Where Can I Use This?	What Do I Need?
• Prisma Access • GlobalProtect Subscription	❑ Prisma Access Mobile Users license (for use with Prisma Access) ❑ PAN-OS 10.1 and later ❑ GlobalProtect Gateway license (for use with PAN-OS) ❑ GlobalProtect app for macOS 6.0.4 and later and 6.1 and later releases ❑ Endpoints on macOS 10.15.4 (Catalina) and later, macOS 11 (Big Sur), macOS 12 (Monterey), or macOS 13 (Ventura)

If you are using Jamf Pro 10.26.0, and you configured the GlobalProtect app 6.0.4 and later or 6.1 releases with the enforce GlobalProtect connections for network access feature (enforcer) on macOS Catalina 10.15.4 and later endpoints, you must add a configuration profile to filter network content and deploy it to your macOS endpoints.

If you are using other versions of Jamf Pro, you can upload the enforcer configuration profile provided by Palo Alto Networks when you Enable GlobalProtect Network Extensions on macOS Catalina Endpoints Using Jamf Pro.

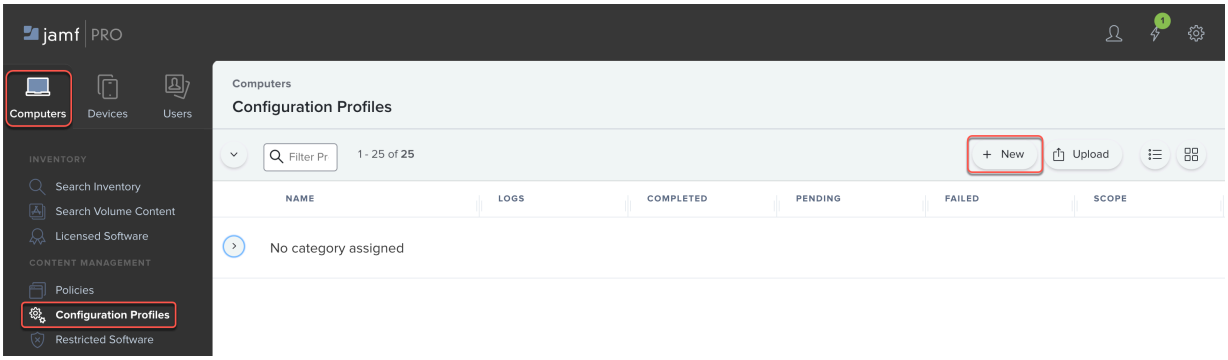
Upon installation or upgrade of the GlobalProtect app, the following notification message appears:



To allow this network extension and suppress the pop-up automatically, you must add a configuration profile to filter network content using Jamf Pro 10.26.0.

For deploying GlobalProtect apps to macOS Big Sur 11 endpoints, you can also use the following instructions on any version of Jamf Pro to allow network extensions and suppress notification messages automatically.

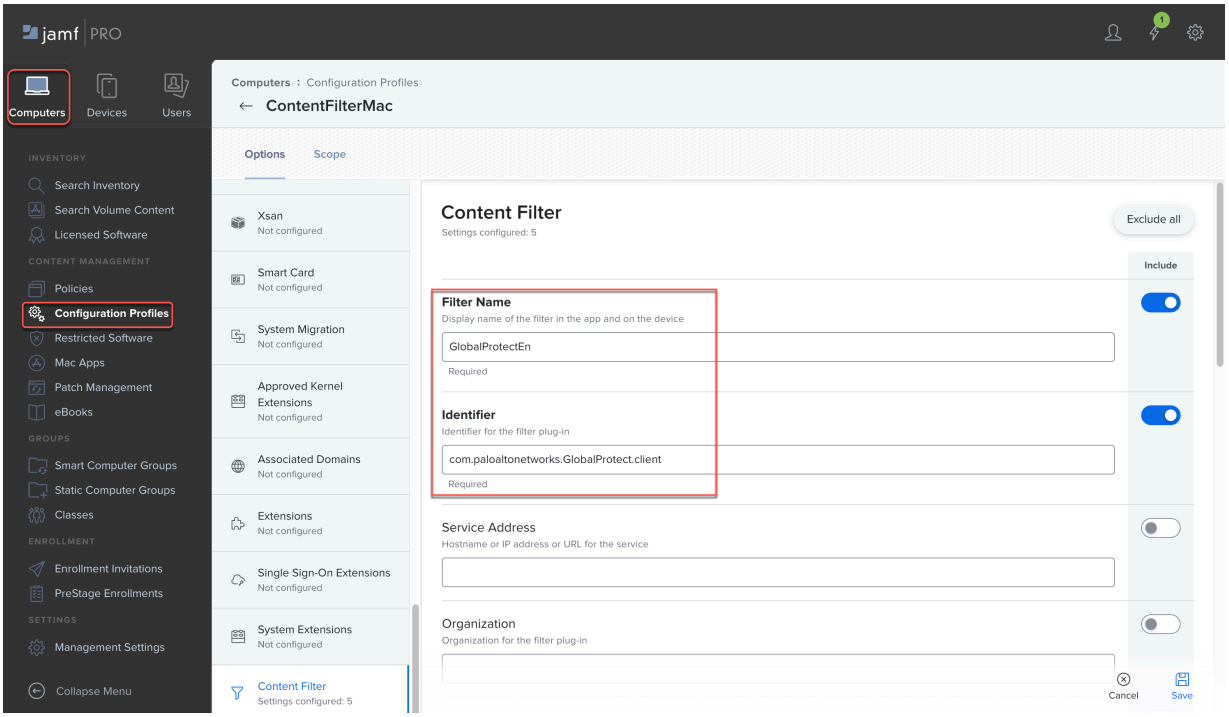
STEP 1 | In Jamf Pro, select **Computers** > **Configuration Profiles** > **New**.

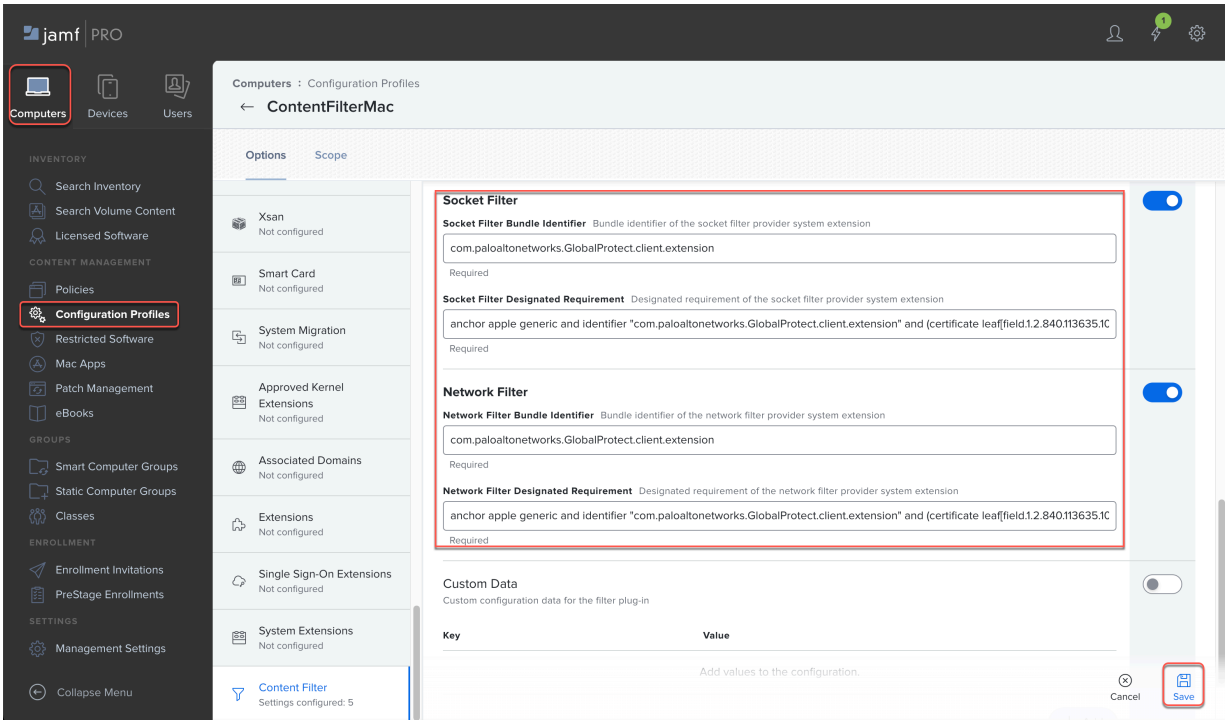


STEP 2 | Select **Content Filter** in the **Options** tab and configure the following values on the page:

- FilterName = **`GlobalProtectEn`**
- Identifier = **`com.paloaltonetworks.GlobalProtect.client`**
- Socket Filter Bundle Identifier = **`com.paloaltonetworks.GlobalProtect.client.extension`**
- Socket Filter Designated Requirement = **`anchor apple generic and identifier "com.paloaltonetworks.GlobalProtect.client.extension" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = PXPZ95SK77)`**
- Network Filter Bundle Identifier = **`com.paloaltonetworks.GlobalProtect.client.extension`**
- Network Filter Designated Requirement = **`anchor apple generic and identifier "com.paloaltonetworks.GlobalProtect.client.extension" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and`**


```
certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and
certificate leaf[subject.OU] = PXPZ95SK77)
```





STEP 3 | **Save** the configuration profile.

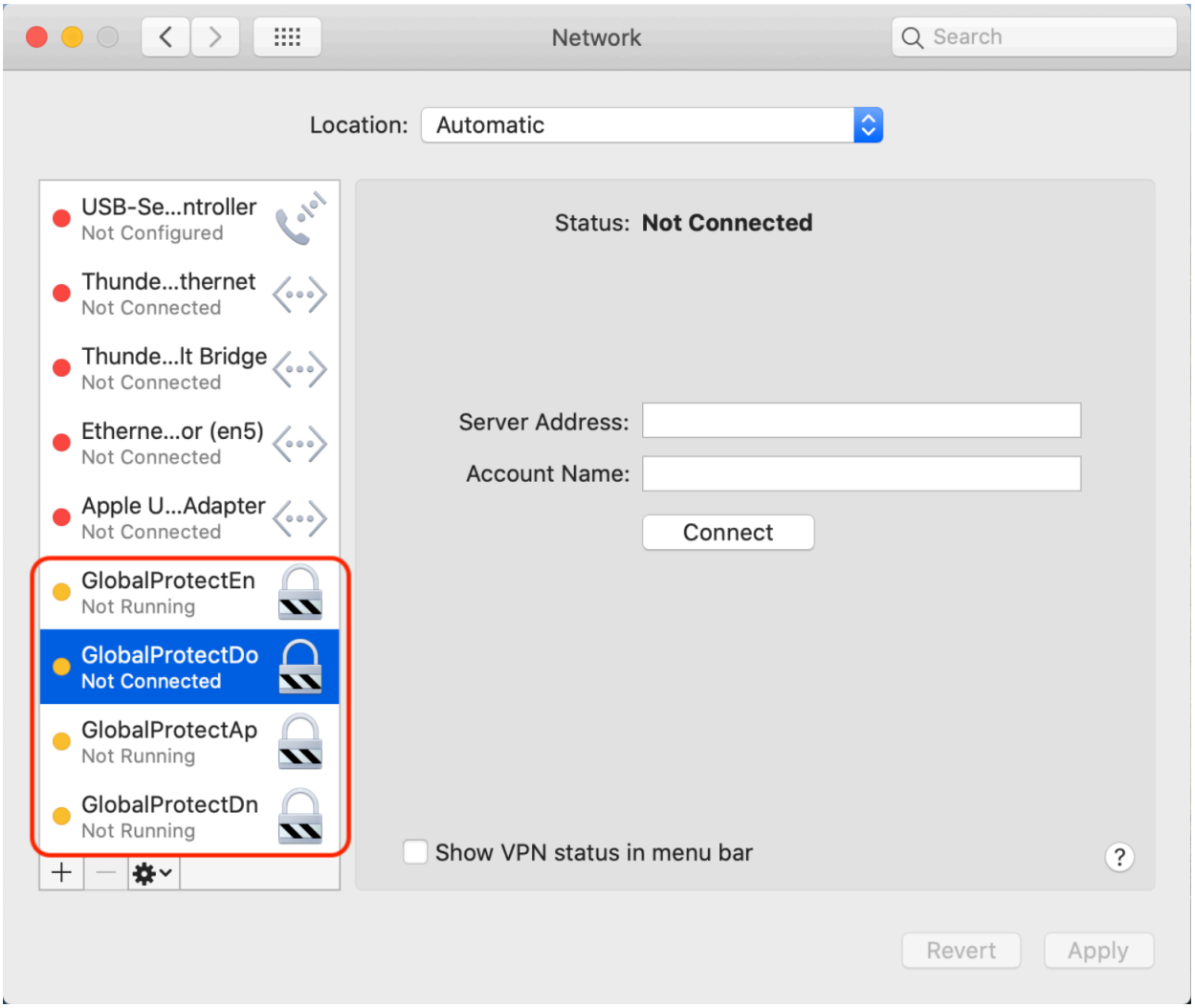
Verify Configuration Profiles Deployed by Jamf Pro

Where Can I Use This?	What Do I Need?
• Prisma Access • GlobalProtect Subscription	❑ Prisma Access Mobile Users license (for use with Prisma Access) ❑ PAN-OS 10.1 and later ❑ GlobalProtect Gateway license (for use with PAN-OS) ❑ GlobalProtect app for macOS 6.0.4 and later and 6.1 and later releases ❑ Endpoints on macOS 10.15.4 (Catalina) and later, macOS 11 (Big Sur), macOS 12 (Monterey), or macOS 13 (Ventura)

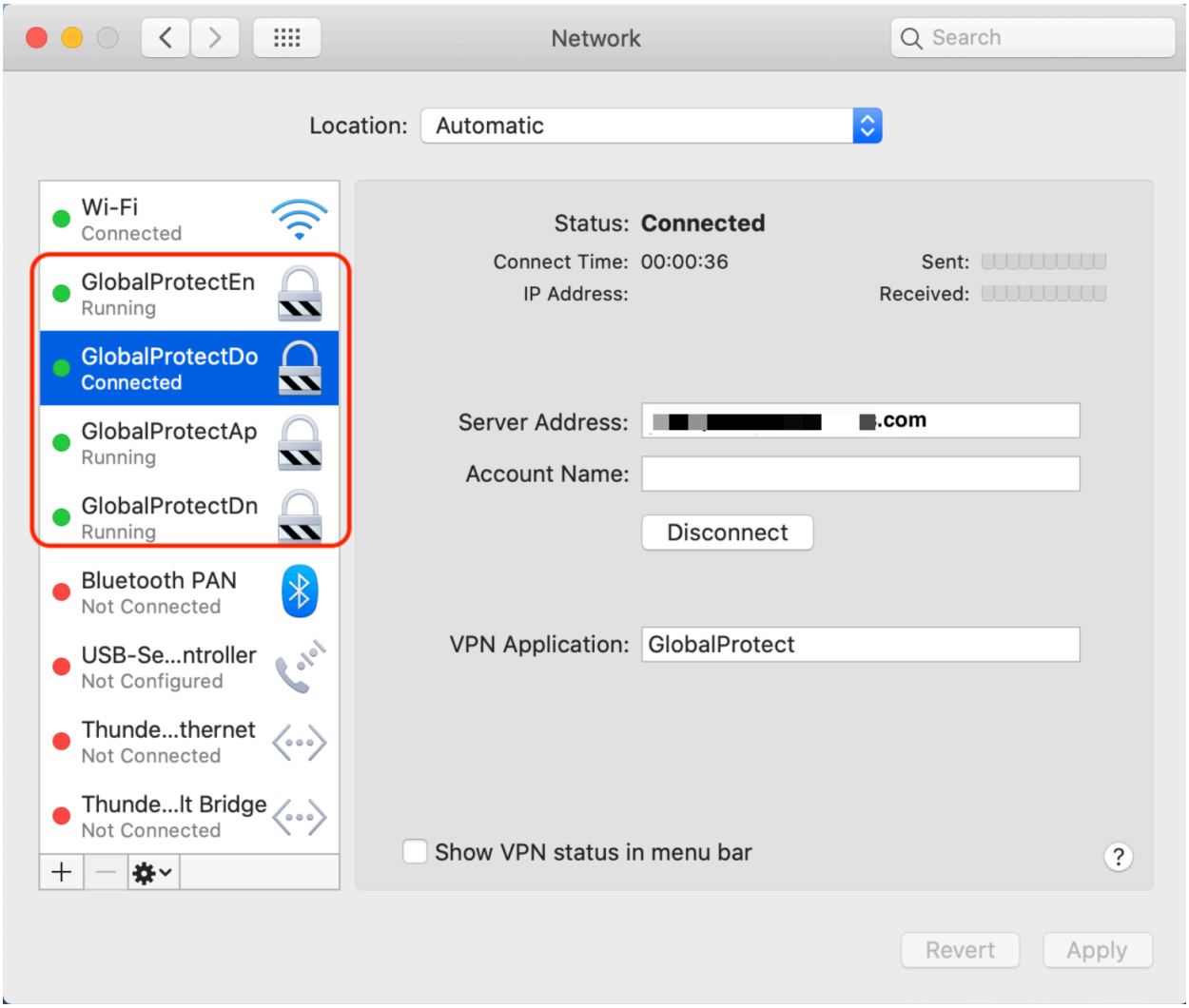
After you have deployed the configuration profiles using Jamf Pro, the following network interfaces are created on the macOS devices:

- `GloblaProtectDo` - Network interface for GlobalProtect Domain
- `GloblaProtectAp` - Network interface for GlobalProtect Application
- `GloblaProtectEn` - Network interface for GlobalProtect Enforcer
- `GloblaProtectDn` - Network interface for GlobalProtect DNS

STEP 1 | Verify that the GlobalProtect network interfaces have been deployed on macOS by selecting **System Preferences** > **Network**.



STEP 2 | After the GlobalProtect VPN tunnel is established, the network interfaces become active, connected, or running as shown below:



Remove System Extensions on macOS Monterey Endpoints Using Jamf Pro

Where Can I Use This?	What Do I Need?
• Prisma Access • GlobalProtect Subscription	☐ Prisma Access Mobile Users license (for use with Prisma Access) ☐ PAN-OS 10.1 and later ☐ GlobalProtect Gateway license (for use with PAN-OS) ☐ GlobalProtect app for macOS 6.0.4 and later and 6.1 and later releases ☐ Endpoints on macOS 10.15.4 (Catalina) and later, macOS 11 (Big Sur), macOS 12 (Monterey), or macOS 13 (Ventura)

In macOS Monterey 12, Apple introduced a feature in which system extensions can be removed using a configuration profile that is pushed from Jamf Pro.

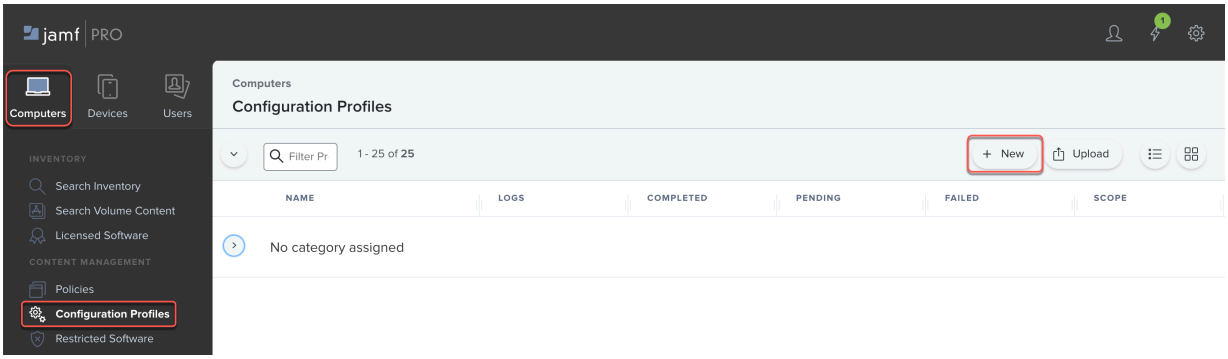
If you Uninstall the GlobalProtect Mobile App Using Jamf Pro the GlobalProtect 6.0.4 and later or 6.1 app from macOS Monterey 12.2.1 endpoints by running the **`/Applications/GlobalProtect.app/Contents/Resources/uninstall_gp.sh`** command inside a shell script, end users are not prompted to enter the administrator username and password to remove system extensions during the uninstallation of the GlobalProtect app.

If you uninstall the GlobalProtect app from macOS Monterey endpoints using the GlobalProtect app PKG file, end users ares still prompted by a pop-up to enter the administrator username and password to remove the system extension.

On macOS endpoints earlier than macOS Monterey, regardless of whether the GlobalProtect app is uninstalled using a command or PKG file, end users ares still prompted by a pop-up to enter the administrator username and password to remove the system extension.

To remove the system extension for the GlobalProtect app by pushing a configuration profile from Jamf Pro:

STEP 1 | Select **Computers** > **Configuration Profiles** > **New**.

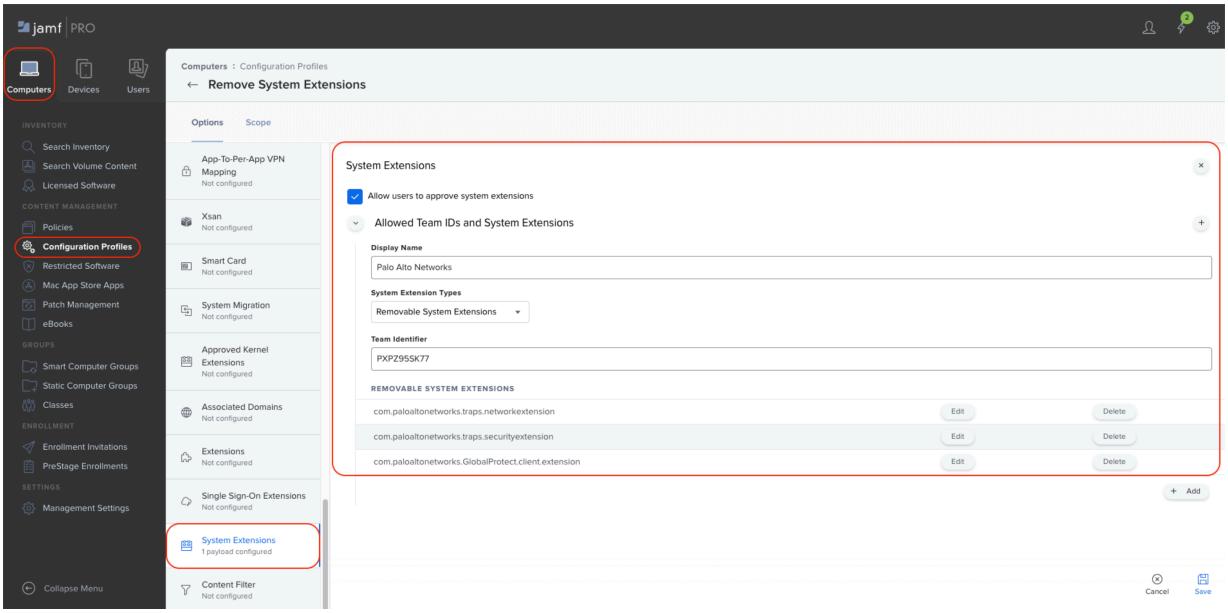


STEP 2 | Create a configuration profile to remove GlobalProtect system extensions.

1. Enter a **Display Name** for the configuration profile.
2. Select **System Extensions** > **Configure**.
3. (Optional) Enter a **Display Name**.
4. In **System Extension Types**, select **Removable System Extensions**.
5. Enter the **Team Identifier** for the GlobalProtect app (**PXPZ95SK77**).
6. In the **REMOVABLE SYSTEM EXTENSIONS** section, **Add** the Bundle Identifier for GlobalProtect system extensions

(**com.paloaltonetworks.GlobalProtect.client.extension**) and **Save** the removable system extension that you configured.

7. **Save** the configuration profile.



Uninstall the GlobalProtect Mobile App Using Jamf Pro

Where Can I Use This?	What Do I Need?
• Prisma Access • GlobalProtect Subscription	❑ Prisma Access Mobile Users license (for use with Prisma Access) ❑ PAN-OS 10.1 and later ❑ GlobalProtect Gateway license (for use with PAN-OS) ❑ GlobalProtect app for macOS 6.0.4 and later and 6.1 and later releases ❑ Endpoints on macOS 10.15.4 (Catalina) and later, macOS 11 (Big Sur), macOS 12 (Monterey), or macOS 13 (Ventura)

Starting with GlobalProtect app 6.0.4 and later and 6.1 releases, you can uninstall the app from macOS endpoints by configuring a policy that contains a script with the GlobalProtect app uninstall command. When the policy is triggered, the GlobaProtect app is uninstalled on macOS endpoints.

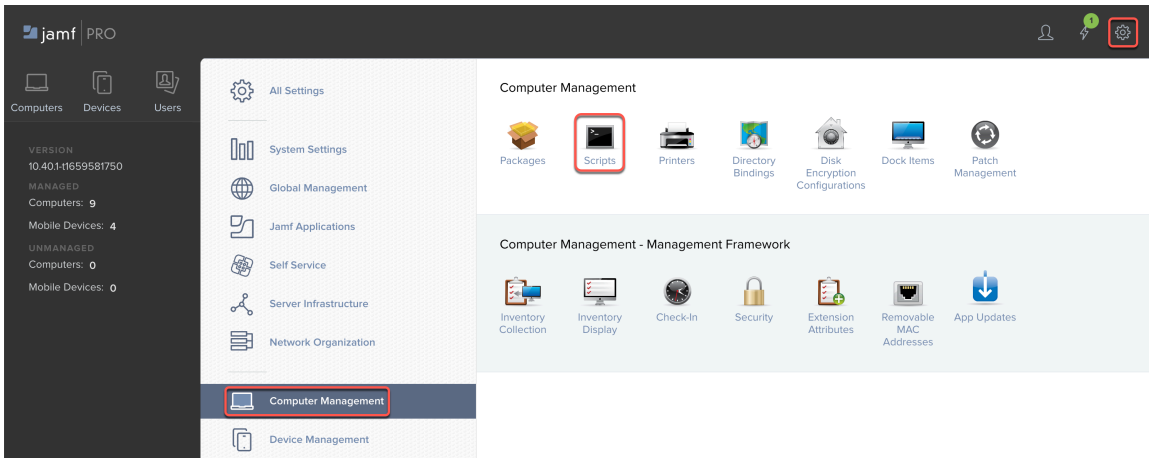
For macOS Monterey 12.2.1 endpoints, before you begin, Remove System Extensions on macOS Monterey Endpoints Using Jamf Pro. During the uninstallation, end users on macOS Monterey 12.2.1 endpoints are not prompted to remove the GlobalProtect system extension.

If you uninstall the GlobalProtect app from macOS Monterey endpoints using the GlobalProtect app PKG file, end users are prompted by a pop-up to enter the administrator username and password to remove the system extension.

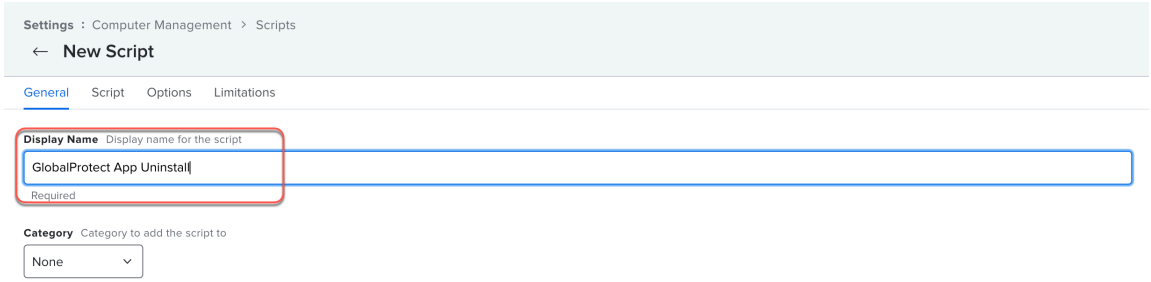
For macOS endpoints earlier than macOS Monterey, regardless of whether the GlobalProtect app is uninstalled using a command or PKG file, end users ares still prompted by a pop-up to enter the administrator username and password to remove the system extension.

STEP 1 | In Jamf Pro, create a script to uninstall the GlobalProtect app from macOS endpoints.

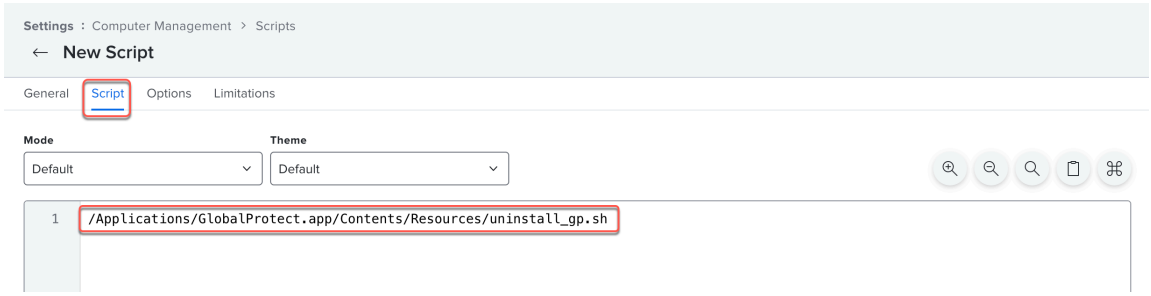
1. Select **Settings** > **Computer Management** > **Scripts**.



2. Click **New**.
3. Enter a **Display Name** for the script.



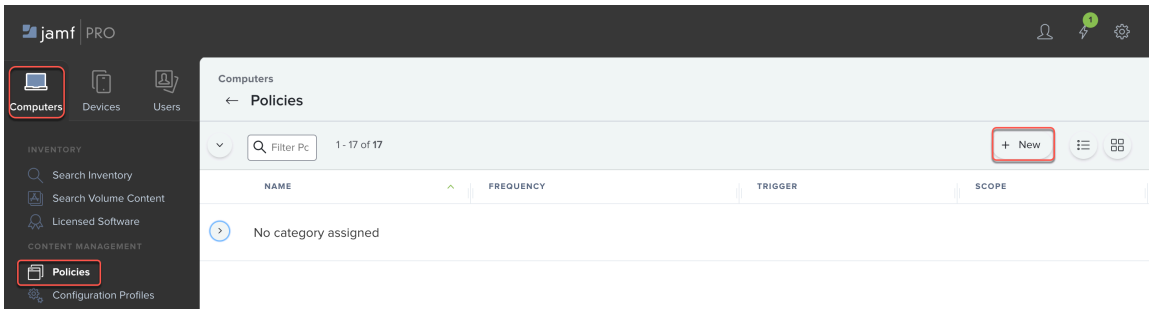
4. Select **Script** and enter the following command in the editor:
   `/Applications/GlobalProtect.app/Contents/Resources/uninstall_gp.sh`



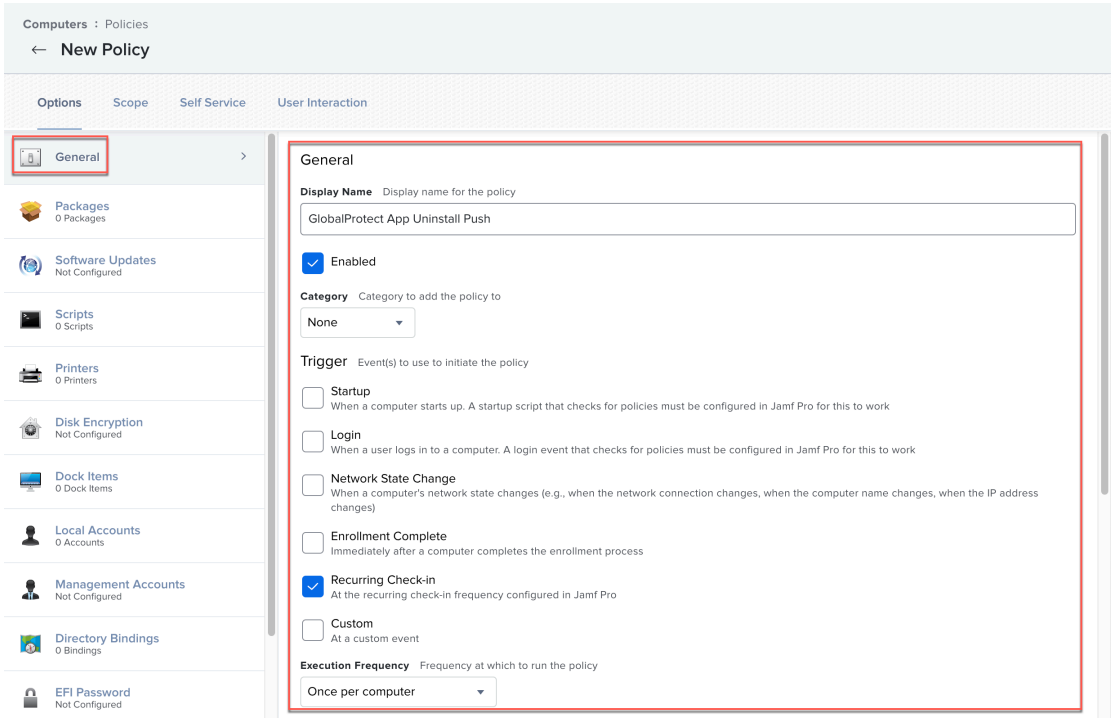
   The script will be run with superuser authority.
5. **Save** the script.

STEP 2 | Create a Jamf policy for running the uninstall script.

1. Select **Computers** > **Policies** > **New**.

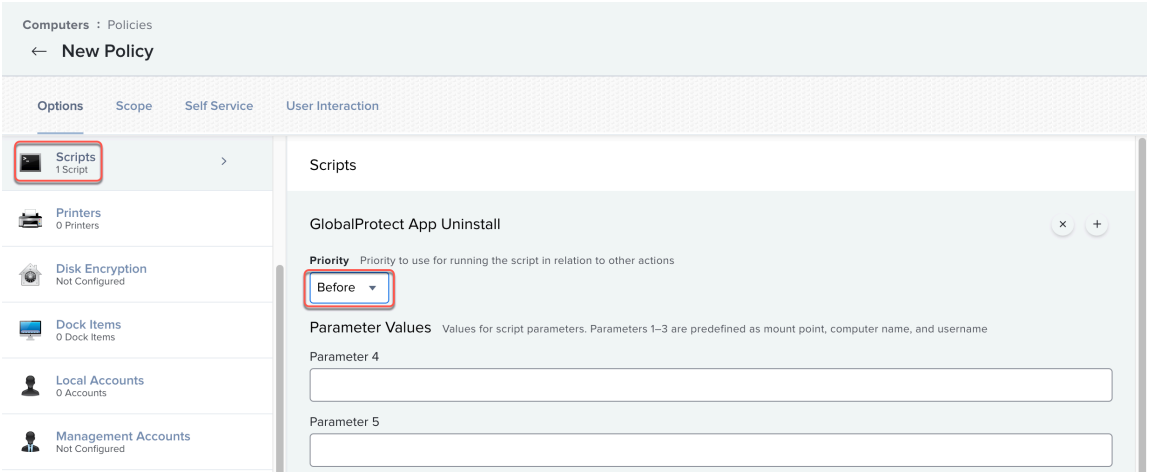


2. In the **General** payload, configure basic settings for the policy:
   - Enter a **Display Name** for the policy and **Enable** the policy.
   - (Optional) Select a **Category**.
   - Specify a **Trigger** that will run the policy.
   - Select an **Execution Frequency**, such as **Once per computer** and **Automatically re-run the policy on failure**.

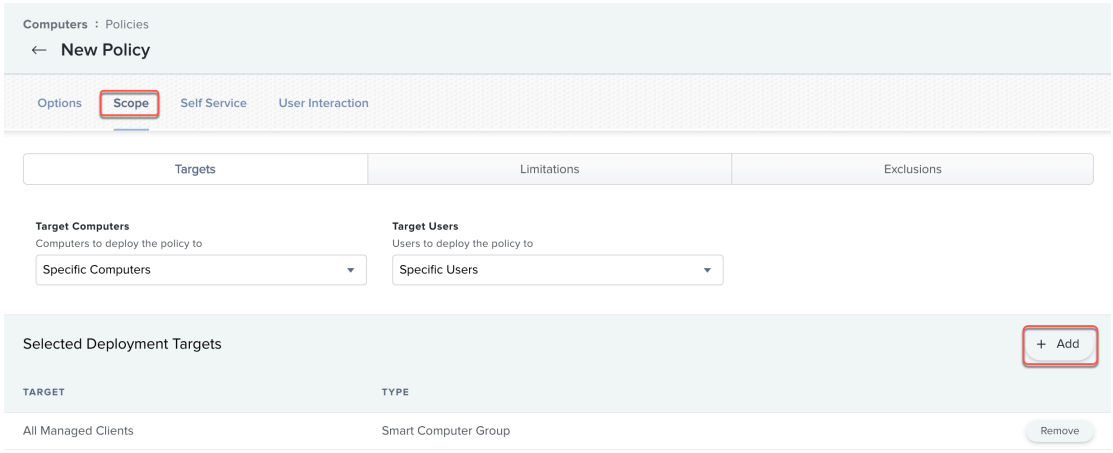


3. Configure the Scripts payload by selecting **Scripts** > **Configure**.

   Add the script that you created in Step 1 and select the **Priority** for running the script.



4. (Optional) If you created a Smart Group for your users, configure the scope of the policy to target that group.
   1. Select **Scope** and **Add** a deployment target.



   2. Click **Computer Groups** and **Add** the Smart Computer Group for your users.
   3. Click **Done**. The computers in the selected computer group will be targeted for uninstallation of the GlobalProtect app.
5. **Save** the policy.

   The next time macOS endpoints check in with Jamf Pro and meet the trigger in the General payload, the policy will run and uninstall the GlobalProtect app from the endpoints.

Suppress Notifications on the GlobalProtect App for macOS Endpoints

The GlobalProtect app on macOS supports two types of extensions—kernel (macOS device running macOS Catalina 10.15.3 or earlier) and system (macOS device running macOS Catalina 10.15.4 or later and GlobalProtect app 5.1.4 or later). If you have configured a Split Tunnel Traffic on GlobalProtect Gateways on the Configure a GlobalProtect Gateway or enforce GlobalProtect connections for network access (see Customize the GlobalProtect App), a notification message displays on the GlobalProtect app. The message prompts users to enable either the kernel extension or system extension in macOS that was blocked from loading when they access the GlobalProtect app that has these features enabled.

To allow GlobalProtect app 6.0.4 and later or 6.1 users to automatically load either the kernel extension or system extension without receiving a notification, you can Enable System and Network Extensions on macOS Endpoints Using Multiple Configuration Profiles.

To allow GlobalProtect app 6.0.3 or earlier users to automatically load either the kernel extension or system extension without receiving a notification, you can use a Qualified MDM Vendors such as Workspace ONE to create a policy for that extension. Refer to the following sections for information on how to suppress notifications on the GlobalProtect app 6.0.3 or earlier for macOS endpoints:

- Enable Kernel Extensions in the GlobalProtect App for macOS Endpoints
- Enable System Extensions in the GlobalProtect App for macOS Endpoints

Enable Kernel Extensions in the GlobalProtect App for macOS Endpoints

Starting with macOS 10.13, Apple introduced a software change that requires users to approve kernel extensions before they can use them.

While users can manually enable the kernel extension on macOS (**System Preferences** > **Security & Privacy** and selecting **Allow** for the kernel extension), you can use any Qualified MDM Vendors to create a policy and automatically approve the kernel extension. Apple Technical Note TN2450 describes the process.

The following workflow has been tested using Workspace ONE.

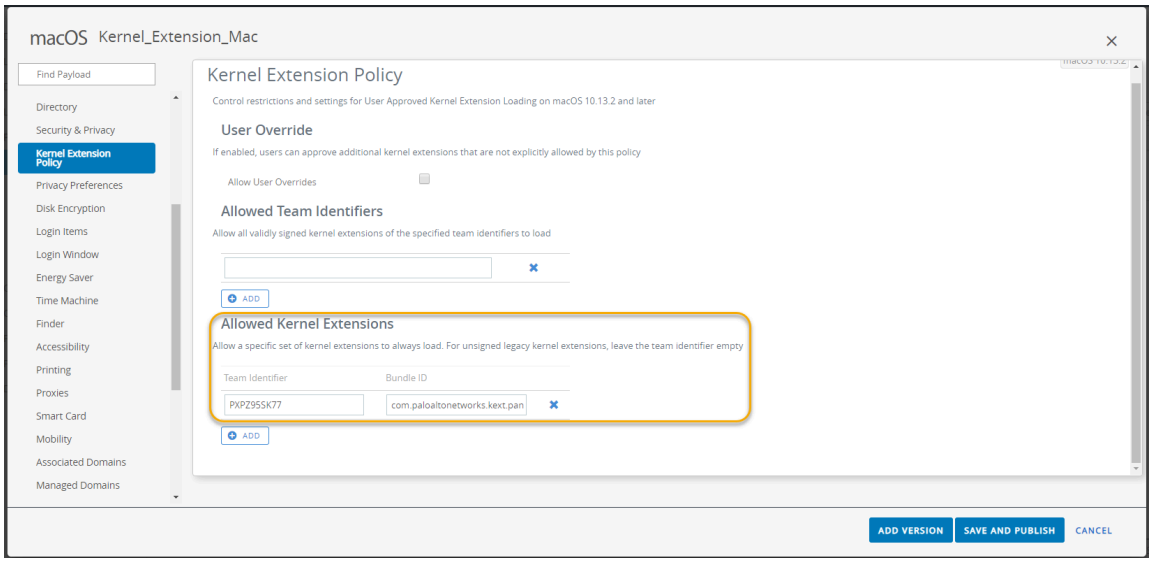
STEP 1 | Create a kernel extension policy.

1. Log in to Workspace ONE UEM as an administrator.
2. Select **Devices** > **Profiles & Resources** > **Profiles**, and then select **Add** > **Add Profile** from the drop-down.
3. In the **Add Profile** area, click **Apple macOS**, and then click the **Device Profile** icon.
4. In the **General** area, specify the name for the profile.

   You can also select an existing kernel extension profile (**Devices** > **Profiles & Resources** > **Profiles**) in the list.

STEP 2 | Add a kernel extension and distribute the relevant policy to macOS devices.

1. Select **Kernel Extension Policy**.
2. Enter the **Team Identifier** used by the GlobalProtect app (**PXPZ95SK77**).
3. Enter the **Bundle ID** (**com.paloaltonetworks.kext.pangpd**).



4. Click **Save and Publish** to save your changes.

Enable System Extensions in the GlobalProtect App for macOS Endpoints

Starting with macOS 10.15.4, Apple has limited the support of kernel extensions. The GlobalProtect app will use system extensions instead of kernel extensions. Users must approve system extensions before they can use them.

*In addition to enabling system extensions, you can enable network extensions in the GlobalProtect app to suppress the **Network Extensions Configuration** pop-up prompts that are used for the Split Tunnel and Enforce GlobalProtect Connections for Network Access features. You can use a mobile device management system (MDM) such as Jamf Pro to load the network extensions automatically without receiving the pop-up prompts.*

- *For GlobalProtect app 6.0.4 and later or 6.1 releases, you can* Enable System and Network Extensions on macOS Endpoints Using Multiple Configuration Profiles.
- *For GlobalProtect app 6.0.3 or earlier, refer to the knowledge base article at* https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAW8 *for information on how to enable system and network extensions using Jamf Pro.*

If you are not using Jamf Pro, use the following steps to configure a profile to approve the system extension automatically using Workspace ONE. While this configuration has been tested with Workspace ONE, you can use any Qualified MDM Vendors to create and implement this profile.

When you are using system extensions and need to switch to Enable Kernel Extensions in the GlobalProtect App for macOS Endpoints, *see* Deploy App Settings in the macOS Plist *for details.*

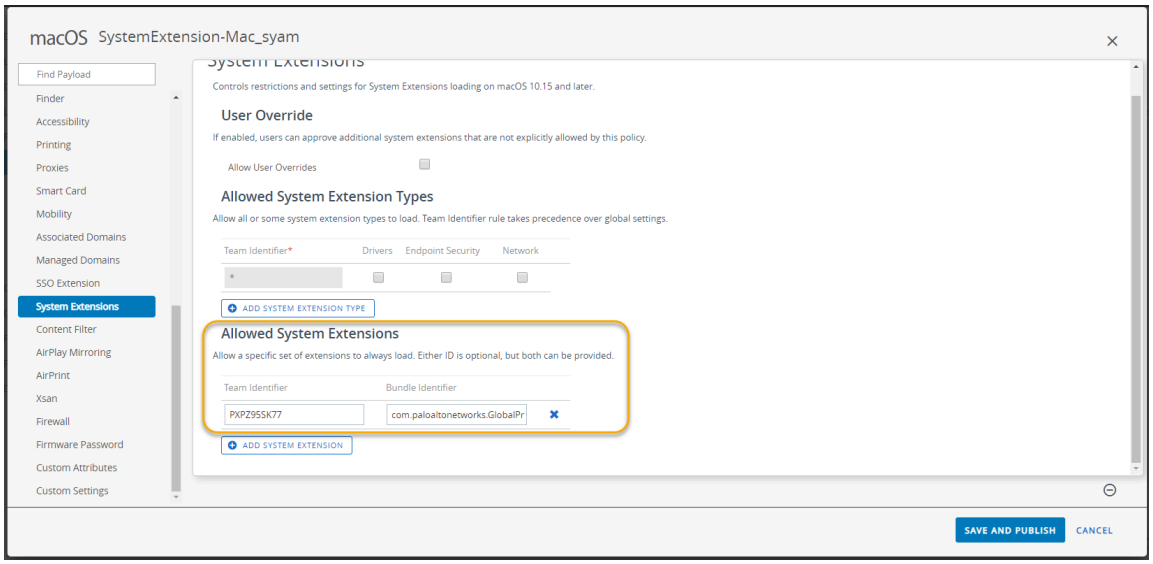
STEP 1 | Create a system extension profile.

1. Log in to Workspace ONE UEM as an administrator.
2. Select **Devices** > **Profiles & Resources** > **Profiles**, and then select **Add** > **Add Profile** from the drop-down.
3. In the **Add Profile** area, click **Apple macOS**, and then click the **Device Profile** icon.
4. In the **General** area, specify the name for the profile.

   You can also select an existing system extension profile (**Devices** > **Profiles & Resources** > **Profiles**) in the list.

STEP 2 | Add a system extension.

1. Select **System Extensions**.
2. Enter the **Team Identifier** used by the GlobalProtect app (**PXPZ95SK77**).
3. Enter the **Bundle Identifier** (**com.paloaltonetworks.GlobalProtect.client.extension**)



4. Click **Save and Publish** to save your changes.

Manage the GlobalProtect App Using Other Third-Party MDMs

If you are not using a Qualified MDM Vendors, you can use other third-party MDM systems to deploy and manage the GlobalProtect app:

- Configure the GlobalProtect App for iOS
  - Example: GlobalProtect iOS App Device-Level VPN Configuration
  - Example: GlobalProtect iOS App App-Level VPN Configuration
- Configure the GlobalProtect App for Android
  - Example: Set VPN Configuration
  - Example: Remove VPN Configuration

Configure the GlobalProtect App for iOS

While a third-party MDM system allows you to push configuration settings that allow access to your corporate resources and provides a mechanism for enforcing endpoint restrictions, it does not secure the connection between the mobile endpoint and the services to which it connects. To enable the app to establish secure connections, you must enable VPN support on the endpoint.

The following table describes typical settings that you can configure using your third-party MDM system:

Setting	Description	Value
Connection Type	Type of connection enabled by the policy.	**Custom SSL**
Identifier	Identifier for the custom SSL VPN in reverse DNS format.	**com.paloaltonetworks.globalprotect.v**
Server	Host name or IP address of the GlobalProtect portal.	**<hostname or IP address>** For example: **gp.paloaltonetworks.com**
Account	User account for authenticating the connection.	**<username>**
User Authentication	Authentication type for the connection.	**Certificate | Password**
Credential	(Certificate User Authentication only) Credential for authenticating the connection.	**<credential>** For example: **clientcredial.p12**

Setting	Description	Value
Enable VPN On Demand	(Optional) Domain and hostname that establish the connection and the on-demand action: • Always establish a connection • Never establish a connection • Establish a connection if needed	**<domain and hostname and the on-demand action>** For example: `gp.acme.com; Never establish`

Example: GlobalProtect iOS App Device-Level VPN Configuration

The following example shows the XML configuration containing a VPN payload that you can use to verify the device-level VPN configuration of the GlobalProtect app for iOS.

```
<?xml version="1.0"
encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://
www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>PayloadContent</key>
<array>
<dict>
<key>PayloadDescription</key>
<string>Configures VPN settings, including authentication.</string>
<key>PayloadDisplayName</key>
<string>VPN (Sample Device Level VPN)</string>
<key>PayloadIdentifier</key>
<string>Sample Device Level VPN.vpn</string>
<key>PayloadOrganization</key>
<string>Palo Alto Networks</string>
<key>PayloadType</key>
<string>com.apple.vpn.managed</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>PayloadUUID</key>
<string>5436fc94-205f-7c59-0000-011d</string>
<key>UserDefinedName</key>
<string>Sample Device Level VPN</string>
<key>Proxies</key>
<dict/>
<key>VPNType</key>
<string>VPN</string>
<key>VPNSubType</key>
<string>com.paloaltonetworks.GlobalProtect.vpnplugin</string>
<key>IPv4</key>
<dict>
<key>OverridePrimary</key>
```



```
<integer>0</integer>
</dict>
<key>VPN</key>
<dict>
<key>RemoteAddress</key>
<string>cademogp.paloaltonetworks.com</string>
<key>AuthName</key>
<string></string>
<key>DisconnectOnIdle</key>
<integer>0</integer>
<key>OnDemandEnabled</key>
<integer>1</integer>
<key>OnDemandRules</key>
<array>
<dict>
<key>Action</key>
<string>Connect</string>
</dict>
</array>
<key>AuthenticationMethod</key>
<string>Password</string>
</dict>
<key>VendorConfig</key>
<dict>
<key>AllowPortalProfile</key>
<integer>0</integer>
<key>FromAspen</key>
<integer>1</integer>
</dict>
</dict>
</array>
<key>PayloadDisplayName</key>
<string>Sample Device Level VPN</string>
<key>PayloadOrganization</key>
<string>Palo Alto Networks</string>
<key>PayloadDescription</key>
<string>Profile Description</string>
<key>PayloadIdentifier</key>
<string>Sample Device Level VPN</string>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>PayloadUUID</key>
<string>5436fc94-205f-7c59-0000-011c</string>
<key>PayloadRemovalDisallowed</key>
<false/>
</dict>
</plist>
```

Example: GlobalProtect iOS App App-Level VPN Configuration

The following example shows the XML configuration containing a VPN payload that you can use to verify the app-level VPN configuration of the GlobalProtect app for iOS.


```
<?xml version="1.0"
encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://
www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>PayloadContent</key>
<array>
<dict>
<key>PayloadDescription</key>
<string>Configures VPN settings, including authentication.</string>
<key>PayloadDisplayName</key>
<string>VPN (Sample App Level VPN)</string>
<key>PayloadIdentifier</key>
<string>Sample App Level VPN.vpn</string>
<key>PayloadOrganization</key>
<string>Palo Alto Networks</string>
<key>PayloadType</key>
<string>com.apple.vpn.managed.applayer</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>VPNUUID</key>
<string>cGFuU2FtcGxlIEFwcCBMZXZlbCBWUE52cG5TYW1wbGUgQXBwIExldmVsIFZQTg==</
string>
<key>SafariDomains</key>
<array>
<string>*.paloaltonetworks.com</string>
</array>
<key>PayloadUUID</key>
<string>54370008-205f-7c59-0000-01a1</string>
<key>UserDefinedName</key>
<string>Sample App Level VPN</string>
<key>Proxies</key>
<dict/>
<key>VPNType</key>
<string>VPN</string>
<key>VPNSubType</key>
<string>com.paloaltonetworks.GlobalProtect.vpnplugin</string>
<key>IPv4</key>
<dict>
<key>OverridePrimary</key>
<integer>0</integer>
</dict>
<key>VPN</key>
<dict>
<key>RemoteAddress</key>
<string>cademogp.paloaltonetworks.com</string>
<key>AuthName</key>
<string></string>
<key>OnDemandMatchAppEnabled</key>
<integer>1</integer>
<key>OnDemandEnabled</key>
<integer>1</integer>
<key>DisconnectOnIdle</key>
<integer>0</integer>
<key>AuthenticationMethod</key>
```



```
<string>Password</string>
</dict>
<key>VendorConfig</key>
<dict>
<key>OnlyAppLevel</key>
<integer>1</integer>
<key>AllowPortalProfile</key>
<integer>0</integer>
<key>FromAspen</key>
<integer>1</integer>
</dict>
</dict>
</array>
<key>PayloadDisplayName</key>
<string>Sample App Level VPN</string>
<key>PayloadOrganization</key>
<string>Palo Alto Networks</string>
<key>PayloadDescription</key>
<string>Profile Description</string>
<key>PayloadIdentifier</key>
<string>Sample App Level VPN</string>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>PayloadUUID</key>
<string>5436fc94-205f-7c59-0000-011c</string>
<key>PayloadRemovalDisallowed</key>
<false/>
</dict>
</plist>
```

Configure the GlobalProtect App for Android

You can deploy and configure the GlobalProtect app on Android For Work endpoints from any third-party mobile device management (MDM) system supporting Android For Work App data restrictions.

On Android endpoints, traffic is routed through the VPN tunnel according to the access routes configured on the GlobalProtect gateway. From your third-party MDM that manages Android for Work endpoints, you can further refine the traffic that is routed though the VPN tunnel.

In an environment where the endpoint is corporately owned, the endpoint owner manages the entire endpoint, including all the apps installed on that endpoint. By default, all installed apps can send traffic through the VPN tunnel according to the access routes defined on the gateway.

In a bring-your-own-device (BYOD) environment, the endpoint is not corporately owned and uses a Work Profile to separate business and personal apps. By default, only managed apps in the Work Profile can send traffic through the VPN tunnel according to the access routes defined on the gateway. Apps installed on the personal side of the endpoint cannot send traffic through the VPN tunnel set by the managed GlobalProtect app that is installed in the Work Profile.

To route traffic from an even smaller set of apps, you can enable Per-App VPN so that GlobalProtect only routes traffic from specific managed apps. For Per-App VPN, you can allow list or block list specific managed apps from having their traffic routed through the VPN tunnel.

Endpoints running Android will not automatically launch the GlobalProtect app when the user launches an application in the allow list. However, endpoints running iOS will automatically launch the GlobalProtect app and establish the VPN tunnel when the user launches an application from the allow list.

As part of the VPN configuration, you can also specify how the user connects to the VPN. When you configure the connect method as **user-logon**, the GlobalProtect app establishes a connection automatically. When you configure the connect method as **on-demand**, users must initiate a connection manually.

The VPN connect method defined in the MDM takes precedence over the connect method defined in the GlobalProtect portal configuration.

Removing the VPN configuration automatically restores the GlobalProtect app to its original configuration settings.

To configure the GlobalProtect app for Android, configure the following Android App Restrictions.

Key	Value Type	Description	Example
portal	String	IP address or fully qualified domain name (FQDN) of the portal.	**10.1.8.190**
username	String	Username for the user.	**john**
password	String	Password for the user.	**Passwd!234**
mobile_id	String	Mobile ID as configured in third-party MDM service to uniquely identify a mobile device. GlobalProtect uses this mobile ID to retrieve device information.	**5188a8193be43f42d332dde5cb2c941e**
certificate	String (in Base64)	Client certificate (cert) used to authenticate the agent and the portal.	**DAFDSaweEWQ23wDSAFD….**
client_certificate_passphrase	String	Key associated with the client certificate.	**PA$$W0RD$123**
app_list	String	Configuration for Per-App VPN. Begin the string with either the **allowlist** keyword or **blocklist** keyword followed by a colon, and follow it with an array of app names separated	**allowlist | blocklist: com.google.calendar; com.android.email; com.android.chrome**

Key	Value Type	Description	Example
		by semicolons. The allow list specifies the apps that will use the VPN tunnel for network communication. The network traffic for any other app that is not in the allow list or expressly listed in the block list will not go through the VPN tunnel.	*The keywords **allow list** and **block list** changed to **allowlist** and **blocklist** in PAN-OS 10.1. You will need to change the setting on your MDM when you upgrade to 10.1.*
connect_method	String	Either user-logon to automatically connect the user to the GlobalProtect portal using their windows credentials or on-demand to manually connect the user to the gateway.	**user-logon | on-demand**
remove_vpn_config_via_restriction	Boolean	Permanently remove all GlobalProtect VPN configuration information.	**true | false**

Example: Set VPN Configuration

```
private static String RESTRICTION_PORTAL
= "portal";
private static String RESTRICTION_USERNAME = "username";
private static String RESTRICTION_PASSWORD = "password";
private static String RESTRICTION_CONNECT_METHOD = "connect_method";
private static String RESTRICTION_CLIENT_CERTIFICATE
= "client_certificate";
private static String RESTRICTION_CLIENT_CERTIFICATE_PASSPHRASE
= "client_certificate_passphrase";
private static String RESTRICTION_APP_LIST = "app_list";
private static String RESTRICTION_REMOVE_CONFIG =
 "remove_vpn_config_via_restriction";

Bundle config = new Bundle();
config.putString(RESTRICTION_PORTAL, "192.168.1.1");
config.putString(RESTRICTION_USERNAME, "john");
config.putString(RESTRICTION_PASSWORD, "Passwd!234");
config.putString(RESTRICTION_CONNECT_METHOD, "user-logon");
config.putString(RESTRICTION_CLIENT_CERTIFICATE,
 "DAFDSaweEWQ23wDSAFD….");
```



```
config.putString(RESTRICTION_CLIENT_CERTIFICATE_PASSPHRASE,
"PA$$W0RD$123");
config.putString(RESTRICTION_APP_LIST, "allow
 list:com.android.chrome;com.android.calendar");

DevicePolicyManager dpm = (DevicePolicyManager)
getSystemService(Context.DEVICE_POLICY_SERVICE);
dpm.setApplicationRestrictions(EnforcerDeviceAdminReceiver.getComponentName(thi
"com.paloaltonetworks.globalprotect", config);
```

Example: Remove VPN Configuration

```
Bundle config = new Bundle();
config.putBoolean(RESTRICTION_REMOVE_CONFIG, true );
DevicePolicyManager dpm = (DevicePolicyManager)
getSystemService(Context.DEVICE_POLICY_SERVICE);
dpm.setApplicationRestrictions(EnforcerDeviceAdminReceiver.
getComponentName(this),"com.paloaltonetworks.globalprotect",
config);
```


GlobalProtect for IoT Devices

With GlobalProtect for IoT, you can secure traffic from and extend security policy enforcement to your IoT devices. After you set up GlobalProtect for IoT, the GlobalProtect app authenticates with the GlobalProtect portal or gateways using client certificates and optionally a username and password. Upon successful authentication, the GlobalProtect app establishes an IPSec tunnel. In the event that a connection using IPSec is unsuccessful, you can configure the GlobalProtect app to fall back to an SSL tunnel. Refer to the Palo Alto Networks Compatibility Matrix for a list of features supported by OS for IoT devices.

- GlobalProtect for IoT Requirements
- Configure the GlobalProtect Portals and Gateways for IoT Devices
- Install GlobalProtect for IoT on Android
- Install GlobalProtect for IoT on Raspbian
- Install GlobalProtect for IoT on Ubuntu
- Install GlobalProtect for IoT on Windows

GlobalProtect for IoT Requirements

GlobalProtect for IoT has the following requirements:

- Either Prisma Access or GlobalProtect subscription
- The firewall is running PAN-OS 10.1 (upgrade now)
- One of the following operating systems:
  - Android
  - Raspbian
  - Ubuntu
  - Windows IoT Enterprise
- 128MB RAM
- 4GB of storage
- x86 and ARMv7 or ARMv5 processor
- Installation using snap app packages from the CLI or WebDM

Configure the GlobalProtect Portals and Gateways for IoT Devices

STEP 1 | Review the GlobalProtect for IoT Requirements.

STEP 2 | Configure your GlobalProtect gateways to support the GlobalProtect app for IoT.

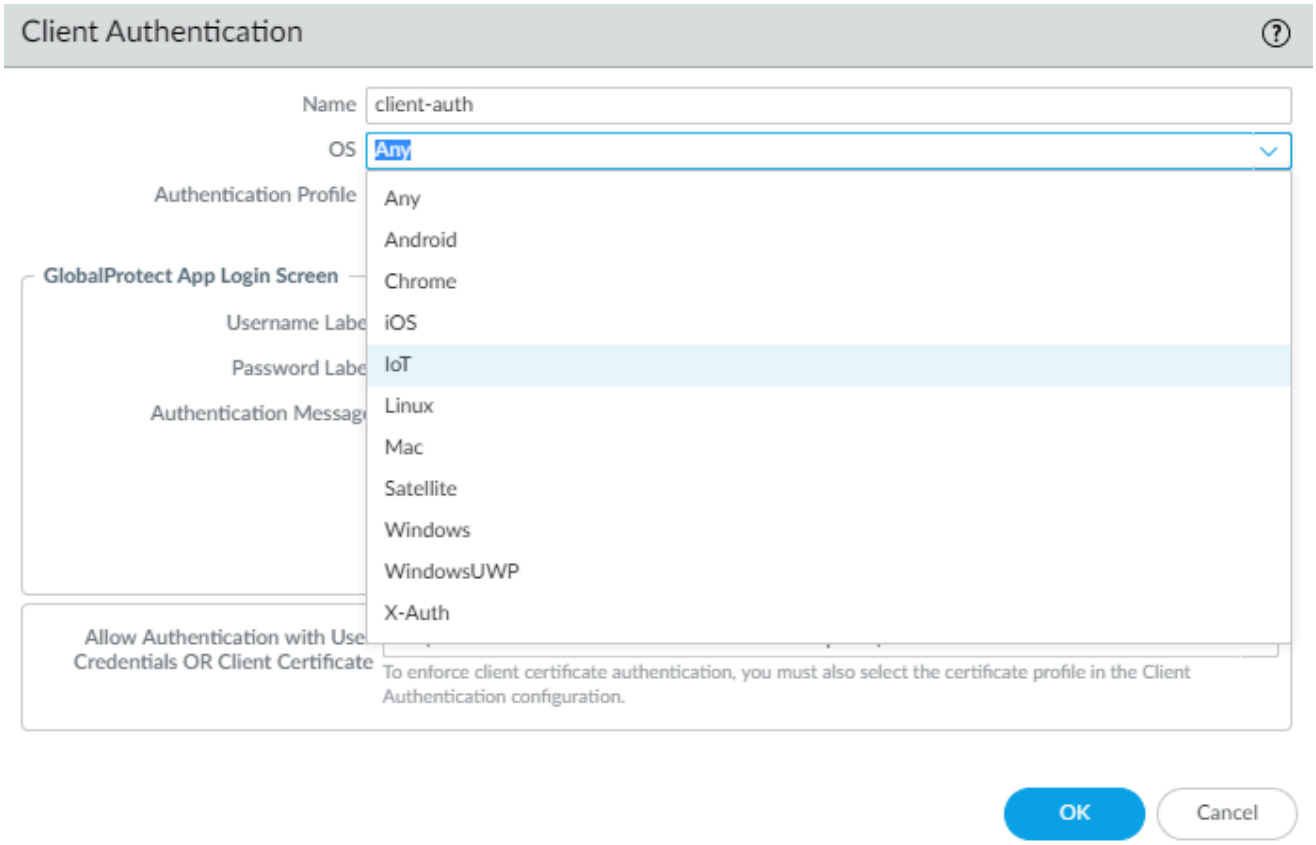
1. Complete the prerequisite tasks for setting up a GlobalProtect gateway.
   - Create the interfaces (and zones) for the firewall on which you plan to configure each gateway. For gateways that require tunnel connections, you must configure both the physical interface and the virtual tunnel interface. See Create Interfaces and Zones for GlobalProtect.
   - Set up the gateway server certificates and SSL/TLS service profile required for the GlobalProtect app to establish an SSL connection with the gateway. See Enable SSL Between GlobalProtect Components.
   - Define the authentication profiles and/or certificate profiles that will be used to authenticate GlobalProtect users. See GlobalProtect User Authentication.
2. Install a GlobalProtect subscription for each gateway that supports the GlobalProtect app for IoT. If you use Prisma Access, a GlobalProtect subscription is not required.
3. Customize a gateway configuration for your IoT devices:

   When you configure a gateway, you can specify client authentication settings that apply specifically to IoT. For example, you can configure Windows and macOS endpoints

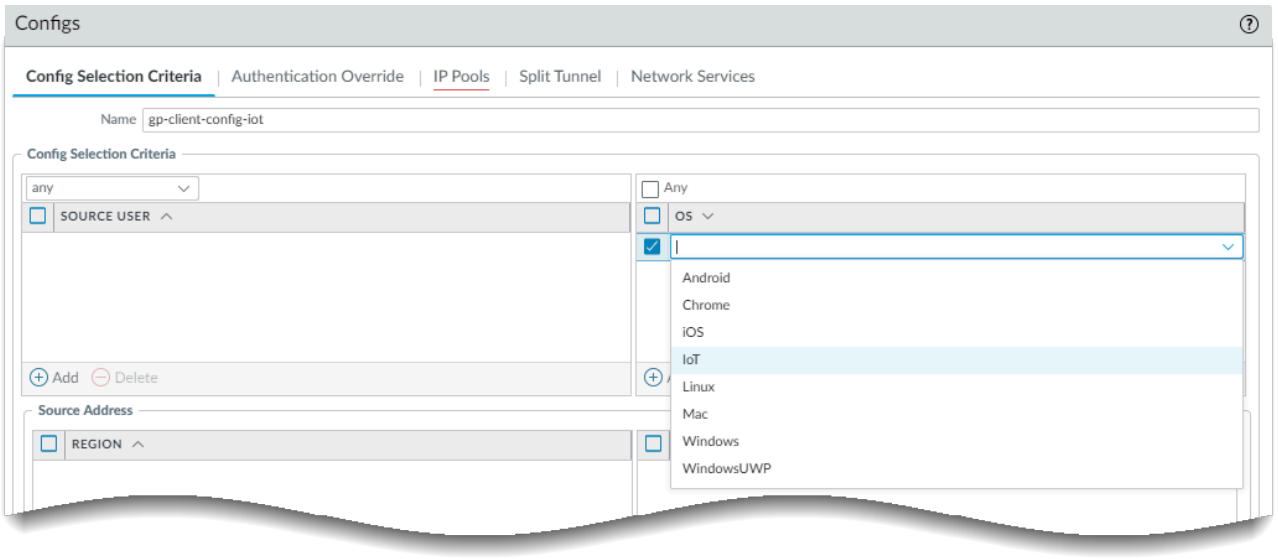
to use two-factor authentication and require IoT devices to use certificate-based authentication.

You can also configure supported network and client settings—such as specific IP pools, access routes, and split tunneling—for IoT devices.

1. Select **Network** > **GlobalProtect** > **Gateways** and then select or **Add** a gateway configuration.
2. Add a Client Authentication configuration for IoT devices:
   1. Select **Authentication** and **Add** a new Client Authentication configuration.
   2. Enter a **Name** to identify the Client Authentication configuration, set **OS** to **IoT**, specify the **Authentication Profile** to use for authenticating users on this gateway. Choose a profile that enables client certificate authentication.



   3. Click **OK**.
3. To configure specific client settings that apply to only IoT endpoints, configure a new Client Settings configuration:
   1. Select **Agent** and **Add** a new Client Settings configuration.
   2. Configure the Client Authentication settings as desired.
   3. Select **User/User Group** and then **Add** an OS, and select **IoT**.



