Palo Alto Networks

Common Criteria Evaluated Configuration Guide

(CCECG)

GlobalProtect 6 App

Revision Date: June 28, 2023

Table of Contents

Introduction

The GlobalProtect App enables users with this software installed on their Windows, Linux, Android, iOS, or macOS computer/mobile to access their corporate network using secured protocols. This document provides details on how to place the GlobalProtect App in FIPS-CC mode so that Approved algorithms and key sizes are used to protect sensitive data between the endpoint and network.

Document Purpose and Scope

This document provides administrative guidance for the GlobalProtect App and is a supplement to the Palo Alto Networks GlobalProtect App Administrator's Guide Version 6.0. This document describes procedures on how to operate and prepare the GlobalProtect App to meet its Common Criteria evaluated configuration, and is referred to as the operational user guide in the Application Software Protection Profile v1.4 and Functional Package for Transport Layer Security v1.1 that meets all the required guidance assurance activities from the AppSWPP and PKGTLS.

The Palo Alto Networks System documentation set includes online help and PDF files.

The following product guidance documents are provided online or by request:

- GlobalProtect App User Guide Version 6.0, Last Revised: See link below
  https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/globalprotect/6-0/globalprotect-app-user-guide/globalprotect-app-user-guide.pdf

- Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG) for GlobalProtect 6 App [This Document]

The most up-to-date versions of the documentation can be accessed on the Palo Alto Networks Support web site (https://support.paloaltonetworks.com) or Technical Documentation (https://www.paloaltonetworks.com/documentation).

Scope of Evaluation

The scope of evaluation only covers security functionalities specified by Protection Profile for Application Software and Functional Package for Transport Layer Security. The security functions tested are outlined in the Security Target (ST), and these functions include TLS trusted channels, X509 authentication, certificate validation and signature checking.

TOE Identification

- Windows
  - GlobalProtect64-6.0.7.msi
- macOS
  - GlobalProtect-6.0.7.pkg
- Android
  - global-protect-6.0.7-signed.apk
- iOS
  - GlobalProtect App downloaded from iTunes Store

- Linux Ubuntu
    - PanGPLinux-6.0.7.tgz

Software Download and Installation

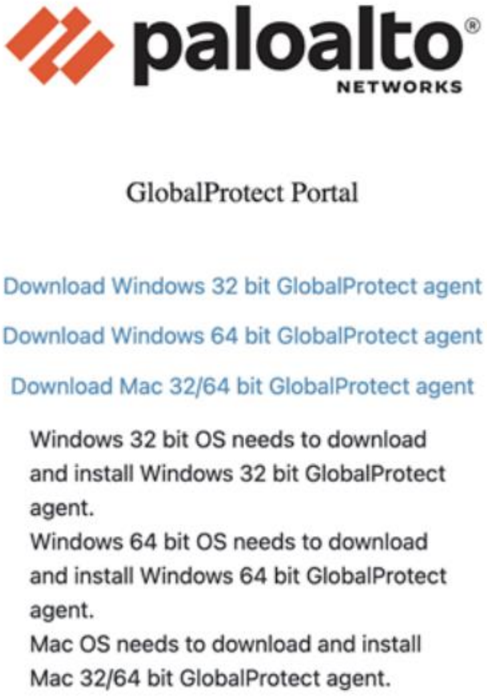
Download

Operators can download the official version of the evaluated GlobalProtect App via Palo Alto Network's support site (https://support.paloaltonetworks.com).

Navigate to the desired type (e.g., macOS, Windows, etc.) and download the file that corresponds to the evaluated version. A checksum is noted on the support site that can be used to verify the correct software once it has been downloaded.

Alternatively, the app can be downloaded by logging into the GlobalProtect portal via the following steps:

1. Launch a web browser and go the following URL:
    a. https://<portal_address>/<IP address or FQDN>
    b. Enter your username and password
2. Navigate to the app download page, and download the evaluated version 6.0. Note: Steps are the same for Mac/Windows/Linux
3. On mobile devices such as IOS or Android, you can push it from the MDM or download it directly from the App Store.



GlobalProtect Portal

Download Windows 32 bit GlobalProtect agent

Download Windows 64 bit GlobalProtect agent

Download Mac 32/64 bit GlobalProtect agent

Windows 32 bit OS needs to download and install Windows 32 bit GlobalProtect agent.
Windows 64 bit OS needs to download and install Windows 64 bit GlobalProtect agent.
Mac OS needs to download and install Mac 32/64 bit GlobalProtect agent.

Figure 1 - GlobalProtect Download

Installation

Follow the procedures below to place the TOE in the proper CC evaluated configuration. In FIPS-CC mode, only the Approved cryptographic module (OpenSSL FIPS canister engine) is utilized to perform all cryptographic functions and operations. Enabling FIPS-CC mode will restrict the scheme to ECC and the curve sizes to P-256, P-384, and P-521 only.

Note to Windows Users: To run GlobalProtect app 6.0 and later, Windows endpoints require Visual C++ Redistributables 12.0.3 for Visual Studio 2013. If you have not already installed any redistributable packages on your endpoint, the GlobalProtect app installs Visual C++ Redistributables 12.0.3 automatically. If you have already installed Visual C++ Redistributables 12.0.2 or an earlier release, you must either uninstall the existing redistributable packages from your endpoint or upgrade to Visual C++ Redistributables 12.0.3 prior to installing the GlobalProtect app.

Windows

1. Download the GlobalProtect app installation file.
2. When prompted, **Run** the software.
3. When prompted again, **Run** the GlobalProtect Setup Wizard.
4. Follow the instructions to select or accept the default installation folder.
5. After installation is complete, **Close** the wizard.
6. Specify your portal address and enter your credentials when prompted to begin the connection process.

Mac

1. Click on **Download Mac 32/64 GlobalProtect agent**.
2. When prompted, **Run** the software.
3. When prompted again, **Run** the GlobalProtect Installer.
4. Complete the GlobalProtect app setup using the GlobalProtect Installer.
5. Specify your portal address and enter your credentials when prompted to begin the connection process.

iOS

1. Launch the App Store.
2. **Search** for **GlobalProtect**.
3. From the research results, select **GlobalProtect**™.
4. From the GlobalProtect app product page, tap **GET**.
5. **Install** the app.
6. When prompted, **Sign In** with Apple ID.
7. Specify your portal address and enter your credentials when prompted to begin the connection process.

Android

1. Launch Google Play.
2. **Search** for **GlobalProtect**.
3. From the search results, select **GlobalProtect**.
4. From the GlobalProtect app product page, tap **Install**.
5. When prompted, review and **Accept** the information for which GlobalProtect needs access.
6. Specify your portal address and enter your credentials when prompted to begin the connection process.

Linux

1. Log in to the Customer Support Portal.
2. Select **Updates > Software Updates**.
3. Filter by GlobalProtect Agent for Linux, and download the associated TGZ file.
4. Extract the files from the package (e.g., tar -xvf ~/pkgs/PanGPLinux-6.0.0.tgz).
5. You will see multiple installation packages for supported operating system versions— DEB for Debian and Ubuntu and RPM for CentOS and Red Hat. The package for the GUI version is denoted by a GlobalProtect_UI prefix.

6. Install the GUI version of the GlobalProtect app for Linux. For Debian and Ubuntu, use the **sudo apt-get install <gp-app-pkg>** command. where <gp-app-pkg> is the path of the UI distribution package for your Linux version. For CentOS and Red Hat, use the **sudo yum install -y <gp-app-pkg>** command.
7. After installation completes, the GlobalProtect app automatically launches. Specify your portal address and enter your credentials when prompted to begin the connection process.

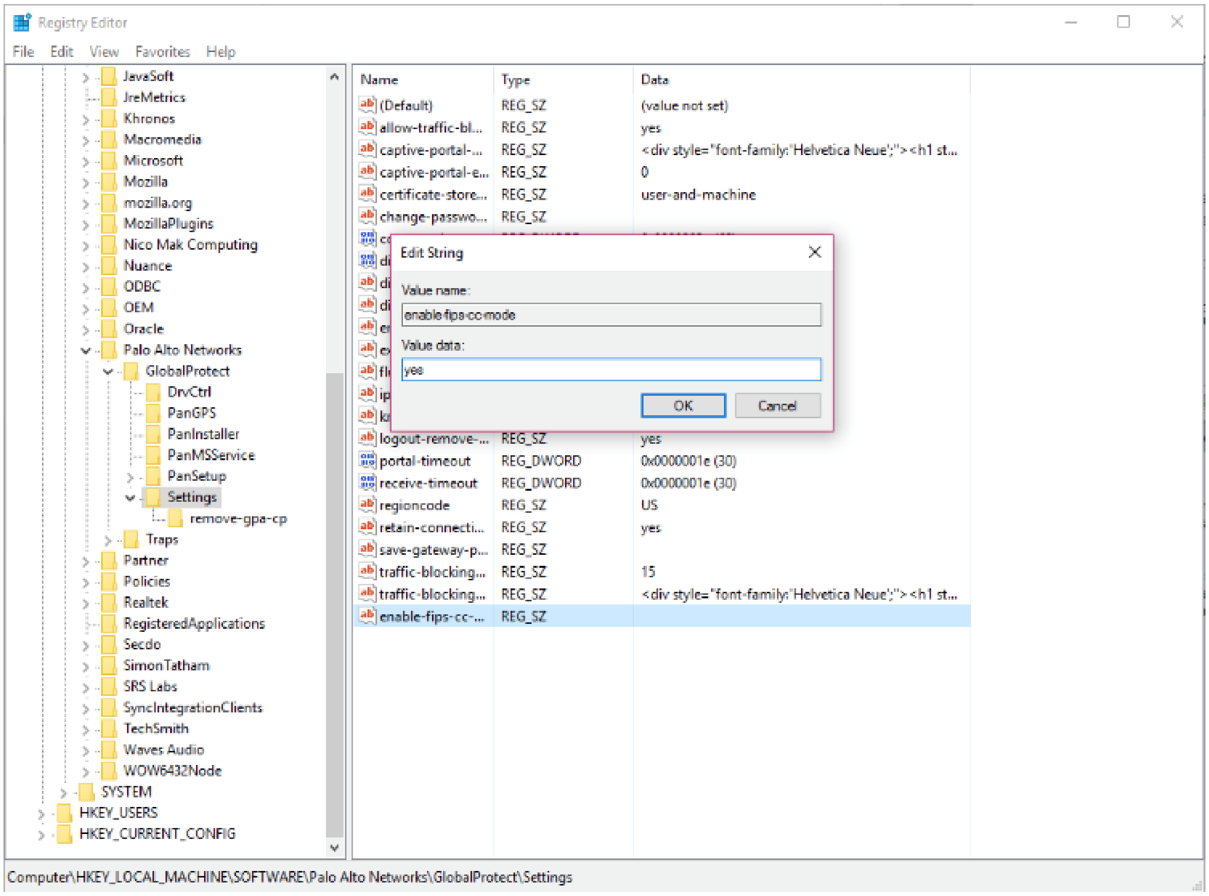
Enable FIPS-CC on Windows Platform

To enable FIPS-CC mode for GlobalProtect, you must first enable FIPS mode for the Windows 10 Operating system to ensure that your Windows endpoint is running in the FIPS compliant manner.

1. Launch the Command Prompt (run as Administrator)
2. Enter **regedit** to open the Windows Registry
3. In the Windows Registry, go to: HKEY_LOCAL_MACHINES\System\ConcurrentControlSet\Control\Lsa\FipsAlgorithmPolicy\
4. Right-click the **Enabled** registry value and then select **Modify**
5. To enable FIPS mode, set the **Value Data** to 1. The default value of 0 indicates that FIPS mode is disabled
6. Click **OK**
7. Restart the endpoint

Once Windows has been placed into FIPS mode, complete the process by performing the following steps:

1. Launch the Command Prompt (run as Administrator)
2. Enter **regedit** to open the Windows Registry
3. In the Windows Registry, go to: HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\
4. Click **Edit** and then select **New > String Value**
5. When prompted, set the **Name** of the new registry value to **enable-fips-cc-mode**
6. Right-click the new registry and then select **Modify** it
7. To enable FIPS-CC mode, set the **Value Data** to **yes**
8. Click **OK**



Name	Type	Data
(Default)	REG_SZ	(value not set)
allow-traffic-bl...	REG_SZ	yes
captive-portal-...	REG_SZ	<div style="font-family:'Helvetica Neue';"><h1 st...
captive-portal-e...	REG_SZ	0
certificate-store...	REG_SZ	user-and-machine
change-passwo...	REG_SZ	
co		
di		
di		
di		
er		
ex		
fl		
ip		
lo		
logout-remove-...	REG_SZ	yes
portal-timeout	REG_DWORD	0x0000001e (30)
receive-timeout	REG_DWORD	0x0000001e (30)
regioncode	REG_SZ	US
retain-connecti...	REG_SZ	yes
save-gateway-p...	REG_SZ	
traffic-blocking...	REG_SZ	15
traffic-blocking...	REG_SZ	<div style="font-family:'Helvetica Neue';"><h1 st...
enable-fips-cc-...	REG_SZ	

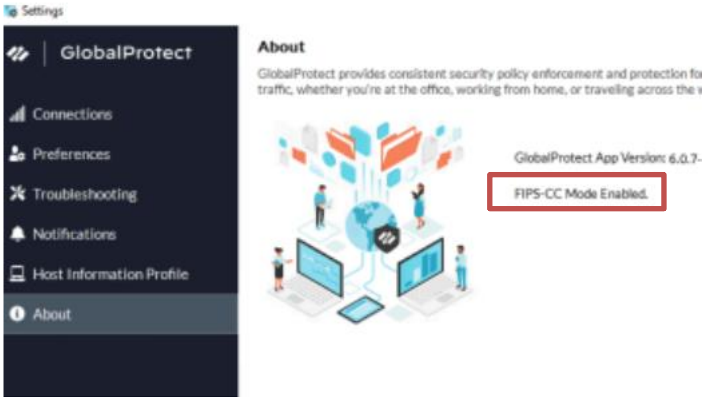
Value name: enable-fips-cc-mode

Value data: yes

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings

Figure 2 - Enabling FIPS-CC Mode on GlobalProtect App on Windows

9. Restart the GlobalProtect service
   - Launch the Command Prompt
   - Enter **services.msc** to open the Windows Services manager
   - From the Services list, select **PanGPS**
   - **Restart** the service
10. Verify that FIPS-CC mode is enabled on your GlobalProtect App
    - Launch GlobalProtect App
    - From the status panel, open the settings dialog (⚙)
    - Select **About**
    - Verify that FIPS-CC mode is enabled. If FIPS-CC mode is enabled, the About dialog displayed the “FIPS-CC Mode Enabled” status.
    - Reboot the system



About

GlobalProtect provides consistent security policy enforcement and protection fo traffic, whether you're at the office, working from home, or traveling across the

GlobalProtect App Version: 6.0.7-

FIPS-CC Mode Enabled.

