# Table of Contents

## GlobalProtect Overview

- About the GlobalProtect Components .......................................................... 9
  - GlobalProtect Portal.................................................................................... 9
  - GlobalProtect Gateways............................................................................ 9
  - GlobalProtect App..................................................................................... 9
- What OS Versions are Supported with GlobalProtect? .......................... 11
  - About GlobalProtect Licenses................................................................. 12

## Get Started

- Create Interfaces and Zones for GlobalProtect ......................................... 15
- Enable SSL Between GlobalProtect Components ...................................... 17
  - About GlobalProtect Certificate Deployment ....................................... 17
  - GlobalProtect Certificate Best Practices ............................................... 17
  - Deploy Server Certificates to the GlobalProtect Components ............... 20

## Authentication

- About GlobalProtect User Authentication ............................................... 27
  - Supported GlobalProtect Authentication Methods.................................. 27
  - How Does the App Know What Credentials to Supply? ......................... 29
  - How Does the App Know Which Certificate to Supply? .......................... 30
- Set Up External Authentication .................................................................... 31
  - Set Up LDAP Authentication ................................................................... 31
  - Set Up SAML Authentication ................................................................... 33
  - Set Up Kerberos Authentication ............................................................... 34
  - Set Up RADIUS or TACACS+ Authentication ............................................ 36
- Set Up Client Certificate Authentication .................................................... 38
  - Deploy Shared Client Certificates for Authentication ............................. 38
  - Deploy Machine Certificates for Authentication ....................................... 38
  - Deploy User-Specific Client Certificates for Authentication .................. 43
- Set Up Two-Factor Authentication ............................................................... 46
  - Enable Two-Factor Authentication Using Certificate and Authentication Profiles .................................................. 46
  - Enable Two-Factor Authentication Using One-Time Passwords (OTPs) .......... 48
  - Enable Two-Factor Authentication Using Smart Cards .......................... 51
- Set Up Authentication for strongSwan Ubuntu and CentOS Endpoints .......... 54
  - Enable Authentication Using a Certificate Profile .................................... 54
  - Enable Authentication Using an Authentication Profile .......................... 56
  - Enable Authentication Using Two-Factor Authentication ....................... 58
- Configure GlobalProtect to Facilitate Multi-Factor Authentication Notifications .................................................. 61
  - Enable Delivery of VSAs to a RADIUS Server ....................................... 64
  - Enable Group Mapping ............................................................................ 65

## GlobalProtect Gateways

- GlobalProtect Gateways Overview.............................................................. 69
- GlobalProtect Gateway Concepts ............................................................... 70
  - Types of Gateways .................................................................................. 70
  - Gateway Priority in a Multiple Gateway Configuration .......................... 70
<table>
<thead>
<tr>
<th>GlobalProtect MIB Support</th>
<th>71</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prerequisite Tasks for Configuring the GlobalProtect Gateway</td>
<td>73</td>
</tr>
<tr>
<td>Configure a GlobalProtect Gateway</td>
<td>74</td>
</tr>
</tbody>
</table>

GlobalProtect Portals | 85 |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>GlobalProtect Portal Overview</td>
<td>87</td>
</tr>
<tr>
<td>Prerequisite Tasks for Configuring the GlobalProtect Portal</td>
<td>88</td>
</tr>
<tr>
<td>Set Up Access to the GlobalProtect Portal</td>
<td>89</td>
</tr>
<tr>
<td>Define the GlobalProtect Client Authentication Configurations</td>
<td>91</td>
</tr>
<tr>
<td>Define the GlobalProtect Agent Configurations</td>
<td>92</td>
</tr>
<tr>
<td>Customize the GlobalProtect App</td>
<td>97</td>
</tr>
<tr>
<td>Customize the GlobalProtect Portal Login, Welcome, and Help Pages</td>
<td>106</td>
</tr>
</tbody>
</table>

GlobalProtect Apps | 109 |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy the GlobalProtect App Software</td>
<td>111</td>
</tr>
<tr>
<td>Host App Updates on the Portal</td>
<td>112</td>
</tr>
<tr>
<td>Host App Updates on a Web Server</td>
<td>113</td>
</tr>
<tr>
<td>Test the App Installation</td>
<td>114</td>
</tr>
<tr>
<td>Download and Install the GlobalProtect Mobile App</td>
<td>118</td>
</tr>
<tr>
<td>Download and Install the GlobalProtect App for Chrome OS</td>
<td>119</td>
</tr>
<tr>
<td>Deploy App Settings Transparently</td>
<td>124</td>
</tr>
<tr>
<td>Customizable App Settings</td>
<td>124</td>
</tr>
<tr>
<td>Deploy App Settings to Windows Endpoints</td>
<td>131</td>
</tr>
<tr>
<td>Deploy App Settings to macOS Endpoints</td>
<td>140</td>
</tr>
</tbody>
</table>

GlobalProtect Clientless VPN | 143 |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Clientless VPN Overview</td>
<td>145</td>
</tr>
<tr>
<td>Supported Technologies</td>
<td>147</td>
</tr>
<tr>
<td>Configure Clientless VPN</td>
<td>148</td>
</tr>
<tr>
<td>Troubleshoot Clientless VPN</td>
<td>153</td>
</tr>
</tbody>
</table>

Mobile Device Management | 157 |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Device Management Overview</td>
<td>159</td>
</tr>
<tr>
<td>Set Up the MDM Integration With GlobalProtect</td>
<td>162</td>
</tr>
<tr>
<td>Manage the GlobalProtect App Using a Supported Third-Party MDM</td>
<td>162</td>
</tr>
<tr>
<td>Manage the GlobalProtect App Using Other Third-Party MDMs</td>
<td>234</td>
</tr>
</tbody>
</table>

Host Information | 243 |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>About Host Information</td>
<td>245</td>
</tr>
<tr>
<td>What Data Does the GlobalProtect App Collect?</td>
<td>245</td>
</tr>
<tr>
<td>How Does the Gateway Use the Host Information to Enforce Policy?</td>
<td>247</td>
</tr>
<tr>
<td>How Do Users Know if Their Systems are Compliant?</td>
<td>248</td>
</tr>
<tr>
<td>How Do I Get Visibility into the State of the Endpoints?</td>
<td>248</td>
</tr>
<tr>
<td>Configure HIP-Based Policy Enforcement</td>
<td>250</td>
</tr>
<tr>
<td>Collect Application and Process Data From Endpoints</td>
<td>258</td>
</tr>
<tr>
<td>Block Endpoint Access</td>
<td>264</td>
</tr>
<tr>
<td>Configure Windows User-ID Agent to Collect Host Information</td>
<td>266</td>
</tr>
<tr>
<td>MDM Integration Overview</td>
<td>266</td>
</tr>
<tr>
<td>Information Collected</td>
<td>266</td>
</tr>
<tr>
<td>System Requirements</td>
<td>268</td>
</tr>
</tbody>
</table>
Configure GlobalProtect to Retrieve Host Information ................................................... 268  
Troubleshoot the MDM Integration Service ................................................................. 271

**GlobalProtect Quick Configs**.................................................................................. 273  
Remote Access VPN (Authentication Profile)............................................................... 275  
Remote Access VPN (Certificate Profile)..................................................................... 278  
Remote Access VPN with Two-Factor Authentication ............................................... 281  
Always On VPN Configuration.................................................................................... 285  
Remote Access VPN with Pre-Logon.......................................................................... 286  
GlobalProtect Multiple Gateway Configuration......................................................... 292  
GlobalProtect for Internal HIP Checking and User-Based Access.............................. 295  
Remote Access VPN with Pre-Logon ........................................................................ 286  
GlobalProtect Multiple Gateway Configuration ......................................................... 292  
GlobalProtect for Internal HIP Checking and User-Based Access.............................. 295  
Mixed Internal and External Gateway Configuration................................................ 299

**GlobalProtect Architecture** .................................................................................... 305  
GlobalProtect Reference Architecture Topology.......................................................... 307  
GlobalProtect Portal...................................................................................................... 307  
GlobalProtect Gateways................................................................................................ 307  
GlobalProtect Reference Architecture Features........................................................ 309  
End User Experience..................................................................................................... 309  
Management and Logging............................................................................................ 309  
Monitoring and High Availability.................................................................................. 310  
GlobalProtect Reference Architecture Configurations................................................. 311  
Gateway Configuration................................................................................................. 311  
Portal Configuration...................................................................................................... 311  
Policy Configurations.................................................................................................... 311

**GlobalProtect Cryptography**..................................................................................... 313  
About GlobalProtect Cipher Selection......................................................................... 315  
Cipher Exchange Between the GlobalProtect App and Gateway.................................. 316  
GlobalProtect Cryptography References..................................................................... 318  
Reference: GlobalProtect App Cryptographic Functions.............................................. 318  
TLS Cipher Suites Supported by GlobalProtect Apps................................................ 319  
Ciphers Used to Set Up IPsec Tunnels........................................................................ 325  
SSL APIs....................................................................................................................... 326

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, the Microsoft Store for Windows 10 UWP endpoints, and the Chrome Web Store for Chromebooks). If you are using the Host Information Profile (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 [Types of 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, whether or not users can uninstall the app—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 Software](#) for details.

The GlobalProtect app for mobile endpoints (iOS, Android, Windows UWP, and Chrome OS) is available through the official store for the endpoint—the Apple App Store for iOS, Google Play for Android, the Microsoft Store for Windows UWP, and the Chrome Web Store for Chromebooks (Chrome OS). You can alternatively [Deploy the GlobalProtect Mobile App Using AirWatch](#), which is a third-party mobile endpoint management system.

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 subscription. 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
- Provides IPv6 connections
- Split tunnels traffic based on the destination domain, application process name, or HTTP/HTTPS video streaming application.

For GlobalProtect Clientless VPN, you must also install a GlobalProtect subscription 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.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Subscription Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single external gateway (Windows and macOS)</td>
<td>—</td>
</tr>
<tr>
<td>Single or multiple internal gateways</td>
<td>—</td>
</tr>
<tr>
<td>Multiple external gateways</td>
<td>—</td>
</tr>
<tr>
<td>HIP Checks</td>
<td>✓</td>
</tr>
<tr>
<td>App for endpoints running Windows and macOS</td>
<td>—</td>
</tr>
<tr>
<td>Mobile app for endpoints running iOS, Android, Chrome OS, and Windows 10 UWP</td>
<td>✓</td>
</tr>
<tr>
<td>App for endpoints running Linux</td>
<td>✓</td>
</tr>
<tr>
<td>IPv6 for external gateways</td>
<td>✓</td>
</tr>
<tr>
<td>IPv6 for internal gateways</td>
<td>✓</td>
</tr>
<tr>
<td>(change to default behavior—starting with GlobalProtect app 4.1.3, a GlobalProtect subscription is not required for this use case)</td>
<td>—</td>
</tr>
<tr>
<td>Clientless VPN</td>
<td>✓</td>
</tr>
<tr>
<td>Split tunneling based on destination domain, client process, and video streaming application</td>
<td>✓</td>
</tr>
</tbody>
</table>

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 Best Practices for Securing Administrative Access 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 13-untrust.
   - Place internal gateways in an internal zone, such as 13-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 13-trust zone.

<table>
<thead>
<tr>
<th>Name</th>
<th>Tags</th>
<th>Zone</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>corp-vpn</td>
<td>any</td>
<td>13-trust</td>
<td>any</td>
<td>allow</td>
</tr>
</tbody>
</table>

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 on page 17
- GlobalProtect Certificate Best Practices on page 17
- Deploy Server Certificates to the GlobalProtect Components on page 20

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:

<table>
<thead>
<tr>
<th>Certificate</th>
<th>Usage</th>
<th>Issuing Process/Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA certificate</td>
<td>Used to sign certificates issued to the GlobalProtect components.</td>
<td>If you plan on using self-signed certificates, we recommend that you generate a CA certificate on the portal, and then use that certificate to issue the required GlobalProtect certificates.</td>
</tr>
</tbody>
</table>
| 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 connection. |
Certificate | Usage | Issuing Process/Best Practices
---|---|---
Gateway server certificate | Enables GlobalProtect apps to establish an HTTPS connection with the gateway. | 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, if applicable, the 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.

- This certificate is identified in an SSL/TLS service profile. You assign the portal server certificate by selecting its associated service profile in a gateway configuration.  
- Generate a CA certificate on the portal and use that CA certificate to generate all gateway 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 gateway.  
- The portal distributes the gateway root CA certificates to agents in the client configuration, so the gateway certificates do not need 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
<table>
<thead>
<tr>
<th>Certificate</th>
<th>Usage</th>
<th>Issuing Process/Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional) Client</td>
<td>Used to enable mutual authentication when establishing an HTTPS</td>
<td>• 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:</td>
</tr>
<tr>
<td>certificate</td>
<td>session between the GlobalProtect apps and the gateways/portal.</td>
<td>• Use a single client certificate across all GlobalProtect apps that receive the same configuration. Assign the <strong>Local</strong> client certificate by uploading the certificate to the portal, and then selecting it in a portal agent configuration.</td>
</tr>
<tr>
<td></td>
<td>This ensures that only endpoints with valid client certificates are</td>
<td>• Use simple certificate enrollment protocol (<strong>SCEP</strong>) 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.</td>
</tr>
</tbody>
</table>
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 Use Simple Certificate Enrollment Protocol (SCEP) to request a server certificate from your enterprise CA.

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.

    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.
Authentication

The GlobalProtect™ portal and gateway must authenticate end users before allowing access to GlobalProtect resources. You must configure authentication mechanisms prior to portal and gateway setup. The following sections detail the supported authentication mechanisms and how to configure them:

- About GlobalProtect User Authentication
- Set Up External Authentication
- Set Up Client Certificate Authentication
- Set Up Two-Factor Authentication
- Set Up Authentication for strongSwan Ubuntu and CentOS Endpoints
- Configure GlobalProtect to Facilitate Multi-Factor Authentication Notifications
- Enable Delivery of VSAs to a RADIUS Server
- Enable Group Mapping
About 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.

- Supported GlobalProtect Authentication Methods
- How Does the App Know What Credentials to Supply?

Supported GlobalProtect Authentication Methods

The following topics describe the authentication methods that GlobalProtect supports and provide usage guidelines for each method.

- Local Authentication on page 27
- External Authentication on page 27
- Client Certificate Authentication on page 27
- Two-Factor Authentication on page 27
- Multi-Factor Authentication for Non-Browser-Based Applications on page 28

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 LDAP, Kerberos, TACACS+, SAML, or RADIUS services (including support for two-factor, token-based authentication mechanisms, such as one-time password (OTP) authentication). To enable external authentication:

- Create a server profile with settings for access to the external authentication service.
- Create an authentication profile that refers to the server profile.
- 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. See Set Up External Authentication for instructions. See Remote Access VPN (Authentication Profile) for an example configuration.

Client Certificate Authentication

For enhanced security, you can configure the portal or gateway to use a client certificate to obtain the username and authenticate the user before granting access to the system.

- 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.)

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).

Two-Factor Authentication

With two-factor authentication, the portal or gateway authenticates users through two mechanisms, such as a one-time password and Active Directory (AD) login credentials. You can enable 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.

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.

Multi-Factor Authentication for Non-Browser-Based Applications

(Windows and macOS endpoints only) For sensitive, non-browser-based network resources (for example, financial applications or software development applications) that may require additional authentication,
the GlobalProtect app can notify and prompt the user to perform the timely, multi-factor authentication required to access these resources.

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 Certificate Selection by 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 Agent.
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 Supported GlobalProtect Authentication Methods or watch a video.

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, the 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. (Recommended) 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 does not support Remote Access VPN with Pre-Logon.
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 SAML identity provider. Refer to SAML 2.0 Authentication for more details.
   - 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 | (For Chromebooks only) Install the SAML SSO for Chrome Apps extension to enable SAML SSO for Chrome applications.

Launch the Chrome Web Store and install the SAML SSO for Chrome Apps extension.

STEP 5 | (For Chromebooks only) Configure SAML Single Sign-On for Chrome apps.

In order for GlobalProtect to support SAML SSO, the GlobalProtect application ID (nicidmbokaedpmoqgdbebhnchpegdcd) must be added to the whitelist configuration file for the SAML SSO for Chrome Apps extension.

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.

*K 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.*

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.

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 of FQDN of the **Kerberos Server**
   - **Port**

5. 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 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.

   - 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.
   - Import a **Kerberos Keytab** file. When prompted, **Browse** for the keytab file, and then click **OK**. 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.
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.

7. Click OK.

STEP 3 | 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.

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

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.

**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 Two-Factor Authentication).

Use the following workflow to create the client certificate and manually deploy it to an endpoint. For more information, see About 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, or sha384; sha512 is not supported with client certificates), 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.

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.

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 **The enrollment challenge password 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 (Mac), 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, or sha384.

     *Sha512 is not supported as a digest algorithm for client certificates on GlobalProtect endpoints.*

**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.
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.

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 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.

**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 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**.
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 porta 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.
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 Block Endpoint Access by adding the device to a block 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 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.
   -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.

- **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](image1)

![Figure 2: OTP Prompt on the GlobalProtect Status Panel](image2)

**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.

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.

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.
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.
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.
STEP 3 | Modify the strongSwan client’s IPsec configuration file (\texttt{ipsec.conf}) and the IPsec password file (\texttt{ipsec.secrets}) to use recommended settings.

The \texttt{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 \texttt{ipsec.conf} file to these recommended settings.

\begin{verbatim}
conn <connection name>
  keyexchange=ikev1
  authby=rsasig
  ike=aes-shal-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
\end{verbatim}

Modify the following items in the \texttt{ipsec.conf} file to these recommended settings.

\begin{verbatim}
:RSA
  <private key file> "<passphrase if used>"
\end{verbatim}

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 \texttt{config <name>} variable to name the tunnel configuration.