4. Click **OK**.

4. Click **OK**.
5. **Commit** the configuration.

STEP 3 | Configure the portal to support the GlobalProtect app for IoT devices.

To support IoT devices, you must configure one or more gateways to which the GlobalProtect app can connect and then configure the portal and app settings. The portal sends configuration information and information about the available gateways to the app. After receiving the configuration from the GlobalProtect portal, the app discovers the gateways listed in the client configuration and selects the best gateway. Use the following workflow to configure the GlobalProtect portal to support the GlobalProtect app for IoT devices.

1. If you have not already done so, complete the prerequisite tasks for setting up a GlobalProtect portal.
   - Create the interfaces (and zones) for the firewall where you plan to configure the portal. See Create Interfaces and Zones for GlobalProtect.
   - Set up the portal server certificate, gateway server certificate, SSL/TLS service profiles, and, optionally, any client certificates to deploy to end users to enable

SSL/TLS connections for the GlobalProtect™ services. See Enable SSL Between GlobalProtect Components.

- Define the optional authentication profiles and certificate profiles that the portal can use to authenticate GlobalProtect users. See GlobalProtect User Authentication.
- Configure a GlobalProtect Gateway and understand Gateway Priority in a Multiple Gateway Configuration.

2. Define client settings for IoT devices to authenticate to the portal.
   1. Select **Network** > **GlobalProtect** > **Portals** and then select a portal configuration.
   2. Configure Client Authentication settings that apply to IoT devices when users access the portal:
      1. Select **Authentication** and then **Add** a new Client Authentication configuration.
      2. Enter a **Name** to identify the Client Authentication configuration, set **OS** to **IoT**, specify the Authentication Profile to use for authenticating users on this portal. Choose a profile that enables client certificate authentication.
3. Customize an agent configuration for IoT devices.

   Whether you modify an existing configuration or create a new one depends on your environment. For example, if you use OS-specific gateways or want to collect host information that is specific to IoT devices, consider creating a new agent configuration.

   For information about supported features, refer to the Palo Alto Networks Compatibility Matrix for a list of features supported by OS for IoT devices.

   1. Define a GlobalProtect Agent Configuration:
   2. Select **Agent** and select an existing or **Add** a new portal agent configuration.
   3. Configure the Authentication settings for IoT devices.
   4. Select **User/User Group** and then add an **OS** and select **IoT**.
   5. Specify the external gateways to which users with this configuration can connect.
   6. (Optional) Select **App** and customize the applicable portal settings for the GlobalProtect app for IoT. The GlobalProtect app discards any settings that do not apply for IoT. For a list of supported features by operating system, refer to the Palo Alto Networks Compatibility Matrix for a list of features supported by OS for IoT devices.
   7. Click **OK** twice.
   8. **Commit** the configuration.
4. Enforce Policies on IoT devices (**Objects** > **GlobalProtect** > **HIP Objects**).

   You can now create HIP objects using Host Info that is specific to IoT devices and use it for match conditions in any HIP profiles. You can then use a HIP profile as a match condition in a policy rule to enforce the corresponding security policy.

   1. Select **General** > **Host Info** > **OS**.
   2. Select **Contains** > **IoT**.
   3. Click **OK**.
   4. Create additional HIP objects as needed.
   5. Configure HIP-Based Policy Enforcement.

STEP 4 | Install and set up the GlobalProtect app for IoT.

Use the provided instructions for the operating system of your IoT device.

- Install GlobalProtect for IoT on Android
- Install GlobalProtect for IoT on Raspbian
- Install GlobalProtect for IoT on Ubuntu
- Install GlobalProtect for IoT on Windows

Install GlobalProtect for IoT on Android

To use GlobalProtect for IoT on Android devices, you must build the app and GlobalProtect configuration into the Android operating system image as a system application. To enable GlobalProtect to operate in headless mode you must deploy a pre-configuration file with the GlobalProtect app package.

STEP 1 | Add the GlobalProtect.apk as a pre-built system app in your Android OS image.

1. From the Support Site, select **Updates** > **Software Updates** and download the GlobalProtect APK.
2. Decode the APK file in the `android_src_tree_root/packages/app/` directory.

   The decoder unpacks the app into a GlobalProtect folder.
3. In the GlobalProtect folder, create the `Android.mk` file. This file defines the sources and shared libraries that the encoder will use to the build system.

   Edit the file to include the following:

```
LOCAL_PATH := $(call my-dir)
include $(CLEAR_VARS)
LOCAL_MODULE_TAGS := optional
LOCAL_MODULE := GlobalProtect
LOCAL_SRC_FILES := $(LOCAL_MODULE).apk
LOCAL_MODULE_CLASS := APPS
LOCAL_MODULE_SUFFIX := $(COMMON_ANDROID_PACKAGE_SUFFIX)
LOCAL_CERTIFICATE := PRESIGNED
include $(BUILD_PREBUILT)
```

4. For any additional MK files in `android_src_tree_root/vendor/`, add the following line:

```
PRODUCT_PACKAGES += GlobalProtect
```

5. Add libgpjni.so to either `/system/lib` or `/system/lib64`, depending which CPU architecture the IoT device supports. The libgpjni.so file can be retrieved from the lib directory after GlobalProtect.apk is decoded by apktool.

STEP 2 | Modify the Android Framework source code to preauthorize the permission request popup for VPN connection.

Edit the `android_src_tree_root/frameworks/base/services/core/java/com/android/server/connectivity/Vpn.java` file to include the following code segment:

```
private boolean isVpnUserPreConsented(String packageName) {

    if (“com.paloaltonetworks.globalprotect”.equals(packageName)){
        Log.v(TAG, "IoT, isVpnUserPreConsented always true");
    return true;
    }
    AppOpsManager appOps =
```



```
        (AppOpsManager)
 mContext.getSystemService(Context.APP_OPS_SERVICE);

    // Verify that the caller matches the given package and has
 permission to activate VPNs.
    return
 appOps.noteOpNoThrow(AppOpsManager.OP_ACTIVATE_VPN,Binder.getCallingUid(),
        packageName) == AppOpsManager.MODE_ALLOWED;
    }
}
```

STEP 3 | Customize Android behavior to suppress the GlobalProtect icon in the notification bar for Android 8.0 and later releases.

Edit the `android_src_tree_root/frameworks/base/services/core/java/com/android/server/am/ActiveServices.java` file to include the following code segment.

```
if ( r.packageName.equals("com.paloaltonetworks.globalprotect") ) {
    Slog.d(TAG, "not to show the foreground service running
 notification for IoT");
} else {
    r.postNotification();
}
```

STEP 4 | Configure the VPN settings you want to predeploy for Android IoT devices.

1. Create a configuration file (`globalprotect.conf`) in the following format and edit the IP address of the GlobalProtect portal, and authentication settings, either: username and password, or client certificate path (client-cert-path) and pass-phrase file (client-cert-passphrase).

   Username-password based authentication

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

<GlobalProtect>
    <PanSetup>
                <Portal>192.168.1.23</Portal>
    </PanSetup>
        <Settings>
                <head-less>yes</head-less>
                <os-type>IoT</os-type>
                <username>user1</username>
                <password>mypassw0rd</password>
                <log-path-service>/home/gptest/Desktop/data/
gps</log-path-service>
                <log-path-agent>/home/gptest/Desktop/data/
gpadata</log-path-agent>
        </Settings>
```



```
</GlobalProtect>
```

Client-certificate based authentication

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

<GlobalProtect>
    <PanSetup>
                <Portal>192.168.1.23</Portal>
    </PanSetup>
        <Settings>
                <head-less>yes</head-less>
                <os-type>IoT</os-type>
                <client-cert-path>/home/gptest/Desktop/data/
pan_client_cert.pfx</client-cert-path>
                <client-cert-passphrase>/home/gptest/Desktop/
data/pan_client_cert_passcode.dat</client-cert-passphrase>
                <username>user1</username>
                <password>paloalto</password>
                <log-path-service>/home/gptest/Desktop/data/
gps</log-path-service>
                <log-path-agent>/home/gptest/Desktop/data/
gpadata</log-path-agent>
        </Settings>
</GlobalProtect>
```

2. Encode the `globalprotect.conf` file in Base64 format and save it to the `android_src_tree_root/system/config/` directory.

   If desired, you can save the file to an alternate location. However, you must edit the location of this configuration in the `android_src_tree_root/assets/gp_conf_location.txt` file.

STEP 5 | Build the GlobalProtect APK file.

STEP 6 | Sign the GlobalProtect APK file.

STEP 7 | Push the new OS to Android devices as part of the system image and then push the new OS to the Android devices.

Install GlobalProtect for IoT on Raspbian

To install GlobalProtect for IoT on Raspbian devices, complete the following steps.

GlobalProtect for IoT for Raspbian and Ubuntu supports an Arm-based architecture only.

STEP 1 | From the Support Site, select **Updates** > **Software Updates** and download the GlobalProtect package for your OS.

STEP 2 | Install the GlobalProtect app for IoT.

From the IoT device, use the **sudo dpkg -i GlobalProtect_deb_arm<*version*>.deb** command to install the software.

```
sudo dpkg -i GlobalProtect_deb_arm-5.1.0.0-84.deb
```

*To later uninstall the software, use the **sudo dpkg -P globalprotect** command.*

STEP 3 | Configure the VPN settings you want to predeploy for Raspbian IoT devices.

1. In the `client-cert` path, import the certificate in pcks12 format and save the file with a .pfx extension (for example, **pan_client_cert.pfx**).
2. In the `client-cert-passphrase` path, save the passcode file with .dat extension (for example, **pan_client_cert_passcode.dat**)
3. In the `log-path-service` path, if you are not using the default path for PanGPS (for example, `/opt/paloaltonetworks/globalprotect`), make sure that the `log-setting` path folder has the same privilege as the globalprotect folder under `opt/paloaltonetworks`.
4. Create the `/opt/paloaltonetworks/globalprotect/pangps.xml` pre-deployment configuration file in the following format and edit the IP address of the GlobalProtect portal, and authentication settings, either: username and password, or client certificate path (**client-cert-path**) and pass-phrase file (**client-cert-passphrase**). You can also specify an optional folder in which to store GlobalProtect service (**log-path-service**) and agent (**log-path-agent**) logs.

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

<GlobalProtect>
 <PanSetup>
          <Portal>192.168.1.160</Portal>       //pre-deployed
 portal address
</PanSetup>
 <PanGPS>
 </PanGPS>
 <Settings>
         <portal-timeout>5</portal-timeout>
         <connect-timeout>5</connect-timeout>
```



```
        <receive-timeout>30</receive-timeout>
        <os-type>IoT</os-type>            //pre-deployed OS type
 for IoT. If this tag does not present, GP will automatic detect
 the OS type.
        <head-less>yes</head-less>       //pre-deployed head-less
 mode
        <username>abc</username>    //optional pre-deployed
 username
        <password>xyz</password>       //optional pre-deployed
 password
        <client-cert-path>cli_cert_path</client-cert-path>
  //optional pre-deployed client certificate file(p12) path
        <client-cert-passphrase>cli_cert_passphrase_path< /client-
cert-passphrase>       //optional pre-deployed client certificate
 passphrase file path
        <log-path-service>/tmp/gps</log-path-service>  //optional
 pre-deployed log folder for PanGPS
        <log-path-agent>/tmp/gpa</log-path-agent>      //optional
 pre-deployed log folder for PanGPA and globalprotect CLI
 </Settings>
</GlobalProtect>
```

STEP 4 | Restart the GlobalProtect process for the pre-deployment configuration to take effect.

STEP 5 | After you deploy the IoT device, you can collect logs as needed using the **`globalprotect collect-log`** command.

```
user@raspbianhost:~/Desktop/data$ globalprotect collect-log
The support file is saved to /home/gptest/.GlobalProtect/
GlobalProtectLogs.tgz
```

STEP 6 | (Optional) If the authentication method is a is combination of username/password and client certificate authentication, make sure that the **CommonName** of the client certificate matches the username.

Install GlobalProtect for IoT on Ubuntu

To install GlobalProtect for IoT on Ubuntu devices, complete the following steps.

GlobalProtect for IoT for Raspbian and Ubuntu supports an Arm-based architecture only.

STEP 1 | From the Support Site, select **Updates** > **Software Updates** and download the GlobalProtect package for your OS.

STEP 2 | Install the GlobalProtect app for IoT.

From the IoT device, use **ARM** command to install the software.

```
$ ./gp_install.sh --help
Usage: $ sudo ./gp_install [--cli-only | --arm | --help]
  --cli-only: CLI Only
  --arm:      ARM
  no options: UI
```

*To later uninstall the software, use **ARM**command:*

```
$ ./gp_uninstall.sh --help
Usage: $ sudo ./gp_uninstall [--cli-only | --arm | --help]
  --cli-only: CLI Only
  --arm:      ARM
  no options: UI
```

STEP 3 | Configure the VPN settings you want to predeploy for Ubuntu IoT devices.

1. In the `client-cert` path, import the certificate in pcks12 format and save the file with a .pfx extension (for example, **pan_client_cert.pfx**).
2. In the `client-cert-passphrase` path, save the passcode file with .dat extension (for example, **pan_client_cert_passcode.dat**)
3. In the `log-path-service` path, if you are not using the default path for PanGPS (for example, `/opt/paloaltonetworks/globalprotect`), make sure that the `log-setting` path folder has the same privilege as the globalprotect folder under `opt/paloaltonetworks`.
4. Create the `/opt/paloaltonetworks/globalprotect/pangps.xml` pre-deployment configuration file in the following format and edit the IP address of the GlobalProtect portal, and authentication settings, either: username and password, or client certificate path (**`client-cert-path`**) and pass-phrase file (**`client-cert-passphrase`**). You can also specify an optional folder in which to store GlobalProtect service (**`log-path-service`**) and agent (**`log-path-agent`**) logs.

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

<GlobalProtect>
```



```
 <PanSetup>
          <Portal>192.168.1.160</Portal>       //pre-deployed
 portal address
</PanSetup>
 <PanGPS>
 </PanGPS>
 <Settings>
        <portal-timeout>5</portal-timeout>
        <connect-timeout>5</connect-timeout>
        <receive-timeout>30</receive-timeout>
        <os-type>IoT</os-type>             //pre-deployed OS type
 for IoT. If this tag does not present, GP will automatic detect
 the OS type.
        <head-less>yes</head-less>       //pre-deployed head-less
 mode
        <username>abc</username>    //optional pre-deployed
 username
        <password>xyz</password>       //optional pre-deployed
 password
        <client-cert-path>cli_cert_path</client-cert-path>
  //optional pre-deployed client certificate file(p12) path
        <client-cert-passphrase>cli_cert_passphrase_path< /client-
cert-passphrase>       //optional pre-deployed client certificate
 passphrase file path
        <log-path-service>/tmp/gps</log-path-service>  //optional
 pre-deployed log folder for PanGPS
        <log-path-agent>/tmp/gpa</log-path-agent>      //optional
 pre-deployed log folder for PanGPA and globalprotect CLI
 </Settings>
</GlobalProtect>
```

STEP 4 | Restart the GlobalProtect process for the pre-deployment configuration to take effect.

STEP 5 | After you deploy the IoT device, you can collect logs as needed using the **`globalprotect collect-log`** command.

```
user@linuxhost:~$ globalprotect collect-log
The support file is saved to /home/gptest/.GlobalProtect/
GlobalProtectLogs.tgz
```

STEP 6 | (Optional) If the authentication method is a is combination of username/password and client certificate authentication, make sure that the **CommonName** of the client certificate matches the username.

Install GlobalProtect for IoT on Windows

Devices running Windows 10 IoT can use the GlobalProtect app. Use your organization's distribution method, such as Microsoft System Center Configuration Manager (SCCM), to deploy and install the GlobalProtect app on your IoT devices running Windows 10 IoT Enterprise.

A GlobalProtect Windows IoT deployment supports certificate-based authentication. You must install the certificate used for authentication on each IoT device in its local machine store. If an IoT device has multiple certificates with the same Root CA, GlobalProtect uses the first certificate in the IoT device's local machine store to authenticate; be sure that your certificates are in the correct order in your devices.

The following sections describe how to install the GlobalProtect app on devices running Windows IoT:

- Download and Install the MSIEXEC File on the IoT Device
- Modify the Registry Keys on the IoT Device (On-Demand or Always On)
- Modify the Registry Keys on the IoT Device (Always On with Pre-logon)

Download and Install the MSIEXEC File on the IoT Device

You can download and install the `msiexec.exe` file to your IoT devices to install the GlobalProtect app for the **On-Demand** connect method or **Always On** connect method. You use the same method to Deploy Scripts Using Msiexec as you do on a non-IoT device.

Modify the Registry Keys on the IoT Device (On-Demand or Always On)

You must specify the OS type as IoT, the device type as headless, and the portal address. Optionally, you can specify a username and password. If you do not specify a username and password, GlobalProtect uses certificate-based authentication.

You can use the following methods of installation for the **On-Demand** connect method or **Always On** connect method:

- Specify the OS Type (Required):

  Registry subkey: `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks \GlobalProtect\Settings`

  Name: os-type

  Type: REG_SZ

  Data: IoT

- Specify a headless IoT device (Required):

  Registry subkey: `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`

  Name: head-less

  Type: REG_SZ

  Data: yes
- Specify the portal address (Required):

  Registry subkey: `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup`

  Name: Portal

  Type: REG_SZ

  Data: Enter the GlobalProtect portal's IP address or FQDN.
- Specify the username (Optional):

  Registry subkey: `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`

  Name: username

  Type: REG_SZ

  Data: Enter the user name to use with the IoT device.
- Specify the password (Optional):

  Registry subkey: `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`

  Name: password

  Type: REG_SZ

  Data: Enter the password to use with the IoT device.

Modify the Registry Keys on the IoT Device (Always On with Pre-logon)

You must specify the portal address, the pre-logon timeout value, and the service-only value. You must delete the GlobalProtect value to prevent the IoT device from automatically launching the app interface upon system restart. A pre-logon VPN tunnel does not associate the username because the user has not logged in.

You can use the following methods of installation for the **Pre-logon (Always On)** connect method:

- Specify the portal address (Required):

  Registry subkey: `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup`

  Name: Portal

  Type: REG_SZ

  Data: Enter the GlobalProtect portal's IP address or FQDN.
- Specify the pre-logon value (Required):

  Registry subkey: `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup`

  Name: Prelogon

  Type: REG_SZ

  Data: 1
- Specify the service-only value (Required):

  Registry subkey: `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`

  Name: service-only

  Type: REG_SZ

  Data: yes
- Delete the GlobalProtect value (Required):

  Registry subkey: `\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

  Name: GlobalProtect

  Type: REG_SZ

Host Information

Although you may have stringent security at your corporate network border, your network is really only as secure as the endpoints that are accessing it. With today's workforce becoming more mobile and often requiring access to corporate resources from a variety of locations—airports, coffee shops, hotels—and from a variety of endpoints—both company-provisioned and personal—you must logically extend your network's security to your endpoints to ensure comprehensive and consistent security enforcement. The GlobalProtect™ Host Information Profile (HIP) feature enables you to collect information about the security status of your endpoints—such as whether they have the latest security patches and antivirus definitions installed, whether they have disk encryption enabled, whether the endpoint is jailbroken or rooted, or whether it is running specific software you require within your organization—and base the decision as to whether to allow or deny access to a specific host based on adherence to the host policies you define.

The following sections provide information about the use of host information in policy enforcement:

About Host Information

One of the jobs of the GlobalProtect app is to collect information about the host it is running on. The app then submits this host information to the GlobalProtect gateway upon successful connection. The gateway matches this raw host information submitted by the app against any HIP objects and HIP profiles that you have defined. If it finds a match, it generates an entry in the HIP Match log. Additionally, if it finds a HIP profile match in a policy rule, it enforces the corresponding security policy.

HIP checks are performed when the app connects to the gateway and subsequent checks are performed hourly while the GlobalProtect agent is connected. The GlobalProtect agent can request an updated HIP report if the previous HIP check has changed. Only the latest HIP report is retained on the gateway per endpoint.

Using host information profiles for policy enforcement enables granular security that ensures the remote hosts accessing your critical resources are adequately maintained and adhere with your security standards before they are allowed access to your network resources. For example, before allowing access to your most sensitive data systems, you might want to ensure that the hosts accessing the data have encryption enabled on their hard drives. You can enforce this policy by creating a security rule that only allows access to the application if the endpoint system has encryption enabled. In addition, for endpoints that are not in compliance with this rule, you could create a notification message that alerts users as to why they have been denied access and links them to the file share where they can access the installation program for the missing encryption software (of course, to allow the user to access that file share you would have to create a corresponding security rule allowing access to the particular share for hosts with that specific HIP profile match).

- What Data Does the GlobalProtect App Collect?
- What Data Does the GlobalProtect App Collect on Each Operating System?
- How Does the Gateway Use the Host Information to Enforce Policy?
- How Do Users Know if Their Systems are Compliant?
- How Do I Get Visibility into the State of the Endpoints?

What Data Does the GlobalProtect App Collect?

By default, the GlobalProtect app collects vendor-specific data about the end user security packages that are running on the endpoint (as compiled by the OPSWAT global partnership program) and reports this data to the GlobalProtect gateway for policy enforcement. See the GlobalProtect 5.1 OPSWAT Support table or GlobalProtect 5.2 OPSWAT Support table for details about the third-party vendor products that GlobalProtect can detect using the specified OPSWAT SDK.

Starting with GlobalProtect app 5.2.6, support for OPSWAT SDK V3 (end-of-life) will be removed and the GlobalProtect app will only use OPSWAT SDK V4. Vendor and product names are based on OPSWAT SDK V4. GlobalProtect app 5.2.6 and later release HIP check functionality will not work with PAN-OS 8.0 (end-of-life) and earlier releases (end-of-life). GlobalProtect app 5.2.6 and later release HIP check functionality will work as expected with PAN-OS 8.1 and later releases.

Because security software must continually evolve to ensure end user protection, your GlobalProtect gateway licenses also enable you to receive dynamic updates for the GlobalProtect data file with the latest patch and software versions available for each package.

By default, the app collects data about the following categories of information to help identify the security state of the host:

Table 8: Table: Data Collection Categories

Category	Data Collected
General	Information about the host itself, including the hostname, logon domain, operating system, app version, and, for Windows systems, the domain to which the machine belongs. *For Windows endpoints' domain, the GlobalProtect app collects the domain defined for `ComputerNameDnsDomain`, which is the DNS domain assigned to the local computer or the cluster associated with the local computer. This data is displayed for the Windows endpoints' **Domain** in the HIP Match log details (**Monitor** > **Logs** > **HIP Match**).*
Mobile Device	Information about the mobile device, including the device name, logon domain, operating system, app version, and information about the network to which the device is connected. In addition, GlobalProtect collects information on whether the device is rooted or jailbroken. *To collect mobile device attributes and utilize them in HIP enforcement policies, GlobalProtect requires an MDM server. GlobalProtect currently supports HIP integration with the Workspace ONE MDM server.* For devices managed by Workspace ONE, host information collected by the GlobalProtect app can be supplemented with additional information collected from the Workspace ONE service. Refer to Configure Windows User-ID Agent to Collect Host Information for a list of attributes that can be retrieved from Workspace ONE.
Patch Management	Information about any patch management software that is enabled and/or installed on the host and whether there are any missing patches.

Category	Data Collected
	*If you want to configure the **Severity** value for missing patches as a match condition in your HIP object (**Objects** > **GlobalProtect** > **HIP Objects** > **<hip-object>** > **Patch Management** > **Criteria**), use the following mappings between the GlobalProtect severity values and the OPSWAT severity ratings to understand what each value means:* • ***0**—Low* • ***1**—Moderate* • ***2**—Important* • ***3**—Critical*
Firewall	Information about any firewalls that are installed and/or enabled on the host.
Anti-Malware	Information about any antivirus or anti-spyware software that is enabled and/or installed on the endpoint, whether or not real-time protection is enabled, the virus definition version, last scan time, and the vendor and product name. GlobalProtect uses OPSWAT technology to detect and assess third-party security applications on the endpoint. By integrating with the OPSWAT OESIS framework, GlobalProtect enables you to assess the compliance state of the endpoint. For example, you can define HIP objects and HIP profiles that verify the presence of a specific version of antivirus software from a specific vendor on the endpoint and also ensure that it has the latest virus definition files. *OPSWAT is unable to detect the following **Anti-Malware** information for the Gatekeeper security feature on macOS endpoints:* • *Engine Version* • *Definition Version* • *Date* • *Last Scanned*
Disk Backup	Information about whether disk backup software is installed, the last backup time, and the vendor and product name of the software.
Disk Encryption	Information about whether disk encryption software is installed, which drives and/or paths are configured for encryption, and the vendor and product name of the software.

Category	Data Collected
	(Requires GlobalProtect app 5.2) If you want to view the encryption status of all drives and/or paths on the endpoint, you must manually enter **All** as the **Encrypted Locations** when creating the HIP object for the **Disk Encryption** category. To verify if all drives or paths are encrypted, you must set the **Encrypted Locations** to **All** and set the **State** to **Is encrypted** from the drop-down.
Data Loss Prevention	Information about whether data loss prevention (DLP) software is installed and/or enabled to prevent sensitive corporate information from leaving the corporate network or from being stored on a potentially insecure device. This information is only collected from Windows endpoints.
Certificate	Information about the machine certificate installed on the endpoint.
Custom Checks	Information about whether specific registry keys (Windows only), property lists (plists) (macOS only), process lists (Linux only), OR operating system processes and user-space application processes are present.

You can exclude certain categories of information from being collected on certain hosts to save CPU cycles and improve response time. To do this, create an agent configuration on the portal, and then exclude the categories you are not interested in (**Network** > **GlobalProtect** > **Portals** > ***<portal-config>*** > **Agent** > ***<agent-config>*** > **Data Collection**). For example, if you do not plan on creating policies based on whether or not endpoints run disk backup software, you can exclude that category to prevent the app from collecting any information about disk backup.

You can also exclude information from being collected on personal endpoints in order to provide user privacy. For example, you can exclude the list of apps installed on endpoints that are not managed by a third-party mobile device manager.

What Data Does the GlobalProtect App Collect on Each Operating System?

The GlobalProtect app collects data to help identify or retrieve the host information profile (HIP) for the device for use in Configure HIP-Based Policy Enforcement.

- What Data Does the GlobalProtect App Collect on Windows?
- What Data Does the GlobalProtect App Collect on macOS?
- What Data Does the GlobalProtect App Collect on Windows UWP?
- What Data Does the GlobalProtect App Collect on Android?
- What Data Does the GlobalProtect App Collect on iOS?
- What Data Does the GlobalProtect App Collect on Linux?

What Data Does the GlobalProtect App Collect on Windows?

The following table describes the data collected by the GlobalProtect app on Windows devices for HIP-based policy enforcement generated by the firewall:

HIP Report Attribute	Description
Report Generation Time	Date and time that the HIP report was generated.
User Name	Username that is used to log in to the VPN.
User IP Address	IP address of the users' Windows device.
Machine Name	Host name and serial number of the Windows device.
Domain	Field is empty on Windows devices.
OS	Application name and vendor name of the target OS.
Host ID	Unique host ID that is assigned by GlobalProtect to identify the host. The host ID value is machine GUID on Windows devices. The machine GUID is stored in the Windows registry (HKEY_Local_Machine\Software\Microsoft\Cryptography \MachineGuid).
Client Version	Version number of the currently installed GlobalProtect app.
Network Interface	Following settings are identified for the network interface: • **Interface**—Type of network interface detected on the Windows device. • **MAC Address**—MAC address is the unique hardware identifier assigned to each network interface on the Windows device. • **IP Address**—IP address assigned to each network interface on the Windows device.
Anti-Malware	Information about any antivirus or anti-spyware that is enabled or installed on the device, whether real-time anti-virus or anti-spyware protection is enabled on the host, virus definition version, last scan time, and the vendor and product name.
Disk Backup	Information about the disk backup status of the device such as whether the disk backup software is installed on the host, the last backup time, and the vendor and product name of the software.
Disk Encryption	Information about the disk encryption status of the device such as whether the disk encryption software is installed on the host,

HIP Report Attribute	Description
	the drive or path to check for disk encryption to determine a match, state of the encrypted location, and the vendor and product name of the software. (Requires GlobalProtect app 5.2) If you want to view the encryption status of all drives or paths on the endpoint, you must manually enter **All** as the **Encrypted Locations** when creating the HIP object for the **Disk Encryption** category. To verify if all drives or paths are encrypted, you must set the **Encrypted Locations** to **All** and set the **State** to **Is encrypted** from the drop-down.
Patch Management	Information about any patch management software that is installed or enabled on the host and whether the host detected missing patches and the specified severity value. See the What Data Does the GlobalProtect App Collect? category for details on each value.
Firewall	Information about whether firewall software is enabled or installed on the host.
Data Loss Prevention	Information about the data loss prevention (DLP) software status on the Windows devices to prevent corporate information from leaving the corporate network or from being stored on a potentially insecure device.
Custom Checks	Information about the Windows Registry collected by the GlobalProtect app from Windows devices. You can enable Collect Application and Process Data From Endpoints to collect data from Windows devices to instruct the app to collect specific registry information (Registry Keys and Registry Key Values). The type of information collected can include whether an application is installed on the device, or specific attributes or properties of that application.

What Data Does the GlobalProtect App Collect on macOS?

The following table describes the data collected by the GlobalProtect app on macOS devices for HIP-based policy enforcement generated by the firewall:

HIP Report Attribute	Description
Report Generation Time	Date and time that the HIP report was generated.
User Name	Username that is used to log in to the VPN.
User IP Address	IP address of the users' macOS device.

HIP Report Attribute	Description
Machine Name	Host name and serial number of the macOS device.
Domain	Field is empty on macOS devices.
OS	Application name and vendor name of the target OS.
Host ID	Unique host ID that is assigned by GlobalProtect to identify the host. The host ID value is the MAC address of the first built-in physical interface.
Client Version	Version number of the currently installed GlobalProtect app.
Network Interface	Following settings are identified for the network interface: • **Interface**—Type of network interface detected on the macOS device. • **MAC Address**—MAC address is the unique hardware identifier assigned to each network interface on the macOS device. • **IP Address**—IP address assigned to each network interface on the macOS device.
Anti-Malware	Information about any antivirus or anti-spyware that is enabled or installed on the device, whether real-time anti-virus or anti-spyware protection is enabled on the host, virus definition version, last scan time, and the vendor and product name.
Disk Backup	Information about the disk backup status of the device such as whether the disk backup software is installed on the host, the last backup time, and the vendor and product name of the software.
Disk Encryption	Information about the disk encryption status of the device such as whether the disk encryption software is installed on the host, the drive or path to check for disk encryption to determine a match, state of the encrypted location, and the vendor and product name of the software. (Requires GlobalProtect app 5.2) If you want to view the encryption status of all drives or paths on the endpoint, you must manually enter **All** as the **Encrypted Locations** when creating the HIP object for the **Disk Encryption** category. To verify if all drives or paths are encrypted, you must set the **Encrypted Locations** to **All** and set the **State** to **Is encrypted** from the drop-down.
Patch Management	Information about any patch management software that is installed or enabled on the host and whether the host detected

HIP Report Attribute	Description
	missing patches and the specified severity value. See the What Data Does the GlobalProtect App Collect? category for details on each value.
Firewall	Information about whether firewall software is enabled or installed on the host.
Custom Checks	Information about the macOS property list (plist) collected by the GlobalProtect app from macOS devices. You can enable Collect Application and Process Data From Endpoints to collect data from macOS devices to instruct the app to collect specific plist information (plist and plist keys). The type of information collected can include whether an application is installed on the device, or specific attributes or properties of that application.

What Data Does the GlobalProtect App Collect on Windows UWP?

The following table describes the data collected by the GlobalProtect app on Windows UWP devices for HIP-based policy enforcement generated by the firewall:

HIP Report Attribute	Description
Report Generation Time	Date and time that the HIP report was generated.
User Name	Username that is used to log in to the VPN.
User IP Address	IP address of the users' Windows UWP device.
Machine Name	Host name and serial number of the Windows UWP device.
Domain	Field is empty on Windows UWP devices.
OS	Application name and vendor name of the target OS.
Host ID	Unique host ID that is assigned by GlobalProtect to identify the host. The host ID value is GUID on Windows UWP devices.
Client Version	Version number of the currently installed GlobalProtect app.
Network Interface	Following settings are identified for the network interface: • **Interface**—Type of network interface detected on the Windows UWP device. • **MAC Address**—MAC address is the unique hardware identifier assigned to each network interface on the Windows UWP device.

HIP Report Attribute	Description
	• **IP Address**—IP address assigned to each network interface on the Windows UWP device.

What Data Does the GlobalProtect App Collect on Android?

The following table describes the data collected by the GlobalProtect app on Android devices for HIP-based policy enforcement generated by the fiirewall:

The GlobalProtect app for Android on a Chromebook uses the same HIP report attributes.

HIP Report Attribute	Description
Report Generation Time	Date and time that the HIP report was generated.
User Name	Username that is used to log in to the VPN.
User IP Address	IP address of the users' Android device.
Machine Name	Host name and serial number of the Android device.
Domain	Field is empty on Android devices.
Serial Number	Serial number of the Android device.
Managed	Value that indicates whether the Android device is managed. If this value is set to **Yes**, the device is managed. If this value is set to **No**, the device is unmanaged.
OS	Application name and vendor name of the target OS.
Host ID	GlobalProtect assigned unique alphanumeric string with length of 16 characters to identify the host. The host ID value is Android ID on Android devices.
Client Version	Version number of the currently installed GlobalProtect app.
WiFi SSID	Specific information about the network connectivity such as **WiFi SSID** on the Android device.
Network Interface	Following settings are identified for the network interface: • **Interface**—Type of network interface detected on the Android device. • **MAC Address**—MAC address is the unique hardware identifier assigned to each network interface on the Android device.

HIP Report Attribute	Description
	• **IP Address**—IP address assigned to each network interface on the Android device.
Mobile Device	Information about the What Data Does the GlobalProtect App Collect?, including the device name, logon domain, operating system, app version, and the network to which the device is connected.
Tags	Tags to enable you to match against other MDM-based attributes.
Device Compliance	The **Rooted/Jailbroken** attribute is used to determine the compliance status of the Android device that has been rooted or jailbroken to obtain administrative privileges. The security policies can be removed or bypassed in the operating system from a compromised device.
MDM Attributes	When you integrate your GlobalProtect deployment with an MDM vendor, the GlobalProtect app for Android devices can obtain the following data attributes and tags from the MDM system: • **udid**—Unique device identifier (UDID) of the Android device. • **managed-by-mdm**—Value that indicates whether the Android device is managed. If this value is set to **Yes**, the Android device is managed. If this value is set to **No**, the Android device is unmanaged. • **tag**—Tags to enable you to match against other MDM-based attributes. • **compliance**—Compliance status that indicates whether the Android device is compliant with the compliance policies that you have defined. • **ownership**—Ownership category of the Android device (for example, **Employee Owned**). This value is appended to the **Tag** attribute in the HIP report.

What Data Does the GlobalProtect App Collect on iOS?

The following table describes the data collected by the GlobalProtect app on iOS devices for HIP-based policy enforcement generated by the firewall:

HIP Report Attribute	Description
Report Generation Time	Date and time that the HIP report was generated.
User Name	Username that is used to log in to the VPN.

HIP Report Attribute	Description
User IP Address	IP address of the users' iOS device.
Machine Name	Host name and serial number of the iOS device.
Domain	Field is empty on iOS devices.
Serial Number	Field is empty on iOS device.
Managed	Value that indicates whether the iOS device is managed. If this value is set to **Yes**, the device is managed. If this value is set to **No**, the device is unmanaged.
OS	Application name and vendor name of the target OS.
Host ID	Unique ID that is assigned by GlobalProtect to identify the host. The host ID value is UDID on iOS devices.
Client Version	Version number of the currently installed GlobalProtect app.
WiFi SSID	Information about the network connectivity such as **WiFi SSID** on the iOS device.
Network Interface	Following settings are identified for the network interface: • **Interface**—Type of network interface detected on the iOS device. • **MAC Address**—MAC address is the unique hardware identifier assigned to each network interface on the iOS device. • **IP Address**—IP address assigned to each network interface on the iOS device.
Mobile Device	Information about the What Data Does the GlobalProtect App Collect?, including the device name, logon domain, operating system, app version, and the network to which the device is connected.
Device Compliance	Following attributes are used to determine the compliance status of the iOS device: • **Rooted/Jailbroken**—Status on the iOS device that has been rooted or jailbroken to obtain administrative privileges. The security policies can be removed or bypassed in the operating system from a compromised device. • **Disk Encryption Not Set**—Status on the iOS device that is enabled for disk encryption.

HIP Report Attribute	Description
	• **Passcode Not Set**—Status on the iOS device that is set to a passcode. • **Has Malware**—Status on the iOS device that has malware-infected apps installed.
MDM Attributes	When you integrate your GlobalProtect deployment with an MDM vendor, the GlobalProtect app for iOS devices can obtain the following data attributes and tags from the MDM system: • **udid**—Unique device identifier (UDID) of the iOS device. • **managed-by-mdm**—Value that indicates whether the iOS device is managed. If this value is set to **Yes**, the iOS device is managed. If this value is set to **No**, the iOS device is unmanaged. • **tag**—Tags to enable you to match against other MDM-based attributes. • **compliance**—Compliance status that indicates whether the iOS device is compliant with the compliance policies that you have defined. • **ownership**—Ownership category of the iOS device (for example, **Employee Owned**). This value is appended to the **Tag** attribute in the HIP report.

What Data Does the GlobalProtect App Collect on Linux?

The following table describes the data collected by the GlobalProtect app on Linux devices for HIP-based policy enforcement generated by the firewall:

HIP Report Attribute	Description
User Name	Username that is used to log in to the VPN.
IP Address	IP address of the users' Linux device.
Generate Time	Date and time that the HIP report was generated.
Host Info	Activate one or more of the following options for configuring the host information: • **Managed**—Value that indicates whether the Linux device is managed. If this value is set to **Yes**, the device is managed. If this value is set to **No**, the device is unmanaged. • **Serial Number**—Serial number of the Linux device. • **Client Version**—Version number of the currently installed GlobalProtect app. • **OS**—Application name of the target OS you want to match.

HIP Report Attribute	Description
	• **OS Vendor**—Vendor name of the target OS you want to match. • **Domain**—Domain name of the Linux device. • **Host Name**—Host name of the Linux device. • **Host ID**—Unique ID that is assigned by GlobalProtect to identify the host. The host ID value is the product unique device identifier (UDID) on Linux devices.
Network Interface	Following settings are identified for the network interface: • **Interface**—Type of network interface detected on the Linux device. • **MAC Address**—MAC address is the unique hardware identifier assigned to each network interface on the Linux device. • **IP Address**—IP address assigned to each network interface on the Linux device.
Anti-Malware	Information about any antivirus or anti-spyware that is enabled or installed on the device, whether real-time anti-virus or anti-spyware protection is enabled on the host, virus definition version, last scan time, and the vendor and product name.
Disk Backup	Information about the disk backup status of the device such as whether the disk backup software is installed on the host, the last backup time, and the vendor and product name of the software.
Disk Encryption	Information about the disk encryption status of the device such as whether the disk encryption software is installed on the host, the drive or path to check for disk encryption to determine a match, state of the encrypted location, and the vendor and product name of the software. (Requires GlobalProtect app 5.2) If you want to view the encryption status of all drives or paths on the endpoint, you must manually enter **All** as the **Encrypted Locations** when creating the HIP object for the **Disk Encryption** category. To verify if all drives or paths are encrypted, you must set the **Encrypted Locations** to **All** and set the **State** to **Is encrypted** from the drop-down.
Firewall	Information about whether firewall software is enabled or installed on the host.
Patch Management	Information about any patch management software that is installed or enabled on the host and whether the host detected

HIP Report Attribute	Description
	missing patches and the specified severity value. See the What Data Does the GlobalProtect App Collect? category for details on each value.
Custom Checks	Information about the Process List collected by the GlobalProtect app from Linux devices. You can enable Collect Application and Process Data From Endpoints to collect data from Linux devices to instruct the app to collect specific information that can include whether an application is installed on the device, or specific attributes or properties of that application.

How Does the Gateway Use the Host Information to Enforce Policy?

While the app gets the information about what information to collect from the client configuration downloaded from the portal, you define which host attributes you are interested in monitoring and/or using for policy enforcement by creating HIP objects and HIP profiles on the gateway(s):

- **HIP Objects**—The matching criteria used to filter out the host information you are interested in using to enforce policy from the raw data reported by the app. For example, while the raw host data may include information about several antivirus packages that are installed on the endpoint, you may only be interested in one particular application that you require within your organization. In this case, you would create a HIP object to match the specific application you are interested in enforcing.

  The best way to determine what HIP objects you need is to determine how you will use the host information you collect to enforce policy. Keep in mind that the HIP objects themselves are merely building blocks that allow you to create the HIP profiles that are used in your security policies. Therefore, you may want to keep your objects simple, matching on one thing, such as the presence of a particular type of required software, membership in a specific domain, or the presence of a specific endpoint OS. By doing this, you have the flexibility to create a very granular (and very powerful) HIP-augmented policy.
- **HIP Profiles**—A collection of HIP objects that are evaluated together, either for monitoring or for security policy enforcement. When you create your HIP profiles, you can combine the HIP objects you previously created (as well as other HIP profiles) using Boolean logic, such that when a traffic flow is evaluated against the resulting HIP profile, it either matches or does not match. If there is a match, the corresponding policy rule is enforced. If there is no match, the flow is evaluated against the next rule, as with any other policy matching criteria.

Unlike a traffic log—which only creates a log entry if there is a policy match—the HIP Match log generates an entry whenever the raw data submitted by an app matches a HIP object and/or a HIP profile you have defined. This makes the HIP Match log a good resource for monitoring the state of the endpoints in your network over time—before attaching your HIP profiles to security policies—in order to help you determine exactly what policies you believe need enforcement. See Configure HIP-Based Policy Enforcement for details on how to create HIP objects and HIP profiles and use them as policy match criteria.

How Do Users Know if Their Systems are Compliant?

By default, end users are not given any information about policy decisions that were made as a result of HIP-enabled security rule enforcement. However, you can enable this functionality by configuring HIP notification messages to display when a particular HIP profile is matched and/or not matched.

The decision as to when to display a message (that is, whether to display it when the user's configuration matches a HIP profile in the policy or when it doesn't match it), depends largely on your policy and what a HIP match (or non-match) means for the user. That is, does a match mean they are granted full access to your network resources? Or does it mean they have limited access due to a non-compliance issue?

For example, consider the following scenarios:

- You create a HIP profile that matches if the required corporate antivirus and anti-spyware software packages are *not* installed. In this case, you might want to create a HIP notification message for users who match the HIP profile, and tell them that they need to install the software (and, optionally, providing a link to the file share where they can access the installer for the corresponding software).
- You create a HIP profile that matches if those same applications *are* installed. In this case, you might want to create the message for users who do not match the profile, and direct them to the location of the install package.

See Configure HIP-Based Policy Enforcement for details on how to create HIP objects and HIP profiles and use in defining HIP notification messages.

How Do I Get Visibility into the State of the Endpoints?

Whenever an endpoint connects to GlobalProtect, the app presents its HIP data to the gateway. The gateway then uses this data to determine which HIP objects and/or HIP profiles the host matches. For each match, it generates a HIP Match log entry. Unlike a traffic log—which only creates a log entry if there is a policy match—the HIP Match log generates an entry whenever the raw data submitted by an app matches a HIP object and/or a HIP profile you have defined. This makes the HIP Match log a good resource for monitoring the state of the endpoints in your network over time—before attaching your HIP profiles to security policies—in order to help you determine exactly what policies you believe need enforcement.

Because a HIP Match log is only generated when the host state matches a HIP object you have created, for full visibility into the endpoint state, you may need to create multiple HIP objects to log HIP matches for endpoints that are in compliance with a particular state (for security policy enforcement purposes) as well as endpoints that are non-compliant (for visibility). For example, suppose you want to prevent an endpoint that does not have antivirus or anti-spyware software installed from connecting to the network. In this case, you would create a HIP object that matches hosts that have a particular antivirus or anti-spyware software installed. By including this object in a HIP profile and attaching it to the security policy rule that allows access from your VPN zone, you can ensure that only hosts that are protected with antivirus or anti-spyware software can connect.

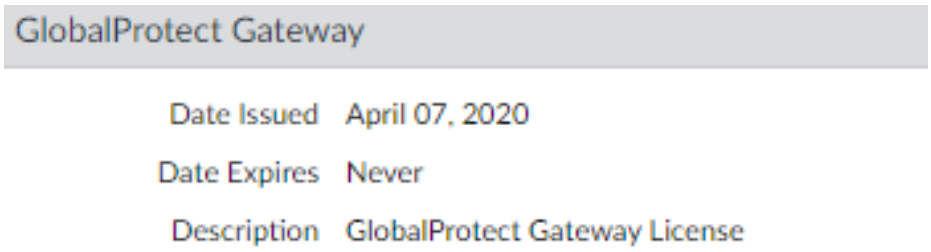
In this example, you would not be able to view which endpoints are not in compliance with this requirement in the HIP Match log. If you want to view a log for endpoints that do not have antivirus or anti-spyware software installed so that you can follow up with these users, you can

also create a HIP object that matches the condition where the antivirus or anti-spyware software is not installed. Because this object is only required for logging purposes, you do not need to add it to a HIP profile or attach it to a security policy rule.

Configure HIP-Based Policy Enforcement

To enable the use of host information in policy enforcement, you must complete the following steps. For more information on the HIP feature, see About Host Information. See What Data Does the GlobalProtect App Collect on Each Operating System? for more details about the data that is collected for the device.

STEP 1 | Verify proper licensing for HIP checks.



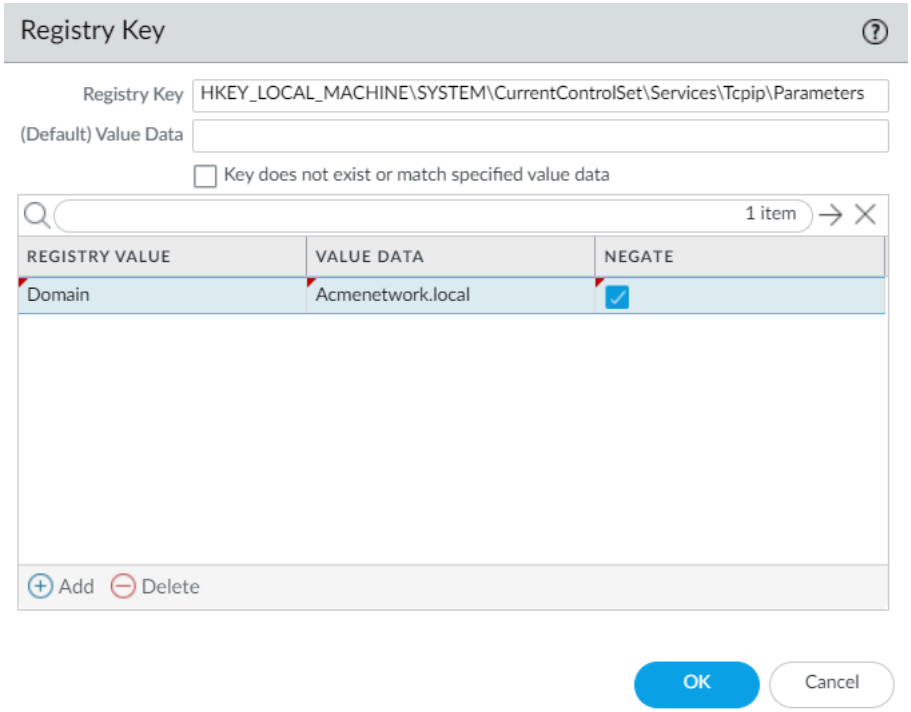
To use the HIP feature, you must purchase and install a GlobalProtect subscription license on each gateway that will perform HIP checks. To verify the status of your licenses on each portal and gateway, select **Device** > **Licenses**.

Contact your Palo Alto Networks Sales Engineer or Reseller if you do not have the required licenses. For more information on licensing, see About GlobalProtect Licenses.

STEP 2 | (Optional) Define any custom host information that you want the app to collect. For example, if you have any required applications that are not included in the Vendor and/or Product lists for creating HIP objects, you could create a custom check that allows you to

determine whether that application is installed (has a corresponding registry or plist key) or is running (has a corresponding running process).

Step 2 and 3 assume that you have already configured a GlobalProtect portal. If you have not yet configured your portal, see Set Up Access to the GlobalProtect Portal for instructions.



1. On the firewall hosting your GlobalProtect portal, select **Network** > **GlobalProtect** > **Portals**.
2. Select the portal configuration that you want to modify.
3. On the **Agent** tab, select the agent configuration to which you want to add a custom HIP check, or **Add** a new one.
4. Select **HIP Data Collection**, and then enable the option to **Collect HIP Data**.
5. Under **Custom Checks**, define the following data that you want to collect from hosts running this agent configuration:
   - **To collect information about specific registry keys**: On the **Windows** tab, **Add** the name of a **Registry Key** for which to collect data in the **Registry Key** area. To restrict data collection to a specific **Registry Value**, **Add** and then define the specific registry value(s). Click **OK** to save the settings.
   - **To collect information about running processes**: Select the appropriate tab (**Windows**, **Mac**, or **Linux**) and then **Add** a process to the **Process List**. Enter the name of the process that you want the app to collect information about. You can optionally

Configure HIP Process Remediation to resolve any issues that arise with the process check.

- **To collect information about specific property lists**: On the **Mac** tab, **Add** the **Plist** for which to collect data. To restrict the data collection to specific key values, **Add** the **Key** values. Click **OK** to save the settings.

6. If this is a new agent configuration, Define the GlobalProtect Agent Configurations as desired.
7. Click **OK** to save the configuration.
8. **Commit** the changes.

STEP 3 | (Optional) Exclude categories from collection.

1. On the firewall that is hosting your GlobalProtect portal, select **Network** > **GlobalProtect** > **Portals**.
2. Select the portal configuration that you want to modify.
3. On the **Agent** tab, select the agent configuration from which to exclude categories, or **Add** a new one.
4. Select **Data Collection**, and then verify that **Collect HIP Data** is enabled.
5. Under **Exclude Categories**, **Add** a new exclude category.
6. Select the **Category** you want to exclude from the drop-down.
7. (Optional) If you want to exclude specific vendors and/or products within the selected category rather than excluding the entire category, click **Add**. On the Edit Vendor dialog, select the **Vendor** that you want to exclude, and then click **Add** to exclude specific products from that vendor. When you are done defining that vendor, click **OK**. You can add multiple vendors and products to the exclude list. You can also Configure HIP Exceptions for Patch Management.
8. Repeat steps 5-7 for each category that you want to exclude.
9. If this is a new agent configuration, Define the GlobalProtect Agent Configurations as desired.
10. Click **OK** to save the configuration.
11. **Commit** the changes.

STEP 4 | Create the HIP objects to filter the raw host data collected by the app.

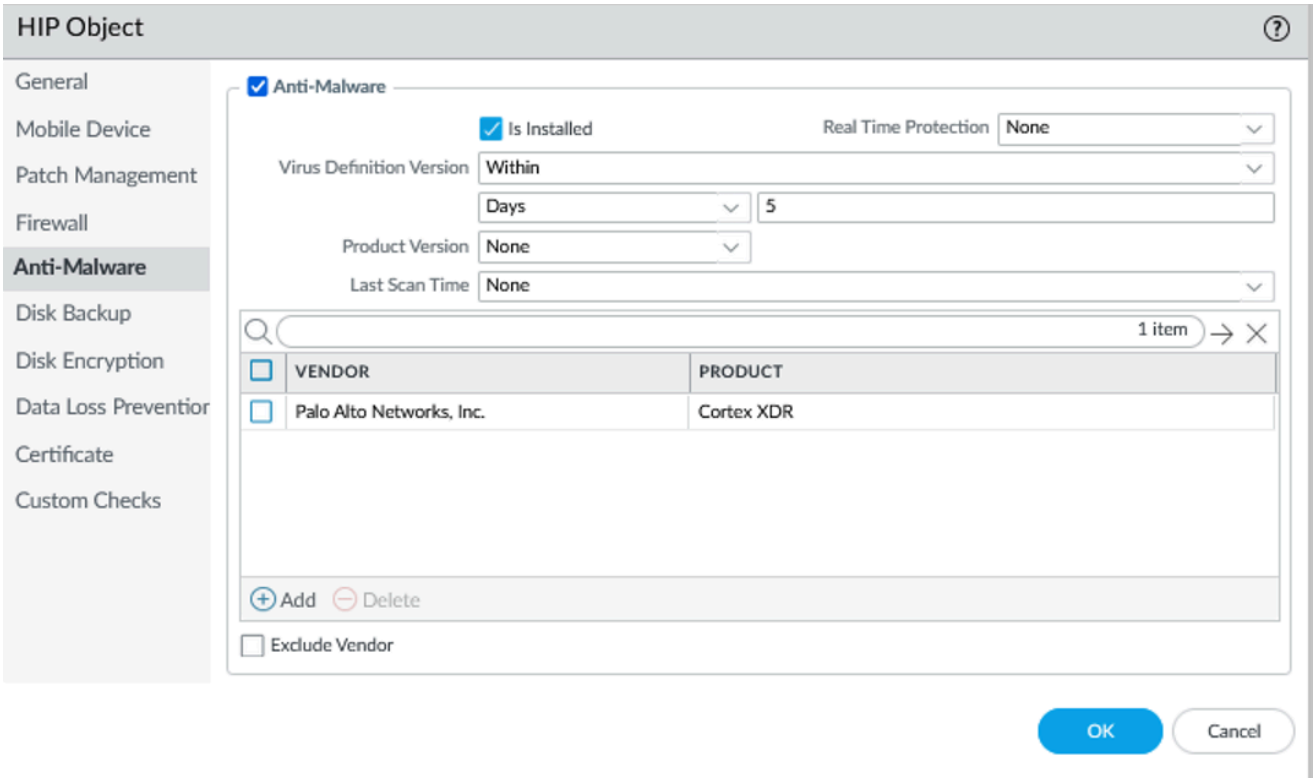
The best way to determine what HIP objects you need is to determine how you will use the host information you collect to enforce policy. Keep in mind that the HIP objects themselves are merely building blocks that allow you to create the HIP profiles that are used in your security policies. Therefore, you may want to keep your objects simple, 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. By doing this, you will have the flexibility to create a very granular (and very powerful) HIP-augmented policy.

For details on a specific HIP category or field, refer to the online help.

1. On the firewall that is hosting your GlobalProtect gateway(s) (or on Panorama if you plan to share the HIP objects among multiple gateways), select **Objects** > **GlobalProtect** > **HIP Objects**, and then **Add** a new HIP object.
2. Enter a **Name** for the object.
3. 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, and then select the **Anti-Malware** check box to enable the corresponding fields. Complete the fields to define the desired matching criteria. For example, 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.



Repeat this step for each category you want to match against in this object. For more information, see Table 8: Table: Data Collection Categories.

4. (Optional) Configure tags to match against the ownership category or compliance status of the endpoint.

   For example, you can create a tag to match against employee-owned endpoints so that you can prevent users from accessing sensitive network resources on their personal endpoints.

   The User-ID agent for Windows queries the MDM server for the following information:

   - Mobile device compliance status.
   - Smart group (ownership category) to which the mobile device belongs.

   The User-ID agent converts this information into tags that are incorporated into the HIP report. You can create HIP objects based on these tag values to enforce HIP-based

security policies for the endpoints in your network. For more information, see Configure Windows User-ID Agent to Collect Host Information.

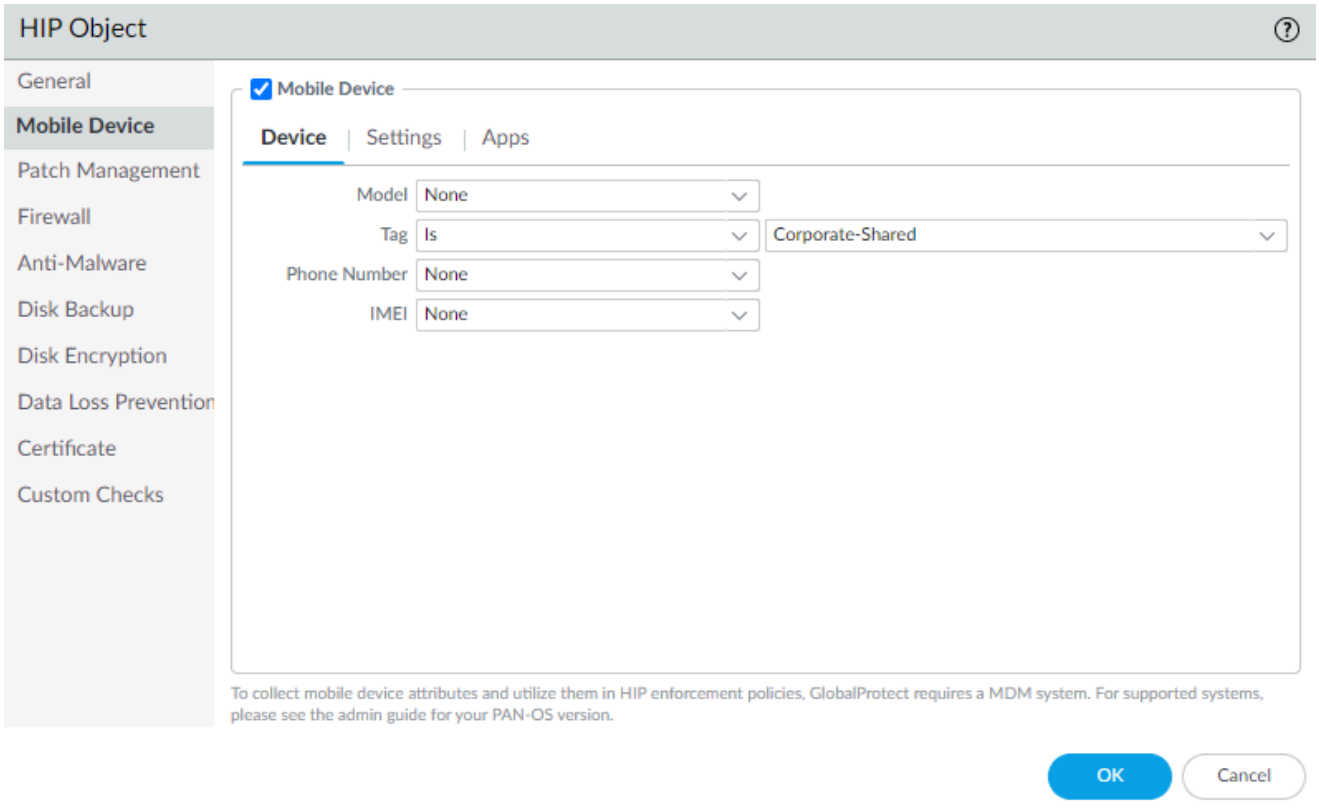
1. Select the **Mobile Device** check box to enable configuration of the **Mobile Device** settings.
2. On the **Device** tab, select a match operator (such as **Contains** or **Is Not**) from the **Tag** drop-down.
3. (Optional) When prompted, enter one of the following ownership category values:

   The ownership category indicates who owns the endpoint.

   - **`Employee Owned`**
   - **`Corporate-Dedicated`**
   - **`Corporate-Shared`**
4. (Optional) When prompted, enter one of the following compliance status values:

   The compliance status indicates whether the endpoint is compliant with the security policies you have defined.

   - **`Compliant`**
   - **`NonCompliant`**
   - **`NotAvailable`**



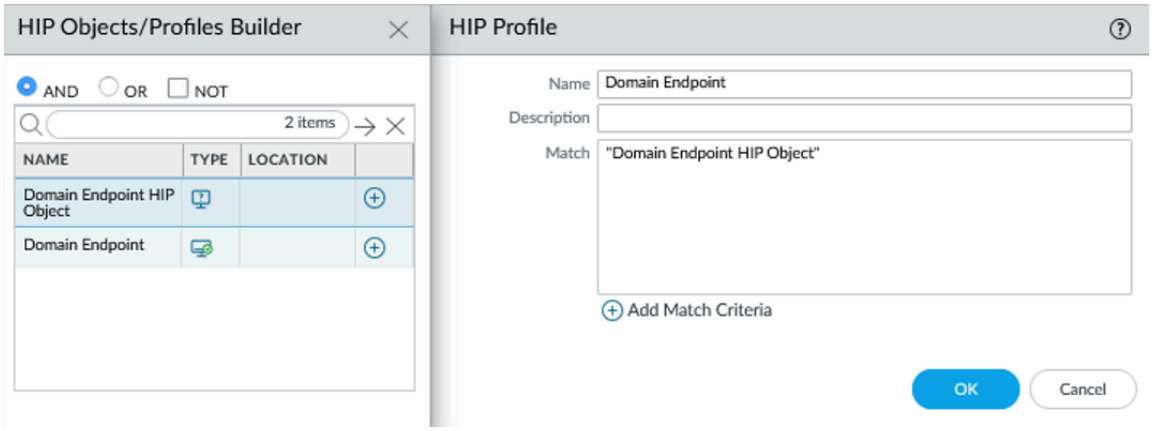
5. Click **OK** to save the HIP object.

6. Repeat these steps to create each additional HIP object you require.
7. **Commit** the changes.

STEP 5 | Create the HIP profiles that you plan to use in your policies.

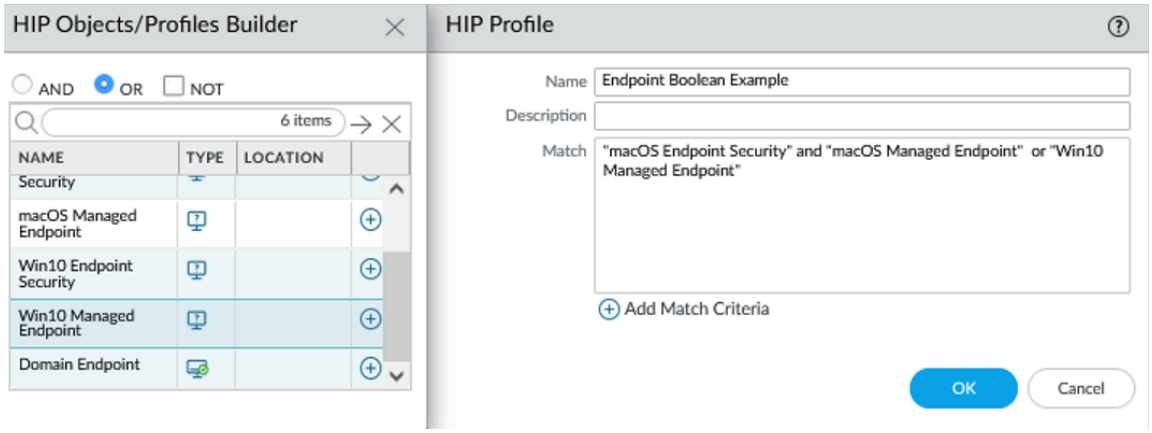
When you create your HIP profiles, you can combine the HIP objects you previously created (as well as other HIP profiles) using Boolean logic, such that when a traffic flow is evaluated against the resulting HIP profile, it will either match or not match. If there is a match, the corresponding policy rule is enforced; if there is not a match, the flow is evaluated against the next rule, as with any other policy matching criteria.

1. On the firewall that is hosting your GlobalProtect gateway(s) (or on Panorama if you plan to share the HIP profiles among multiple gateways), select **Objects** > **GlobalProtect** > **HIP Profiles**, and then **Add** a new HIP profile.
2. Enter a **Name** and **Description** to identify the profile.
3. Click **Add Match Criteria** to open the HIP Object/Profiles Builder.
4. Select the HIP object or profile that you want to use as match criteria, and then click the add icon (⊕) to move it to the **Match** text box on the HIP Profile dialog. If you want the HIP profile to evaluate the object as a match only when the criteria in the object is not true for a flow, select the **NOT** check box before adding the object.



5. Continue adding match criteria for the profile that you are building, making sure to select the appropriate Boolean operator radio button (**AND** or **OR**) between each addition (and, again, using the **NOT** check box when appropriate). The HIP profile can be up to 2048 characters in length.
6. If you are creating a complex Boolean expression, you must manually add the parenthesis in the proper places in the **Match** text box to ensure that the HIP profile is evaluated using the logic you intend. For example, the following HIP profile matches traffic from a host that has either FileVault disk encryption (for macOS systems) or

TrueCrypt disk encryption (for Windows systems), belongs to the required Domain, and has a Symantec antivirus client installed:



7. After you add all your match criteria, click **OK** to save the profile.
8. Repeat these steps to create each additional HIP profile you require.
9. **Commit** the changes.

STEP 6 | Verify that the HIP objects and HIP profiles you created match your GlobalProtect traffic as expected.

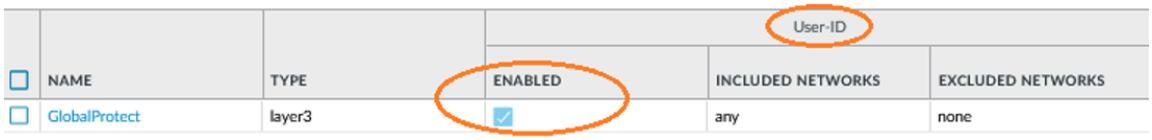
Consider monitoring HIP objects and profiles as a means to monitor the security state and activity of your host endpoints. By monitoring the host information over time, you can better understand where your security and compliance issues are, which can guide you in creating useful policy. For more details, see How Do I Get Visibility into the State of the Endpoints?

On the gateway(s) to which your GlobalProtect users are connecting, select **Monitor** > **Logs** > **HIP Match**. This log shows all of the matches identified by the gateway when evaluating the raw HIP data reported by the app against the defined HIP objects and HIP profiles. Unlike other logs, a HIP match does not require a security policy match in order to be logged.

RECEIVE TIME	SOURCE IPV4	SOURCE IPV6	SOURCE USER	MACHINE NAME	OPERATING SYSTEM	HIP	HIP TYPE
08/11 08:42:55			\casey	DESKTOP-	Windows	Domain Endpoint	profile
08/11 08:42:55			\casey	DESKTOP-	Windows	Windows Endpoint	object
08/11 08:42:37			pre-logon	DESKTOP-	Windows	Domain Endpoint	profile
08/11 08:42:36			pre-logon	DESKTOP-	Windows	Windows Endpoint	object
08/08 13:09:34			pre-logon	DESKTOP-	Windows	Domain Endpoint	profile
08/08 13:09:34			pre-logon	DESKTOP-	Windows	Windows Endpoint	object
08/08 13:07:38			pre-logon	DESKTOP-	Windows	Domain Endpoint	profile
08/08 13:07:38			pre-logon	DESKTOP-	Windows	Windows Endpoint	object
08/08 13:07:36			pre-logon	DESKTOP-	Windows	Domain Endpoint	profile
08/08 13:07:35			pre-logon	DESKTOP-	Windows	Windows Endpoint	object

STEP 7 | Enable User-ID on the source zones containing the GlobalProtect users that send requests requiring HIP-based access controls. You must enable User-ID even if you do not plan on using the user identification feature, otherwise the firewall cannot generate any HIP Match logs entries.

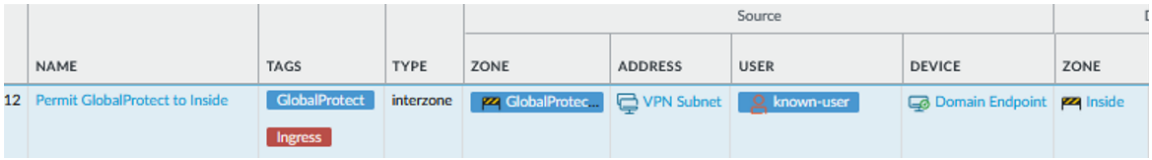
1. Select **Network** > **Zones**.
2. Click the **Name** of the zone on which you want to enable User-ID.
3. **Enable User Identification**, and then click **OK**.



STEP 8 | Create the HIP-enabled security rules on your gateway(s).