Figure 3 - FIPS-CC Mode Enabled Status Indicator

Enable FIPS-CC Mode on macOS Platform

For the GlobalProtect app running on macOS, complete the steps below. To enable FIPS-CC mode for GlobalProtect, your macOS endpoint must be FIPS 140-2 compliant. By default, FIPS mode for the Mac operating system is automatically enabled on endpoints running macOS 10.8 and later releases.

1. Launch a plist editor, such as Xcode.
2. In the plist editor, open the following plist file:
   /Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist
3. Locate the GlobalProtect Settings dictionary: /Palo Alto Networks/GlobalProtect/Settings
   - Note: If the Settings dictionary does not exist, create it by connecting GP to any portal.
4. Enable FIPS-CC mode for GlobalProtect by adding the following key-value pair in the Settings dictionary:

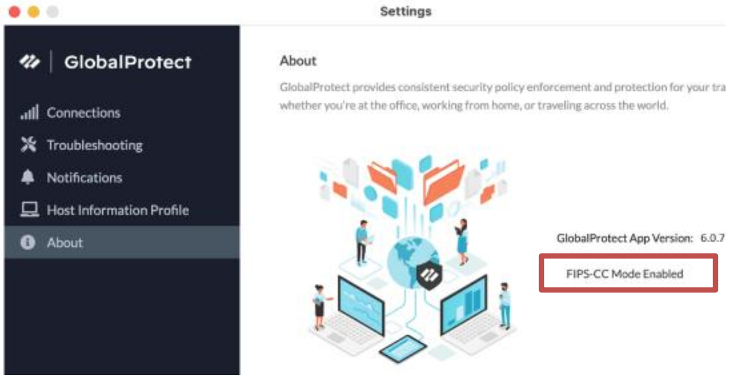
   ```
   <key>enable-fips-cc-mode</key>
   <string>yes</string>
   ```

5. Restart the GlobalProtect service by one of the following methods:
   - Reboot your endpoint
     - Launch Finder
     - From the Finder sidebar, select Applications
     - Open the Utilities folder
     - Open Activity Monitor
     - Stop the PanGPS service
   - Restart the GlobalProtect application and GlobalProtect service (PanGPS)
     - Launch Terminal
     - Execute the following commands:

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

Once complete, you can verify that FIPS-CC mode is enabled via the following steps:

1. Launch GlobalProtect App
2. From the status panel, open the settings dialog (⚙)
3. Select About
4. Verify that FIPS-CC mode is enabled. If FIPS-CC mode is enabled, the About dialog displayed the “FIPS-CC Mode Enabled” status.



About

GlobalProtect provides consistent security policy enforcement and protection for your tra
whether you're at the office, working from home, or traveling across the world.

GlobalProtect App Version: 6.0.7

FIPS-CC Mode Enabled

Figure 4 – FIPS-CC Mode Indicator on macOS Platform

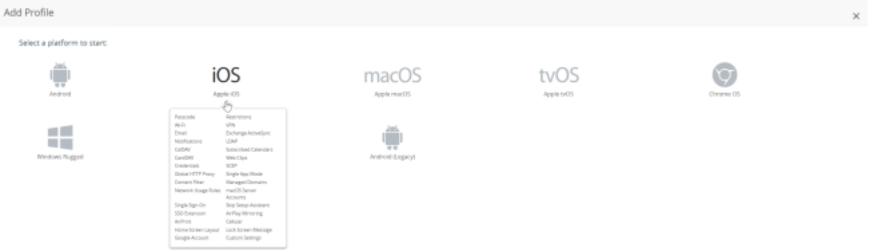
Enable FIPS-CC on iOS Endpoint Using Workspace ONE

To enable FIPS-CC mode for GlobalProtect IOS, you must complete the steps below. By default, FIPS mode for IOS operating system is automatically enabled on endpoints running IOS 16 and later releases.

1. You must use your MDM (Mobile Device Management) to enable FIPS-CC mode on the endpoints. In this example, we will be using Workspace ONE MDM[1].
2. Configure Workspace ONE for iOS endpoints.
3. Download the GlobalProtect app for IOS and Deploy the GlobalProtect Mobile App Using Workspace ONE.
4. From the Workspace ONE console, modify an existing Apple IOS profile or add a new one.

   To add a new profile:

   a. Select Resources > Profiles & Baselines > Profiles > ADD, then Add Profile.
   b. Select IOS from the platform list.

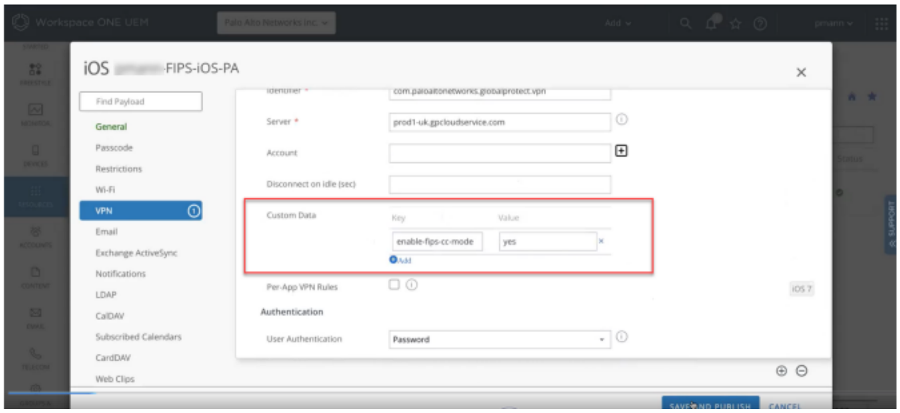


[1] Additional MDMs are supported in the Operational Environment. https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/mobile-endpoint-management/mobile-endpoint-management-overview

Figure 5 – Select the IOS Profile

   c. Select Device Profile from the Select Context Window.

5. On the Resources > Profiles & Baselines > Profiles page, select the <IOS profile> for which you want to enable FIPS-CC mode.
6. Configure the General, VPN, and Credentials (Optional) settings for the <IOS profile> that you want to create.
7. On the VPN page, under Custom Data:
   a. Specify the Key value as: enable-fips-cc-mode
   b. Set the Value to: yes



iOS [redacted] FIPS-iOS-PA

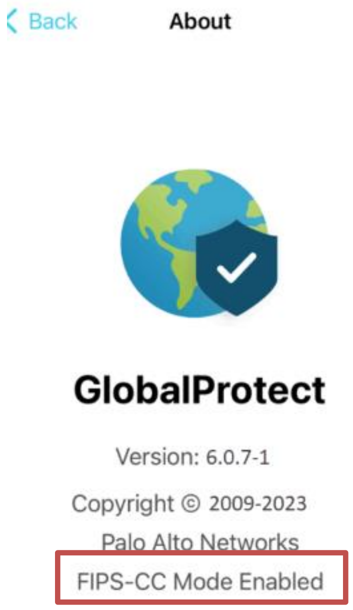
Identifier *: com.paloaltonetworks.globalprotect.vpn
Server *: prod1-uk.gpcloudservice.com
Account:
Disconnect on idle (sec):
Custom Data — Key: enable-fips-cc-mode, Value: yes
Per-App VPN Rules: □
Authentication
User Authentication: Password

Figure 6 – Enable FIPS-CC mode via Workspace ONE Console

8. Save and Publish your changes.

   After you enable the FIPS-CC mode from the Workspace ONE, the console pushes the updated FIPS-CC mode configuration to the IOS endpoints.

9. Ensure that the updated configuration is pushed from console to the IOS endpoints. On the IOS endpoint, select Settings > General > VPN & Device Management > VPN. The VPN Configuration screen displays the latest configuration.
10. Launch the GlobalProtect app on your IOS endpoint device.
11. From the status panel, open the settings dialog (⚙).
12. Select About.
13. Verify that FIPS-CC mode is enabled.



GlobalProtect

Version: 6.0.7-1

Copyright © 2009-2023

Palo Alto Networks

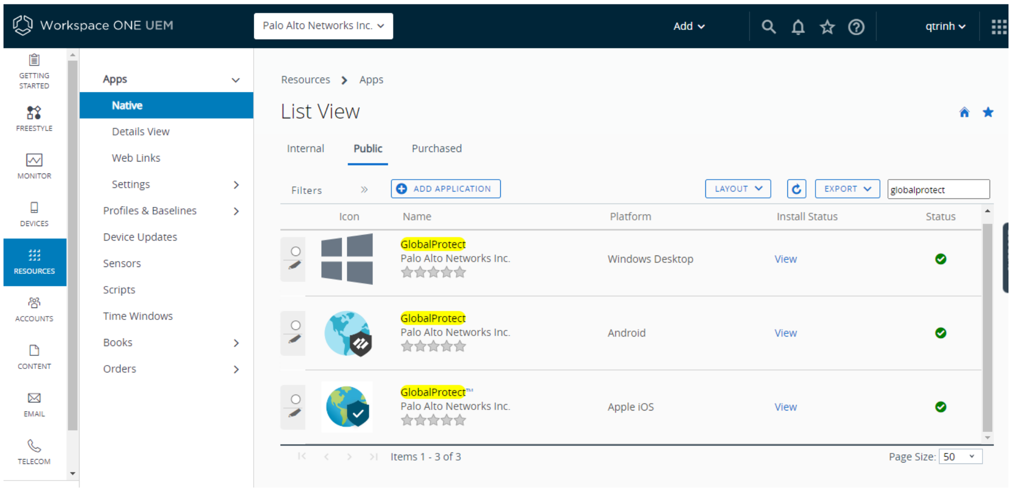
FIPS-CC Mode Enabled

Figure 7 – FIPS-CC Mode Indicator on IOS Platform

Enable FIPS-CC on Android Endpoint using Workspace ONE

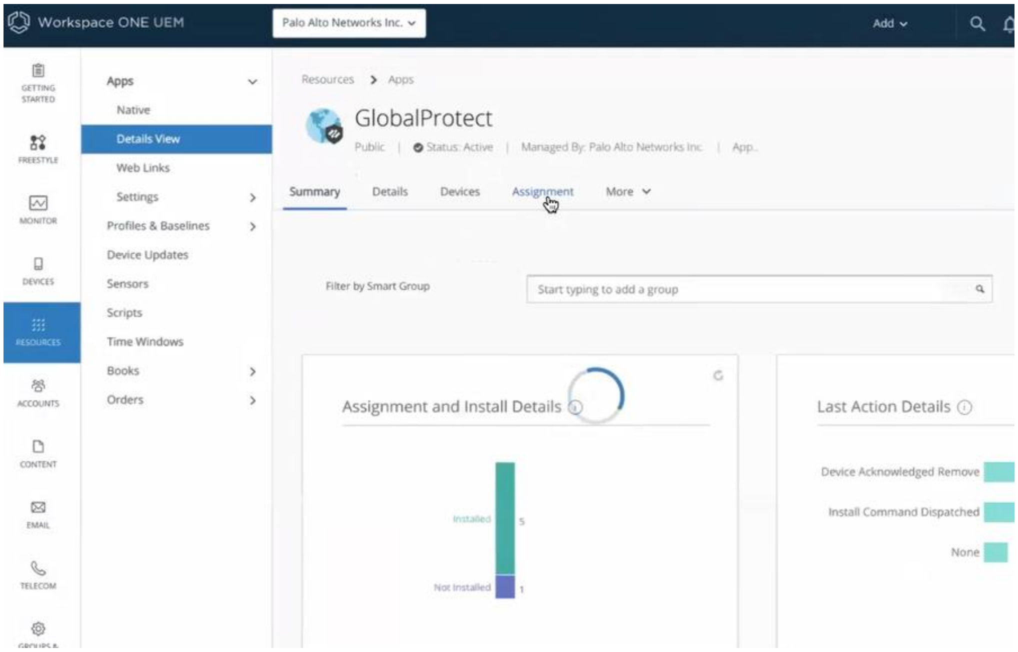
To enable FIPS-CC mode for GlobalProtect Android, you must complete the steps below.