- Ubuntu:
  \begin{verbatim}
  ipsec start
  ipsec up <name>
  \end{verbatim}

- CentOS:
  \begin{verbatim}
  strongSwan start
  strongswan up <name>
  \end{verbatim}

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.

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:

```
ike_lifetime=20m
reauth=yes
rekey=yes
keylife=10m
rekeymargin=3m
rekeyfuzz=0%
```
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:

```plaintext
conn <connection name>
keyexchange=ikev1
ike-lifetime=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:

```plaintext
: 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:

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

- CentOS:

```plaintext
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:
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.
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:

ike lifet ime=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-shal-modp1024
esp=aes-shal
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 (MFA). 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. For more information, see Configure Multi-Factor Authentication.

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 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. For more information, refer to Configure Multi-Factor Authentication.

- 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 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 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 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 in Configure 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 on group 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 click Add.
2. Enter a Name for the configuration.
3. Select the Server Profile you just created.
4. Make sure the Enabled check box is selected.

STEP 3 | (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. Select the Group Include List tab.
   2. In the Available Groups list, select the groups you want to appear in policy rules and click the Add icon.

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. Select the Custom Group tab and click Add.
   2. 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).
   3. 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 4 | Commit your changes.

Click OK and Commit.
GlobalProtect Gateways Overview

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 enable HIP collection on the gateway for enhanced security policy granularity. For more information on enabling HIP checks, see Host Information.
- 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.

You can also configure GlobalProtect gateways on VM-Series firewalls deployed in the AWS cloud. By deploying the VM-Series firewall in the AWS cloud, you can quickly and easily deploy GlobalProtect gateways in any region without the expense or IT logistics that are typically required to set up this infrastructure. For details, see Use Case: VM-Series Firewalls as GlobalProtectGateways in AWS.
GlobalProtect Gateway Concepts

These sections provide information about gateway connection priority in a multiple gateway configuration and MIB support for GlobalProtect gateways.

- Types of Gateways on page 70
- Gateway Priority in a Multiple Gateway Configuration on page 70
- GlobalProtect MIB Support on page 71

Types of 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 next-generation firewall. You can run both a gateway and portal on the same firewall, or you can have multiple distributed gateways throughout your enterprise.

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.

- **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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Priority</th>
<th>Response Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>gw1</td>
<td>Highest</td>
<td>80 ms</td>
</tr>
<tr>
<td>gw2</td>
<td>High</td>
<td>25 ms</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Priority</th>
<th>Response Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>gw1</td>
<td>Highest</td>
<td>30 ms</td>
</tr>
<tr>
<td>gw2</td>
<td>High</td>
<td>25 ms</td>
</tr>
<tr>
<td>gw3</td>
<td>Medium</td>
<td>50 ms</td>
</tr>
</tbody>
</table>

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.

**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 Explore MIBs and Objects in the PAN-OS 8.1 Administrator’s Guide).

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.
<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>panGPGWUtilizationPct</td>
<td>Utilization (as a percentage) of the GlobalProtect gateway</td>
</tr>
<tr>
<td>panGPGWUtilizationMaxTunnels</td>
<td>Maximum number of tunnels allowed</td>
</tr>
<tr>
<td>panGPGWUtilizationActiveTunnels</td>
<td>Number of active tunnels</td>
</tr>
</tbody>
</table>

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.
Prerequisite Tasks for Configuring the GlobalProtect Gateway

Before you can configure the GlobalProtect gateway, you must have completed the following tasks:

- 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 Authentication.
Configure a GlobalProtect Gateway

After you have completed the prerequisite tasks, configure the GlobalProtect Gateways:

**STEP 1 | Add a gateway.**
1. Select `Network > GlobalProtect > Gateways`, and then **Add** a new gateway.
2. Enter a **Name** for the gateway. The gateway name should have no spaces and, as a best practice, should include the location or other descriptive information to help users and administrators identify the gateway.
3. **(Optional)** Select the virtual system to which this gateway belongs from the **Location** field.

**STEP 2 | Specify the network information that enables endpoints to connect to the gateway.**

If you have not created the network interface for the gateway, [Create Interfaces and Zones for GlobalProtect](#).

*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 [Best Practices for Securing Administrative Access](#) to ensure that you are securing administrative access to your firewalls in a way that will prevent successful attacks.*

1. Select the **Interface** that the endpoints will use for communication with the gateway.
2. Specify the **IP Address Type** and **IP Address** for the gateway web service:
   - You can 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 3 | Specify how the gateway authenticates users.**

If you have not created an SSL/TLS service profile for the gateway, [Deploy Server Certificates to the GlobalProtect Components](#).

If you have not set up the authentication profiles or certificate profiles, see [Authentication](#) for instructions.

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.

  *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:
  - Enter 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**).
• 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).
• To use two-factor authentication, select both an authentication profile and a certificate profile. The user must authenticate successfully using both methods in order to be granted access.

**STEP 4** | Enable tunneling, and then configure the tunnel parameters.

Tunnel parameters are required if you are configuring an external gateway. If you are configuring an internal gateway, they are optional.

- **If you want to force the use of SSL-VPN tunnel mode, clear the Enable IPSec check box.**
  - **By default, SSL-VPN is only used if the endpoint fails to establish an IPSec tunnel.**
- **Extended authentication (X-Auth) is only supported on IPSec tunnels.**
- **If you Enable X-Auth Support, GlobalProtect IPSec Crypto profiles are not applicable.**

*For more information on supported cryptographic algorithms, see Reference: GlobalProtect App Cryptographic Functions.*

1. On 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 in step 2 of Create Interfaces and Zones for GlobalProtect.
4. *(Optional)* Enter a **Max User** value to specify the maximum number of users 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 gateway. The default profile uses AES-128-CBC encryption and sha1 authentication.

You can also create a new IPSec crypto profile by selecting **New GlobalProtect IPSec Crypto** from the **GlobalProtect IPSec Crypto** drop-down, and then configuring the following settings:

1. Enter a **Name** to identify the profile.
2. **Add** the **Authentication** and **Encryption** algorithms that VPN peers can use to negotiate the keys for securing the data in the tunnel:
   - **Encryption**—If you are not certain of 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 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 applies 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 since 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**.

   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** on page 54 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 the 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 5 | (Optional)** Modify the default timeout settings for endpoints.

On the GlobalProtect Gateway Configuration dialog, select **Agent > Timeout Settings**, and then configure the following:

- **Modify the maximum Login Lifetime** for a single gateway login session (default login lifetime 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.
- **Modify the Inactivity Logout** period to specify the amount of time after which an inactive session is automatically logged out (default period is 3 hours). Users are logged out of GlobalProtect if the gateway does not receive a HIP check from the endpoint during the configured time period.
- **Modify the Disconnect on Idle** to specify the number of minutes after which idle users are logged out of GlobalProtect (default period is 180 minutes). Users are logged out of GlobalProtect if the GlobalProtect app has not routed traffic through the VPN tunnel within the configured time period. This setting applies to GlobalProtect apps that use the On-Demand connect method only.

**STEP 6 | (Tunnel Mode Only) (Optional)** Configure the global IP 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 only configure IP pools 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).

(Optional) You can use address objects—which allow you to group specific source or destination addresses—when configuring gateway IP address pools or access routes.

1. On the GlobalProtect Gateway Configuration dialog, select **Agent > Client IP Pool**.
2. **Add** the IP address subnet/range or address object used to assign IPv4 or IPv6 addresses to all endpoints that connect to the gateway. 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 7 | (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 be granted access.

*If you must immediately block access to a device whose cookie has not yet expired (for example, if the device is lost or stolen), you can immediately Block Endpoint Access by adding the device to a block 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 (Network > GlobalProtect > Gateways > <gateway-config> > Agent > Client Settings > <client-setting> > Authentication Override):
   - **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.
   - **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.
   - **Cookie Lifetime**—Specifies the hours, days, or weeks for which the cookie is valid (default is 24 hours). The range for hours is 1–72; weeks, 1–52; and days, 1–365. After the cookie expires, the user must re-enter the 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 decrypt the cookie (using the private certificate key).

**STEP 8 | (Tunnel Mode Only)** Configure the user (or user group) and the endpoint OS to which the agent configuration applies.

The gateway uses the user/user group settings to determine which configuration to deliver to the GlobalProtect apps that connect. If you have multiple configurations, you must make sure to order them properly. As soon as the gateway finds a match, it delivers the configuration. Therefore, more specific configurations must precede more general ones. See step 13 for instructions on ordering the list of agent configurations.
Network settings are not required in internal gateway configurations in non-tunnel mode since the GlobalProtect app uses the network settings assigned to the physical network adapter.

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 User/User Group settings (Network > GlobalProtect > Gateways > <gateway-config> > Agent > Client Settings > <client-setting> > User/User Group):
   - To deliver the configuration to apps running on a specific operating system, Add the OS to which this configuration applies. To deploy the configuration based on user/user group only, select the check box for Any.
   - To restrict this configuration to a specific user and/or user group, Add a Source User, and then select the user or user group from the drop-down. Repeat this step for each user/user group you want to add.

   Before you can restrict the configuration to specific groups, you must map users to groups as described in Enable Group Mapping.
   - To restrict the configuration to users who have not yet logged in to their systems, select pre-logon from the Source User drop-down.
   - To apply the configuration to any user regardless of login status (both pre-logon and logged in users), select any from the Source User drop-down.
4. Click OK to save the user/user group configuration.

**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 configure IP pools at 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 since apps use the network settings assigned to the physical network adapter.

(Optional) You can use address objects—which allow you to group specific source or destination addresses—when configuring gateway IP address pools or access routes.

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 (Network > GlobalProtect > Gateways > <gateway-config> > Agent > Client Settings > <client-setting> > IP Pools):
   - To specify the authentication server IP address pool for endpoints that require static IP addresses, select the Retrieve Framed-IP-Address attribute from authentication server check box, and then Add the subnet or IP address range to 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 or address object. 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 split tunnel settings based on the access route. These settings are assigned to the virtual network adapter on the endpoint when the GlobalProtect app establishes a tunnel with the gateway.

*When configuring access routes, keep in mind the following:*

- More specific access routes take precedence over less specific routes.
- Avoid specifying the same access route as both an include and exclude access route as this leads to a misconfiguration.

To route only some traffic—likely traffic destined for your LAN—to GlobalProtect, specify the destination subnets or address object (of type IP Netmask) that must be included or excluded from the tunnel. In this case, traffic that is not destined for a specified access route will be routed through the endpoint's physical adapter rather than through the virtual adapter (the tunnel).

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 access route-based Split Tunnel settings (Split Tunnel > Access Route):

   - To disable split tunneling, including direct access to local networks on Windows and macOS endpoints, enable No direct access to local network. If this option is enabled, users cannot send traffic to proxies or local resources while connected to GlobalProtect.

   - To define which destination subnets to route through the tunnel, enter the following routes under the Access Route tab:
     - (Optional) In the Includes section, Add the destination subnets or address object (of type IP Netmask) to route only certain traffic—likely traffic destined for your LAN—to GlobalProtect. These are the routes that the gateway pushes to the remote users’ endpoint, and thereby determines what traffic the users’ endpoint can send through the VPN connection. You can include IPv6 or IPv4 subnets.

     The number of access routes the firewall supports varies by PAN-OS release version:

     - PAN-OS 8.0.0 and PAN-OS 8.0.1—Up to 100 include access routes, and with GlobalProtect app 4.0.2 or a later release, up to 200 include access routes
     - PAN-OS 8.0.2 and later releases—Up to 100 include access routes, and with GlobalProtect app 4.0.2 or later releases, up to 1000 include access routes

     - (Optional) In the Excludes section, Add the destination subnets or address object (of type IP Netmask) that you want the app to exclude. These routes are sent through the endpoint’s physical adapter rather than the virtual adapter (the tunnel). Excluded routes should be more specific than the included routes; otherwise, you may exclude more traffic than you intended. You can exclude IPv6 or IPv4 subnets. The firewall supports up to 100 exclude access routes, or with GlobalProtect app 4.0.0 or later releases, up to 200 exclude access routes.
4. Click OK to save the split tunnel configuration.

Excluding routes is not supported on Android. Only IPv4 routes are supported on Chrome.

STEP 11 | (Tunnel Mode only) (Optional) For Windows and macOS endpoints, 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.

This feature is supported on Windows 7 Service Pack 2 and later releases and macOS 10.10 and later releases.

When you configure a split tunnel based on the destination domain, all traffic going to that specific domain and port (optional) is either sent through the tunnel for inspection and policy enforcement or sent directly to the physical adapter on the endpoint without inspection. This option enables you to configure a split tunnel for an entire domain without having to specify a destination IP address subnet, thereby extending the split tunnel capability to domains and applications with dynamic public IP addresses, such as SaaS and public cloud applications.

Both IPv4 and IPv6 traffic is 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. Disable the No direct access to local network option (Split Tunnel > Access Route). If enabled, this setting disables split tunneling on Windows, Linux, and macOS networks.
4. (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 *.office365.com to allow all Office 365 traffic to go through the VPN tunnel.
5. (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 *.engadget.com to exclude all Engadget traffic from the VPN tunnel.
6. Click OK to save the split tunnel settings.

STEP 12 | (Tunnel Mode only) (Optional) For Windows and macOS endpoints, configure split tunnel settings based on the application process name. These settings are assigned to the virtual network adapter on the endpoint when the GlobalProtect app establishes a tunnel with the gateway.

This feature is supported on Windows 7 Service Pack 2 and later releases and macOS 10.10 and later releases.

When you configure a split tunnel based on the application process name, all traffic for that application is either sent through the tunnel for inspection and policy enforcement or sent directly to the physical adapter on the endpoint without inspection. This option enables you to configure a split tunnel without having to specify a destination IP address subnet, thereby extending the split tunnel capability to applications with dynamic public IP addresses, such as SaaS and public cloud applications.

Both IPv4 and IPv6 traffic is 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. Disable the **No direct access to local network** option (**Split Tunnel > Access Route**). If enabled, this setting disables split tunneling on Windows, Linux, and macOS networks.
4. **(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 `/Application/Safari.app/Contents/MacOS/Safari` to allow all Safari-based traffic to go through the VPN tunnel on macOS endpoints.
5. **(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.
6. Click **OK** to save the split tunnel settings.

**STEP 13** | *(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 have 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 on the list of configurations, select the configuration and click **Move Up**.
- To move a gateway configuration down on the list of configurations, select the configuration and click **Move Down**.

**STEP 14** | *(Tunnel Mode Only)* Specify the network configuration settings for the endpoints.

*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.*

On the GlobalProtect Gateway Configuration dialog, select **Agent > Network Services**, and then configure the network configuration settings in one of the following ways:

- 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 received by the DHCP client. You can also enable the check box 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 15** | *(Tunnel Mode Only)* For Windows and macOS endpoints, exclude HTTP/HTTPS video streaming traffic from the VPN tunnel.

*This feature is supported on Windows 7 Service Pack 2 and later releases and macOS 10.10 and later releases.*
By excluding lower risk video streaming traffic (such as YouTube and Netflix) from the VPN tunnel, you can decrease bandwidth consumption on the gateway.

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

The App-ID functionality on the firewall identifies the video stream before traffic can be split tunneled.

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. In this case, ensure that the IP pools used to assign IP addresses to the virtual network adapters on these endpoints do not include any IPv6 addresses (Network > GlobalProtect > Gateways > Agent > Client IP Pool or Client Settings > IP Pools).

If you exclude video streaming traffic from the VPN tunnel (Network > GlobalProtect > Gateways > <gateway-config> > Agent > Video Traffic), do not include web browser applications, such as Firefox or Chrome, in the VPN tunnel (Network > GlobalProtect > Gateways > <gateway-config> > Agent > Client Settings > <client-setting> > Split Tunnel > Domain and Application). 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, use application-based split tunneling (Network > GlobalProtect > Gateways > <gateway-config> > Agent > Client Settings > <client-setting-config> > Split Tunnel > Domain and Application).

1. On 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 select specific video streaming applications to exclude 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 application(s) that you want to exclude. For example, click the add icon for directv to exclude DIRECTV video streaming traffic from the VPN tunnel.

4. (Optional) 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 that contains some of the most popular video streaming applications. For example, select youtube-streaming from the Applications drop-down to exclude all YouTube-based video streaming traffic from the VPN tunnel.
STEP 16 | *(Optional)* Define the notification messages end-users see when a security rule with a host information profile (HIP) is enforced.

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

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 it is not matched, select **Match Message** or **Not Match Message**, and then **Enable** notifications. In some cases, you might want to create messages for both a match and a non-match, 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 in the **Template** text box, and then click **OK**.
   - Repeat these steps for each message you want to define.

STEP 17 | Save the gateway configuration.

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

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. For more details on supported versions, see What OS Versions are Supported with GlobalProtect?

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. 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. Refer to GlobalProtect Clientless VPN.
Prerequisite Tasks for Configuring the GlobalProtect Portal

Before you can configure the GlobalProtect portal, you must complete the following tasks:

☐ 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 Authentication.

☐ Configure a GlobalProtect Gateway and understand Gateway Priority in a Multiple Gateway Configuration.
Set Up Access to the GlobalProtect Portal

After you have completed the Prerequisite Tasks for Configuring the GlobalProtect Portal, configure the GlobalProtect portal as follows:

STEP 1 | Add the portal.
1. Select Network > GlobalProtect > Portals, and then Add a portal.
2. Enter a Name for the portal. The name cannot contain spaces.
3. (Optional) Select the virtual system to which this portal belongs from the Location field.

STEP 2 | 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 Best Practices for Securing Administrative Access to ensure that you are securing administrative access to your firewalls in a way that will prevent successful attacks.

1. Select an Interface.
2. 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.
3. Select an SSL/TLS Service Profile.

STEP 3 | 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.

In the Appearance area of the GlobalProtect Portal Configuration dialog (Network > GlobalProtect > Portals > <portal-config> > General), configure 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 4 | Specify how the portal authenticates the users.

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

Configure any of the following portal Authentication settings (Network > GlobalProtect > Portals > <portal-config> > Authentication):

- 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, select the corresponding Certificate Profile. A valid client certificate must be pre-deployed on all endpoints.

**STEP 5 |** 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 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. By default, the configuration applies to all endpoints. You can apply the configuration to endpoints running a specific OS or to endpoints that access the portal from a web Browser with the intent of downloading the GlobalProtect app or creating a new client authentication configuration specifically for GlobalProtect Clientless VPN.
- Select or add an Authentication Profile for authenticating endpoints that try to access the gateway.
- (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).

**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.
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.

1. **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 portal **Authentication** settings: (Network > GlobalProtect > Portals > portal-config > Agent > agent-config > Authentication):

- 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 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, or **No** to never save credentials.

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).

### STEP 4

<table>
<thead>
<tr>
<th>If the GlobalProtect endpoint does not require tunnel connections when it is on the internal network, configure internal host detection.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enable <strong>Internal Host Detection</strong> ([IPv4 or IPv6](Network &gt; GlobalProtect &gt; Portals &gt; &lt;portal-config&gt; &gt; Agent &gt; &lt;agent-config&gt; &gt; Internal)).</td>
</tr>
<tr>
<td>2. Enter the <strong>IP Address</strong> 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](Network &gt; GlobalProtect &gt; Portals &gt; &lt;portal-config&gt; &gt; Agent &gt; &lt;agent-config&gt; &gt; Internal) or [IPv6](Network &gt; GlobalProtect &gt; Portals &gt; &lt;portal-config&gt; &gt; Agent &gt; &lt;agent-config&gt; &gt; Internal)). For example, 172.16.1.0 for IPv4 or 21DA:D3:0:2F3b for IPv6.</td>
</tr>
<tr>
<td>3. Enter the DNS <strong>Hostname</strong> 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.</td>
</tr>
</tbody>
</table>

### STEP 5

<table>
<thead>
<tr>
<th>Set up access to a third-party mobile endpoint management system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>2. Specify the <strong>Enrollment Port</strong> 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).</td>
</tr>
</tbody>
</table>

### STEP 6

<table>
<thead>
<tr>
<th>Configure the user or user group and the OS to which the agent configuration applies.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The portal uses the user/user group settings 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.</td>
</tr>
<tr>
<td>Specify the <strong>User/User Group</strong> and/or operating systems to which this agent configuration should apply ([Network](Network &gt; GlobalProtect &gt; Portals &gt; &lt;portal-config&gt; &gt; Agent &gt; &lt;agent-config&gt; &gt; User/User Group)):</td>
</tr>
<tr>
<td>1. <strong>To deliver this configuration to apps running on a specific operating system, Add</strong> and select the OS ([Android](Network &gt; GlobalProtect &gt; Portals &gt; &lt;portal-config&gt; &gt; Agent &gt; &lt;agent-config&gt; &gt; User/User Group), [Chrome](Network &gt; GlobalProtect &gt; Portals &gt; &lt;portal-config&gt; &gt; Agent &gt; &lt;agent-config&gt; &gt; User/User Group), [iOS](Network &gt; GlobalProtect &gt; Portals &gt; &lt;portal-config&gt; &gt; Agent &gt; &lt;agent-config&gt; &gt; User/User Group), [Linux](Network &gt; GlobalProtect &gt; Portals &gt; &lt;portal-config&gt; &gt; Agent &gt; &lt;agent-config&gt; &gt; User/User Group), [Mac](Network &gt; GlobalProtect &gt; Portals &gt; &lt;portal-config&gt; &gt; Agent &gt; &lt;agent-config&gt; &gt; User/User Group), [Windows](Network &gt; GlobalProtect &gt; Portals &gt; &lt;portal-config&gt; &gt; Agent &gt; &lt;agent-config&gt; &gt; User/User Group), or [WindowsUWP](Network &gt; GlobalProtect &gt; Portals &gt; &lt;portal-config&gt; &gt; Agent &gt; &lt;agent-config&gt; &gt; User/User Group)) to which this configuration applies.</td>
</tr>
<tr>
<td>Or <strong>leave the value in this section set to Any</strong> to deploy the configuration based on user/group only.</td>
</tr>
<tr>
<td>2. <strong>To restrict this configuration to a specific user and/or group,</strong> Add and select the <strong>User/User Group</strong> you want to receive this configuration. Repeat this step for each user/group you want to add.</td>
</tr>
<tr>
<td><strong>Before you can restrict the configuration to specific groups, you must map users to groups as described in Enable Group Mapping.</strong></td>
</tr>
<tr>
<td>• <strong>To restrict the configuration to users who have not yet logged in to their endpoints,</strong> select <strong>pre-logon</strong> from the <strong>User/User Group</strong> drop-down.</td>
</tr>
</tbody>
</table>
To apply 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.

**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. **Add** the External Gateways to which users can connect (Network > GlobalProtect > Portals > <portal-config> > Agent > <agent-config> > External).
2. 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.
3. 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.
4. **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.
5. 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.
6. 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. **Add** the Internal Gateways to which users can connect (Network > GlobalProtect > Portals > <portal-config> > Agent > <agent-config> > Internal).
2. 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.
3. 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.
4. **(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.
5. Click **OK** to save your changes.
6. (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.

7. (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 (Network > GlobalProtect > Portals > <portal-config> > Agent > <agent-config> > App). 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 HIP categories from collection.

This step only applies 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.

1. Enable the GlobalProtect app to Collect HIP Data (Network > GlobalProtect > Portals > <portal-config> > Agent > <agent-config> > Data Collection).
2. 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.