As a best practice, you should create your security rules and test that they match the expected flows (based on the source and destination criteria) before adding your HIP profiles. By doing this, you can better determine the proper placement of the HIP-enabled rules within the policy.

1. Select **Policies** > **Security**, and the select the rule to which you want to add a HIP profile.
2. On the **Source** tab, make sure the **Source Zone** is a zone for which you enabled User-ID.
3. On the **Source** tab under **Source Device**, **Add** the **HIP Profiles** used to identify devices (you can add up to 63 HIP profiles to a rule).
4. Click **OK** to save the rule.
5. **Commit** the changes.



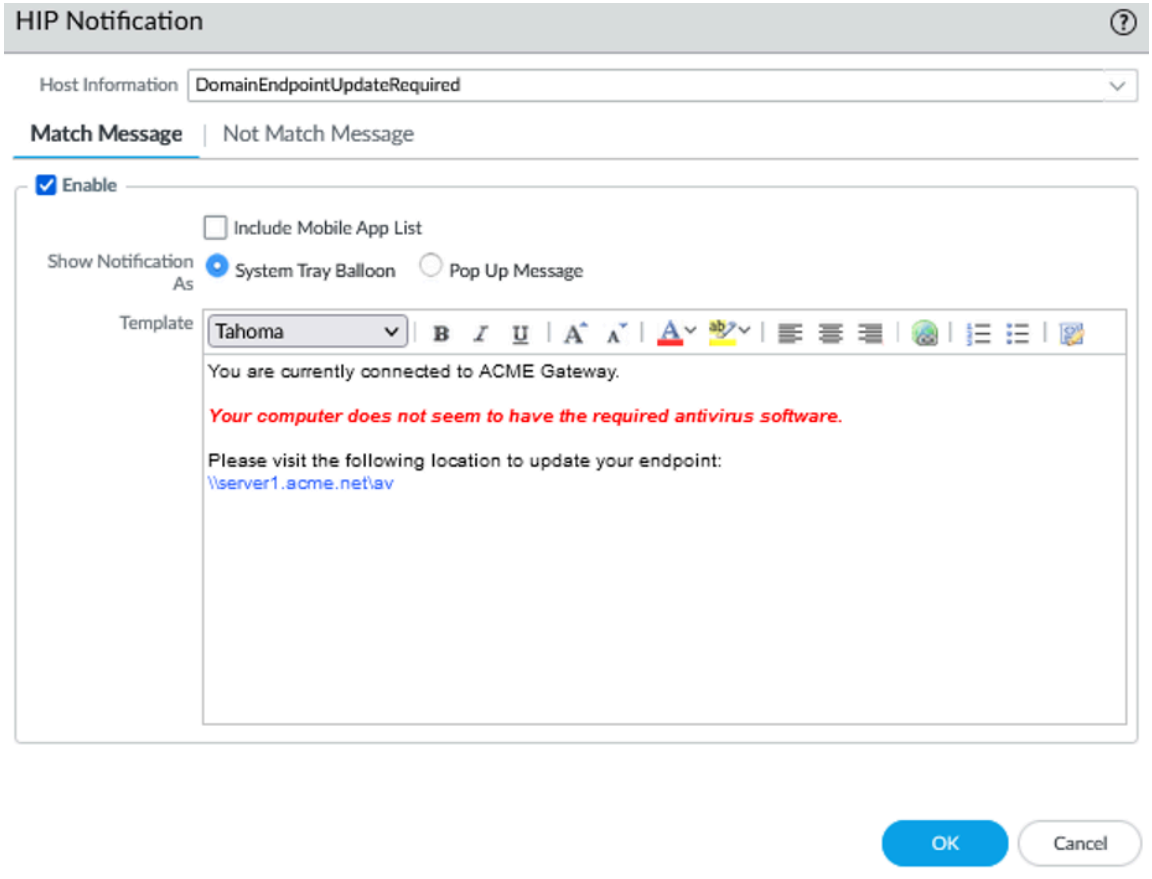
STEP 9 | Define the notification messages end-users see when a security rule with a HIP profile is enforced.

The decision as to when you want to display a notification message (that is, whether to display it when the user's configuration matches a HIP profile in the policy or when it doesn't match), depends largely on your policy and what a HIP match (or non-match) means for the user. That is, does a match mean they are granted full access to your network resources? Or does it mean they have limited access due to a non-compliance issue?

For example, suppose you create a HIP profile that matches if the required corporate antivirus and anti-spyware software packages are not installed. In this case, you might want to create a HIP notification message for users who match the HIP profile, informing them that they need

to install the software. Alternatively, if your HIP profile matches when those same applications are installed, you might want to create the message for users who do not match the profile.

1. On the firewall hosting your GlobalProtect gateway(s), select **Network** > **GlobalProtect** > **Gateways**.
2. Select the gateway configuration for which you want to add HIP notification messages.
3. Select **Agent** > **HIP Notification**, and then click **Add**.
4. Select the HIP profile to which this message applies from the **Host Information** drop-down.
5. Depending on whether you want to display the message when the corresponding HIP profile is matched or not matched, select **Match Message** or **Not Match Message**. In some cases, you might want to create messages for both a match and a non-match, depending on what objects you are matching and what your objectives are for the policy.
6. **Enable** the **Match Message** or **Not Match Message**, and then select whether you want to display the message as a **Pop Up Message** or a **System Tray Balloon**.
7. Enter your message text in the **Template** text box, and then click **OK**. The text box provides both a WYSIWYG view of the text and an HTML source view, which you can toggle between using the **Source Edit** icon. The toolbar also provides various options for formatting your text and creating hyperlinks to external documents (for example, linking users directly to the download URL for a required software program).

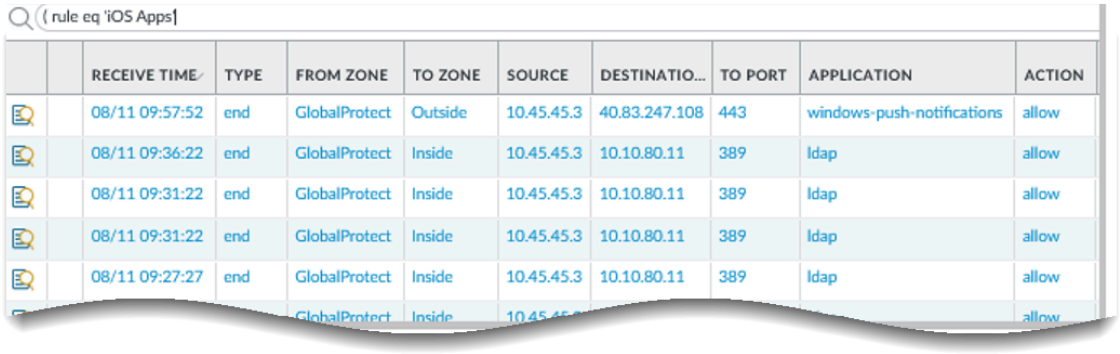


8. Repeat this procedure for each message that you want to define.
9. **Commit** the changes.

STEP 10 | Verify that your HIP profiles are working as expected.

You can monitor the traffic that is hitting your HIP-enabled policies using the **Traffic** log:

1. On the firewall that is hosting your gateway, select **Monitor** > **Logs** > **Traffic**.
2. Filter the log to display only the traffic that matches the rule with the HIP profile you are interested in monitoring. For example, to search for traffic that matches a security rule named “iOS Apps” you would enter **(rule eq 'iOS Apps')** in the filter text box as follows:



Configure HIP Exceptions for Patch Management

Where Can I Use This?	What Do I Need?
• Prisma Access • GlobalProtect Subscription	• Prisma Access Mobile Users license (for use with Prisma Access) • GlobalProtect app version 6.2 or later for Windows, macOS • Content release version 8699-7991 or later

Use the following procedure to configure the GlobalProtect app to exempt specific security patches from being reported as missing from the endpoint HIP report to prevent the endpoint from failing the HIP check in cases where patch updates happen frequently (for example some companies update their patches multiple times a day with threat updates).

STEP 1 | Configure HIP-Based Policy Enforcement.

STEP 2 | Define the patches you want to exclude from the HIP report and the date until which to exclude them.

1. On the firewall that is hosting your GlobalProtect portal, select **Network** > **GlobalProtect** > **Portals**.
2. Select the portal configuration that you want to modify.
3. On the **Agent** tab, select the agent configuration from which to exclude categories, or **Add** a new one.
4. Under **Exclude Categories**, **Add** a new exclude category.
5. Select **patch-management** as the **Vendor** and then **Add** the vendor.
6. Specify the patch name or number <kb-article-id value> and optionally a date <MM/DD/YYYY> until which you want to exclude the patch updates from the HIP report.

   Use the following format:

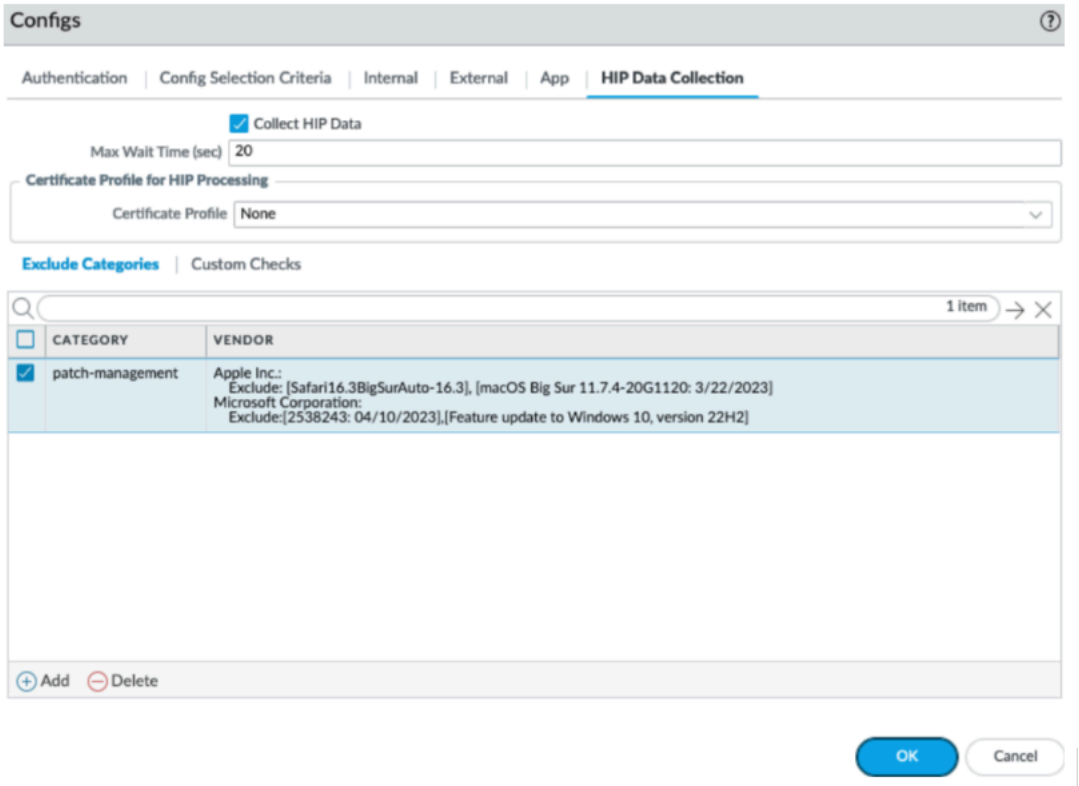
   `Exclude:[kb-article-id1: MM/DD/YYYY], [kb-article-id2: MM/DD/YYYY]`

   Where `kb-article` value is the number in the attribute, example `<kb-article-id>2267602</kb-article-id>` and the `MM/DD/YYYY` specifies the date up to which the patch is excluded from the HIP report. If you do not set a date, the patch will be

excluded from the HIP report indefinitely. If you choose to set a date, the patch will be excluded until the specified date.

The Kb-article id should be in the same format displayed in the logs, for example:

```
<info-url></info-url>
<kb-article-id>2267602</kb-article-id>
<security-bulletin-id></security-bulletin-id>
<severity>2</severity>
```



Repeat this step for each patch you want to exclude from the HIP report.

If you want to exclude all patches from a specific vendor, you would just Configure HIP-Based Policy Enforcement instead of specifying specific patches.

STEP 3 | To save the settings, click **OK** and then **Commit** your changes.

Collect Application and Process Data From Endpoints

The Windows Registry, macOS plist, and Linux process list can be used to configure and store settings for Windows and macOS operating systems, respectively. You can create a custom check that allows you to determine whether an application is installed (has a corresponding registry or plist key) or is running (has a corresponding running process) on a Windows, macOS, or Linux endpoint. Enabling custom checks instructs the GlobalProtect app to collect specific registry information (Registry Keys and Registry Key Values from Windows endpoints) or preference list (plist) information (plist and plist keys from macOS endpoints) or has a corresponding process (name of the process from Linux endpoints). The data that you define to be collected in a custom check is included in the raw Host Information data collected by the GlobalProtect app and then submitted to the GlobalProtect gateway when the app authenticates and connects to the gateway. For more information on defining app settings directly from the Windows Registry, the global macOS plist, or the Linux pre-deployment configuration, see Deploy App Settings Transparently.

To monitor the data collected with custom checks, you can create a HIP object. You can then add the HIP object to a HIP profile to use the collected data to match to endpoint traffic and enforce security rules. The gateway uses the HIP object (which matches to the data defined in the custom check) to filter the raw host information submitted by the app. When the gateway matches the endpoint data to a HIP object, a HIP Match log entry is generated for the data. The HIP profile also allows the gateway to match the collected data to a security rule. If the HIP profile is used as criteria for a security policy rule, the gateway enforces that security rule on the matching traffic.

Use the following steps to enable custom checks to collect data from Windows macOS, or Linux endpoints. This workflow also includes optional steps to create a HIP object and HIP profile for a custom check, which allows you to use endpoint data as matching criteria for security policies to monitor, identify, and act on traffic.

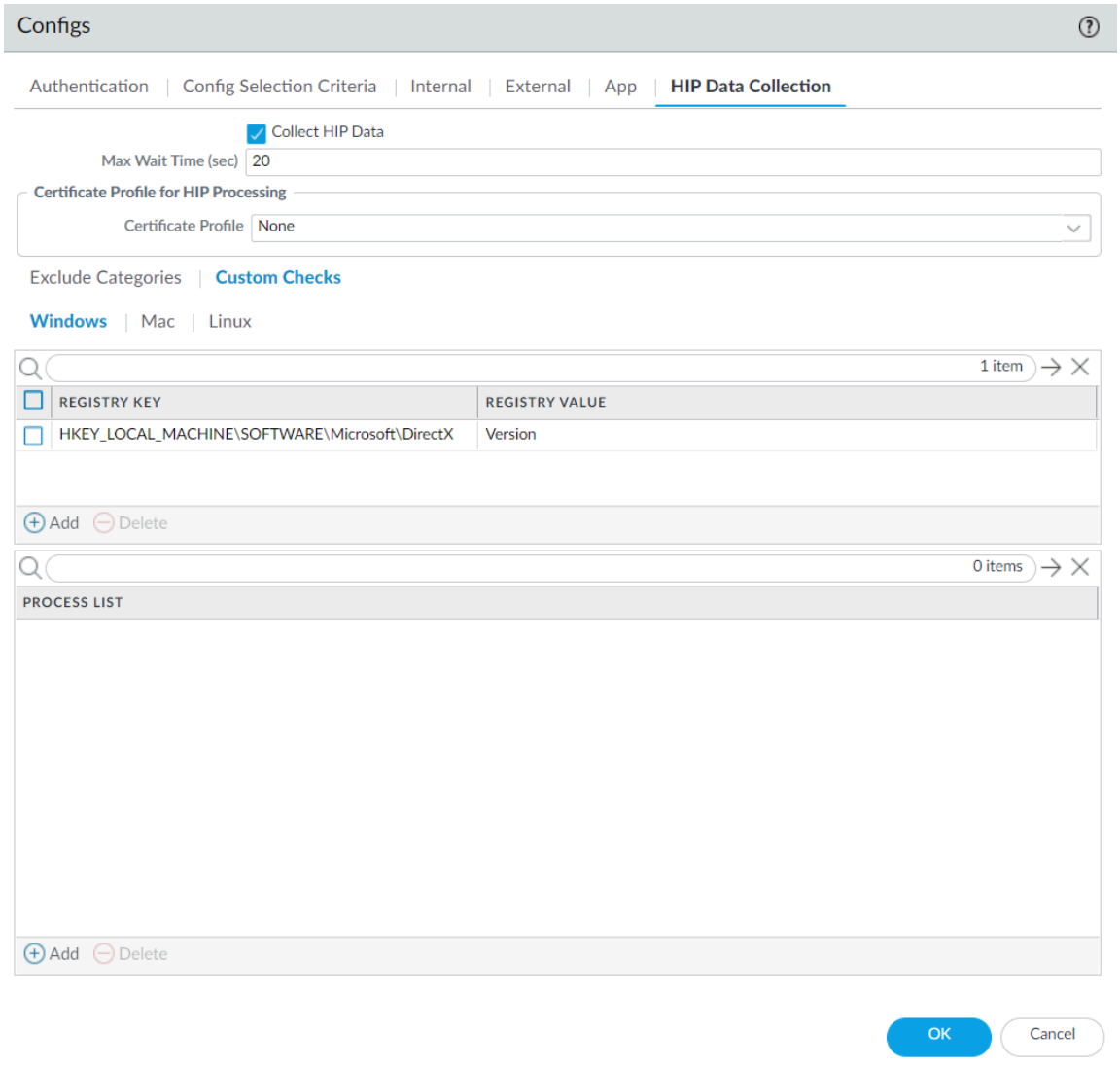
*On Windows, macOS, and Linux devices, when you configure **Custom Checks** such as to collect registry or plist entries, GlobalProtect hides this information in the Host Profile summary of the GlobalProtect app.*

STEP 1 | Enable the GlobalProtect app to collect Windows Registry information from Windows endpoints, plist information from macOS endpoints, or process list information from Linux

endpoints. The type of information collected can include whether or not an application is installed on the endpoint, or specific attributes or properties of that application.

Collect data from a Windows endpoint:

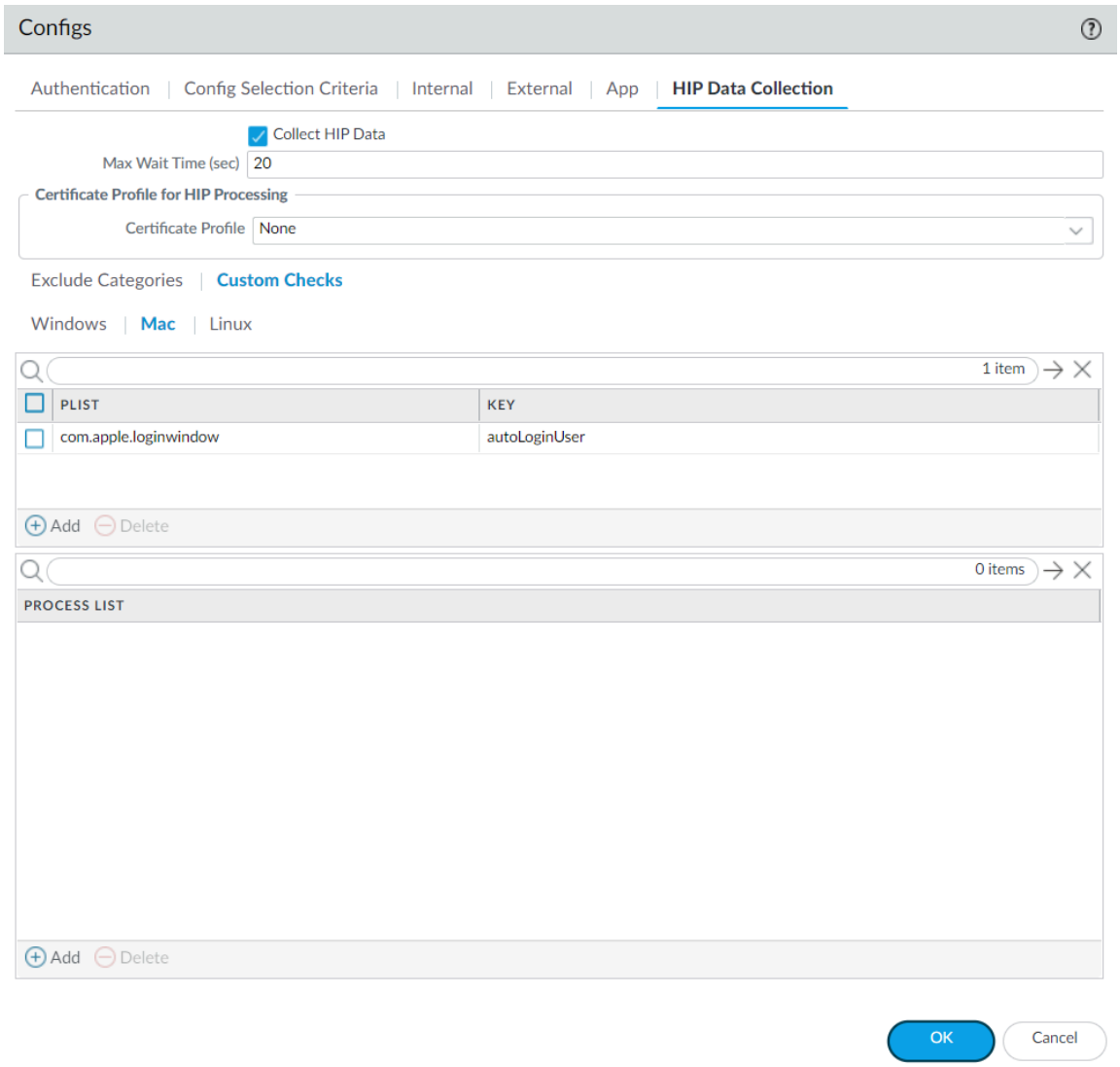
1. Select **Network** > **GlobalProtect** > **Portals**.
2. Select an existing portal configuration or **Add** a new one.
3. On the **Agent** tab, select the agent configuration that you want to modify or **Add** a new one.
4. Select **HIP Data Collection**.
5. Enable the GlobalProtect app to **Collect HIP Data**.
6. Select **Custom Checks** > **Windows**, and then **Add** the **Registry Key** that you want to collect information about. If you want to restrict data collection to a value contained within that Registry Key, add the corresponding **Registry Value**.



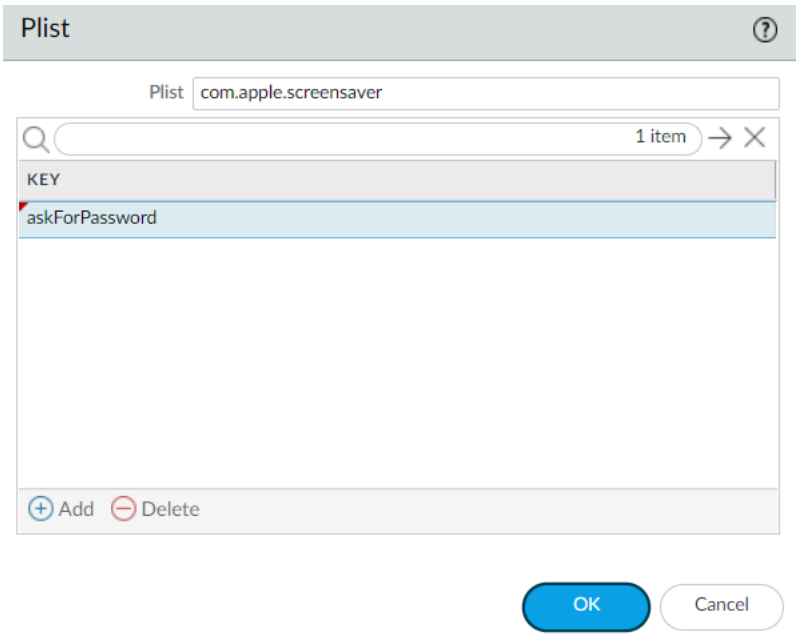
Collect data from a macOS endpoint:

1. Select **Network** > **GlobalProtect** > **Portals**.

2. Select an existing portal configuration or **Add** a new one.
3. On the **Agent** tab, select the agent configuration that you want to modify or **Add** a new one.
4. Select **HIP Data Collection**.
5. Enable the GlobalProtect app to **Collect HIP Data**
6. Select **Custom Checks** > **Mac**, and then **Add** the **Plist** that you want to collect information about and the corresponding plist **Key** to determine if the application is installed.

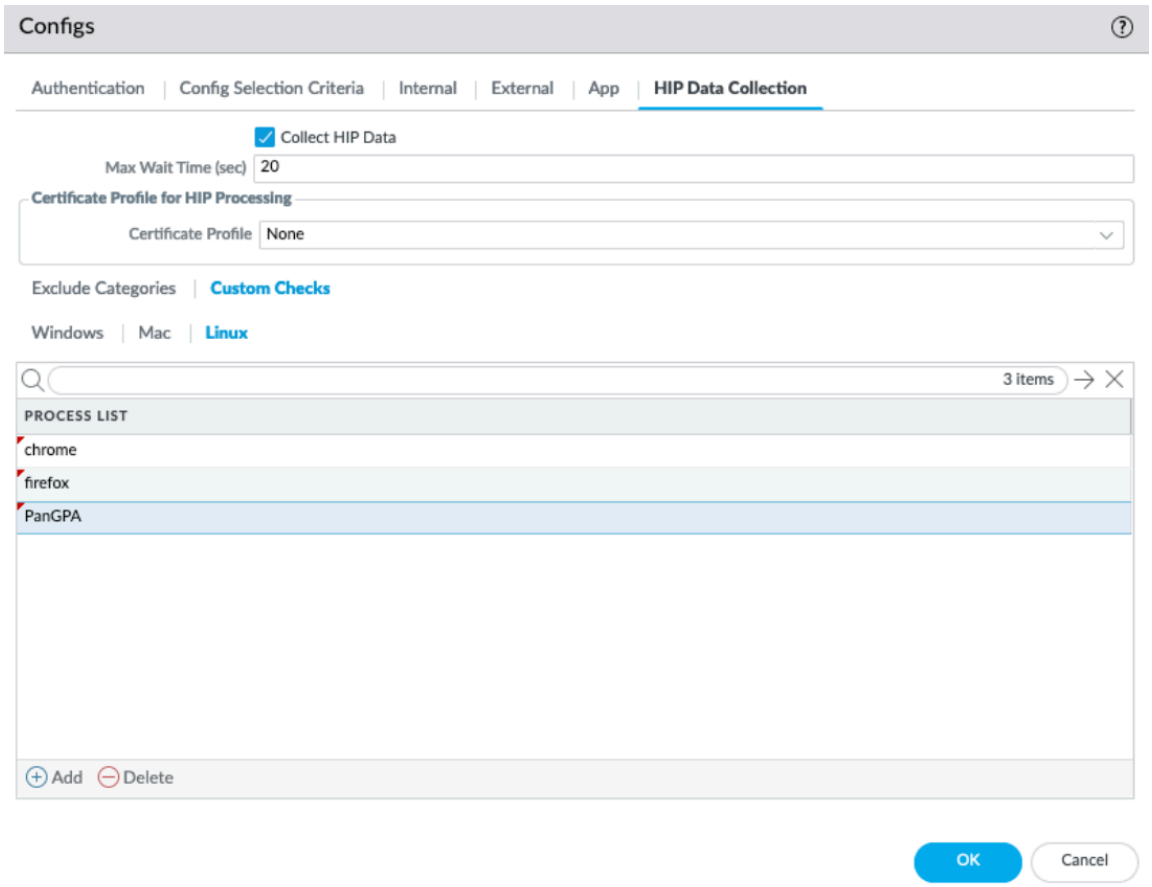


For example, **Add** the **Plist** **`com.apple.screensaver`** and the **Key** **`askForPassword`** to collect information on whether a password is required to wake the macOS endpoint after the screen saver begins:



Collect data from a Linux endpoint:

1. Select **Network** > **GlobalProtect** > **Portals**.
2. Select an existing portal configuration or **Add** a new one.
3. On the **Agent** tab, select the agent configuration that you want to modify or **Add** a new one.
4. Select **HIP Data Collection**.
5. Enable the GlobalProtect app to **Collect HIP Data**.
6. Select **Custom Checks** > **Linux**, and then **Add** the **Process List** that you want to collect information about.



STEP 2 | (Optional) Check if a specific process is running on the endpoint.

1. Select **Network** > **GlobalProtect** > **Portals**.
2. Select an existing portal configuration or **Add** a new one.
3. On the **Agent** tab, select the agent configuration that you want to modify or **Add** a new one.
4. Select **HIP Data Collection**.
5. Enable the GlobalProtect app to **Collect HIP Data**
6. Select **Custom Checks** > **Windows**, **Mac**, or **Linux**.
7. **Add** the name of the process that you want to collect information about to the **Process List**.

STEP 3 | Save the custom check.

Click **OK** and **Commit** the changes.

STEP 4 | (Optional) Create a HIP Object to match to a Registry Key (Windows), plist (macOS), or process list (Linux), which allows you to filter the raw host information collected from the GlobalProtect app to monitor the data for the custom check.

With a HIP object defined for the custom check data, the gateway matches the raw data submitted from the app to the HIP object, and a HIP Match log entry is generated for the data (**Monitor** > **HIP Match**).

For Windows, macOS, and Linux endpoints:

1. Select **Objects** > **GlobalProtect** > **HIP Objects**.
2. Select an existing HIP object or **Add** a new one.
3. On the **Custom Checks** tab, select the check box to enable **Custom Checks**.

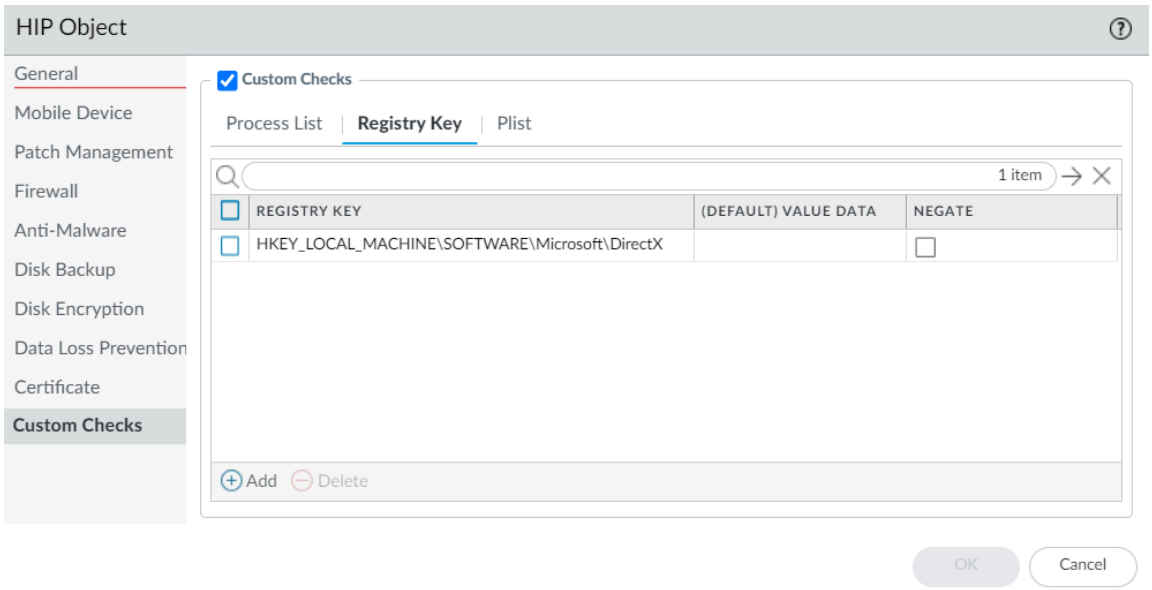
For Windows endpoints only:

1. To check Windows endpoints for a specific registry key, select **Custom Checks** > **Registry Key**, and then **Add** the registry key to match. When prompted, enter the **Registry Key** and then configure one of the following options:
   - To match on the default value data for the registry key, enter the **(Default) Value Data**.
   - To match endpoints that do not have the specified registry key, select **Key does not exist or match the specified value data**.

   *Do not configure both the **(Default) Value Data** and **Key does not exist or match the specified value data** options simultaneously.*
2. To match on specific values within the registry key, select **Custom Checks** > **Registry Key**, and then **Add** the registry key to match. When prompted, enter the **Registry Key**. Click **Add** and then configure one of the following options:
   - To match on specific values within the registry key, enter the **Registry Value** and corresponding **Value Data**.
   - To match endpoints that do not have a specified registry value, enter the **Registry Value** and then select the **Negate** check box.

   *To use this option, do not enter any **Value Data** for your **Registry Key**.*

If you add more than one registry value to your registry key, the GlobalProtect gateway checks endpoints for all specified registry values.

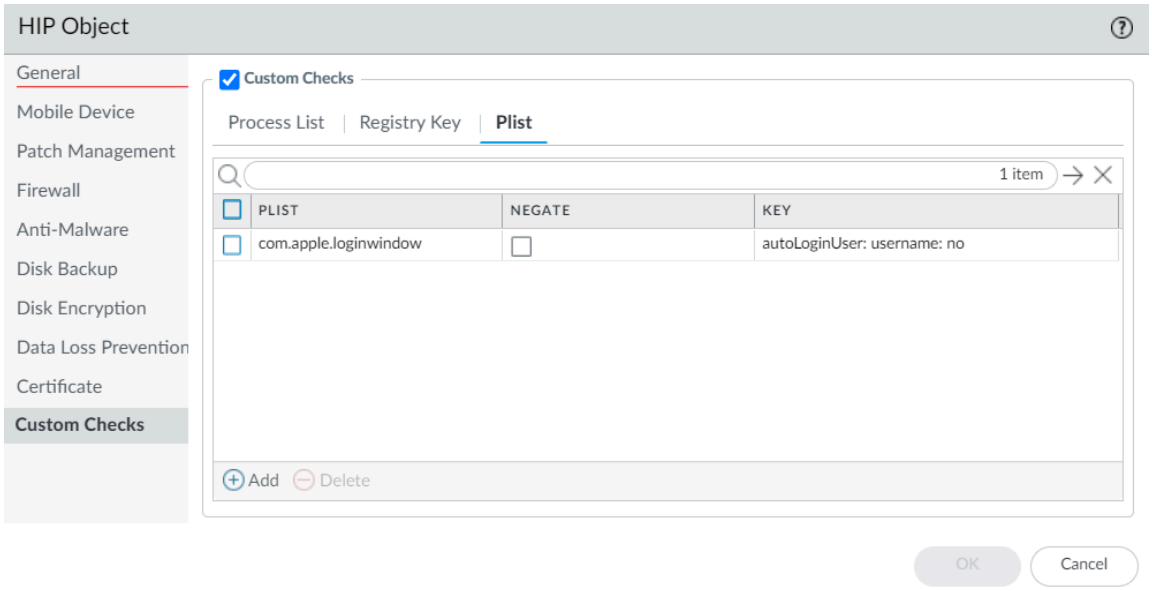


3. Click **OK** to save the HIP object. You can **Commit** the changes to view the data in the **HIP Match** logs at the next device check-in or continue to step 6.

For macOS endpoints only:

1. To check macOS endpoints for a specific plist, select **Plist**, and then **Add** the plist for which you to want to check. When prompted, enter the name of the **Plist**. If you want to match macOS endpoints that do not have the specified plist, enable the **Plist does not exist** option.
2. To match on a specific key-value pair within a plist, select **Plist**, and then **Add** the plist for which you to want to check. When prompted, enter the name of the **Plist** and then **Add** a **Key** and corresponding **Value** to match. Alternatively, if you want to identify

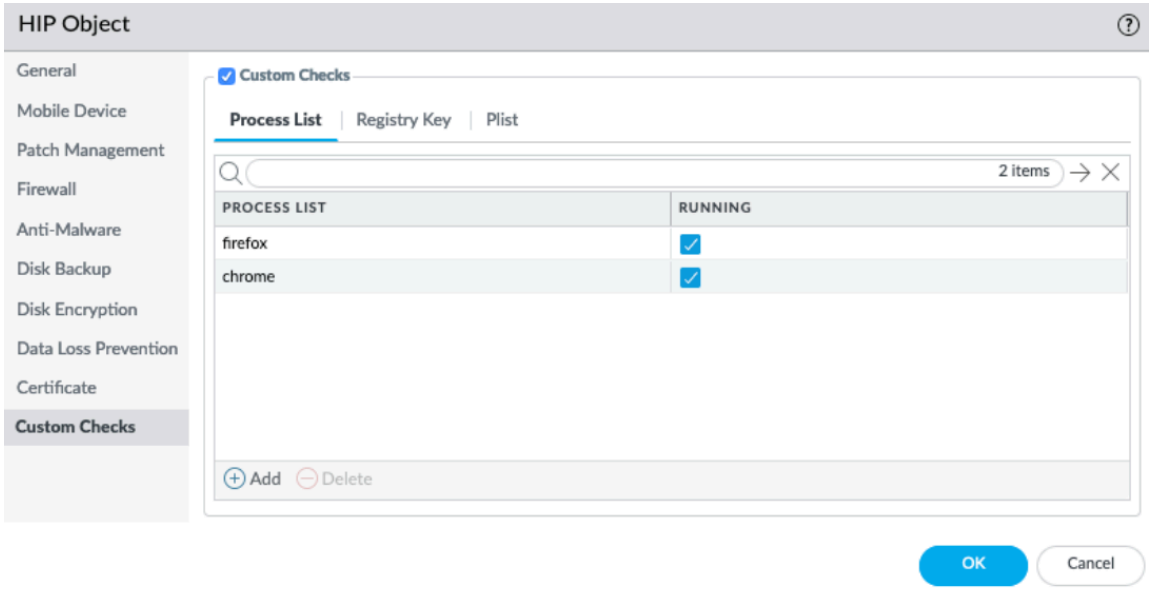
endpoints that do not have a specific key and value, you can select **Negate** after you add the **Key** and **Value**.



3. Click **OK** to save the HIP object. You can **Commit** the changes to view the data in the **HIP Match** logs at the next device check-in or continue to step 6.

For Linux endpoints only:

1. To check if a specific process is running on the Linux endpoint, select **Process List**, and then **Add** the corresponding process for which you to want to check. When prompted, enter the name of the **Process List**.



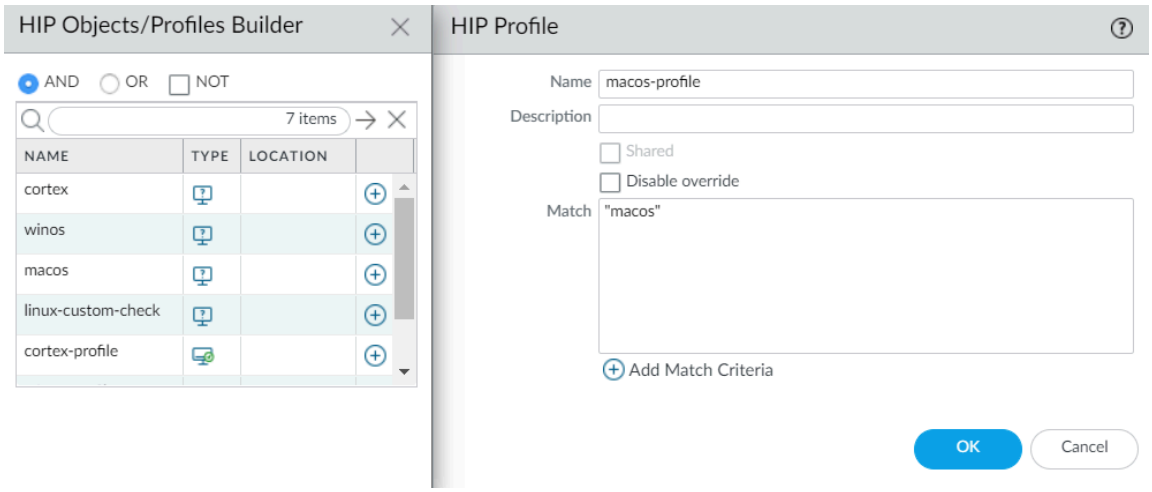
2. Click **OK** to save the HIP object. You can **Commit** the changes to view the data in the **HIP Match** logs at the next device check-in or continue to step 6.

STEP 5 | (Optional) Create a HIP profile to allow the HIP object to be evaluated against traffic.

The HIP profile can be added to a security policy as an additional check for traffic matching that policy. When the traffic is matched to the HIP profile, the security policy rule is enforced on the traffic.

For more details on creating a HIP profiles, see Configure HIP-Based Policy Enforcement.

1. Select **Objects** > **GlobalProtect** > **HIP Profiles**.
2. Select an existing HIP profile or **Add** a new one.
3. Click **Add Match Criteria** to open the HIP Objects/Profile Builder.
4. Select the **HIP object** that you want to use as match criteria, and then click the add ( ) icon to move it to the **Match** area of the HIP Profile.
5. After you add the objects to the new HIP profile, click **OK**, and then **Commit** the changes.



STEP 6 | Add the HIP profile to a security policy so the data collected with the custom check can be used to match to and act on traffic.

Select **Policies** > **Security**, and then select an existing security policy or **Add** a new one. On the **User** tab, **Add** the **HIP Profiles** to the policy. For more details on security policies components and using security policies to match to and act on traffic, see Security Policy.

Configure HIP Process Remediation

Where Can I Use This?	What Do I Need?
• Prisma Access • GlobalProtect Subscription	• Prisma Access Mobile Users license (for use with Prisma Access) • GlobalProtect app version 6.2 or later for Windows and macOS • Content release version 8699-7991 or later

Use the following procedure to configure the GlobalProtect app to run a remediation script whenever a GlobalProtect endpoint fails one or more process checks to help the endpoint recover from a HIP check failures. With this feature enabled, the GlobalProtect app will provide a specified timeout period in which the endpoint can run the remediation script if it fails a process check. After the timeout period expires, the GlobalProtect app resubmits the HIP report.

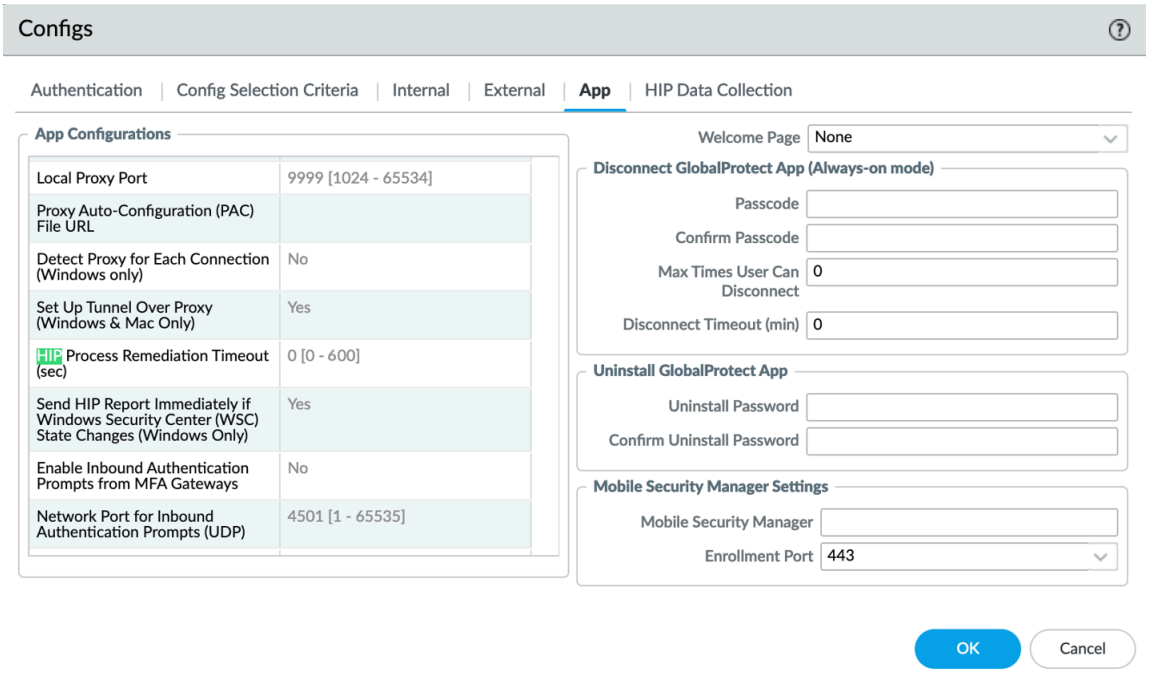
STEP 1 | Set up Configure HIP-Based Policy Enforcement.

The remediation scripts you write should check whether the processes you have set up in the **Custom Checks** are running and, if not, execute the script and start the process.

STEP 2 | Configure a HIP remediation timeout on the portal.

1. Select **Network** > **GlobalProtect** > **Portals**.
2. Select the portal configuration to which you are adding the agent configuration, and then select the **Agent** tab.
3. Select the agent configuration that you want to modify, or **Add** a new one.
4. Select the **App** tab.
5. To enable the HIP remediation feature, set a **HIP Remediation Process Timeout (sec)**.

   By default, this field is set to 0, indicating that the feature is disabled. Enter a value from 1-600 seconds to indicate the amount of time you want to allow for the remediation script to finish.



6. Click **OK** twice to save your app and portal configurations.
7. **Commit** the changes.

STEP 3 | Deploy the remediation script to your endpoints using mobile device management (MDM).

As a best practice, use standard formats for the scripts you deploy (for example, deploy shell scripts on macOS endpoints and batch scripts on Windows endpoints). The name of the script is case sensitive and must use the predefined name and location as follows:

- **Windows**

  Location: `\Program Files\Palo Alto Networks\GlobalProtect\`

  Naming convention: `hip-remediation-script.bat`

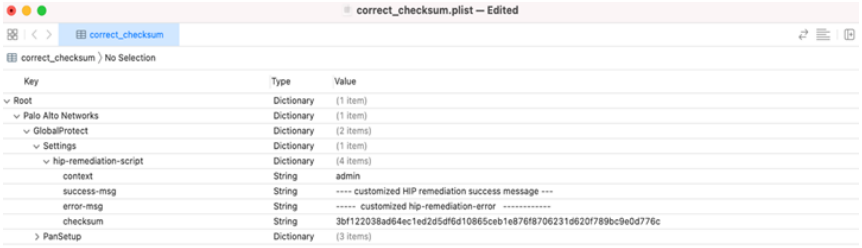
- **macOS**

  Location: `/Applications/GlobalProtect.app/Contents/Resources/`

  Naming convention: `hip-remediation-script.sh`

STEP 4 | (Optional) Customize how the script runs on the endpoint by setting a checksum and/or a custom error message and defining the context in which the script will run.

- **macOS**
  1. Calculate the sha 256 checksum: `shasum -a 256 hip-remediation-script.sh`.
  2. Edit the following values in the plist as needed:
     - `checksum`—Specify the checksum you generated
     - `error-msg`—Enter the custom error message you want to display to the end user when remediation fails
     - `success-msg`—Enter the custom error message you want to display to the end user when remediation succeeds
     - `context`—set to **`admin`** or **`user`** to specify the context in which to run the remediation script. By default, the script runs in the user context.
  3. Replace the GlobalProtect plist by copying the modified.plist to overwrite the default plist: `sudo cp modified.plist /Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`.

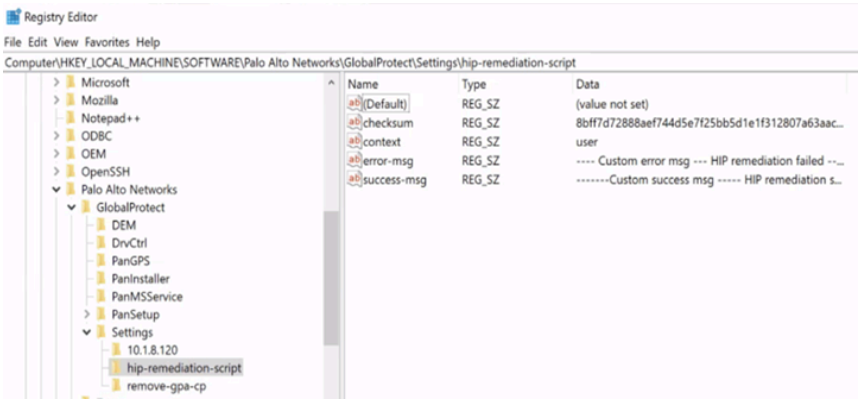
  4. Stop/start PanGPS:

     ```
     launchctl stop com.paloaltonetworks.gp.pangps
     launchctl start com.paloaltonetworks.gp.pangps
     ```

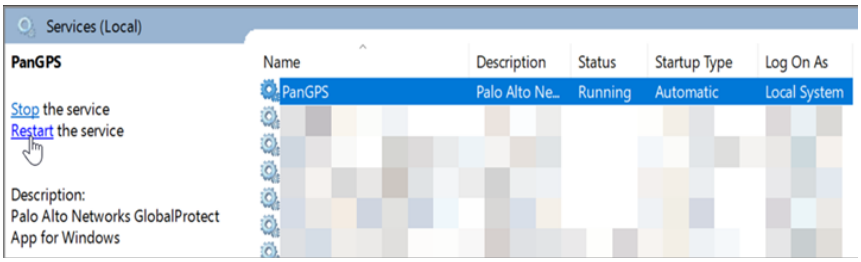
- **Windows**
  1. Create the checksum for the remediation script: `certutil -hashfile hip-remediation-script.bat HASH256 .`
  2. Deploy the registry setting using the Windows default registry editor.

     In the Windows Registry, go to: **\HKEY_LOCAL_MACHINE > SOFTWARE> Palo Alto Networks > GlobalProtect > Settings > hip-remediation-script** and set the following keys:In the Windows Registry, go to: **\HKEY_LOCAL_MACHINE > SOFTWARE> Palo**

Alto Networks > GlobalProtect > Settings > hip-remediation-script and set the following keys:



- `checksum`—Specify the checksum you generated
- `error-msg`—Enter the custom error message you want to display to the end user when remediation fails
- `success-msg`—Enter the custom error message you want to display to the end user when remediation succeeds
- `context`—set to **`admin`** or **`user`** to specify the context in which to run the remediation script. By default, the script runs in the user context.

3. To restart GlobalProtect, in the Windows Services screen, find the **PanGPS** service and click **Restart the service**.
4. 

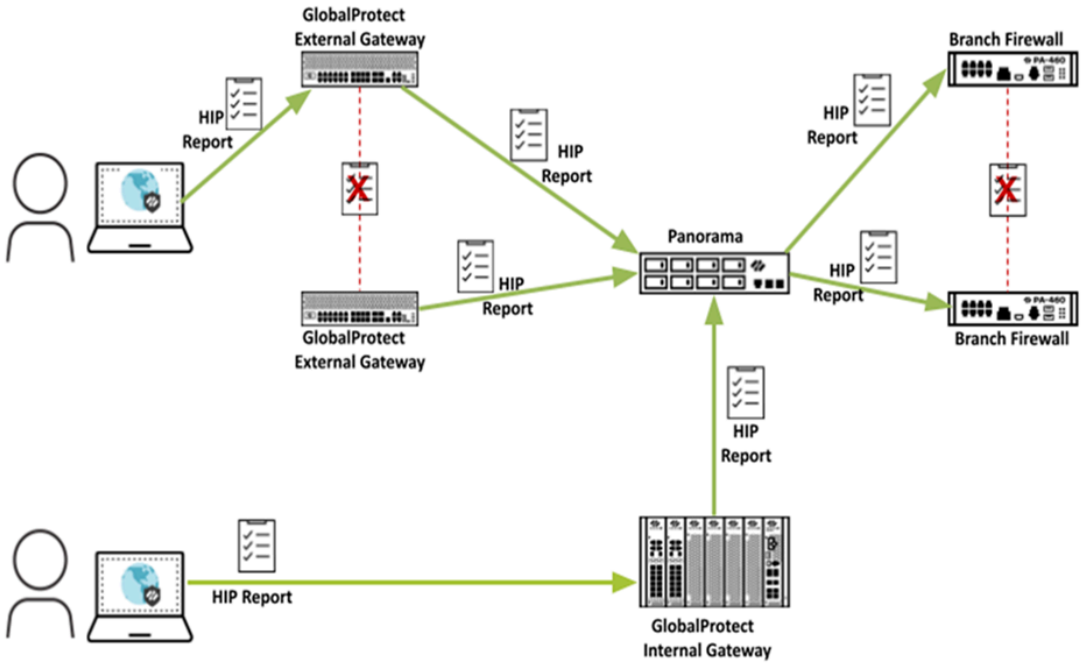
Redistribute HIP Reports

Where Can I Use This?	What Do I Need?
• GlobalProtect Subscription • Prisma Access	• All GlobalProtect gateways and firewalls that redistribute HIP reports must have a GlobalProtect Gateway license (Panorama appliances that redistribute HIP reports do not require a GlobalProtect gateway license.) • This functionality is included with a Prisma Access Mobile User license

To ensure consistent Host Information Profile (HIP) policy enforcement and to simplify policy management, you can distribute HIP reports from the GlobalProtect internal or external gateway to other firewalls, and Panorama appliances in the enterprise. HIP report redistribution can be useful in the following cases:

- You want to apply consistent policies to both internal and external GlobalProtect gateways.
- You want to apply consistent HIP policies for traffic for a specific user that goes through multiple firewalls.

To redistribute HIP reports, use the same deployment recommendations and best practices that you use to redistribute User-ID information. Keep in mind that GlobalProtect internal and external gateways do not support bi-directional HIP redistribution. Therefore, the best practice is to use your Panorama appliance as your redistribution point. In this deployment, you would configure your internal and external gateways to send the HIP reports to Panorama and have Panorama forward them on to your firewalls for consistent policy enforcement across your environment.



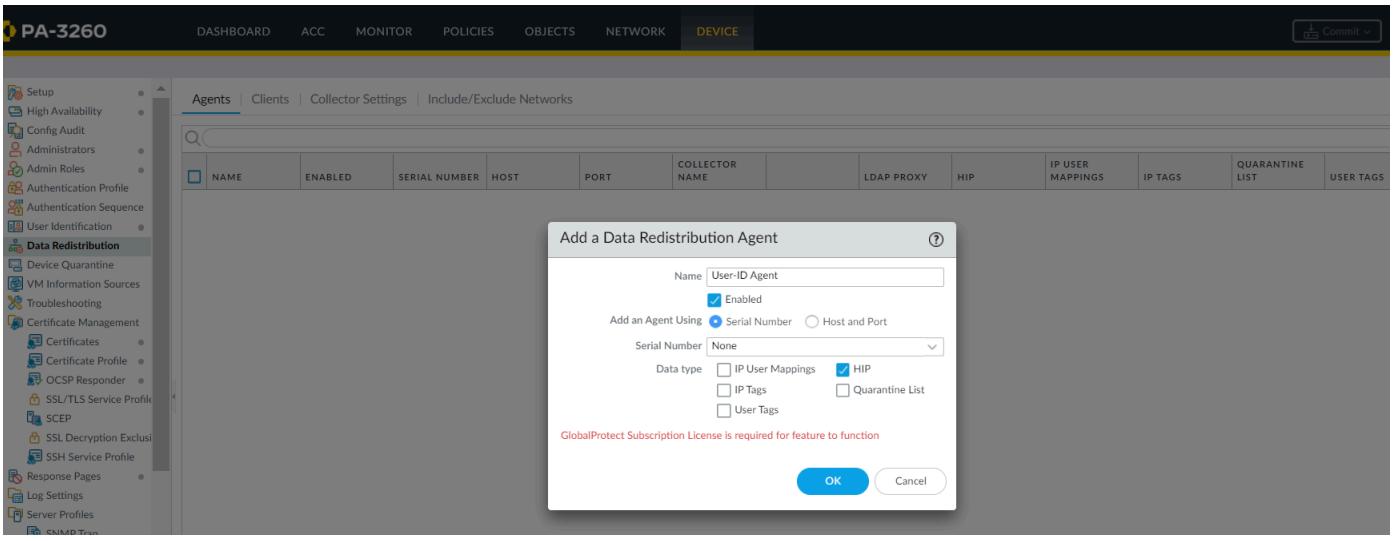
Use the following steps to configure HIP report redistribution.

STEP 1 | Configure HIP-Based Policy Enforcement for your gateways and firewalls.

STEP 2 | Configure HIP report redistribution.

1. Select **Device** > **Agents** > **Data Redistribution**.
2. Select an existing or **Add** a new data redistribution agent.

   The agent must be a Palo Alto Networks next-generation firewall, a GlobalProtect gateway, or a Panorama appliance.
3. Select **HIP Report**.



4. Click **OK**.

STEP 3 | If you use GlobalProtect firewalls or gateways to distribute HIP reports, make sure that the group mapping settings on the firewalls or gateways that you use to redistribute the HIP reports match the following attributes on the firewalls or gateways where you have User-ID configured.

If you use a Panorama appliance to distribute HIP reports, skip this step.

- Configure the user attributes on the HIP report redistribution firewalls or gateways to match the user attributes on the User-ID firewalls or gateways.

  For example, if the firewalls or gateways used for HIP report redistribution has a sAMAccountName of **Primary attribute** and a User Principal Name (UPN) of **Alternate Username 1**, make sure that you configure the same values on the firewalls or gateways where you have configured User-ID.

  *The attributes do not have to be in the same order; for example, if the HIP report redistribution firewall has a sAMAccountName of **Primary attribute** and a UPN of **Alternate Username 1**, you can configure the User-ID firewall with a sAMAccountName of **Alternate Username** and a UPN of **Primary attribute 1**.*
- If your deployment has user domains configured in its group mapping, configure the user domain attributes on the HIP report redistribution firewalls or gateways to match the user domain attributes on the User-ID firewalls or gateways. User domain attributes must be consistent across all firewalls and gateways.
- Configure the common user groups (the user groups on the firewalls and gateways that connect to the same authentication servers and retrieve the same user groups) on the HIP report redistribution firewalls or gateways to match the user groups on the User-ID firewalls or gateways.

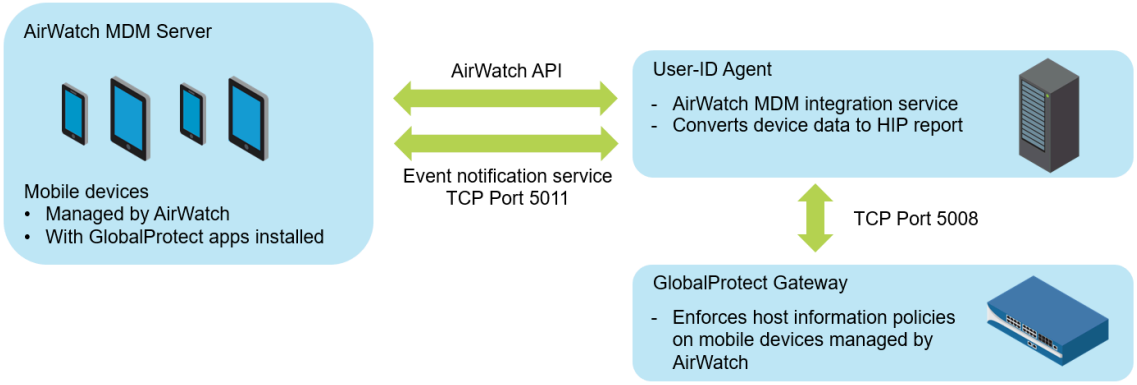
STEP 4 | Redistribute the HIP reports to your managed Panorama appliances, gateways, firewalls, and virtual systems using the same workflow you use to redistribute User-ID information to managed firewalls.

Configure Windows User-ID Agent to Collect Host Information

The Windows-based User-ID agent has been extended to support a new Workspace ONE MDM integration service. This service enables GlobalProtect to use the host information collected by the service to enforce HIP-based policies on devices managed by Workspace ONE. Running as part of the Windows-based User-ID agent, the Workspace ONE MDM integration service uses the Workspace ONE API to collect information from mobile endpoints that are managed by VMware Workspace ONE and translate this data into host information.

For Android endpoints managed by Workspace ONE, this feature supports Android for Work endpoints but does not support other types of Android endpoints.

- MDM Integration Overview
- Information Collected
- System Requirements
- Configure GlobalProtect to Retrieve Host Information
- Troubleshoot the MDM Integration Service



MDM Integration Overview

The MDM integration service included with the Windows-based User-ID agent performs a full HIP query to the Workspace ONE MDM server to retrieve the complete host information for a mobile device. GlobalProtect apps on the mobile devices also send HIP information to the gateway, which merges HIP information from the GlobalProtect apps and the MDM integration service. When a mobile device running the GlobalProtect app is connected to a GlobalProtect gateway, GlobalProtect can apply security policies with host information profiles.

You can configure the MDM integration service to fetch Workspace ONE device information at regular intervals and push this information to the GlobalProtect gateways. In addition, the service can monitor Workspace ONE event notifications and fetch updated device information when Workspace ONE events (such as compliance changes) occur.

Information Collected

The following table shows how information collected from endpoints that are managed by Workspace ONE are translated into HIP report attributes. The mapping is done automatically.

Workspace ONE Attributes	HIP Report Attributes
Device Information	
SerialNumber	serial-number
MacAddress	wifimac
Imei	IMEI
OperatingSystem	version
Model	model
DeviceFriendlyName	devname
IsSupervised	supervised
Udid (Unique Device Identifier)	udid
UserName	user
LastEnrolledOn	enroll-time
Platform	os
EnrollmentStatus	managed-by-mdm
LastSeen	last-checkin-time
ComplianceStatus (User-ID agent 8.0.3 and later)	Compliant NonCompliant NotAvailable
Ownership (User-ID agent 8.0.3 and later)	Employee Owned Corporate-Dedicated Corporate-Shared
Security Information	
DataProtectionEnabled	disk-encrypted

Workspace ONE Attributes	HIP Report Attributes
IsPasscodePresent	passcode-set
IsPasscodeCompliant	passcode-compliant
Network Information	
DataRoamingEnabled	data-roaming
GPS Coordinates	
Latitude	latitude
Longitude	longitude
SampleTime	last-location-time
Application Details	
ApplicationName	appname
Version	version
ApplicationIndentifier	package

System Requirements

Workspace ONE MDM integration service requires the following software:

Software	Minimum Supported Version
User-ID Agent	8.0.1
PAN-OS	7.1.0
GlobalProtect App for Android	4.0.0
GlobalProtect App for iOS	4.0.1
Workspace ONE Server	8.4.7.0
Windows Server	2008 and 2012 2016 with User-ID Agent 8.0.4 and PAN-OS 8.0.4

Configure GlobalProtect to Retrieve Host Information

Use the following instructions to configure GlobalProtect to retrieve host information from devices managed by Workspace ONE.

STEP 1 | Install the User-ID Agent. The User-ID agent must be in a location that enables secure connections to the VMware Workspace ONE Mobile Device Management (MDM) system.

The Workspace ONE MDM integration service is included with the PAN-OS Windows-based User-ID agent.

STEP 2 | Configure SSL authentication between the Windows-based User-ID agent and the GlobalProtect gateway.

When you configure SSL authentication, make sure:

- The server certificate configured on the Windows-based User-ID agent has the same Common Name (CN) as the hostname/IP address of the User-ID agent host.
- The server certificate is trusted by the firewall (included in the trusted CA list in the MDM configuration on the firewall).
- The root certificate authority (CA) certificate of the MDM client certificate configured on the firewall must be imported into Windows trust store of the Windows server.
  1. Obtain a server certificate and private key for authentication between the Windows-based User-ID agent and the GlobalProtect gateway. The certificate bundle must be in PEM format that contains a PEM certificate, full certificate chain, and private key.
  2. Open the Windows-based User-ID agent and select **Server Certificate**.
  3. **Add** the server certificate.
- **Browse** to the certificate file and **Open** the file to upload the certificate to the Windows-based User-ID agent.
- Enter a **Private Key Password** for the certificate.
- Click **OK.**

The agent verifies the certificate is valid and stores the encryption password of the private key in the host machine's Windows credential store.

If installation is successful, detailed information about the certificate (including common name, expiration date, and issuer) appears on the **Server Certificate** tab.

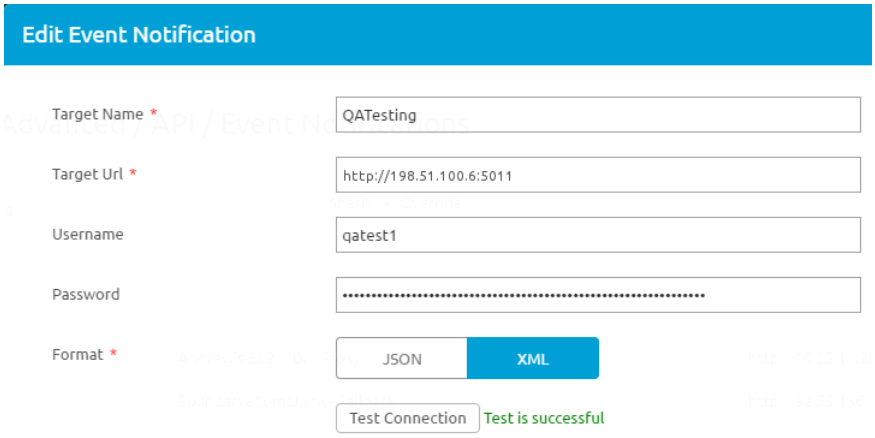
1. Restart the Windows-based User-ID agent.

STEP 3 | Configure the MDM integration service on the Windows-based User-ID agent.

1. Select **MDM Integration** in the Windows-based User-ID agent.
2. Specify a **Gateway Connection TCP Port** for TCP communications. The Windows-based User-ID agent listens at this port for all MDM-related messages. The default port is 5008. To change the port, specify a number from 1 to 65535.
3. On the **Setup** tab, click **Edit**.
4. Choose **Workspace ONE** for the **MDM Vendor**.

STEP 4 | Specify the **MDM Event Notification** settings to monitor and collect Workspace ONE events (for example, device enrollment, device wipe, and compliance changes). When an event occurs, the MDM integration service fetches the updated device information from the Workspace ONE API and pushes this information to all configured GlobalProtect gateways.

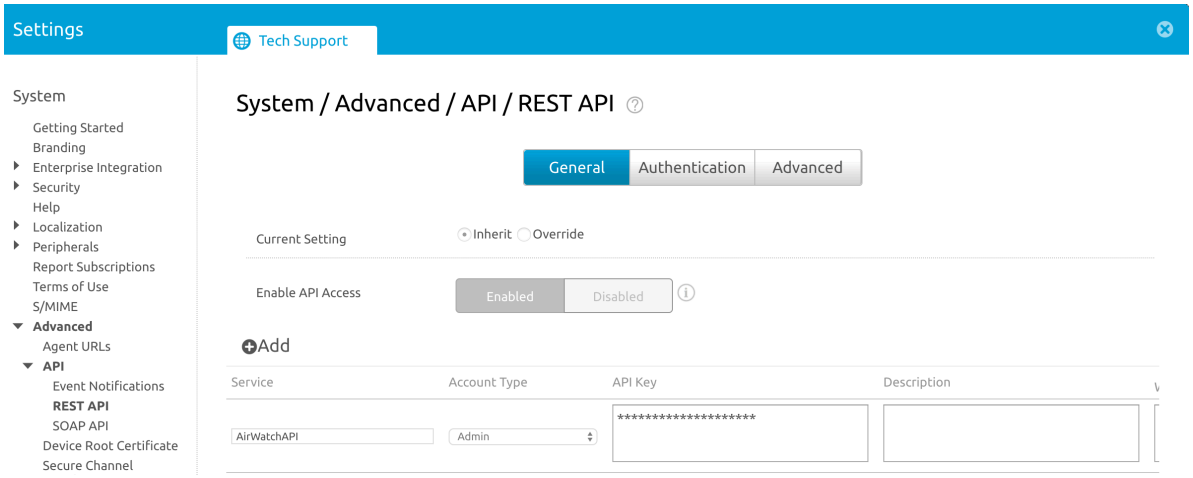
*For **MDM Event Notification**, make sure the values you enter here are also configured in the Workspace ONE console under **Groups & Settings** > **All Settings** > **System** > **Advanced** > **API** > **Event Notifications**.*



- Set the **TCP Port** for communicating with the event notification service. Use this format: **`http://<external_hostname>/<ip_address>:<port>`** where **`<ip-address>`** is the IP address for the MDM integration service. The default port is 5011. To change the port, specify a number from 1 to 65535.
- For event notification, enter the **Username** and **Password** credentials needed to authenticate incoming requests.
- Enter the **Permitted IP** addresses to access MDM events. This is a comma-separated list of IP addresses from where MDM events are posted. For example, the IP address of the Workspace ONE server. Contact your Workspace ONE Support team for guidance on which IP addresses to specify.