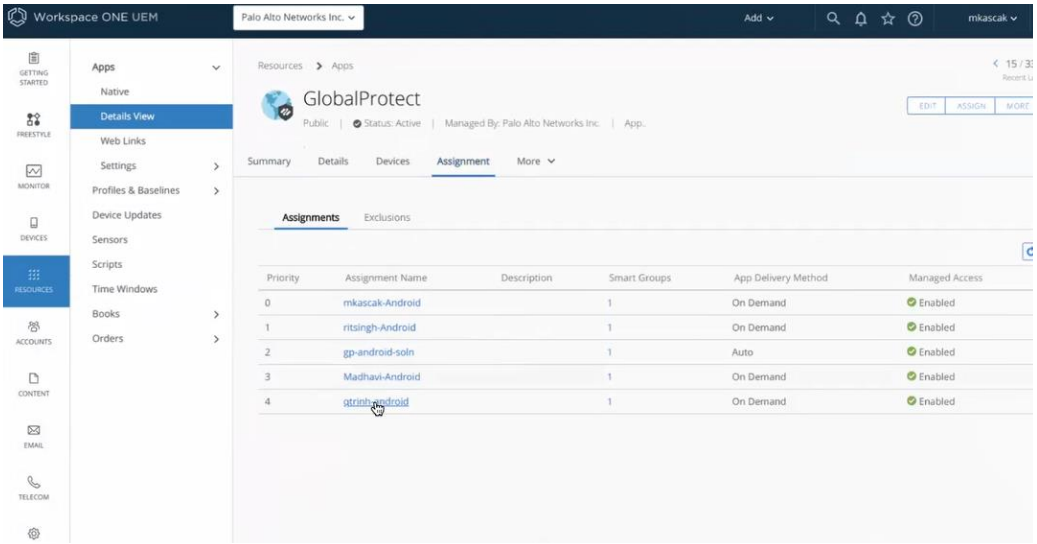
1. Download the GlobalProtect app for Android and Deploy the GlobalProtect Mobile App using Workspace ONE.
2. From the Workspace ONE console, go to Resources > Apps > Native > Public [Tab] and search for GlobalProtect App. Click on the GlobalProtect with Android as Platform.



Icon	Name	Platform	Install Status	Status
	GlobalProtect Palo Alto Networks Inc.	Windows Desktop	View	✓
	GlobalProtect Palo Alto Networks Inc.	Android	View	✓
	GlobalProtect™ Palo Alto Networks Inc.	Apple iOS	View	✓

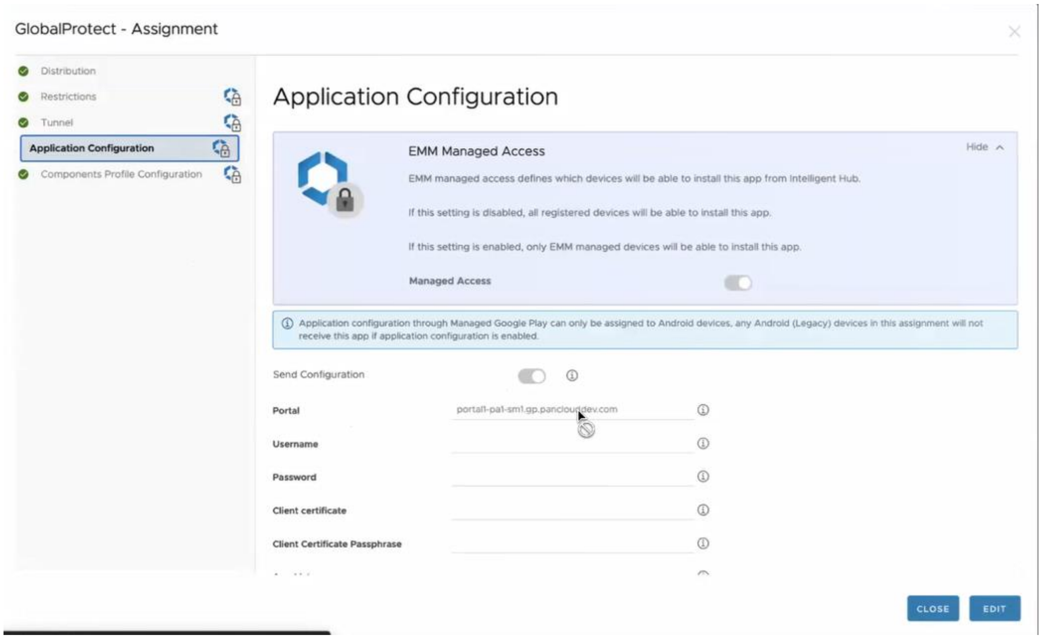
3. Click on the Assignment Tab. Assuming that you created an Assignment Group already with your managed device assigned, click on that Assignment Group Name.





Priority	Assignment Name	Description	Smart Groups	App Delivery Method	Managed Access
0	mkascak-Android		1	On Demand	✓ Enabled
1	ritsingh-Android		1	On Demand	✓ Enabled
2	gp-android-soln		1	Auto	✓ Enabled
3	Madhavi-Android		1	On Demand	✓ Enabled
4	qtrinh-android		1	On Demand	✓ Enabled

4. Click on Application Configuration.



GlobalProtect - Assignment

- Distribution
- Restrictions
- Tunnel
- **Application Configuration**
- Components Profile Configuration

Application Configuration

EMM Managed Access

EMM managed access defines which devices will be able to install this app from Intelligent Hub.

If this setting is disabled, all registered devices will be able to install this app.

If this setting is enabled, only EMM managed devices will be able to install this app.

Managed Access

Application configuration through Managed Google Play can only be assigned to Android devices, any Android (Legacy) devices in this assignment will not receive this app if application configuration is enabled.

Send Configuration

Portal portal1-pa1-sm1.gp.pancloudev.com

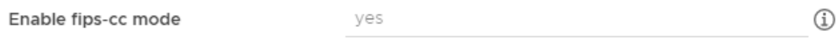
Username

Password

Client certificate

Client Certificate Passphrase

5. Set Managed Account to on (green icon) and Send Config to on (green icon):
   a. Look for: Enable fips-cc mode
   b. Set the Value to: yes

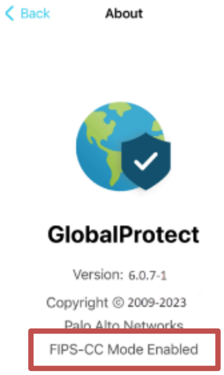


Enable fips-cc mode yes

14. Save and Publish your changes.

    After you enable the FIPS-CC mode from the Workspace ONE, the console pushes the updated FIPS-CC mode configuration to the Android endpoints.

15. Launch the GlobalProtect app on your Android endpoint device.
16. From the status panel, open the settings dialog (⚙).
17. Select About.
18. Verify that FIPS-CC mode is enabled.



Version: 6.0.7-1

Copyright © 2009-2023

Palo Alto Networks

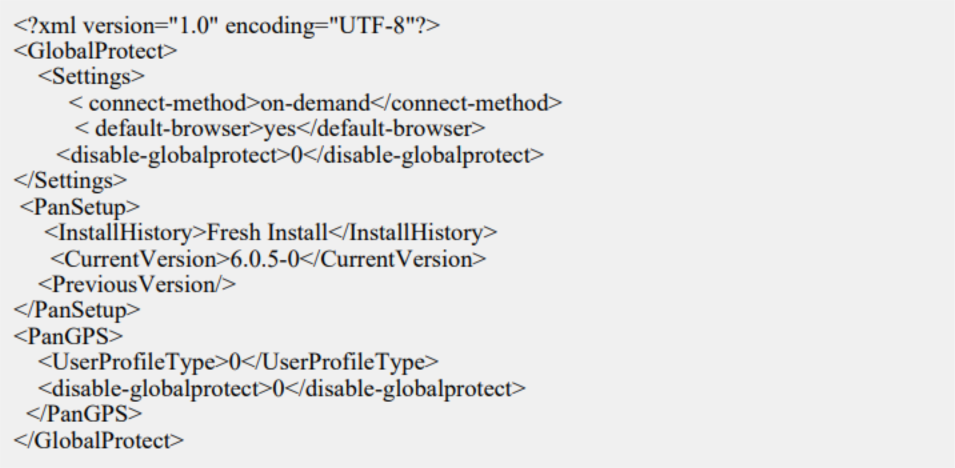
FIPS-CC Mode Enabled

Figure 8 – FIPS-CC Mode Indicator on Android Platform

Enable FIPS-CC on Linux Platform (Ubuntu/RHEL)

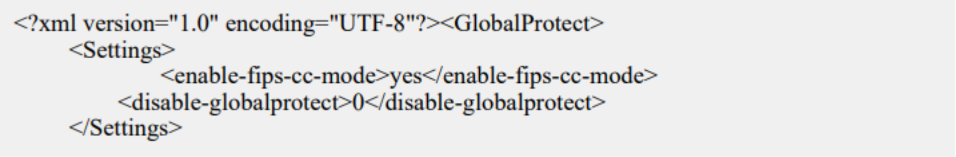
To enable FIPS-CC mode for GlobalProtect, you must complete the steps below. You should enable FIPS mode on the Linux (e.g., Ubuntu or Redhat) prior to enabling FIPS-CC mode for GP.

1. Install GlobalProtect app on your Linux platform.
2. (Optional) If client certificate is used for authentication, install and setup client certificate.
3. Create the /opt/paloaltonetworks/globalprotect/pangps.xml pre-deployment configuration file and modify the pangps.xml file to enable FIPS-CC mode.
   For example,



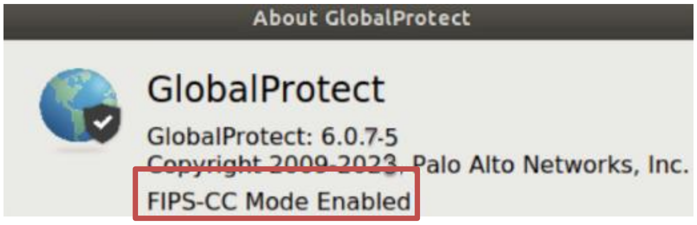
```
<?xml version="1.0" encoding="UTF-8"?>
<GlobalProtect>
   <Settings>
       < connect-method>on-demand</connect-method>
        < default-browser>yes</default-browser>
     <disable-globalprotect>0</disable-globalprotect>
</Settings>
 <PanSetup>
    <InstallHistory>Fresh Install</InstallHistory>
     <CurrentVersion>6.0.5-0</CurrentVersion>
   <PreviousVersion/>
</PanSetup>
<PanGPS>
   <UserProfileType>0</UserProfileType>
   <disable-globalprotect>0</disable-globalprotect>
  </PanGPS>
</GlobalProtect>
```

4. Modify the pangps.xml to enable FIPS-CC mode.
5. On Linux platforms, the pre-deployment configuration file (pangps.xml) is located in /opt/paloaltonetworks/globalprotect.
   - In the pangps.xml file, under Settings, add yes
   - For example,



```
<?xml version="1.0" encoding="UTF-8"?><GlobalProtect>
       <Settings>
                   <enable-fips-cc-mode>yes</enable-fips-cc-mode>
             <disable-globalprotect>0</disable-globalprotect>
       </Settings>
```

6. Once complete, save the changes.
7. Reboot the Linux system for the changes to take effect.
8. Launch the GlobalProtect app on your Linux platform.
9. From the status panel, open the settings dialog (⚙).
10. Select About.
11. Verify that FIPS-CC mode is enabled.



About GlobalProtect

GlobalProtect

GlobalProtect: 6.0.7-5

Copyright 2009-2023, Palo Alto Networks, Inc.

FIPS-CC Mode Enabled

Figure 9 – FIPS-CC Mode Indicator on Linux Platform

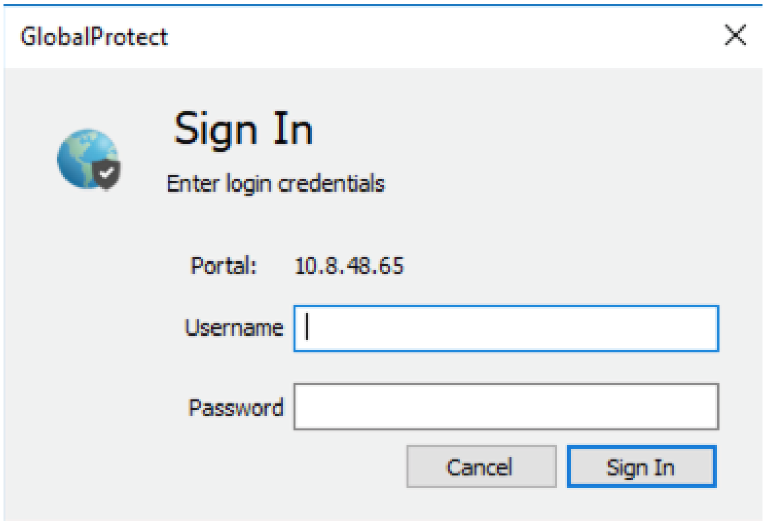
TOE Operation

Once the TOE has been placed in FIPS-CC mode, it will enforce all necessary CC requirements[2]. No additional changes are needed to be made by the administrator.