3. Select Custom Checks to define any custom data you want to collect from hosts running this agent configuration, and add the category and vendor. For more details, see Host Information.

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 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.

Additional settings that are available only through the Windows Registry or Windows Installer (Msiexec) enable you to:

- 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.

For more information, see Customizable App Settings.

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 Mac 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.

STEP 3 | Specify whether to enforce GlobalProtect connections for network access.

*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.*

- To permit traffic required to establish a connection with a captive portal, specify a **Captive Portal Exception Timeout**. The user must authenticate with the portal before the timeout expires. To provide additional instructions, configure a **Captive Portal Detection Message**.
STEP 4 | 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 only) Set **Use Single Sign-On** to **No** to prevent GlobalProtect from using the Windows login credentials to automatically authenticate the user upon Active Directory login.
- 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 a later version.

- Configure an **Automatic Restoration of VPN Connection Timeout** to specify the action GlobalProtect takes when the tunnel is disconnected. Set this option to **Yes** to allow GlobalProtect to attempt to reestablish the connection after the tunnel is disconnected. Set this option to **No** to prevent GlobalProtect from attempting to reconnect after the tunnel is disconnected. 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).

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 5 | 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**. The advanced view is enabled by default, which allows users to perform tasks (such as changing saved passwords) and view detailed statistical, host, and troubleshooting information.
• 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 6 | 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.

STEP 7 | 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.

If the GlobalProtect system tray icon is not visible, users cannot disable the GlobalProtect app. See step 5 for more details.

• To prevent users with the user-logon connect method from disabling GlobalProtect, set Allow User to Disable GlobalProtect to Disallow.

• To allow users to disable GlobalProtect only if they provide a passcode, set Allow User to Disable GlobalProtect 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.

![Generate Ticket](image)

- 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 8** | 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 the PAN-OS 7.1 New Features Guide.

• 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 9** 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). 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 10** *(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.

This feature requires Content Release version 731 or later releases and GlobalProtect app 4.0.3 and later releases.

To configure DNS settings for GlobalProtect app 4.0.2 and earlier releases, use the Update DNS Settings at Connect option.

- **Update DNS Settings at Connect**—Select Yes to enable the Windows endpoint to resolve all DNS queries with the DNS servers you configure for the gateway instead of the DNS servers set for the physical adapter on the endpoint. When you enable this option, GlobalProtect strictly enforces the gateway DNS settings and overrides the static settings for all physical adapters. This is useful when a Windows endpoint fails to resolve a DNS query sent to the DNS server configured on the physical adapter instead of on the GlobalProtect tunnel adapter. Select No (default) 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.

This feature is deprecated in 4.0.3 and later releases. To configure DNS resolution settings for GlobalProtect agent 4.0.3 and later releases, use the Resolve All FQDNs Using DNS Servers Assigned by the Tunnel (Windows Only) option.

- **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 11** *(Windows only)* Configure the GlobalProtect app for Windows endpoints to Detect Proxy for Each Connection.

Consider the following GlobalProtect app behaviors when a proxy is configured on Windows and macOS endpoints:

**Table 1: GlobalProtect App Behaviors With Proxies**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Traffic to the portal and gateways goes through the proxy.</td>
<td>Traffic to the portal and gateways goes through the proxy.</td>
<td>Traffic to the portal and gateways goes through the proxy.</td>
<td>Traffic to the portal and gateways does not go through the proxy.</td>
</tr>
<tr>
<td></td>
<td>Post-connection traffic does not</td>
<td>Post-connection traffic does not</td>
<td>Post-connection traffic does not</td>
<td>Post-connection traffic does not</td>
</tr>
</tbody>
</table>
### Operating System (OS)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>macOS</td>
<td>go through the proxy.</td>
<td>go through the proxy.</td>
<td>go through the proxy.</td>
<td>go through the proxy.</td>
</tr>
</tbody>
</table>

- Traffic to the portal and gateways goes through the proxy.
- Traffic to the portal and gateways goes through the proxy.
- Traffic to the portal and gateways goes through the proxy.
- Traffic to the portal and gateways does not go through the proxy.
- Post-connection traffic goes through the proxy.
- Post-connection traffic goes through the proxy.
- Post-connection traffic goes through the proxy.
- Post-connection traffic does not go through the proxy.

• 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 12** | 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 13** | 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 14 | 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 5 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 3.1.3 agent connecting to a GlobalProtect 3.1.1 portal is not upgraded.

STEP 15 | 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 16 | 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 default browser on Windows, macOS, and Chrome OS endpoints, or within the GlobalProtect app on mobile endpoints. 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 17 | 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, 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 Default predefined page and click Export.

STEP 2 | Edit the exported page.
1. Use the HTML text editor of your choice to edit the page.
2. If you want to edit the logo image that is displayed, host the new logo image on a web server that is accessible from the remote GlobalProtect endpoints. For example, edit the following line in the HTML to point to the new logo image:

   `<img src="http://cdn.slidesharecdn.com/ Acme-logo-96x96.jpg?1382722588"/>

3. Save the edited page with a new filename. Make sure that the page retains its UTF-8 encoding.

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 and App Help Page:
  1. Select Network > GlobalProtect > Portals.
  2. Select the portal to which you want to add the login 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:
  4. Select Network > GlobalProtect > Portals.
5. Select the portal to which you want to add the welcome page.
6. On the Agent tab, select the agent configuration to which you want to add the welcome page.
7. On the App tab, select the new page from the Welcome Page drop-down.
8. 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 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.
GlobalProtect Apps

- Deploy the GlobalProtect App Software
- Define the GlobalProtect Agent Configurations
- Customize the GlobalProtect App
- Deploy Agent Settings Transparently
Deploy the GlobalProtect App Software

In order to connect to GlobalProtect™, an endpoint must be running the GlobalProtect app software. The software deployment method depends on the type of endpoint as follows:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Deployment Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mac and Windows endpoints</strong></td>
<td>There are several options you can use to distribute and install the software on Mac and Windows endpoints:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Directly from the portal</strong>—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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>From a web server</strong>—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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Transparently from the command line</strong>—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 Mac endpoints, by configuring settings in the Mac plist. See Deploy App Settings Transparently.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Using group policy rules</strong>—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 <a href="http://support.microsoft.com/kb/816102">http://support.microsoft.com/kb/816102</a> for more information on how to use Group Policy to automatically distribute programs to endpoints or users.</td>
</tr>
<tr>
<td></td>
<td>• <strong>From a mobile endpoint management system</strong>—If you use a mobile management system, such as an MDM or EMM, to manage your mobile endpoints, you can use the system to deploy and configure the GlobalProtect app. See Mobile Endpoint Management.</td>
</tr>
<tr>
<td><strong>Windows 10 phone and Windows 10 UWP</strong></td>
<td>• <strong>From a mobile endpoint management system</strong>—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 Endpoint Management.</td>
</tr>
<tr>
<td></td>
<td>• <strong>From the Microsoft Store</strong>—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.</td>
</tr>
<tr>
<td><strong>iOS and Android endpoints</strong></td>
<td>• <strong>From a mobile endpoint management system</strong>—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 Endpoint Management.</td>
</tr>
<tr>
<td>Platform</td>
<td>Deployment Options</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------</td>
</tr>
<tr>
<td>• <strong>From an app store</strong>—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.</td>
<td></td>
</tr>
</tbody>
</table>

| Chromebooks | • **From the Chromebook Management Console**—If you use the Chromebook Management Console to manage Chromebooks in your organization, you can use the system to deploy and configure the GlobalProtect app. See Deploy the GlobalProtect App Using the Chromebook Management Console. |
| • **From the Chrome Web Store**—The end user can also download and install the GlobalProtect app for Chrome OS directly from the Chrome Web Store. For instructions on how to download and test the GlobalProtect app installation, see Install the GlobalProtect App from the Chrome Web Store. |

| 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 RHEL repositories). 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.

**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 app 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 must have a valid Palo Alto Networks account to log in to and download software from the Software Updates page. If you cannot log in and need assistance, go to https://www.paloaltonetworks.com/support/tabs/overview.html.

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.

You must have a valid Palo Alto Networks account to log in to and download software from the Software Updates page. If you cannot log in and need assistance, go to: https://www.paloaltonetworks.com/support/tabs/overview.html

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, manually Download the latest app software image from the Palo Alto Networks Software Updates support site. 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, go to the Palo Alto Networks Software Updates site, and then Download the file to your computer.

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>`

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, \url{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), or click **Browse** to select a new location and then click **Next** twice.
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—Google Play
- Windows 10 phones and Windows 10 UWP endpoints—Microsoft Store
- Chromebooks—For details on installing the GlobalProtect app for Chrome OS, see Download and Install the GlobalProtect App for Chrome OS.

This workflow describes how to install the GlobalProtect app directly on the mobile endpoint. For instructions on how to deploy the GlobalProtect app from AirWatch, see Deploy the GlobalProtect Mobile App Using AirWatch.

**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.

**Download and Install the GlobalProtect App for Chrome OS**

The GlobalProtect app for Chrome OS provides a simple way to extend the enterprise security policies out to Chromebooks. As with other remote endpoints running the GlobalProtect app, the GlobalProtect app for Chrome OS provides secure access to your corporate network over an IPsec or SSL VPN tunnel. After the user initiates a connection, the app connects to the gateway that is closest to the end user’s current location. In addition, traffic to and from the Chromebook is automatically subject to the same security policy
enforcement as other endpoints on your corporate network. The app also collects information about the host configuration and can use this information for enhanced HIP-based security policy enforcement.

Use the following procedures to install and test the GlobalProtect app for Chrome OS.

- Install the GlobalProtect App from the Chrome Web Store
- Deploy the GlobalProtect App Using the Chromebook Management Console
- Test the GlobalProtect App for Chrome OS

**Install the GlobalProtect App from the Chrome Web Store**

You can install the GlobalProtect app on a Chromebook by downloading the app from the Chrome Web Store. As an alternative, you can Deploy the GlobalProtect App Using the Chromebook Management Console.

**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 who are responsible for administering the firewall.

1. Select **Network > GlobalProtect > Portals**
2. Select an existing portal configuration or **Add** a new one.
3. On the **Agent** tab, select an existing agent 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** that will test the app.
5. Select the **OS** you are testing (in this example, select **Chrome**), and then click **OK**.
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 in the list than the more generic configurations you have created.
7. Click **OK**, and then **Commit** the changes.

**STEP 2** Install the GlobalProtect app for Chrome OS.

You can also force-install the app on managed Chromebooks using the Chromebook Management Console. See Deploy the GlobalProtect App Using the Chromebook Management Console.

1. From your Chromebook, search for the app in the Chrome Web Store or go directly to the GlobalProtect app page.
2. Click **Add to Chrome**, and then follow the prompts to download and install the app.

**STEP 3** Launch the app.

After the GlobalProtect app is installed successfully, the Chrome App Launcher displays the GlobalProtect app icon in the list of apps. Click the icon to launch the app.

**STEP 4** Configure the portal.

1. When prompted, enter the IP address or FQDN of the **Portal**. The portal address should not include the **https://**.
2. Click **Add Connection** to add the GlobalProtect configuration.

The home screen displays after the GlobalProtect app adds the GlobalProtect configuration to the Internet connection settings of your Chromebook but does not initiate a connection.

**STEP 5** Test the GlobalProtect App for Chrome OS.
Deploy the GlobalProtect App Using the Google Admin Console

The Google Admin console enables you to manage Chromebook settings and apps from a central, web-based location. From the console, you can deploy the GlobalProtect app and customize VPN settings.

Use the following workflow to manage policies and settings for the GlobalProtect app for Chrome OS:

**STEP 1** | View the user settings for the GlobalProtect app.

1. From the Google Admin console, select **Device management > Chrome management > App management**.

   The console displays the list of apps configured in all organization (org) units in your domain and also indicates the status of each app. Click an app **Status** to display the org units to which that status is applied.

2. Select the GlobalProtect app and then select **User settings**.

   If the app is not present, **SEARCH** for GlobalProtect in the Chrome Web Store.

![User settings](image)

**STEP 2** | Configure policies and settings for everyone in an org unit.

1. Select the org unit for which you want to configure settings, and then configure any of the following options:

   Selecting the top-level org unit applies settings to everyone in that unit; selecting a child org unit applies settings only to users within that child org unit.

   - **Allow installation**—Allows users to install this app from the Chrome Web Store. By default, an org unit inherits the settings of its parent organization. To override the default settings, select **Inherit**, which toggles the **Override** setting.
   - **Force installation**—Installs the app automatically and prevents users from removing it.
   - **Pin to taskbar**—If the app is installed, pins the app to the taskbar (in Chrome OS only).
   - **Add to Chrome Web Store collection**—Recommends this app to your users in the Chrome Web Store.

2. If you have not already done so, create a JSON format text file that uses the following syntax and includes the FQDN or IP address of your GlobalProtect portal:

   ```
   {
   "PortalAddress": {
   "Value": "192.0.2.191"
   }
   ```
3. On the User settings page, select UPLOAD CONFIGURATION FILE and then Browse for the GlobalProtect settings file.

4. SAVE your changes. Settings typically take effect within minutes, but it may take up to an hour to propagate through your organization.

STEP 3 | Test the connection.

After Google Admin console successfully deploys the app, Test the GlobalProtect App for Chrome OS

Test the GlobalProtect App for Chrome OS

Use the GlobalProtect app to view the connection status and information about the app, collect logs, or reset the GlobalProtect connection settings. After you install and configure the app, it is not necessary to open the app to establish a connection. Instead, you can connect by selecting the portal from the VPN settings on the Chromebook.

STEP 1 | Log in to GlobalProtect.

1. Click the status area at the bottom right corner of the Chromebook.

2. Select VPN disconnected, and then select the portal that you entered when configuring the GlobalProtect VPN settings.

   To view VPN settings before connecting, select the portal from Settings > Private network, and then click Connect.

3. Enter the Username and Password for the portal, and then click Connect. Repeat this step for the gateway. If authentication is successful, GlobalProtect connects you to your corporate network, and the GlobalProtect welcome page appears (if configured).

STEP 2 | View the connection status.

When the app is connected, the status area displays the VPN icon along the bottom of the Wi-Fi icon :

- To view the portal to which you are connected, click the status area.
To view additional information about the connection, including the gateway to which you are connected, launch the GlobalProtect app. The main page displays the connection information and any applicable errors or warnings.
Deploy App Settings Transparently

As an alternative to deploying app settings from the portal configuration, you can define them directly from the Windows Registry, global macOS plist, or—on Windows endpoints only—using the Windows Installer (Msiexec). The benefit is that it enables deployment of GlobalProtect app settings to endpoints prior to their first connection to the GlobalProtect portal.

Settings defined in the portal configuration always override settings defined in the Windows Registry or macOS plist. If you define settings in the registry or plist, 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 and macOS endpoints:

- Customizable App Settings
- Deploy App Settings to Windows Endpoints
- Deploy App Settings to macOS Endpoints

In addition to using the Windows Registry and macOS plist 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 (HKEY_LOCAL_MACHINE \SOFTWARE\Palo Alto Networks\GlobalProtect). To Deploy App Settings to macOS Endpoints you define entries in the PanSetup dictionary of the macOS plist (/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist). 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 additional settings include: can-prompt-user-credential, wrap-cp-guid, and filter-non-gpcp.

- 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 and macOS plist to customize the display of the GlobalProtect app.

### Table 2: Customizable App Settings

<table>
<thead>
<tr>
<th>Portal Agent Configuration</th>
<th>Windows Registry/ macOS Plist</th>
<th>Msiexec Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Advanced View</td>
<td>enable-advanced-view yes</td>
<td>ENABLEADVANCEDVIEW=&quot;yes &quot; no&quot;</td>
<td>yes</td>
</tr>
<tr>
<td>Display GlobalProtect Icon</td>
<td>show-agent-icon yes</td>
<td>SHOWAGENTICON=&quot;yes</td>
<td>no&quot;</td>
</tr>
<tr>
<td>Enable Rediscover Network Option</td>
<td>rediscover-network yes</td>
<td>REDISCOVERNETWORK=&quot;yes</td>
<td>no&quot;</td>
</tr>
<tr>
<td>Enable Resubmit Host Profile Option</td>
<td>resubmit-host-info yes</td>
<td>RESUBMITTEDHOSTINFO=&quot;yes</td>
<td>no&quot;</td>
</tr>
<tr>
<td>Show System Tray Notifications</td>
<td>show-system-tray-notifications yes</td>
<td>SHOWSYSTEMTRAYNOTIFICATIONS=&quot;yes</td>
<td>no&quot;</td>
</tr>
</tbody>
</table>

## 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.

### Table 3: Customizable User Behavior Options

<table>
<thead>
<tr>
<th>Portal Agent Configuration</th>
<th>Windows Registry/ macOS Plist</th>
<th>Msiexec Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow User to Change Portal Address</td>
<td>can-change-portal yes</td>
<td>CANCHANGEPORTAL=&quot;yes</td>
<td>no&quot;</td>
</tr>
<tr>
<td>Allow User to Dismiss Welcome Page</td>
<td>enable-hide-welcome-page yes</td>
<td>ENABLEHIDEWELCOMEPAGE=&quot;yes</td>
<td>no&quot;</td>
</tr>
<tr>
<td>Allow User to Continue with Invalid Portal Server Certificate</td>
<td>can-continue-if-portal-cert-invalid yes</td>
<td>CANCONTINUEIFPORTALCERTINVALID=&quot;yes</td>
<td>no&quot;</td>
</tr>
<tr>
<td>Allow User to Disable GlobalProtect App</td>
<td>disable-allowed yes</td>
<td>DISABLEALLOWED=&quot;yes</td>
<td>no&quot;</td>
</tr>
</tbody>
</table>
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.

Table 4: Table: Customizable App Behavior Options

<table>
<thead>
<tr>
<th>Portal Agent Configuration</th>
<th>Windows Registry/macOS Plist</th>
<th>Msiexec Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect Method</td>
<td>connect-method on-demand</td>
<td>CONNECTMETHOD=&quot;on-demand</td>
<td>user-logon</td>
</tr>
<tr>
<td></td>
<td>pre-logon</td>
<td>pre-logon</td>
<td>user-logon”</td>
</tr>
<tr>
<td>GlobalProtect App Config</td>
<td>refresh-config-interval &lt;hours&gt;</td>
<td>REFRESHCONFIGINTERVAL= ”&lt;hours&gt;”</td>
<td>24</td>
</tr>
</tbody>
</table>

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.

Not in portal

The Allow user to save password setting is deprecated 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.
<table>
<thead>
<tr>
<th>Portal Agent Configuration</th>
<th>Windows Registry/macOS Plist</th>
<th>Msiexec Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh Interval (hours)</td>
<td>flushdns yes</td>
<td>no</td>
<td>FLUSHDNS=&quot;yes</td>
</tr>
<tr>
<td>Update DNS Settings at Connect (Windows Only)</td>
<td>wscautodetect yes</td>
<td>no</td>
<td>WSCAUTODETECT=&quot;yes</td>
</tr>
<tr>
<td>Detect Proxy for Each Connection (Windows Only)</td>
<td>ProxyMultipleAuto Detection yes</td>
<td>no</td>
<td>ProxyMultipleAuto Detection=&quot;yes</td>
</tr>
<tr>
<td>Clear Single Sign-On Credentials on Logout (Windows Only)</td>
<td>LogoutRemoveSSO yes</td>
<td>no</td>
<td>LogoutRemoveSSO=&quot;yes</td>
</tr>
<tr>
<td>Use Default Authentication on Kerberos Authentication Failure (Windows Only)</td>
<td>krb-auth-fail-fallback yes</td>
<td>no</td>
<td>KRBAUTHFAILFALLBACK=&quot;yes</td>
</tr>
<tr>
<td>Custom Password Expiration Message (LDAP Authentication Only)</td>
<td>PasswordExpireMessage &lt;message&gt;</td>
<td></td>
<td>PasswordExpireMessage &quot;&lt;message&gt;&quot;</td>
</tr>
<tr>
<td>Portal Connection Timeout (sec)</td>
<td>PortalTimeout &lt;portaltimeout&gt;</td>
<td>PORTALTIMEOUT=&quot;&lt;portaltimeout&gt;&quot;</td>
<td>5</td>
</tr>
<tr>
<td>TCP Connection Timeout (sec)</td>
<td>ConnectTimeout &lt;connecttimeout&gt;</td>
<td>CONNECTTIMEOUT=&quot;&lt;connecttimeout&gt;&quot;</td>
<td>5</td>
</tr>
<tr>
<td>TCP Receive Timeout (sec)</td>
<td>ReceiveTimeout &lt;receivetimeout&gt;</td>
<td>RECEIVETIMEOUT=&quot;&lt;receivetimeout&gt;&quot;</td>
<td>30</td>
</tr>
<tr>
<td>Client Certificate Store Lookup</td>
<td>certificate-store-lookup user</td>
<td>machine</td>
<td>user and machine</td>
</tr>
<tr>
<td>Portal Agent Configuration</td>
<td>Windows Registry/macOS Plist</td>
<td>Msiexec Parameter</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>------------------------------------------------------------------</td>
<td>------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>SCEP Certificate Renewal Period (days)</td>
<td>scep-certificate-renewal-period &lt;renewalPeriod&gt;</td>
<td>n/a</td>
<td>7</td>
</tr>
<tr>
<td>Maximum Internal Gateway Connection Attempts</td>
<td>max-internal-gateway-connection-attempts &lt;maxValue&gt;</td>
<td>MIGCA=&quot;&lt;maxValue&gt;&quot;</td>
<td>0</td>
</tr>
<tr>
<td>Extended Key Usage OID for Client Certificate</td>
<td>ext-key-usage-oid-for-client-cert &lt;oidValue&gt;</td>
<td>EXTCERTOID=&quot;&lt;oidValue&gt;&quot;</td>
<td>n/a</td>
</tr>
<tr>
<td>User Switch Tunnel Rename Timeout (sec)</td>
<td>user-switch-tunnel-rename-timeout &lt;renameTimeout&gt;</td>
<td>n/a</td>
<td>0</td>
</tr>
<tr>
<td>Use Single Sign-On (Windows Only)</td>
<td>use-sso yes</td>
<td>no</td>
<td>USESSO=&quot;yes</td>
</tr>
<tr>
<td>Not in portal</td>
<td>portal &lt;IPaddress&gt;</td>
<td>PORTAL=&quot;&lt;IPaddress&gt;&quot;</td>
<td>n/a</td>
</tr>
<tr>
<td>Not in portal</td>
<td>prelogon 1</td>
<td>PRELOGON=&quot;1&quot;</td>
<td>1</td>
</tr>
<tr>
<td>Windows only/Not in portal</td>
<td>can-prompt-user-credential yes</td>
<td>no</td>
<td>CANPROMPTUSERCRENDENTIAL=&quot;yes</td>
</tr>
<tr>
<td>Portal Agent Configuration</td>
<td>Windows Registry/macOS Plist</td>
<td>Msiexec Parameter</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------</td>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>the user for credentials if SSO fails.</td>
<td>wrap-cp-guid {third party credential provider guid}</td>
<td>WRAPCPGUID=&quot;{guid_value}&quot; FILTERNONGPCP=&quot;yes</td>
<td>no&quot;</td>
</tr>
<tr>
<td>Windows only/ Not in portal</td>
<td>filter-non-gpcp no</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Windows only/ Not in portal</td>
<td>reserved-ipv4 &lt;reserved-ipv4&gt; reserved-ipv6 &lt;reserved-ipv6&gt;</td>
<td>RESERVEDIPV4=&quot;&lt;reserved-ipv4&gt;&quot; RESERVEDIPV6=&quot;&lt;reserved-ipv6&gt;&quot;</td>
<td>n/a</td>
</tr>
</tbody>
</table>

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.

### Table: Customizable Script Deployment Options

<table>
<thead>
<tr>
<th>Portal Agent Configuration</th>
<th>Windows Registry/macOS Plist</th>
<th>Msiexec Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute the script specified in the command setting (including any parameters passed to the script).</td>
<td>command <code>&lt;parameter1&gt;</code> <code>&lt;parameter2&gt;</code> [...]</td>
<td>PREVPNCONNECTCOMMAND= &quot;&lt;parameter1&gt; <code>&lt;parameter2&gt;</code> [...]&quot;</td>
<td>n/a</td>
</tr>
<tr>
<td>Environmental variables are supported.</td>
<td>Windows example: command <code>%userprofile%\vpn_script.bat c: test_user</code></td>
<td>POSTVPNCONNECTCOMMAND= &quot;&lt;parameter1&gt; <code>&lt;parameter2&gt;</code> [...]&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>macOS example: command <code>$HOME/vpn_script.sh / Users/test_user test_user</code></td>
<td>PREVPNDISCONNECTCOMMAND= &quot;&lt;parameter1&gt; <code>&lt;parameter2&gt;</code> [...]&quot;</td>
<td></td>
</tr>
<tr>
<td>Specifying the full path in commands.</td>
<td>context admin</td>
<td>POSTVPNCONNECTCONTEXT= &quot;admin</td>
<td>user&quot;</td>
</tr>
<tr>
<td></td>
<td>timeout <code>&lt;value&gt;</code></td>
<td>PREVPNDISCONNECTCONTEXT= &quot;admin</td>
<td>user&quot;</td>
</tr>
<tr>
<td>(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).</td>
<td>timeout <code>&lt;value&gt;</code></td>
<td>PREVPNCONNECTTIMEOUT= &quot;&lt;value&gt;&quot;</td>
<td>0</td>
</tr>
<tr>
<td>(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.</td>
<td>timeout <code>&lt;value&gt;</code></td>
<td>POSTVPNCONNECTTIMEOUT= &quot;&lt;value&gt;&quot;</td>
<td></td>
</tr>
<tr>
<td>Not supported for post-vpn-connect.</td>
<td></td>
<td>PREVPNDISCONNECTTIMEOUT= &quot;&lt;value&gt;&quot;</td>
<td></td>
</tr>
<tr>
<td>Portal Agent Configuration</td>
<td>Windows Registry/macOS Plist</td>
<td>Msiexec Parameter</td>
<td>Default</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------</td>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>(Optional)</strong> Specify the full path of a file used in a command. The GlobalProtect app verifies the integrity of the file by checking it against the value specified in the checksum key. Environmental variables are supported.</td>
<td>file <code>&lt;path_file&gt;</code></td>
<td><code>PREVPNCONNECTFILE= &quot;&lt;path_file&gt;&quot;</code></td>
<td>n/a</td>
</tr>
<tr>
<td><strong>(Optional)</strong> 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.</td>
<td>checksum <code>&lt;value&gt;</code></td>
<td><code>PREVPNCONNECTCHECKSUM= &quot;&lt;value&gt;&quot;</code></td>
<td>n/a</td>
</tr>
<tr>
<td><strong>(Optional)</strong> 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.</td>
<td>error-msg <code>&lt;message&gt;</code> Example: error-msg Failed executing pre-vpn-connect action!</td>
<td><code>PREVPNCONNECTERRORMSG= &quot;&lt;message&gt;&quot;</code></td>
<td>n/a</td>
</tr>
</tbody>
</table>

**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 Agent Settings in the Windows Registry**
- **Deploy Agent Settings from Msiexec**
- **Deploy Scripts Using the Windows Registry**
Deploy Scripts Using Msiexec
• 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 also 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\n```

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.

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`.

![Registry Editor](image)
STEP 3 | Deploy various settings to the Windows endpoint, including the connect method for the GlobalProtect app and single sign-on (SSO).

View Customizable App Settings for a full list of the commands and values you can set up using the Windows Registry.

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.*

<table>
<thead>
<tr>
<th>Msiexec Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>msiexec.exe /i GlobalProtect.msi /quiet PORTAL=&quot;portal.acme.com&quot;</td>
<td>Install GlobalProtect in quiet mode (no user interaction) and configure the portal address.</td>
</tr>
<tr>
<td>msiexec.exe /i GlobalProtect.msi CANCONTINUEIFPORTALCERTINVALID=&quot;no&quot;</td>
<td>Install GlobalProtect with the option to prevent users from connecting to the portal if the certificate is not valid.</td>
</tr>
</tbody>
</table>

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](#).