STEP 5 | Add **MDM API Authentication** settings to connect with the Workspace ONE API.

- Enter the **Server Address** of the Workspace ONE MDM server to which the Windows-based User-ID agent will connect. For example, **`api.awmdm.com`**.
- Enter the **Username** and **Password** credentials needed to access the Workspace ONE MDM API.
- Enter the **Tenant Code.**This is a unique hexadecimal code number required to access the Workspace ONE MDM API. On the Workspace ONE console, you can find the tenant code at **System** > **Advanced** > **API** > **REST API** > **API Key**.



- Enter the **Mobile Device State Retrieval Interval**. This setting controls how often host information is retrieved from devices managed by Workspace ONE. The default interval is 30 minutes. To change the interval, specify a number from 1 to 600.

STEP 6 | **Commit** your changes.

STEP 7 | Click **Test Connection** to make sure the Windows-based User-ID agent can connect to the Workspace ONE API.

STEP 8 | Configure the GlobalProtect gateway to communicate with the MDM integration service to retrieve the HIP reports for the devices managed by Workspace ONE.

1. In the PAN-OS web interface, select **Network** > **GlobalProtect** > **MDM**.
2. **Add** the following information about the MDM integration service.

- **Name**—Enter a name for the MDM integration service (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
- (Optional) Select the virtual system to which the gateway belongs.
- **Server**—Enter the IP address or FQDN of the interface on the Workspace ONE MDM integration service where the gateway connects to retrieve HIP reports. Ensure that you have a service route to this interface.
- **Connection Port**—Enter the connection port where the MDM integration service listens for HIP report requests. The default port is 5008. To change the port, specify a number from 1 to 65535.
- **Client Certificate**—Choose the client certificate for the gateway to present to the MDM integration service when it establishes an HTTPS connection. You can choose a client certificate from the drop down, or import a new client certificate. The **Certificate Purpose** must indicate that it is a client authentication certificate.

The root certificate authority (CA) certificate of the client certificate must be imported into the Windows trust store of the Windows server where the User-ID Agent is installed.

1. **Add** the root CA certificate associated with the server certificate installed on the MDM integration service host. You need both the root CA certificate and the server certificate to establish a secure connection between the gateway and the MDM integration service. You can choose a root CA certificate from the drop down, or *Import* a new certificate.
2. Click **OK**.
3. **Commit** your changes.

STEP 9 | Check your connection to make sure Workspace ONE device data is transferred to GlobalProtect.

1. Open the Windows-based User-ID agent and select **MDM Integration** > **Mobile Devices**. You should see a list of unique device IDs and user names for all the devices managed by Workspace ONE.
2. (Optional) You can **Filter** the list to find a specific **Mobile Device**.
3. (Optional). Select a device from the list of device IDs and click **Retrieve Device State** to extract the latest information about the device and see how it maps to host information profiles on the GlobalProtect gateway.

Troubleshoot the MDM Integration Service

Follow these instructions if you have trouble with event notifications or trouble authenticating to the Workspace ONE REST API.

- Event notifications from the Workspace ONE MDM server are not received by the MDM integration service.
  1. Set the **Debug** option (in the **File** menu) to **Debug** or **Verbose**.
  2. Go the User-ID agent installation folder on the Windows server, and then open the `MaDebug` file. Look for messages similar to the following:

     ```
     The address x.x.x.x
     is not in the permitted ip list for event notifications.
     ```

  3. Add this IP address as a **Permitted IP** address (**MDM Integration** > **Setup** > **Permitted IP**).

- Authentication to the Workspace ONE REST API is unsuccessful.

  Make sure that:

  - The credentials used for the MDM integration service to authenticate to the Workspace ONE MDM service are valid.
  - The user account used to access the Workspace ONE REST API has API access permissions and read-only permissions (at minimum) to data for the mobile devices and users managed by Workspace ONE.
  - The **Tenant Code** (API key) is correctly associated with the user account. Remove all unused API keys.

Quarantine Devices Using Host Information

GlobalProtect allows you to either Manually Add and Delete Devices From the Quarantine List or Automatically Quarantine a Device add compromised devices to a quarantine list. After you quarantine the device, you can Use GlobalProtect and Security Policies to Block Access to Quarantined Devices from that device using GlobalProtect. You can also restrict traffic to a compromised device, from a compromised device, or both. If you use a Panorama appliance, you can also Redistribute Device Quarantine Information from Panorama to other next-generation firewalls. Use the following topics to learn how to quarantine a device, including the GlobalProtect subscription license requirements, and how to redistribute the quarantine information.

- Identification and Quarantine of Compromised Devices Overview and License Requirements
- View Quarantined Device Information
- Manually Add and Delete Devices From the Quarantine List
- Automatically Quarantine a Device
- Use GlobalProtect and Security Policies to Block Access to Quarantined Devices
- Redistribute Device Quarantine Information from Panorama

Identification and Quarantine of Compromised Devices Overview and License Requirements

GlobalProtect makes it easier for you to block compromised devices from your network by identifying a compromised device with its Manually Add and Delete Devices From the Quarantine List and, optionally, serial number instead of its source IP address. This ability can be preferable to blocking a compromised endpoint from a network based on its IP address, because if a device's IP address changes (for example, if a user moves their endpoint from a work location to their home), security policies based on IP addresses could allow the endpoint back on the network.

After you identify a device as compromised (for example, if a device has been infected with malware and is performing command and control actions), you can manually add the device's Host ID to a quarantine list and configure GlobalProtect to prevent users from connecting to the GlobalProtect gateway from a quarantined device. You can also automatically quarantine the device using log forwarding profiles with security policies or HIP Match log settings.

Starting with Android 8.0 version, GlobalProtect app is unable to retrieve device serial number as GlobalProtect app is not device owner app or profile owner app. In this case, you can use ANDROID_ID as the device serial number. ANDROID_ID is application specific on an Android device and the ID may change when resetting your Android device to factory settings.

Before you begin to quarantine devices, make sure that your GlobalProtect users are running a minimum GlobalProtect app version of 5.1. In addition, make sure that a valid GlobalProtect subscription license is present on the firewall in order for the firewall to be able to add compromised devices to the quarantine list. The GlobalProtect subscription license requirements for this feature are enforced as described in the following list.

- The firewall requires a GlobalProtect subscription license to manually or automatically add devices to the quarantine list. You receive the following error message if you attempt to add a

device without a license: `The device cannot be quarantined. You must have a valid GlobalProtect subscription to add the device to the quarantine list.`

However, you can delete quarantined devices from the quarantine list without a license.

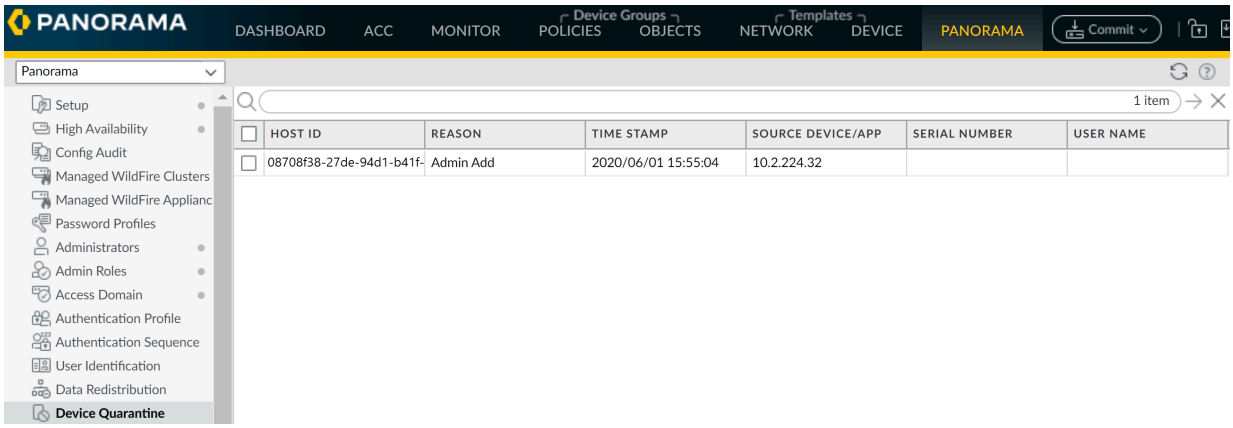
- If your GlobalProtect subscription license expires, the quarantine list is retained and not deleted.

  GlobalProtect performs a license check hourly.
- If you do not have a valid GlobalProtect license and one of the following conditions is true, your firewall or Panorama displays a warning message when you commit the change:
  - You selected **Quarantine List** in a Data Redistribution Agent.
  - You selected **Quarantine** as a built-in action for a **Log Forwarding Profile**.

View Quarantined Device Information

You view quarantined device information from the **Device Quarantine** page. The page's location differs if you are viewing it from a next-generation firewall or a Panorama appliance.

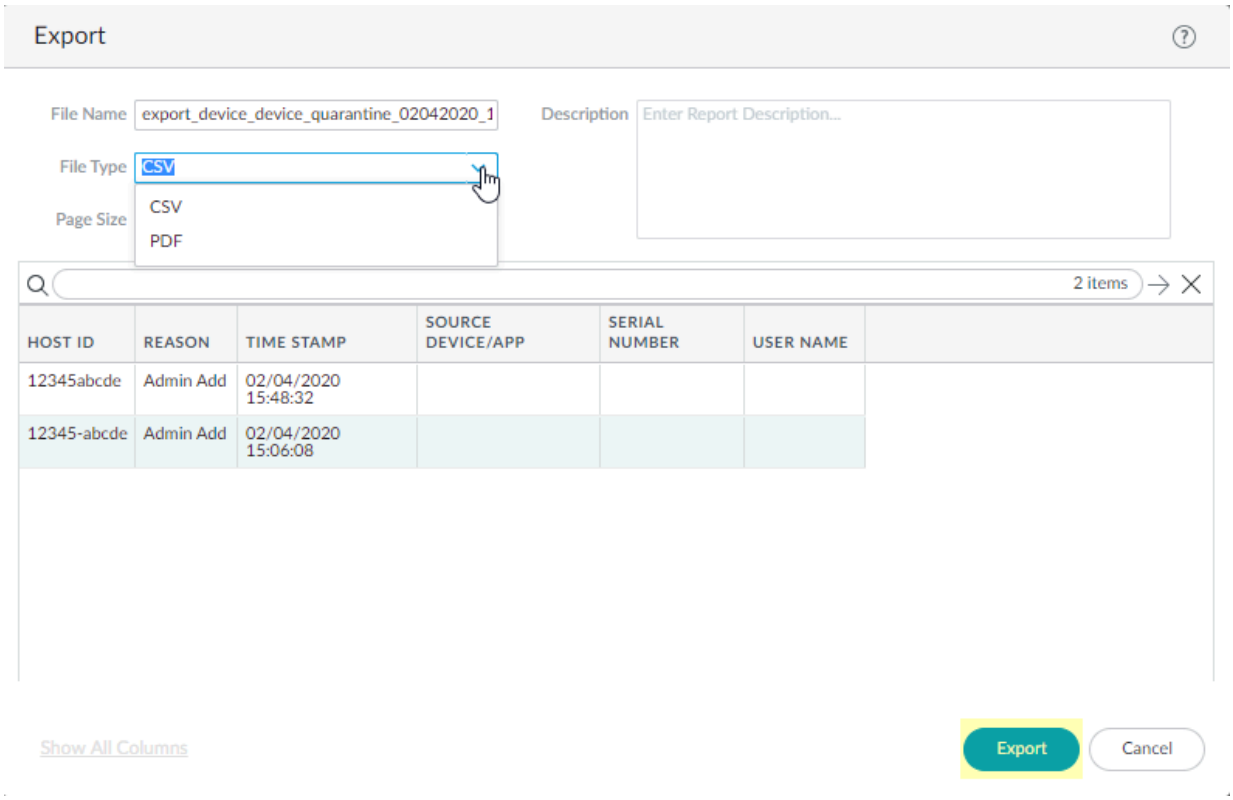
- In next-generation firewalls, view the list of quarantined devices by selecting **Device** > **Device Quarantine**.
- For Panorama appliances, view the **Device** > **Device Quarantine** by selecting **Panorama** > **Device Quarantine**.



- You can also view GlobalProtect quarantine activity from the ACC. The **GlobalProtect Quarantine Activity** tab in the ACC contains a pane, **GlobalProtect Quarantine Activity**, that displays a chart view summary of devices that have been quarantined. Use the toggle at the top of the chart to view the quarantined devices by the actions that caused GlobalProtect to

quarantine the device, the reason GlobalProtect quarantined the device, and the location of the quarantined devices.

- To export the list of quarantined devices to a pdf or csv file, select **PDF/CSV** at the bottom of the **Device Quarantine** page to open the **Export** page.

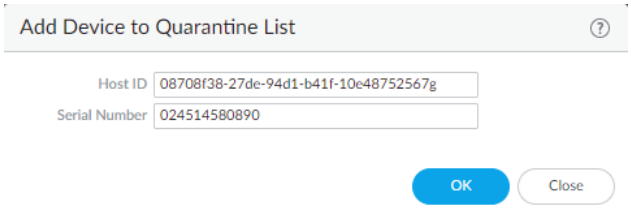


Manually Add and Delete Devices From the Quarantine List

You can add a device manually from either the quarantine pages, from the GlobalProtect, Threat, Traffic, or Unified logs, or by using an API. You can also manually delete the device from the quarantine pages, as shown in the following steps.

- To manually add a device to the quarantine list from the **Device Quarantine** page, select **Device** > **Device Quarantine** or **Panorama** > **Device Quarantine** and **Add** the device.

  Add the **Host ID** and, optionally, the **Serial Number** of the device. GlobalProtect uses the Host ID to identify the device.



- To add a device to the quarantine list from the GlobalProtect, Threat, Traffic, or Unified logs, complete the following steps.

  1. (Threat, Traffic, and Unified Logs Only) To add Host ID information to the Traffic, Threat, and Unified logs, select **Policies** > **Security** and **Add** a security policy rule; then, select **Quarantine** as the **Source Device** for **Source** traffic.

     A Host ID is required to add a device to the quarantine list. When a user connects to the network with the GlobalProtect app, GlobalProtect automatically adds Host ID information

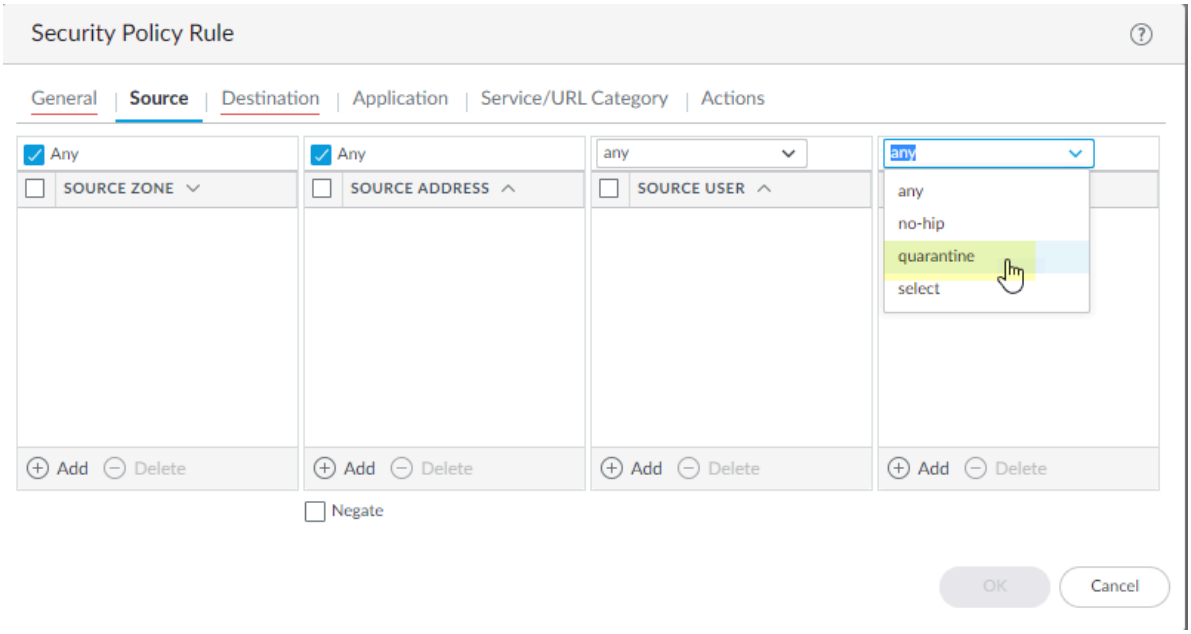
for the connected endpoint to the GlobalProtect log. The host ID value varies by endpoint type:

- Windows—Machine GUID stored in the Windows registry (HKEY_Local_Machine \Software\Microsoft\Cryptography\MachineGuid)
- macOS—MAC address of the first built-in physical network interface
- Android—Android ID
- iOS—UDID
- Chrome—GlobalProtect assigned unique alphanumeric string with length of 32 characters.

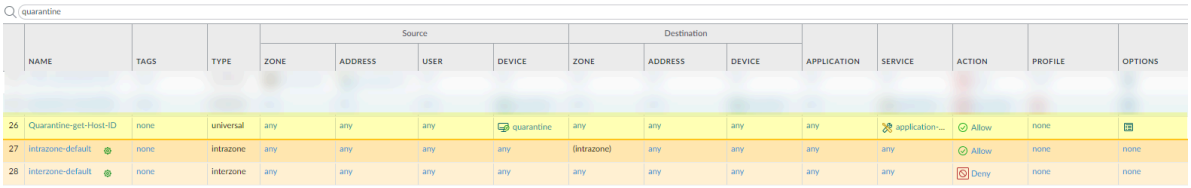
If you do not know the host ID, you can correlate the user-ID to the host ID in the HIP Match logs:

- Select **Monitor** > **Logs** > **HIP Match**.
- Filter the HIP match logs for the source user associated with the endpoint.
- Open the HIP match log and identify the host ID under **OS** > **Host ID** and optionally the hostname under **Host Information** > **Machine Name**.

For GlobalProtect to automatically add Host ID information to the Traffic, Threat, or Unified logs, you must add a policy rule that has **Quarantine** selected for source traffic.

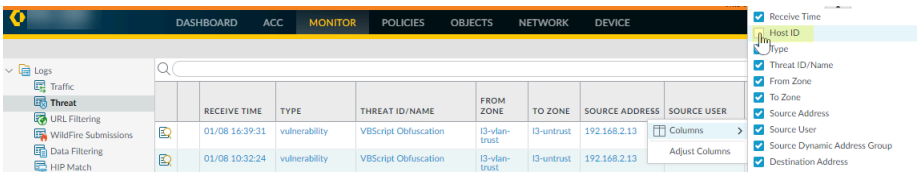


To make sure that you are adding the Host ID for all devices you want to quarantine (either manually or automatically), create a security policy that allows all traffic and specify ***Quarantine*** *as the* ***Source Device****. It does not matter what order you place this policy in the list of policies for it to work.*



2. Right-click the **Host ID** associated with the device and click **Block Device**.

If the **Host ID** column does not display, select the header of any column and then select the **Host ID** field to display the Host ID.



- To create an API to manually add the devices, see the instructions in the PAN-OS and Panorama API Usage Guide.

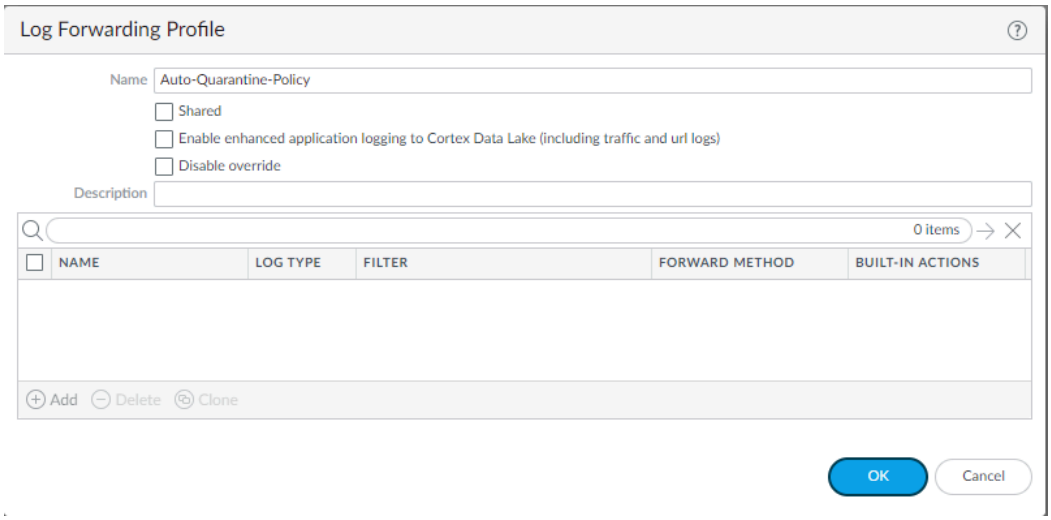
- After your administrator has performed remediation on the device, you can delete it from the list by selecting **Device** > **Device Quarantine** for next-generation firewalls or **Panorama** > **Device Quarantine** for Panorama appliances, selecting one or more devices, then selecting **Delete**.

Automatically Quarantine a Device

You can automatically quarantine a device using a log forwarding profile with a security policy rule or HIP match log settings.

- To quarantine a device using a log forwarding profile, complete the following steps.

1. select **Object** > **Log Forwarding** and either **Add** a new log forwarding profile or select an existing profile to modify it.

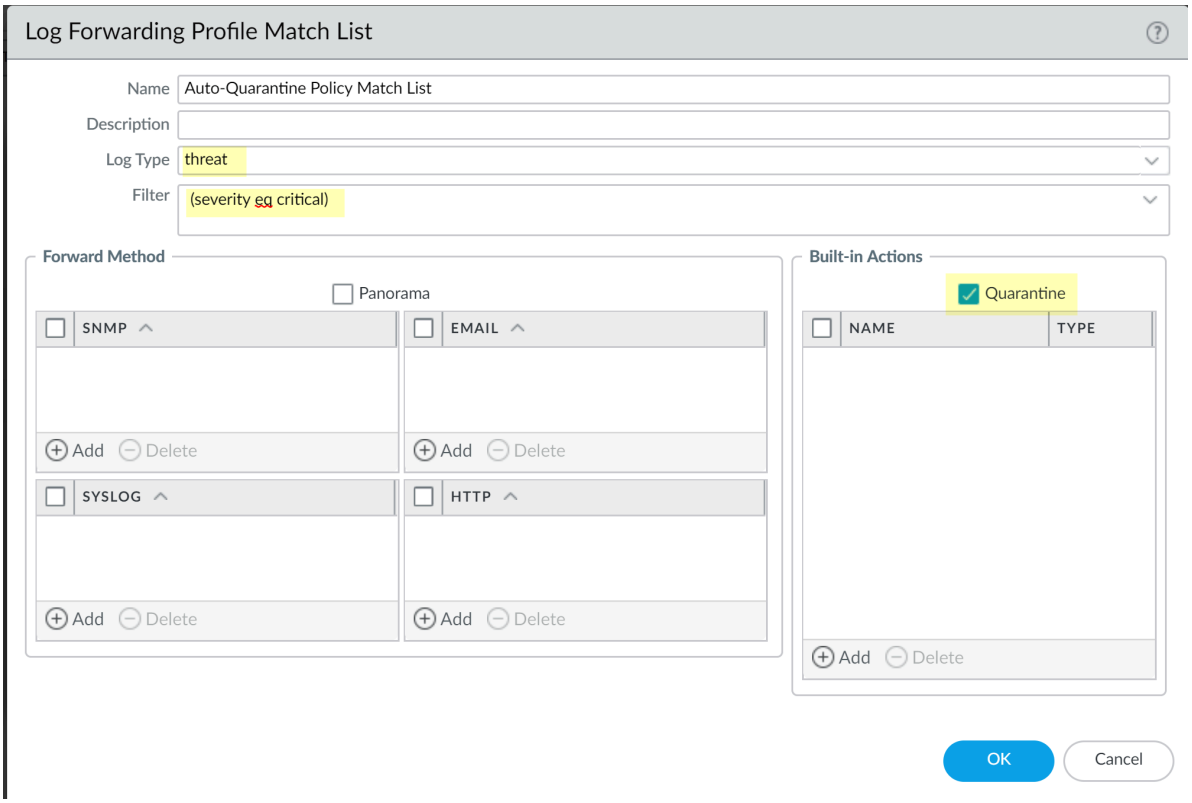


2. **Add** a **Log Forwarding Profile Match List** and, in the **Built-in Actions** section, select **Quarantine**.

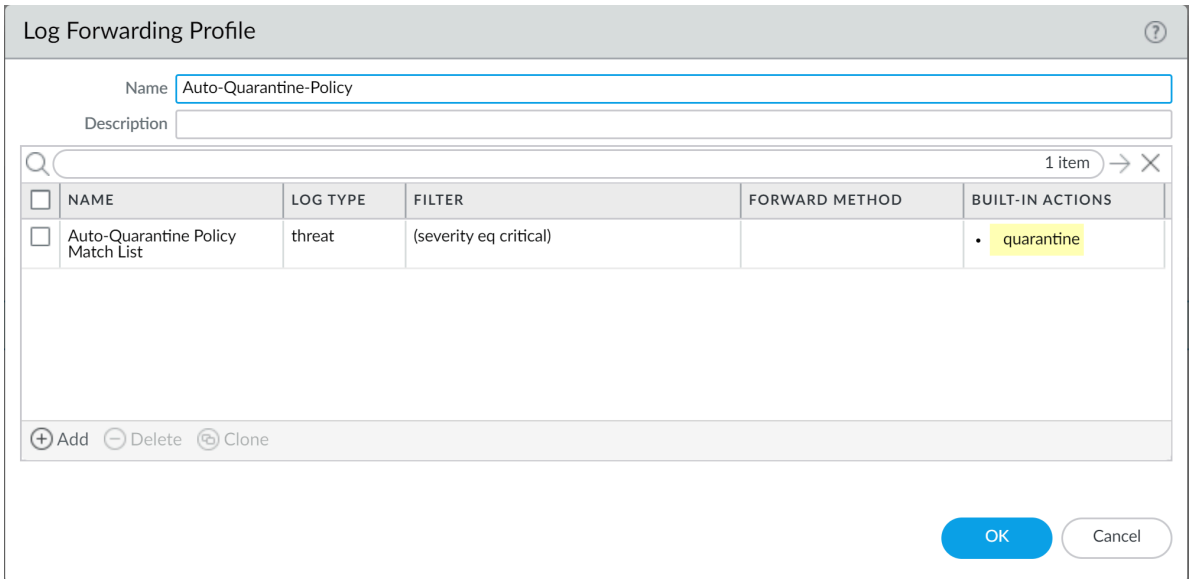
   Specify a **Log Type** of **GlobalProtect**, **Threat**, or **Traffic**.

   *If you specify a **Log Type** of **Threat** or **Traffic**, make sure that a Host ID is associated with a device by creating a security policy rule that has **Quarantine** as the **Source Device** for **Source** traffic, in order to add the Host ID. Without a Host ID, you cannot add a device to the quarantine list.*

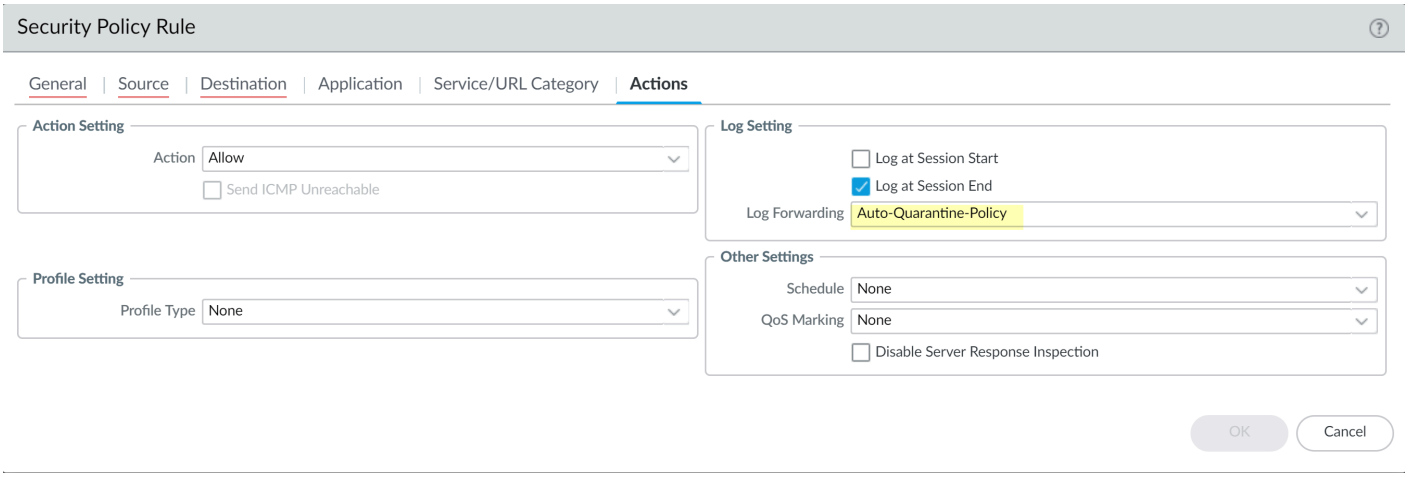
   The following example uses a **Log Type** of **Threat** and a severity of critical. After you add this profile to a security policy and these criteria are matched, the firewall adds devices from where this traffic originated to the quarantine list.



After you add the match list, the log forwarding profile displays **Quarantine** under **Built-In Actions**.



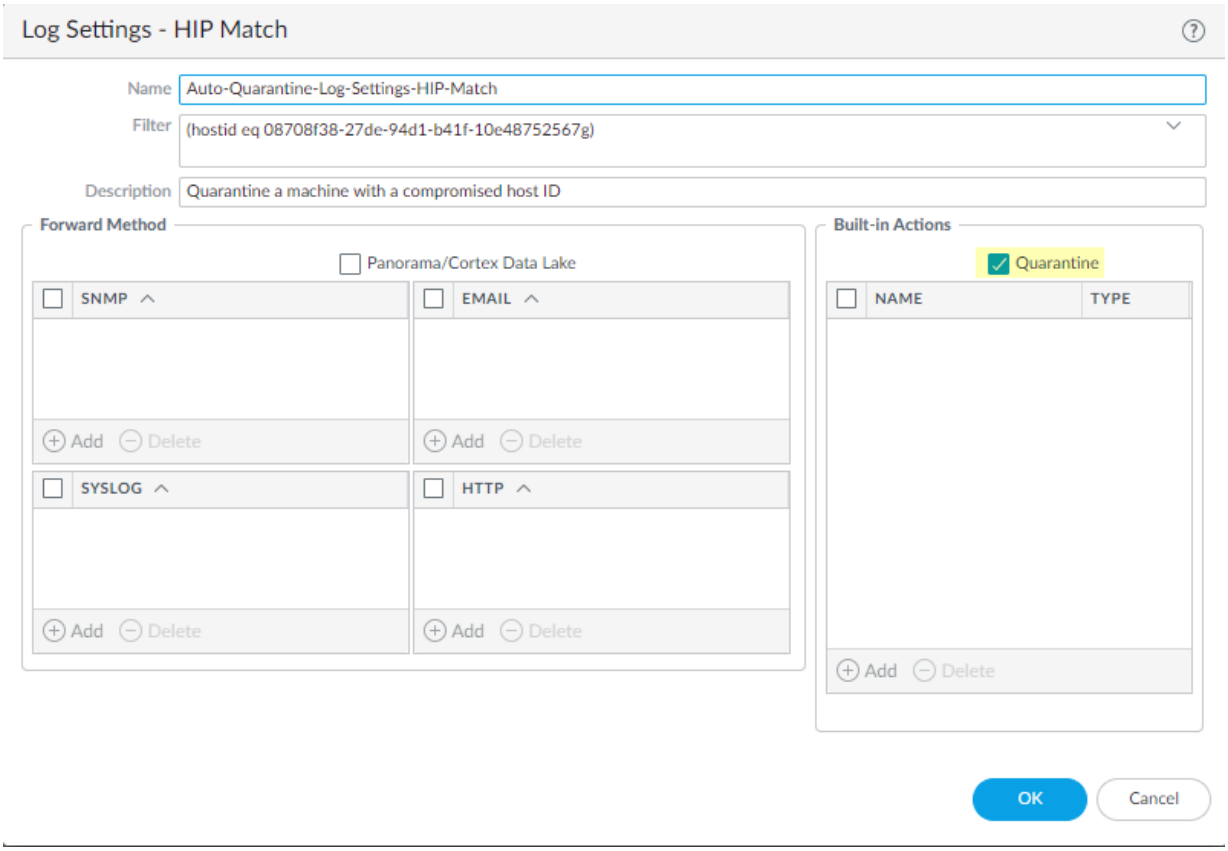
3. Select **Policies** > **Security** and **Add** a security policy.
4. Select **Actions**, then select the **Log Forwarding** profile you created.



- To automatically quarantine a device using HIP Match log settings, select **Device** > **Log Settings** > **HIP Match** and **Add** a log setting with a **Built-In Actions** of **Quarantine**.

  The following log setting has a **Filter** that with a host ID of 08708f38-27de-94d1-b41f-10e48752567g. If the HIP Match logs find a match for that host

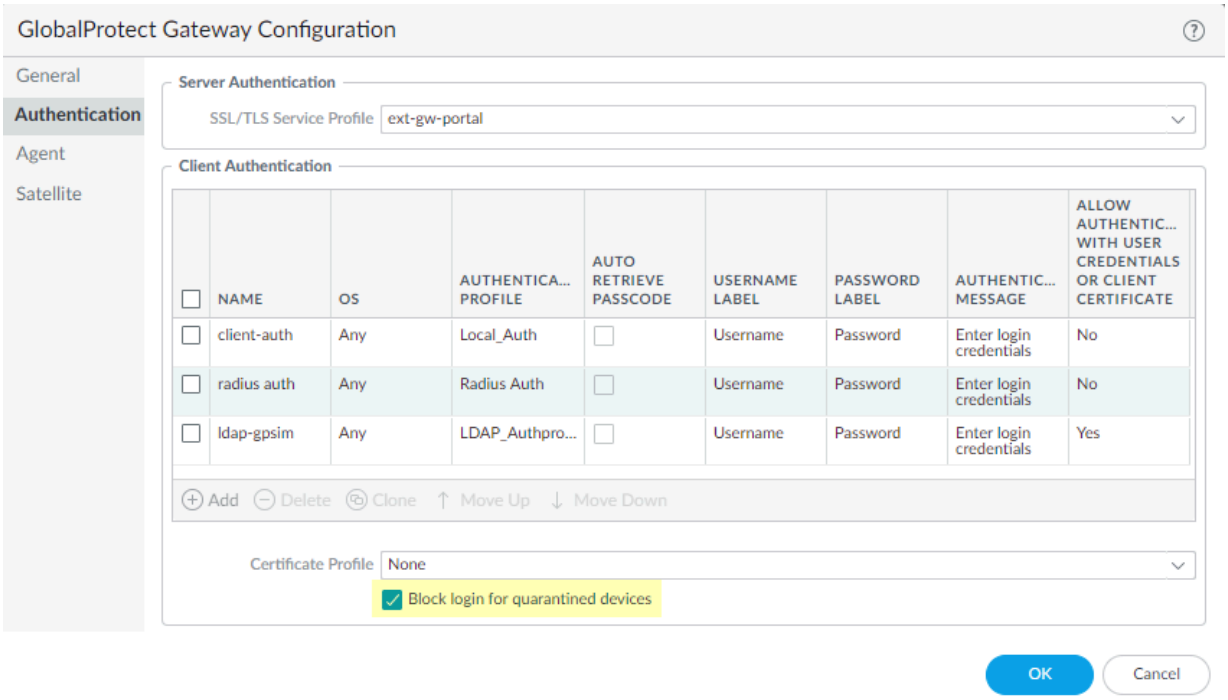
ID, this log setting adds that device to the quarantine list. Unlike a log forwarding profile, you do not need to attach this log setting to a security policy for it to take effect.



Use GlobalProtect and Security Policies to Block Access to Quarantined Devices

You can prevent users from logging into GlobalProtect from a quarantined device by configuring gateway authentication. In addition, you can block a quarantined device from sending or receiving traffic in the network by specifying options in a security policy rule. Use the following tasks to block GlobalProtect users or manage network access for a quarantined device.

- To block users from logging in to GlobalProtect from a quarantined device, configure GlobalProtect gateway authentication (**Network** > **GlobalProtect** > **Gateways** > ***gateway-configuration*** > **Authentication**) and select **Block login for quarantined devices**.



  If a user attempts to log in from a quarantined device to a gateway that has **Block login for quarantined devices** enabled, the GlobalProtect app notifies the user that the device is quarantined and the user cannot log in from that device. If this setting is not enabled, the user receives the notification but is able to log in from that device.

- To block access from a quarantined device using a security policy rule, specify **Quarantine** for either source or destination traffic; then, specify an action that blocks the quarantined device.

  Specifying **Quarantine** in a security policy rule means that the rule uses devices in the quarantine list as the match criteria, whether you specify **Quarantine** as the **Source Device** for **Source** traffic or the **Destination Device** for **Destination** traffic. The following example shows a source **Device** of **Quarantine** a destination IP address of the HQ server, and an action of

Deny. With this security policy rule, any devices in the quarantine list will not be able to access the HQ server.

	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION
26	Block-quarantined-devices-from-HQ-server	none	universal	any	any	any	quarantine	any	HQ-server	any	any	any	Deny
27	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow
28	interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny

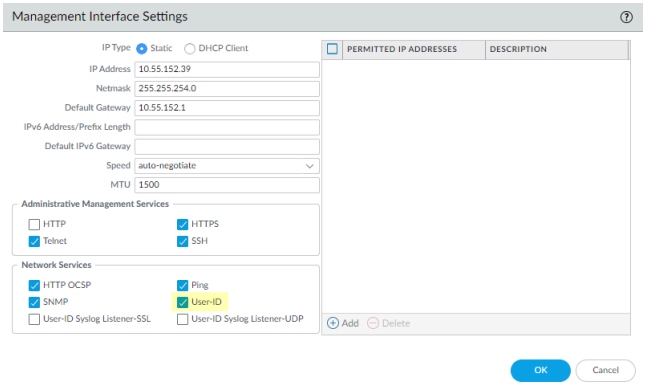
For a quarantined device to be valid in a policy on a firewall, a GlobalProtect user must successfully log in to GlobalProtect from the quarantined device, and the firewall must be aware of that login event. If the firewall is configured as a GlobalProtect gateway, the user can log in to that gateway from the quarantined device to validate the device in the policy. After a user successfully logs in to a gateway from a quarantined device, the gateway enforces the policy, and you can Redistribute Device Quarantine Information from Panorama *and have it enforced in a policy on any firewall or gateway in your network. If the user is blocked from logging in to the gateway (for example, if you have selected* ***Block login for quarantined devices*** *in the gateway configuration), that login is not counted as a successful login.*

Redistribute Device Quarantine Information from Panorama

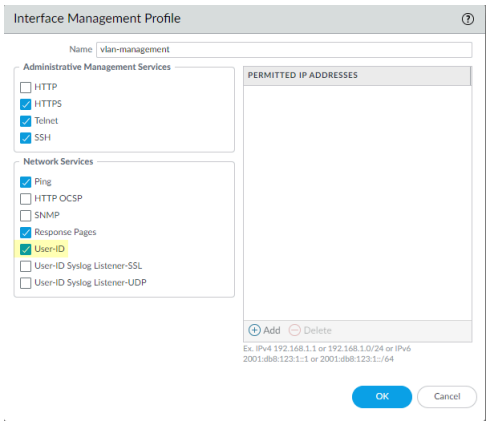
If you manage your next-generation firewalls using a Panorama appliance, you can create a quarantine list for all firewalls in **Panorama** > **Device Quarantine** and distribute that information to your managed firewalls. You redistribute device quarantine information the same way as you redistribute User-ID information. Complete the following steps to redistribute quarantine information from Panorama.

STEP 1 | Enable User-ID on the agent server if you have not done so already.

- If the redistribution agent server uses the management interface, select **Device** > **Setup** > **Interfaces** > **Management** and select **User-ID**.

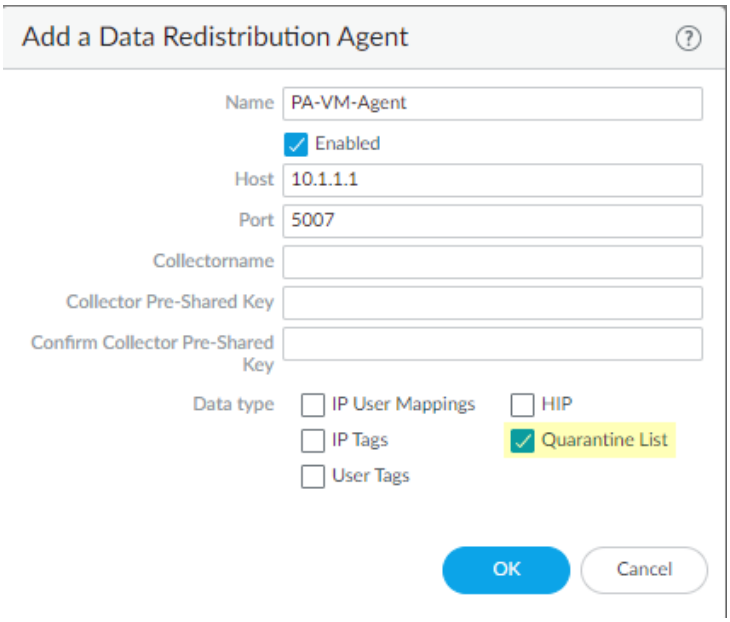


- If the redistribution agent uses an interface on the dataplane (for example, an Ethernet or VLAN interface), select **Network** > **Interface Mgmt**, select an existing management profile or **Add** a new one, and select **User-ID**.



STEP 2 | To create a data redistribution agent, select **Panorama** > **Data Redistribution** and **Add** the agent.

The following example shows a data redistribution agent where Panorama distributes the **Quarantine List** information to the firewall with an IP address of 10.1.1.1 using port 5007.



GlobalProtect FIPS-CC Certification

The GlobalProtect™app for Windows, and macOS endpoints, ARM-based devices running on Windows, and macOS, iOS, Android,and Linux provide a FIPS-CC mode that can be enabled that incorporate requirements from the Common Criteria (CC) and Federal Information Processing Standard (FIPS 140-3).

You can view the status page to track the FIPS and CCcertification status.

These security certifications ensure a standard set of security assurances and functionalities and are often required by U.S. government agencies and other domestic and international regulated industries. For more details on product certifications and third-party validation, refer to the Palo Alto Networks Certifications page.

Refer to the following sections for information on how to configure and troubleshoot the GlobalProtect app for Windows and macOS endpoints, ARM-based devices running on Windows, and macOS, iOS, Android,and Linux endpoints in FIPS-CC mode:

- Enable and Verify FIPS-CC Mode
- FIPS-CC Security Functions

Enable and Verify FIPS-CC Mode

You can enable and verify FIPS-CC mode for the GlobalProtect app using the following methods:

- Enable and Verify FIPS-CC Mode on Windows Endpoints
- Enable and Verify FIPS-CC Mode on macOS Endpoints
- Enable and Verify FIPS-CC Mode Using Workspace ONE on iOS Endpoints
- Enable FIPS Mode on Linux EndPoints with Ubuntu or RHEL
- Enable and Verify FIPS-CC Mode Using Microsoft Intune on Android Endpoints

The GlobalProtect app -FIPS-CC mode is supported on x86 and ARM-based platforms.

We recommend that you enable FIPS-CC mode on the GlobalProtect portal/gateway to efficiently operate FIPS-CC mode on endpoints.

To modify the Windows Registry or macOS plist, you must have an administrator account in Windows or macOS.

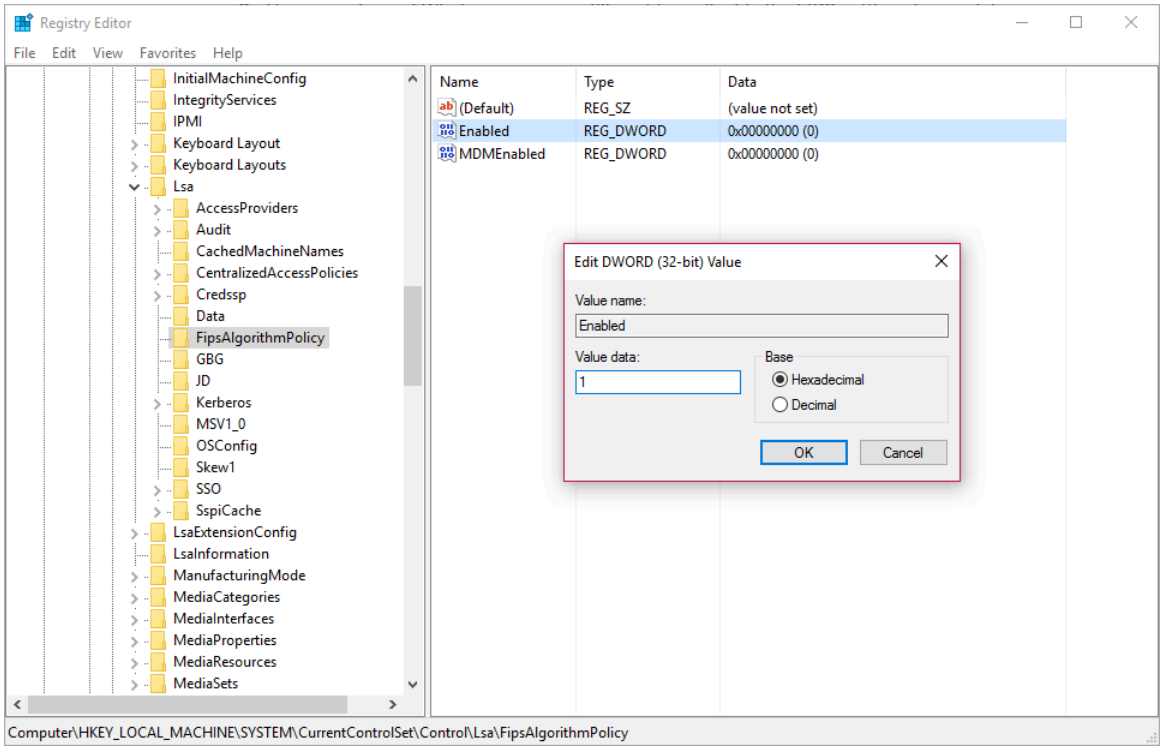
Enable and Verify FIPS-CC Mode on Windows Endpoints

On Windows endpoints, use the following steps to enable and verify FIPS-CC mode for GlobalProtect™ using the Deploy App Settings in the Windows Registry:

STEP 1 | Enable FIPS mode for the Windows operating system.

To enable FIPS-CC mode for GlobalProtect, you must first enable FIPS-CC mode for the Windows operating system.

1. Launch the Command Prompt.
2. Enter **`regedit`** to open the Windows Registry.
3. In the Windows Registry, go to: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy\`.
4. Right-click the **Enabled** registry value and **Modify** it.
5. To enable FIPS mode, set the **Value Data** to **1**. The default value of **`0`** indicates that FIPS mode is disabled.

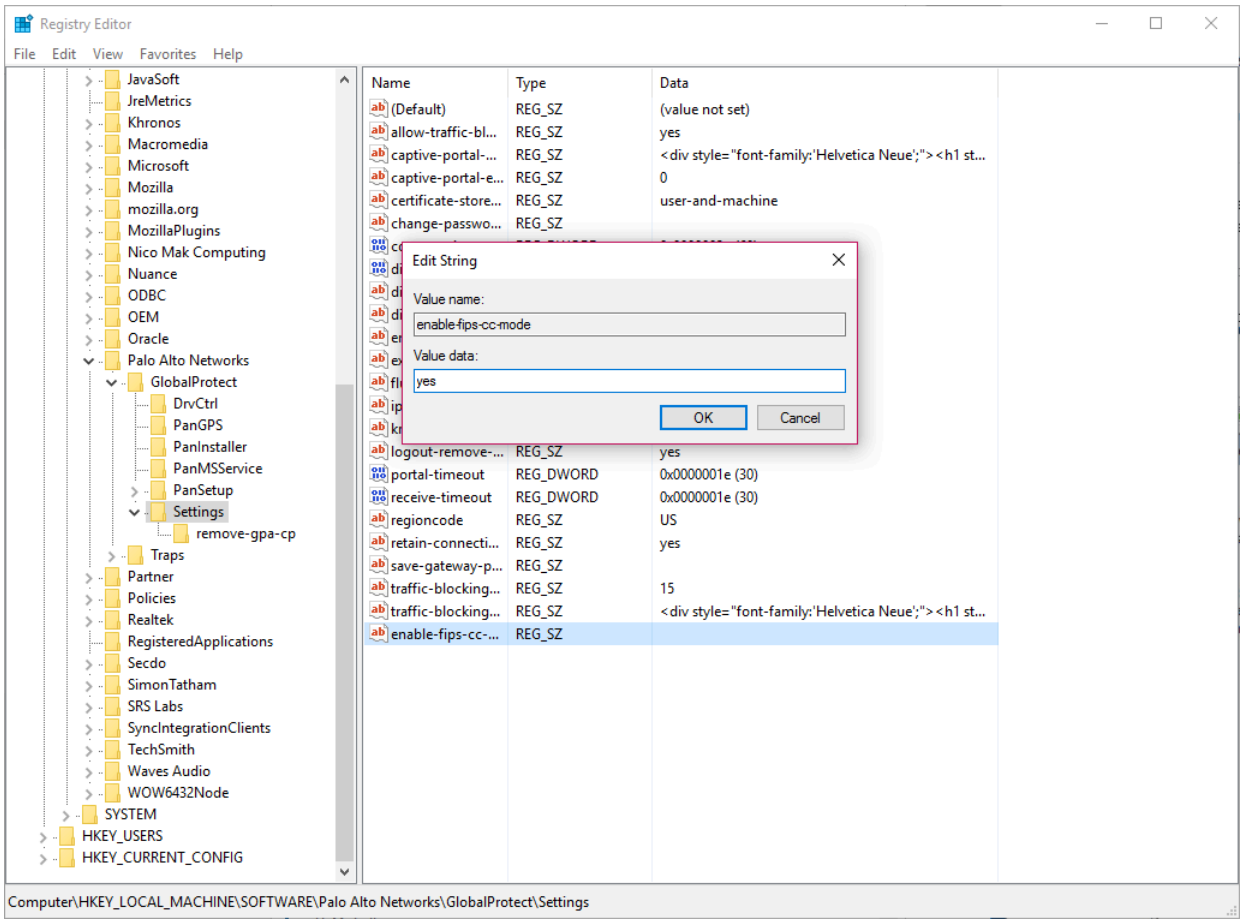


6. Click **OK**.
7. Restart your endpoint.

STEP 2 | Enable FIPS-CC mode for GlobalProtect.

You cannot disable FIPS-CC mode after you enable it. To run GlobalProtect in non-FIPS-CC mode, end users must uninstall and then reinstall the GlobalProtect app. This clears all FIPS-CC mode settings from the Windows Registry.

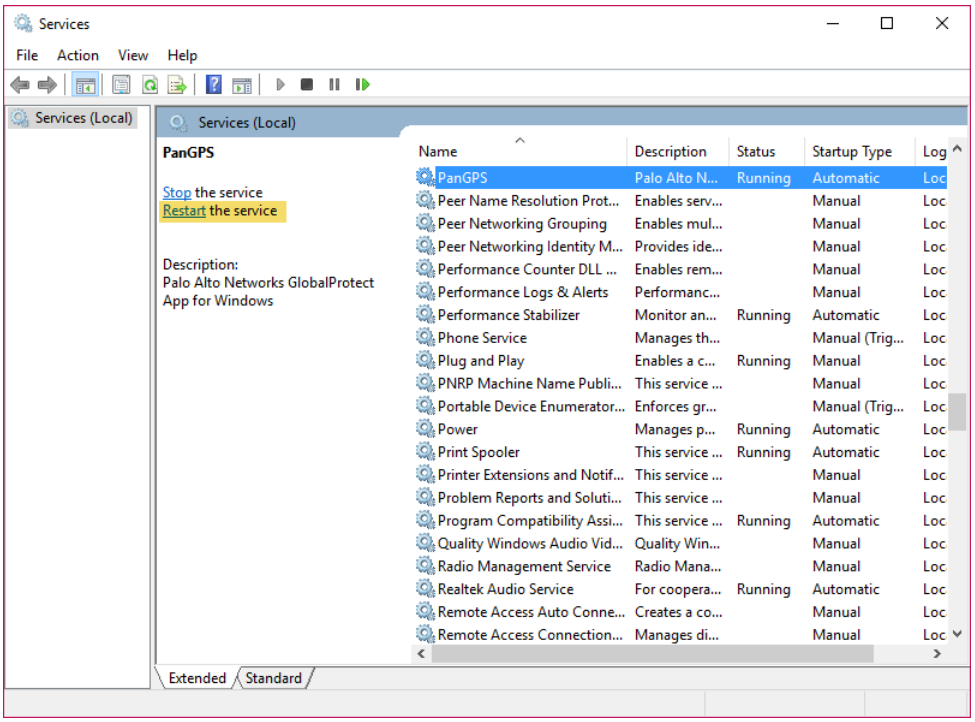
1. Launch the Command Prompt.
2. Enter **regedit** to open the Windows Registry.
3. In the Windows Registry, go to: `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\`.
4. Click **Edit** and then select **New** > **String Value**.
5. When prompted, specify the **Name** of the new registry value as **enable-fips-cc-mode**.
6. Right-click the new registry value and **Modify** it.
7. To enable FIPS-CC mode, set the **Value Data** to **yes**.
8. Click **OK**.



STEP 3 | Restart GlobalProtect.

To enable the GlobalProtect app to initialize in FIPS-CC mode, you must restart GlobalProtect using one of the following methods:

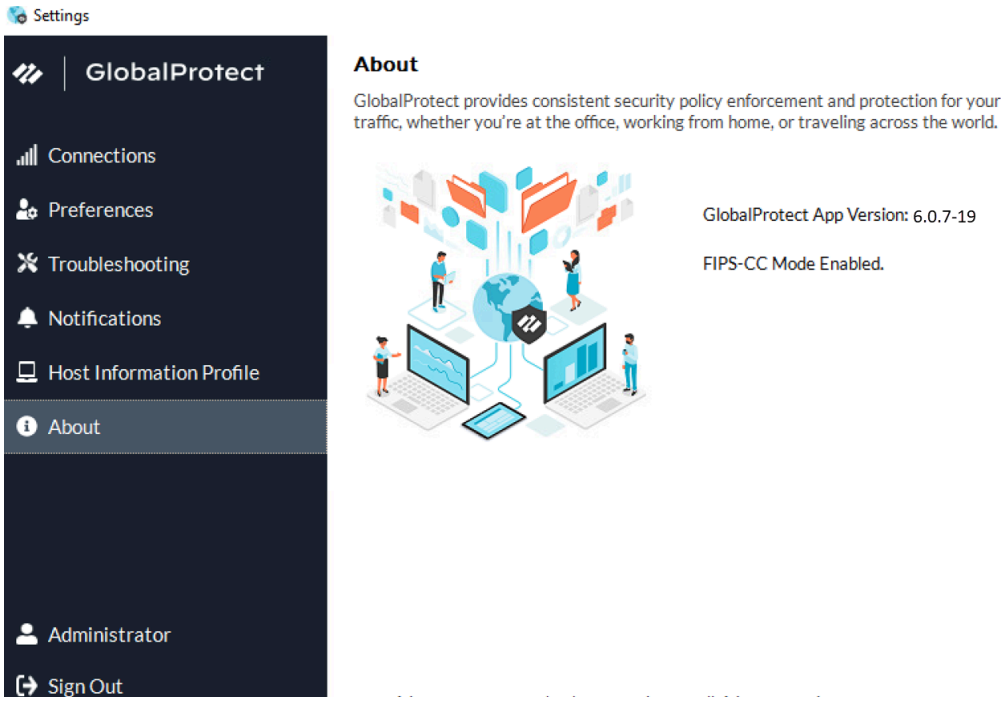
- Reboot your endpoint.
- Restart the GlobalProtect application and GlobalProtect service (PanGPS):
  1. Launch the Command Prompt.
  2. Enter **`services.msc`** to open the Windows Services manager.
  3. From the Services list, select **PanGPS**.
  4. **Restart** the service.



STEP 4 | Alternatively, you can enable FIPS-CC mode using the following msiexec syntax through the Microsoft Windows Installer (Msiexec): **`msiexec /i GlobalProtect64.msi ENABLEFIPSCCMODE=YES`**

STEP 5 | Verify that FIPS-CC mode is enabled on the GlobalProtect app.

1. Launch the GlobalProtect app.
2. From the status panel, open the settings dialog ( ).
3. Select **About**.
4. Verify that FIPS-CC mode is enabled. If FIPS-CC mode is enabled, the About dialog displays the `FIPS-CC Mode Enabled` status.



Enable and Verify FIPS-CC Mode on macOS Endpoints

On macOS endpoints, use the following steps to enable and verify FIPS-CC mode for GlobalProtect™ using the Deploy App Settings to macOS Endpoints (property list):

To enable FIPS-CC mode for GlobalProtect, your must first enable FIPS-CC mode for macOS operating system. By default, FIPS mode for the macOS operating system is automatically enabled on endpoints running macOS 10.8 and later releases.

STEP 1 | Open the GlobalProtect plist file and locate the GlobalProtect customization settings.

1. Launch a plist editor, such as Xcode.
2. In the plist editor, open the following plist file: `/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`.
3. Locate the GlobalProtect Settings dictionary: `/Palo Alto Networks/GlobalProtect/Settings`.

   If the Settings dictionary does not exist, create it. You can add each key to the Settings dictionary as a string.

STEP 2 | Enable FIPS-CC mode for GlobalProtect.

You cannot disable FIPS-CC after you enable it. To run GlobalProtect in non-FIPS-CC mode, end users must uninstall and then reinstall the GlobalProtect app. This clears all FIPS-CC mode settings from the macOS plist.