When connecting to the PAN-OS gateway, the administrator will need to load the server's CA certificate(s) into the computer's trust store for the TOE to properly handle the certificate chain validation. In addition, the PAN-OS firewall/gateway must have GlobalProtect Gateway license PAN-PA-**XYZ**-GP-3YR or PAN-PA-**XYZ**-GP-5YR, where **XYZ** is the PAN-OS model number such as 5250.

Portal Login

When the connection starts, the administrator will be provided with a prompt to provide their login credentials. These credentials are to access the PAN-OS Firewall portal and should be entered accordingly. If incorrect credentials are provided, the TOE will ask for the administrator to try again. There are no credentials needed to login to the TOE itself.



GlobalProtect

Sign In

Enter login credentials

Portal: 10.8.48.65

Username

Password

Figure 10 - Logging into Portal

Portal Login with Client Certificate

A user can opt to use a client certificate for authenticating into the PAN-OS Gateway. To achieve this, the administrator must create a client certificate and import it into the platform's certificate store. On Windows, import the client's certificate and necessary CAs into the Microsoft Certificate Management Console, and add it to the User Account. For macOS, import the necessary client certificate and CA certificate into the Keychain Access.

[2] Restrict TLS version to 1.2 and Approved cipher suites only, RFC 6125 strict checking, X509 Key Usage and Extended Key Usage strict checking.

Viewing the Current Version

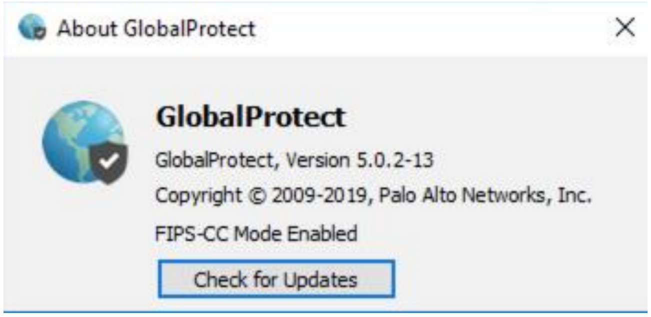
To view the current TOE version, the administrator can first navigate to the settings by opening the settings dialog (⚙) and select ‘About’.

Checking for Updates

To update the TOE, the administrator can first navigate to the settings by opening the settings dialog (⚙), selecting ‘About’, and then clicking ‘Check for Updates’ button. If there is an update[3] available, the administrator can select ‘yes’ to continue with the download/installation.

NOTE: Make sure you have the platform administrator privileges. During the installation process, a digital signature verification check is automatically performed to verify that the update has not been modified. If the check fails, this error message will be displayed: “The Installation Failed: The Installer encountered an error that caused the installation to fail”. More details on the error can be found in the install.log. If the process succeeds and the TOE is updated, this is also logged in the install.log.

During the installation, the VPN connectivity will be disabled, but re-enabled once the update is completed.



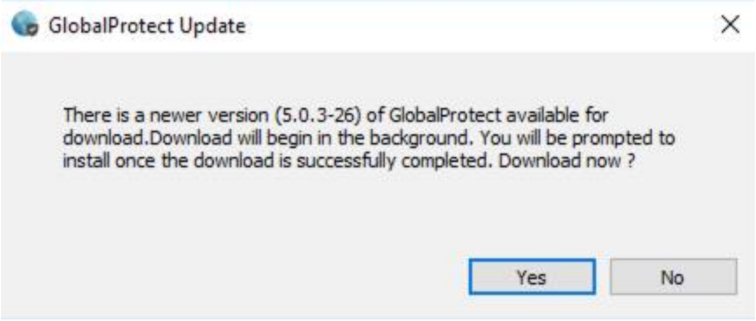
GlobalProtect

GlobalProtect, Version 5.0.2-13

Copyright © 2009-2019, Palo Alto Networks, Inc.

FIPS-CC Mode Enabled

Figure 11 - Checking for Updates



There is a newer version (5.0.3-26) of GlobalProtect available for download.Download will begin in the background. You will be prompted to install once the download is successfully completed. Download now ?

Figure 12 - Update Available

[3] For Debian and Ubuntu, use the **sudo apt-get upgrade <gp-app-pkg>** command. where <gp-app-pkg> is the path of the UI distribution package for your Linux version. For CentOS and Red Hat, use the **sudo yum update -y <gp-app-pkg>** command.

Configuring the Portal and Gateway

To configure the TOE Portal and Gateway, the administrator can first navigate to the settings by opening the settings dialog (⚙), selecting ‘Settings’, and on the ‘General’ tab, click ‘Add’ (Windows) or ‘+’ (macOS). Enter the Portal IP address or hostname and click ‘Save’.

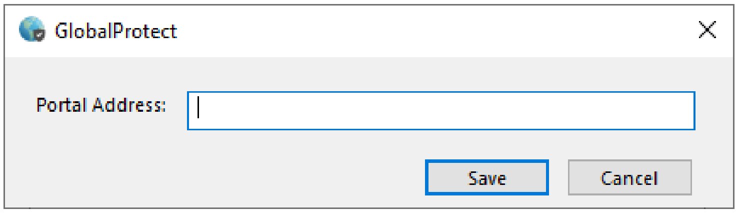
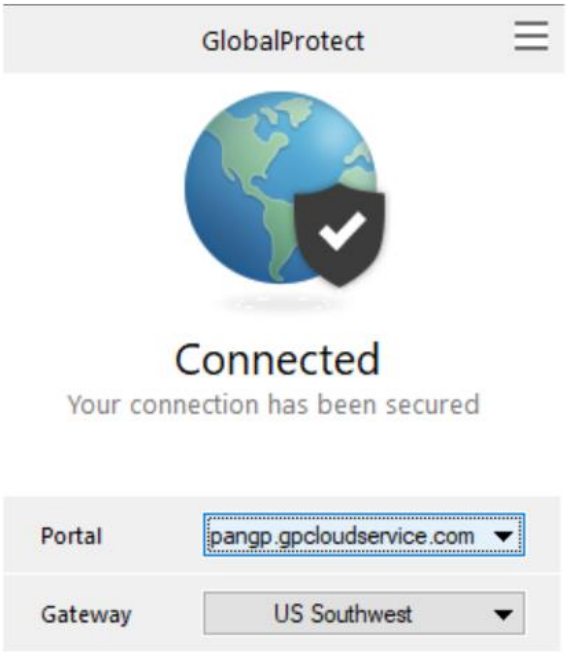


Figure 13 – Enter Portal Address

On the main GlobalProtect App page, click on the drop-down menu to select that portal. To change the Gateway, click on the drop-down menu to select a different Gateway.



Connected

Your connection has been secured

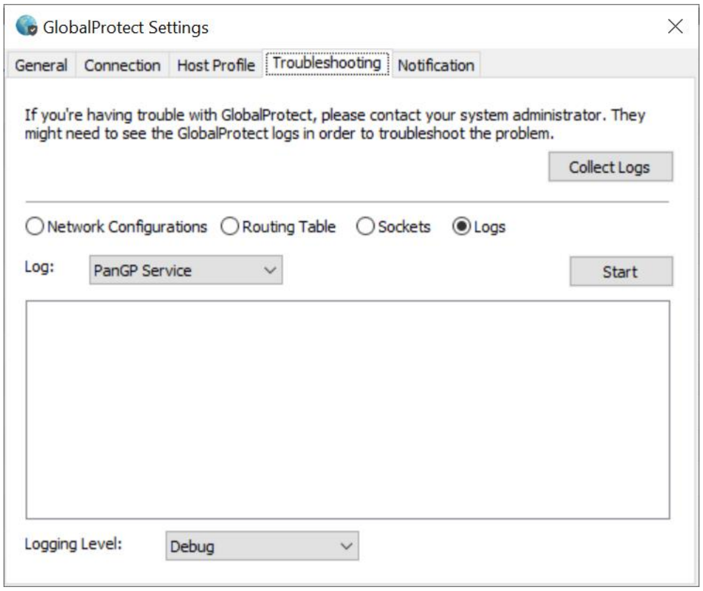
Portal pangp.gpcloudservice.com

Gateway US Southwest

Figure 14 – Select the Portal and/or Gateway

Collecting Logs

To collect logs for troubleshooting, the administrator can first navigate to the settings by opening the settings dialog (⚙), selecting ‘Settings’, and on the ‘Troubleshooting’ tab, click on the ‘Collect Logs’ button.



If you're having trouble with GlobalProtect, please contact your system administrator. They might need to see the GlobalProtect logs in order to troubleshoot the problem.

○ Network Configurations ○ Routing Table ○ Sockets ● Logs

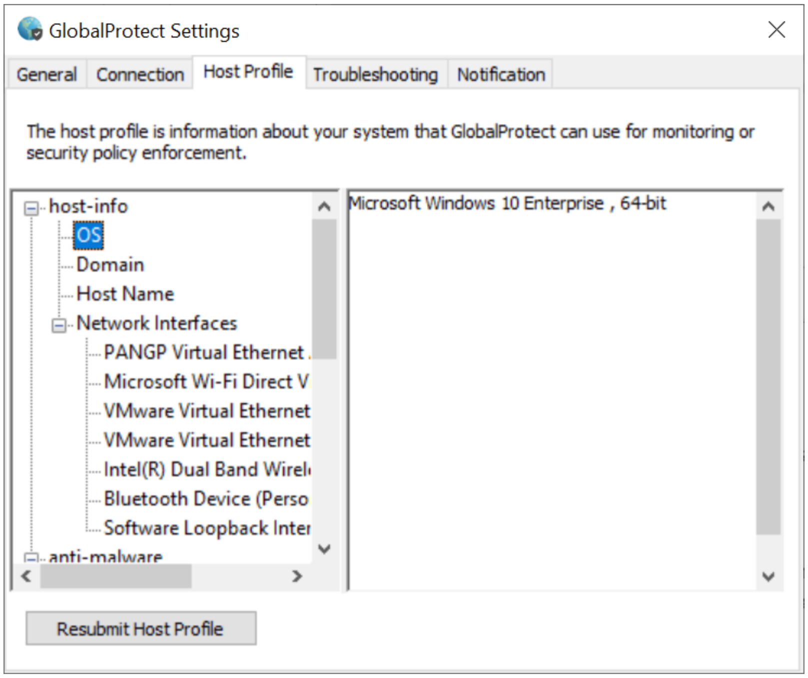
Log: PanGP Service

Logging Level: Debug

Figure 15 – Troubleshooting Tab

Sending System Information to Portal

To send system information to Portal, the administrator can first navigate to the settings by opening the settings dialog (⚙), selecting ‘Settings’, and on the ‘Host Profile’ tab, click on the ‘Resubmit Host Profile’ button.



The host profile is information about your system that GlobalProtect can use for monitoring or security policy enforcement.

```
⊟ host-info
    OS
    Domain
    Host Name
  ⊟ Network Interfaces
      PANGP Virtual Ethernet .
      Microsoft Wi-Fi Direct V
      VMware Virtual Ethernet
      VMware Virtual Ethernet
      Intel(R) Dual Band Wirel
      Bluetooth Device (Perso
      Software Loopback Inter
⊟ anti-malware
```

Microsoft Windows 10 Enterprise , 64-bit

Figure 16 – Host Profile Tab

Hardware Resources

The GlobalProtect app needs network connectivity which requires access to the platform hardware such as the network interface cards (NICs) or Wi-Fi chips. For a complete list of network interfaces (both physical and virtual), please check the system information in the Host Profile. Network connectivity is required because GlobalProtect app is a VPN client that secures the network communication from the host platform to the VPN gateway and portal.

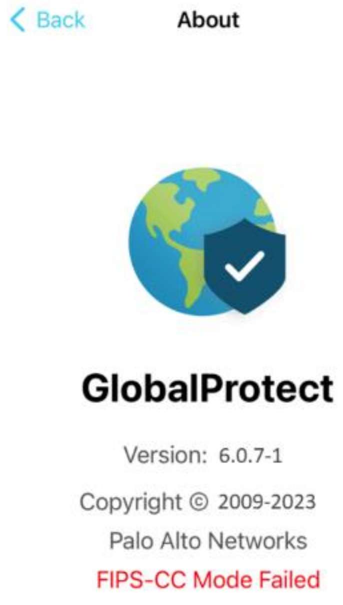
Troubleshooting

In the event of a failure, the sections below will provide the administrator with information on diagnosing the issue.

FIPS-CC Initialization Error

After you enable FIPS-CC mode, the GlobalProtect app performs FIPS power-on self-tests and integrity tests during app initialization and system/app reboots. If either of these tests fail, the GlobalProtect app goes into a disabled state, and the About window displays the FIPS-CC Mode Failed error message.

If this occurs, restart the app to clear the error condition. If the issue persists, the administrator will be required to uninstall the app and then reinstall the app.