```bash
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="a48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b0118647ccf599"
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](#).

```bash
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="a48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b0118647ccf599"
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="b48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b0118647ccf598"
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="c48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b0118647ccf597"
PREVPNDISCONNECTERRORMSG="Failed executing pre-vpn-disconnect action."

For a complete list of settings and the corresponding default values, see Customizable App Settings.

**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.

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:
   ```plaintext
   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:
      
   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.
   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.
   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):

```bash
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):

```bash
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 Mac 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.

**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 Mac 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:

- /Palo Alto 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.
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
> Supported Technologies
> Configure Clientless VPN
> 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.

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.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Supported Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web application technologies</td>
<td>• HTML • HTML5 • HTML5-Web-Sockets • Javascript • Remote desktop protocol (RDP), VNC, or SSH</td>
</tr>
<tr>
<td></td>
<td>• Virtual Desktop Infrastructure (VDI) and Virtual Machine (VM) environments, such as Citrix XenApp and XenDesktop or 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.</td>
</tr>
<tr>
<td></td>
<td>• 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 HOBLink or Thinfinity, to RDP through Clientless VPN.</td>
</tr>
<tr>
<td></td>
<td>• Adobe Flash—With Clientless VPN, browsers can display flash content or files like Microsoft Word documents or Adobe PDFs; however, Clientless VPN cannot rewrite HTML content links inside the content to route the links through the tunnel.</td>
</tr>
<tr>
<td>Other technologies (such as Microsoft Silverlight or XML/XSLT) are not supported.</td>
<td></td>
</tr>
</tbody>
</table>

| Operating systems               | • Windows • macOS • iOS • Android • Chrome • Linux |

| Supported browsers              | • Chrome • Internet Explorer • Safari • Firefox |
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 GlobalProtect Clientless VPN dynamic update (see Install Content and Software Updates).
- 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 appear.
   - **Application Home URL**—The URL where the web application is located (up to 4095 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 appear.