In the Settings dictionary, add the following key-value pair to enable FIPS-CC mode:

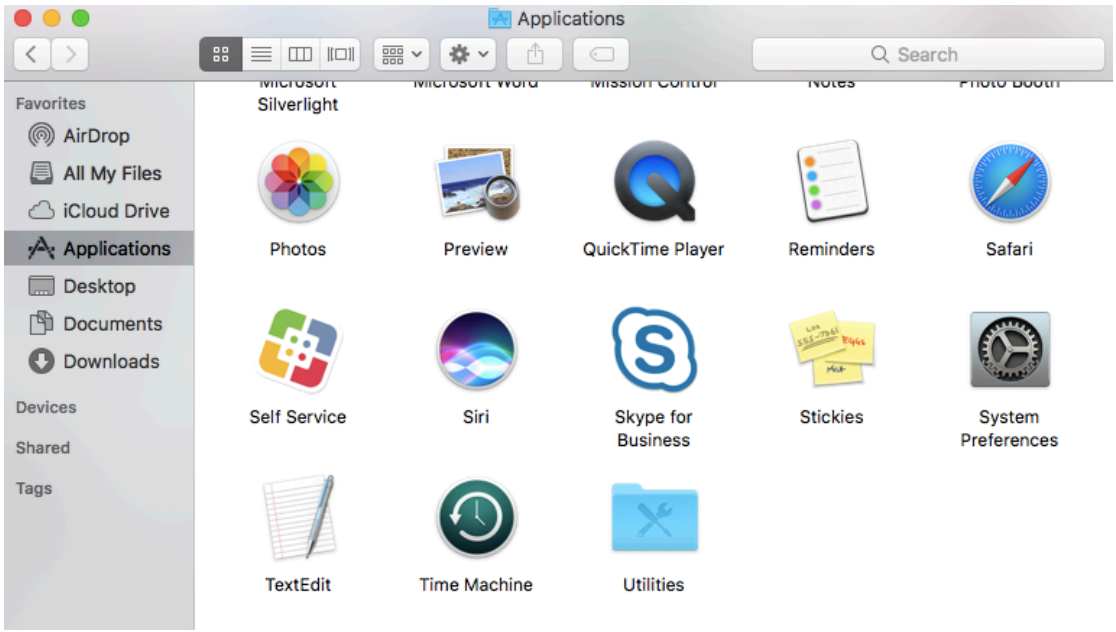
<key>enable-fips-cc-mode</key>
<string>yes</string>

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>Palo Alto Networks</key>
        <dict>
                <key>GlobalProtect</key>
                <dict>
                        <key>PanGPS</key>
                        <dict>
                                <key>UserProfileType</key>
                                <integer>0</integer>
                                <key>disable-globalprotect</key>
                                <integer>0</integer>
                        </dict>
                        <key>PanSetup</key>
                        <dict>
                                <key>CurrentVersion</key>
                                <string>6.0.5-27</string>
                                <key>InstallHistory</key>
                                <string>Fresh Install</string>
                                <key>PreviousVersion</key>
                                <string></string>
                        </dict>
                        <key>Settings</key>
                        <dict>
                                <key>enable-fips-cc-mode</key>
                                <string>yes</string>
                                <key>disable-globalprotect</key>
                                <integer>0</integer>
                        </dict>
                </dict>
        </dict>
</dict>
</plist>
~
```

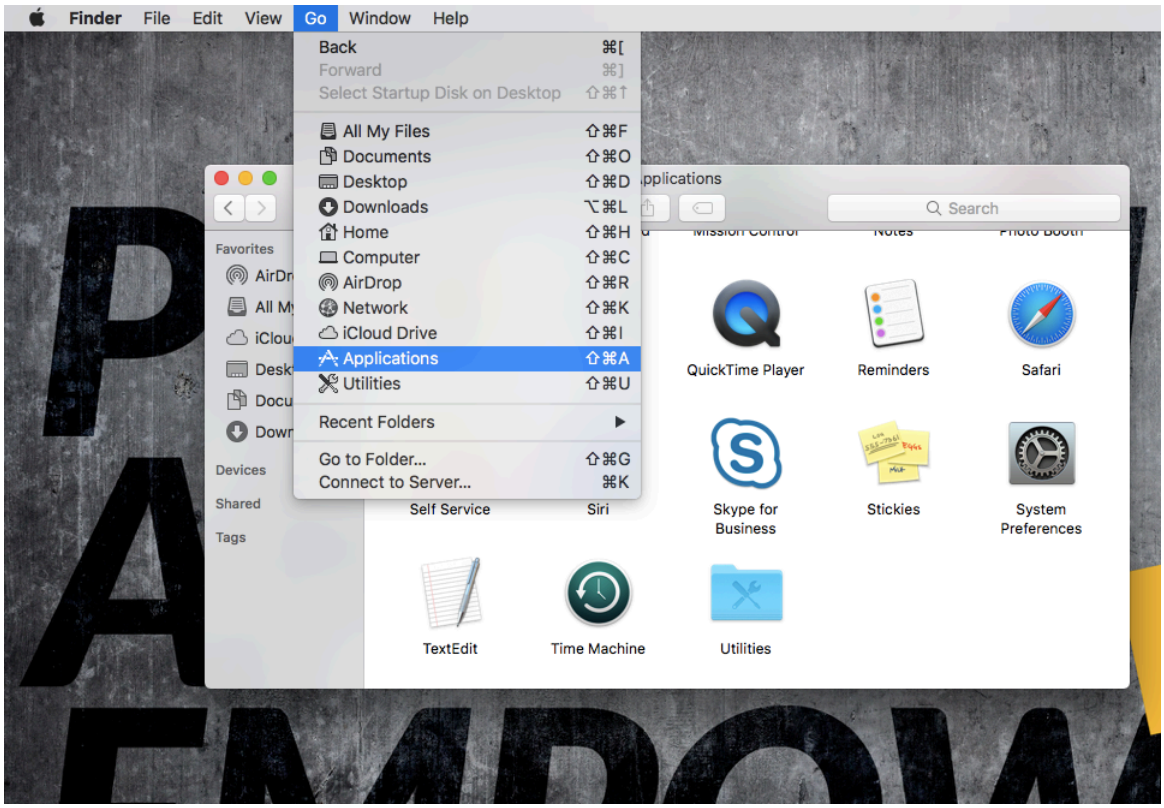

STEP 3 | Restart GlobalProtect.

To enable the GlobalProtect app to initialize in FIPS-CC mode, you must restart GlobalProtect using one of the following methods:

- Reboot your endpoint.
- Restart the GlobalProtect application and GlobalProtect service (PanGPS):
  1. Launch the Finder.
  2. Open the Applications folder:
     - From the Finder sidebar, select **Applications**.



     - If you do not see **Applications** in the Finder sidebar, select **Go** > **Applications** from the Finder menu bar.



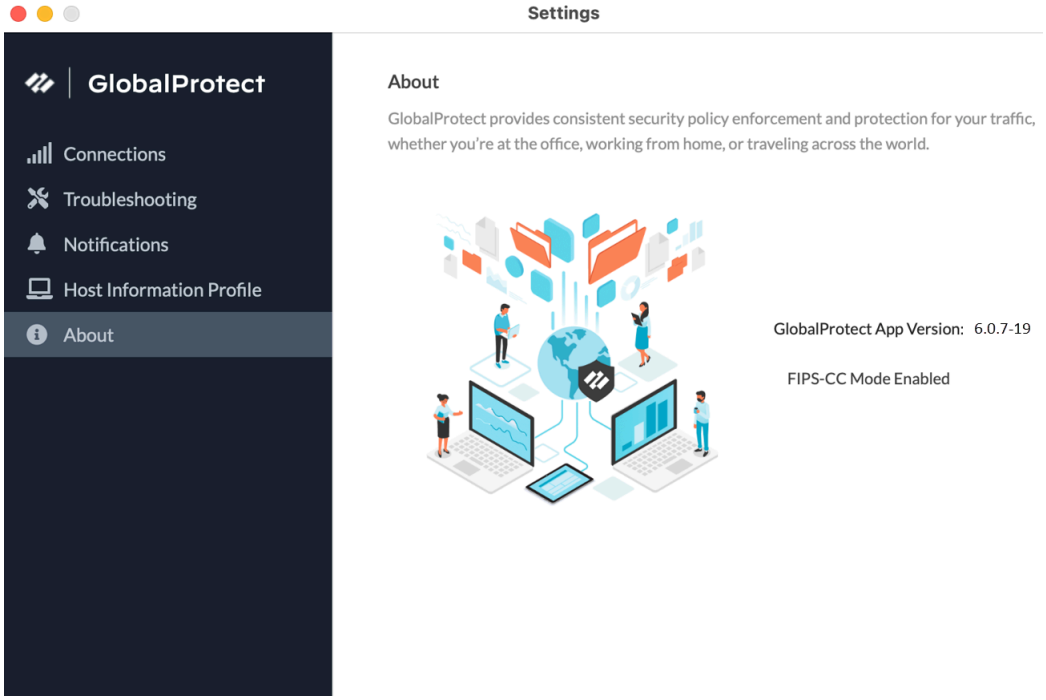
*To display **Applications** in the Finder sidebar, select **Finder** > **Preferences** from the Finder menu bar. From the Finder Preferences, select **Sidebar** and then enable the option to display **Applications.***

3. Open the Utilities folder.
4. Launch Terminal.
5. Execute the following commands:

```
username>$ launchctl unload -S Aqua
/Library/LaunchAgents/com.paloaltonetworks.gp.pangpa.plist
username>$ launchctl unload -S Aqua
/Library/LaunchAgents/com.paloaltonetworks.gp.pangps.plist
username>$ launchctl load -S Aqua
/Library/LaunchAgents/com.paloaltonetworks.gp.pangps.plist
username>$ launchctl load -S Aqua
/Library/LaunchAgents/com.paloaltonetworks.gp.pangpa.plist
```


STEP 4 | Verify that FIPS-CC mode is enabled on the GlobalProtect app.

1. Launch the GlobalProtect app.
2. From the status panel, open the settings dialog ( ).
3. Select **About**.
4. Verify that FIPS-CC mode is enabled. If FIPS-CC mode is enabled, the About dialog displays the `FIPS-CC Mode Enabled` status.



STEP 5 | View the logs to view the GlobalProtect app logs related to FIPS-CC mode on endpoints running macOS.

STEP 6 | View, collect, and send the logs to administrator to troubleshoot and resolve the issues related to FIPS-CC mode on devices running macOS.

Enable and Verify FIPS-CC Mode Using Workspace ONE on iOS Endpoints

Use the following steps to enable and verify FIPS-CC mode for GlobalProtect™ on iOS endpoints using Configure Workspace ONE for iOS Endpoints.

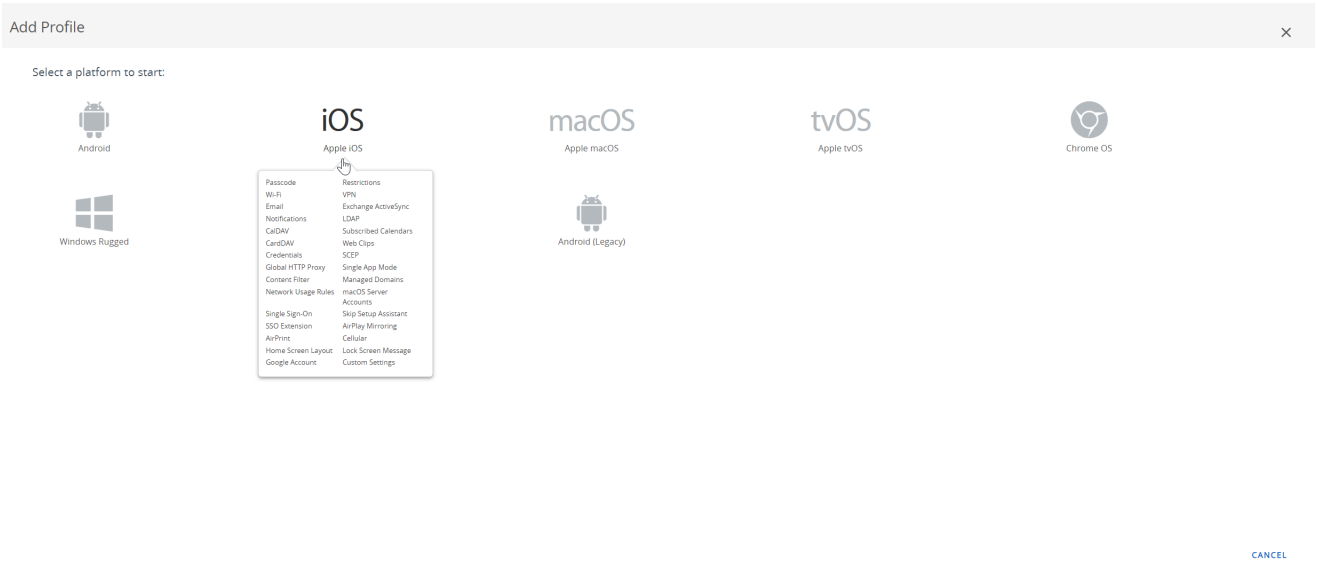
To enable FIPS-CC for iOS and Android endpoints, you must use the GlobalProtect version GlobalProtect for Governments. Contact Palo Alto Support and create a case to access the GlobalProtect for Governments version, which is privately distributed.

STEP 1 | Enable FIPS mode for iOS endpoints.

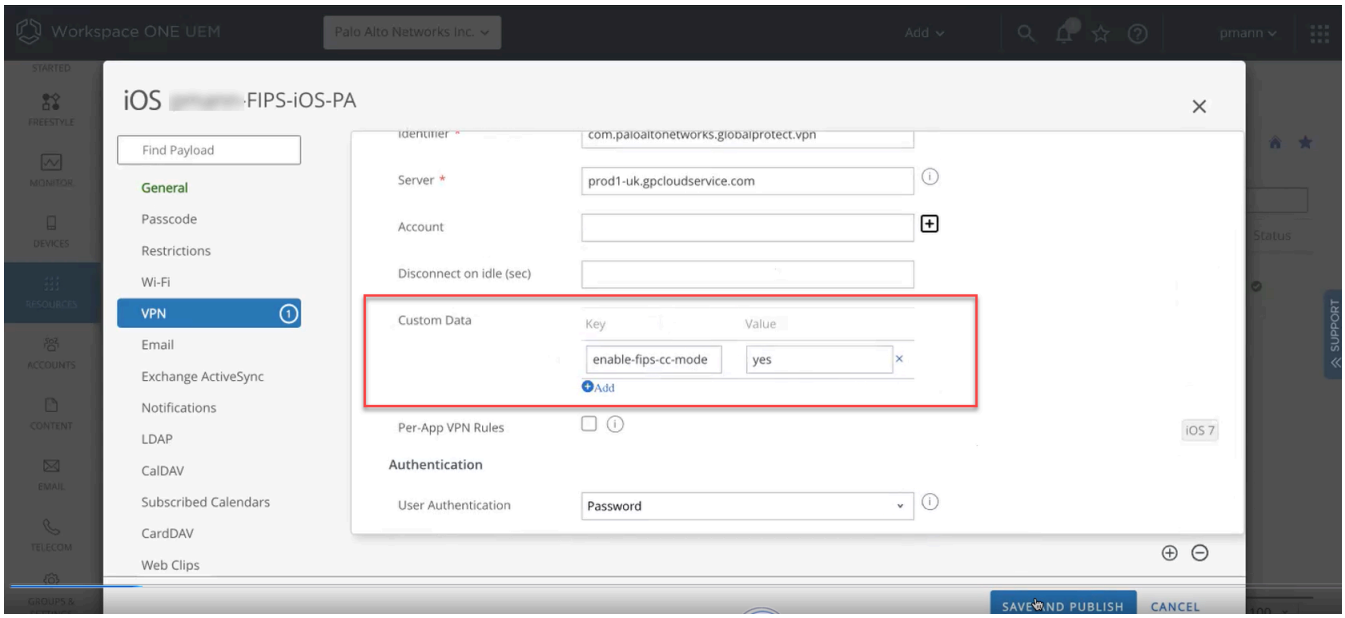
1. Configure Workspace ONE for iOS endpoints.
2. Download the GlobalProtect app for iOS endpoints and Deploy the GlobalProtect Mobile App Using Workspace ONE.
3. From the Workspace ONE console, modify an existing Apple iOS profile or add a new one.

   To add a new profile:

   - Select **Resources** > **Profiles & Baselines** > **Profiles** > **ADD**, then **Add Profile**.
   - Select **iOS** from the platform list.



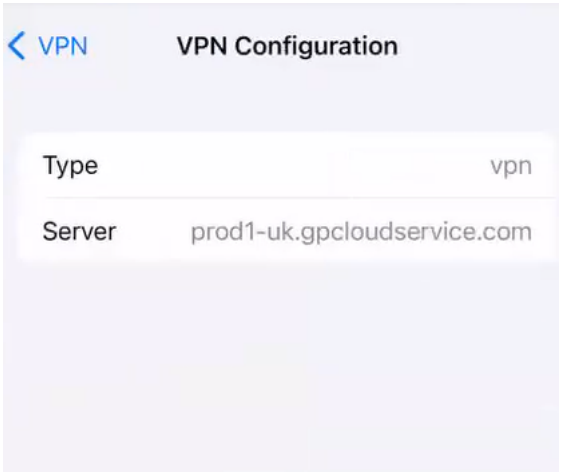
   - Select **Device Profile** from the **Select Context Window**.
4. On the **Resources** > **Profiles & Baselines** > **Profiles** page, select the `<iOS profile>` for which you want to enable FIPS-CC mode.
5. Configure the General, VPN, and Credentials (Optional) settings for the `<iOS profile>` that you want to create.
6. On the VPN page, under **Custom Data**:
   - Specify the **Key** value as `enable-fips-cc-mode`.
   - Set the **Value** to `Yes`.



7. **Save and Publish** your changes.

   After you enable the FIPS-CC mode on the Workspace ONE console, the console pushes the updated FIPS-CC mode configuration to the iOS endpoints.

8. Ensure that the updated configuration is pushed from the console to the iOS endpoints. On the iOS endpoint, select **Settings** > **General** > **VPN & Device Management** > **VPN**. The **VPN Configuration** screen displays the latest configuration.The following screenshot shows an example of VPN configuration.



STEP 2 | Verify that FIPS-CC mode is enabled on the GlobalProtect app.

1. Launch the GlobalProtect app.
2. From the status panel, open the settings dialog (⚙).
3. Select **About**.
4. Verify that FIPS-CC mode is enabled. If FIPS-CC mode is enabled, the About dialog displays the `FIPS-CC Mode Enabled` status.

If FIPS-CC mode could not be enabled successfully, the About dialog displays the `FIPS-CC Mode Failed` status.

You cannot disable the FIPS-CC mode on iOS endpoints. To disable the FIPS-CC mode, you must remove the iOS device from the respective configuration profile through the Workspace ONE console.

STEP 3 | View the logs to view the GlobalProtect app logs related to FIPS-CC mode on iOS endpoints.

STEP 4 | View, collect, and send the logs to the administrator to troubleshoot and resolve the issues related to FIPS-CC mode on iOS devices.

Enable FIPS Mode on Linux EndPoints with Ubuntu or RHEL

Use the following steps to enable and verify FIPS-CC mode for GlobalProtect™ on Linux endpoints running Ubuntu or Red Hat Enterprise Linux (RHEL) 8.1 platforms.

STEP 1 | Ensure that FIPS-CC mode is disabled on the Linux endpoints with Ubuntu or Red Hat Enterprise Linux (RHEL) 8.1.

STEP 2 | Install the GlobalProtect app on your Linux endpoint.

STEP 3 | (Optional) If a client certificate is used for authentication, install and set up client certificate.

STEP 4 | Modify `pangps.xml` to enable FIPS-CC mode.

On Linux endpoints, the pre-deployment configuration file (`pangps.xml`) is located in `/opt/paloaltonetworks/globalprotect`.

In `pangps.xml` file, under `Settings`, add `<enable-fips-cc-mode>yes</enable-fips-cc-mode>`

For example:

```
<?xml version="x.x" encoding="UTF-8"?><GlobalProtect>
        <Settings>
      <enable-fips-cc-mode>yes</enable-fips-cc-mode>
                <disable-globalprotect>0</disable-globalprotect>
        </Settings>
```

STEP 5 | Enable FIPS-CC mode on the Linux endpoint with Ubuntu or Red Hat Enterprise Linux (RHEL) 8.1.

STEP 6 | Reboot the Linux endpoint in order for the pre-deployment configuration changes to take effect.

STEP 7 | Verify that FIPS-CC mode is enabled on the GlobalProtect app.

1. Launch the GlobalProtect app.
2. From the status panel, open the settings dialog (⚙).
3. Select **About**.
4. Verify that FIPS-CC mode is enabled. If FIPS-CC mode is enabled, the About dialog displays the **FIPS-CC Mode Enabled** status. For CLI version, you can use the CLI command `globalprotect show --version`.

If FIPS-CC mode could not be enabled successfully, the About dialog displays the **FIPS-CC Mode Failed** status.

STEP 8 | View the logs to view the GlobalProtect app logs related to FIPS-CC mode on Linux endpoints.

STEP 9 | View, collect, and send the logs to the administrator to troubleshoot and resolve the issues related to FIPS-CC mode on Linux devices.

Enable and Verify FIPS-CC Mode Using Microsoft Intune on Android Endpoints

Use the following steps to enable and verify FIPS-CC mode for GlobalProtect™ on Android endpoints using Microsoft Intune

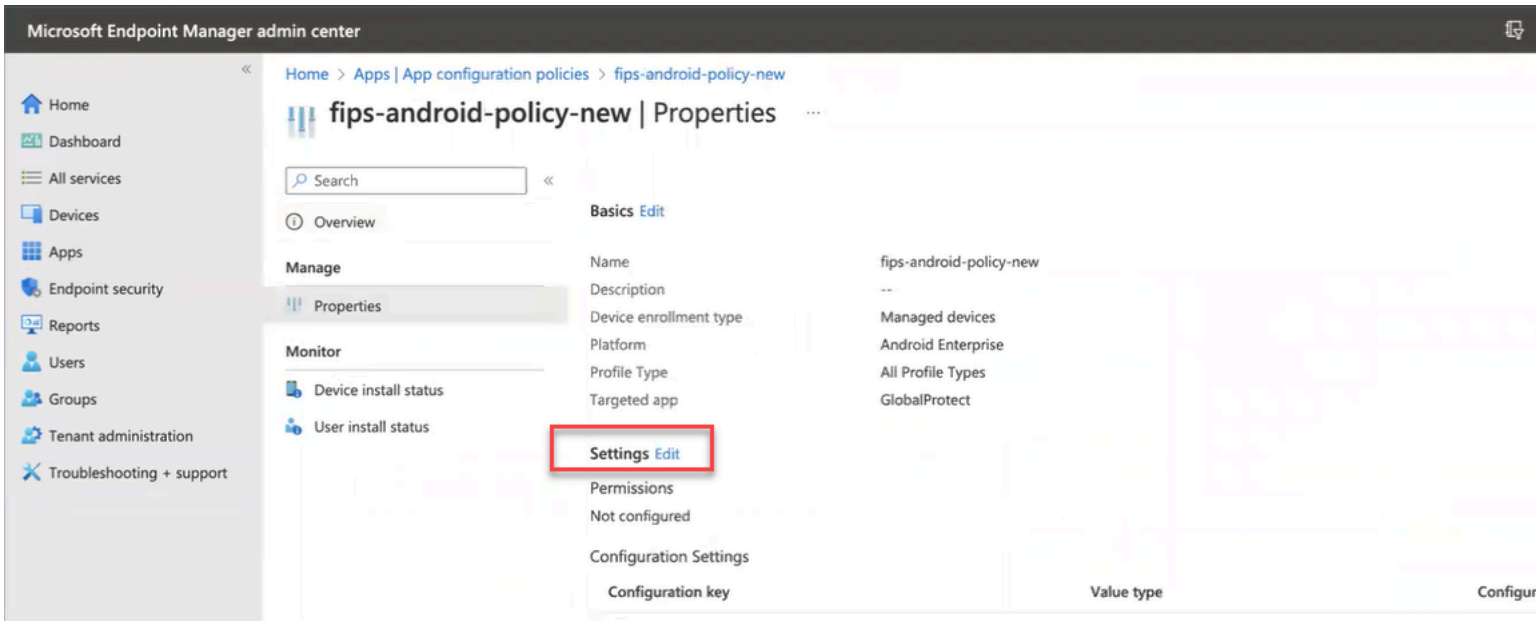
To enable FIPS-CC for iOS and Android endpoints, you must use the GlobalProtect version GlobalProtect for Governments. Contact Palo Alto Support and create a case to access the GlobalProtect for Governments version, which is privately distributed.

STEP 1 | Enable FIPS mode on Android endpoints.

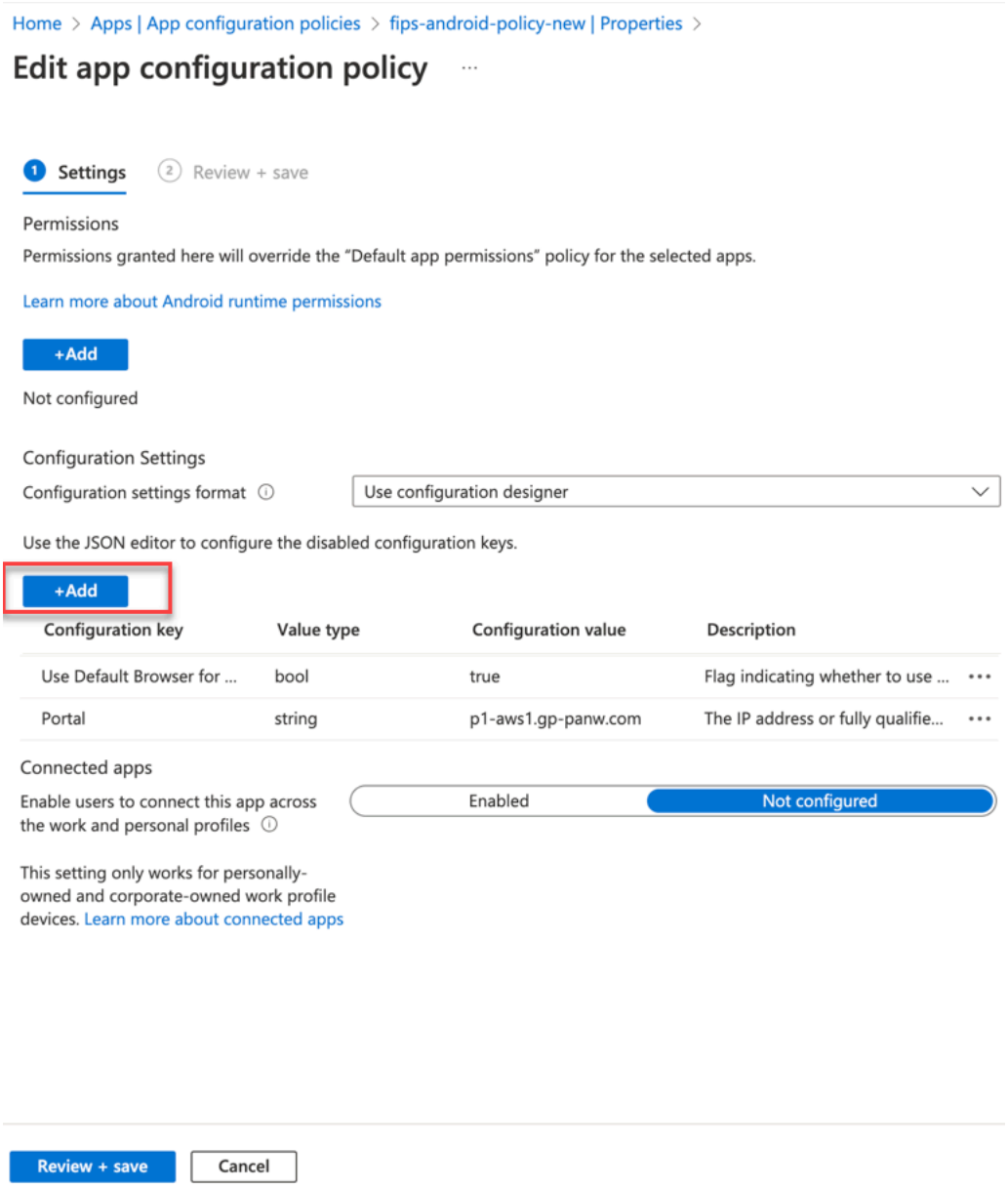
1. Download the GlobalProtect app for Android and Deploy the GlobalProtect Mobile App Using Microsoft Intune.
2. From the Microsoft Intune console, add **Configuration Settings** to enable FIPS-CC mode.

   To add configuration settings for `Enable fips-cc-mode`:

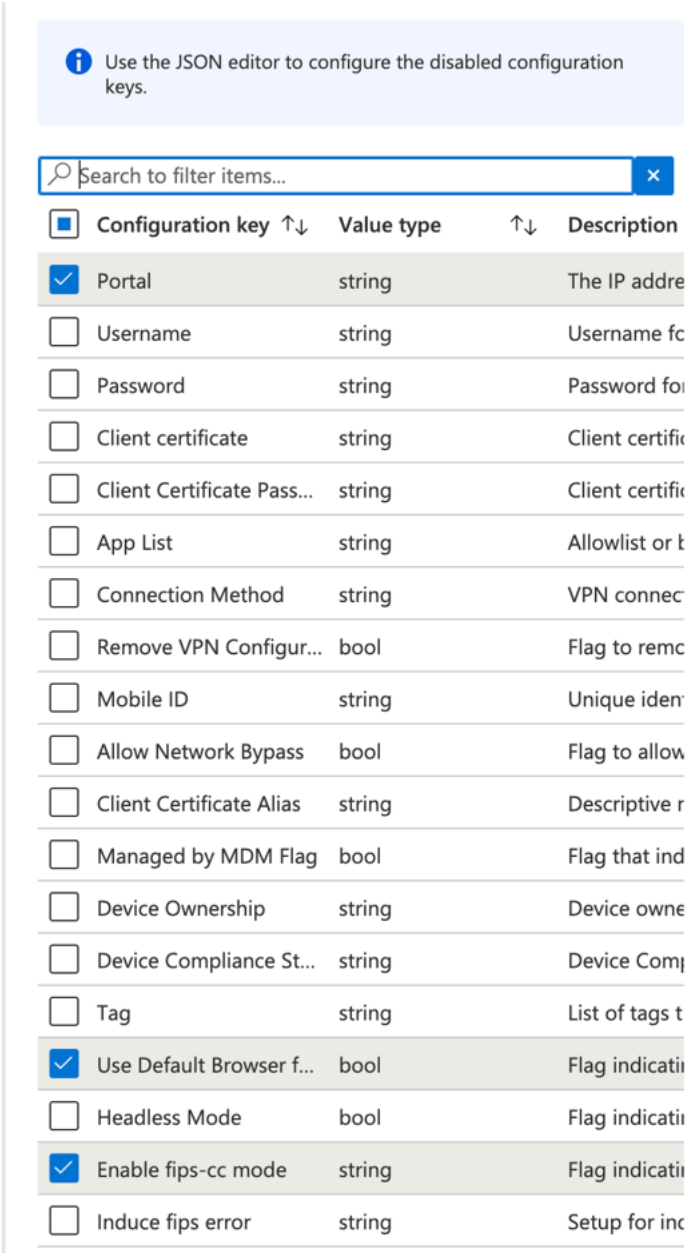
   1. Select **APPS** > **Policy** > **App configuration policies** > **<policy>** > **Properties**.
   2. **Edit** the **Settings**.



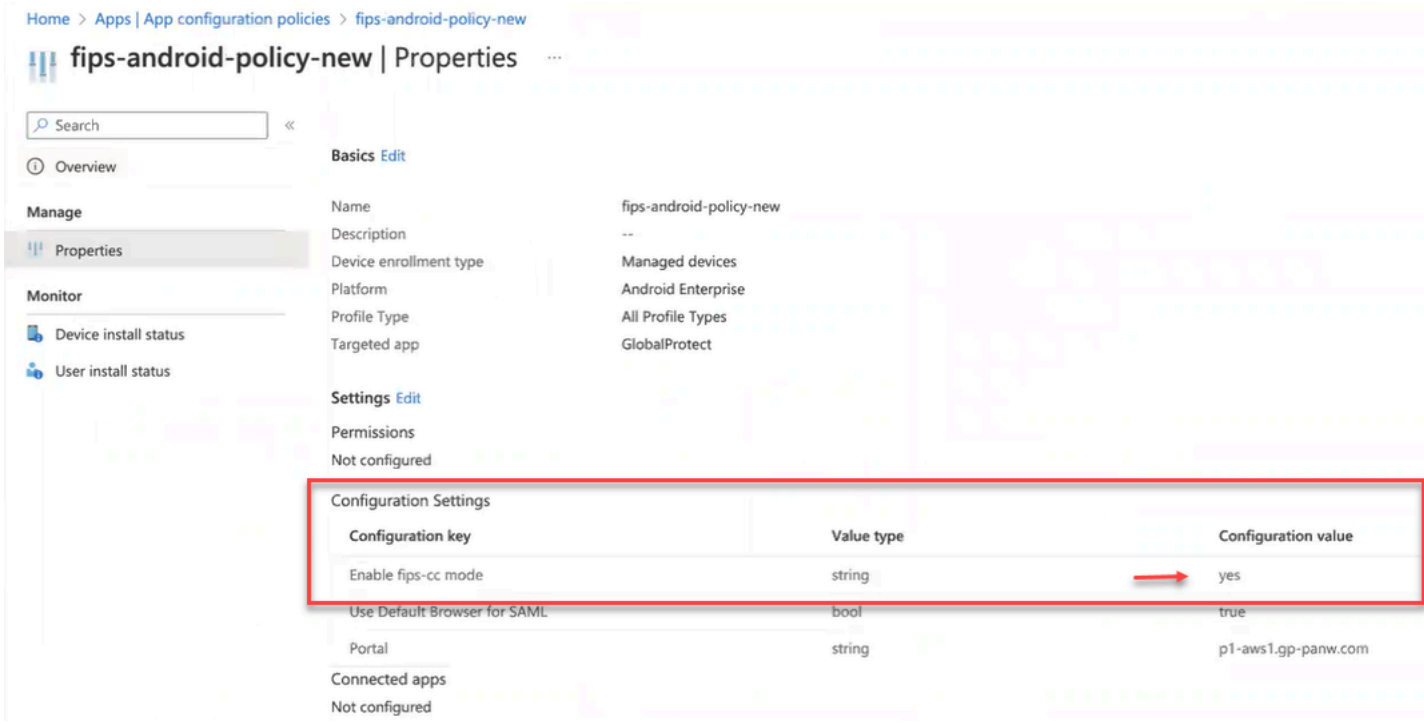
3. On the Edit app configuration policies page, **Add** the **Configuration Settings** for enabling FIPS-CC mode.



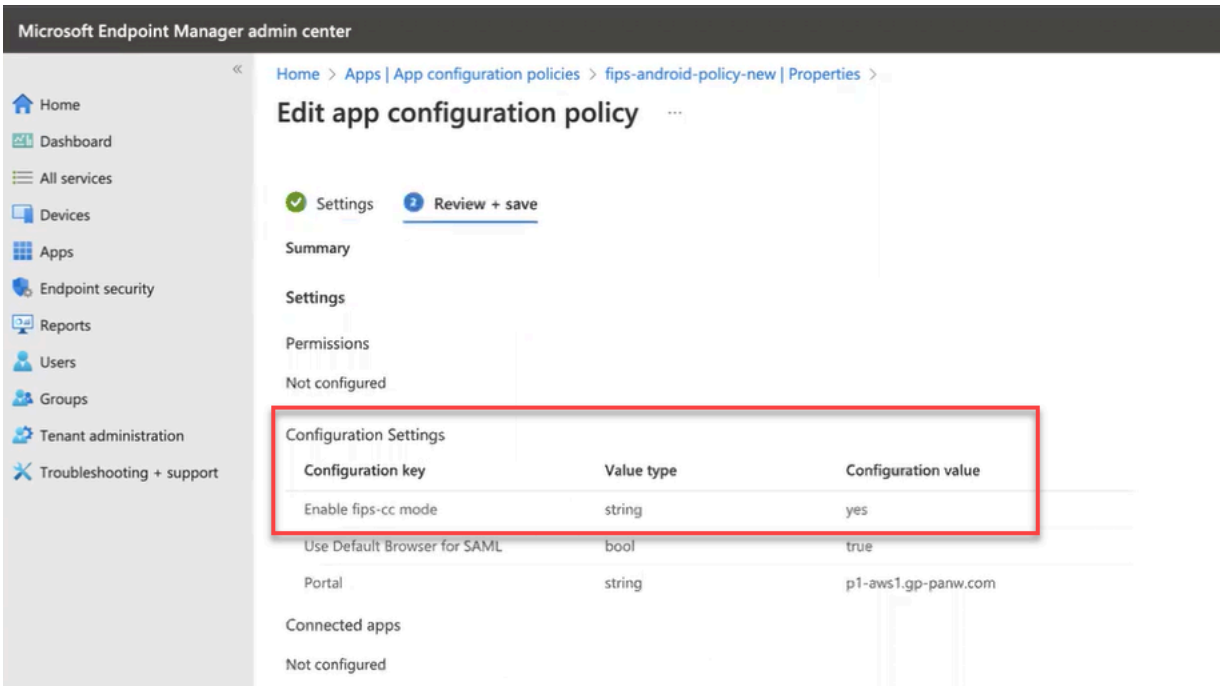
4. From the list of configuration keys, select **Enable fips-cc mode**.



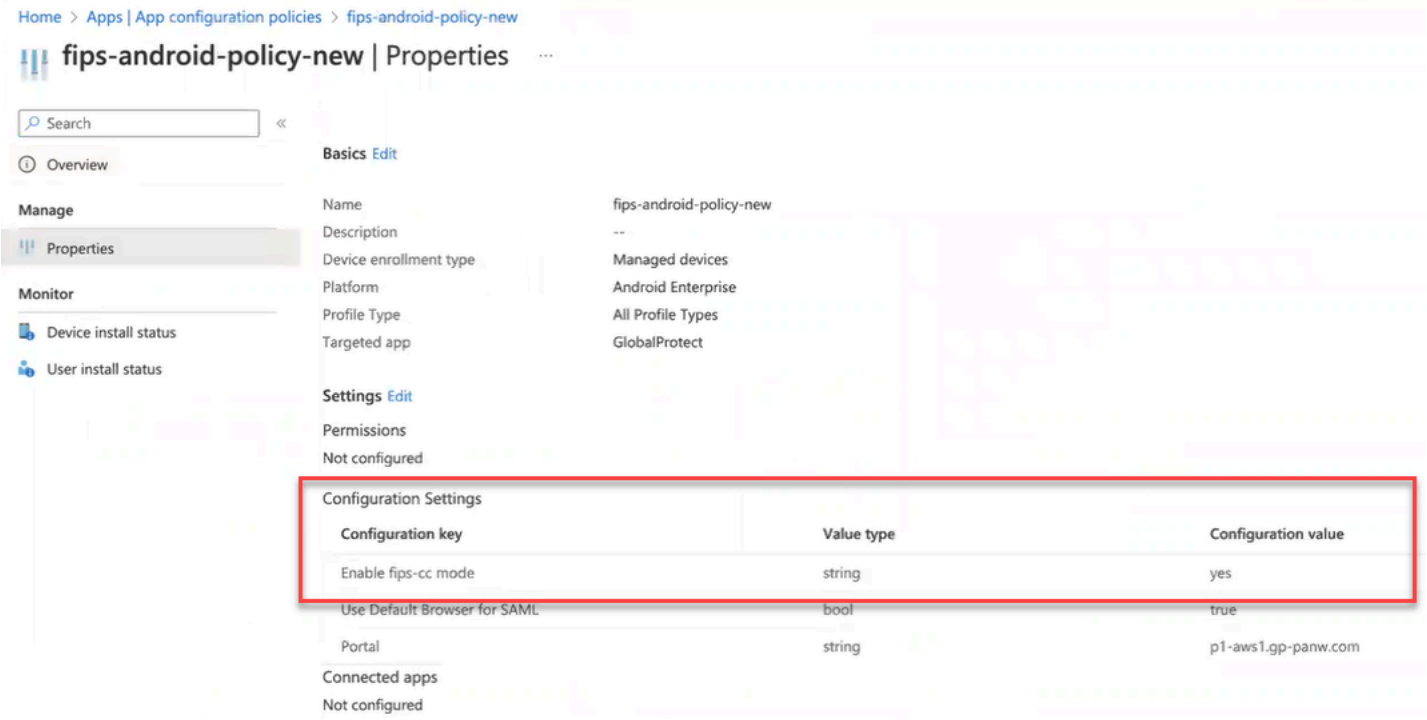
5. Set the **Configuration Value** to **Yes** for **Enable fips-cc mode** configuration key.



6. Click **Review and Save**. The Edit app configuration policies page displays the newly added `Enable-fips-cc-mode` configuration settings.



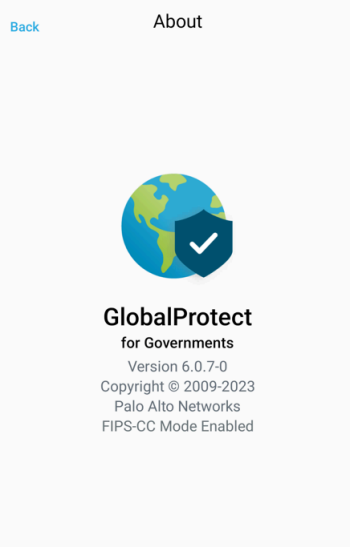
The configuration setting for Enable fips-cc mode is also displayed under the Configuration Settings area (**APPS** > **Policy** > **App configuration policies** > **<policy>** > **Properties**.



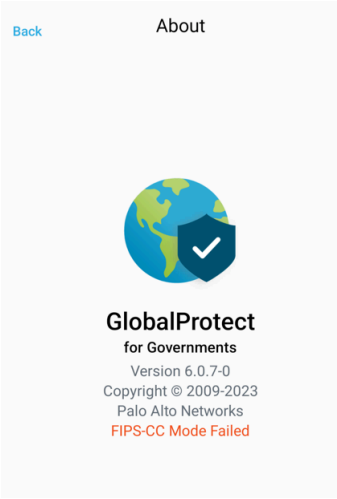
After you enable the FIPS-CC mode on the Microsoft Intune console and synchronize the device with the Microsoft Intune, the console pushes the updated FIPS-CC mode configuration to the Android endpoints.

STEP 2 | Verify that FIPS-CC mode is enabled is enabled successfully on an Android endpoint.

1. Launch the GlobalProtect app.
2. From the status panel, open the settings dialog (⚙).
3. Select **About**.
4. Verify that FIPS-CC mode is enabled. If FIPS-CC mode is enabled, the About dialog displays the `FIPS-CC Mode Enabled` status.



If FIPS-CC mode could not be enabled successfully, the About dialog displays the `FIPS-CC Mode Failed` status.



STEP 3 | View the logs to view the GlobalProtect app logs related to FIPS-CC mode on Android endpoints.

STEP 4 | View, collect, and send the logs to the administrator to troubleshoot and resolve the issues related to FIPS-CC mode on Android devices.

FIPS-CC Security Functions

When you enable FIPS-CC mode for GlobalProtect, the following security functions are applied to all managed GlobalProtect apps on Windows and macOS, iOS, Android, and Linux endpoints:

- You must configure the gateway to encrypt all VPN tunnels between the GlobalProtect app and gateways using TLS or IPSec.
- When you configure an IPSec VPN tunnel on the gateway, you must select a cipher suite option presented during IPSec setup.
- When you configure an IPSec VPN tunnel on the gateway, you can specify one of the following encryption algorithms:
  - AES-CBC-128 (with the HMAC-SHA-1 authentication algorithm)
  - AES-GCM-128
  - AES-GCM-256
- Both server and client certificates must use one of the following signature algorithms:
  - RSA 2048 bit (or greater)
  - ECDSA P-256
  - ECDSA P-384
  - ECDSA P-521

  In addition, you must use a signature hash algorithm of SHA-256, SHA-384, or SHA-512.
- GlobalProtect app will enforce strict X.509v3 verification checks on the server certificate.
  - The verifications checks are based on NIAP's FIA_X509_EXT.1 and FIA_X509_EXT.2 certificate validation and authentication requirements.

Resolve FIPS-CC Mode Issues

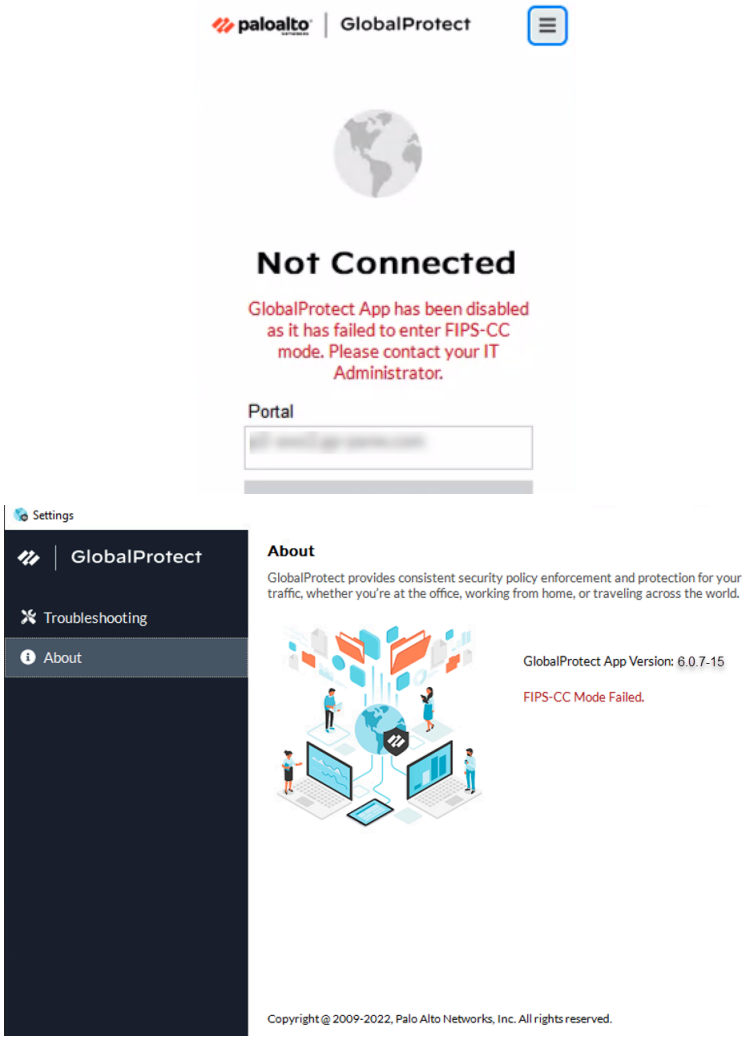
The following section describes possible FIPS-CC mode issues and the corresponding solutions. If you encounter any issues that are not described below, please contact your GlobalProtect™ administrator for troubleshooting assistance.

View the status page to track the FIPS and CC status.

- **Issue:**

  The GlobalProtect app fails to initialize in FIPS-CC mode due to a FIPS Power-On Self-Test (POST) or integrity test failure.

  - **Description:** After you enable FIPS-CC mode, the GlobalProtect app performs FIPS Power-On Self-Tests (POST) and integrity tests during app initialization and system or app reboots. If either of these tests fail, the GlobalProtect app is disabled and the About window displays the `FIPS-CC Mode Failed` error message:



  - **Resolution:** Restart the app to clear the error condition. If the issue persists, uninstall and then reinstall the app.

- **Issue:**

  The GlobalProtect app is unable to establish a connection in FIPS-CC mode due to a FIPS conditional self-test failure.

  - **Description:** After the GlobalProtect app initializes in FIPS-CC mode, it performs FIPS conditional self-tests. If the self-tests fail, the GlobalProtect app terminates the session and remains disconnected.
    - **Resolution:** To establish a GlobalProtect connection, you must re-authenticate to the GlobalProtect portal and enable FIPS-CC mode again.

*If GlobalProtect is unable to initialize or connect in FIPS-CC mode, you can access the **Troubleshooting** tab of the GlobalProtect Settings panel to view and collect logs for troubleshooting. All other tabs are unavailable until GlobalProtect connects successfully.*

The following tables list the error messages displayed when certificate validation fails for Windows and macOS platforms. Administrators can view the error messages for troubleshooting and resolving the issues.

FIPS-CC Certification Validation	Error Messages
Trusted root CA certificate not found.	Failed validation of the X.509v3 certificate: The portal certificate is not signed by a trusted certificate authority.
CA certificate expired.	Failed validation of the X.509v3 certificate: The portal certificate is not within its validity period.
CA certificate revoked.	Failed validation of the X509v3 certificate. Certificate revoked.
CA certificate BasicConstraints cA flag not found.	**Windows**: Failed validation of the X.509v3 certificate. CA certificate basicConstraints flag not found or invalid. **macOS**: Basic Constraints extension required per policy, but not present.
CA certificate BasicConstraints cA flag set to 'False'.	BasicConstraintsCA = 0;StatusCodes = ("-2147408893")
EC Explicit Parameter missing.	FIPS-CC error: Non compliant FIPS-CC mode certificate. ECDSA cert with Explicit EC parameters.
Intermediate CA with basic constraints missing.	**Windows**: Failed validation of the X.509v3 certificate. CA certificate basicConstraints flag not found or invalid. **macOS**: Basic Constraints extension required per policy, but not present.

FIPS-CC Certification Validation	Error Messages
CA certificate with no CA Signing purpose in intermediate.	**Windows**: Failed validation of the X509v3 certificate. CA certificate basicConstraints flag not found or invalid. **macOS**: Invalid Key Usage for policy.
CA certificate with no CA Signing purpose in root.	**Windows**: Failed validation of the X.509v3 certificate. Missing caSigning field in the CA chain. **macOS**: Failed validation of the X.509v3 certificate. Trusted Root CA certificate not found. KeyUsage = 0;StatusCodes = ("-2147408890")
Certificate validation for revoked certificate.	Failed validation of the X.509v3 certificate: The certificate is not fips compliant. Please access the system logs for more information.
Certificate validation with certificate without cRLsign key usage bit set.	Failed validation of the X.509v3 certificate. Missing CRL Sign purpose in the (Extended) KeyUsage field.
Certificate (OCSP) validation for revoked GlobalProtect client certificate.	Connection Failed: A valid certificate is required for authentication. If the issue persists, contact your administrator.
Certificate (OCSP) validation for certificate missing OCSP signing purpose.	Failed validation of the X.509v3 OCSP signing certificate. Missing Extended Key Usage field.
Certificate validation with OCSP when the server is unreachable.	Failed validation of the X509v3 certificate. Read/Access OCSP or CRL failed.

Server Certificate Validation	Error Messages
Supported SHA-256, SHA-384, and SHA-512 only. Connection fails if any other algorithm is used (e.g. MD5). Certificates with SHA-1 are not allowed.	Failed to pre-login to the <portal> with return value 0(0).
RSA Key: Failure when length is less than 2048	Failed to pre-login to the <portal> with return value 0(0).
ECDSA Key: Failure when length is not P-256/384/521.	Failed to pre-login to the <portal> with return value 0(0).

Server Certificate Validation	Error Messages
RSA key exponent failure.	**Windows**: FIPS-CC error: Non-compliant FIPS-CC mode certificate. **macOS**: CSSMERR_CSP_UNSUPPORTED_KEY_SIZE
Server certificate expired.	Failed validation of the X.509v3 certificate: The portal certificate is not within its validity period.
Server certificate (OCSP) revoked.	Failed validation of the X509v3 certificate. Certificate revoked.
Connection failure when Extended Key Usage field is missing in server certificate.	Failed to pre-login to the <portal> with return value 0(0).
Connection failure when Server Authentication purpose is missing in the Extended key Used field.	Failed to pre-login to the <portal> with return value 0(0).

The following tables list the error messages displayed when certificate validation fails for the iOS platform. In some cases, the error messages displayed are slightly different from the expected error messages as listed out in the table. Administrators can view the error messages for troubleshooting and resolving the issues.

FIPS-CC Certification Validation	Error Messages Displayed
Key Usage missing CA Signing purpose.	Unable to build chain to root certificate.
RSA Key: Failure when length is less than 2048.	One or more certificates is using a weak signature algorithm.
RSA Key -Failure when 1024 bit server certificate is used.	One or more certificates is using a weak key size.
Missing Extended Key Usage field.	Failed validation of the X.509v3 certificate. Missing Extended Key Usage field.
Verifying server certificate must have serverAuth in EKU.	Policy requirements not met.
Verifying client certificate must have clientAuth in EKU.	Failed validation of the X.509v3 certificate. CA certificate 'CA Signing' is absent but basicConstraints may or may not be valid.

FIPS-CC Certification Validation	Error Messages Displayed
Certification path leads to an untrusted root or any CA certificate in the path has expired or revoked.	Failed validation of the X509v3 certificate. Trusted Root CA certificate not found.
Basic Constraints missing	Failed validation of the X509v3 certificate. Trusted Root CA certificate not found.
CA certificate basicConstraints flag not set to True.	Unable to build chain to root certificate.
Certificate Expired	One or more certificates have expired or are not valid yet.
Certificate Revoked	One or more certificates have expired or are not valid yet.
Weak Algorithm Used	One or more certificates is using a weak signature algorithm.
CA signing field missing	Policy requirements not met.
Read/Access for CRL Failed	Failed validation of the X509v3 certificate. Read/Access OCSP or CRL failed.
Read/Access the OCSP Failed	Failed validation of the X509v3 certificate. Read/Access OCSP or CRL failed.
OCSP certificate validation failed.	Failed validation of the X509v3 certificate. Certificate revoked.
Missing OCSP Signing purpose in the ExtendedKeyUsage field.	Failed validation of the X.509v3 OCSP signing certificate. Missing Extended Key Usage field.
OCSP certificate validation for revoked GlobalProtect client certificate	Failed validation of the X509v3 certificate. Certificate revoked.
Certificate revoked - server Certificate (OCSP)	Failed validation of the X509v3 certificate. Certificate revoked.

GlobalProtect Quick Configs

The following sections provide step-by-step instructions for configuring some common GlobalProtect™ deployments:

- Remote Access VPN (Authentication Profile)
- Remote Access VPN (Certificate Profile)
- Remote Access VPN with Two-Factor Authentication
- Always On VPN Configuration
- Remote Access VPN with Pre-Logon
- GlobalProtect Multiple Gateway Configuration
- GlobalProtect for Internal HIP Checking and User-Based Access
- Mixed Internal and External Gateway Configuration
- Captive Portal and Enforce GlobalProtect for Network Access

Refer to the knowledge base article at https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClGYCA0 for information on how to change the Active Directory password using GlobalProtect.

Remote Access VPN (Authentication Profile)

In the Figure 5: GlobalProtect VPN for Remote Access, the GlobalProtect portal and gateway are configured on **ethernet1/2**, so this is the physical interface where GlobalProtect users connect. After a user connects and authenticates to the portal and gateway, the endpoint establishes a tunnel from its virtual adapter, which has been assigned an IP address from the IP pool associated with the gateway tunnel.2 configuration—10.31.32.3-10.31.32.118 in this example. Because GlobalProtect VPN tunnels terminate in a separate **corp-vpn** zone, you have visibility into the connection traffic as well as the ability to customize security policies for remote users.

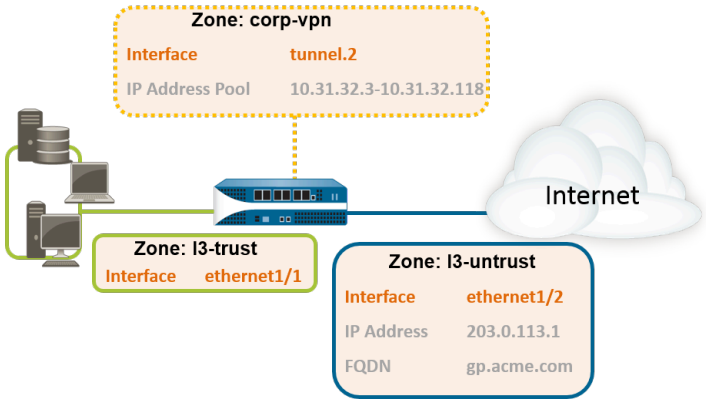


Figure 5: GlobalProtect VPN for Remote Access

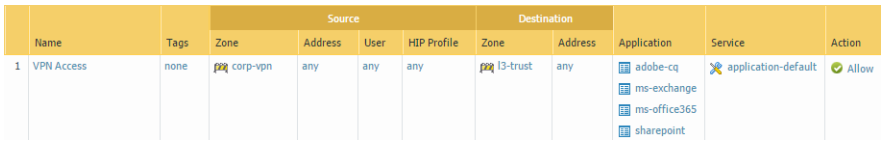
STEP 1 | Create Interfaces and Zones for GlobalProtect.

*Use the **default** virtual router for all interface configurations to avoid having to create inter-zone routing.*

- Select **Network** > **Interfaces** > **Ethernet**. Configure **ethernet1/2** as a Layer 3 Ethernet interface with IP address 203.0.113.1, and then assign it to the **l3-untrust Security Zone** and the default **Virtual Router**.
- Create a DNS "A" record that maps IP address **203.0.113.1** to **gp.acme.com**.
- Select **Network** > **Interfaces** > **Tunnel** and **Add** the **tunnel.2** interface. **Add** the tunnel interface to a new **Security Zone** called **corp-vpn**, and then assign it to the default **Virtual Router**.
- Enable User Identification on the **corp-vpn** zone.

STEP 2 | Create security policies to enable traffic flow between the **corp-vpn** zone and the **l3-trust** zone, which enables access to your internal resources.

1. Select **Policies** > **Security**, and then **Add** a new rule.
2. For this example, you would define the rule with the following settings:
   - **Name** (**General** tab)—VPN Access
   - **Source Zone** (**Source** tab)—corp-vpn
   - **Destination Zone** (**Destination** tab)—l3-trust



STEP 3 | Use one of the following methods to obtain a server certificate for the interface hosting the GlobalProtect portal and gateway:

- (Recommended) Import a server certificate from a well-known, third-party CA.
- Use the root CA on the portal to generate a self-signed server certificate.

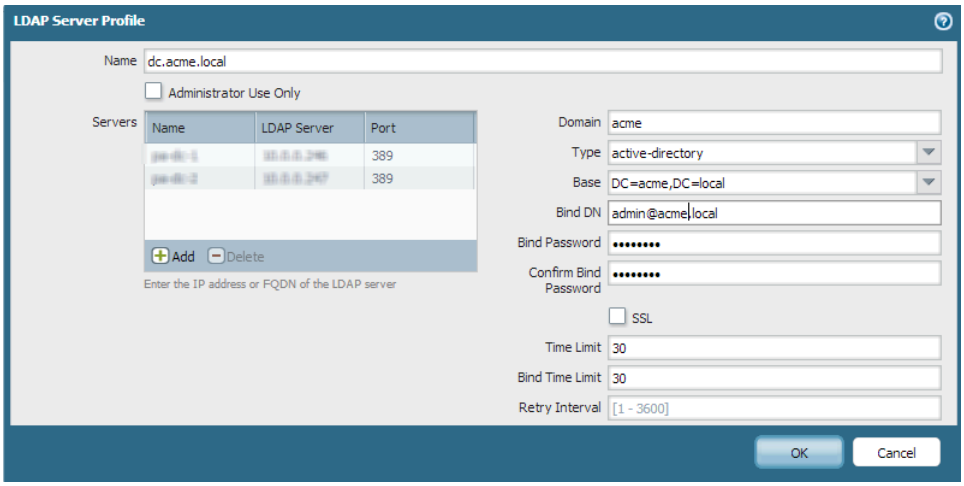
Select **Device** > **Certificate Management** > **Certificates** to manage certificates as follows:

- Obtain a server certificate. Because the portal and gateway are on the same interface, the same server certificate can be used for both components.
- The CN of the certificate must match the FQDN, `gp.acme.com`.
- To enable users to connect to the portal without receiving certificate errors, use a server certificate from a public CA.

STEP 4 | Create a server profile.

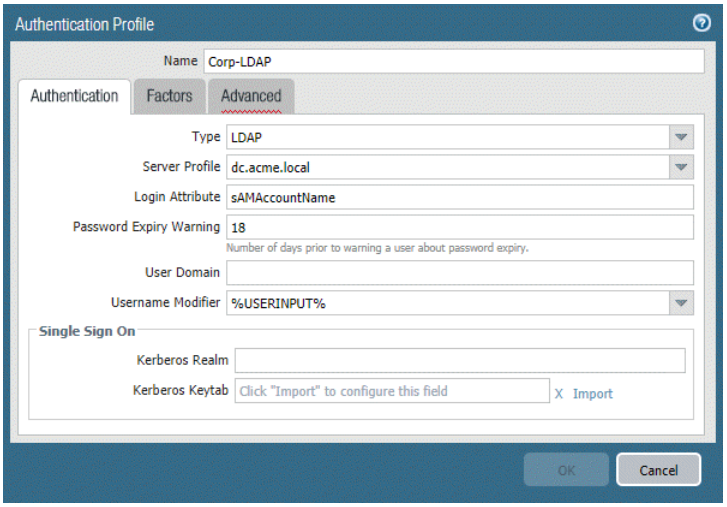
The server profile instructs the firewall on how to connect to the authentication service. Local, RADIUS, Kerberos, SAML, and LDAP authentication methods are supported. This example shows an LDAP authentication profile for authenticating users against the Active Directory.

Create the server profile for connecting to the LDAP server (**Device** > **Server Profiles** > **LDAP**).



STEP 5 | (Optional) Create an authentication profile.

Attach the server profile to an authentication profile (**Device** > **Authentication Profile**).



STEP 6 | Configure a GlobalProtect Gateway.

Select **Network** > **GlobalProtect** > **Gateways**, and then **Add** the following configuration:

Interface—`ethernet1/2`

IP Address—`203.0.113.1`

Server Certificate—`GP-server-cert.pem issued by GoDaddy`

Authentication Profile—`Corp-LDAP`

Tunnel Interface—`tunnel.2`

IP Pool—`10.31.32.3 - 10.31.32.118`

STEP 7 | Configure the GlobalProtect Portals.

Select **Network** > **GlobalProtect** > **Portals**, and then **Add** the following configuration:

1. Set Up Access to the GlobalProtect Portal:

   Interface—`ethernet1/2`

   IP Address—`203.0.113.1`

   Server Certificate—`GP-server-cert.pem issued by GoDaddy`

   Authentication Profile—`Corp-LDAP`
2. Define the GlobalProtect Client Authentication Configurations:

   Connect Method—`On-demand` (Manual user initiated connection)

   External Gateway Address—`gp.acme.com`

STEP 8 | Deploy the GlobalProtect App to End Users.

Select **Device** > **GlobalProtect Client**. Follow the procedure to Host App Updates on the Portal.

STEP 9 | (Optional) Enable use of the GlobalProtect mobile app.

Purchase and install a GlobalProtect subscription (**Device** > **Licenses**) to enable use of the app.

STEP 10 | Save the GlobalProtect configuration.

Click **Commit**.

Remote Access VPN (Certificate Profile)

With certificate authentication, the user must present a valid client certificate that identifies them to the GlobalProtect portal or gateway. To verify that a client certificate is valid, the portal or gateway checks if the client holds the private key of the certificate by using the Certificate Verify message exchanged during the SSL handshake. In addition, the client certificate is signed by the certificate authority (CA) specified in the **Issuer** field of the certificate chain. In addition to the certificate itself, the portal or gateway can use a certificate profile to determine whether the user that sent the certificate is the user to which the certificate was issued.

When a client certificate is the only means of authentication, the certificate that the user presents must contain the username in one of the certificate fields; typically the username corresponds to the common name (CN) in the Subject field of the certificate.

Upon successful authentication, the GlobalProtect app establishes a tunnel with the gateway and is assigned an IP address from the IP pool in the gateway's tunnel configuration. To support user-based policy enforcement on sessions from the **corp-vpn** zone, the username from the certificate is mapped to the IP address assigned by the gateway. If a security policy requires a domain name in addition to the user name, the domain value specified in the certificate profile is appended to the username.

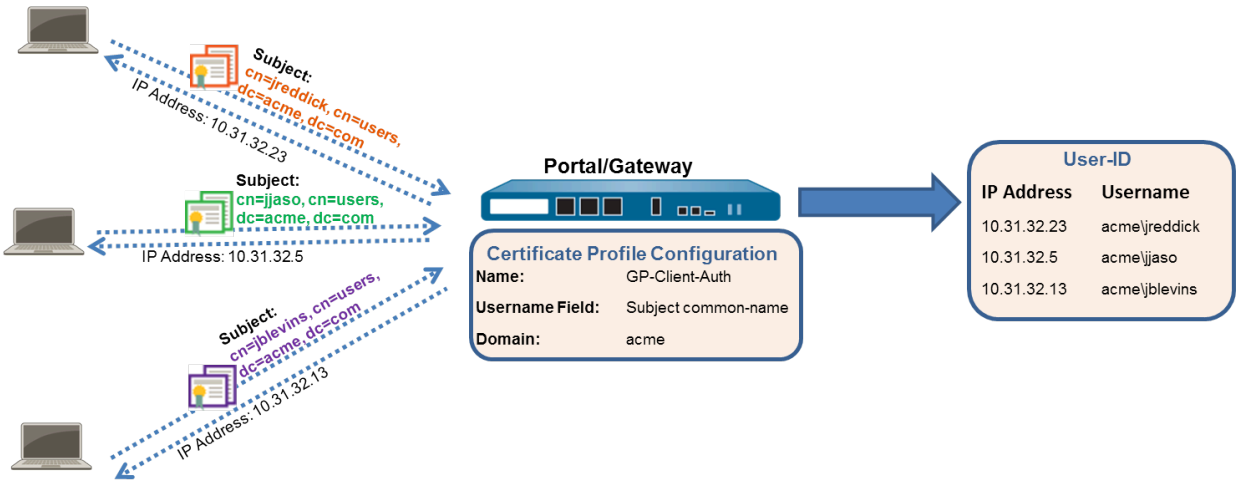


Figure 6: GlobalProtect Client Certificate Authentication Configuration

This quick configuration uses the same topology as Figure 5: GlobalProtect VPN for Remote Access. The only configuration difference is that instead of authenticating users against an external authentication server, this configuration uses client certificate authentication only.

STEP 1 | Create Interfaces and Zones for GlobalProtect.

> *Use the **default** virtual router for all interface configurations to avoid having to create inter-zone routing.*

- Select **Network** > **Interfaces** > **Ethernet**. Configure **ethernet1/2** as a Layer 3 Ethernet interface with IP address **`203.0.113.1`**, and then assign it to the **`l3-untrust`** **Security Zone** and the default **Virtual Router**.
- Create a DNS "A" record that maps IP address **`203.0.113.1`** to **`gp.acme.com`**.
- Select **Network** > **Interfaces** > **Tunnel** and **Add** the **tunnel.2** interface. Add the tunnel interface to a new **Security Zone** called `corp-vpn`, and then assign it to the default **Virtual Router**.
- Enable User Identification on the **`corp-vpn`** zone.

STEP 2 | Create security policies to enable traffic flow between the **`corp-vpn`** zone and the **`l3-trust`** zone, which enables access to your internal resources.

1. Select **Policies** > **Security**, and then **Add** a new rule.
2. For this example, you would define the rule with the following settings:
   - **Name** (**General** tab)—**`VPN Access`**
   - **Source Zone** (**Source** tab)—**`corp-vpn`**
   - **Destination Zone** (**Destination** tab)—**`l3-trust`**

	Name	Tags	Source				Destination		Application	Service	Action
			Zone	Address	User	HIP Profile	Zone	Address			
1	VPN Access	none	corp-vpn	any	any	any	l3-trust	any	adobe-cq ms-exchange ms-office365 sharepoint	application-default	Allow

STEP 3 | Use one of the following methods to obtain a server certificate for the interface hosting the GlobalProtect portal and gateway:

- (Recommended) Import a server certificate from a well-known, third-party CA.
- Use the root CA on the portal to generate a self-signed server certificate.

Select **Device** > **Certificate Management** > **Certificates** to manage certificates as follows:

- Obtain a server certificate. Because the portal and gateway are on the same interface, the same server certificate can be used for both components.
- The CN of the certificate must match the FQDN, `gp.acme.com`.
- To enable users to connect to the portal without receiving certificate errors, use a server certificate from a public CA.

STEP 4 | Issue client certificates to GlobalProtect clients and endpoints.

1. Use your enterprise PKI or a public CA to issue a unique client certificate to each GlobalProtect user.
2. Install certificates in the personal certificate store on the endpoints.

STEP 5 | Create a client certificate profile.

1. Select **Device** > **Certificate Management** > **Certificate Profile**. **Add** a new certificate profile, and then enter a profile **Name** such as **`GP-client-cert`**.
2. Select **Subject** from the **Username Field** drop-down.
3. In the **CA Certificates** area, **Add** the CA certificate that issued the client certificates. Click **OK** twice.

STEP 6 | Configure a GlobalProtect Gateway.

See the topology diagram shown in Figure 5: GlobalProtect VPN for Remote Access.

Select **Network** > **GlobalProtect** > **Gateways**, and then **Add** the following configuration:

Interface—**`ethernet1/2`**

IP Address—**`203.0.113.1`**

Server Certificate—**`GP-server-cert.pem issued by GoDaddy`**

Certificate Profile—**`GP-client-cert`**

Tunnel Interface—**`tunnel.2`**

IP Pool—**`10.31.32.3 - 10.31.32.118`**

STEP 7 | Configure the GlobalProtect Portals.

Select **Network** > **GlobalProtect** > **Portals**, and then **Add** the following configuration:

1. Set Up Access to the GlobalProtect Portal:

   Interface—`ethernet1/2`

   IP Address—`203.0.113.1`

   Server Certificate—`GP-server-cert.pem issued by GoDaddy`

   Certificate Profile—`GP-client-cert`
2. Define the GlobalProtect Agent Configurations:

   Connect Method—`On-demand` (Manual user initiated connection)

   External Gateway Address—`gp.acme.com`

STEP 8 | Deploy the GlobalProtect App to End Users.

Select **Device** > **GlobalProtect Client**. Follow the procedure to Host App Updates on the Portal.

STEP 9 | (Optional) Enable use of the GlobalProtect mobile app.

Purchase and install a GlobalProtect subscription (**Device** > **Licenses**) to enable use of the app.

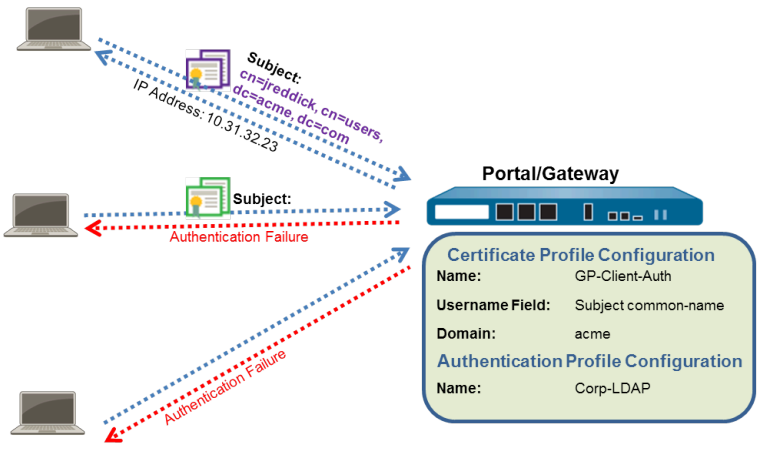
STEP 10 | Save the GlobalProtect configuration.

Click **Commit**.

Remote Access VPN with Two-Factor Authentication

If you configure a GlobalProtect portal or gateway with an authentication profile and a certificate profile (which together can provide two-factor authentication), the end user must authentication through both profiles successfully before gaining access. For portal authentication, this means that certificates must be pre-deployed on the endpoints before their initial portal connection. Additionally, the client certificate presented by a user must match what is defined in the certificate profile.

- If the certificate profile does not specify a username field (**Username Field** is set to **None**), the client certificate does not require a username. In this case, the user must provide the username when authenticating against the authentication profile.
- If the certificate profile specifies a username field, the certificate that the user presents must contain a username in the corresponding field. For example, if the certificate profile specifies that the username field is **Subject**, the certificate presented by the user must contain a value in the common-name field, or else authentication fails. In addition, when the username field is required, the value from the username field of the certificate is automatically populated as the username when the user attempts to enter credentials for authenticating to the authentication profile. If you do not want force users to authenticate with a username from the certificate, do not specify a username field in the certificate profile.



This quick configuration uses the same topology as Figure 5: GlobalProtect VPN for Remote Access. However, in this configuration, users must authenticate against a certificate profile and an authentication profile. For more details on a specific type of two-factor authentication, see the following topics:

- Enable Two-Factor Authentication Using Certificate and Authentication Profiles
- Enable Two-Factor Authentication Using One-Time Passwords (OTPs)
- Enable Two-Factor Authentication Using Smart Cards
- Enable Two-Factor Authentication Using a Software Token Application

Use the following procedure to configure remote VPN access with two-factor authentication.

STEP 1 | Create Interfaces and Zones for GlobalProtect.

> *Use the **default** virtual router for all interface configurations to avoid having to create inter-zone routing.*

- Select **Network** > **Interfaces** > **Ethernet**. Configure **ethernet1/2** as a **Layer3** Ethernet interface with IP address **`203.0.113.1`** and assign it to the **`l3-untrust` Security Zone** and the default **Virtual Router**.
- Create a DNS "A" record that maps IP address **`203.0.113.1`** to **`gp.acme.com`**.
- Select **Network** > **Interfaces** > **Tunnel** and **Add** the **tunnel.2** interface. Add the tunnel interface to a new **Security Zone** called **`corp-vpn`**, and then assign it to the default **Virtual Router**.
- Enable User Identification on the **`corp-vpn`** zone.

STEP 2 | Create security policies to enable traffic flow between the **`corp-vpn`** zone and the **`l3-trust`**zone, which enables access to your internal resources.

1. Select **Policies** > **Security**, and then click **Add** to create a new rule.
2. For this example, you would define the rule with the following settings:
   - **Name** (**General** tab)—**`VPN Access`**
   - **Source Zone** (**Source** tab)—**`corp-vpn`**
   - **Destination Zone** (**Destination** tab)—**`l3-trust`**

	Name	Tags	Source				Destination		Application	Service	Action
			Zone	Address	User	HIP Profile	Zone	Address			
1	VPN Access	none	corp-vpn	any	any	any	l3-trust	any	adobe-cq ms-exchange ms-office365 sharepoint	application-default	Allow

STEP 3 | Use one of the following methods to obtain a server certificate for the interface hosting the GlobalProtect portal and gateway:

- (Recommended) Import a server certificate from a well-known, third-party CA.
- Use the root CA on the portal to generate a self-signed server certificate.

Select **Device** > **Certificate Management** > **Certificates** to manage certificates as follows:

- Obtain a server certificate. Because the portal and gateway are on the same interface, the same server certificate can be used for both components.
- The CN of the certificate must match the FQDN, **`gp.acme.com`**.
- To enable users to connect to the portal without receiving certificate errors, use a server certificate from a public CA.

STEP 4 | Issue client certificates to GlobalProtect clients and endpoints.

1. Use your enterprise PKI or a public CA to issue a unique client certificate to each GlobalProtect user.
2. Install certificates in the personal certificate store on the endpoints.

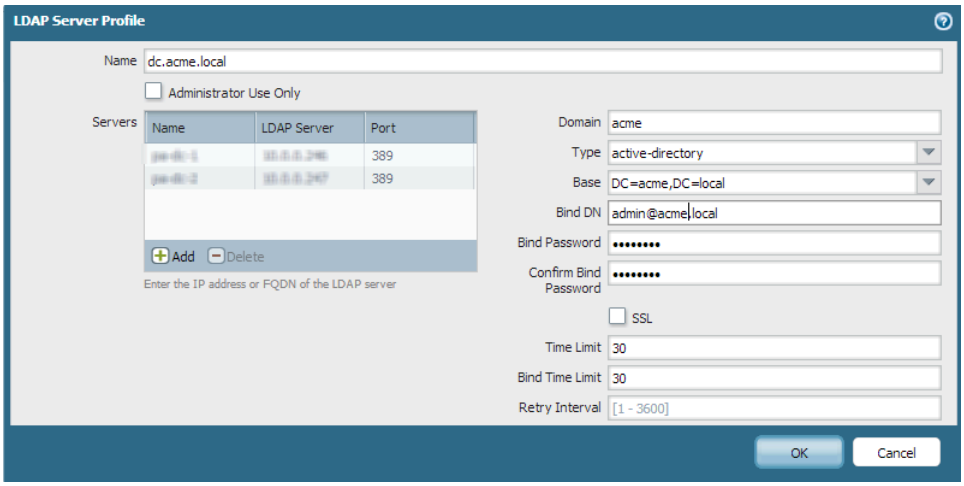
STEP 5 | Create a client certificate profile.

1. Select **Device** > **Certificate Management** > **Certificate Profile**. **Add** a new certificate profile, and then enter a profile **Name** such as **`GP-client-cert`**.
2. Specify where to obtain the username that will be used to authenticate the end user:
   - **From user**—If you want the end user to supply a username when authenticating to the service specified in the authentication profile, select **None** as the **Username Field**.
   - **From certificate**—If you want to extract the username from the certificate, select **Subject** as the **Username Field**. If you use this option, the CN contained in the certificate automatically populates the username field when the user is prompted to log in to the portal/gateway. The user is required to log in using that username.
3. In the **CA Certificates** area, **Add** the CA certificate that issued the client certificates. Click **OK** twice.

STEP 6 | Create a server profile.

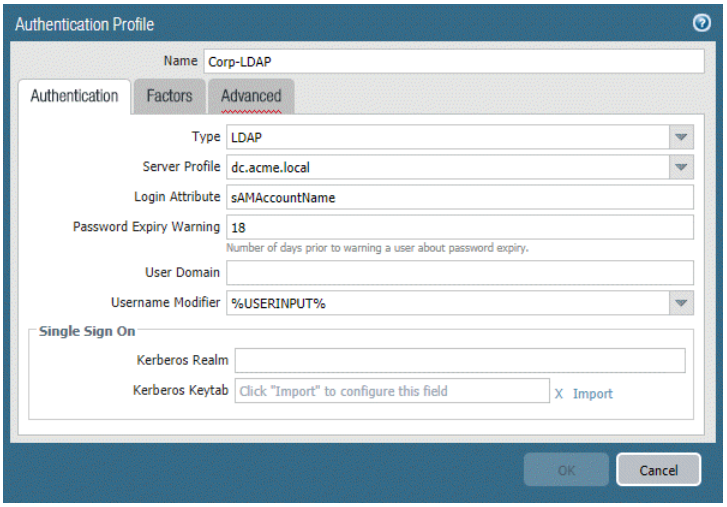
The server profile instructs the firewall on how to connect to the authentication service. Local, RADIUS, Kerberos, SAML, and LDAP authentication methods are supported. This example shows an LDAP authentication profile for authenticating users against the Active Directory.

Create the server profile for connecting to the LDAP server (**Device** > **Server Profiles** > **LDAP**).



STEP 7 | (Optional) Create an authentication profile.

Attach the server profile to an authentication profile (**Device > Authentication Profile**).



STEP 8 | Configure a GlobalProtect Gateway.

See the topology diagram shown in Figure 5: GlobalProtect VPN for Remote Access.

Select **Network** > **GlobalProtect** > **Gateways**, and then **Add** the following configuration:

Interface—**ethernet1/2**

IP Address—**203.0.113.1**

Server Certificate—**GP-server-cert.pem issued by GoDaddy**

Certificate Profile—**GP-client-cert**

Authentication Profile—**Corp-LDAP**

Tunnel Interface—**tunnel.2**

IP Pool—**10.31.32.3 - 10.31.32.118**

STEP 9 | Configure the GlobalProtect Portals.

Select **Network** > **GlobalProtect** > **Portals**, and then **Add** the following configuration:

1. Set Up Access to the GlobalProtect Portal:

   Interface—**ethernet1/2**

   IP Address—**203.0.113.1**

   Server Certificate—**GP-server-cert.pem issued by GoDaddy**

   Certificate Profile—**GP-client-cert**

   Authentication Profile—**Corp-LDAP**
2. Define the GlobalProtect Agent Configurations:

   Connect Method—**On-demand** (Manual user initiated connection)

   External Gateway Address—**gp.acme.com**

STEP 10 | Deploy the GlobalProtect App to End Users.

Select **Device** > **GlobalProtect Client.**. Follow the procedure to Host App Updates on the Portal.

STEP 11 | (Optional) Deploy App Settings Transparently.

As an alternative to deploying app settings from the portal configuration, you can define settings directly from the Windows registry or global macOS plist. Examples of settings that you can deploy include specifying the portal IP address or enabling GlobalProtect to initiate a VPN tunnel before a user logs in to the endpoint and connects to the GlobalProtect portal. On Windows endpoints only, you can also configure settings using the MSIEXEC installer. For additional information, see Customizable App Settings.

STEP 12 | (Optional) Enable use of the GlobalProtect mobile app.

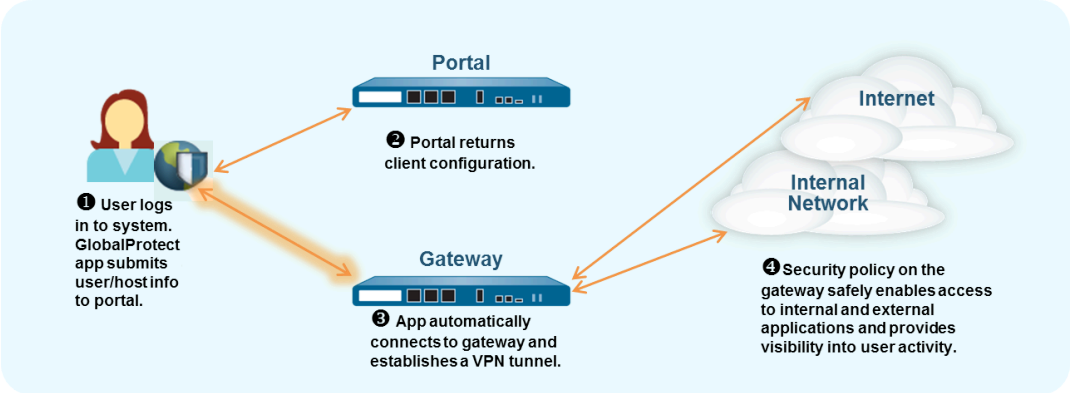
Purchase and install a GlobalProtect subscription (**Device** > **Licenses**) to enable use of the app.

STEP 13 | Save the GlobalProtect configuration.

Click **Commit**.

Always On VPN Configuration

In an “Always On” GlobalProtect configuration, the app connects to the GlobalProtect portal (upon user login) to submit user and host information and receive the client configuration. The app then automatically connects and establishes a VPN tunnel to the gateway that was specified in the client configuration delivered by the portal, as shown in the following image:



To switch one of the following remote access VPN configurations to an Always On configuration, you can change the connect method:

- Remote Access VPN (Authentication Profile)
- Remote Access VPN (Certificate Profile)
- Remote Access VPN with Two-Factor Authentication

Use the following steps to switch a remote access VPN configuration to an Always On configuration.

STEP 1 | Select **Network** > **GlobalProtect** > **Portals**, and then select a portal configuration.

STEP 2 | On the **Agent** tab, select the agent configuration that you want to modify.

STEP 3 | Select **App**, and then set the **Connect Method** to **User-logon (Always On)**.

STEP 4 | Click **OK** to save the agent configuration.

STEP 5 | Repeat steps 2-4 for each agent configuration that you want to modify.

STEP 6 | Click **OK** to save the portal configuration, and then **Commit** your changes.

Remote Access VPN with Pre-Logon

Pre-logon is a connect method that establishes a VPN tunnel before a user logs in. The purpose of pre-logon is to authenticate the endpoint (not the user) and enable domain scripts or other tasks to run as soon as the endpoint powers on. Machine certificates enable the endpoint to establish a VPN tunnel to the GlobalProtect gateway. A common practice for IT administrators is to install the machine certificate while staging the endpoint for the user.

A pre-logon VPN tunnel has no username association because the user has not logged in. To allow endpoints to access resources, you must create security policies that match the pre-logon user. These policies should allow access to only the basic services for starting up the system, for example DHCP, DNS, specific Active Directory services, antivirus, or operating system update services. After the user authenticates to the gateway, the GlobalProtect app reassigns the VPN tunnel to that user (the IP address mapping on the firewall changes from the pre-logon endpoint to the authenticated user).

As a best practice, you must create security policies to allow access to only specific services (for example, DHCP, DNS, specific Active Directory services, or operating system update services) that are sufficient for machine authentication and to enable services that are necessary for the corporate network. We recommend that you create security policies to deny pre-logon users access to other resources and applications.

Follow these guidelines if the user's endpoint is lost or stolen:

- *You must revoke the machine certificate that is issued to the endpoint for pre-logon. Once the machine certificate is revoked for the pre-logon connect method, you cannot use the certificate to authenticate against the portal and gateway because authentication to the endpoint failed and the endpoint is unable to connect to the corporate network.*
- *You can quarantine lost or stolen endpoints by Manually Add and Delete Devices From the Quarantine List, Use GlobalProtect and Security Policies to Block Access to Quarantined Devices from that endpoint, and to prevent VPN connections from these compromised endpoints.*
- *You must disable the stolen endpoint computer account in the Active Directory to block VPN connections from disabled machine accounts based on the presence of the Define the GlobalProtect Agent Configurations. When this feature is used, authentication attempts from the disabled computer account will fail while attempting to prevent VPN connections from the lost or stolen endpoint.*

The GlobalProtect Credential Provider logon screen for Windows 7 and Windows 10 endpoints also displays the pre-logon connection status prior to user login, which allows end users to determine whether they can access network resources upon login. If the GlobalProtect app detects an endpoint as internal, the logon screen displays the **Internal** pre-logon connection status. If the Globalprotect app detects an endpoint as external, the logon screen displays the **Connected** or **Not Connected** pre-logon connection status.

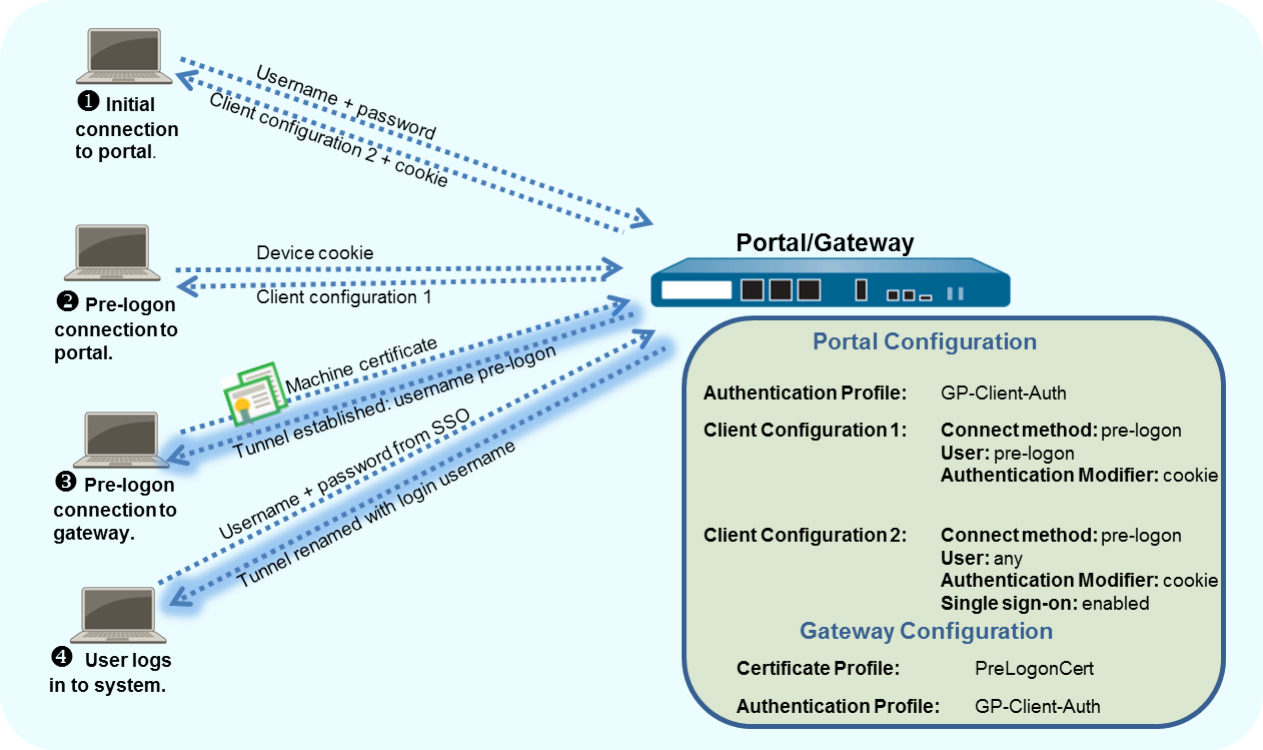
Windows endpoints behave differently from macOS endpoints with pre-logon. With macOS endpoints, the pre-logon tunnel is torn down, and then a new tunnel is created when the user logs in.

When a user requests a new connection, the portal authenticates the user through an authentication profile. The portal can also use an optional certificate profile that validates the client certificate (if the configuration includes a client certificate). In this case, the certificate must identify the user. After authentication, the portal determines if the endpoint's GlobalProtect configuration is current. If the portal's configuration has changed, it pushes an updated configuration to the endpoint.

If the configuration on the portal or a gateway includes cookie-based authentication, the portal or gateway installs an encrypted cookie on the endpoint. Subsequently, the portal or gateway uses the cookie to authenticate users and refresh the agent configuration. If an agent configuration profile includes the pre-logon connect method in addition to cookie-authentication, the GlobalProtect components can use the cookie for pre-logon.

If users never log in to an endpoint (for example, a headless endpoint) or a pre-logon connection is required on a system that a user has not previously logged in to, you can let the endpoint initiate a pre-logon tunnel without first connecting to the portal to download the pre-logon configuration. To do this, you must override the default behavior by creating entries in the Windows Registry or macOS plist.

The GlobalProtect endpoint will then connect to the portal specified in the configuration, authenticate the endpoint by using its machine certificate (as specified in a certificate profile configured on the gateway), and then establish the GlobalProtect connection. When the end-user subsequently logs in to the machine, and if single sign-on (SSO) is enabled in the agent configuration, the username and password are captured when the user logs in. If SSO is not enabled in the agent configuration, or SSO is not supported on the endpoint (for example, a macOS system) the user's credentials must be stored in the app (the **Save User Credentials** option must be set to **Yes**). After successful authentication to the gateway, the tunnel is renamed (Windows) or rebuilt (macOS), and user and group-based policy can be enforced.



This example uses the GlobalProtect topology shown in Figure 5: GlobalProtect VPN for Remote Access.

STEP 1 | Create Interfaces and Zones for GlobalProtect.

*Use the **default** virtual router for all interface configurations to avoid having to create inter-zone routing.*

- For this example, select the **Network** > **Interfaces** > **Ethernet** tab, and then configure the following settings:
  1. Select **ethernet1/2**.
  2. Select **Layer 3** from the **Interface Type** drop-down.
  3. On the **Config** tab, **Assign interface to** the default **Virtual Router** and the **`l3-untrust`** **Security Zone**.
  4. On the **IPv4** tab, click **Add** to select the **`203.0.113.1`** IP address (or the object that maps **`203.0.113.1`**) or add a **New Address** to create a new object and address mapping

(leave the address type as **Static**). For example, create a DNS "A" record that maps IP address **203.0.113.1** to **gp.acme.com**.

- Select **Network** > **Interfaces** > **Tunnel** to **Add** a new tunnel interface.
  1. For the **Interface Name**, enter **tunnel.2**.
  2. On the **Config** tab, **Assign Interface To** a new **Security Zone** called **corp-vpn** and the default **Virtual Router**.
- Enable User Identification on the **corp-vpn** zone.

STEP 2 | Create the security policy rules.

This configuration requires the following policies (**Policies** > **Security**):

1. For enhanced security, **Add** a rule that enables pre-logon users access to basic services that are required for the endpoint to come up, such as required authentication services, DNS, DHCP, and Microsoft Updates.

   You must ensure that all security policy rules are properly setup to allow pre-logon users access to only services that are required for the endpoint.
2. **Add** a rule to deny pre-logon users access to all other resources and applications.
3. **Add** any additional rules to enable different users or user groups access to specific resources and applications. Follow the Best Practice Internet Gateway_Security_Policy recommendations for creating these rules.

STEP 3 | Use one of the following methods to obtain a server certificate for the interface that is hosts the GlobalProtect portal and gateway:

- (Recommended) Import a server certificate from a well-known, third-party CA.
- Use the root CA on the portal to generate a self-signed server certificate.

Select **Device** > **Certificate Management** > **Certificates** to manage certificates with the following criteria:

- Obtain a server certificate. Because the portal and gateway are on the same interface, the same server certificate can be used for both components.
- The CN of the certificate must match the FQDN, **gp.acme.com**.
- To enable endpoints to connect to the portal without receiving certificate errors, use a server certificate from a public CA.

STEP 4 | Generate a machine certificate for each endpoint that connects to GlobalProtect, and then import the certificate into the personal certificate store on each machine.

Although you can generate self-signed certificates for each endpoint, as a best practice, use your own public-key infrastructure (PKI) to issue and distribute certificates to your endpoints.

1. Issue client certificates to GlobalProtect clients and endpoints.
2. Install certificates in the personal certificate store on the endpoints. (Local Computer store on Windows endpoints or System Keychain on macOS endpoints)

STEP 5 | Import the trusted root CA certificate from the CA that issued the machine certificates onto the portal and gateway(s).

You do not have to import the private key.

1. Download the CA certificate in Base64 format.
2. Use the following steps to import the certificate onto each firewall that hosts a portal or gateway:
   1. Select **Device** > **Certificate Management** > **Certificates** > **Device Certificates** and **Import** the certificate.
   2. Enter a **Certificate Name** that identifies the certificate as your client CA certificate.
   3. **Browse** for the **Certificate File** that you downloaded from the CA.
   4. Set the **File Format** to **Base64 Encoded Certificate (PEM)**.
   5. Click **OK** to save your certificate.
   6. On the **Device Certificates** tab, select the certificate that you just imported.
   7. Select the check box for **Trusted Root CA**, and then click **OK**.

STEP 6 | On each firewall that hosts a GlobalProtect gateway, create a certificate profile to identify the CA certificate for validating the machine certificates.

If you plan to use client certificate authentication to authenticate users when they log in to the system, make sure that the CA certificate that issues the client certificates is referenced in the certificate profile in addition to the CA certificate that issued the machine certificates (if they are different).

1. Select **Device** > **Certificates** > **Certificate Management** > **Certificate Profile** and **Add** a new certificate profile.
2. Enter a **Name** to identify the profile, such as **`PreLogonCert`**.
3. Set the **Username Field** to **None**.
4. (Optional) If you also use client certificate authentication to authenticate users upon login, add the CA certificate that issued the client certificates if it is different from the one that issued the machine certificates.
5. In the **CA Certificates** field, **Add** the CA certificate.
6. Select the Trusted Root **CA Certificate** that you imported in step 5, and then click **OK**.
7. Click **OK** to save the profile.

STEP 7 | Configure a GlobalProtect Gateway.

See the topology diagram shown in Figure 5: GlobalProtect VPN for Remote Access.

Although you must create a certificate profile for pre-logon access to the gateway, you can use either client certificate authentication or authentication profile-based authentication for

logged in users. In this example, the same LDAP profile is used that is used to authenticate users to the portal.

1. Select **Network** > **GlobalProtect** > **Gateways**, and then **Add** the following gateway configuration:

   Interface—**ethernet1/2**

   IP Address—**203.0.113.1**

   Server Certificate—**GP-server-cert.pem issued by GoDaddy**

   Certificate Profile—**PreLogonCert**

   Authentication Profile—**Corp-LDAP**

   Tunnel Interface—**tunnel.2**

   IP Pool—**10.31.32.3 - 10.31.32.118**
2. **Commit** the gateway configuration.

STEP 8 | Configure the GlobalProtect Portals.

Configure the **Device** details (networking parameters, authentication service profile, and certificate for the authentication server).

Select **Network** > **GlobalProtect** > **Portals**, and then **Add** the following portal configuration:

Set Up Access to the GlobalProtect Portal:

Interface—**ethernet1/2**

IP Address—**203.0.113.1**

Server Certificate—**GP-server-cert.pem issued by GoDaddy**

Certificate Profile—**None**

Authentication Profile—Corp-LDAP

STEP 9 | Define the GlobalProtect Agent Configurations for pre-logon users and for logged in users.

You must create security policy rules to deny access to services not required for pre-logon users and only allow access to services that are mandatory for pre-logon users.

Use a single configuration if you want pre-logon users to access the same gateways before and after they log in.

To direct pre-logon users to different gateways before and after they log in, create two configuration profiles. In the first configuration's **User/User Group**, select the **pre-logon** filter. With pre-logon, the portal first authenticates the endpoint (not the user) to set up a

connection even though the pre-logon parameter is associated with the user. Subsequently, the portal authenticates the user when he or she logs in.

After the portal authenticates the user, it deploys the second configuration. In this case, **User/User Group** is **any**.

*As a best practice, enable SSO in the second configuration so that the correct username is immediately reported to the gateway when the user logs in to the endpoint. If SSO is not enabled, the saved username in the **Agent** settings panel is used.*

Select the **Agent** tab of the **GlobalProtect Portal Configuration** window (**Network** > **GlobalProtect** > **Portals** > **<portal-config>**), and then **Add** one of the following configurations:

- Use the same gateway before and after pre-logon users log in:

  Use single sign-on—**`enabled`**

  Connect Method—**`pre-logon`**

  External Gateway Address—**`gp1.acme.com`**

  User/User Group—**`any`**

  Authentication Override—Cookie authentication for transparently authenticating users and for configuration refresh
- Use separate gateways for pre-logon users before and after they log in:

  First Agent Configuration:

  Connect Method—**`pre-logon`**

  External Gateway Address—**`gp1.acme.com`**

  User/User Group—**`pre-logon`**

  Authentication Override—Cookie authentication for transparently authenticating users and for configuration refresh

  Second Agent Configuration:

  Use single sign-on—**`enabled`**

  Connect Method—**`pre-logon`**

  External Gateway Address—**`gp2.acme.com`**

  User/User Group—**`any`**

  Authentication Override—Cookie authentication for transparently authenticating users and for configuration refresh

  Make sure the pre-logon configuration is first in the list of configurations. If it is not, select it and click **Move Up**.

STEP 10 | Save the GlobalProtect configuration.

Click **Commit**.

STEP 11 | (Optional) If users never log in to an endpoint (for example, a headless endpoint), or a pre-logon connection is required on an endpoint that users have not previously logged in to, create the `Prelogon` registry entry on the endpoint.

You must also pre-deploy the default portal IP address.

For more information about registry settings, see Deploy App Settings Transparently.

1. Go to the following Windows Registry location to view the list of GlobalProtect settings:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup`
2. Select **Edit** > **New** > **String Value** to create the following registry entries:
   - Create a **String Value** named **`Prelogon`** with a value of **`1`**. This setting enables GlobalProtect to initiate a connection before the user logs in to the endpoint.
   - Create a **String Value** named **`Portal`** that specifies the IP address or hostname of the default portal for the GlobalProtect endpoint.

User-Initiated Pre-Logon Connection

Where Can I Use This?	What Do I Need?
• GlobalProtect	• Supported only on Windows 10 or later endpoints • GlobalProtect app version 5.0.3 or later for Windows

Enable end users to initiate the GlobalProtect Remote Access VPN with Pre-Logon connection manually on Windows 10 endpoints. User-initiated pre-logon requires that you **Use Single Sign-On** in your portal configuration. In this deployment, users can initiate the pre-logon connection only when their endpoint requires access to the corporate network before login, such as when new employees connect to the network remotely for the first time or when administrators must remotely connect and troubleshoot issues on the endpoint. To initiate the pre-logon connection, users must **Start GlobalProtect Connection** from the GlobalProtect credential provider logon screen after the endpoint boots up.

*If users are unable to establish the pre-logon connection using this option, the pre-logon connection status remains **Disconnected**.*

When users log out of their endpoint, the VPN tunnel is not renamed from the user tunnel back to the pre-logon tunnel. Instead, the tunnel disconnects.

Use the following steps to enable users to initiate the pre-logon connection manually:

You can configure this option only in the Windows Registry. This configuration can be done either manually after GlobalProtect is installed or pre-deployed as part of the Windows image that includes the GlobalProtect software.

STEP 1 | Configure remote access VPN with pre-logon.

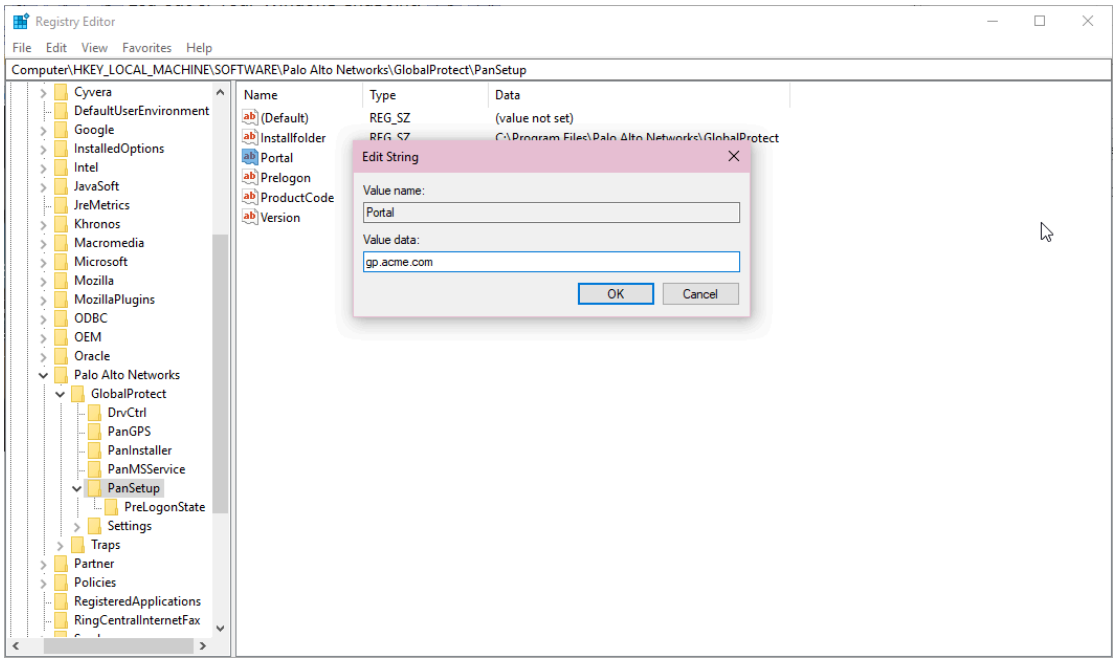
Use one of the following options to configure remote access VPN with pre-logon:

- If your end user will be connecting to the GlobalProtect portal before using this feature (for example, an existing employee who has previously connected to GlobalProtect), you can configure remote access VPN with pre-logon in the portal configuration.

  To enable users to initiate the pre-logon connection manually, you must configure the following options in your portal configuration:

  - Specify a portal **IP address** (**Network** > **GlobalProtect** > **Portals** > ***<portal-config>*** > **General**).
  - Set the GlobalProtect **Connect Method** to **Pre-logon (Always On)** or **Pre-logon then On-demand** (**Network** > **GlobalProtect** > **Portals** > ***<portal-config>*** > **Agent** > ***<agent-config>*** > **App**).
  - Set the **Use Single Sign-On** option to **Yes** to enable GlobalProtect to use Windows login credentials to automatically authenticate users upon Active Directory login (**Network** > **GlobalProtect** > **Portals** > ***<portal-config>*** > **Agent** > ***<agent-config>*** > **App**).
- If your end user will not be connecting to the GlobalProtect portal before using this feature (for example, a new employee who is connecting to the network remotely for the first time), you must pre-deploy the pre-logon settings in the Windows Registry:

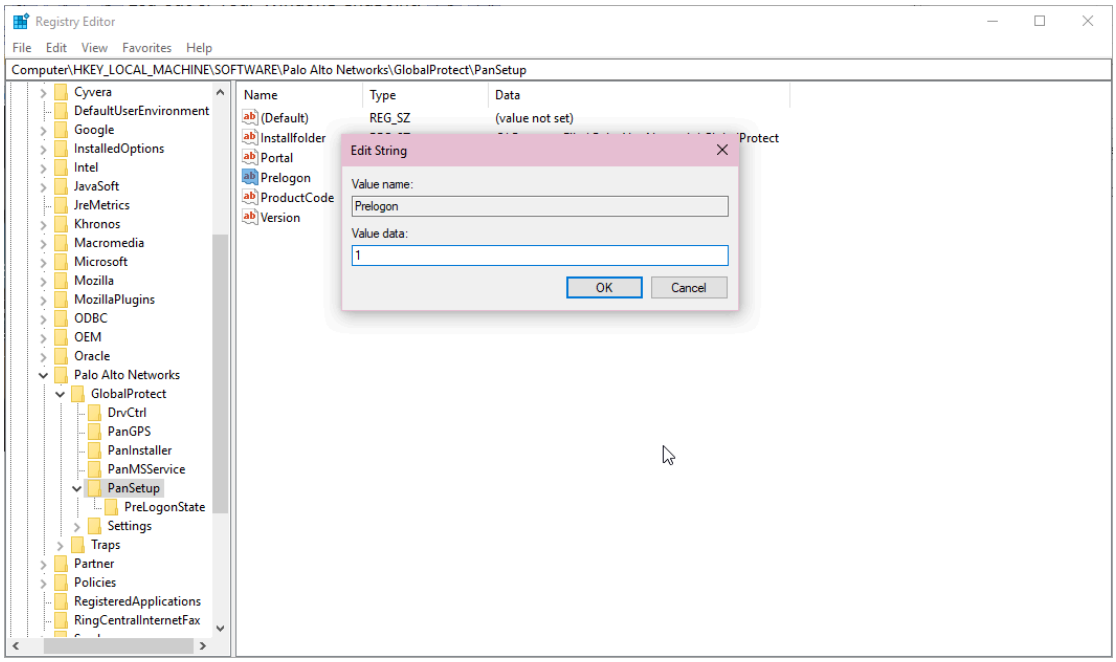
  1. From your Windows endpoint, launch the Command Prompt.
  2. Enter **`regedit`** to open the Windows Registry.
  3. In the Windows Registry, go to: `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup\`.
  4. Specify a portal address:
     1. From the list of PanSetup options, right-click **Portal** and then select **Modify...** to update the portal address.
     2. Enter the portal address in the **Value data** field.



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

5. Enable pre-logon:

   1. From the list of PanSetup options, right-click **Prelogon** and then select **Modify...**.
   2. To enable pre-logon, set the **Value data** to **1**.



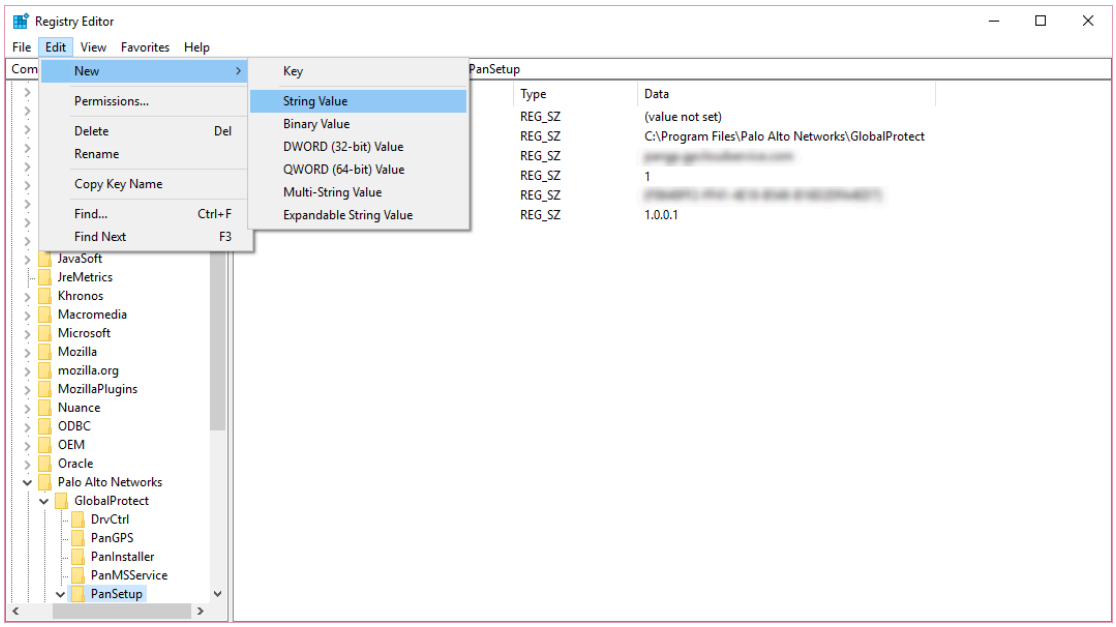
*To disable pre-logon, set the **Value data** to **0**.*

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

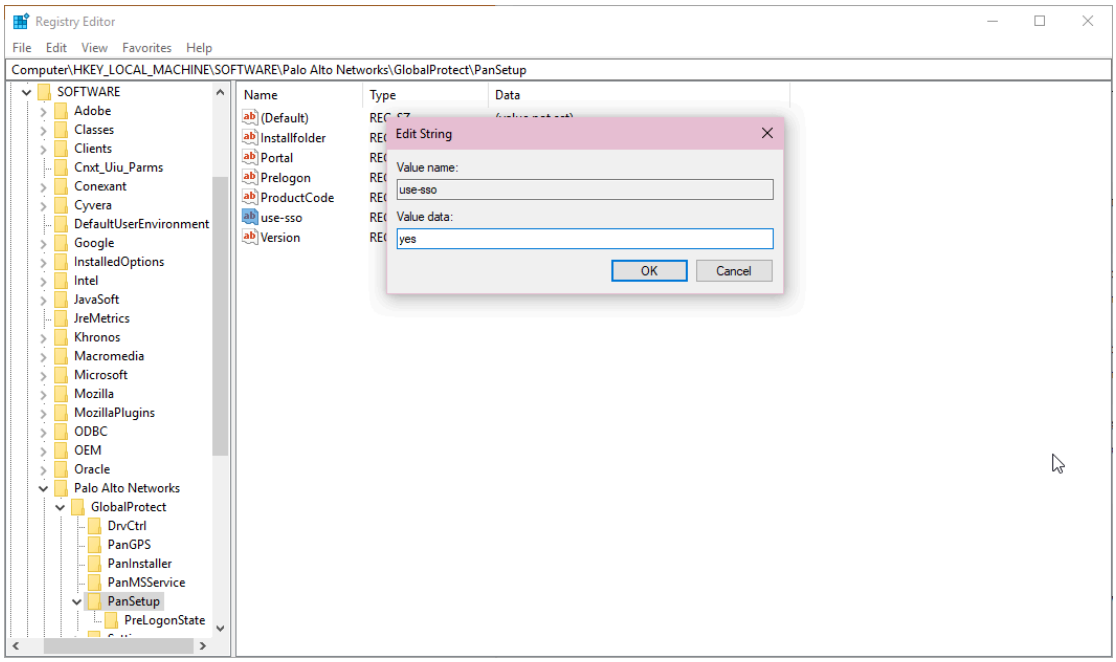
6. Enable single sign-on (SSO):

   When you enable single sign-on, GlobalProtect uses Windows login credentials to automatically authenticate users upon Active Directory login.

   1. Select **Edit** > **New** > **String Value** to add the option to use single sign-on.



2. When prompted, set the **Name** to **`use-sso`**.
3. Right-click **Use-SSO** and then select **Modify...** to update the single sign-on settings.
4. To enable single sign-on, set the **Value data** to **yes**

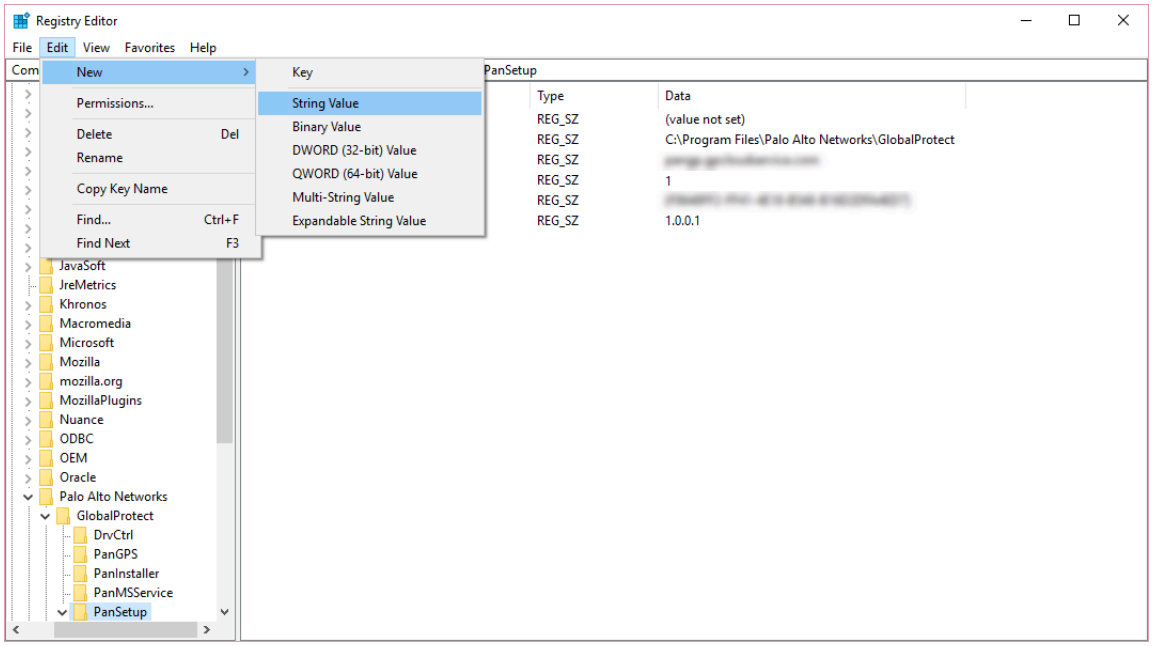


*To disable single sign-on, set the **Value data** to **no**.*

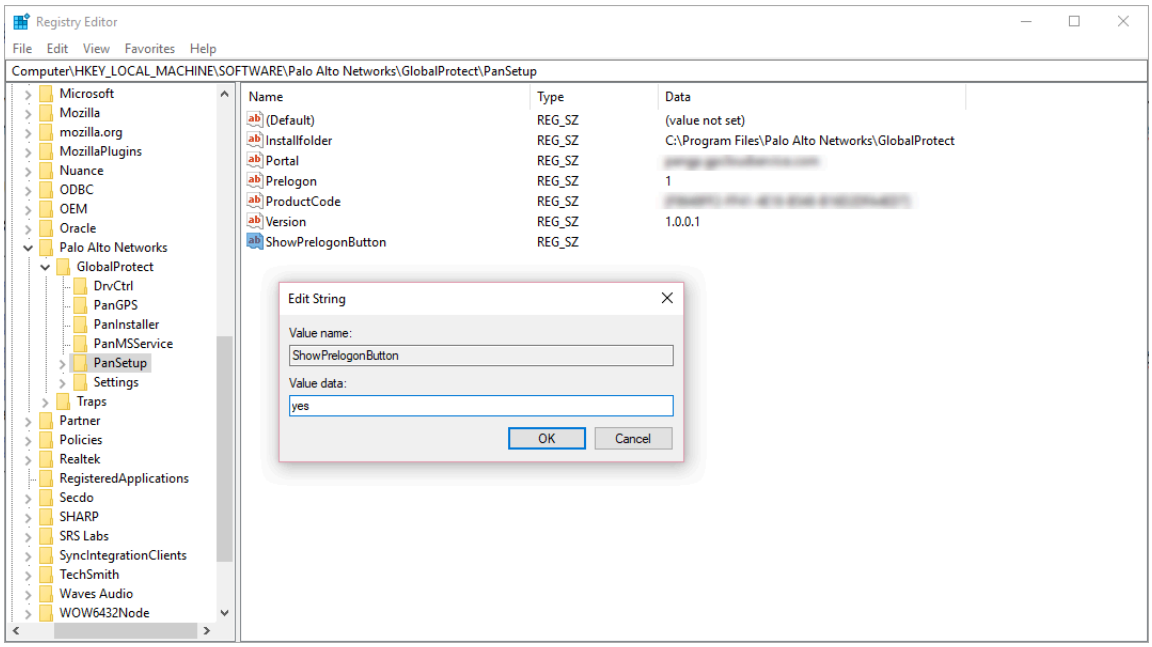
5. Click **OK** to save your changes.

STEP 2 | From the Windows Registry, enable the option to display the **Start GlobalProtect Connection** button on the GlobalProtect credential provider logon screen.

1. From your Windows endpoint, launch the Command Prompt.
2. Enter **`regedit`** to open the Windows Registry.
3. In the Windows Registry, go to: `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup\`.
4. Select **Edit** > **New** > **String Value** to add the button display option.



5. When prompted, set the **Name** to **`ShowPrelogonButton`**.
6. Right-click **ShowPrelogonButton** and then select **Modify...** to update the button display settings.
7. To enable the GlobalProtect credential provider to display the **Start GlobalProtect Connection** button, set the **Value data** to **`yes`**.



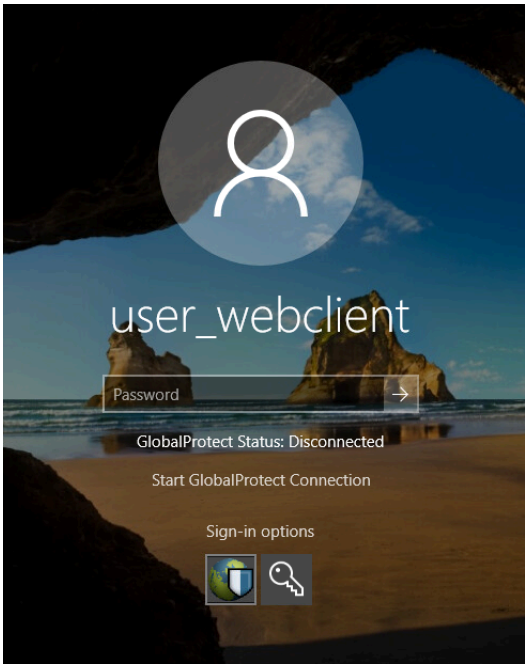
*To disable the **ShowPrelogonButton** option, set the **Value data** to **no**. Alternatively, you can right-click **ShowPrelogonButton** to **Delete** the option.*

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

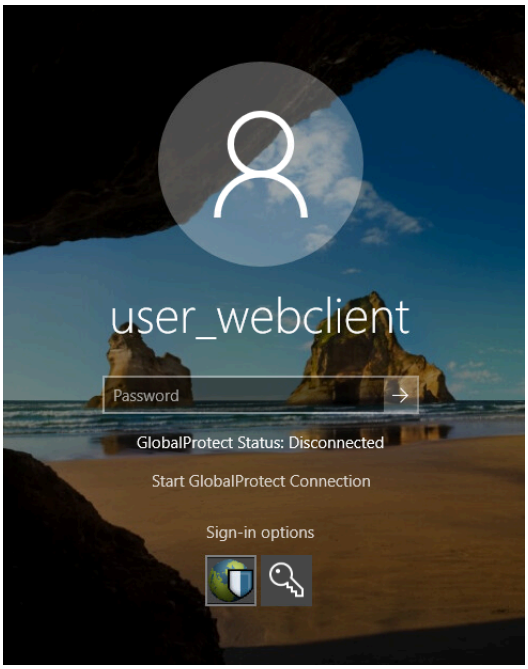
STEP 3 | Verify that the GlobalProtect credential provider displays the **Start GlobalProtect Connection** button so users can initiate the pre-logon connection manually.

Depending on which option you used to configure remote access VPN with pre-logon (step 1), use one of the following options to verify that the GlobalProtect credential provider displays the **Start GlobalProtect Connection** button:

- If you configured remote access VPN with pre-logon on your firewall, use the following steps to verify that the button is displayed:
  1. From you Windows endpoint, launch the GlobalProtect app.
  2. **Connect** to GlobalProtect to download the portal agent configuration that you configured in step 1.
  3. Reboot your Windows endpoint.
  4. When the GlobalProtect credential provider logon screen appears, ensure that the **Start GlobalProtect Connection** button is displayed and the pre-logon connection status is **Disconnected**.



- If you pre-deployed the pre-logon settings in the Windows Registry, use the following steps to verify that the button is displayed:
  1. Reboot your Windows endpoint.
  2. When the GlobalProtect credential provider logon screen appears, ensure that the **Start GlobalProtect Connection** button is displayed and the pre-logon connection status is **Disconnected**.



GlobalProtect Multiple Gateway Configuration

In the Figure 7: GlobalProtect Multiple Gateway Topology below, a second external gateway is added to the configuration. In this topology, you must configure an additional firewall to host the second GlobalProtect gateway. When you add the client configurations to be deployed by the portal, you can also specify different gateways for different client configurations or allow access to all gateways.

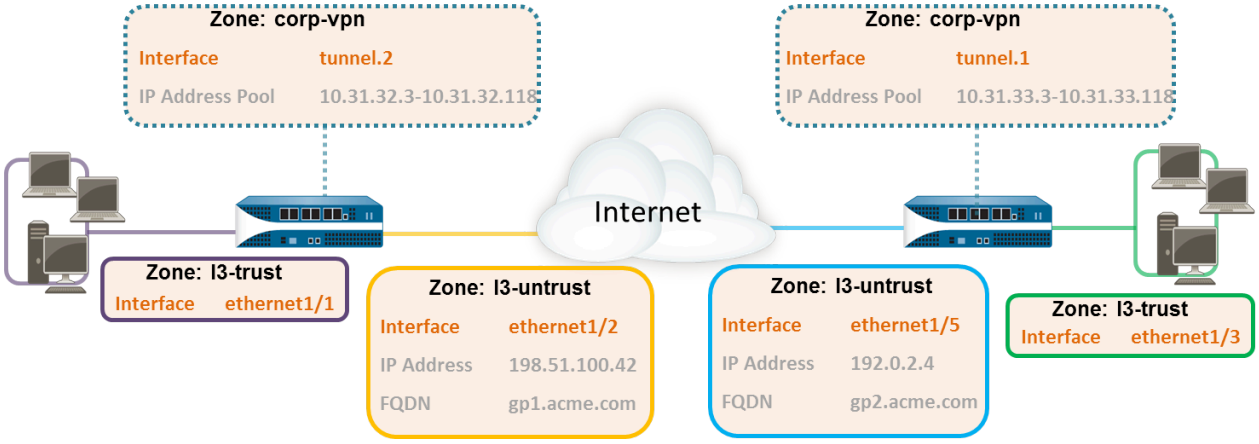


Figure 7: GlobalProtect Multiple Gateway Topology

If a client configuration contains more than one gateway, the app attempts to connect to all gateways listed in its client configuration. The app uses priority and response time to determine the gateway to which it will connect. The app only connects to a lower priority gateway if the response time for the higher priority gateway is greater than the average response time across all gateways. For more information, see Gateway Priority in a Multiple Gateway Configuration.

STEP 1 | Create Interfaces and Zones for GlobalProtect.

In this configuration, you must set up interfaces on each firewall hosting a gateway.

*Use the **default** virtual router for all interface configurations to avoid having to create inter-zone routing.*

On the firewall hosting the portal/gateway (gw1):

- Select **Network** > **Interfaces** > **Ethernet**, and then select **ethernet1/2**.
- Configure **ethernet1/2** as a Layer 3 interface with an IP address of **198.51.100.42**, and then assign it to the **l3-untrust Security Zone** and the **default Virtual Router**.
- Create a DNS "A" record that maps IP address **198.51.100.42** to **gp1.acme.com**.
- Select **Network** > **Interfaces** > **Tunnel**, and then **Add** the **tunnel.2** interface. Add the interface to a new **Security Zone** called **corp-vpn**. Assign it to the **default Virtual Router**.
- Enable User Identification on the **corp-vpn** zone.

On the firewall hosting the second gateway (gw2):

- Select **Network** > **Interfaces** > **Ethernet**, and then select **ethernet1/5**.
- Configure **ethernet1/5** as a Layer 3 interface with an IP address of **192.0.2.4**, and then assign it to the **l3-untrust Security Zone** and the **default Virtual Router**.
- Create a DNS "A" record that maps IP address **192.0.2.4** to **gp2.acme.com**.
- Select **Network** > **Interfaces** > **Tunnel**, and then **Add** the **tunnel.1** interface. Add the interface to a new **Security Zone** called **corp-vpn**. Assign it to the default **Virtual Router**.
- Enable User Identification on the **corp-vpn** zone.

STEP 2 | Purchase and install a GlobalProtect subscription on each gateway if your end-users will be using the GlobalProtect app on their mobile endpoints or if you plan on using the HIP-enabled security policy.

After you purchase the GlobalProtect subscription and receive your activation code, install the license on the firewall hosting the portal, as follows:

1. Select **Device** > **Licenses**.
2. Select **Activate feature using authorization code**.
3. When prompted, enter the **Authorization Code**, and then click **OK**.
4. Verify that the license was activated successfully:

STEP 3 | On each firewall hosting a GlobalProtect gateway, create security policies.

This configuration requires policy rules to enable traffic flow between the **corp-vpn** zone and the **l3-trust** zone to provide access to your internal resources (**Policies** > **Security**).

STEP 4 | Use the following recommendations to obtain server certificates for each interface hosting your GlobalProtect portal and GlobalProtect gateways:

- (On the firewall hosting the portal or portal/gateway) Import a server certificate from a well-known, third-party CA.
- (On a firewall hosting only a gateway) Use the root CA on the portal to generate a self-signed server certificate.

On each firewall hosting a portal/gateway or gateway, select **Device** > **Certificate Management** > **Certificates** to manage certificates as follows:

- Obtain a server certificate for the interface hosting portal/gw1. Because the portal and the gateway are on the same interface, you must use the same server certificate. The CN of the certificate must match the FQDN, `gp1.acme.com`. To enable endpoints to connect to the portal without receiving certificate errors, use a server certificate from a public CA.
- Obtain a server certificate for the interface hosting gw2. Because this interface hosts only a gateway, you can use a self-signed certificate. The CN of the certificate must match the FQDN, `gp2.acme.com`.

STEP 5 | Define how you will authenticate users to the portal and the gateways.

You can use any combination of certificate profiles and/or authentication profiles as necessary to ensure the security of your portal and gateways. Portals and individual gateways can also use different authentication schemes. See the following sections for step-by-step instructions:

- Set Up External Authentication (authentication profile)
- Set Up Client Certificate Authentication (certificate profile)
- Set Up Two-Factor Authentication (token- or OTP-based)

You must then reference the certificate profile and/or authentication profiles that you define in the portal and gateway configurations.

STEP 6 | Configure a GlobalProtect Gateway.

The following example shows the configuration for gp1 and gp2, as seen in Figure 7: GlobalProtect Multiple Gateway Topology.

On the firewall hosting gp1, select **Network** > **GlobalProtect** > **Gateways**. Configure the gateway settings as follows:

Interface—**ethernet1/2**

IP Address—**198.51.100.42**

Server Certificate—**GP1-server-cert.pem issued by GoDaddy**

Tunnel Interface—**tunnel.2**

IP Pool—**10.31.32.3 - 10.31.32.118**

On the firewall hosting gp2, select **Network** > **GlobalProtect** > **Gateways**. Configure the gateway settings as follows:

Interface—**ethernet1/2**

IP Address—**192.0.2.4**

Server Certificate—**self-signed certificate, GP2-server-cert.pem**

Tunnel Interface—**tunnel.1**

IP Pool—**10.31.33.3 - 10.31.33.118**

STEP 7 | Configure the GlobalProtect Portals.

Select **Network** > **GlobalProtect** > **Portals**. Configure the portal settings as follow:

1. Set Up Access to the GlobalProtect Portal:

   Interface—**ethernet1/2**

   IP Address—**198.51.100.42**

   Server Certificate—**GP1-server-cert.pem issued by GoDaddy**
2. Define the GlobalProtect Agent Configurations:

   The number of client configurations you create depends on your specific access requirements, including whether you require user/group-based policy and/or HIP-enabled policy enforcement.

STEP 8 | Deploy the GlobalProtect App to End Users.

Select **Device** > **GlobalProtect Client**.

In this example, follow the procedure to Host App Updates on the Portal.

STEP 9 | Save the GlobalProtect configuration.

Commit the configuration on the firewall hosting the portal and gateway(s).

GlobalProtect for Internal HIP Checking and User-Based Access

When used in conjunction with User-ID and/or HIP checks, an internal gateway provides a secure, accurate method of identifying and controlling traffic by user and/or device state, replacing other network access control (NAC) services. Internal gateways are useful in sensitive environments that require authenticated access to critical resources.

In a configuration with only internal gateways, all endpoints must be configured with User-Logon (Always On); On-Demand mode is not supported. It is also recommended that you configure all client configurations to use single sign-on (SSO). In addition, since internal hosts do not need to establish a tunnel connection with the gateway, the IP address of the physical network adapter on the endpoint is used.

In this quick config, the internal gateways enforce group-based policies that allow users in the Engineering group access to the internal source control and bug databases and users in the Finance group access to the CRM applications. All authenticated users have access to internal web resources. In addition, HIP profiles configured on the gateway check each host to ensure compliance with internal maintenance requirements, such as whether the latest security patches are installed, whether disk encryption is enabled, or whether the required software is installed.