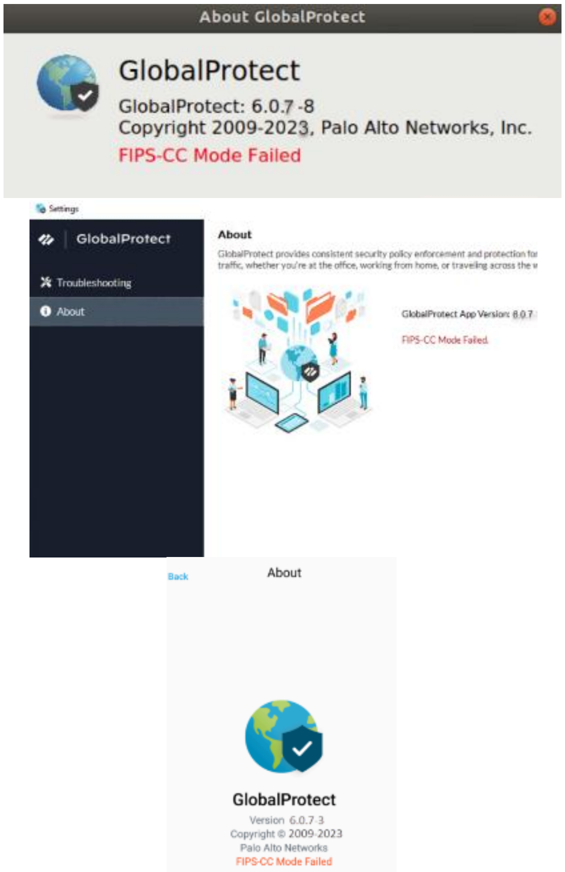


GlobalProtect

Version: 6.0.7-1

Copyright © 2009-2023
Palo Alto Networks
FIPS-CC Mode Failed

Figure 17 - FIPS-CC Mode Failure (iOS)



GlobalProtect

GlobalProtect: 6.0.7 -8
Copyright 2009-2023, Palo Alto Networks, Inc.
FIPS-CC Mode Failed

About

GlobalProtect provides consistent security policy enforcement and protection for traffic, whether you're at the office, working from home, or traveling across the w

GlobalProtect App Version: 6.0.7

FIPS-CC Mode Failed.

GlobalProtect
Version 6.0.7-3
Copyright © 2009-2023
Palo Alto Networks
FIPS-CC Mode Failed

Figure 18 - FIPS-CC Mode Failure (Linux, Windows, and Android)

FIPS-CC Conditional Test Failure

After the GlobalProtect app initializes in FIPS-CC mode, it performs FIPS conditional self-tests. If the self-tests fail, the GlobalProtect app terminates the session and remains disconnected.

To establish a GlobalProtect connection, you must re-authenticate to the GlobalProtect portal.

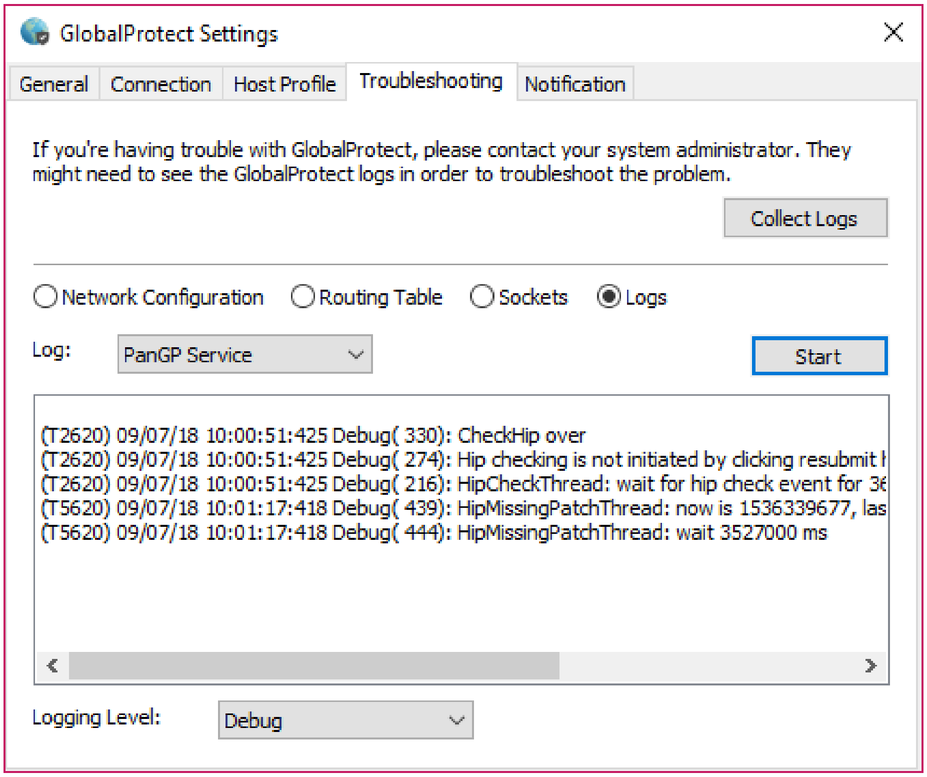
Accessing System Logs

The GlobalProtect app produces logs to help troubleshoot issues that are encountered during the operational of the TOE.

To view the system logs, perform the following:

1. Launch the GlobalProtect app
2. From the status panel, open the settings dialog (⚙).
3. Select Settings
4. From the GlobalProtect Settings panel, select Troubleshooting
5. Select a Logging Level
6. View your GlobalProtect logs (Optional – Windows Only)
    a. Select Logs
    b. Choose a Log type

c. Start collecting logs



If you're having trouble with GlobalProtect, please contact your system administrator. They might need to see the GlobalProtect logs in order to troubleshoot the problem.

○ Network Configuration ○ Routing Table ○ Sockets ● Logs

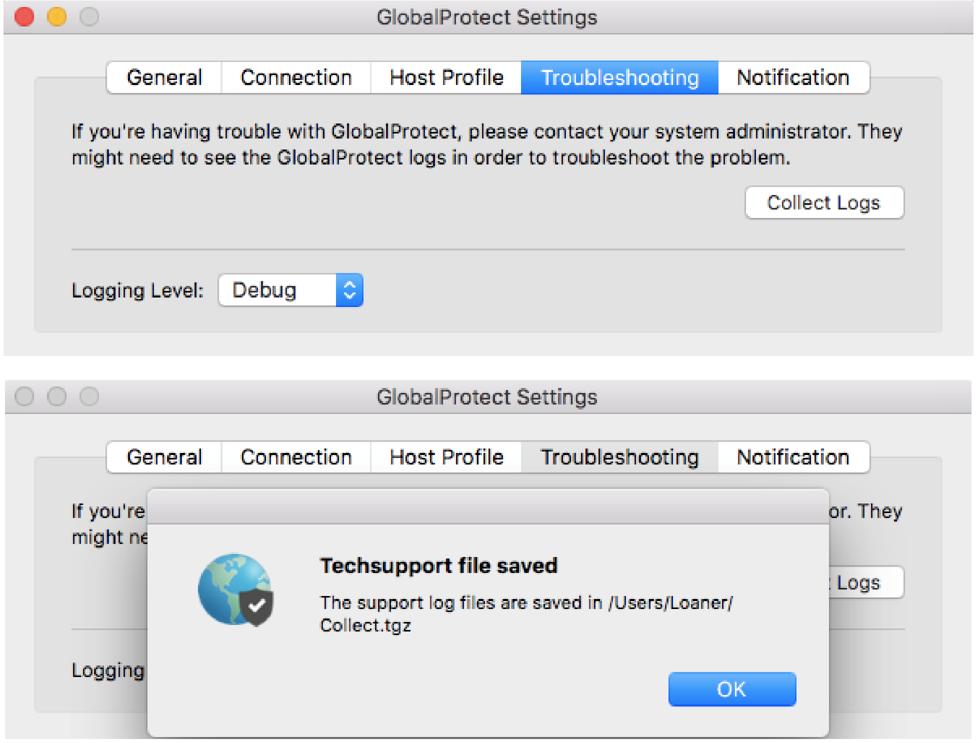
Log: PanGP Service

```
(T2620) 09/07/18 10:00:51:425 Debug( 330): CheckHip over
(T2620) 09/07/18 10:00:51:425 Debug( 274): Hip checking is not initiated by clicking resubmit l
(T2620) 09/07/18 10:00:51:425 Debug( 216): HipCheckThread: wait for hip check event for 36
(T5620) 09/07/18 10:01:17:418 Debug( 439): HipMissingPatchThread: now is 1536339677, las
(T5620) 09/07/18 10:01:17:418 Debug( 444): HipMissingPatchThread: wait 3527000 ms
```

Logging Level: Debug

Figure 19 - GlobalProtect Logs on Windows System

7. Collect Logs to send to your GlobalProtect administrator for troubleshooting



If you're having trouble with GlobalProtect, please contact your system administrator. They might need to see the GlobalProtect logs in order to troubleshoot the problem.

Logging Level: Debug

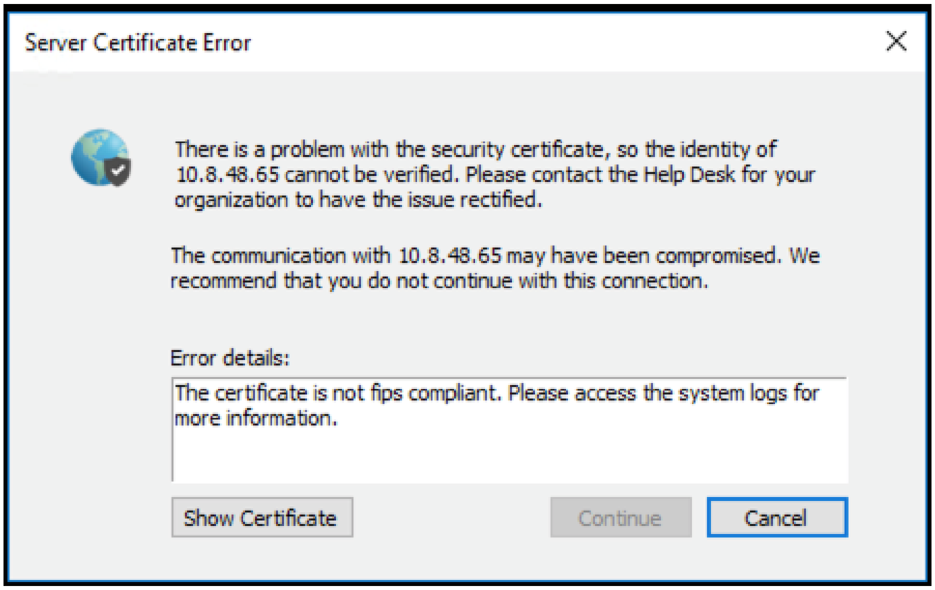
Techsupport file saved

The support log files are saved in /Users/Loaner/Collect.tgz

Figure 20 - Collecting Logs on macOS

Connection Failures

The TOE performs various checks on the certificates that are presented to it during connection establishment in FIPS-CC mode. In the event of an error (e.g. incorrect key size, wrong identifier, X509 certificate issues, etc.), the TOE will present an error message. The administrator can view the system logs to determine the specific problem. Once the error occurs, the TOE will remain in a disconnected state with the 'continue' option greyed out until the problem is addressed.


Server Certificate Error

There is a problem with the security certificate, so the identity of 10.8.48.65 cannot be verified. Please contact the Help Desk for your organization to have the issue rectified.

The communication with 10.8.48.65 may have been compromised. We recommend that you do not continue with this connection.

Error details:

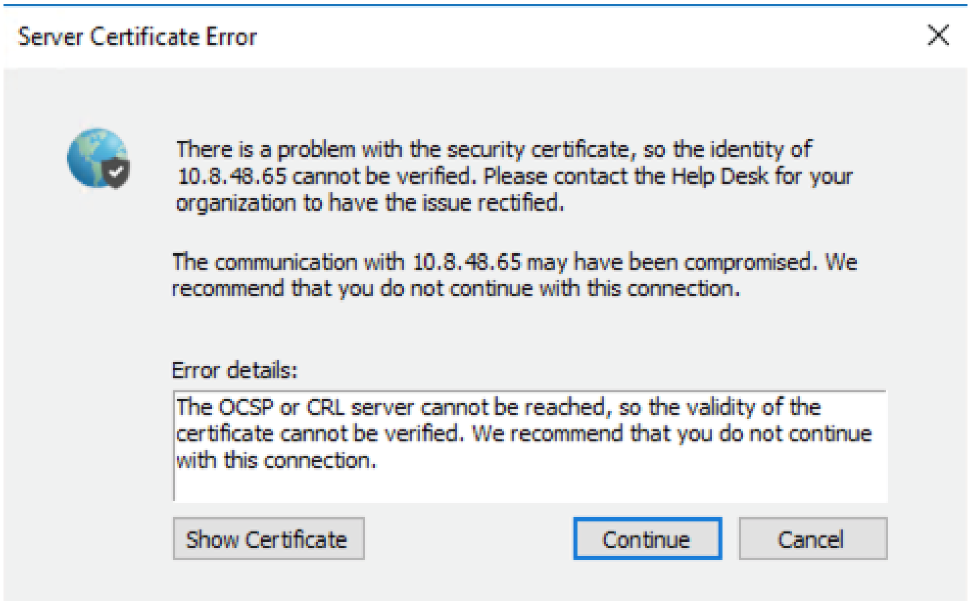
The certificate is not fips compliant. Please access the system logs for more information.

Figure 21 - Connection Failure

Revocation Checking

There is no additional configuration needed on the TOE for OCSP/CRL checking. If a certificate is presented with an OCSP/CRL in its certificate, the TOE will automatically perform the necessary checks.

If the OCSP/CRL can't be accessed, the administrator is provided with a warning message and the option to continue if they want to proceed.