2. In the Applications area, 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 fully-qualified domain name) 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 can be accessed.
   - 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 hours or minutes that a Clientless VPN session is valid. The typical session time is 3 hours. The range for hours is 1-24; the range for minutes is 60-1440. After the session expires, users must re-authenticate and start a new Clientless VPN session.
   - Inactivity Timeout—Specify the number of hours or minutes that a Clientless VPN session can remain idle. The typical inactivity timeout is 30 minutes. The range for hours is 1-24; the range for minutes is 5 to 1440. If there is no user activity during the specified amount 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 into 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 properly and map to all of the required applications, as 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 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. Controlling access to applications (published or not) is done using security policies.

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 click the Application URL link on the page and specify a URL.

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.
• **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. AES128 or higher is recommended.

• **Authentication Algorithms**—Select the supported authentication algorithms. Choices are: MD5, SHA1, SHA256, or SHA384. SHA256 or higher is recommended.

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 host name 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 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, host names, 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 host and domain names. The wildcard character (*) for host names and domain names can only appear at the beginning of the name (for example, *.etradecom).

**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.

![GlobalProtect Portal Configuration](image)

- 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 Enable User Identification is set in order to create user-based rules for accessing published applications.

By default Service/URL in Security Policy Rule is set 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.

![Security Policy Rule](image)

- 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.

![Proxy Configuration](image)

The source IP address of Clientless VPN traffic (as seen by the application) will either be 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 5: Table: Rewrite Engine Statistics**

<table>
<thead>
<tr>
<th>Action</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CLI Commands</strong></td>
<td></td>
</tr>
<tr>
<td>List the version of Clientless VPN dynamic</td>
<td><code>show system setting ssl-decrypt memory</code></td>
</tr>
<tr>
<td>content being used</td>
<td>proxy uses shared allocator</td>
</tr>
<tr>
<td>You can also view the dynamic update version</td>
<td></td>
</tr>
<tr>
<td>from the Device &gt; Dynamic Updates &gt;</td>
<td><code>show system setting ssl-decrypt memory</code></td>
</tr>
<tr>
<td>GlobalProtect Clientless VPN</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>show system setting ssl-decrypt memory</code></td>
</tr>
<tr>
<td></td>
<td>proxy uses shared allocator</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>show system setting ssl-decrypt memory</code></td>
</tr>
<tr>
<td></td>
<td>proxy uses shared allocator</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>In this example, the current dynamic update</td>
<td></td>
</tr>
<tr>
<td>is version 61-62, and the last installed</td>
<td></td>
</tr>
<tr>
<td>dynamic update is version 60-47.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>List active (current) users of Clientless</td>
<td><code>show global-protect-portal current-user</code></td>
</tr>
<tr>
<td>VPN</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>show global-protect-portal current-user</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>GlobalProtect Portal</td>
<td>GPClientlessPortal</td>
</tr>
<tr>
<td>Vsys-Id</td>
<td>1</td>
</tr>
<tr>
<td>User</td>
<td>paloaltonetworks.com</td>
</tr>
<tr>
<td>\johndoe</td>
<td></td>
</tr>
<tr>
<td>Session-id</td>
<td></td>
</tr>
<tr>
<td>1SU2vPIdfGf0-7gahMTciX8PuL0S0</td>
<td></td>
</tr>
<tr>
<td>Client-IP</td>
<td>5.5.5.5</td>
</tr>
<tr>
<td>Inactivity Timeout</td>
<td>1800</td>
</tr>
<tr>
<td>Seconds before inactivity timeout</td>
<td>1750</td>
</tr>
<tr>
<td>Login Lifetime</td>
<td>10800</td>
</tr>
<tr>
<td>Seconds before login lifetime</td>
<td>10748</td>
</tr>
<tr>
<td>Total number of user sessions: 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Show DNS resolution results</td>
<td><code>show system setting ssl-decrypt dns-cache</code></td>
</tr>
<tr>
<td>This can be useful to determine if there</td>
<td></td>
</tr>
<tr>
<td>are DNS issues. If there is a DNS issue, you</td>
<td></td>
</tr>
<tr>
<td>will notice querying against an FQDN that</td>
<td></td>
</tr>
<tr>
<td>was not</td>
<td></td>
</tr>
<tr>
<td>Total DNS cache entries: 89</td>
<td></td>
</tr>
<tr>
<td>Site</td>
<td>IP</td>
</tr>
<tr>
<td>Interface</td>
<td></td>
</tr>
<tr>
<td>bugzilla.panw.local</td>
<td>10.0.2.15</td>
</tr>
<tr>
<td>0</td>
<td>216.58.216.4</td>
</tr>
<tr>
<td>Action</td>
<td>Command</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>resolvable in the CLI output.</td>
<td><code>stats.g.doubleclick.net 74.125.199.154 Expired 0</code></td>
</tr>
</tbody>
</table>

**Show all Clientless VPN user sessions and cookies stored**

```
pancpe@cagp> show system setting ssl-decrypt gp-cookie-cache
```

User: johndoe, Session-id: 1SU2vrFIDfdomGf-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 **Table: Rewrite Engine Statistics** for information on rewrite statistics and their meaning or purpose.

```
pancpe@cagp> 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
- `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

<table>
<thead>
<tr>
<th>Action</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug dataplane packet-diag set log feature ssl all</td>
<td></td>
</tr>
<tr>
<td>debug dataplane packet-diag set log feature misc all</td>
<td></td>
</tr>
<tr>
<td>debug dataplane packet-diag set log feature proxy all</td>
<td></td>
</tr>
<tr>
<td>debug dataplane packet-diag set log feature flow basic</td>
<td></td>
</tr>
<tr>
<td>debug dataplane packet-diag set log on</td>
<td></td>
</tr>
</tbody>
</table>

Enable packet capture on the firewall running Clientless VPN Portal

<table>
<thead>
<tr>
<th>Action</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug dataplane packet-diag set capture username &lt;portal-username&gt;</td>
<td></td>
</tr>
<tr>
<td>debug dataplane packet-diag set capture stage clientless-vpn-client file clss_client1.pcap</td>
<td></td>
</tr>
<tr>
<td>debug dataplane packet-diag set capture stage clientless-vpn-server file clss_server1.pcap</td>
<td></td>
</tr>
<tr>
<td>debug dataplane packet-diag set capture stage firewall file clss_fw1.pcap</td>
<td></td>
</tr>
<tr>
<td>debug dataplane packet-diag set capture stage receive file clss_rx1.pcap</td>
<td></td>
</tr>
<tr>
<td>debug dataplane packet-diag set capture stage transmit file clss_tx1.pcap</td>
<td></td>
</tr>
<tr>
<td>debug dataplane packet-diag set capture on</td>
<td></td>
</tr>
</tbody>
</table>

Table 6: Table: Rewrite Engine Statistics

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>initiate_connection_failure</td>
<td>Connection initiation failed to back-end host</td>
</tr>
<tr>
<td>setup_connection_failure</td>
<td>Connection setup failed</td>
</tr>
<tr>
<td>setup_connection_duplicate</td>
<td>Duplicate peer session exists</td>
</tr>
<tr>
<td>session_notify_mismatch</td>
<td>Mostly invalid session</td>
</tr>
<tr>
<td>packet_mismatch_session</td>
<td>Failed to find right session for incoming packet</td>
</tr>
<tr>
<td>peer_queue_update_rcvd_failure</td>
<td>Session was invalid when packet update received by peer</td>
</tr>
<tr>
<td>peer_queue_update_sent_failure</td>
<td>Failed to send packet updates to peer or failed to send packet queue length updates to peer</td>
</tr>
<tr>
<td>exceed_pkt_queue_limit</td>
<td>Too many packets queued</td>
</tr>
<tr>
<td>proxy_connection_failure</td>
<td>Proxy connection failed</td>
</tr>
<tr>
<td>setup_connection_r</td>
<td>Installing the peer session to the application server. This value should match the values for initiate_connection and setup_connection.</td>
</tr>
<tr>
<td>setup_connection_duplicate_r</td>
<td>Duplicate sessions already in proxy</td>
</tr>
<tr>
<td>Statistic</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>setup_connection_failure_r</td>
<td>Failed to set up the peer session</td>
</tr>
<tr>
<td>session_notify_mismatch_r</td>
<td>Peer session not found</td>
</tr>
<tr>
<td>packet_mismatch_session_r</td>
<td>Peer session not found when trying to get the packet</td>
</tr>
<tr>
<td>exceed_pkt_queue_limit_r</td>
<td>Too many packets held</td>
</tr>
<tr>
<td>unknown_dest</td>
<td>Failed to find destination host</td>
</tr>
<tr>
<td>pkt_no_dest</td>
<td>No destination for this packet</td>
</tr>
<tr>
<td>cookie_suspend</td>
<td>Suspended session to fetch cookies</td>
</tr>
<tr>
<td>cookie_resume</td>
<td>Received response from MP with updated cookies. This value generally matches the value of cookie_suspend.</td>
</tr>
<tr>
<td>decompress_failure</td>
<td>Failed to decompress</td>
</tr>
<tr>
<td>memory_alloc_failure</td>
<td>Failed to allocate memory</td>
</tr>
<tr>
<td>wait_for_dns_resolve</td>
<td>Suspended session to resolve DNS requests</td>
</tr>
<tr>
<td>dns_resolve_reschedule</td>
<td>Rescheduled DNS query due to no response (retry before timeout)</td>
</tr>
<tr>
<td>dns_resolve_timeout</td>
<td>DNS query timeout</td>
</tr>
<tr>
<td>setup_site_conn_failure</td>
<td>Failed to setup connection to site (proxy, DNS)</td>
</tr>
<tr>
<td>site_dns_invalid</td>
<td>DNS resolve failed</td>
</tr>
<tr>
<td>multiple_multipart</td>
<td>Multi-part content-type processed</td>
</tr>
<tr>
<td>site_from_referer</td>
<td>Received the back-end host from referrer. This can indicate failed rewrite links from flash or other content which Clientless VPN does not rewrite.</td>
</tr>
<tr>
<td>received_fin_for_pending_req</td>
<td>Received FIN from server for pending request from client</td>
</tr>
<tr>
<td>unmatched_http_state</td>
<td>Unexpected HTTP content. This can indicate an issue parsing the http headers or body.</td>
</tr>
</tbody>
</table>
Mobile Device Management

- Mobile Device Management Overview on page 159
- Set Up the MDM Integration With GlobalProtect on page 162
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 (AirWatch only)

You can configure the Windows User-ID agent to communicate with the AirWatch 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 on PAN-OS 8.0 and later releases.

Firewall integration is supported only with VMware AirWatch.

GlobalProtect app integration is qualified with VMware AirWatch, 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.

<table>
<thead>
<tr>
<th>MDM Attribute</th>
<th>HIP Report Attribute</th>
<th>HIP Report Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mobile_id</td>
<td>Host ID</td>
<td>General</td>
<td>Unique device identifier (UDID) of the endpoint.</td>
</tr>
<tr>
<td>MDM Attribute</td>
<td>HIP Report Attribute</td>
<td>HIP Report Category</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------</td>
<td>---------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>managed</td>
<td>Managed</td>
<td>General</td>
<td>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.</td>
</tr>
<tr>
<td>compliance</td>
<td>Tag</td>
<td>Mobile Device</td>
<td>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.</td>
</tr>
<tr>
<td>ownership</td>
<td>Tag</td>
<td>Mobile Device</td>
<td>Ownership category of the endpoint (for example, Employee Owned). This value is appended to the Tag attribute in the HIP report.</td>
</tr>
<tr>
<td>tag</td>
<td>Tag</td>
<td>Mobile Device</td>
<td>Tags to match against other MDM-based attributes.</td>
</tr>
</tbody>
</table>
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 on page 15.
2. Enable SSL Between GlobalProtect Components on page 17.
3. Set up GlobalProtect User Authentication. Refer to About GlobalProtect User Authentication on page 27.
5. Configure a GlobalProtect Gateway on page 74.
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 on page 89.

**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.**
- App store—Download and Install the GlobalProtect Mobile App on page 118
- Supported mobile device management systems—Deploy the GlobalProtect Mobile App on page 164
- 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 on page 266
- GlobalProtect app integration with an MDM or EMM system:
  - Manage the GlobalProtect App Using a Supported Third-Party MDM on page 162
  - Manage the GlobalProtect App Using Other Third-Party MDMs on page 234

**STEP 5 | Configure policies that target mobile endpoints using host information.**
Configure HIP-Based Policy Enforcement on page 250 for managed endpoints.

Manage the GlobalProtect App Using a Supported Third-Party MDM

Refer to the following sections for information on how to deploy, configure, and manage the GlobalProtect app for mobile endpoints using a supported third-party MDM system:
- Supported MDM Vendors on page 163
• Deploy the GlobalProtect Mobile App on page 164
• Always On VPN Configurations on page 168
• User-Initiated Remote Access VPN Configurations on page 183
• Per-App VPN Configurations on page 199
• Enable App Scan Integration with WildFire on page 234

If you are not using a supported third-party MDM system, you can Manage the GlobalProtect App Using Other Third-Party MDMs on page 234.

## Supported MDM Vendors

The following table lists the supported 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 a different MDM vendor, Manage the GlobalProtect App Using Other Third-Party MDMs on page 234.

<table>
<thead>
<tr>
<th>Supported MDM Vendor</th>
<th>Android</th>
<th>iOS</th>
<th>Chrome</th>
<th>Windows</th>
<th>Windows 10 UWP</th>
<th>Mac</th>
<th>Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirWatch</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>(Per-App VPN only)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Intune</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>(Always On and Per-App VPN only)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MobileIron</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>(Always On VPN only)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google Admin console</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>You can use the Google Admin console only to deploy the GlobalProtect</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(app deployment only)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supported MDM Vendor</td>
<td>Android</td>
<td>iOS</td>
<td>Chrome</td>
<td>Windows</td>
<td>Windows 10 UWP</td>
<td>Mac</td>
<td>Linux</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------</td>
<td>-----</td>
<td>--------</td>
<td>---------</td>
<td>----------------</td>
<td>-----</td>
<td>-------</td>
</tr>
</tbody>
</table>

You cannot use the console to configure VPN configurations. You must configure the VPN configuration through the GlobalProtect portal before you can deploy the app using the Google Admin console.

**Deploy 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 connects to the gateway that is closest to the end user’s current location. In addition, traffic to and from the mobile endpoint is automatically subject to the same security policy enforcement as other endpoints in your corporate network. The 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: 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 AirWatch) and transparently push the app to your managed endpoints.

- Deploy the GlobalProtect Mobile App Using AirWatch on page 165
- Deploy the GlobalProtect Mobile App Using Microsoft Intune on page 166
- Deploy the GlobalProtect Mobile App Using MobileIron on page 166
- Deploy the GlobalProtect App Using the Google Admin Console on page 121
Deploy the GlobalProtect Mobile App Using AirWatch

You can deploy the GlobalProtect app to managed endpoints that are enrolled with AirWatch. Endpoints running iOS or Android must download the AirWatch agent to enroll with the AirWatch MDM. Windows 10 endpoints do not require the AirWatch 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.

STEP 1 | Before you begin, ensure that the endpoints to which you want to deploy the GlobalProtect app are enrolled with AirWatch:

- **Android and iOS**—Download the AirWatch agent and follow the prompts to enroll.
- **Windows Phone and Windows 10 UWP**—Configure the Windows 10 UWP endpoint to enroll with AirWatch (from the endpoint, select Settings > Accounts > Work access > Connect).

STEP 2 | From AirWatch, select APPS & BOOKS > Public > Add Application.

STEP 3 | Select the organization group by which this app will be managed.

STEP 4 | Select the Platform (Apple iOS, Android, or Windows Phone).

STEP 5 | Search for the GlobalProtect app in the endpoint app store, or enter one of the following URLs for the GlobalProtect app page:

- **Windows Phone**—https://www.microsoft.com/store/apps/9NBLGGH6BZL3

STEP 6 | 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.

> 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 7 | On the Assignment tab, select the Assigned Smart Groups that will have access to this app.

STEP 8 | Choose the App Delivery Method, either Auto which pushes the app to the device automatically or On Demand.

STEP 9 | (GlobalProtect App for Android only) Enable the Application Configuration to use the UDID to identify the endpoint.

Add the following Key-Value pair:
- Configuration Key—`mobile_id`
- Value Type—`String`
- Configuration Value—`{DeviceUid}`
STEP 10 | Select **Save & Publish** to push the App Catalog to the endpoints in the Smart Groups you assigned in the **Assignment** section.

**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 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.

**Deploy the GlobalProtect App Using the Google Admin Console**

The Google Admin console enables you to manage Chromebook settings and apps from a central, web-based location. From the console, you can deploy the GlobalProtect app and customize VPN settings.

Use the following workflow to manage policies and settings for the GlobalProtect app for Chrome OS:

**STEP 1 | View the user settings for the GlobalProtect app.**

1. From the Google Admin console, select **Device management > Chrome management > App management**.

   The console displays the list of apps configured in all organization (org) units in your domain and also indicates the status of each app. Click an app **Status** to display the org units to which that status is applied.

2. Select the GlobalProtect app and then select **User settings**.

   If the app is not present, **SEARCH** for GlobalProtect in the Chrome Web Store.

   ![User settings](image)

**STEP 2 | Configure policies and settings for everyone in an org unit.**

1. Select the org unit for which you want to configure settings, and then configure any of the following options:

   *Selecting the top-level org unit applies settings to everyone in that unit; selecting a child org unit applies settings only to users within that child org unit.*
• **Allow installation**—Allows users to install this app from the Chrome Web Store. By default, an org unit inherits the settings of its parent organization. To override the default settings, select **Inherit**, which toggles the **Override** setting.

• **Force installation**—Installs the app automatically and prevents users from removing it.

• **Pin to taskbar**—If the app is installed, pins the app to the taskbar (in Chrome OS only).

• **Add to Chrome Web Store collection**—Recommends this app to your users in the Chrome Web Store.

2. If you have not already done so, create a JSON format text file that uses the following syntax and includes the FQDN or IP address of your GlobalProtect portal:

```json
{
  "PortalAddress": {
    "Value": "192.0.2.191"
  }
}
```

3. On the **User settings** page, select **UPLOAD CONFIGURATION FILE** and then **Browse** for the GlobalProtect settings file.

4. **SAVE** your changes. Settings typically take effect within minutes, but it may take up to an hour to propagate through your organization.

**STEP 3 | Test the connection.**

After Google Admin console successfully deploys the app, Test the GlobalProtect App for Chrome OS

**Always On VPN Configurations**

In an Always On VPN configuration, the secure GlobalProtect connection is always on. The GlobalProtect app connects to the GlobalProtect portal (upon user login) to submit user and host information and retrieve the agent configuration. After the app receives the agent configuration from the portal, it automatically connects and establishes a VPN tunnel to the GlobalProtect gateway that was specified in the agent configuration.

Refer to the following sections for information on how to configure an Always On VPN configuration using supported mobile device management systems:

• **Configure an Always On VPN Configuration Using AirWatch** on page 168

• **Configure an Always On VPN Configuration Using Microsoft Intune** on page 181

• **Configure an Always On VPN Configuration Using MobileIron** on page 182

**Configure an Always On VPN Configuration Using AirWatch**

AirWatch 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 AirWatch 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 configure an Always On VPN configuration using AirWatch:

• **Configure an Always On VPN Configuration for iOS Endpoints Using AirWatch** on page 169

• **Configure an Always On VPN Configuration for Windows 10 UWP Endpoints Using AirWatch** on page 173
Configure an Always On VPN Configuration for iOS Endpoints Using AirWatch

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 AirWatch:

**STEP 1 |** Download the GlobalProtect app for iOS.
- Deploy the GlobalProtect Mobile App Using AirWatch.
- Download the GlobalProtect app directly from the App Store.

**STEP 2 |** From the AirWatch 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** (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 AirWatch 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 following bundle ID in the **Identifier** field to identify the GlobalProtect app:
   ```
   com.paloaltonetworks.globalprotect.vpn
   ```
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. Disable the option to **Enable VPN On Demand** (enabled by default).
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 **HIP integration with MDM**, 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 an Always On VPN Configuration for Windows 10 UWP Endpoints Using AirWatch*

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 AirWatch 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 AirWatch:

**STEP 1** | Download the GlobalProtect app for Windows 10 UWP:
- Deploy the GlobalProtect Mobile App Using AirWatch.
- Download the GlobalProtect app directly from the Microsoft Store.

**STEP 2** | From the AirWatch 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 AirWatch 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, AirWatch 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, AirWatch 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 AirWatch 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 AirWatch 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. AirWatch 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 `LocURI` element that specifies the `PluginPackageFamilyName`, change the element to:
     ```xml
     <LocURI>./Vendor/MSFT/VPNv2/PaloAltoNetworks/PluginProfile/PluginPackageFamilyName</LocURI>
     ```
   - In the `Data` element that follows, change the value to:
     ```xml
     <Data>PaloAltoNetworks.GlobalProtect_rn9aerfb38dg</Data>
     ```

1. Save your changes to the exported profile.
2. Return to AirWatch 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. AirWatch moves the profile to the Inactive list.

STEP 9 | Test the configuration.

Configure an Always On VPN Configuration 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 configure an Always On VPN configuration using Microsoft Intune:

- Configure an Always On VPN Configuration for iOS Endpoints Using Microsoft Intune on page 181
- Configure an Always On VPN Configuration for Windows 10 UWP Endpoints Using Microsoft Intune on page 181

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 on page 166.
- 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 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 on page 166.
- 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 an Always On VPN Configuration 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 configure an Always On VPN configuration using MobileIron:
- Configure an Always On VPN Configuration for iOS Endpoints Using MobileIron on page 182
- Configure an Always On VPN Configuration for Android Endpoints Using MobileIron on page 182

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 on page 166.
  - 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 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 on page 166.
• 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.

### User-Initiated Remote Access VPN Configurations

In a remote access (On-Demand) VPN configuration, users must manually launch the GlobalProtect app to establish the secure GlobalProtect connection. The GlobalProtect app connects to the GlobalProtect portal (upon user login) to submit user and host information and retrieve the agent configuration. After the app receives the agent configuration from the portal, it connects and establishes a VPN tunnel to the GlobalProtect gateway that was specified in the agent configuration.

Refer to the following sections for information on how to configure a user-initiated remote access VPN configuration using supported mobile device management systems:

- Configure a User-Initiated Remote Access VPN Configuration Using AirWatch on page 183
- Configure a User-Initiated Remote Access VPN Configuration Using Microsoft Intune on page 198
- Configure a User-Initiated Remote Access VPN Configuration Using MobileIron on page 198

#### Configure a User-Initiated Remote Access VPN Configuration Using AirWatch

AirWatch 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 AirWatch managed mobile endpoints and the firewall 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 configure a user-initiated remote access VPN configuration using AirWatch:

- Configure a User-Initiated Remote Access VPN Configuration for iOS Endpoints Using AirWatch on page 183
- Configure a User-Initiated Remote Access VPN Configuration for Windows 10 UWP Endpoints Using AirWatch on page 191

#### Configure a User-Initiated Remote Access VPN Configuration for iOS Endpoints Using AirWatch

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 AirWatch:

**STEP 1** | Download the GlobalProtect app for iOS.
  • Deploy the GlobalProtect Mobile App Using AirWatch.
  • Download the GlobalProtect app directly from the App Store.

**STEP 2** | From the AirWatch 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 AirWatch 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 following bundle ID in the Identifier field to identify the GlobalProtect app:
   
   com.paloaltonetworks.globalprotect.vpn

<table>
<thead>
<tr>
<th>Connection info</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Name *</td>
</tr>
<tr>
<td>Connection Type *</td>
</tr>
<tr>
<td>Identifier</td>
</tr>
</tbody>
</table>

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.

**On-Demand Rule**

<table>
<thead>
<tr>
<th>Action</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluate Connection</td>
<td></td>
</tr>
<tr>
<td>Connect</td>
<td></td>
</tr>
<tr>
<td>Disconnect</td>
<td></td>
</tr>
<tr>
<td>Ignore</td>
<td></td>
</tr>
</tbody>
</table>

- (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.

**Action Parameter**

<table>
<thead>
<tr>
<th>Domain Action</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect if Needed</td>
<td></td>
</tr>
<tr>
<td>Never Connect</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain.local</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>URL Probe</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.example.com">www.example.com</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DNS Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.8.8.8</td>
</tr>
</tbody>
</table>

- 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 HIP integration with MDM, 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 User-Initiated Remote Access VPN Configuration for Windows 10 UWP Endpoints Using AirWatch

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 AirWatch 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 AirWatch:

**STEP 1 | Download the GlobalProtect app for Windows 10 UWP:**
- Deploy the GlobalProtect Mobile App Using AirWatch.
- Download the GlobalProtect app directly from the Microsoft Store.

**STEP 2 | From the AirWatch 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 AirWatch 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, AirWatch 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 to 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, AirWatch 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 AirWatch 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 AirWatch 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. AirWatch 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 LocURI 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 AirWatch 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. AirWatch moves the profile to the Inactive list.
STEP 9 | Test the configuration.

Configure a User-Initiated Remote Access VPN Configuration 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 section for information on how to configure a user-initiated remote access VPN configuration using Microsoft Intune:

- Configure a User-Initiated Remote Access VPN Configuration for iOS Endpoints Using Microsoft Intune on page 198

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 on page 166.
- 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 User-Initiated Remote Access VPN Configuration 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 section for information on how to configure a user-initiated remote access VPN configuration using MobileIron:

- Configure a User-Initiated Remote Access VPN Configuration for iOS Endpoints Using MobileIron on page 199
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 on page 166.
- 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.

**Per-App VPN Configurations**

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.

Refer to the following sections for information on how to configure a per-app VPN configuration using supported mobile device management systems:

- Configure a Per-App VPN Configuration Using AirWatch on page 199
- Configure a Per-App VPN Configuration Using Microsoft Intune on page 232
- Configure a Per-App VPN Configuration Using MobileIron on page 233

**Configure a Per-App VPN Configuration Using AirWatch**

AirWatch 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 AirWatch managed mobile endpoints and the firewall 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 configure a per-app VPN configuration using AirWatch:

- Configure a Per-App VPN Configuration for iOS Endpoints Using AirWatch on page 200
- Configure a Per-App VPN Configuration for Android Endpoints Using AirWatch on page 209
- Configure a Per-App VPN Configuration for Windows 10 UWP Endpoints Using AirWatch on page 219
Configure a Per-App VPN Configuration for iOS Endpoints Using AirWatch

You can enable access to internal resources from your managed mobile endpoints by configuring GlobalProtect VPN access using AirWatch. 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 AirWatch:

**STEP 1 |** Download the GlobalProtect app for iOS:

- Deploy the GlobalProtect Mobile App Using AirWatch.
- Download the GlobalProtect app directly from the App Store.

**STEP 2 |** From the AirWatch 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.
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 AirWatch 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 following bundle ID in the **Identifier** field to identify the GlobalProtect app:
   ```
   com.paloaltonetworks.globalprotect.vpn
   ```
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.
   - Select a **Provider Type** to indicate how traffic will be tunneled—either at the application layer or the IP layer.
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 HIP integration with MDM, 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 (-pencil) icon in the actions menu next to the row.

<table>
<thead>
<tr>
<th>Application</th>
<th>Platform</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon</td>
<td>Apple iOS</td>
<td>Assigned</td>
</tr>
<tr>
<td>Box</td>
<td>Android</td>
<td>Assigned</td>
</tr>
<tr>
<td>Box</td>
<td>Apple iOS</td>
<td>View</td>
</tr>
<tr>
<td>Dropbox</td>
<td>Windows Phone</td>
<td>Assigned</td>
</tr>
<tr>
<td>GlobalProtect</td>
<td>apple iOS</td>
<td>View</td>
</tr>
</tbody>
</table>

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](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 AirWatch App Catalog.

8. (Optional) Assign the app to pre-defined or custom **Categories** for ease-of-access in the AirWatch 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 a Per-App VPN Configuration for Android Endpoints Using AirWatch**

You can enable access to internal resources from your managed mobile endpoints by configuring GlobalProtect VPN access using AirWatch. 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 AirWatch:

**STEP 1 |** Download the GlobalProtect app for Android:

- Deploy the GlobalProtect Mobile App Using AirWatch.
- Download the GlobalProtect app directly from Google Play.

**STEP 2 |** From the AirWatch 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 AirWatch 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.

   ![Add a New Android Profile](image)

**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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Platform</th>
<th>Source</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Box</td>
<td>Android</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Box</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Box</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Box</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

**Configure a Per-App VPN Configuration for Windows 10 UWP Endpoints Using AirWatch**

You can enable access to internal resources from your managed mobile endpoints by configuring GlobalProtect VPN access using AirWatch. 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 AirWatch 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 AirWatch:

**STEP 1** | Download the GlobalProtect app for Windows 10 UWP:
- Deploy the GlobalProtect Mobile App Using AirWatch.
- Download the GlobalProtect app directly from the Microsoft Store.

**STEP 2** | From the AirWatch 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 AirWatch 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, AirWatch 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 to 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, AirWatch 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 AirWatch 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 (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 AirWatch App Catalog.
8. **(Optional)** Assign the app to pre-defined or custom **Categories** for ease-of-access in the AirWatch 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. AirWatch 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 **LocURI** element that specifies the PluginPackageFamilyName, change the element to:
     
     ```xml
     <LocURI>./Vendor/MSFT/VPNv2/PaloAltoNetworks/PluginProfile/PluginPackageFamilyName</LocURI>
     ```
   - In the **Data** element that follows, change the value to:
     
     ```xml
     <Data>PaloAltoNetworks.GlobalProtect_rn9aeerfb38dg</Data>
     ```
4. Save your changes to the exported profile.
5. Return to AirWatch and select **Devices > Profiles > List View**.
6. Create (select **Add > Add Profile > Windows > Windows Phone**) and name a new profile.
7. Select **Custom Settings > Configure**, and then copy and paste the edited configuration.
8. 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. AirWatch moves the profile to the Inactive list.

STEP 10 | Test the configuration.

**Configure a Per-App VPN Configuration 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 configure per-app VPN configuration using Microsoft Intune:

- Configure a Per-App VPN Configuration for iOS Endpoints Using Microsoft Intune on page 232
- Configure a Per-App VPN Configuration for Windows 10 UWP Endpoints Using Microsoft Intune on page 232

**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 on page 166.
- 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 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 on page 166.
• 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.

Configure a Per-App VPN Configuration 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 section for information on how to configure a per-app VPN configuration using MobileIron:

• Configure a Per-App VPN Configuration for iOS Endpoints Using MobileIron on page 233

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 on page 166.
• 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.
Enable App Scan Integration with WildFire

By enabling App Scan in AirWatch, you can leverage WildFire threat intelligence about apps to detect malware on Android endpoints. When enabled, the AirWatch agent sends the list of apps that are installed on the Android endpoint to AirWatch. This occurs during enrollment and subsequently on any endpoint check-in. AirWatch 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 AirWatch, 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 AirWatch 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 AirWatch 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. AirWatch 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 Other Third-Party MDMs

If you are not using a supported third-party MDM vendor, you can use other third-party MDM systems to deploy and manage the GlobalProtect app:
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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Type</td>
<td>Type of connection enabled by the policy.</td>
<td>Custom SSL</td>
</tr>
<tr>
<td>Identifier</td>
<td>Identifier for the custom SSL VPN in reverse DNS format.</td>
<td>com.paloaltonetworks. GlobalProtect.vpnplugin</td>
</tr>
<tr>
<td>Server</td>
<td>Host name or IP address of the GlobalProtect portal.</td>
<td>&lt;hostname or IP address&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example: gp.paloaltonetworks.com</td>
</tr>
<tr>
<td>Account</td>
<td>User account for authenticating the connection.</td>
<td>&lt;username&gt;</td>
</tr>
<tr>
<td>User Authentication</td>
<td>Authentication type for the connection.</td>
<td>Certificate</td>
</tr>
<tr>
<td>Credential</td>
<td>(Certificate User Authentication only) Credential for authenticating the connection.</td>
<td>&lt;credential&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example: clientcredial.p12</td>
</tr>
<tr>
<td>Enable VPN On Demand</td>
<td>(Optional) Domain and hostname that establish the connection and the on-demand action:</td>
<td>&lt;domain and hostname and the on-demand action&gt;</td>
</tr>
<tr>
<td></td>
<td>- Always establish a connection</td>
<td>For example: gp.acme.com; Never establish</td>
</tr>
<tr>
<td></td>
<td>- Never establish a connection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Establish a connection if needed</td>
<td></td>
</tr>
</tbody>
</table>

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
<?xml version="1.0"
```
<?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>VendorConfig</key>
    <dict>
     <key>AllowPortalProfile</key>
     <integer>0</integer>
    </dict>
   </dict>
  </array>
 </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>
<key>VendorConfig</key>
<dict>
 <key>AllowPortalProfile</key>
 <integer>0</integer>
</dict>
<key>FromAspen</key>
<integer>1</integer>
</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
<?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>cGFuU2FtcGxlIEFwcCBMZXZlbCBWUE52cG5TYW1wbGUgQXBwIElmdVsIFZQTg==</string>
                <key>SafariDomains</key>
                <array>
                    <string>*.paloaltonetworks.com</string>
                </array>
                <key>Proxies</key>
                <dict/>
                <key>VPNType</key>
            </dict>
        </array>
    </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 through 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 whitelist or blacklist specific managed apps from having their traffic routed through the VPN tunnel.

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.