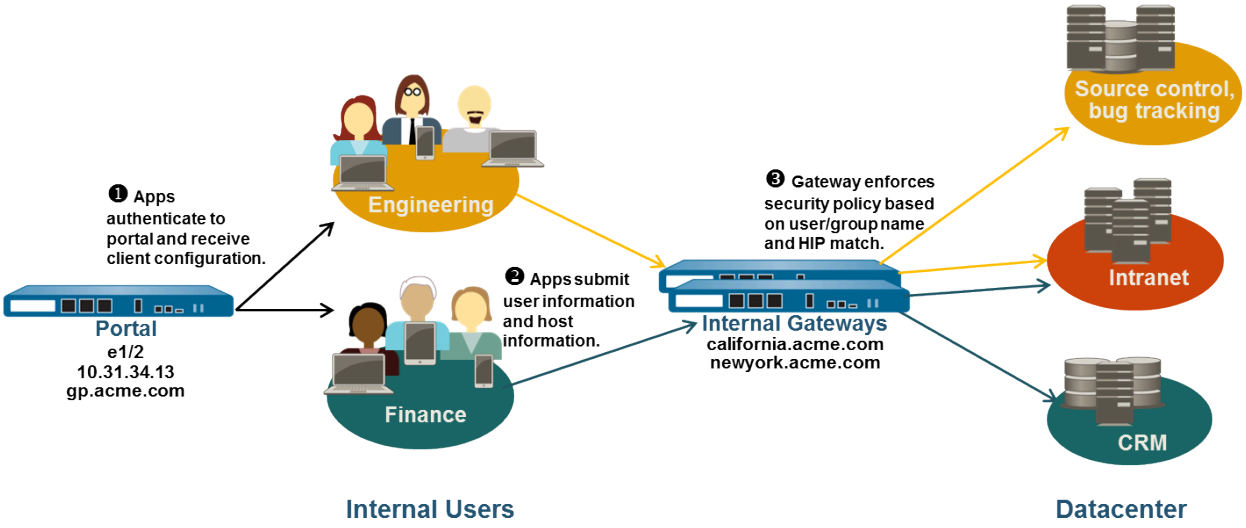


Figure 8: GlobalProtect Internal Gateway Configuration

Use the following steps to configure a GlobalProtect internal gateway.

STEP 1 | Create Interfaces and Zones for GlobalProtect.

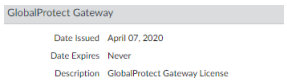
In this configuration, you must set up interfaces on each firewall hosting a portal and/or a gateway. Because this configuration uses internal gateways only, you must configure the portal and gateways on interfaces in the internal network.

*Use the **default** virtual router for all interface configurations to avoid creating inter-zone routing.*

On each firewall hosting a portal/gateway:

1. Select an Ethernet port to host the portal/gateway, and then configure a Layer3 interface with an IP address in the **`l3-trust` Security Zone** (**Network** > **Interfaces** > **Ethernet**).
2. **Enable User Identification** on the **`l3-trust`** zone.

STEP 2 | If any of your end users will be accessing the GlobalProtect app on their mobile devices, or if you plan on using HIP-enabled security policy, purchase and install a GlobalProtect subscription for each firewall hosting an internal gateway.



After you purchase the GlobalProtect subscriptions and receive your activation code, install the GlobalProtect subscriptions on the firewalls hosting your gateways, as follows:

1. Select **Device** > **Licenses**.
2. Select **Activate feature using authorization code**.
3. When prompted, enter the **Authorization Code**, and then click **OK**.
4. Verify that the license was activated successfully.

Contact your Palo Alto Networks Sales Engineer or Reseller if you do not have the required licenses. For more information on licensing, see About GlobalProtect Licenses.

STEP 3 | Obtain server certificates for the GlobalProtect portal and each GlobalProtect gateway.

In order to connect to the portal for the first time, the endpoints must trust the root CA certificate used to issue the portal server certificate. You can either use a self-signed certificate on the portal and deploy the root CA certificate to the endpoints before the first portal connection, or obtain a server certificate for the portal from a trusted CA.

You can use self-signed certificates on the gateways.

The recommended workflow is as follows:

1. On the firewall hosting the portal:
    1. Import a server certificate from a well-known, third-party CA.
    2. Create the root CA certificate for issuing self-signed certificates for the GlobalProtect components.
    3. Use the root CA on the portal to generate a self-signed server certificate. Repeat this step for each gateway.
2. On each firewall hosting an internal gateway, Deploy the self-signed server certificates.

STEP 4 | Define how you will authenticate users to the portal and gateways.

You can use any combination of certificate profiles and/or authentication profiles as necessary to ensure the security of your portal and gateways. Portals and individual gateways can also use different authentication schemes. See the following sections for step-by-step instructions:

- Set Up External Authentication (authentication profile)
- Set Up Client Certificate Authentication (certificate profile)
- Set Up Two-Factor Authentication (token- or OTP-based)

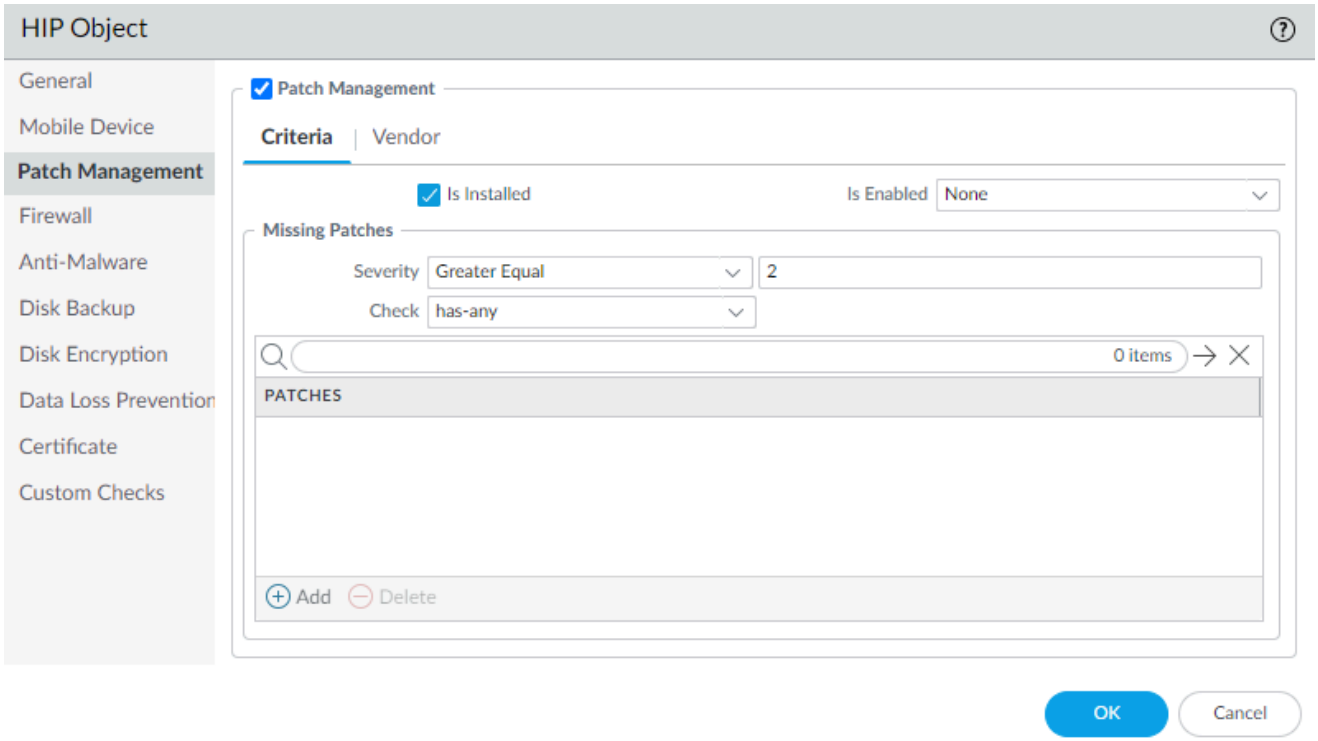
You must then reference the certificate profile and/or authentication profiles that you defined in the portal and gateway configurations.

STEP 5 | Create the HIP profiles you need to enforce security policies on gateway access.

See Host Information for more information on HIP matching.

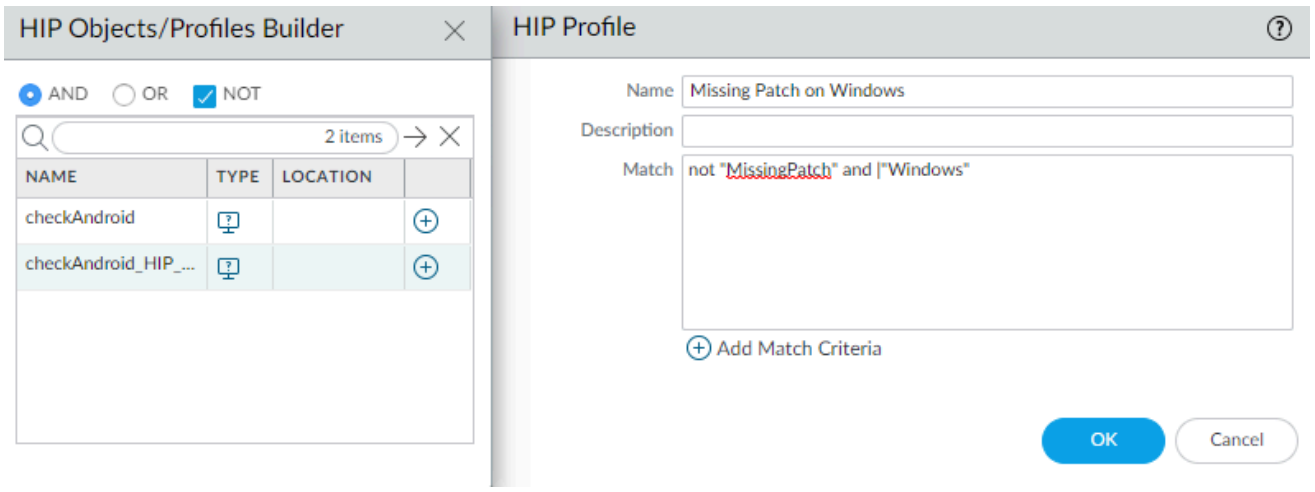
1. Create the HIP objects to filter the raw host data collected by the app. For example, if you want to prevent users that are not up-to-date with required patches from

connecting, you might create a HIP object to match on whether the patch management software is installed and that all patches with a given severity are up-to-date.



2. Create the HIP profiles that you plan to use in your policies.

   For example, if you want to ensure that only Windows users with up-to-date patches can access your internal applications, you might attach the following HIP profile that will match hosts that do NOT have a missing patch:



STEP 6 | Configure the internal gateways.

Select **Network** > **GlobalProtect** > **Gateways**, and then select an existing internal gateway or **Add** a new gateway. Configure the following gateway settings:

- **Interface**
- **IP Address**
- **Server Certificate**
- **Authentication Profile** and/or **Configuration Profile**

Note that it is not necessary to configure the client settings in the gateway configurations (unless you want to set up HIP notifications) because tunnel connections are not required. See Configure a GlobalProtect Gateway for step-by-step instructions on creating the gateway configurations.

STEP 7 | Configure the GlobalProtect Portals.

*Although all of the previous configurations can use the **User-logon (Always On)** or **On-demand (Manual user initiated connection)** connect methods, an internal gateway configuration must always be on, and therefore requires the **User-logon (Always On)** connect method.*

Select **Network** > **GlobalProtect** > **Portals**, and then select an existing portal or **Add** a new portal. Configure the portal as follows:

1. Set Up Access to the GlobalProtect Portal:

   Interface—**`ethernet1/2`**

   IP Address—**`10.31.34.13`**

   Server Certificate—**`GP-server-cert.pem issued by GoDaddy`** with **`CN=gp.acme.com`**
2. Define the GlobalProtect Client Authentication Configurations:

   Use single sign-on—**`enabled`**

   Connect Method—**`User-logon (Always On)`**

   Internal Gateway Address—**`california.acme.com, newyork.acme.com`**

   User/User Group—**`any`**
3. **Commit** the portal configuration.

STEP 8 | Deploy the GlobalProtect App to End Users.

Select **Device** > **GlobalProtect Client**.

In this example, use the procedure to Host App Updates on the Portal.

STEP 9 | Create the HIP-enabled and/or user/group-based security rules on your gateway(s).

Add the following security rules for this example:

1. Select **Policies** > **Security**, and click **Add**.
2. On the **Source** tab, set the **Source Zone** to **l3-trust**.
3. On the **User** tab, add the HIP profile and user/group to match.
   - Click **Add** in the **HIP Profiles** area, and select the **MissingPatch** HIP profile.
   - **Add** the **Source User** group (Finance or Engineering depending on which rule you are creating).
4. Click **OK** to save the rule.
5. **Commit** the gateway configuration.

			Source				Destination				
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	CRM access	none	l3-trust	any	Finance	Missing Patch ...	l3-trust	any	sap	application-default	
2	Eng access	none	l3-trust	any	Engineering	Missing Patch ...	l3-trust	any	bugzilla perforce	application-default	

Mixed Internal and External Gateway Configuration

In a GlobalProtect mixed internal and external gateway configuration, you can configure separate gateways for VPN access and for access to your sensitive internal resources. With this configuration, the GlobalProtect app performs internal host detection to determine if it is on the internal or external network. If the app determines that it is on the external network, it attempts to connect to the external gateways listed in its client configuration, and then it establishes a connection to the gateway with the highest priority and shortest response time.

*If you configure all external gateways as manual-only gateways but the GlobalProtect connect method as **User-Logon (Always On)** or **Pre-Logon (Always On)**, the GlobalProtect app does not automatically connect to any external gateways. GlobalProtect remains in the **Not Connected** state until the external user establishes a gateway connection manually. This behavior enables you to deploy GlobalProtect to derive User-ID for internal users while supporting **On-Demand** VPN behavior for external users.*

Because security policies are defined separately on each gateway, you have granular control over the resources to which your external and internal users have access. In addition, you also have granular control over the gateways to which users have access by configuring the portal to deploy different client configurations based on user/group membership or HIP profile matching.

In this example, the portals and all three gateways (one external and two internal) are deployed on separate firewalls. The external gateway at gpvpn.acme.com provides remote VPN access to the corporate network, while the internal gateways provide granular access to sensitive datacenter resources based on group membership. In addition, HIP checks are used to ensure that hosts accessing the datacenter are up-to-date on security patches.

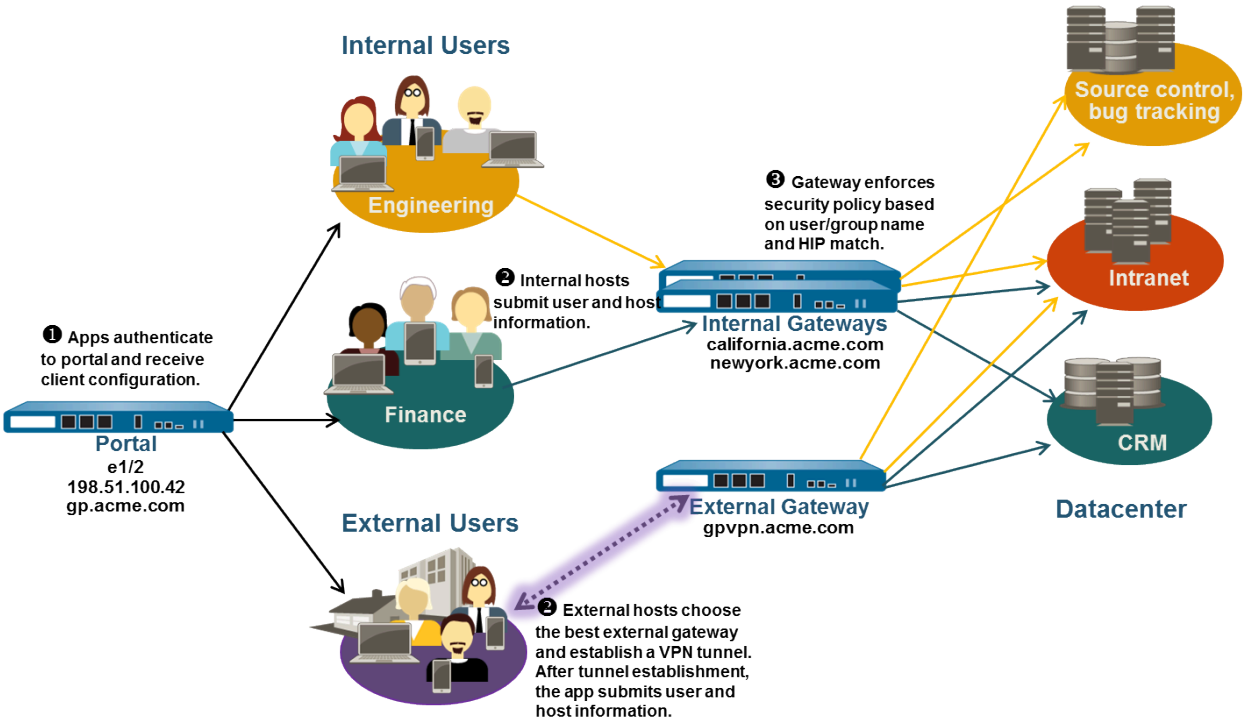


Figure 9: GlobalProtect Deployment with Internal and External Gateways

Use the following steps to configure a mix of internal and external GlobalProtect gateways.

STEP 1 | Create Interfaces and Zones for GlobalProtect.

In this configuration, you must set up interfaces on the firewall hosting a portal and each firewall hosting a gateway.

Do not attach an interface management profile that allows HTTP, HTTPS, Telnet, or SSH on the interface where you have configured a GlobalProtect portal or gateway because this enables access to your management interface from the internet. Follow the Adminstrative Access Best Practices to ensure that you are securing administrative access to your firewalls in a way that will prevent successful attacks.

*Use the **default** virtual router for all interface configurations to avoid having to create inter-zone routing.*

On the firewall hosting the portal gateway (gp.acme.com):

- Select **Network** > **Interfaces** > **Ethernet** and configure **ethernet1/2** as a Layer 3 Ethernet interface with IP address **198.51.100.42**. Assign it to the **l3-untrust Security Zone** and the default **Virtual Router**.
- Create a DNS "A" record that maps IP address 198.51.100.42 to gp.acme.com.
- Select **Network** > **Interfaces** > **Tunnel** and **Add** the **tunnel.2** interface. Assign it to a new **Security Zone** called corp-vpn and the default **Virtual Router**.
- Enable User Identification on the corp-vpn zone.

On the firewall hosting the external gateway (gpvpn.acme.com):

- Select **Network** > **Interfaces** > **Ethernet** and configure **ethernet1/5** as a Layer 3 Ethernet interface with IP address **192.0.2.4**. Assign it to the **l3-untrust Security Zone** and the default **Virtual Router**.
- Create a DNS "A" record that maps IP address 192.0.2.4 to gpvpn.acme.com.
- Select **Network** > **Interfaces** > **Tunnel** and **Add** the **tunnel.3** interface. Assign it to a new **Security Zone** called corp-vpn and the default **Virtual Router**.
- Enable User Identification on the corp-vpn zone.

On the firewall hosting the internal gateways (california.acme.com and newyork.acme.com):

- Select **Network** > **Interfaces** > **Ethernet** and configure a Layer 3 Ethernet interface with IP addresses on the internal network. Assign them to the **l3-trust Security Zone** and the default **Virtual Router**.
- Create a DNS "A" record that maps the internal IP addresses california.acme.com and newyork.acme.com.
- Enable User Identification on the l3-trust zone.

STEP 2 | Purchase and install a GlobalProtect subscription for each firewall hosting a gateway (internal and external) if your end users will be using the GlobalProtect app on their mobile endpoints or if you plan on using HIP-enabled security policy.

After you purchase the GlobalProtect subscriptions and receive your activation code, install the GlobalProtect subscriptions on the firewalls hosting your gateways:

1. Select **Device** > **Licenses**.
2. Select **Activate feature using authorization code**.
3. When prompted, enter the **Authorization Code** and then click **OK**.
4. Verify that the license and subscriptions were successfully activated.

Contact your Palo Alto Networks Sales Engineer or Reseller if you do not have the required licenses. For more information on licensing, see About GlobalProtect Licenses.

STEP 3 | Obtain server certificates for the GlobalProtect portal and each GlobalProtect gateway.

In order to connect to the portal for the first time, the endpoints must trust the root CA certificate used to issue the portal server certificate.

You can use self-signed certificates on the gateways and deploy the root CA certificate to the apps in the client configuration. The best practice is to generate all of the certificates on firewall hosting the portal and deploy them to the gateways.

The recommended workflow is as follows:

1. On the firewall hosting the portal:
    1. Import a server certificate from a well-known, third-party CA.
    2. Create the root CA certificate for issuing self-signed certificates for the GlobalProtect components.
    3. Use the root CA on the portal to generate a self-signed server certificate. Repeat this step for each gateway.
2. On each firewall hosting an internal gateway:
    - Deploy the self-signed server certificates.

STEP 4 | Define how you authenticate users to the portal and gateways.

You can use any combination of certificate profiles and/or authentication profiles to ensure the security of your portal and gateways. Portals and individual gateways can also use different authentication schemes. See the following sections for step-by-step instructions:

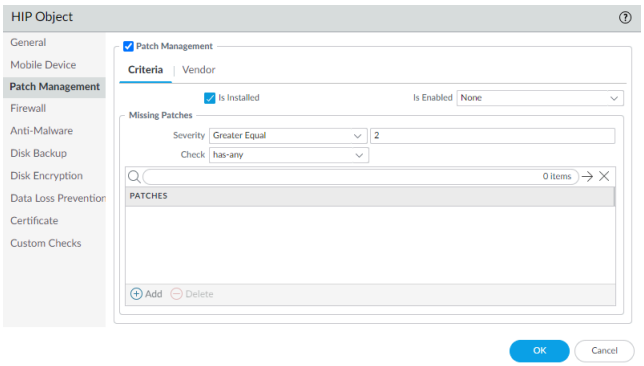
- Set Up External Authentication (authentication profile)
- Set Up Client Certificate Authentication (certificate profile)
- Set Up Two-Factor Authentication (token- or OTP-based)

You must then reference the certificate profile and/or authentication profiles that you defined in your portal and gateway configurations.

STEP 5 | Create the HIP profiles you will need to enforce security policy on gateway access.

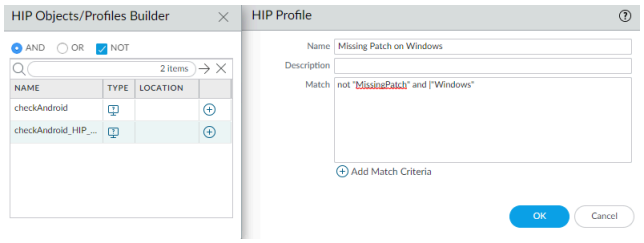
See Host Information for more information on HIP matching.

1. Create the HIP objects to filter the raw host data collected by the app. For example, if you are interested in preventing users that are not up to date with required patches, you might create a HIP object to match on whether the patch management software is installed and that all patches with a given severity are up to date.



2. Create the HIP profiles that you plan to use in your policies.

   For example, if you want to ensure that only Windows endpoints with up-to-date patches can access your internal applications, you might attach the following HIP profile to match hosts that do NOT have a missing patch:



STEP 6 | Configure the internal gateways.

Select **Network** > **GlobalProtect** > **Gateways** and **Add** gateway configurations with the following settings:

- **Interface**
- **IP Address**
- **Server Certificate**
- **Authentication Profile** and/or **Configuration Profile**

Notice that it is not necessary to configure the client configuration settings in the gateway configurations (unless you want to set up HIP notifications) because tunnel connections are not required. See Configure a GlobalProtect Gateway for step-by-step instructions on creating the gateway configurations.

STEP 7 | Configure the GlobalProtect Portals.

Although this example shows how to create a single client configuration to be deployed to all apps, you could also create separate configurations for different uses and then deploy them based on user/group name and/or the endpoint operating system on which the app is running.

Select **Network** > **GlobalProtect** > **Portals** and **Add** the following portal configuration:

1. Set Up Access to the GlobalProtect Portal:

   Interface—**`ethernet1/2`**

   IP Address—**`198.51.100.42`**

   Server Certificate—**`GP-server-cert.pem issued by GoDaddy`** with **`CN=gp.acme.com`**
2. Define the GlobalProtect Client Authentication Configurations:

   Internal Host Detection—**`enabled`**

   Use single sign-on—**`enabled`**

   Connect Method—**`User-logon (Always On)`**

   External Gateway Address—**`gpvpn.acme.com`**

   Internal Gateway Address—**`california.acme.com, newyork.acme.com`**

   User/User Group—any
3. **Commit** the portal configuration.

STEP 8 | Deploy the GlobalProtect App to End Users.

Select **Device** > **GlobalProtect Client**.

In this example, use the procedure to Host App Updates on the Portal.

STEP 9 | Create security policy rules on each gateway to safely enable access to applications for your VPN users.

- Create security policies (**Policies** > **Security**) to enable traffic flow between the corp-vpn zone and the l3-trust zone.
- Create HIP-enabled and user/group-based policy rules to enable granular access to your internal datacenter resources.
- For visibility, create rules that allow all users web-browsing access to the l3-untrust zone using the default security profiles to protect you from known threats.

			Source				Destination					
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile
1	CRM access	none	corp-vpn l3-trust	any	Finance	Missing Patch ...	l3-trust	any	sap	application-default	✓	none
2	Eng access	none	corp-vpn l3-trust	any	Engineering	Missing Patch ...	l3-trust	any	bugzilla perforce	application-default	✓	none
3	GP access	none	corp-vpn l3-trust	any	any	any	l3-untrust	any	web-browsing	application-default	✓	

STEP 10 | Save the GlobalProtect configuration.

Commit your portal and gateway configurations.

Captive Portal and Enforce GlobalProtect for Network Access

In most instances, mobile users connect to Wi-Fi networks on which a captive portal has been enabled, such as those used in coffee shops, airports, and hotels. Internet access becomes available only after users log in to the captive portal. Users can log in through a browser-based captive portal login page or OS-based captive portal assistant using identifiers such as a name and email address. With this configuration, you can limit the amount of time for which users can log in to the captive portal. If a user logs in successfully and the internet becomes reachable, the GlobalProtect app automatically establishes a connection. If a user fails to log in within the specified time period, all traffic will be blocked.

To further reduce the risk of exposing your network to security threats, you can also Enforce GlobalProtect for Network Access. When you enable this option, GlobalProtect blocks all network traffic until the app connects to a GlobalProtect gateway. All traffic is required to go through the VPN tunnel for inspection and policy enforcement, thereby enabling you to maintain full visibility and control over your users' traffic.

Based on the presence of a captive portal and whether the GlobalProtect connection is required for network access, users must follow a specific workflow to access the network:

Captive Portal	Enforce GlobalProtectfor Network Access	Workflow
Yes	Yes	If the GlobalProtect connection is required for network access, and your end users must also log in to a captive portal to access the internet, they must use the following steps to access the network: **1.** Connect to the Wi-Fi network. After you connect to the Wi-Fi network, GlobalProtect automatically detects the captive portal. If your administrator configures a captive portal detection message, the GlobalProtect app notifies you that you must log in to the captive portal to access the network. *Administrators can also configure the amount of time after which the captive portal detection message is displayed.*

Captive Portal	Enforce GlobalProtectfor Network Access	Workflow
		2. Use one of the following options to log in to the captive portal: • Open a web browser to log in through the captive portal login page. • Log in through the native captive portal assistant built in to the endpoint operating system (OS). If captive portal log in is successful, the internet becomes reachable and the GlobalProtect app connects automatically. If the app does not connect immediately, and your administrator configures a traffic blocking notification message to indicate that you must connect to GlobalProtect for network access, it displays this message until the connection is established. *Administrators can also configure the amount of time after which the traffic blocking notification is displayed.* If captive portal log in fails and the captive portal login page times out or if GlobalProtect is unable to establish a connection, you will be blocked from using the network. To re-initiate portal login and thereby re-trigger the captive portal login period, launch the GlobalProtect app and then select **Refresh Connection** from the app settings ( ) menu.
Yes	No	If your end users must log in to a captive portal to access the internet, but the GlobalProtect connection is not required for network access, they must use the following steps to access the network: **1.** Connect to the Wi-Fi network. After you connect to the Wi-Fi network, GlobalProtect automatically detects the captive portal.

Captive Portal	Enforce GlobalProtectfor Network Access	Workflow
		2. Use one of the following options to log in to the captive portal: • Open a web browser to log in through the captive portal login page. • Log in through the native captive portal assistant built in to the endpoint operating system (OS). If log in is successful and the internet becomes reachable, the GlobalProtect app connects automatically.
No	Yes	If the GlobalProtect connection is required for network access, but your end users do not have to log in to a captive portal to access the internet, they must connect to the Wi-Fi network. As soon as the Wi-Fi is connected and internet is reachable, the GlobalProtect app connects automatically. If the app does not connect immediately, and your administrator configures a traffic blocking notification message to indicate that you must connect to GlobalProtect for network access, it displays this message until the connection is established. If GlobalProtect is unable to establish a connection, you will be locked out of the network. You must re-initiate network discovery by disconnecting and then reconnecting to the Wi-Fi network, rebooting your endpoint, or refreshing the GlobalProtect connection.

Use the following steps to the customize captive portal settings and indicate whether the GlobalProtect connection is required for network access:

*Configure the **Enforce GlobalProtect for Network Access** option only if you configure GlobalProtect with the Always On connect method.*

STEP 1 | Set Up Access to the GlobalProtect Portal.

STEP 2 | Define the GlobalProtect Agent Configurations.

STEP 3 | Customize the GlobalProtect App.

- To ensure that the GlobalProtect connection is always on, set the **Connect Method** to **User-logon (Always On)**.
- If your users must log in to a captive portal to access the internet, you can customize the captive portal settings by configuring the following options:
  - In the **Captive Portal Exception Timeout (sec)** field, enter the amount of time (in seconds) within which users can log in to the captive portal (range is 0 to 3600 seconds; default is 0 seconds). If users do not log in within this time period, the captive portal login page times out and users will be blocked from using the network.
  - To enable the GlobalProtect app to notify users when it detects a captive portal, set the **Display Captive Portal Detection Message** to **Yes**.
    - In the **Captive Portal Notification Delay (sec)** field, enter the amount of time (in seconds) after which the GlobalProtect app displays the captive portal detection message (range is 1 to 120 seconds; default is 5 seconds). GlobalProtect initiates this timer after the captive portal has been detected but before the internet becomes reachable.
    - Customize the **Captive Portal Detection Message** that displays when GlobalProtect detects a captive portal.
- To force all network traffic to traverse the GlobalProtect VPN tunnel, configure the following options:
  - Set the **Enforce GlobalProtect for Network Access** option to **Yes**.
  - To enable the GlobalProtect app to notify users that the GlobalProtect connection is required for network access, set the **Display Traffic Blocking Notification Message** to **Yes**. The GlobalProtect app displays this message when the internet becomes reachable but before the GlobalProtect connection is established.
    - In the **Traffic Blocking Notification Delay (sec)** field, enter the amount of time (in seconds) after which the GlobalProtect app displays the traffic blocking notification message (range is 5 to 120 seconds; default is 15 seconds). GlobalProtect initiates this timer after the internet becomes reachable.
    - Customize the **Traffic Blocking Notification Message** that displays when the GlobalProtect connection is required for network access. This message must be 512 characters or less.

STEP 4 | **Commit** the changes.

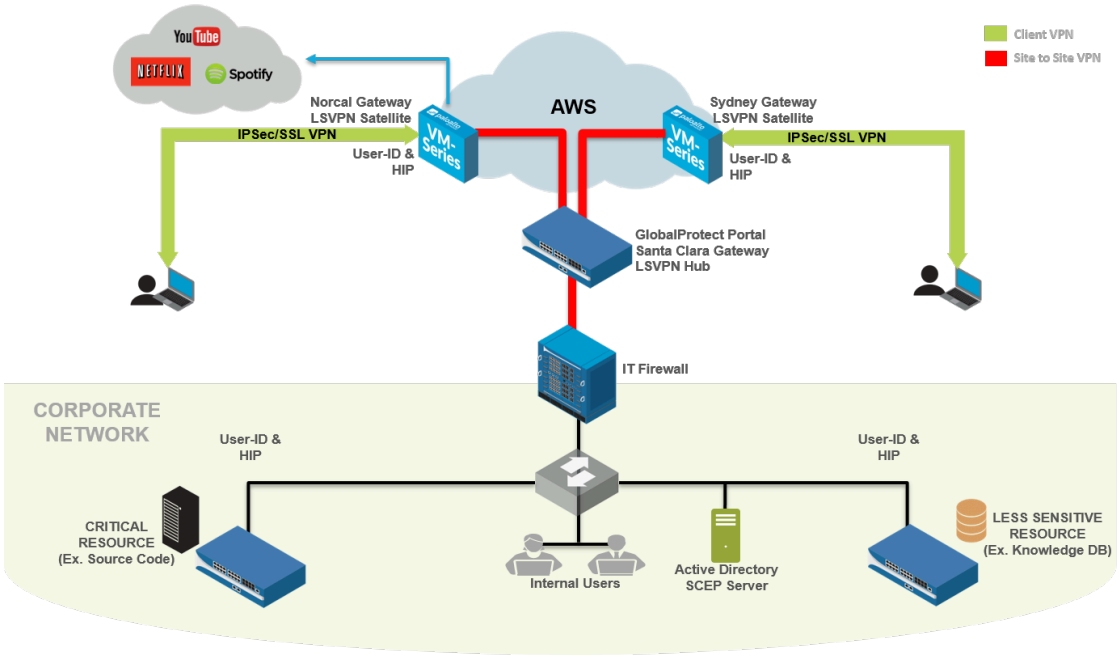
GlobalProtect Architecture

This section outlines an example reference architecture for deploying GlobalProtect™, which secures internet traffic and provides secure access to corporate resources.

The reference architecture and guidelines described in this section provide a common deployment scenario. Before adopting this architecture, identify your corporate security, infrastructure manageability, and end user experience requirements, and then deploy GlobalProtect based on those requirements.

Although the requirements may be different for each enterprise, you can leverage the common principles and design considerations outlined in this document, along with the best practice configuration guidelines, to meet your enterprise security needs.

GlobalProtect Reference Architecture Topology



- GlobalProtect Portal
- GlobalProtect Gateways

GlobalProtect Portal

In this topology, a PA-3020 in the co-location space functions as a GlobalProtect portal.

Employees and contractors can authenticate to the portal using two-factor authentication (2FA) consisting of Active Directory (AD) credentials and a one-time password (OTP). The portal deploys GlobalProtect client configurations based on user and group membership and operating system.

By configuring a separate portal client configuration that applies to a small group or set of pilot users, you can test features before rolling them out to a wider user base. Any client configuration containing new features—such as the Enforce GlobalProtect or Simple Certificate Enrollment Protocol (SCEP) features that were made available with PAN-OS 7.1 and content updates that followed—is enabled in the pilot configuration first and validated by those pilot users before it is made available to other users.

The GlobalProtect portal also pushes configurations to GlobalProtect satellites. This configuration includes the GlobalProtect gateways to which satellites can connect and establish a site-to-site tunnel.

GlobalProtect Gateways

The PA-3020 in the co-location space (mentioned previously) also doubles as a GlobalProtect gateway (the Santa Clara Gateway). 10 additional gateways are deployed in Amazon Web Services (AWS) and the Microsoft Azure public cloud. The regions or POP locations where these AWS and Azure gateways are deployed are based on the distribution of employees across the globe.

- **Santa Clara Gateway**—Employees and contractors can authenticate to the Santa Clara Gateway (PA-3020 in the co-location space) using 2FA. This gateway requires users to provide their Active Directory credentials and their OTP. Because this gateway protects sensitive resources, it is configured as a manual-only gateway. As a result, users do not connect to this gateway automatically and must manually choose to connect to this gateway. For example, when users connect to AWS-Norcal, which is not a manual-only gateway, some sensitive internal resources are not accessible. The user must then manually switch to and authenticate with the Santa Clara Gateway to access these resources.

  In addition, the Santa Clara Gateway is configured as a Large Scale VPN (LSVPN) tunnel termination point for all satellite connections from gateways in AWS and Azure. The Santa Clara Gateway is also configured to set up an Internet Protocol Security (IPSec) tunnel to the IT firewall in corporate headquarters. This is the tunnel that provides access to resources in the corporate headquarters.
- **Gateways in Amazon Web Services and Microsoft Azure**—This gateway requires 2FA: a client certificate and Active Directory credentials. The GlobalProtect portal distributes the client certificate that is required to authenticate with these gateways using the GlobalProtect SCEP feature.

  These gateways in the public cloud also act as GlobalProtect satellites. They communicate with the GlobalProtect portal, download the satellite configuration, and establish a site-to-site tunnel with the Santa Clara Gateway. GlobalProtect satellites initially authenticate using serial numbers, and subsequently authenticate using certificates.
- **Gateways Inside Corporate Headquarters**—Within the corporate headquarters, three firewalls function as GlobalProtect gateways. These are internal gateways that do not require endpoints to set up a tunnel. Users authenticate to these gateways using their Active Directory credentials. These internal gateways use GlobalProtect to identify the User-ID and to collect the Host Information Profile (HIP) from the endpoints.

  To make the end user experience as seamless as possible, you can configure these internal gateways to authenticate users with certificates provisioned by SCEP or with Kerberos service tickets.

GlobalProtect Reference Architecture Features

End User Experience

End users who are remote (outside the corporate network) connect to one of the gateways in AWS or Azure. When you configure the GlobalProtect portal client configuration, assign equal priority to the gateways. With this configuration, the gateway to which users connect depends on the SSL response time of each gateway measured on the endpoint during tunnel setup.

For example, a user in Australia would typically connect to the AWS-Sydney gateway. After the user is connected to AWS-Sydney, the GlobalProtect app tunnels all traffic from the endpoint to the AWS-Sydney firewall for inspection. GlobalProtect sends traffic to public internet sites directly via the AWS-Sydney gateway and tunnels traffic to corporate resources through a site-to-site tunnel between the AWS-Sydney gateway and the Santa Clara gateway, and then through an IPsec site-to-site tunnel to the corporate headquarters. This architecture is designed to reduce any latency the user may experience when accessing the internet. If the AWS-Sydney gateway (or any gateway closer to Sydney) was unreachable, the GlobalProtect app would back-haul the internet traffic to the firewall in the corporate headquarters and cause latency issues.

Active Directory servers reside inside the corporate network. When remote users authenticate, the GlobalProtect app sends authentication requests through the site-to-site tunnel in AWS/Azure to the Santa Clara gateway. The gateway then forwards the request through an IPsec site-to-site tunnel to the Active Directory Server in corporate headquarters.

To reduce the time it takes for remote user authentication and tunnel setup, consider replicating the Active Directory Server and making it available in AWS.

End users inside the corporate network authenticate to the three internal gateways immediately after they log in. The GlobalProtect app sends the HIP report to these internal gateways. Users that are inside the office on the corporate network must meet the User-ID and HIP requirements to access any resource at work.

Management and Logging

In this deployment, you can manage and configure all firewalls from Panorama, which is deployed in the co-location space.

To provide consistent security, all firewalls in AWS and Azure use the same security policies and configurations. To simplify configuration of the gateways, Panorama also uses one device group and one template. In this deployment, all gateways forward all logs to Panorama. This enables you to monitor network traffic or troubleshoot issues from a central location instead of requiring you to log in to each firewall.

When software updates are required, you can use Panorama to deploy the software updates to all firewalls. Panorama first upgrades one or two firewalls and verifies whether the upgrade was successful before updating the remaining firewalls.

Monitoring and High Availability

To monitor the firewalls in this deployment, you can use Nagios, which is an open-source server, network, and log monitoring software. Configure Nagios to periodically verify the response from the portal and the gateways' pre-login page and send an alert if the response does not match the expectations. You can also configure GlobalProtect Simple Network Management Protocol (SNMP) Management Information Base (MIB) objects to monitor gateway usage.

In this deployment, there is only one instance of the GlobalProtect portal. If the portal becomes unavailable, new users (who have never connected to the portal before) will not be able to connect to GlobalProtect. However, existing users can use the cached portal client configuration to connect to one of the gateways.

Multiple virtual machine (VM) firewalls in AWS configured as GlobalProtect gateways provide gateway redundancy. Therefore, configuring gateways as a high availability (HA) pair is not required.

GlobalProtect Reference Architecture Configurations

To align your deployment with the reference architecture, review the following configuration checklists.

- Gateway Configuration
- Portal Configuration
- Policy Configurations

Gateway Configuration

- Disable split tunneling. To do this, ensure there are no Access Routes specified in **Agent** > **Client Settings** > **Split Tunnel** settings. See Configure a GlobalProtect Gateway.
- Enable **No direct access to local network** in **Agent** > **Client Settings** > **Split Tunnel**. See Configure a GlobalProtect Gateway.
- Enable the gateway to **Accept cookie for authentication override**. See Configure a GlobalProtect Gateway.

Portal Configuration

- Configure the **Connect Method** as **Always-on (User logon)**. See Customize the GlobalProtect App.
- Set **Use Single Sign-On** (Windows only) to **Yes**. See Customize the GlobalProtect App.
- Configure the portal to **Save User Credentials** (set the value to **Yes**). See Define the GlobalProtect Agent Configurations.
- Enable the portal to **Accept cookie for authentication override**. See Define the GlobalProtect Agent Configurations.
- Configure the **Cookie Lifetime** as 20 hours. See Define the GlobalProtect Agent Configurations.
- **Enforce GlobalProtect** for network access. See Customize the GlobalProtect App.
- When **Enforce GlobalProtect for Network Access** is enabled, allow users to disable the GlobalProtect app with a passcode. See Customize the GlobalProtect App.
- Configure **Internal Host Detection**. See Define the GlobalProtect Agent Configurations.
- Enable the **Collect HIP Data** option in Data Collection. See Define the GlobalProtect Agent Configurations.
- Distribute and install the SSL Forward Proxy CA certificate used for SSL Decryption. See Define the GlobalProtect Agent Configurations.

Policy Configurations

- Configure all firewalls to use security policies and profiles based on the Best Practice Internet Gateway Security Policy. In this reference deployment, this includes the Santa Clara Gateway in the co-location space and gateways in the AWS/Azure public cloud.
- Enable SSL Decryption on all gateways in AWS and Azure.

- Configure Policy-Based Forwarding rules for all gateways in AWS to forward traffic to certain websites through the Santa Clara Gateway. This ensures that sites like www.stubhub.com and www.lowes.com that block traffic from AWS IP address ranges are still accessible when users connect to gateways in AWS.

GlobalProtect Cryptography

About GlobalProtect Cipher Selection

GlobalProtect supports both IPsec and SSL tunnel modes. GlobalProtect also supports the ability to enable and require the GlobalProtect app to always attempt to set up an IPsec tunnel first before falling back to an SSL tunnel. With an IPsec tunnel, the GlobalProtect app uses SSL/TLS to exchange encryption and authentication algorithms and the keys. The selection of cipher suite that GlobalProtect uses to secure the SSL/TLS tunnel depend on:

- **SSL/TLS versions accepted by the gateway**—The GlobalProtect portal and gateways can restrict the list of cipher suites available for the app using SSL/TLS profiles. On the firewall, you create the SSL/TLS profile by specifying the certificate and the allowed protocol versions and associate that to the GlobalProtect portal and gateway.
- **Algorithm of the server certificate of the gateway**—The operating system of the endpoint determines what cipher suites the GlobalProtect app includes in its Client Hello message. As long as the GlobalProtect app includes the cipher suite that the gateway prefers to use, the gateway will select that cipher suite for the SSL session. The order of cipher suites within the Client Hello message does not affect the cipher suite selection: The gateway selects the cipher suite based on the SSL/TLS service profile and the algorithm of the gateway server certificate and its preferred list. You select the service profile from the GlobalProtect gateway authentication configuration.

Cipher Exchange Between the GlobalProtect App and Gateway

The following figure displays the exchange of ciphers between GlobalProtect gateways and GlobalProtect apps when creating the VPN tunnel.

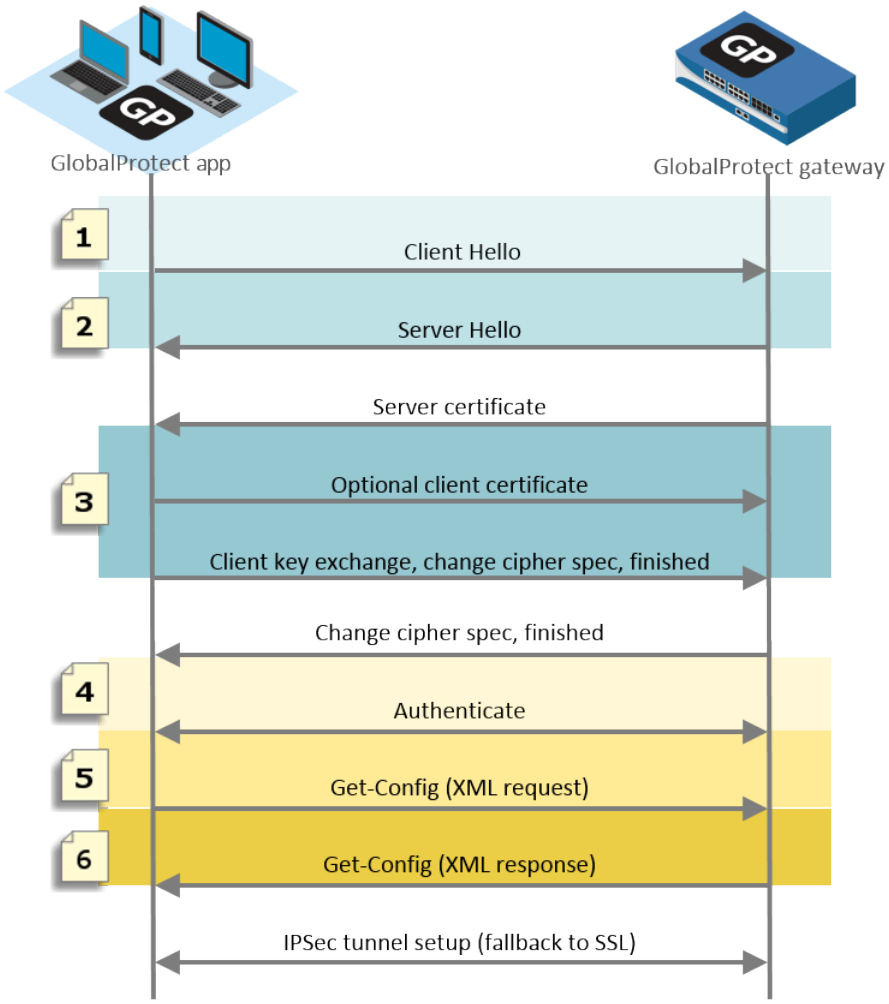


Figure 10: Cipher Exchange Between the App and the Gateway

The following table describes these stages in more detail.

Table 9: Cipher Exchange Between the App and Gateway

Communication Stage	Description
1. Client Hello	The app proposes a list of cipher suites depending on the OS of the endpoint.
2. Server Hello	The gateway selects the cipher suite proposed by the app. When selecting the ciphers to set up the tunnel, the gateway ignores

Communication Stage	Description
	both the number and order of cipher suites proposed by the app and instead relies on the SSL/TLS versions and algorithm of the gateway server certificate and its preferred list (as described in About GlobalProtect Cipher Selection).
3. Optional Client Certificate	The gateway can optionally request a client certificate from the app to use to trust the identity of the user or endpoint.
4. SSL Session	After setting up the SSL/TLS session, the app authenticates with the gateway and requests the gateway configuration (Get-Config-Request). To request the configuration, the app proposes the encryption and authentication algorithms and other settings such as preferred IP address for the tunnel interface. The gateway responds to the request and selects the encryption and authentication algorithm to use based on the configuration of the GlobalProtect IPSec Crypto Profile (Get-Config-Response).

The following table displays an example of the cipher exchange between an app on a macOS endpoint and the gateway.

Table 10: Example: Cipher Exchange for macOS Endpoints

Communication Stage	Example: macOS Endpoints
1. Client Hello	TLS 1.2 37 Cipher Suites (Reference: TLS Ciphers Supported by GlobalProtect Apps on macOS Endpoints)
2. Server Hello	• When GlobalProtect uses an ECDSA certificate and TLS 1.2 is accepted, the SSL session uses ECDSA-AES256-CBC-SHA. • When GlobalProtect uses an RSA certificate and TLS 1.2 is accepted, the SSL session uses RSA-AES256-CBC-SHA256.
3. Optional Client Certificate	Client certificates signed with ECDSA or RSA and using SHA1, SHA256, or SHA384

4. SSL Session	• SSL Session uses ECDSA-AES256-CBC-SHA or RSA-AES256-CBC-SHA256
	• Get-Config-Request
	  • Encryption—AES-256-GCM, AES-128-GCM, AES-128-CBC
	  • Authentication—SHA1 and OS type, Preferred IP address etc

Communication Stage	Example: macOS Endpoints

	• Get-Config-Response
	  • Client to server, and server to client SPIs, encryption keys, and authentication keys
	  • Tunnel type, ports, split tunnel mode, IP, and DNS etc

GlobalProtect Cryptography References

Reference: GlobalProtect App Cryptographic Functions

The GlobalProtect app uses the OpenSSL library 1.0.1h to establish secure communication with the GlobalProtect portal and GlobalProtect gateways. The following table lists each GlobalProtect app function that requires a cryptographic function and the cryptographic keys the GlobalProtect app uses:

Crypto Function	Key	Usage
Winhttp (Windows) and NSURLConnection (macOS) aes256-sha	Dynamic key negotiated between the GlobalProtect app and the GlobalProtect portal and/or gateway for establishing the HTTPS connection.	Used to establish the HTTPS connection between the GlobalProtect app and the GlobalProtect portal and GlobalProtect gateway for authentication.
OpenSSL aes256-sha	Dynamic key negotiated between the GlobalProtect app and the GlobalProtect gateway during the SSL handshake.	Used to establish the SSL connection between the GlobalProtect app and the GlobalProtect gateway for HIP report submission, SSL tunnel negotiation, and network discovery.
IPSec encryption and authentication aes-128-sha1, aes-128-cbc, aes-128-gcm, and aes-256-gcm	The session key sent from the GlobalProtect gateway.	Used to establish the IPSec tunnel between the GlobalProtect app and the GlobalProtect gateway. Use the strongest algorithm supported by your network (AES-GCM is recommended). To provide data integrity and authenticity protection, the aes-128-cbc cipher requires the sha1 authentication algorithm. Because AES-GCM encryption algorithms (aes-128-gcm and aes-256-gcm) natively provide ESP integrity protection, the sha1 authentication algorithm is ignored for these ciphers even

Crypto Function	Key	Usage
		though it is required during configuration.

TLS Cipher Suites Supported by GlobalProtect Apps

The following sections provide examples of TLS ciphers supported on GlobalProtect apps installed on various endpoint operating systems. The lists are not exhaustive for all supported operating systems.

Renegotiations (secure or insecure) are not supported.

- Reference: TLS Ciphers Supported by GlobalProtect Apps on macOS Endpoints
- Reference: TLS Ciphers Supported by GlobalProtect Apps on Windows 10 Endpoints
- Reference: TLS Ciphers Supported by GlobalProtect Apps on Android 6.0.1 Endpoints
- Reference: TLS Ciphers Supported by GlobalProtect Apps on iOS 10.2.1 Endpoints
- Reference: TLS Ciphers Supported by GlobalProtect Apps on Chromebooks

Reference: TLS Ciphers Supported by GlobalProtect Apps on macOS Endpoints

TLS Ciphers Supported by GlobalProtect Apps on macOS Endpoints	
TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA (0xc00d)
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)

TLS Ciphers Supported by GlobalProtect Apps on macOS Endpoints	
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc003)	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007)
	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)
	TLS_ECDH_ECDSA_WITH_RC4_128_SHA (0xc002)
	TLS_ECDH_RSA_WITH_RC4_128_SHA (0xc00c)
	TLS_RSA_WITH_RC4_128_SHA (0x0005)
	TLS_RSA_WITH_RC4_128_MD5 (0x0004)

Reference: TLS Ciphers Supported by GlobalProtect Apps on Windows 10 Endpoints

TLS Ciphers Supported by GlobalProtect Apps on Windows 10 Endpoints	
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)

TLS Ciphers Supported by GlobalProtect Apps on Windows 10 Endpoints	
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

Reference: TLS Ciphers Supported by GlobalProtect Apps on Android 6.0.1 Endpoints

The GlobalProtect app for Android 6.0.1 supports 20 cipher suites.

TLS Ciphers Supported by GlobalProtect Apps on Android 6.0.1 Endpoints	
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007)
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)	TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
	TLS_RSA_WITH_RC4_128_SHA (0x0005)

TLS Ciphers Supported by GlobalProtect Apps on Android 6.0.1 Endpoints	
	TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

Reference: TLS Ciphers Supported by GlobalProtect Apps on iOS 10.2.1 Endpoints

The GlobalProtect app for iOS 10.2.1 supports 19 cipher suites.

TLS Ciphers Supported by GlobalProtect Apps on iOS 10.2.1 Endpoints	
TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

Reference: TLS Ciphers Supported by GlobalProtect Apps on Chromebooks

The GlobalProtect app for Chrome OS 55.0.2883 supports 91 cipher suites.

TLS Ciphers Supported by GlobalProtect Apps on Chromebooks (Chrome OS 55.0.2883)	
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA (0x0085)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032)

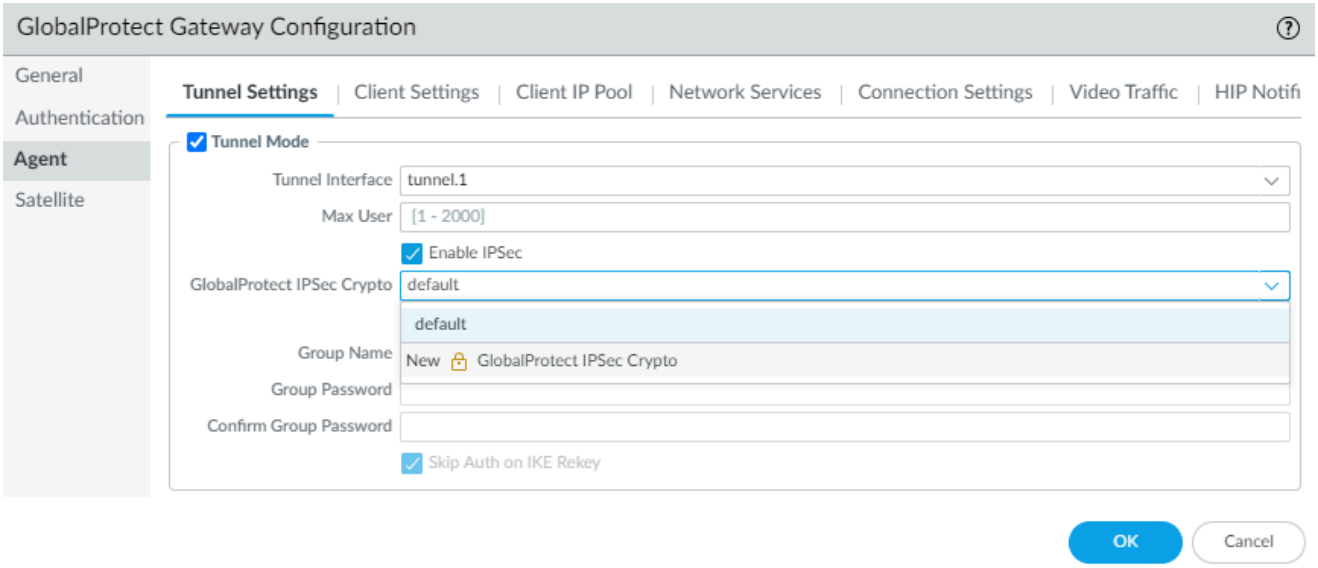
TLS Ciphers Supported by GlobalProtect Apps on Chromebooks (Chrome OS 55.0.2883)	
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
TLS_DH_DSS_WITH_AES_256_GCM_SHA384 (0x00a5)	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (0x00a3)	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
TLS_DH_RSA_WITH_AES_256_GCM_SHA384 (0x00a1)	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0084)
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (0x006a)	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
TLS_DH_RSA_WITH_AES_256_CBC_SHA256 (0x0069)	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
TLS_DH_DSS_WITH_AES_256_CBC_SHA256 (0x0068)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
TLS_DH_RSA_WITH_AES_256_CBC_SHA (0x0037)	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
TLS_DH_DSS_WITH_AES_256_CBC_SHA (0x0036)	TLS_DH_DSS_WITH_AES_128_GCM_SHA256 (0x00a4)
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0088)	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 (0x00a2)
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA (0x0087)	TLS_DH_RSA_WITH_AES_128_GCM_SHA256 (0x00a0)
TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0086)	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)

TLS Ciphers Supported by GlobalProtect Apps on Chromebooks (Chrome OS 55.0.2883)	
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (0x0040)	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
TLS_DH_RSA_WITH_AES_128_CBC_SHA256 (0x003f)	TLS_RSA_WITH_SEED_CBC_SHA (0x0096)
TLS_DH_DSS_WITH_AES_128_CBC_SHA256 (0x003e)	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0041)
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)	TLS_RSA_WITH_IDEA_CBC_SHA (0x0007)
TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)
TLS_DH_RSA_WITH_AES_128_CBC_SHA (0x0031)	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007)
TLS_DH_DSS_WITH_AES_128_CBC_SHA (0x0030)	TLS_ECDH_RSA_WITH_RC4_128_SHA (0xc00c)
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x009a)	TLS_ECDH_ECDSA_WITH_RC4_128_SHA (0xc002)
TLS_DHE_DSS_WITH_SEED_CBC_SHA (0x0099)	TLS_RSA_WITH_RC4_128_SHA (0x0005)
TLS_DH_RSA_WITH_SEED_CBC_SHA (0x0098)	TLS_RSA_WITH_RC4_128_MD5 (0x0004)
TLS_DH_DSS_WITH_SEED_CBC_SHA (0x0097)	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0045)	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008)
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA (0x0044)	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0043)	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA (0x0042)	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA (0x0010)
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031)	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA (0x000d)
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA (0xc00d)
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc003)
	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)

TLS Ciphers Supported by GlobalProtect Apps on Chromebooks (Chrome OS 55.0.2883)	
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)	TLS_DHE_RSA_WITH_DES_CBC_SHA (0x0015) TLS_DHE_DSS_WITH_DES_CBC_SHA (0x0012) TLS_DH_RSA_WITH_DES_CBC_SHA (0x000f) TLS_DH_DSS_WITH_DES_CBC_SHA (0x000c) TLS_RSA_WITH_DES_CBC_SHA (0x0009) TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

Ciphers Used to Set Up IPsec Tunnels

GlobalProtect can restrict and/or set preferential order for what encryption and authentication algorithm the GlobalProtect app can use for the IPsec tunnel. The algorithms and preferences are defined in the **GlobalProtect IPSec Crypto** profile that you configure when you set up the tunnel for the GlobalProtect gateway (**Network** > **GlobalProtect** > **Gateways** > **<gateway-config>** > **GlobalProtect Gateway Configuration** > **Agent** > **Tunnel Settings**).



When the GlobalProtect app sets up an SSL session with a GlobalProtect gateway, the cipher suite used for this SSL session is governed by the SSL/TLS profile configured on the gateway and the type of algorithm used by the gateway certificate. After the SSL session is established, the GlobalProtect app initiates a VPN tunnel setup by requesting the configuration over SSL.

Using the same SSL session, the GlobalProtect gateway responds with the encryption and authentication algorithms, keys, and SPIs that the app should use to set up the IPsec tunnel.

AES-GCM is recommended for more secure requirements. To provide data integrity and authenticity protection, the aes-128-cbc cipher requires the SHA1 authentication algorithm. Because AES-GCM encryption algorithms (aes-128-gcm and aes-256-gcm) natively provide ESP integrity protection, the SHA1 authentication algorithm is ignored for these ciphers even though it is required during configuration.

The **GlobalProtect IPSec Crypto** profile that you configure on the gateway determines the encryption and authentication algorithm used to set up the IPsec tunnel. The GlobalProtect gateway responds with the first matching encryption algorithm listed in the profile that matches the app's proposal.

The GlobalProtect app then attempts to set up a tunnel based on the response from the gateway.

SSL APIs

GlobalProtect uses both OpenSSL and native system APIs to perform SSL handshakes. Operations such as the GlobalProtect gateway latency measurement (used by GlobalProtect to select the best gateway), gateway logout, and HIP check message and report transmission are performed over SSL sessions that are set up using OpenSSL library. Operations such as gateway pre-login, login, and get-config are performed over SSL sessions that are set up using the native system API.

GlobalProtect App Log Collection for Troubleshooting

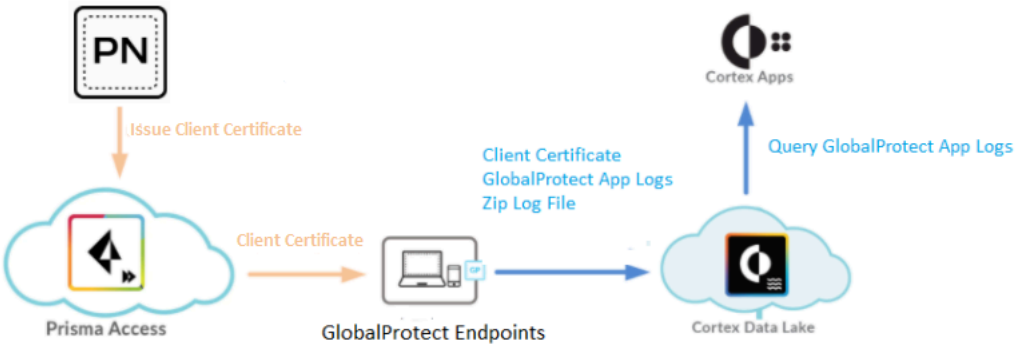
GlobalProtect App Log Collection for Troubleshooting Overview

With Prisma Access and next-generation firewall deployments, you can now quickly resolve mobile user connection, performance, and access issues. The GlobalProtect app can now be configured to send troubleshooting and diagnostic logs from the end user's endpoint to Cortex Data Lake for further analysis. By using this feature, when the end user reports an issue from the GlobalProtect app (upon user request), the app can generate and send an easy to read, comprehensive report to help you to quickly identify the root cause of the remote end user issue. Additionally, the GlobalProtect app can run end-to-end diagnostic tests to probe the state and performance of the network connection and the performance of specific web applications from the remote end user's endpoint. This results in faster resolution of the remote end user issues, enables increased productivity, and optimizes the user experience for the remote end user.

End users can now report an issue from their endpoint directly to Cortex Data Lake to which the administrator can access without manually collecting and sending the GlobalProtect app logs, for example, through email or storing them on a cloud drive. If end users consent to run diagnostic tests and to include diagnostic logs on the GlobalProtect app, the troubleshooting log bundle and diagnostic logs are sent to Cortex Data Lake from their endpoint so you can review them easily using the Explore app on the hub. If end users do not consent to run diagnostic tests and to include diagnostic logs and troubleshooting logs on the GlobalProtect app, only troubleshooting reports without the troubleshooting log bundle are sent to Cortex Data Lake from their endpoint for further analysis.

For example, if you want to run diagnostic tests for HTTPS-based destination URLs that can contain IP addresses or fully qualified domain names (for example, https://10.10.10.10/resource.html, https://webserver/file.pdf, or https://google.com) to determine whether there is an issue with latency or network performance, you can configure these HTTPS-based destination URLs that are critical to your end user's productivity by enabling the GlobalProtect app log collection for troubleshooting on the portal. By default, the GlobalProtect app log collection for troubleshooting is disabled, and as a result, end users cannot send troubleshooting and diagnostic logs to Cortex Data Lake from their endpoint. They would have to manually collect and send the GlobalProtect app logs to the administrator for troubleshooting and debugging purposes.

The following diagram illustrates the Checklist for GlobalProtect App Log Collection for Troubleshooting for sending the GlobalProtect app troubleshooting reports and diagnostic logs from the end user's endpoint to Cortex Data Lake:



Before you begin to enable the GlobalProtect app log collection for troubleshooting and to view the GlobalProtect app troubleshooting and diagnostic log records on the Explore app, follow these recommendations to communicate:

- Purchase a Cortex Data Lake license for the volume of logs in your GlobalProtect deployment and log in to the Explore app on the hub.
- Use the Cortex Data Lake logging infrastructure to manage the delivery mechanism of the GlobalProtect app troubleshooting and diagnostic logs.
- Use the Cortex Sizing Calculator to calculate the amount of storage you need in Cortex Data Lake.
- Obtain the Panorama and Cloud Services plugin and upgrade to cloud services plugin version 1.8, cloud services plugin 2.0 Preferred, or cloud services plugin 2.0 Innovation.
- Retrieve the Cortex Data Lake certificate.
- Purchase and install a GlobalProtect subscription license on each gateway. For more information on licensing, see About GlobalProtect Licenses.
- Configure the App Log Collection Settings on the GlobalProtect Portal on the GlobalProtect portal.

Checklist for GlobalProtect App Log Collection for Troubleshooting

Use the following workflow to enable the GlobalProtect app log collection for troubleshooting:

With Cloud Managed Prisma Access, you can enable Log Collection for Troubleshooting for the GlobalProtect app by using the Prisma Access app on the hub to generate the certificate and to automatically import it so that the app can authenticate with Cortex Data Lake for log collection.

- **Step 1: In Panorama, Set Up GlobalProtect Connectivity to Cortex Data Lake**

  With the Cloud Services plugin 2.0 Innovation, if you have a deployment that uses Prisma Access or the next-generation firewall, you must use the Panorama web interface to set up GlobalProtect connectivity.

  - Generate a client certificate that is used to establish a connection from the GlobalProtect app to Cortex Data Lake.

    The **globalprotect_app_log_cert** certificate is automatically exported from the Panorama certificate store, and then automatically imported to the Panorama template where the GlobalProtect portal configuration resides.
  - Create or modify the existing Define the GlobalProtect Client Authentication Configurations for a specific group of users.
  - Select the **globalprotect_app_log_cert** certificate as the client certificate in the GlobalProtect portal configuration.

  With the Cloud Services plugin 1.8 and Cloud Services plugin 2.0 Preferred, you must use the commands to set up GlobalProtect connectivity.

  - Generate a client certificate that is used to establish a connection from the GlobalProtect app to Cortex Data Lake.
  - Export the **gp_app_log_cert** certificate from the Panorama certificate store.
  - Import the **gp_app_log_cert** certificate to the Panorama template where the GlobalProtect portal configuration resides.
  - Create or modify the existing Define the GlobalProtect Client Authentication Configurations for a specific group of users.
  - Select the **gp_app_log_cert** certificate as the client certificate in the GlobalProtect portal configuration.
- **Step 2: Configure the App Log Collection Settings on the GlobalProtect Portal**
  - Enable the GlobalProtect app log collection for troubleshooting on the GlobalProtect portal.
  - Configure the HTTPS-based destination URLs that can contain IP addresses or fully qualified domain names on the GlobalProtect portal. Later, these HTTPS-based destination URLs are used to initiate performance tests for probing.

- **Step 3: Report an issue from the GlobalProtect app for Windows, macOS, iOS, Android, and Linux**
  - Open the GlobalProtect app.
  - Report an issue from the GlobalProtect from the end user's endpoint.
  - (Optional) Allow the GlobalProtect app to run additional diagnostic and performance tests both inside and outside of the tunnel, and also send the troubleshooting log bundle together with the issue reports upon user request.
- **Step 4: View the GlobalProtect App Troubleshooting and Diagnostic Logs on the Explore App**
  - View the troubleshooting or diagnostics log record uploaded to Cortex Data Lake.
  - Details Within the GlobalProtect App Troubleshooting and Diagnostic Logs to help you to identify the root cause and to resolve connectivity, network access, or performance issues.

Set Up GlobalProtect Connectivity to Cortex Data Lake

You must set up GlobalProtect connectivity so that the GlobalProtect app can authenticate with Cortex Data Lake for log collection. Only one client certificate is used per tenant. For example, all the end users endpoints that are hosted by a Prisma Access tenant will obtain the same certificate pushed from the portal configuration. The client certificate is valid for 1 year. The GlobalProtect app uses the client certificate and the Cortex Data Lake instance to send the GlobalProtect App Troubleshooting logs to Cortex Data Lake.

Based on the Cloud Services plugin version, you must set up GlobalProtect connectivity to Cortex Data Lake by using the command line interface (CLI) or the Panorama web interface that manages Prisma Access:

- Set Up GlobalProtect Connectivity to Cortex Data Lake (Cloud Services Plugin 2.0 Innovation)
- Set Up GlobalProtect Connectivity to Cortex Data Lake (Cloud Services Plugin 1.8 and 2.0 Preferred)

With Cloud Managed Prisma Access, you can enable Log Collection for Troubleshooting *for the GlobalProtect app by using the Prisma Access app on the hub to generate the certificate and to automatically import it so that the app can authenticate with Cortex Data Lake for log collection. The certificate is automatically displayed in the* ***Certificate Management*** *page, and is pushed as the client certificate to the Prisma Access portal.*

Set Up GlobalProtect Connectivity to Cortex Data Lake (Cloud Services Plugin 2.0 Innovation)

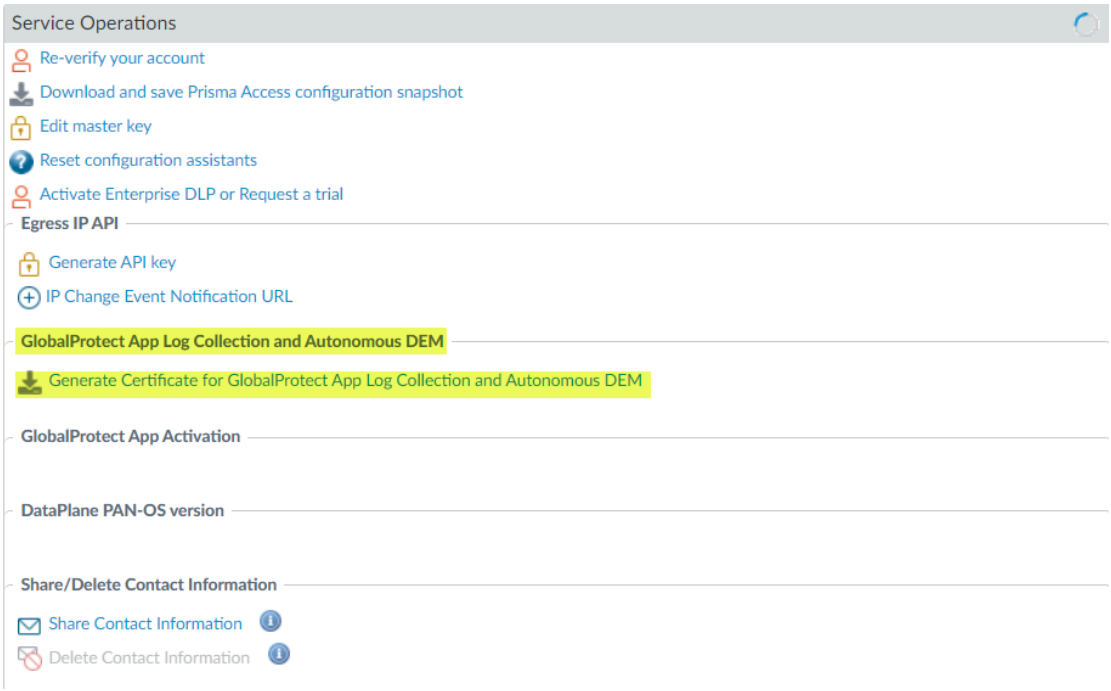
With the Cloud Services plugin 2.0 Innovation, if you have a deployment that uses Prisma Access or the next-generation firewall, you must use the Panorama web interface to set up GlobalProtect connectivity so that the GlobalProtect app can authenticate with Cortex Data Lake for log collection.

STEP 1 | Use the Cortex Sizing Calculator to calculate the amount of storage you need in Cortex Data Lake.

STEP 2 | Generate a client certificate that is used to establish a connection from the GlobalProtect app to Cortex Data Lake.

1. Use the Panorama web interface that manages Prisma Access to generate a client certificate.

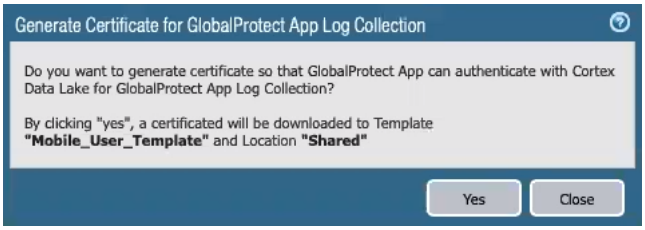
   1. Log in to the Panorama that manages Prisma Access.
   2. Select **Panorama** > **Cloud Services** > **Configuration** > **Service Setup**.
   3. Select **Generate Certificate for GlobalProtect App Log Collection and Autonomous DEM**.



   4. For Prisma Access deployments, click **Yes** to generate a client certificate.

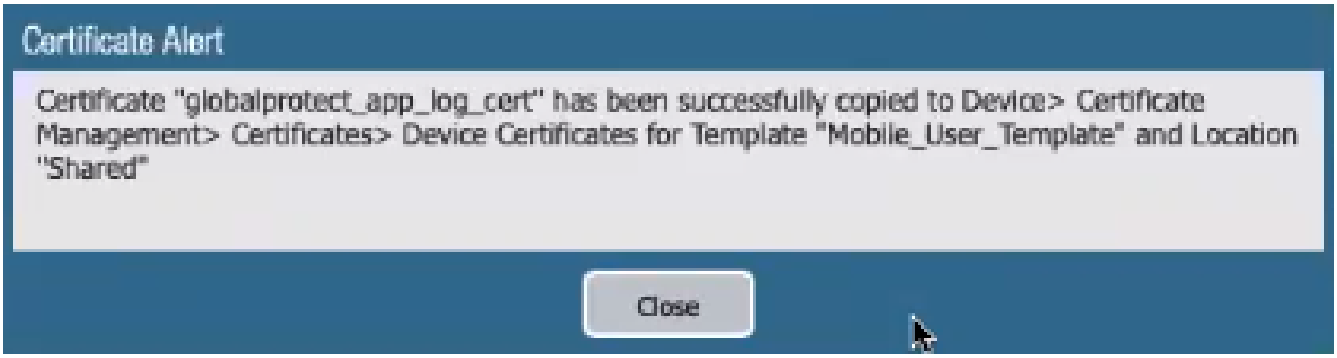
      If you configure Prisma Access to manage a single tenant, the **`globalprotect_app_log_cert`** certificate is automatically imported to the **Mobile_User_Template** and the **Shared** location.

      If you configure Prisma Access to manage multiple tenants, the **`globalprotect_app_log_cert`** certificate is automatically imported to the second mobile user template after the first and named **mu-tpl-***tenant*. The **`globalprotect_app_log_cert`** certificate is imported to the additional tenants.



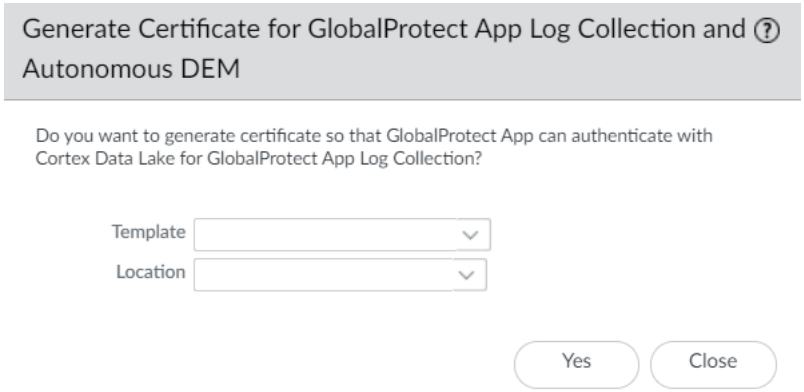
      After the **`globalprotect_app_log_cert`** certificate has been generated and downloaded to **Device** > **Certificate Management** > **Certificates**, you receive a

success message. The **Mobile_User_Template** is selected automatically as the **Template** and **Shared** is selected automatically as the **Location**.



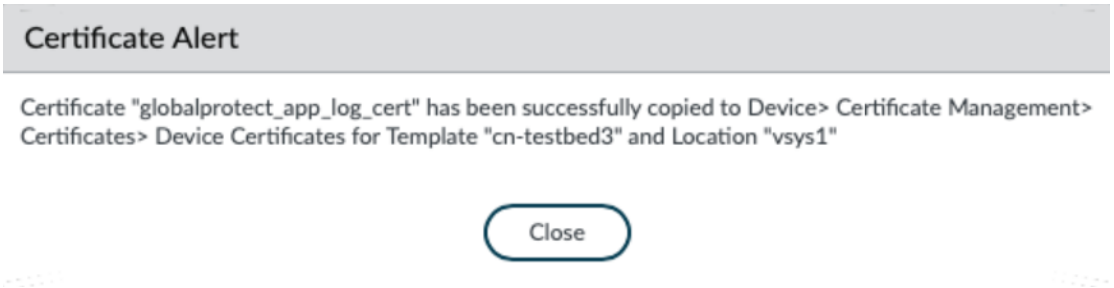
5. In next-generation firewall deployments, select any **Template** from the drop-down and **Location** from the drop-down.

   Click **Yes** to generate a client certificate.



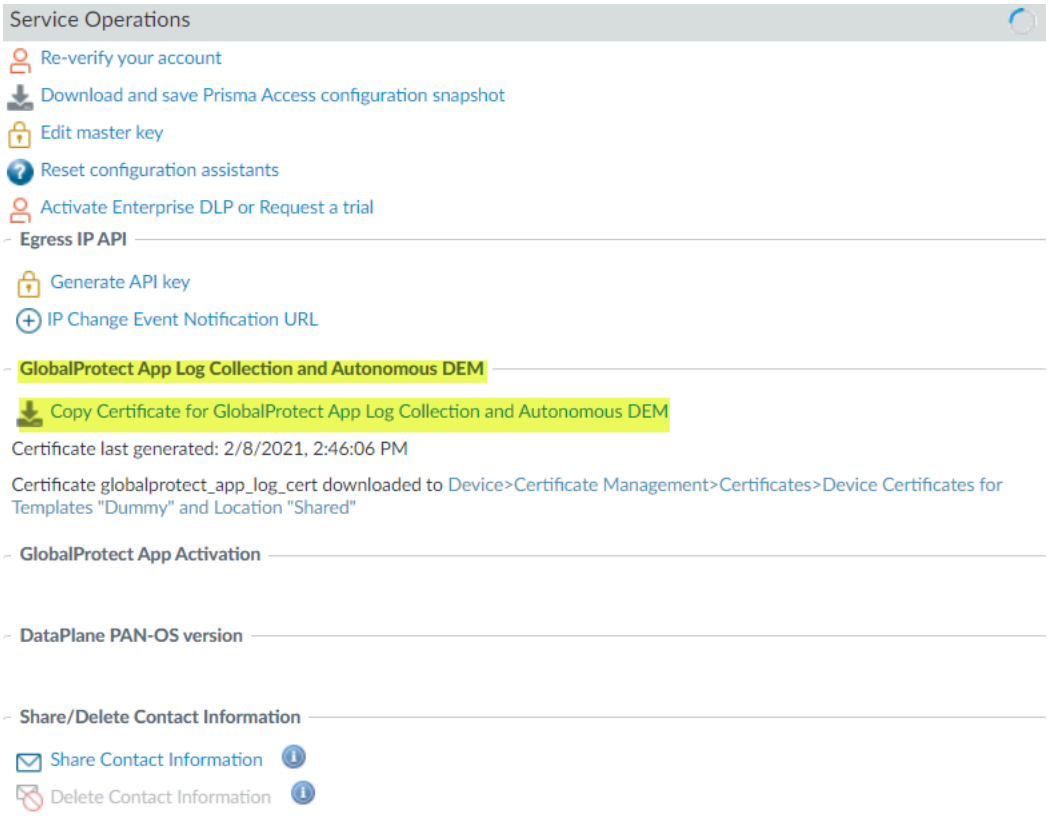
   After the **globalprotect_app_log_cert** certificate has been generated and downloaded to **Device** > **Certificate Management** > **Certificates** > **Device Certificates**, you receive a success message. The assigned template is selected

automatically as the **Template** and the assigned location is selected automatically as the **Location**.



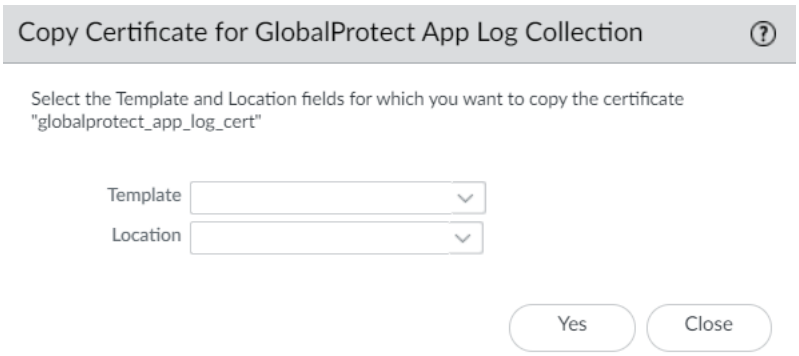
6. (Optional) In next-generation firewall deployments, copy the **`globalprotect_app_log_cert`** certificate to another template and location.

   Select **Copy Certificate for GlobalProtect App Log Collection and Autonomous DEM**.



   Select another **Template** from the drop-down and **Location** from the drop-down.

   Click **Yes** to generate a client certificate.

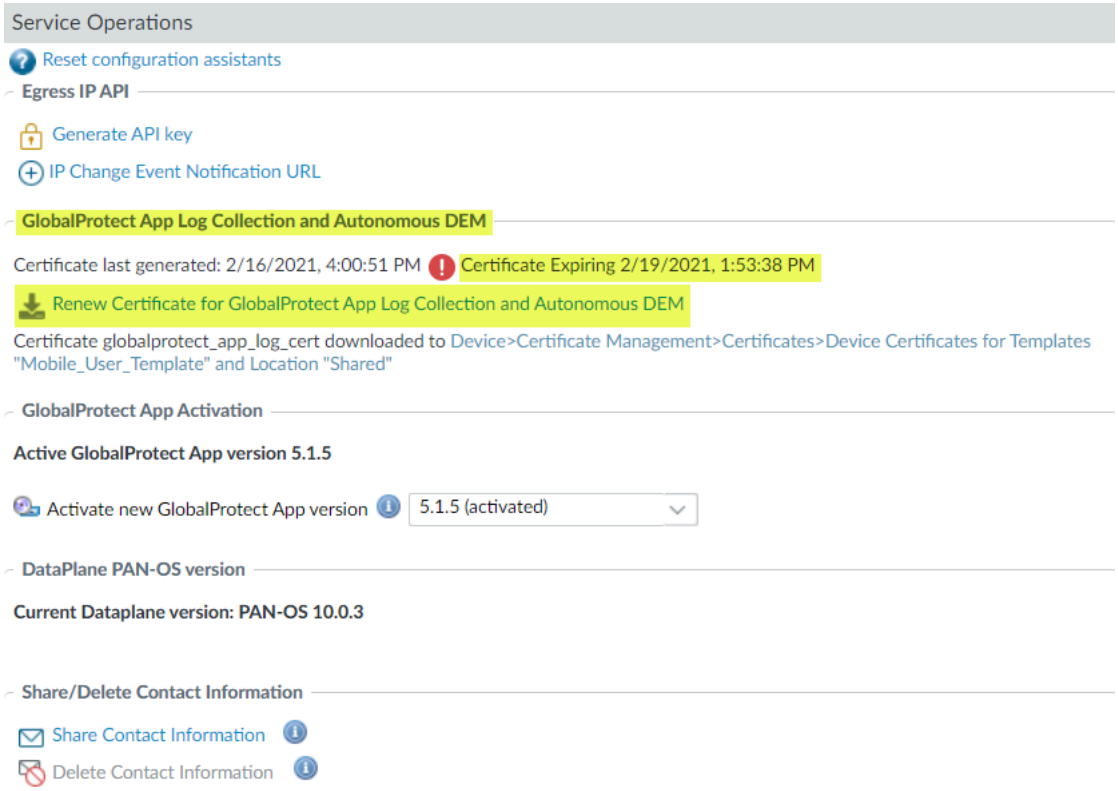


After the **`globalprotect_app_log_cert`** certificate has been generated and downloaded to **Device** > **Certificate Management** > **Certificates** > **Device Certificates**, you receive a success message. The assigned template is selected automatically as the **Template** and the assigned location is selected automatically as the **Location**.

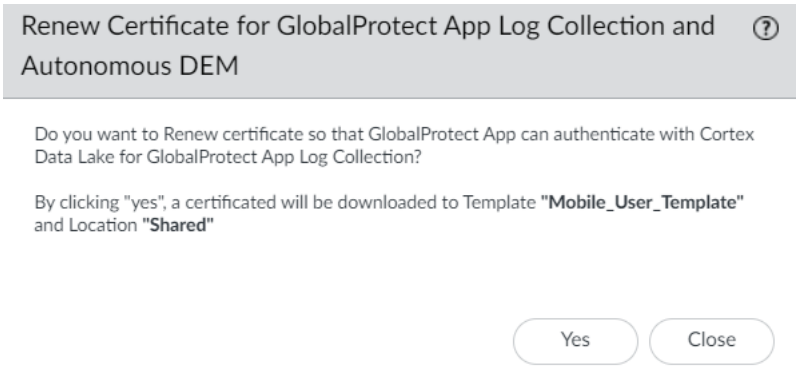
STEP 3 | (Optional) Request a new client certificate before the certificate expires.

The client certificate has a lifespan of 90 days.

1. In Panorama, select **Panorama** > **Cloud Services** > **Configuration** > **Tenants**
2. Select the tenant you created from the **Tenant** drop-down.
3. Select **Panorama** > **Cloud Services** > **Configuration** > **Service Setup**.
4. Select **Renew Certificate for GlobalProtect App Log Collection and Autonomous DEM**.



5. Click **Yes** to renew and download another client certificate. The assigned template is associated automatically as the **Template** and the assigned location is associated automatically as the **Location**.



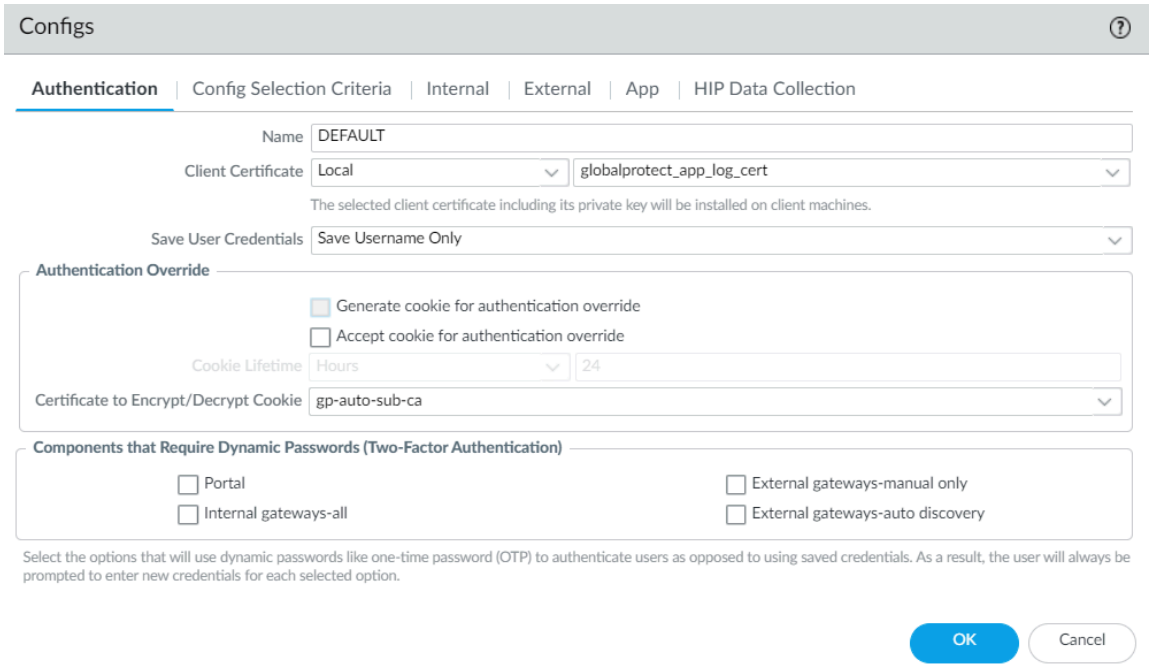
STEP 4 | Create or modify the existing Define the GlobalProtect Client Authentication Configurations for a specific group of users.

To enable the GlobalProtect app log collection for troubleshooting, you must define the agent configuration for a specific group of users to send the logs to Cortex Data Lake.

1. In Panorama, select **Network** > **GlobalProtect** > **Portals**.
2. Select the **Mobile_User_Template** from the **Template** drop-down.

   If you set up a deployment that includes multiple instances of Prisma Access on a single Panorama (multi-tenancy), you can select another template associated with the configuration.
3. Select **GlobalProtect_Portal** to edit the Prisma Access portal configuration.
4. Select the **Agent** tab.
5. Select the **Agent** tab and select the agent configuration.
6. Select the **Local** (default) and **DEFAULTglobalprotect_app_log_cert** from the **Client Certificate** drop-down.

   *Because the **Client Certificate** is used to push the Cortex Data Lake certificate, you cannot push the client certificate to authenticate to the portal or gateway either using a **Local** certificate type (default) or Simple Certificate Enrollment Protocol (SCEP).*



Set Up GlobalProtect Connectivity to Cortex Data Lake (Cloud Services Plugin 1.8 and 2.0 Preferred)

With the Cloud Services plugin 1.8 and 2.0 Preferred, you must use the commands to set up GlobalProtect connectivity so that the GlobalProtect app can authenticate with Cortex Data Lake for log collection.

STEP 1 | Use the Cortex Sizing Calculator to calculate the amount of storage you need in Cortex Data Lake.

STEP 2 | Generate a client certificate that is used to establish a connection from the GlobalProtect app to Cortex Data Lake.

1. Open a CLI session with administrator privileges, using the same IP address that you use to log in to the Panorama that manages Prisma Access.
2. Enter the **request plugins cloud_services gpclient_cert fetch** command, as shown in the following example:

```
admin-Panorama>request plugins cloud_services gpclient_cert
 fetch
Success
Successfully imported globalprotect_gp_log_cert into candidate
 configuration
```

If a client certificate is already generated, the command output is as follows:

```
admin-Panorama> request plugins cloud_services gpclient_cert
 fetch
certificate exists and not expired
```

3. Commit your changes on Panorama.
4. Verify the status of the client certificate by entering the following command:

```
admin-Panorama> request plugins cloud_services gpclient_cert
 status
certificate globalprotect_app_log_cert is valid till Oct 22
 21:55:39 2021 GMT
```

STEP 3 | Export the **gp_app_log_cert** certificate from the Panorama certificate store.

1. In Panorama, select **Panorama** > **Certificate Management** > **Certificates**, select the **gp_app_log_cert** certificate, and **Export Certificate**.
2. Select **Encrypted Private Key and Certificate (PKCS12)** from the **File Format** drop-down to export the certificate and private key in a single file.
3. Enter a **Passphrase** and **Confirm Passphrase** to import the certificate key.
4. Click **OK** and save the certificate/key file to your computer.

STEP 4 | Import the **gp_app_log_cert** certificate to the Panorama template where the GlobalProtect portal configuration resides.

If you configure Prisma Access to manage a single tenant, you must import the **gp_app_log_cert** certificate to the **Mobile_User_Template**.

If you configure Prisma Access to manage multiple tenants, you must import the **gp_app_log_cert** certificate to the second mobile user template automatically created after

the first and named **mu-tpl-***tenant*. You must import the **gp_app_log_cert** certificate to the additional tenants.

1. In Panorama, select **Device** > **Certificate Management** > **Certificates**, and then click **Import**.
2. For the **Certificate Type**, select **Local**.
3. Enter **gp_app_log_cert** as the **Certificate Name**.
4. **Browse** for the certificate file that you exported.
5. Enter the **Passphrase** and **Confirm Passphrase** used to encrypt the private key.
6. Click **OK** to import the certificate.

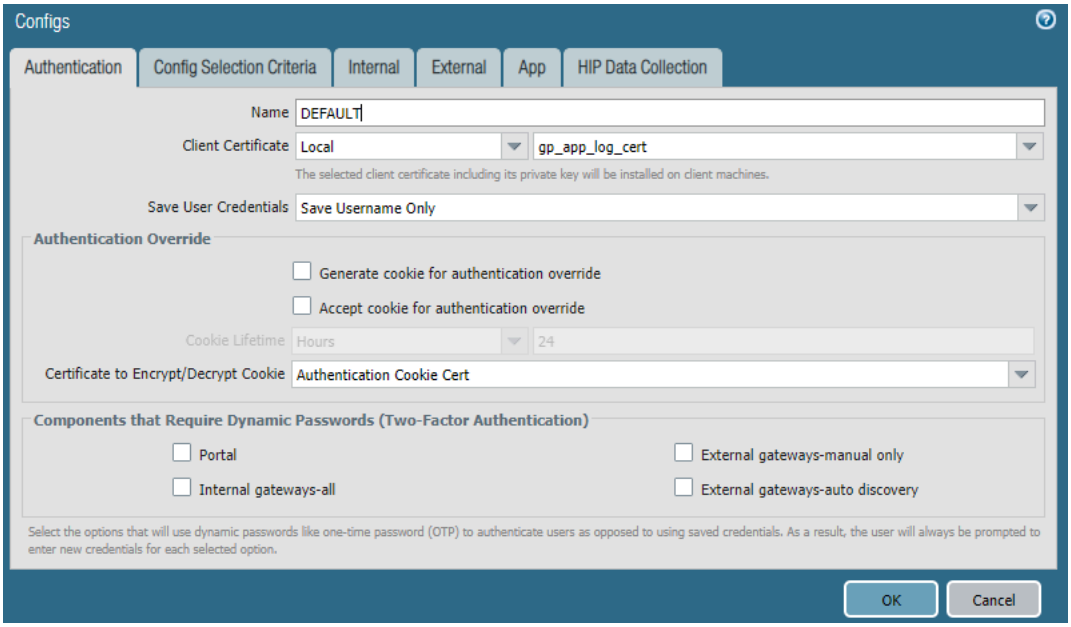
STEP 5 | Create or modify the existing Define the GlobalProtect Client Authentication Configurations for a specific group of users.

To enable the GlobalProtect app log collection for troubleshooting, you must define the agent configuration for a specific group of users to send the logs to Cortex Data Lake.

1. In Panorama, select **Network** > **GlobalProtect** > **Portals**.
2. Select the **Mobile_User_Template** from the **Template** drop-down.

   If you set up a deployment that includes multiple instances of Prisma Access on a single Panorama (multi-tenancy), you can select another template associated with the configuration.
3. Select **GlobalProtect_Portal** to edit the Prisma Access portal configuration.
4. Select the **Agent** tab.
5. Select the **Agent** tab and select the **DEFAULT** agent configuration.
6. Select the **Local** (default) and **gp_app_log_cert** from the **Client Certificate** drop-down.

   *Because the **Client Certificate** is used to push the Cortex Data Lake certificate, you cannot push the client certificate to authenticate to the portal or gateway either using a **Local** certificate type (default) or Simple Certificate Enrollment Protocol (SCEP).*

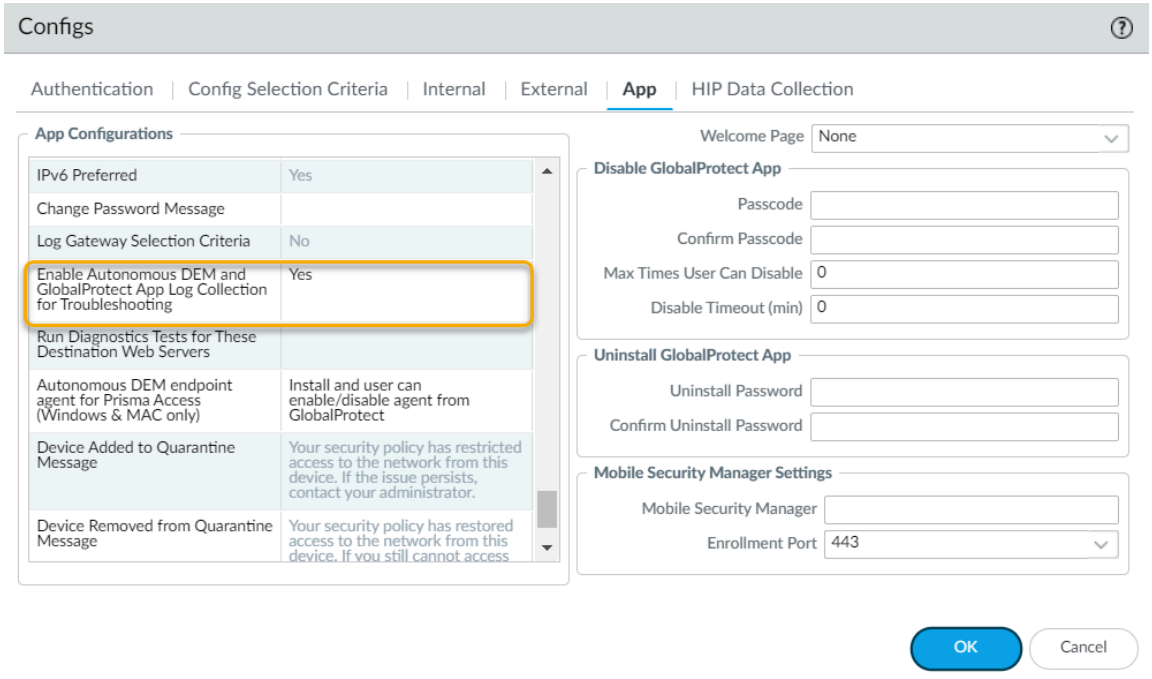


Configure the App Log Collection Settings on the GlobalProtect Portal

You must enable the GlobalProtect app to display the **Report an Issue** option on the GlobalProtect app to allow end users to send the GlobalProtect app troubleshooting and diagnostic logs directly from their endpoint to the Cortex Data Lake instance that is associated with the Prisma Access deployment for further analysis.

STEP 1 | Enable the GlobalProtect app log collection for troubleshooting on the GlobalProtect portal.

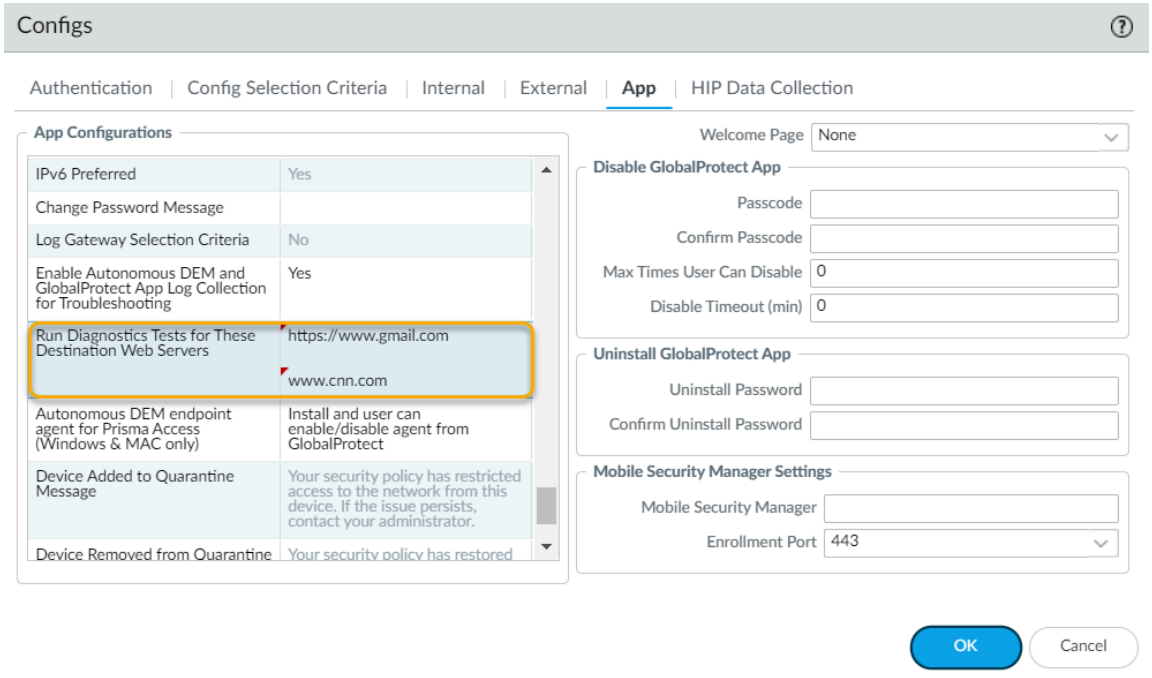
1. In Panorama, select **Network** > **GlobalProtect** > **Portals** > ***GlobalProtect_Portal*** > **Agent** ***DEFAULT*** > **App** > **Enable Autonomous DEM and GlobalProtect Log Collection for Troubleshooting**.
2. Set **Enable Autonomous DEM and GlobalProtect Log Collection for Troubleshooting** to **Yes** to enable the GlobalProtect app to display the **Report an Issue** option on the GlobalProtect app to allow end users to send the troubleshooting and diagnostic logs directly to Cortex Data Lake. You must configure the Cortex Data Lake certificate that is pushed from the portal as a client certificate to display the **Report an Issue** option. This certificate is used for the client to authenticate to Cortex Data Lake when sending the logs. When this setting is set to **No** (default), the GlobalProtect app will not display the **Report an Issue** option and end users cannot send the troubleshooting and diagnostic logs to Cortex Data Lake.



STEP 2 | Configure the HTTPS-based destination URLs that can contain IP addresses or fully qualified domain names on the GlobalProtect portal. Later, these HTTPS-based destination URLs are used to initiate performance tests for probing.

1. In Panorama, select **Network** > **GlobalProtect** > **Portals** > ***GlobalProtect_Portal*** > **Agent** ***DEFAULT*** > **App** > **Run Diagnostics Tests for These Destination Web Servers**.
2. Specify up to ten HTTPS-based destination URLs that can contain IP addresses or fully qualified domain names (for example, https://10.10.10.10/resource.html, https://webserver/file.pdf, or https://google.com) to **Run Diagnostics Tests for These Destination Web Servers** on the GlobalProtect portal. To help you accurately identify download speed results, you can specify a download file location that has the relevant size. For example, the size of the file can range from 10 MB to 50 MB to calculate the sufficient download speed. However, this calculation is not true for the size limitation of the web page to fetch and download the file that can take less than a second, which is not a sufficient sample size to determine strong download speed results. This field is empty by default.

   The HTTPS-based destination URLs that can contain IP addresses or fully qualified domain names that you provide are used only when **Enable Autonomous DEM and GlobalProtect App Log Collection for Troubleshooting** is set to **Yes** and when diagnostics are performed. These HTTPS-based destination URLs are not used when the GlobalProtect app creates troubleshooting reports when encountering an issue. Use commas, semi-colons, or separate lines to separate multiple fully qualified domain names (for example, google.com, gmail.com).



View the GlobalProtect App Troubleshooting and Diagnostic Logs on the Explore App

You must use the Explore app to view all GlobalProtect app troubleshooting reports and diagnostic logs that are forwarded to Cortex Data Lake from the end user's endpoint. The Details Within the GlobalProtect App Troubleshooting and Diagnostic Logs help you to identify the root cause and to resolve connectivity, network access, or performance issues.

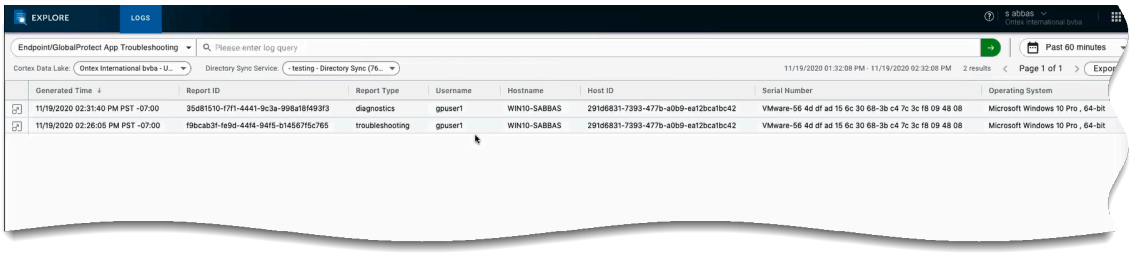
STEP 1 | Retrieve the GlobalProtect app troubleshooting and log records forwarded to Cortex Data Lake.

1. Log in to the Palo Alto Networks hub and select **Explore**.
2. Select **Endpoint/GlobalProtect App Troubleshooting**.

STEP 2 | View the entire troubleshooting or diagnostics log record.

1. Click the icon next to the row.

   You can change the fields that are displayed in the log table, their order, which fields are pinned, and to use the Search field to quickly find specific fields in the troubleshooting log from the end user's endpoint. For example, you can retrieve the endpoint serial number, hostname, username, or the endpoint's unique host ID.



2. Verify the entire troubleshooting and diagnostics log record in the **Log Details** window. The log record may only include troubleshooting information or diagnostic log based on user consent.

   The individual log fields are placed into logical groupings. If you did not enable the app to run diagnostic tests and to include diagnostic logs, the log fields for the **Endpoint State**, **GlobalProtect App Health**, **Gateway Network Impairments**, and **App Access Performance** groups are empty.

3. (Optional) If end users have consented to run diagnostic tests on the GlobalProtect app, click **Debug Logs** to download the GlobalProtect debug log files to your desktop for further analysis.

   You can unzip the GlobalProtect debug log files from the `reportid_GlobalProtectLogs.zip` zip package. You can enter the **reportid** search

criteria in the Search field to quickly find `reportid_GlobalProtectLogs.zip` zip package.

Details Within the GlobalProtect App Troubleshooting and Diagnostic Logs

Use the following topics to help you to identify the root cause for connectivity, network access, or performance issues experienced by end users by viewing the entire troubleshooting and diagnostics log record in the **Log Details** window:

- General Log Details
- Portal Log Details
- Gateway Log Details
- Network Log Details
- Endpoint State Log Details
- GlobalProtect App Health Log Details
- Gateway Network Impairments
- App Access Performance

General Log Details

The following table describes the individual log fields placed into the **General** logical group of the **Endpoint/GlobalProtect App Troubleshooting** log.

Log Field	Description
Generated Time	Date and time when the log was generated on the end user's endpoint. This string displays a timestamp value in UTC format (default).
Report ID	Unique identifier that is assigned by the GlobalProtect app to the report.

Log Field	Description
Report Type	Identifies the troubleshooting or diagnostics report type generated from the end user's endpoint.
Username	Username that is used to log in to the GlobalProtect.
Hostname	Hostname (IP address or fully qualified domain name) for the end user's endpoint.
Host ID	Unique host ID that is assigned by GlobalProtect to identify the host.
Serial Number	Serial number of the end user's endpoint.
Operating System	OS type of the end user's endpoint on which the GlobalProtect app is deployed.
Locale	System language of the end users endpoint on which the GlobalProtect is deployed.
GlobalProtect Version	GlobalProtect app version number.
Error Stage	Identifies what stage in the GlobalProtect connection workflow such as portal pre-login, gateway pre-login, gateway, get-config, or network discovery that the portal or gateway error occurred.
Error Message	The last error message that triggered the report generation. The identical error message is also displayed on the GlobalProtect app.
Error Details	Additional information to help you to identify the root cause to resolve connectivity, network access, or performance issues from the end user's endpoint.
Error Generated Time	Time when the error was generated from the end user's endpoint. This string displays a timestamp value in UTC format (default).
Host Time Offset	Time Zone offset from Greenwich Mean Time (GMT) in minutes of the host. For example, the value of `-420` is displayed for the PST time zone when daylight saving time is enabled.

Portal Log Details

The following table describes the individual log fields placed into the **Portal** logical group of the **Endpoint/GlobalProtect App Troubleshooting** log.

Log Field	Description
Portal Address	GlobalProtect portal that the end user last connected to.
Portal Reachable	Whether the portal is reachable and accepted the TCP connection request.
Portal SSL Certificate Valid	Whether the portal server certificate is valid.
Portal Authentication	Authentication methods used to establish a connection with the portal (for example, the client certificate authentication, username/password, or SAML).
Portal Status	Whether the GlobalProtect app was able to establish a connection with the portal.
Cached Configuration	Whether the local cached portal configuration is used (for example, when the portal is unreachable).
Configuration Refresh	Whether the GlobalProtect portal login is automatically used for configuration refresh.
Last Connect Time	The last time the end user connected to the portal. This string displays a timestamp value in UTC format (default).

Gateway Log Details

The following table describes the individual log fields placed into the **Gateway** logical group of the **Endpoint/GlobalProtect App Troubleshooting** log.

Log Field	Description
Gateway Address	GlobalProtect gateway that the end user last connected to or attempted to connect to based on failed gateway connection reports.
Location	Location of the GlobalProtect gateway that the end user connected to. You can also use this location information to determine the end user's proximity to the gateway.

Log Field	Description
	If you do not specify a gateway location, the Explore app displays an empty location field.
Gateway Reachable	Whether the gateway is reachable and accepted the TCP connection request.
Attempted Gateways	List of attempted gateways before connecting to a specific gateway.
Gateway SSL Certificate Valid	Whether the gateway server certificate is valid to allow the GlobalProtect app to connect to a gateway.
Gateway Authentication	Authentication methods used to establish a connection with the gateway (for example, the client certificate authentication, username/password, or SAML).
Gateway Status	Whether the GlobalProtect app is able to establish a connection with the gateway. **Connected** indicates a successful VPN connection. **Disconnected** indicates that the end user is not connected. **RestoringVPN connection** indicates that GlobalProtect attempted to reestablish the connection after the tunnel is disconnected.
IPSec Enabled	IPSec is enabled to secure the VPN tunnels between the GlobalProtect app and the gateway.
IPSec Failure Reason	Failure information for unsuccessful IPSec tunnel connection. For example, when port 4501 is specified for UDP and blocked, the IPSec connection cannot be established.
SSL Failure Reason	Failure information for unsuccessful SSL tunnel connection. For example, the SSL tunnel failed to establish a connection or the keepalive timeout disconnected after the tunnel connection was established.
Fallback to SSL Reason	Information about the GlobalProtect app to fall back to an SSL tunnel when the IPSec tunnel cannot be established.

Log Field	Description
DLSA Status	Whether the **No direct access to local network** option is enabled.
Logout Time	The last time the end user successfully logged out of the gateway. This string displays a timestamp value in UTC format (default).
Tunnel Rename	(Windows only) Whether the pre-logon tunnel was successfully renamed to the user tunnel.

Network Log Details

The following table describes the individual log fields placed into the **Network** logical group of the **Endpoint/GlobalProtect App Troubleshooting** log.

Log Field	Description
Network Access	Whether network access is available.
Type	Type of network connectivity such as Ethernet, WiFi, or Wireless Wide Area Network (WWAN) on the end user's endpoint.
Internet Access	Whether internet access is available on the end user's endpoint.
Internal Network	Whether the end user's endpoint is on the internal network.
Captive Portal	Whether the captive portal is detected so that end user must log in to a captive portal to access the internet.
Proxy Server	Hostname of the proxy server if the proxy is configured.
Dual Stack Tunnel Interface	Whether the dual stack network of the tunnel interface is enabled.
DNS Reachable	Whether the DNS servers are configured for internet access and reachable through the physical adapter.
Portal/Gateway Latency	The number of milliseconds before the TCP connection times out for the portal or gateway due to unresponsiveness.

Log Field	Description
GlobalProtect MTU	The **GlobalProtect MTU** value that is used by the app for the virtual adapter (see GlobalProtect App Customization).

Endpoint State Log Details

The following table describes the individual log fields placed into the **Endpoint State** logical group of the **Endpoint/GlobalProtect App Troubleshooting** log.

*If you did not enable the GlobalProtect app to run diagnostic tests and to include diagnostic logs, the log fields are empty for the **Endpoint State** group.*

Log Field	Description
CPU Usage	The percentage of CPU used on the end user's endpoint.
GlobalProtect CPU Usage	The percentage of CPU used by the GlobalProtect app.
Total Memory	Total memory in GB.
Memory Usage	The percentage of total memory used on the end user's endpoint.
GlobalProtect Memory Usage	The percentage of total memory used by the GlobalProtect app.
Total Disk Space	The total disk space used on the end user's endpoint.
Disk Available	The total disk space that is available on the end user's endpoint.

GlobalProtect App Health Log Details

The following table describes the individual log fields placed into the **GlobalProtect App Health** logical group of the **Endpoint/GlobalProtect App Troubleshooting** log.

*If you did not enable the GlobalProtect app to run diagnostic tests and to include diagnostic logs, the log fields are empty for the **GlobalProtect App Heath** group.*

Log Field	Description
Install History	Whether the GlobalProtect app was installed for the first time, upgraded to a newer version, or downgraded to a previous version.

Log Field	Description
	If end users are upgrading from GlobalProtect app 5.2.5 to a newer version, **Install History** displays that they upgraded from GlobalProtect app 5.2.5. If end users are upgrading from GlobalProtect app 5.2.4 to 5.2.5, **Install History** displays **Fresh Install**. If end users are downgrading from a newer version such as GlobalProtect app 5.2.6 to 5.2.5, **Install History** displays that they downgraded from GlobalProtect app 5.2.6 to 5.2.5. If end users are downgrading to older versions of the app (5.2.4 and earlier releases), the GlobalProtect App Log Collection for Troubleshooting feature is not supported.
Enforcer Status	Whether the GlobalProtect connections for network access is enabled or disabled on the GlobalProtect Portal but not enforced on the portal (see GlobalProtect App Customization).
Privileges	(macOS only) Whether end users are granted privileges to perform tasks such as enabling the system extensions to configure a split tunnel based on the destination domain and application and to enforce GlobalProtect connections for network access without requiring kernel extensions.
App Tampered	(Windows and macOS only) Whether GlobalProtect application files are altered or modified on the end user's endpoint.
Jailbroken Status	(iOS and Android only) Whether these end user endpoints have been jailbroken.
Last HIP Report Time	Last time that the host information report (HIP) report was sent. This string displays a timestamp value in UTC format (default).
Last Logout Time	Last time that the GlobalProtect app logged out. This string displays a timestamp value in UTC format (default).
Disable History	Number of times listed when end users enabled or disabled the GlobalProtect app. This string displays a timestamp value in UTC format (default).
Split-tunnel Configuration	(Windows and macOS only) Type of split tunnel capability that is configured based on an access

Log Field	Description
	route, destination domain, application, and HTTP/HTTPS video streaming application.
Crash history	(Windows and macOS only) Number of timestamps that correspond to the GlobalProtect app crashes (if any).

Gateway Network Impairments

The following table describes the individual log fields placed into the **Gateway Network Impairments** logical group of the **Endpoint/GlobalProtect App Troubleshooting** log.

*If you did not enable the GlobalProtect app to run diagnostic tests and to include diagnostic logs, the log fields are empty for the **Gateway Network Impairments** group.*

In order for the GlobalProtect app to run end-to-end diagnostic tests to test the network impairments, the GlobalProtect gateway must be allowed to send ICMP ping requests.

Log Field	Description
Latency	Latency that is measured between the end user's endpoint and the Prisma Access gateway in milliseconds.
Jitter	Jitter that is measured between the end user's endpoint and the Prisma Access gateway over a period of time in milleseconds.
Packet Loss	The percentage of packet loss that is used to measure the number of packets sent over a network that failed to reach the destination of the Prisma Access gateway. ICMP ping requests must be allowed on the gateway interface.

App Access Performance

You can specify up to ten HTTPS-based destination URLs that can contain IP addresses or fully qualified domain names (for example, https://10.10.10.10/resource.html, https://webserver/file.pdf, or https://google.com) for which you want to Configure the App Log Collection Settings on the GlobalProtect Portal by configuring the GlobalProtect portal.

*If you configured split tunneling to include or exclude traffic based on access routes (**Split Tunnel** > **Access Route**) or based on destination domain or application (**Split Tunnel** > **Domain and Application**) and run diagnostic tests and check performance tests inside or outside the tunnel, split tunneling takes precedence over the routing table and more specific routes take precedence over the default route.*

In order for the GlobalProtect app to run end-to-end diagnostic tests to probe the access performance, the following limitations apply:

- On iOS, the server performance tests include only the metrics that are tested through the physical adapter.
- On iOS 14 or later, the trace route tests are not supported.
- The web server must allow ICMP ping requests for latency, jitter, and packet loss tests.

The following table describes the individual log fields placed into the **App Access Performance** logical group of the **Endpoint/GlobalProtect App Troubleshooting** log.

*If you did not enable the GlobalProtect app to run diagnostic tests and to include diagnostic logs, the log field is empty for the **App Access Performance** group.*

Log Field	Description
Server Performance	Server performance data is tested from the end user's endpoint for each destination HTTPS-based web servers/applications that you configured on the portal. The following network metrics are tested through the physical adapter and outside of the tunnel: • `out_latency`—Latency that is measured in milliseconds between the end user's endpoint and for each destination HTTPS-based web servers/applications through the physical adapter. • `out_jitter`—Jitter that is measured over a period of time in milleseconds between the end user's endpoint and for each destination HTTPS-based web servers/applications through the physical adapter. • `out__packet_loss`—The percentage of packet loss that is used to measure the number of packets sent over a network that failed to reach each destination HTTPS-based web servers/applications through the physical adapter. • `out_tcp_connect_time`—TCP connection time that is measured to the server through the physical adapter. • `out_first_byte_time`—Time to first byte that is measured in milliseconds to connect to the server through the physical adapter. On macOS endpoints, time to first byte is calculated when the GlobalProtect client received the server certificate time and the API processing time. • `out_download_size`—Size of the file in bytes that is downloaded from the physical adapter. • `out_download_speed`—Speed that is measured in Kbps at which the file is downloaded from the physical adapter. We recommend that you use a binary file to test the download speed instead of using the web page. • `out_trace_route`—Result of the trace route that is configured on the destination through the physical adapter.

Log Field	Description
Server Performance	Server performance data is tested from the end user's endpoint for each destination HTTPS-based web servers/applications that you configured on the portal. The following network metrics are tested through the GlobalProtect tunnel: • `in_latency`—Latency that is measured in milliseconds between the end user's endpoint and for each destination HTTPS-based web servers/applications through the GlobalProtect tunnel. • `in_jitter`—Jitter that is measured over a period of time in milleseconds between the end user's endpoint and for each destination HTTPS-based web servers/applications through the GlobalProtect tunnel. • `in__packet_loss`—The percentage of packet loss that is used to measure the number of packets sent over a network that failed to reach each destination HTTPS-based web servers/applications through the GlobalProtect tunnel. • `in_tcp_connect_time`—TCP connection time that is measured to the server through the GlobalProtect tunnel. • `in_first_byte_time`—Time to first byte that is measured in milliseconds to connect to the server through the GlobalProtect tunnel. On macOS endpoints, time to first byte is calculated when the GlobalProtect client received the server certificate time and the API processing time. • `in_download_size`—Size of the file in bytes that is downloaded from the GlobalProtect tunnel. • `in_download_speed`—Speed that is measured in Kbps at which the file is downloaded from the GlobalProtect tunnel. We recommend that you use a binary file to test the download speed instead of using the web page. • `in_trace_route`—Result of the trace route that is configured on the destination through the GlobalProtect tunnel.

Logging for GlobalProtect in PAN-OS

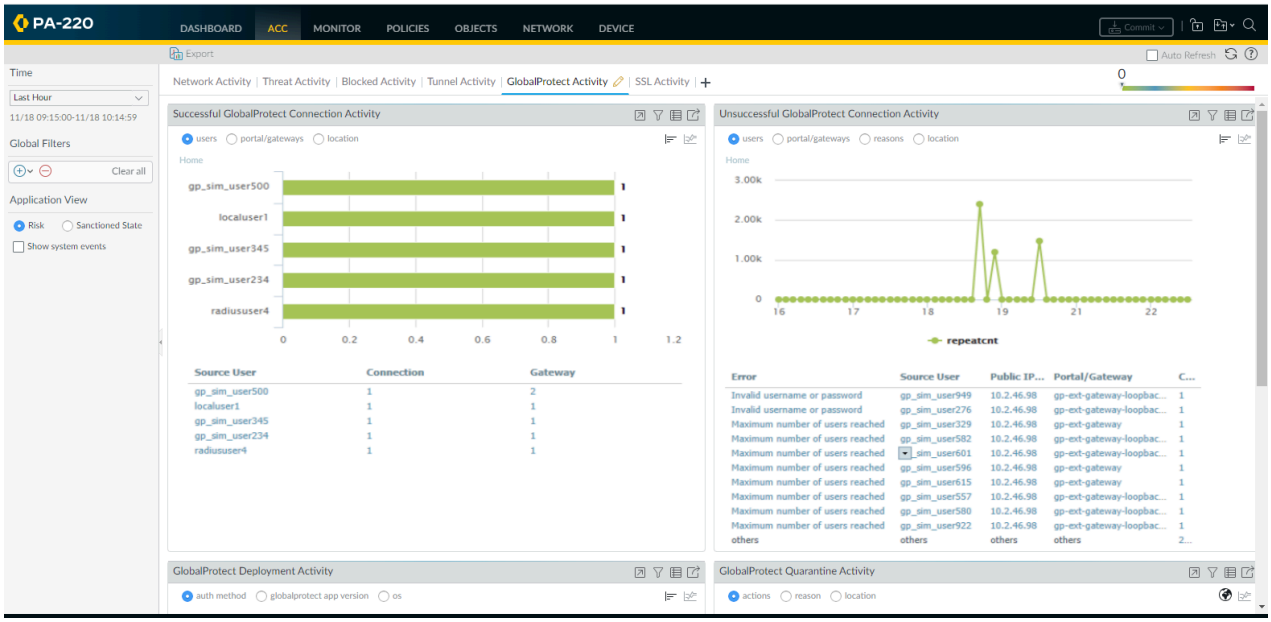
To help you monitor and troubleshoot issues with your GlobalProtect deployment, PAN-OS provides the following logging for GlobalProtect:

- View a Graphical Display of GlobalProtect User Activity in PAN-OS
- View All GlobalProtect Logs on a Dedicated Page in PAN-OS
- Event Descriptions for the GlobalProtect Logs in PAN-OS
- Filter GlobalProtect Logs for Gateway Latency in PAN-OS
- Restrict Access to GlobalProtect Logs in PAN-OS
- Forward GlobalProtect Logs to an External Service in PAN-OS
- Configure Custom Reports for GlobalProtect in PAN-OS

These features are available for any Palo Alto Networks next-generation firewall deployed as a GlobalProtect gateway or portal.

View a Graphical Display of GlobalProtect User Activity in PAN-OS

The Application Command Center (ACC) in PAN-OS displays a graphical view of user activity in your GlobalProtect deployment on the GlobalProtect Activity tab.



The GlobalProtect Activity charts and graphs are interactive and support similar drill-down functionality to other ACC charts and graphs.

STEP 1 | In PAN-OS, select **ACC** > **GlobalProtect Activity**.

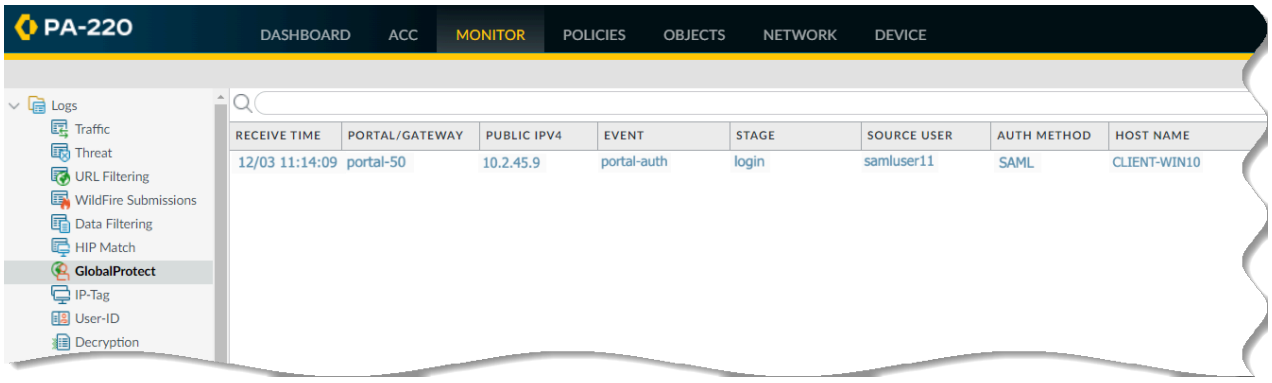
STEP 2 | View the charts as follows:

- **Successful GlobalProtect Connection Activity**—Chart view of GlobalProtect connection activity over the selected time period. Use the toggle at the top of the chart to switch between connection statistics by users, portals and gateways, and location.
- **Unsuccessful GlobalProtect Connection Activity**—Chart view of unsuccessful GlobalProtect connection activity over the selected time period. Use the toggle at the top of the chart to switch between connection statistics by users, portals and gateways, and location. To help you identify and troubleshoot connection issues, you can also view the reasons chart or graph. For this chart, the ACC indicates the error, source user, public IP address and other information to help you identify and resolve the issue quickly.
- **GlobalProtect Deployment Activity**—Chart view summary of your deployment. Use the toggle at the top of the chart to view the distribution of users by authentication method, GlobalProtect app version, and operating system version.

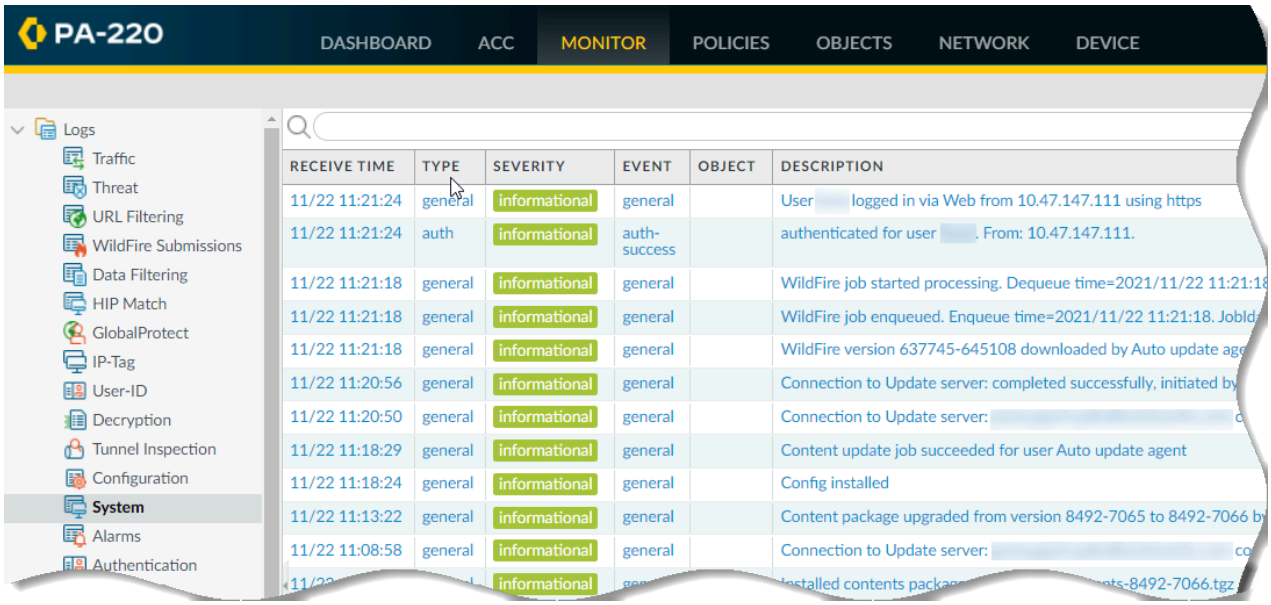
View All GlobalProtect Logs on a Dedicated Page in PAN-OS

In PAN-OS, GlobalProtect logs have a dedicated page that enables you to view GlobalProtect events in one place. The dedicated GlobalProtect log category eliminates the need for using complex log queries to locate GlobalProtect logs. You can also sort, filter, and query the GlobalProtect logs.

The GlobalProtect log page displays information that includes the authentication method. The following screenshot shows an example of logs in the **Monitor** > **Logs** > **GlobalProtect** page; note the **Auth Method** of **SAML**.



However, GlobalProtect authentication event logs remain in **Monitor** > **Logs** > **System**.



STEP 1 | In PAN-OS, select **Monitor** > **Logs**.

STEP 2 | View the following logs:

- LSVPN/satellite events.
- GlobalProtect portal and gateway logs.
- Clientless VPN logs.
- System logs related to GlobalProtect.

Event Descriptions for the GlobalProtect Logs in PAN-OS

Use the following descriptions to help you to identify GlobalProtect portal, gateway, or Clientless VPN events when viewing GlobalProtect logs in PAN-OS at **Monitor** > **Logs** > **GlobalProtect**:

Portal Event Details

The following table describes log events related to the GlobalProtect portal.

Event	Description
portal-auth	Indicates a GlobalProtect portal authentication stage. See Status for results.
portal-gen-cookie	Indicates a GlobalProtect portal authentication override cookie generation event. See Status for results.
portal-getconfig	Indicates a GlobalProtect portal event for generating GlobalProtect client configuration, such as dynamic app configuration or gateway list.
portal-prelogin	Indicates a GlobalProtect portal pre-login event. As a part of the event, the GlobalProtect client does the following: • Certificate: validates whether a client certificate is valid. • SAML: generates a SAML request and sends it back to a GlobalProtect client. • Kerberos: triggers a Kerberos authentication process.

Gateway Event Details

The following table describes log events related to the GlobalProtect gateway.

Event	Description
gateway-agent-msg	Indicates a GlobalProtect gateway event for a message received from the GlobalProtect client, such as GlobalProtect client disable reason message.
gateway-auth	Indicates GlobalProtect gateway authentication stage. See Status for results.
gateway-config-release	Indicates a GlobalProtect gateway event for configuration release, such as remove ip-user mapping or remove tunnel.
gateway-connected	Indicates a GlobalProtect gateway event for a GlobalProtect client successful connection for tunnel or non-tunnel mode.
gateway-framed-ip	Indicates a GlobalProtect gateway event where the gateway retrieved a framed IPv4 address from RADIUS for a GlobalProtect client.
gateway-getconfig	Indicates a GlobalProtect gateway event for generating GlobalProtect client configuration, such as split-tunnel, virtual IP, or tunnel information.
gateway-hip-check	Indicates a GlobalProtect gateway event to confirm whether a GlobalProtect HIP report was updated or not, and to refresh ip-user mapping. Refer to the description for latency reported information. Examples include items such as HIP report is not needed or HIP report is needed.
gateway-hip-report	Indicates a GlobalProtect gateway event to confirm whether a HIP report was received from a GlobalProtect client, to update ip-user mapping, and to enforce HIP policy.
gateway-inheritance	Indicates a GlobalProtect gateway event where a GlobalProtect gateway is using a dynamic IP address and the IP address changed.
gateway-logout	Indicates a GlobalProtect gateway event for a GlobalProtect client logout.

Event	Description
gateway-prelogin	Indicates a GlobalProtect gateway event. As a part of the event, the GlobalProtect client does the following: • Certificate: validates whether a client certificate is valid. • SAML: generates a SAML request and sends it back to a GlobalProtect client. • Kerberos: triggers a Kerberos authentication process.
gateway-register	Indicates GlobalProtect client user information, such as username, domain-name, computer name, hostid, serial number, public ip, or login time is added on the gateway.
gateway-setup-ipsec	Indicates a GlobalProtect gateway event for setting up an IPSec VPN tunnel.
gateway-setup-ssl	Indicates a GlobalProtect gateway event for setting up a SSL VPN tunnel.
gateway-switch-to-ssl	Indicates a GlobalProtect gateway tunnel switch from IPSec to SSL considering IPSec tunnel was not successful.
gateway-tunnel-latency	Indicates GlobalProtect gateway latency provided by a GlobalProtect client. Refer to description for latency reported information, such as Pre-tunnel latency: 10ms or Post-tunnel latency: 1ms
quarantine-add	Indicates a GlobalProtect gateway event for a GlobalProtect client, confirming that the client is added to the quarantine list.
quarantine-delete	Indicates a GlobalProtect gateway event for a GlobalProtect client, confirming that the client is removed from the quarantine list.

Clientless VPN Event Details

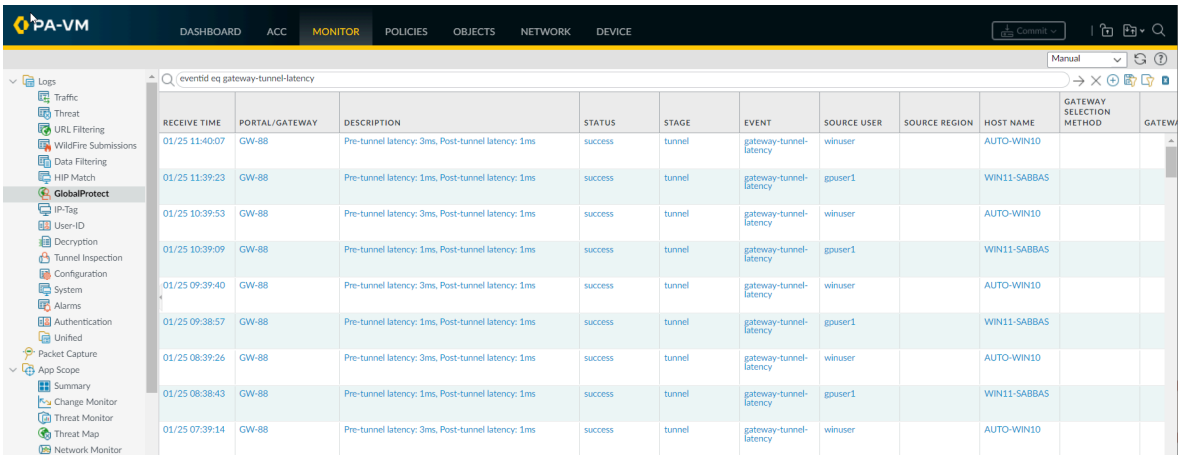
The following table describes log events related to the GlobalProtect Clientless VPN.

Event	Description
clientlessvpn-login	Indicates a GlobalProtect portal event for GlobalProtect Clientless VPN login.
clientlessvpn-logout	Indicates a GlobalProtect portal event for GlobalProtect Clientless VPN logout.
clientlessvpn-prelogin	Indicates a GlobalProtect portal event for GlobalProtect Clientless VPN. As a part of the event, the following takes place: • Certificate: validate whether a client certificate is valid. • SAML: generate a SAML request and send it back to a GlobalProtect client. • Kerberos: trigger a Kerberos authentication process.

Filter GlobalProtect Logs for Gateway Latency in PAN-OS

To help you troubleshoot connection and performance issues for a specific user, GlobalProtect collects and reports telemetry information for latency between the GlobalProtect gateway and the endpoint. With this information, you can identify the gateway the user is connected to, the current stage of the connection, and statistics about the pre-tunnel and post-tunnel network latency.

- Pre-tunnel latency measurements are based on the OpenSSL handshake. The time is measured from the initial SYN until the TCP 3-way handshake is completed.
- Post-tunnel latency measurements are taken after the tunnel is established. The time is measured for the round trip time (RTT) of a single tunnel keep-alive from an ICMP probe. The post-tunnel time is often faster, as it measures the single keep-alive and not the whole TCP handshake.



STEP 1 | In PAN-OS, select **Monitor** > **Logs** > **GlobalProtect**.

STEP 2 | Filter for **`eventid eq gateway-tunnel-latency`** in the GlobalProtect Logs.

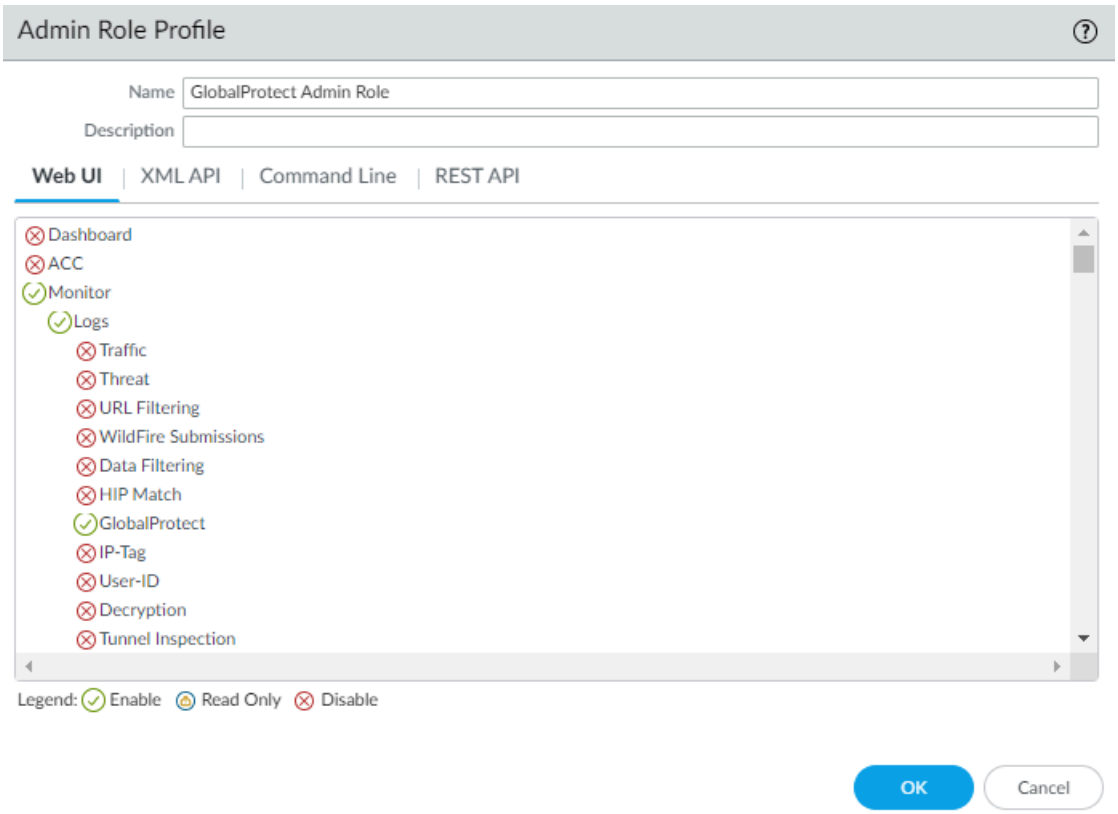
Restrict Access to GlobalProtect Logs in PAN-OS

If access to GlobalProtect logs and data is a concern (such as for regulatory compliance or data privacy concerns), you can restrict access to these logs in PAN-OS.

STEP 1 | In PAN-OS, create an Admin Role profile.

STEP 2 | Specify the **GlobalProtect Admin** role.

STEP 3 | Select **Monitor**, **Logs**, and **GlobalProtect** to enable, disable, or provide read-only access to the GlobalProtect logs.



Forward GlobalProtect Logs to an External Service in PAN-OS

In PAN-OS, you can forward GlobalProtect logs to an external service such as a syslog receiver or ticketing system. In cases where some teams in your organization can achieve greater efficiency by monitoring only the GlobalProtect logs that are relevant to their operations, you can create forwarding filters based on GlobalProtect log attributes. For example, you can filter by:

- GlobalProtect authentication events generated by GlobalProtect (type eq globalprotect)

  GlobalProtect authentication events generated by the authentication service (type eq auth) remain in **Monitor** > **Logs** > **System**.
- All other GlobalProtect events (non-authentication)

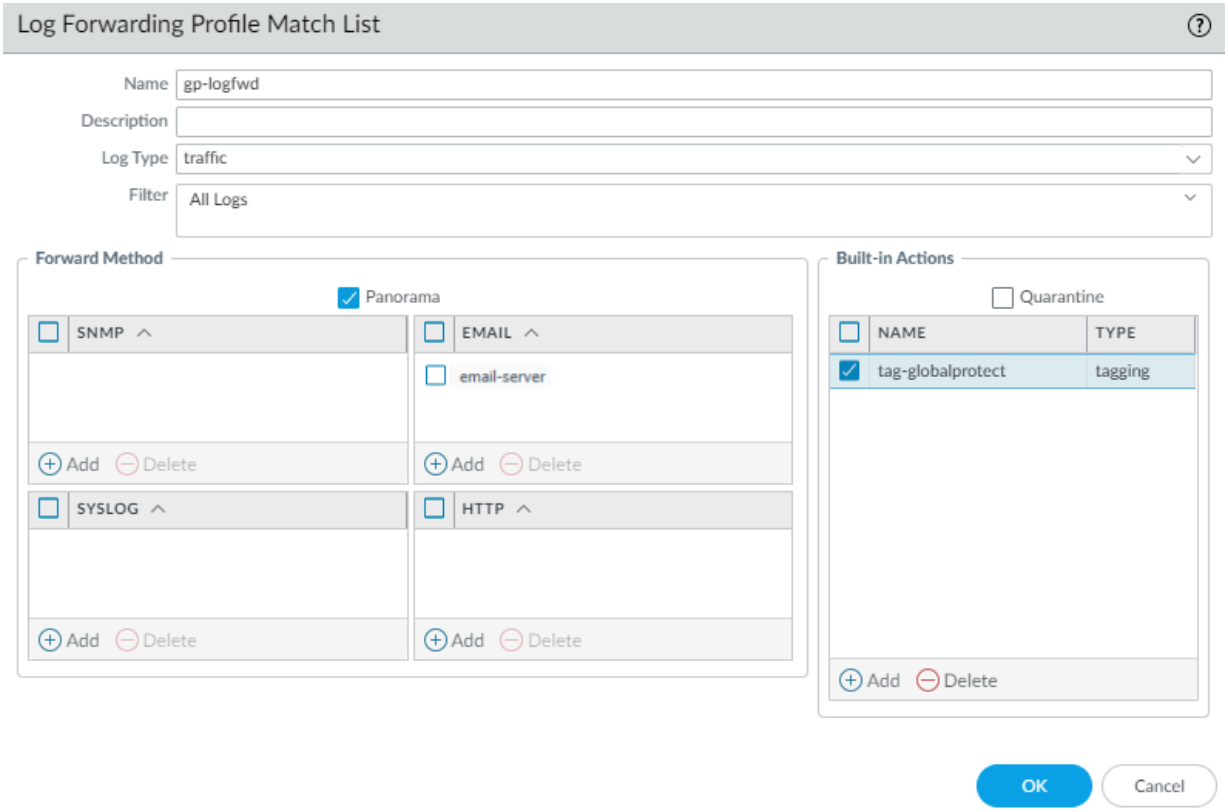
Palo Alto Networks firewalls forward GlobalProtect logs using the following format. To facilitate parsing, the delimiter is a comma: each field is a comma-separated value (CSV) string.

Format: domain, receive_time, serial, seqno, actionflags, type, subtype, config_ver, time_generated, vsys, eventid, stage, auth_method, tunnel_type, srcuser, srcregion, machinename, public_ip, public_ipv6, private_ip, private_ipv6, hostid, serialnumber, client_ver, client_os, client_os_ver, repeatcnt, reason, error, opaque, status, location, login_duration, connect_method, error_code, portal

STEP 1 | In PAN-OS, configure log forwarding for GlobalProtect logs.

STEP 2 | Configure a server profile for each external service that will receive log information.

STEP 3 | Configure the destinations for GlobalProtect logs.



You can also add or remove tags from a source or destination IP address in a log entry.

STEP 4 | Commit and verify your changes.

Configure Custom Reports for GlobalProtect in PAN-OS

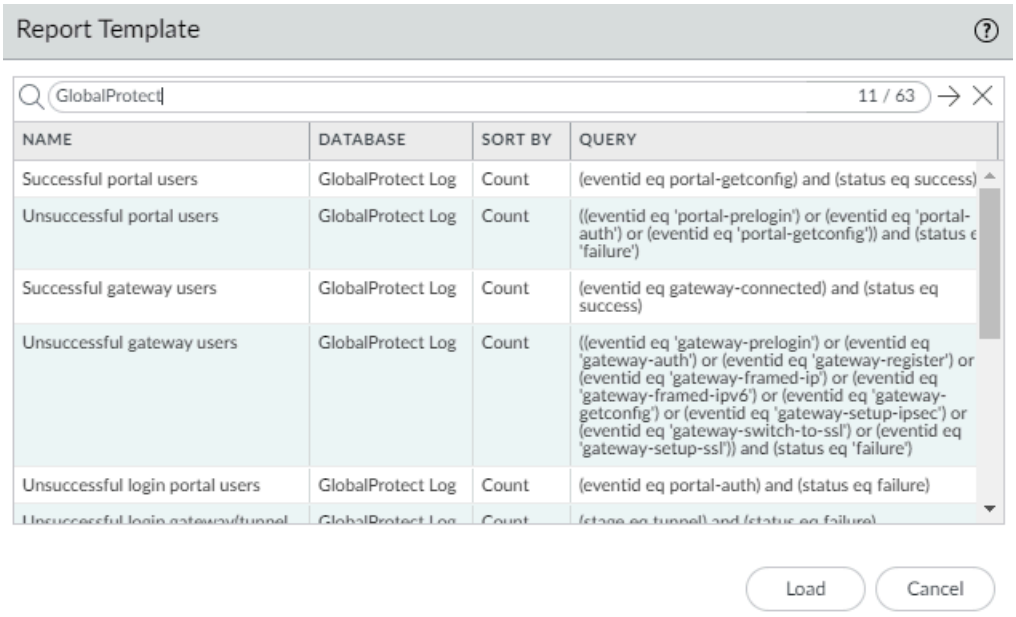
You can configure custom reports based on GlobalProtect logs that the firewall generates immediately (on demand) or on schedule (each night).

STEP 1 | In PAN-OS, Generate a Custom Report for GlobalProtect.

STEP 2 | Select **Monitor** > **Manage Custom Reports**.

STEP 3 | Click **Add** and then enter a **Name** for the report.

STEP 4 | To base a report on an predefined template, click **Load Template** and choose the template. You can then edit the template and save it as a custom report.



STEP 5 | If you choose to build the report from scratch, select the database you want to use for the report as **Device GlobalProtect Log**.

STEP 6 | Select the **Scheduled** check box to run the report each night. The report is then available for viewing in the **Reports** column on the side.

STEP 7 | Define the filtering criteria. Select the **Time Frame**, the **Sort By** order, **Group By** preference, and select the columns that must display in the report.

STEP 8 | (Optional) Select the **Query Builder** attributes if you want to further refine the selection criteria. To build a report query, specify the following and click **Add**. Repeat as needed to construct the full query.

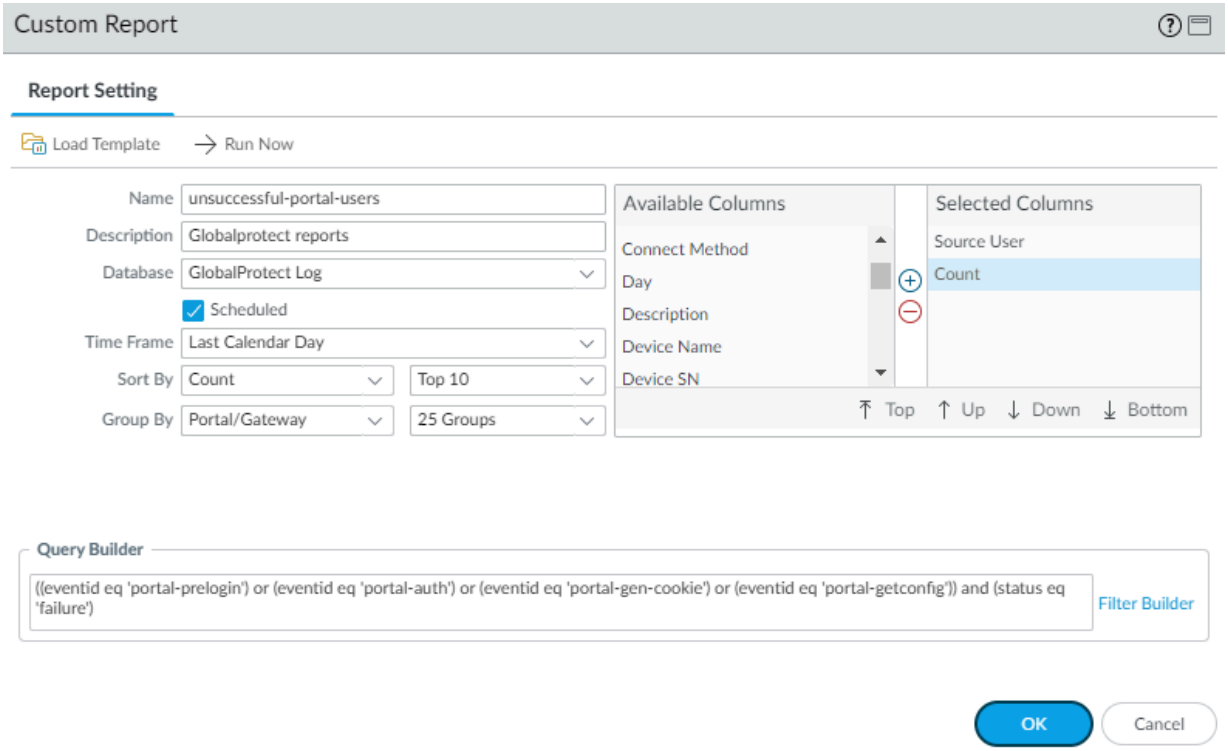
- **Connector**—Choose the connector (and/or) to precede the expression you are adding.
- **Negate**—Select the check box to interpret the query as a negation. If, for example, you choose to match entries in the last 24 hours and/or are originating from the untrust zone,

the negate option causes a match on entries that are not in the past 24 hours and/or are not from the untrust zone.

- **Attribute**—Choose a data element. The available options depend on the choice of database.
- **Operator**—Choose the criterion to determine whether the attribute applies (such as =). The available options depend on the choice of database.
- **Value**—Specify the attribute value to match.

For example, to build a report for GlobalProtect portal users with unsuccessful login attempts, use a query similar to the following:

```
((eventid eq 'portal-prelogin') or (eventid eq 'portal-auth') or
(eventid eq 'portal-gen-cookie') or (eventid eq 'portal-getconfig'))
and (status eq 'failure')
```



STEP 9 | To test the report settings, select **Run Now**. Modify the settings as required to change the information that is displayed in the report.

STEP 10 | Click **OK** to save the custom report.