Server Certificate Error

There is a problem with the security certificate, so the identity of 10.8.48.65 cannot be verified. Please contact the Help Desk for your organization to have the issue rectified.

The communication with 10.8.48.65 may have been compromised. We recommend that you do not continue with this connection.

Error details:

The OCSP or CRL server cannot be reached, so the validity of the certificate cannot be verified. We recommend that you do not continue with this connection.

Figure 22 - OCSP/CRL Unreachable

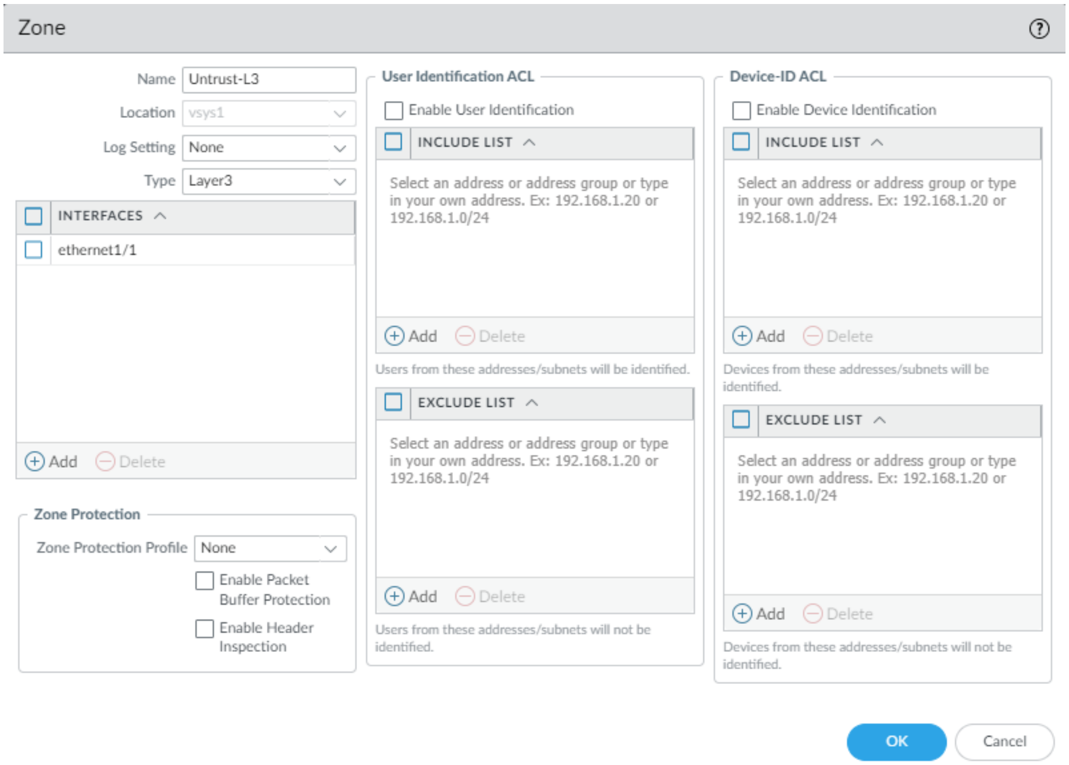
PAN-OS Portal/Gateway Configuration

Enable configuration settings on the Palo Alto Networks Firewall

To connect the GlobalProtect app to the PAN-OS portal/gateway in the operational environment, the administrator needs to configure the PAN-OS server to have the proper settings for connection. The section below details steps needed on the Firewall to support this connection. Note: Individual settings may vary per vendor/administrator – these directions are general.

Create necessary certificates

1. Navigate to PAN-OS Device > Certificates
    a. Create CAs and leaf certificate for the server with the proper IP-address for the interface that will be connected (e.g. Common Name = 10.X.X.X signed by Root CA created)
2. Select SSL/TLS Service Profile
    a. Create a profile that includes the leaf certificate generated in Step 1 above with a minimum version of TLS 1.2 to max (TLS 1.2)
3. Navigate to Network > Zones
    a. Create a zone that will be used for the GlobalProtect interface and attach the network interface to it



Zone

Name: Untrust-L3
Location: vsys1
Log Setting: None
Type: Layer3

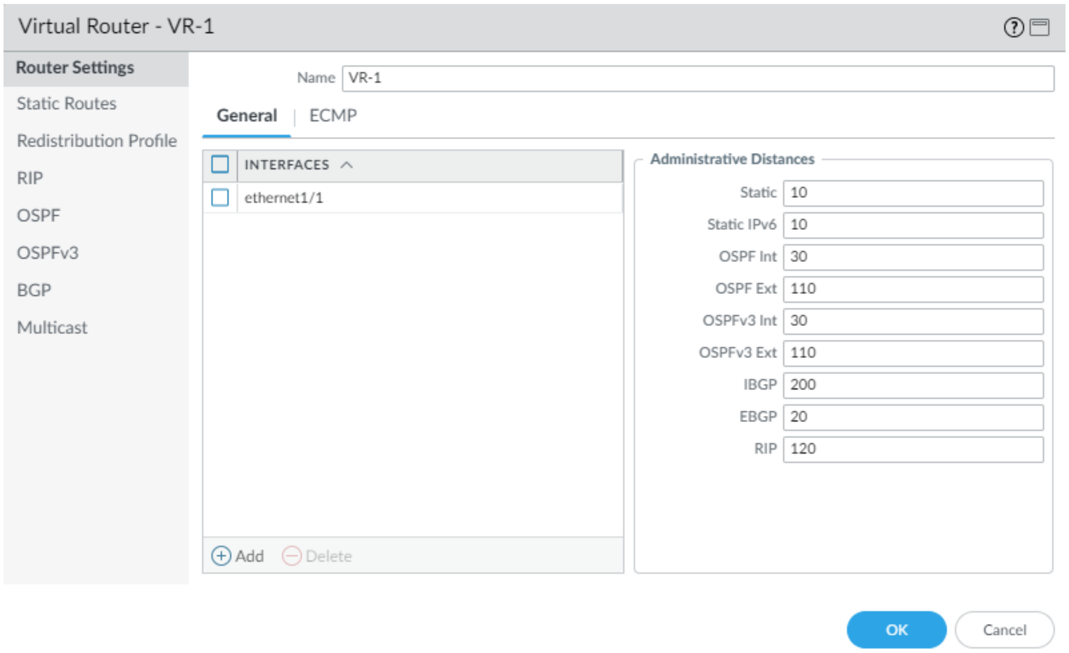
□ INTERFACES
□ ethernet1/1

Zone Protection
Zone Protection Profile: None
□ Enable Packet Buffer Protection
□ Enable Header Inspection

User Identification ACL
□ Enable User Identification
□ INCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Users from these addresses/subnets will be identified.
□ EXCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Users from these addresses/subnets will not be identified.

Device-ID ACL
□ Enable Device Identification
□ INCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Devices from these addresses/subnets will be identified.
□ EXCLUDE LIST
Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24
Devices from these addresses/subnets will not be identified.

4. Navigate to Network > Virtual Routers
   a. Create a virtual router that will be attached to the interface, and include it here
   b. On the static routes, add a route for the connection (example shown)



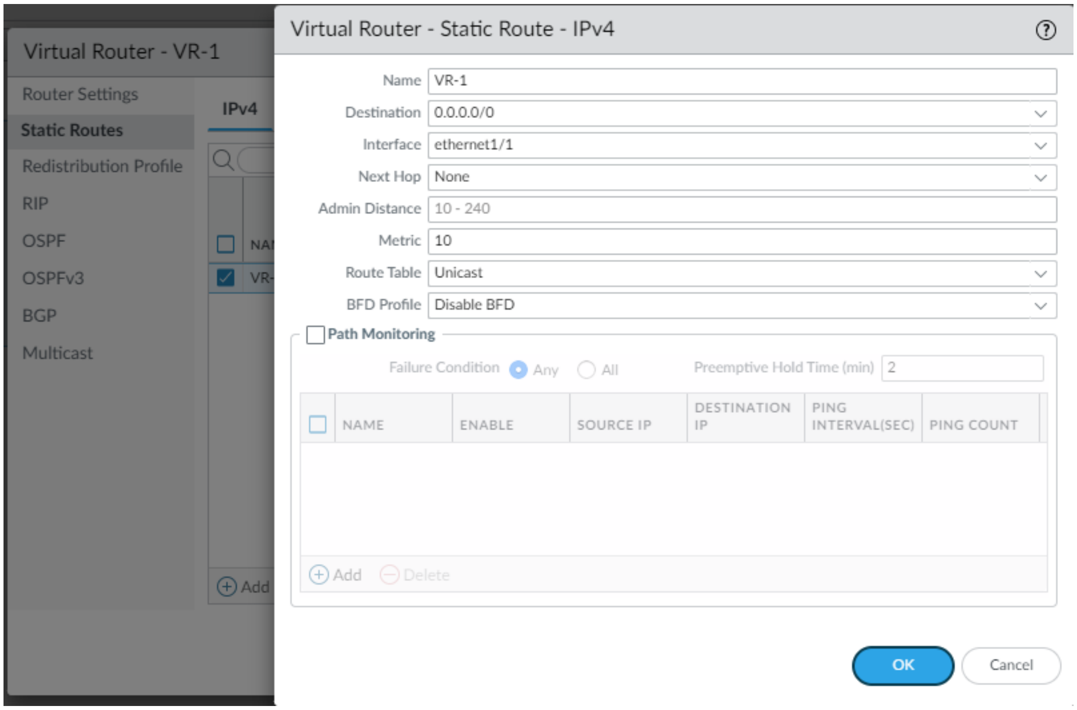
Virtual Router - VR-1

Name: VR-1

Interfaces: ethernet1/1

Administrative Distances

Static	10
Static IPv6	10
OSPF Int	30
OSPF Ext	110
OSPFv3 Int	30
OSPFv3 Ext	110
IBGP	200
EBGP	20
RIP	120



Virtual Router - Static Route - IPv4

Name	VR-1
Destination	0.0.0.0/0
Interface	ethernet1/1
Next Hop	None
Admin Distance	10 - 240
Metric	10
Route Table	Unicast
BFD Profile	Disable BFD

□ Path Monitoring

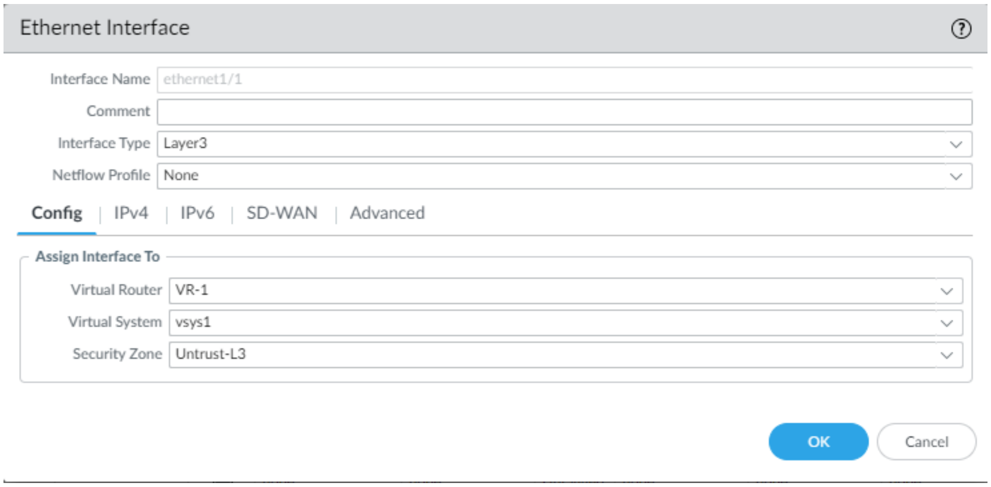
Failure Condition ● Any ○ All Preemptive Hold Time (min) 2

□	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT

5. Select Interfaces, and add the virtual router and security zone created in the steps above to the interface desired

a. On the IPv4 tab, include the IP address of the interface to be used

   i. Note: ensure that the CN/SAN lines up with this configuration properly

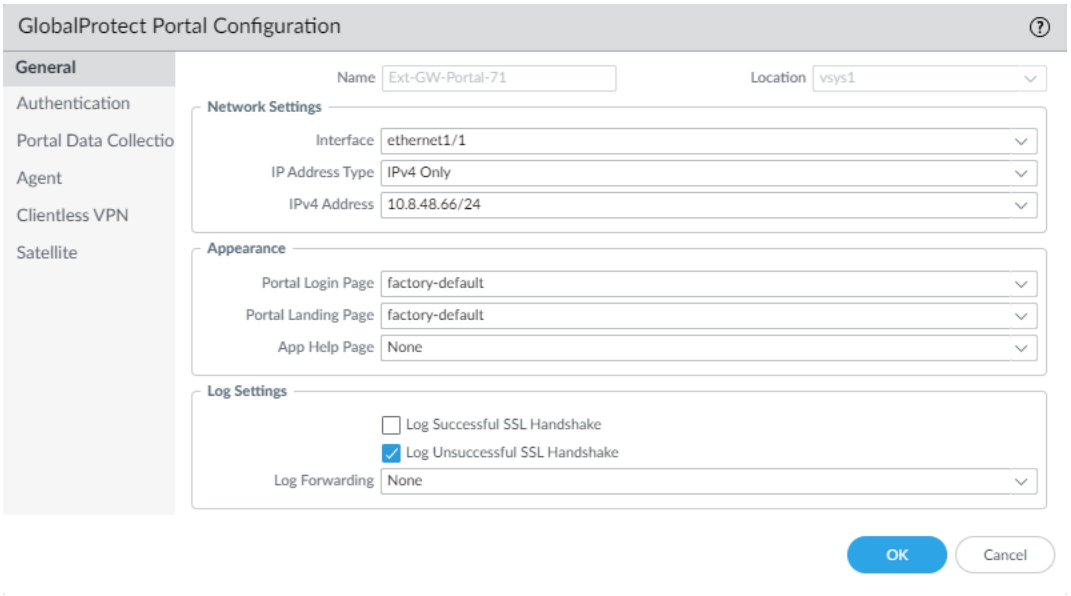


Interface Name: ethernet1/1
Comment:
Interface Type: Layer3
Netflow Profile: None