<table>
<thead>
<tr>
<th>Key</th>
<th>Value Type</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>portal</td>
<td>String</td>
<td>IP address or fully qualified domain name (FQDN) of the portal.</td>
<td>10.1.8.190</td>
</tr>
<tr>
<td>username</td>
<td>String</td>
<td>Username for the user.</td>
<td>john</td>
</tr>
<tr>
<td>password</td>
<td>String</td>
<td>Password for the user.</td>
<td>Passwd!234</td>
</tr>
<tr>
<td>mobile_id</td>
<td>String</td>
<td>Mobile ID as configured in third-party MDM service to uniquely identify a mobile device. GlobalProtect uses this mobile ID to retrieve device information.</td>
<td>5188a8193be43f42d332dde5cb2c941e</td>
</tr>
<tr>
<td>certificate</td>
<td>String (in Base64)</td>
<td>Client certificate (cert) used to authenticate the agent and the portal.</td>
<td>DAFDSaweEWQ23wD5AFD....</td>
</tr>
<tr>
<td>client_certificate_passphrase</td>
<td>String</td>
<td>Key associated with the client certificate.</td>
<td>PA$$WORD$123</td>
</tr>
<tr>
<td>app_list</td>
<td>String</td>
<td>Configuration for Per-App VPN. Begin the string with either the whitelist or blacklist, and follow it with an array of app names separated by semicolons. The whitelist specifies the apps that will use the VPN tunnel for</td>
<td>whitelist</td>
</tr>
<tr>
<td>Key</td>
<td>Value Type</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-----</td>
<td>------------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>connect_method</td>
<td>String</td>
<td>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.</td>
<td>user-logon</td>
</tr>
<tr>
<td>remove_vpn_config_via_restriction</td>
<td>Boolean</td>
<td>Permanently remove all GlobalProtect VPN configuration information.</td>
<td>true</td>
</tr>
</tbody>
</table>

**Example: Set VPN Configuration**

```java
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, "whitelist:com.android.chrome;com.android.calendar");

DevicePolicyManager dpm = (DevicePolicyManager) getSystemService(Context.DEVICE_POLICY_SERVICE);
dpm.setApplicationRestrictions(EnforcerDeviceAdminReceiver.getComponentName(this), "com.paloaltonetworks.globalprotect", config);
```

**Example: Remove VPN Configuration**

```java
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);
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
> Configure HIP-Based Policy Enforcement
> Collect Application and Process Data From Endpoints
> Block Device Access
> Configure Windows User-ID Agent to Collect Host Information
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.

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?
- 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.

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.

While the GlobalProtect app collects a comprehensive amount of data about the host it is running on, you may require your end users to run additional software in order to connect to the network or access certain resources. In this case, you can define custom checks that instruct the app to collect specific registry information (on Windows endpoints), preference list (plist) information (on macOS endpoints), or information about whether or not specific services are running on the host.

By default, the app collects data about the following categories of information to help identify the security state of the host:

Table 7: Table: Data Collection Categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Data Collected</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>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.</td>
</tr>
</tbody>
</table>

For Windows endpoints’ domain, the GlobalProtect app collects the domain defined for
<table>
<thead>
<tr>
<th>Category</th>
<th>Data Collected</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ComputerNameDnsDomain</strong>, 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 &gt; Logs &gt; HIP Match).</td>
<td></td>
</tr>
<tr>
<td><strong>Mobile Device</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>To collect mobile device attributes and utilize them in HIP enforcement policies, GlobalProtect requires an MDM server. GlobalProtect currently supports HIP integration with the AirWatch MDM server.</strong></td>
</tr>
<tr>
<td></td>
<td>For devices managed by AirWatch, host information collected by the GlobalProtect app can be supplemented with additional information collected from the AirWatch service. Refer to Configure Windows User-ID Agent to Collect Host Information for a list of attributes that can be retrieved from AirWatch.</td>
</tr>
<tr>
<td><strong>Patch Management</strong></td>
<td>Information about any patch management software that is enabled and/or installed on the host and whether there are any missing patches.</td>
</tr>
<tr>
<td></td>
<td><strong>If you want to configure the Severity value for missing patches as a match condition in your HIP object (Objects &gt; GlobalProtect &gt; HIP Objects &gt; &lt;hip-object&gt; &gt; Patch Management &gt; Criteria), use the following mappings between the GlobalProtect severity values and the OPSWAT severity ratings to understand what each value means:</strong></td>
</tr>
</tbody>
</table>
|                   | - -2 — Not Available
|                   | - -1 — Unknown
|                   | 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
## Data Collected

<table>
<thead>
<tr>
<th>Category</th>
<th>Data Collected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk Backup</td>
<td>Information about whether disk backup software is installed, the last backup time, and the vendor and product name of the software.</td>
</tr>
<tr>
<td>Disk Encryption</td>
<td>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.</td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

### 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.

---

**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
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.

**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 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 or Mac) and then Add a process to the Process List. Enter the name of the process that you want the app to collect information about.

• 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.
8. Repeat step f and step g 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.

![Image of HIP Object](image.png)

Repeat this step for each category you want to match against in this object. For more information, see 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:
   - **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).
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 Mac OS systems) or TrueCrypt disk encryption (for Windows systems), belongs to the required Domain, and has a Symantec antivirus client installed:

![HIP Objects/Profiles Builder and HIP Profile](image)

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.
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 User tab, Add the HIP Profiles used to identify users (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 \( \text{rule eq 'iOS Apps'} \) in the filter text box as follows:

```
Receive Time | Type | From Zone | To Zone | Source | Source Leaf | Destination | To Port
-------------|------|----------|--------|--------|------------|-------------|--------
02/08 17:47:25 | end  | 15-trust | 15-untrust | 10.31.32.4 | PaloAltoNetworks | 17.154.66.16 | 443
02/08 17:47:25 | end  | 15-trust | 15-untrust | 10.31.32.4 | PaloAltoNetworks | 17.158.36.34 | 443
02/08 17:47:22 | end  | 15-trust | corp-vpn  | 10.31.32.30 | PaloAltoNetworks | 10.0.0.296 | 53
02/08 17:47:22 | end  | 15-trust | corp-vpn  | 10.31.32.30 | PaloAltoNetworks | 10.0.0.296 | 53
02/08 17:47:22 | end  | 15-trust | corp-vpn  | 10.31.32.30 | PaloAltoNetworks | 10.0.0.296 | 53
02/08 17:47:22 | end  | 15-trust | corp-vpn  | 10.31.32.30 | PaloAltoNetworks | 10.0.0.296 | 53
02/08 17:47:21 | end  | 15-trust | corp-vpn  | 10.31.32.30 | PaloAltoNetworks | 10.0.0.296 | 53
02/08 17:47:21 | end  | 15-trust | corp-vpn  | 10.31.32.30 | PaloAltoNetworks | 10.0.0.296 | 53
02/08 17:47:08 | end  | 15-trust | 15-untrust | 10.31.32.34 | PaloAltoNetworks | 107.20.172.241 | 443
02/08 17:47:08 | end  | 15-trust | 15-untrust | 10.31.32.34 | PaloAltoNetworks | 74.123.129.104 | 80
02/08 17:47:07 | end  | 15-trust | 15-untrust | 10.31.32.34 | PaloAltoNetworks | 17.167.103.105 | 443
02/08 17:47:07 | end  | 15-trust | 15-untrust | 10.31.32.34 | PaloAltoNetworks | 17.167.103.106 | 443
```
Collect Application and Process Data From Endpoints

The Windows Registry and macOS plist can be used to configure and store settings for Windows and Mac 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 or macOS 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). 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 connects.

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 and macOS 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.

For more information on defining app settings directly from the Windows Registry or the global macOS plist, see Deploy App Settings Transparently.

STEP 1 | Enable the GlobalProtect app to collect Windows Registry information from Windows endpoints or plist information from macOS 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, and then select an existing portal configuration or Add a new one.
2. On the Agent tab, select the agent configuration that you want to modify or Add a new one.
3. On the Data Collection tab, verify that Collect HIP Data is enabled.
4. 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, and then select an existing portal configuration or Add a new one.
2. On the Agent tab, select the agent configuration that you want to modify or Add a new one.
3. On the Data Collection tab, verify that Collect HIP Data is enabled.
4. 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:
Confirm that the **Plist** and **Key** are added to the Mac custom checks:

**STEP 2 | (Optional) Check if a specific process is running on the endpoint.**
1. Select Custom Checks > Windows or Mac (Network > GlobalProtect > Portals > <portal-config> > Agent > <agent-config> > Data Collection).
2. 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 | Verify that the GlobalProtect app is collecting the data defined in the custom check from the endpoint.**
For Windows endpoints:
1. Launch the GlobalProtect app for Windows endpoints by clicking the system tray icon. The GlobalProtect status panel opens.
2. Click the settings ( ) icon to open the settings menu.
3. Select **Settings** to open the GlobalProtect Settings panel.
4. Select the Host Profile tab to view the information that the GlobalProtect app is collecting from the endpoint. Verify that the custom-checks drop-down displays the data that you defined for collection.

For macOS endpoints:
1. Launch the GlobalProtect app for macOS endpoints by clicking the system tray icon. The GlobalProtect status panel opens.
2. Click the settings ( } icon to open the settings menu.
3. Select Settings to open the GlobalProtect Settings panel.
4. Select the Host Profile tab to view the information that the GlobalProtect app is collecting from the endpoint. Verify that the custom-checks drop-down displays the data you defined for collection.

STEP 5 | (Optional) Create a HIP Object to match to a Registry Key (Windows) or plist (macOS), 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 and macOS endpoints:
1. Select Objects > GlobalProtect > HIP Objects, and then Add a HIP Object.
2. 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. Select **Custom Checks > Plist (Objects > GlobalProtect > HIP Objects > <hip-object>)**, and then **Add** the plist for which you want to check macOS endpoints. 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. **(Optional)** To match traffic to a specific key-value pair within a plist, select a plist from **Custom Checks > Plist (Objects > GlobalProtect > HIP Objects > <hip-object>)**, 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.

**STEP 6 | (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 7 | 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.
Block Endpoint Access

In the event that a user loses an endpoint that provides GlobalProtect access to your network, that endpoint is stolen, or a user leaves your organization, you can block the endpoint from gaining access to the network by placing the endpoint in a block list.

A block list is local to a logical network location (vsys, 1 for example) and can contain a maximum of 1,000 endpoints per location. Therefore, you can create separate block lists for each location hosting a GlobalProtect deployment.

**STEP 1 | Identify the host ID for the endpoints you want to block.**

The host ID is a unique ID that GlobalProtect assigns to identify the host. 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:

1. Select **Monitor > Logs > HIP Match**.
2. Filter the HIP match logs for the source user associated with the endpoint.
3. Open the HIP match log and identify the host ID under **OS > Host ID** and optionally the hostname under **Host Information > Machine Name**.

**STEP 2 | Create a device block list.**
You cannot use Panorama templates to push a device block list to firewalls.

1. Select **Network > GlobalProtect > Device Block List** and **Add** a device block list.
2. Enter a descriptive **Name** for the list.
3. For a firewall with more than one virtual system (vsys), select the **Location** (vsys or Shared) where the profile is available.

**STEP 3 | Add a device to a block list.**

1. **Add** endpoints. Enter the host ID (required) and hostname (optional) for the endpoint that you need to block.
2. **Add** additional endpoints, if needed.
3. Click **OK** to save and activate the block list.

*The device block list does not require a commit and is immediately active.*
Configure Windows User-ID Agent to Collect Host Information

The Windows-based User-ID agent has been extended to support a new AirWatch 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 AirWatch. Running as part of the Windows-based User-ID agent, the AirWatch MDM integration service uses the AirWatch API to collect information from mobile endpoints that are managed by VMware AirWatch and translate this data into host information.

For Android endpoints managed by AirWatch, 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 AirWatch 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 AirWatch device information at regular intervals and push this information to the GlobalProtect gateways. In addition, the service can monitor AirWatch event notifications and fetch updated device information when AirWatch events (such as compliance changes) occur.

Information Collected

The following table shows how information collected from endpoints that are managed by AirWatch are translated into HIP report attributes. The mapping is done automatically.
<table>
<thead>
<tr>
<th>AirWatch Attributes</th>
<th>HIP Report Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Information</td>
<td></td>
</tr>
<tr>
<td>SerialNumber</td>
<td>serial-number</td>
</tr>
<tr>
<td>MacAddress</td>
<td>wifimac</td>
</tr>
<tr>
<td>Imei</td>
<td>IMEI</td>
</tr>
<tr>
<td>OperatingSystem</td>
<td>version</td>
</tr>
<tr>
<td>Model</td>
<td>model</td>
</tr>
<tr>
<td>DeviceFriendlyName</td>
<td>devname</td>
</tr>
<tr>
<td>IsSupervised</td>
<td>supervised</td>
</tr>
<tr>
<td>Udid (Unique Device Identifier)</td>
<td>udid</td>
</tr>
<tr>
<td>UserName</td>
<td>user</td>
</tr>
<tr>
<td>LastEnrolledOn</td>
<td>enroll-time</td>
</tr>
<tr>
<td>Platform</td>
<td>os</td>
</tr>
<tr>
<td>EnrollmentStatus</td>
<td>managed-by-mdm</td>
</tr>
<tr>
<td>LastSeen</td>
<td>last-checkin-time</td>
</tr>
<tr>
<td>ComplianceStatus</td>
<td>Compliant</td>
</tr>
<tr>
<td>(User-ID agent 8.0.3 and later)</td>
<td>NonCompliant</td>
</tr>
<tr>
<td></td>
<td>NotAvailable</td>
</tr>
<tr>
<td>Ownership</td>
<td>Employee Owned</td>
</tr>
<tr>
<td>(User-ID agent 8.0.3 and later)</td>
<td>Corporate-Dedicated</td>
</tr>
<tr>
<td></td>
<td>Corporate-Shared</td>
</tr>
<tr>
<td>Security Information</td>
<td></td>
</tr>
<tr>
<td>DataProtectionEnabled</td>
<td>disk-encrypted</td>
</tr>
<tr>
<td>IsPasscodePresent</td>
<td>passcode-set</td>
</tr>
<tr>
<td>IsPasscodeCompliant</td>
<td>passcode-compliant</td>
</tr>
<tr>
<td>Network Information</td>
<td></td>
</tr>
<tr>
<td>DataRoamingEnabled</td>
<td>data-roaming</td>
</tr>
<tr>
<td>GPS Coordinates</td>
<td></td>
</tr>
<tr>
<td>AirWatch Attributes</td>
<td>HIP Report Attributes</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Latitude</td>
<td>latitude</td>
</tr>
<tr>
<td>Longitude</td>
<td>longitude</td>
</tr>
<tr>
<td>SampleTime</td>
<td>last-location-time</td>
</tr>
</tbody>
</table>

**Application Details**

<table>
<thead>
<tr>
<th>ApplicationName</th>
<th>appname</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>version</td>
</tr>
<tr>
<td>ApplicationIndentifier</td>
<td>package</td>
</tr>
</tbody>
</table>

**System Requirements**

AirWatch MDM integration service requires the following software:

<table>
<thead>
<tr>
<th>Software</th>
<th>Minimum Supported Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-ID Agent</td>
<td>8.0.1</td>
</tr>
<tr>
<td>PAN-OS</td>
<td>7.1.0</td>
</tr>
<tr>
<td>GlobalProtect App for Android</td>
<td>4.0.0</td>
</tr>
<tr>
<td>GlobalProtect App for iOS</td>
<td>4.0.1</td>
</tr>
<tr>
<td>AirWatch Server</td>
<td>8.4.7.0</td>
</tr>
<tr>
<td>Windows Server</td>
<td>2008 and 2012</td>
</tr>
<tr>
<td></td>
<td>2016 with User-ID Agent 8.0.4 and PAN-OS 8.0.4</td>
</tr>
</tbody>
</table>

**Configure GlobalProtect to Retrieve Host Information**

Use the following instructions to configure GlobalProtect to retrieve host information from devices managed by AirWatch.

**STEP 1 | Install the User-ID Agent.** The User-ID agent must be in a location that enables secure connections to the VMware AirWatch Mobile Device Management (MDM) system.

The AirWatch 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 **AirWatch** for the **MDM Vendor**.

**STEP 4** | Specify the **MDM Event Notification** settings to monitor and collect AirWatch 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 AirWatch 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 AirWatch 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 AirWatch server. Contact your AirWatch Support team for guidance on which IP addresses to specify.

STEP 5 | Add MDM API Authentication settings to connect with the AirWatch API.
• Enter the Server Address of the AirWatch 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 AirWatch MDM API.
• Enter the Tenant Code. This is a unique hexadecimal code number required to access the AirWatch MDM API. On the AirWatch 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 AirWatch. 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 AirWatch API.

STEP 8 | Configure the GlobalProtect gateway to communicate with the MDM integration service to retrieve the HIP reports for the devices managed by AirWatch.

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 AirWatch 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 AirWatch 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 AirWatch.
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 AirWatch REST API.

- **Event notifications from the AirWatch 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 Airwatch REST API is unsuccessful.**
  Make sure that:
  
  - The credentials used for the MDM integration service to authenticate to the AirWatch MDM service are valid.
  - The user account used to access the Airwatch REST API has API access permissions and read-only permissions (at minimum) to data for the mobile devices and users managed by AirWatch.
  - The **Tenant Code** (API key) is correctly associated with the user account. Remove all unused API keys.
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
- Live KB: Active Directory Password Changes
Remote Access VPN (Authentication Profile)

In the 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.

Watch the video.

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 13-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 tunnel2 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 13-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)—13-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 Software.

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. 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 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 **13-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 | 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 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 Software.**
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 authenticate 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 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

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 **13-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 **13-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)**—**13-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 | 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).

![LDAP Server Profile](image)

**STEP 7 | (Optional) Create an authentication profile.**

Attach the server profile to an authentication profile (Device > Authentication Profile).

![Authentication Profile](image)

**STEP 8 | Configure a GlobalProtect Gateway.**

See the topology diagram shown in 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
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 Software.

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 in the trust zone, 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, such as DHCP, DNS, Active Directory (for example, to change an expired password), 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).

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 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. Add a rule that enables pre-logon users access to basic services that are required for the endpoint to come up, such as authentication services, DNS, DHCP, and Microsoft Updates.
2. **Add** a rule to deny pre-logon users access to all other destinations and applications.
3. **Add** any additional rules to enable different users or user groups access to specific destinations 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 the 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).

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 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.

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 this 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 a device (for example, a headless device), 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 additional settings such as the default portal IP address and connect method.

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. In the Value data field, create a DWORD named **Prelogon** with a value of 1, and set the Base to Hexadecimal. This setting enables GlobalProtect to initiate a connection before the user logs in to the endpoint.

3. Create a String Value named **Portal** that specifies the IP address or hostname of the default portal for the GlobalProtect endpoint.

4. Create a String Value named **connect-method** with a value of **pre-logon**. This setting enables GlobalProtect to initiate a VPN tunnel before a user logs in to the endpoint and connects to the GlobalProtect portal.
GlobalProtect Multiple Gateway Configuration

In the 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 13-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 13-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:
   
   ![License Activation](image)

**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 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 Agent Software.

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](image)

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.

![HIP Object](image1)

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:

![HIP Profile](image2)

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 Software.**

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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Tag</th>
<th>Source Zone</th>
<th>Source Address</th>
<th>User</th>
<th>HIP Profile</th>
<th>Destination Zone</th>
<th>Destination Address</th>
<th>Application</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM access</td>
<td>mana</td>
<td>l3-trust</td>
<td>any</td>
<td>Finance</td>
<td>MissingPatch</td>
<td>l3-trust</td>
<td>any</td>
<td>tap</td>
<td>application-default</td>
<td></td>
</tr>
<tr>
<td>Eng access</td>
<td>mana</td>
<td>l3-trust</td>
<td>any</td>
<td>Engineering</td>
<td>MissingPatch</td>
<td>l3-trust</td>
<td>any</td>
<td>bugzilla</td>
<td>application-default</td>
<td></td>
</tr>
</tbody>
</table>

| CRM access | mana  | l3-trust    | any            | Finance | MissingPatch | l3-trust         | any  | tap     | application-default |
| Eng access | mana  | l3-trust    | any            | Engineering | MissingPatch | l3-trust         | any  | bugzilla | application-default |

| CRM access | mana  | l3-trust    | any            | Finance | MissingPatch | l3-trust         | any  | tap     | application-default |
| Eng access | mana  | l3-trust    | any            | Engineering | MissingPatch | l3-trust         | any  | bugzilla | 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.
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 Best Practices for Securing Administrative Access 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 13-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 13-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**—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:**
   - **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 Software.**

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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Tags</th>
<th>Zone</th>
<th>Address</th>
<th>User</th>
<th>HIP Profile</th>
<th>Zone</th>
<th>Address</th>
<th>Application</th>
<th>Service</th>
<th>Action</th>
<th>Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>none</td>
<td>corp-vpn</td>
<td>any</td>
<td>Finance</td>
<td>Missing Patch</td>
<td>l3-trust</td>
<td>any</td>
<td>sap</td>
<td>application-default</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>none</td>
<td>corp-vpn</td>
<td>any</td>
<td>Engineering</td>
<td>Missing Patch</td>
<td>l3-trust</td>
<td>any</td>
<td>telnet</td>
<td>application-default</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>none</td>
<td>corp-vpn</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>l3-untrust</td>
<td>any</td>
<td>web-browsing</td>
<td>application-default</td>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>

**STEP 10 | Save the GlobalProtect configuration.**

**Commit** your portal and gateway configurations.
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 Reference Architecture Features
> GlobalProtect Reference Architecture Configurations
GlobalProtect Reference Architecture Topology

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** on page 309
- **Management and Logging** on page 309
- **Monitoring and High Availability** on page 310

### 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** on page 311
- **Portal Configuration** on page 311
- **Policy Configurations** on page 311

**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 on page 74.
- Enable **No direct access to local network** in **Agent > Client Settings > Split Tunnel**. See Configure a GlobalProtect Gateway on page 74.
- Enable the gateway to **Accept cookie for authentication override**. See Configure a GlobalProtect Gateway on page 74.

**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
- Cipher Exchange Between the GlobalProtect Agent and Gateway
- GlobalProtect Cryptography References
- Ciphers Used to Set Up IPSec Tunnels
- SSL APIs
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 8: Cipher Exchange Between the App and Gateway

<table>
<thead>
<tr>
<th>Communication Stage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Client Hello</td>
<td>The app proposes a list of cipher suites depending on the OS of the endpoint.</td>
</tr>
<tr>
<td>2. Server Hello</td>
<td>The gateway selects the cipher suite proposed by the app. When selecting the ciphers to set up the tunnel, the gateway ignores both the number and order of cipher suites proposed by the app and instead relies on the SSL/TLS</td>
</tr>
</tbody>
</table>
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 9: Example: Cipher Exchange for Mac Endpoints**

<table>
<thead>
<tr>
<th>Communication Stage</th>
<th>Example: Mac Endpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Client Hello</td>
<td>TLS 1.2</td>
</tr>
<tr>
<td></td>
<td>37 Cipher Suites</td>
</tr>
<tr>
<td></td>
<td>(Reference: TLS Ciphers Supported by GlobalProtect Apps on macOS Endpoints)</td>
</tr>
<tr>
<td>2. Server Hello</td>
<td>• When GlobalProtect uses an ECDSA certificate and TLS 1.2 is accepted, the SSL session uses ECDSA-AES256-CBC-SHA.</td>
</tr>
<tr>
<td></td>
<td>• When GlobalProtect uses an RSA certificate and TLS 1.2 is accepted, the SSL session uses RSA-AES256-CBC-SHA256.</td>
</tr>
<tr>
<td>3. Optional Client Certificate</td>
<td>Client certificates signed with ECDSA or RSA and using SHA1, SHA256, or SHA384</td>
</tr>
<tr>
<td>4. SSL Session</td>
<td>• SSL Session uses ECDSA-AES256-CBC-SHA or RSA-AES256-CBC-SHA256</td>
</tr>
<tr>
<td></td>
<td>• Get-Config-Request</td>
</tr>
<tr>
<td></td>
<td>• Encryption—AES-256-GCM, AES-128-GCM, AES-128-CBC</td>
</tr>
<tr>
<td></td>
<td>• Authentication—SHA1 and OS type, Preferred IP address etc</td>
</tr>
<tr>
<td></td>
<td>• Get-Config-Response</td>
</tr>
<tr>
<td></td>
<td>• Client to server, and server to client SPIs, encryption keys, and authentication keys</td>
</tr>
<tr>
<td></td>
<td>• Tunnel type, ports, split tunnel mode, IP, and DNS etc</td>
</tr>
</tbody>
</table>
GlobalProtect Cryptography References

- Reference: GlobalProtect App Cryptographic Functions
- TLS Cipher Suites Supported by GlobalProtect Apps
- TLS Cipher Suites Supported by GlobalProtect Gateways in PAN-OS 8.1

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:

<table>
<thead>
<tr>
<th>Crypto Function</th>
<th>Key</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Winhttp (Windows) and NSURLConnection (macOS)</td>
<td>aes256-sha</td>
<td>Dynamic key negotiated between the GlobalProtect app and the GlobalProtect portal and/or gateway for establishing the HTTPS connection.</td>
</tr>
<tr>
<td>OpenSSL</td>
<td>aes256-sha</td>
<td>Dynamic key negotiated between the GlobalProtect app and the GlobalProtect gateway during the SSL handshake.</td>
</tr>
<tr>
<td>IPSec encryption and authentication</td>
<td>aes-128-sha1, aes-128-cbc, aes-128-gcm, and aes-256-gcm</td>
<td>The session key sent from the GlobalProtect gateway.</td>
</tr>
</tbody>
</table>

Used to establish the HTTPS connection between the GlobalProtect app and the GlobalProtect portal and GlobalProtect gateway for authentication.

Used to establish the SSL connection between the GlobalProtect app and the GlobalProtect gateway for HIP report submission, SSL tunnel negotiation, and network discovery.

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 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.

- Reference: TLS Ciphers Supported by GlobalProtect Agents on Mac Endpoints
- Reference: TLS Ciphers Supported by GlobalProtect Agents on Windows 7 Endpoints
- Reference: TLS Ciphers Supported by GlobalProtect Agents on Android 6.0.1 Endpoints
- Reference: TLS Ciphers Supported by GlobalProtect Agents on iOS 10.2.1 Endpoints
- Reference: TLS Ciphers Supported by GlobalProtect Agents on Chromebooks

Reference: TLS Ciphers Supported by GlobalProtect Apps on macOS Endpoints

<table>
<thead>
<tr>
<th>TLS Ciphers Supported by GlobalProtect Apps on macOS Endpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_EMPTY_RENEGOTIATION_INFO_SCSV        (0x00ff)</td>
</tr>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)</td>
</tr>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)</td>
</tr>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA   (0xc00a)</td>
</tr>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA   (0xc009)</td>
</tr>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA  (0xc008)</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384  (0xc028)</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256  (0xc027)</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA     (0xc014)</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA     (0xc013)</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA    (0xc012)</td>
</tr>
<tr>
<td>TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)</td>
</tr>
<tr>
<td>TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)</td>
</tr>
<tr>
<td>TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA    (0xc005)</td>
</tr>
<tr>
<td>TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA    (0xc004)</td>
</tr>
<tr>
<td>TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384   (0xc02a)</td>
</tr>
<tr>
<td>TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256   (0xc029)</td>
</tr>
<tr>
<td>TLS_ECDH_RSA_WITH_AES_256_CBC_SHA     (0xc00f)</td>
</tr>
<tr>
<td>TLS_ECDH_RSA_WITH_AES_128_CBC_SHA     (0xc00e)</td>
</tr>
<tr>
<td>TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA    (0xc00d)</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_256_CBC_SHA256   (0xc006b)</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_128_CBC_SHA256   (0xc0067)</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_256_CBC_SHA      (0xc0039)</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_128_CBC_SHA      (0xc0033)</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA    (0xc0016)</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_256_CBC_SHA256       (0xc003d)</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_128_CBC_SHA256       (0xc003c)</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_256_CBC_SHA         (0xc0035)</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_128_CBC_SHA         (0xc002f)</td>
</tr>
<tr>
<td>TLS_RSA_WITH_3DES_EDE_CBC_SHA        (0xc00a)</td>
</tr>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_RC4_128_SHA     (0xc007)</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_RC4_128_SHA       (0xc011)</td>
</tr>
</tbody>
</table>
### TLS Ciphers Supported by GlobalProtect Apps on macOS Endpoints

<table>
<thead>
<tr>
<th>Cipher Suite</th>
<th>Reference: TLS Ciphers Supported by GlobalProtect Apps on Windows 7 Endpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc003)</td>
<td></td>
</tr>
<tr>
<td>TLS_ECDH_ECDSA_WITH_RC4_128_SHA (0xc002)</td>
<td></td>
</tr>
<tr>
<td>TLS_ECDH_RSA_WITH_RC4_128_SHA (0xc00c)</td>
<td></td>
</tr>
<tr>
<td>TLS_RSA_WITH_RC4_128_SHA (0x0005)</td>
<td></td>
</tr>
<tr>
<td>TLS_RSA_WITH_RC4_128_MD5 (0x0004)</td>
<td></td>
</tr>
</tbody>
</table>

### Reference: TLS Ciphers Supported by GlobalProtect Apps on Windows 7 Endpoints

<table>
<thead>
<tr>
<th>Cipher Suite</th>
<th>Reference: TLS Ciphers Supported by GlobalProtect Apps on Windows 7 Endpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)</td>
<td></td>
</tr>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)</td>
<td></td>
</tr>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)</td>
<td></td>
</tr>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)</td>
<td></td>
</tr>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)</td>
<td></td>
</tr>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc014)</td>
<td></td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)</td>
<td></td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_256_CBC_SHA (0x003c)</td>
<td></td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Cipher Suite</th>
<th>Reference: TLS Ciphers Supported by GlobalProtect Apps on Windows 7 Endpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)</td>
<td></td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc027)</td>
<td></td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)</td>
<td></td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_256_CBC_SHA (0x003c)</td>
<td></td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)</td>
<td></td>
</tr>
</tbody>
</table>
## TLS Ciphers Supported by GlobalProtect Apps on Android 6.0.1 Endpoints

<table>
<thead>
<tr>
<th>Cipher Suite</th>
<th>Hex Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</td>
<td>0xc02f</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384</td>
<td>0xc030</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_128_GCM_SHA256</td>
<td>0x009e</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_256_GCM_SHA384</td>
<td>0x009f</td>
</tr>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA</td>
<td>0xc009</td>
</tr>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_AES_1256_CBC_SHA</td>
<td>0xc00a</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA</td>
<td>0xc013</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA</td>
<td>0xc014</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_128_GCM_SHA256</td>
<td>0x009c</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_256_GCM_SHA384</td>
<td>0x009d</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_128_CBC_SHA</td>
<td>0x0039</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_256_CBC_SHA</td>
<td>0x0035</td>
</tr>
<tr>
<td>TLS_RSA_WITH_RC4_128_SHA</td>
<td>0x0005</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Cipher Suite</th>
<th>Hex Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_EMPTY_RENEGOTIATION_INFO_SCSV</td>
<td>0x00ff</td>
</tr>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384</td>
<td>0xc02c</td>
</tr>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</td>
<td>0xc02b</td>
</tr>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384</td>
<td>0xc024</td>
</tr>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA</td>
<td>0xc023</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA</td>
<td>0xc014</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_256_GCM_SHA384</td>
<td>0x0039</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_128_GCM_SHA256</td>
<td>0x0035</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_256_CBC_SHA</td>
<td>0x0035</td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_128_CBC_SHA</td>
<td>0x0005</td>
</tr>
</tbody>
</table>
Reference: TLS Ciphers Supported by GlobalProtect Apps on Chromebooks

The GlobalProtect app for Chrome OS 55.0.2883 supports 91 cipher suites.

<table>
<thead>
<tr>
<th>TLS Ciphers Supported by GlobalProtect Apps on Chromebooks (Chrome OS 55.0.2883)</th>
<th>TLS DH DSS WITH CAMELLIA 256_CBC_SHA (0x0085)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)</td>
<td>TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA (0x0085)</td>
</tr>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)</td>
<td>TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032)</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)</td>
<td>TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e)</td>
</tr>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)</td>
<td>TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)</td>
</tr>
<tr>
<td>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)</td>
<td>TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)</td>
</tr>
<tr>
<td>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)</td>
<td>TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)</td>
</tr>
<tr>
<td>TLS_DH_DSS_WITH_AES_256_GCM_SHA384 (0x00a5)</td>
<td>TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)</td>
</tr>
<tr>
<td>TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (0x00a3)</td>
<td>TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)</td>
</tr>
<tr>
<td>TLS_DH_RSA_WITH_AES_256_GCM_SHA384 (0x00a1)</td>
<td>TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)</td>
<td>TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)</td>
</tr>
<tr>
<td>TLS_DH_RSA_WITH_AES_256_CBC_SHA256 (0x006b)</td>
<td>TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0084)</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006a)</td>
<td>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)</td>
</tr>
<tr>
<td>TLS_DH_RSA_WITH_AES_256_CBC_SHA256 (0x0069)</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x0068)</td>
<td>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)</td>
</tr>
<tr>
<td>TLS_DH_RSA_WITH_AES_256_CBC_SHA (0x0039)</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0038)</td>
<td>TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc013)</td>
</tr>
<tr>
<td>TLS_DH_RSA_WITH_AES_256_CBC_SHA (0x0037)</td>
<td>TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc009)</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0036)</td>
<td>TLS_DH_DSS_WITH_AES_128_GCM_SHA256 (0x00a4)</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0088)</td>
<td>TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 (0x00a2)</td>
</tr>
<tr>
<td>TLS_CIPHER聩</td>
<td>TLS_CIPHER聩</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA (0x0087)</td>
<td>TLS_DH_RSA_WITH_AES_128_GCM_SHA256 (0x00a0)</td>
</tr>
<tr>
<td>TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0086)</td>
<td>TLS_DH_RSA_WITH_AES_128_GCM_SHA256 (0x009e)</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0040)</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)</td>
</tr>
<tr>
<td>TLS_DH_RSA_WITH_AES_128_CBC_SHA256 (0x003f)</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA (0x0096)</td>
</tr>
<tr>
<td>TLS_DH_DSS_WITH_AES_128_CBC_SHA256 (0x003e)</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA (0x0032)</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA (0x0031)</td>
</tr>
<tr>
<td>TLS_DH_RSA_WITH_AES_128_CBC_SHA (0x0030)</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA (0x0030)</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x009a)</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x0099)</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)</td>
</tr>
<tr>
<td>TLS_DH_RSA_WITH_SEED_CBC_SHA (0x0098)</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)</td>
</tr>
<tr>
<td>TLS_DH_DSS_WITH_SEED_CBC_SHA (0x0097)</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)</td>
</tr>
<tr>
<td>TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0045)</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)</td>
</tr>
<tr>
<td>TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0044)</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)</td>
</tr>
<tr>
<td>TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0043)</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)</td>
</tr>
<tr>
<td>TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA (0x0042)</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)</td>
</tr>
<tr>
<td>TLS_ECDH_RSA WITH_AES_128_GCM_SHA256 (0xc031)</td>
<td>TLS_ECDH_RSA WITH_AES_128_GCM_SHA256 (0xc031)</td>
</tr>
<tr>
<td>TLS_ECDH_ECDSA WITH_AES_128_GCM_SHA256 (0xc02d)</td>
<td>TLS_ECDH_RSA WITH_AES_128_GCM_SHA256 (0xc02d)</td>
</tr>
<tr>
<td>TLS_ECDH_RSA WITH_AES_128_CBC_SHA256 (0xc029)</td>
<td>TLS_ECDH_RSA WITH_AES_128_CBC_SHA256 (0xc029)</td>
</tr>
<tr>
<td>TLS_DH_RSA_WITH_AES_128_CBC_SHA (0x000f)</td>
<td>TLS_DH_RSA WITH_AES_128_CBC_SHA (0x000f)</td>
</tr>
<tr>
<td>TLS_DH_RSA WITH_AES_128_CBC_SHA (0x000e)</td>
<td>TLS_DH_RSA WITH_AES_128_CBC_SHA (0x000e)</td>
</tr>
<tr>
<td>TLS_DH_RSA WITH_AES_128_CBC_SHA (0x000d)</td>
<td>TLS_DH_RSA WITH_AES_128_CBC_SHA (0x000d)</td>
</tr>
<tr>
<td>TLS_DH_RSA WITH_AES_128_CBC_SHA (0x000c)</td>
<td>TLS_DH_RSA WITH_AES_128_CBC_SHA (0x000c)</td>
</tr>
</tbody>
</table>
### TLS Ciphers Supported by GlobalProtect Apps on Chromebooks (Chrome OS 55.0.2883)

<table>
<thead>
<tr>
<th>Cipher Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)</td>
<td></td>
</tr>
<tr>
<td>TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)</td>
<td></td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)</td>
<td></td>
</tr>
<tr>
<td>TLS_RSA_WITH_DES_CBC_SHA (0x0009)</td>
<td></td>
</tr>
<tr>
<td>TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)</td>
<td></td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_128_CBC_SHA (0xc00e)</td>
<td></td>
</tr>
<tr>
<td>TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)</td>
<td></td>
</tr>
<tr>
<td>TLS_RSA_WITH_DES_CBC_SHA (0x0009)</td>
<td></td>
</tr>
<tr>
<td>TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)</td>
<td></td>
</tr>
</tbody>
</table>
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.