Assign Interface To
Virtual Router: VR-1
Virtual System: vsys1
Security Zone: Untrust-L3

6. Click on Portals under GlobalProtect

   a. Create a configuration of a GlobalProtect portal by including the interface and relevant IP-address created in steps prior



Name: Ext-GW-Portal-71
Location: vsys1

Network Settings
Interface: ethernet1/1
IP Address Type: IPv4 Only
IPv4 Address: 10.8.48.66/24

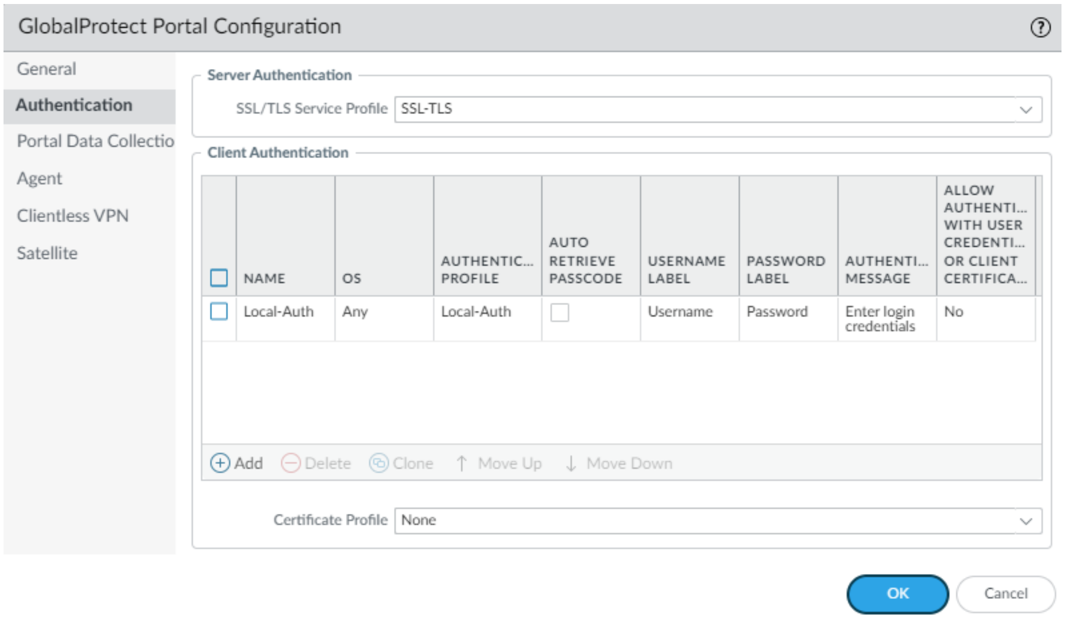
Appearance
Portal Login Page: factory-default
Portal Landing Page: factory-default
App Help Page: None

Log Settings
☐ Log Successful SSL Handshake
☑ Log Unsuccessful SSL Handshake
Log Forwarding: None

   b. On the Authentication tab, add the SSL/TLS Service profile that was created

   c. Include client authentication here that includes the necessary username/password

      i. Note: If using client certificate auth, leave the authentication blank, but add a certificate profile with the relevant CAs for checking the client certificate's chain



Server Authentication

SSL/TLS Service Profile: SSL-TLS

Client Authentication

☐	NAME	OS	AUTHENTIC... PROFILE	AUTO RETRIEVE PASSCODE	USERNAME LABEL	PASSWORD LABEL	AUTHENTI... MESSAGE	ALLOW AUTHENTI... WITH USER CREDENTI... OR CLIENT CERTIFICA...
☐	Local-Auth	Any	Local-Auth	☐	Username	Password	Enter login credentials	No

Certificate Profile: None

7. Create the GlobalProtect Gateway Configuration by selecting "Gateways" under GlobalProtect
    a. Assign the desired Interface along with necessary IP address
    b. On the Authentication tab, include the SSL/TLS Service profile of the server
        i. If using client authentication with password, add it to the Client Authentication section
        ii. If using client certificate-based authentication, leave this blank, and add a certificate profile with the relevant CAs. This will enable mutual authentication.
    c. Using the Agent tab, add a Tunnel Interface
        i. If one has not been created, click "add"
            1. Add a number to identify this tunnel interface
            2. Assign the Virtual Router noted above
            3. Create a new "Zone" (e.g. VPN-Zone) with this tunnel specified in the interface
8. Commit the configuration, and start the connection via the GlobalProtect app.

Use the following procedures to configure the firewall to authenticate GlobalProtect clients by their x509v3 certificates (i.e., Mutual Authentication). You can deploy the client certificate on the platform by generating the certificate internally or obtaining the certificate from your enterprise CA or a trusted third-party CA.

Generate the Client Certificate for GlobalProtect on the firewall.

1. Login with Administrator Role.
2. Create the root CA certificate for using client certificate to GP clients.
3. Select **Device > Certificate Management > Certificates > Device Certificates** and then click **Generate**.
4. Enter a **Certificate Name**. The name cannot contain any spaces.
5. Enter the IP Address or FQDN that will appear on the certificate in the **Common Name** field.

6. Select your root CA from the **Signed By** drop-down.
7. Select an **OCSP Responder** to verify the revocation status of certificates.
8. Configure the **Cryptographic Settings** for the certificate, including the encryption **Algorithm**, key length **(Number of bits)**, **Digest** algorithm, and **Expiration** (in days) for the certificate.
9. In the **Certificate Attribute** 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.
10. Click **OK** to generate the certificate.

Deploy the Client Certificate on the Windows Platform with GlobalProtect

1. Login with Administrator Role on the Windows platform[4].
2. From the command prompt, enter **mmc**.
3. Select **File > Add/Remove Snap-in**.
4. 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.
   a. Computer account
   b. My user account
5. From the **Console Root**, expand **Certificates**, and then select **Personal**.
6. 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.
7. **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.
8. Verify that the certificate has been added to the certificate store.

If you use an external root CA or third-party CA to generate the client certificate, you must import that root CA certificate into the firewall.

Import the root CA certificate used to issue the client certificate into the firewall

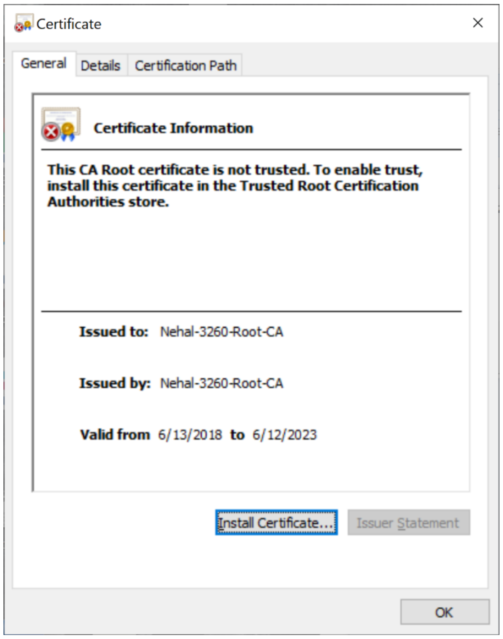
1. Login with Administrator Role.
2. Download the root CA certificate (Base64 format) used to issue the client certificate.
3. Select **Device > Certificate Management > Certificates > Device Certificates** and then click **Import**.
4. Set the **Certificate Type** to **Local** (default).
5. Enter a **Certificate Name** that identifies the certificate.
6. **Browse** to the select the **Certificate File** you download from the CA.

[4] On MacOS platform, install the client certificates to the Keychain on MacOS.

7. Set the **File Format** to **Base64 Encoded Certificate (PEM)**, and then click **OK**.
8. On the **Device Certificates** tab, select the certificate you just imported to open the Certificate Information.
9. Select **Trusted Root CA** and then click **OK**.

Deploy the Trusted CA Certificate on the Windows Platform with GlobalProtect

1. Login to Windows with Administrator rights.
2. Double-click on the Trusted Root Certificate (NOTE: Format .crt or .cert).
3. Click on **Install Certificate…**.



Certificate Information

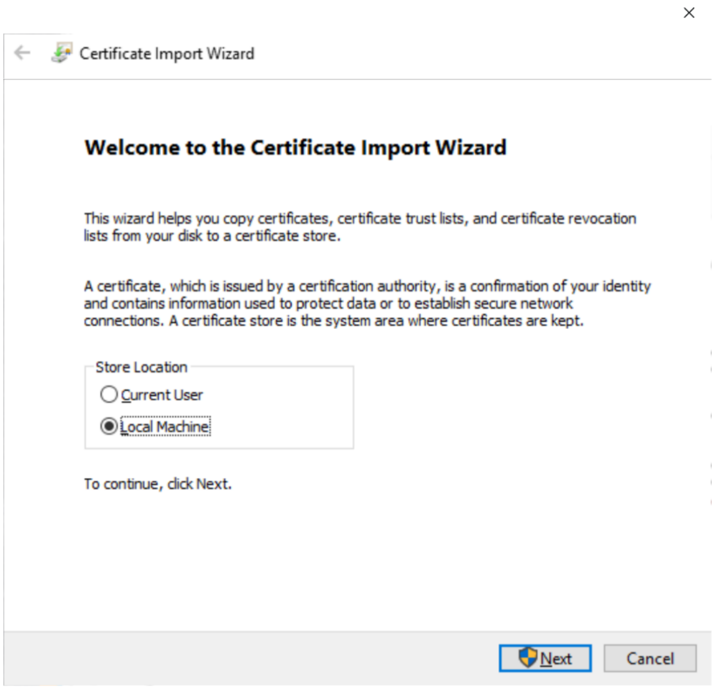
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: Nehal-3260-Root-CA

Issued by: Nehal-3260-Root-CA

Valid from 6/13/2018 to 6/12/2023

4. Check the radio box with **Local Machine**.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

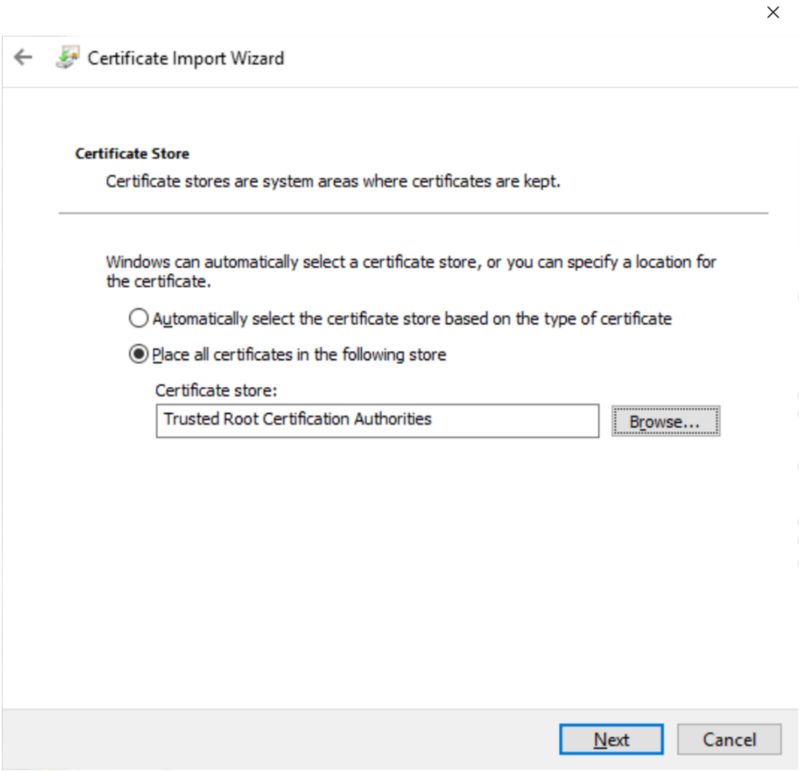
Store Location

○ Current User

● Local Machine

To continue, click Next.

5. Click **Browse...** and click **Trusted Root Certification Authorities**.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

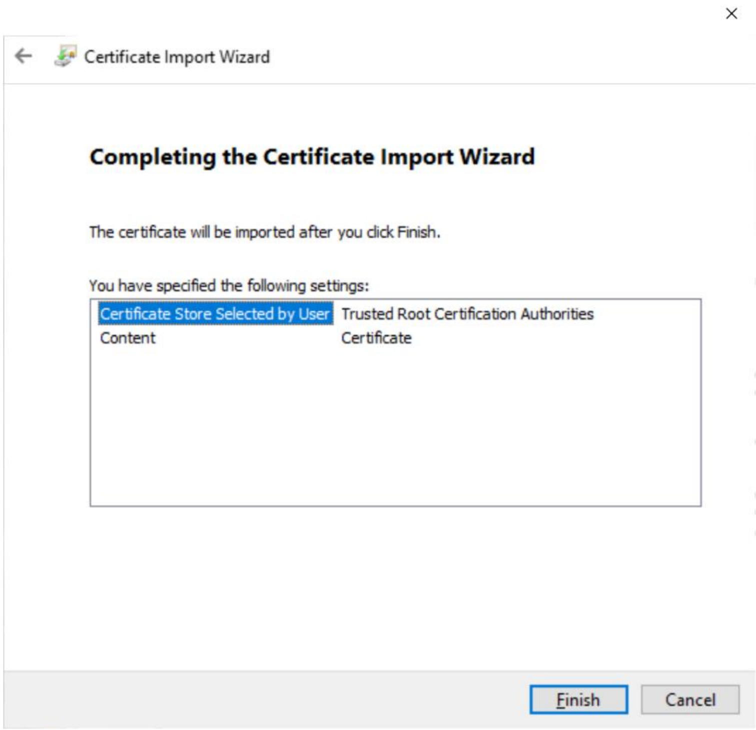
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

6. Click **Finish**.



Certificate Import Wizard

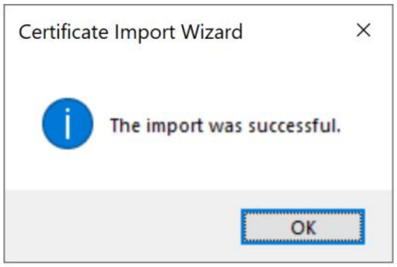
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

7. Verify the import was successful.



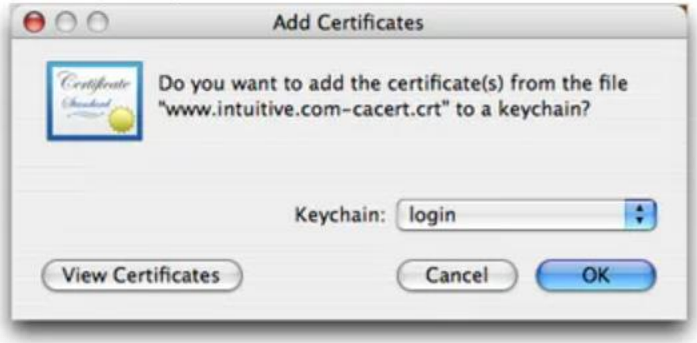
Certificate Import Wizard

The import was successful.

Deploy the Trusted CA Certificate on the Mac Platform with GlobalProtect

1. Save the Trusted Root Certificate to the MacOS and double-click it.

2. It will launch the Keychain Access application.

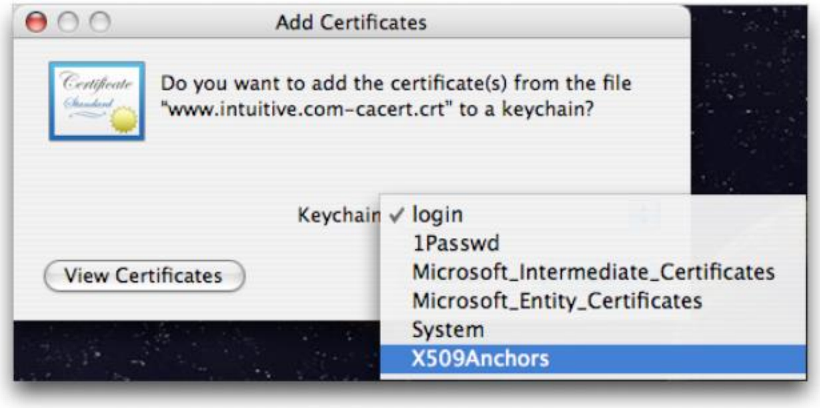


Add Certificates

Do you want to add the certificate(s) from the file "www.intuitive.com-cacert.crt" to a keychain?

Keychain: login

3. Click on the **Keychain** dro-down menu and select **X509Anchors**.



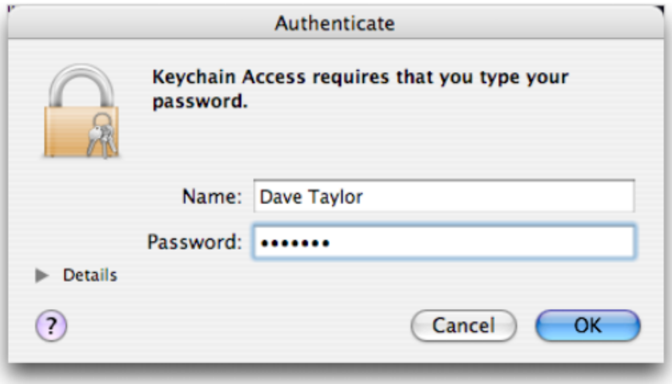
Add Certificates

Do you want to add the certificate(s) from the file "www.intuitive.com-cacert.crt" to a keychain?

Keychain: ✓ login

1Passwd
Microsoft_Intermediate_Certificates
Microsoft_Entity_Certificates
System
X509Anchors
View Certificates

4. Click **OK** and enter your administrative password when prompted.



Authenticate

Keychain Access requires that you type your password.

Name: Dave Taylor

Password: •••••••

5. Confirm the certificate is imported successful.

Deploy the Client Certificate on the Linux Platform with GlobalProtect

When you want to pre-deploy a client certificate to an endpoint for certificate-based authentication, you can copy the certificate to the endpoint and import it for use by the GlobalProtect app. Use the globalprotect import-certificate --location command to import the certificate on the endpoint. When prompted you must supply the certificate password.

```
user@linuxhost:~$ globalprotect import-certificate --location /
home/mydir/Downloads/cert_client_cert.p12
Please input passcode:
Import certificate is successful.
```

Deploy the Trusted CA Certificate on the iOS Platform with GlobalProtect

There are three common ways to install a CA's root certificate on an iOS device:

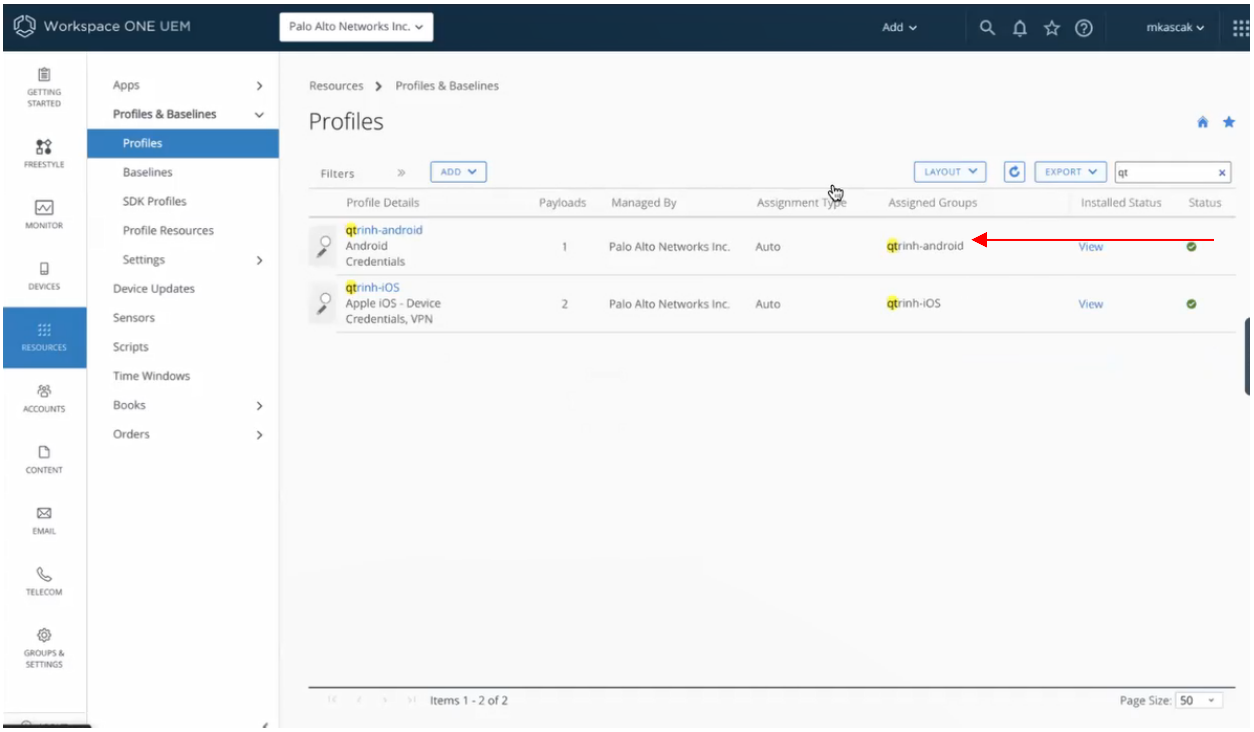
1. Put the .cer file on a web server and navigate to it in Safari. iOS will then ask you whether you want to install and trust that root certificate.
2. Attach the root certificate to an email and then email it to yourself; when you open the attachment, iOS will ask you whether you want to install and trust that root certificate.
3. Use Apple Configurator to create a configuration profile that includes the root certificate and then drag that configuration profile to the device in the main Apple Configurator window. In most cases, you'll need to complete the install process on the iOS device itself.

Important: Regardless of how you install the root certificate you must specifically enable it in Settings > General > About > Certificate Trust Settings. You need to "Enable Full Trust for Root Certificate" for every certificate added.

Deploy the Trusted CA Certificate on the Android Platform with GlobalProtect

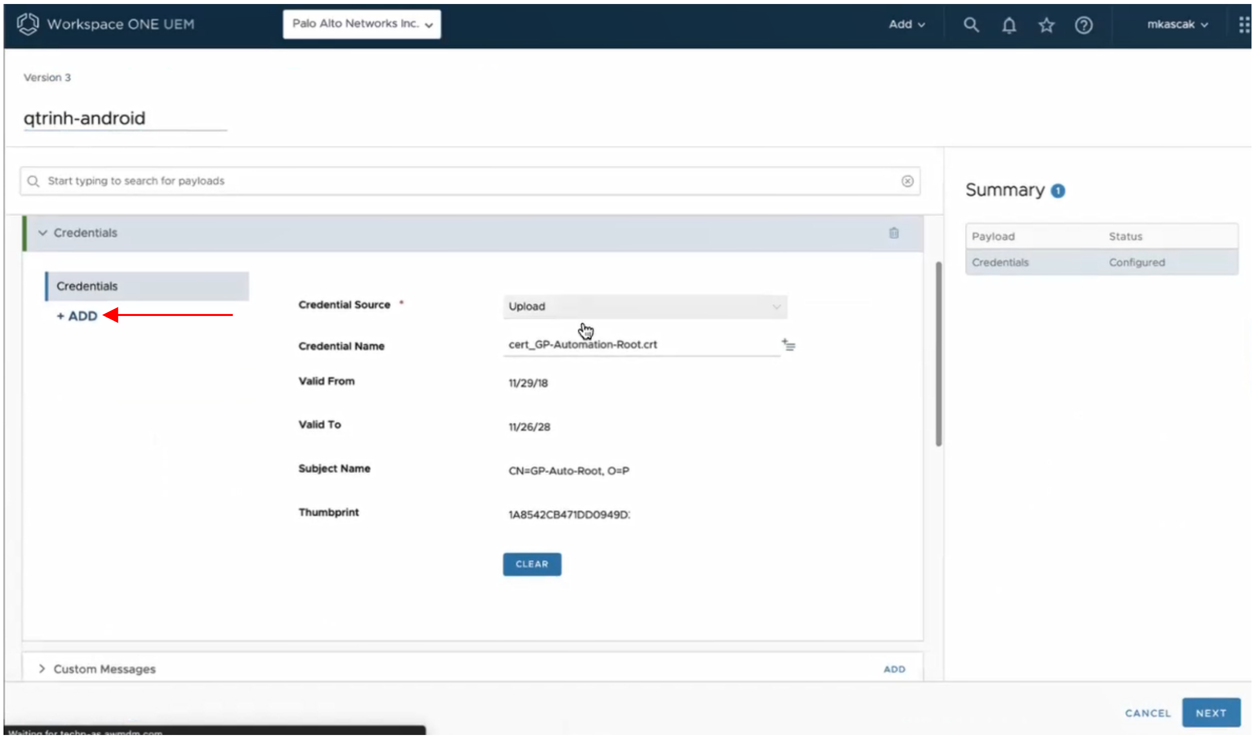
For Samsung devices, use the MDM (e.g., Workspace ONE) to deploy the CA certificates.

1. Go to Resources > Profiles & Baselines > Profiles.
2. Select or click on your Profiles.



Profile Details	Payloads	Managed By	Assignment Type	Assigned Groups	Installed Status	Status
qtrinh-android Android Credentials	1	Palo Alto Networks Inc.	Auto	qtrinh-android	View	●
qtrinh-iOS Apple iOS - Device Credentials, VPN	2	Palo Alto Networks Inc.	Auto	qtrinh-iOS	View	●

3. Click on Credentials.



Version 3

qtrinh-android

Credential Source * Upload

Credential Name cert_GP-Automation-Root.crt

Valid From 11/29/18

Valid To 11/26/28

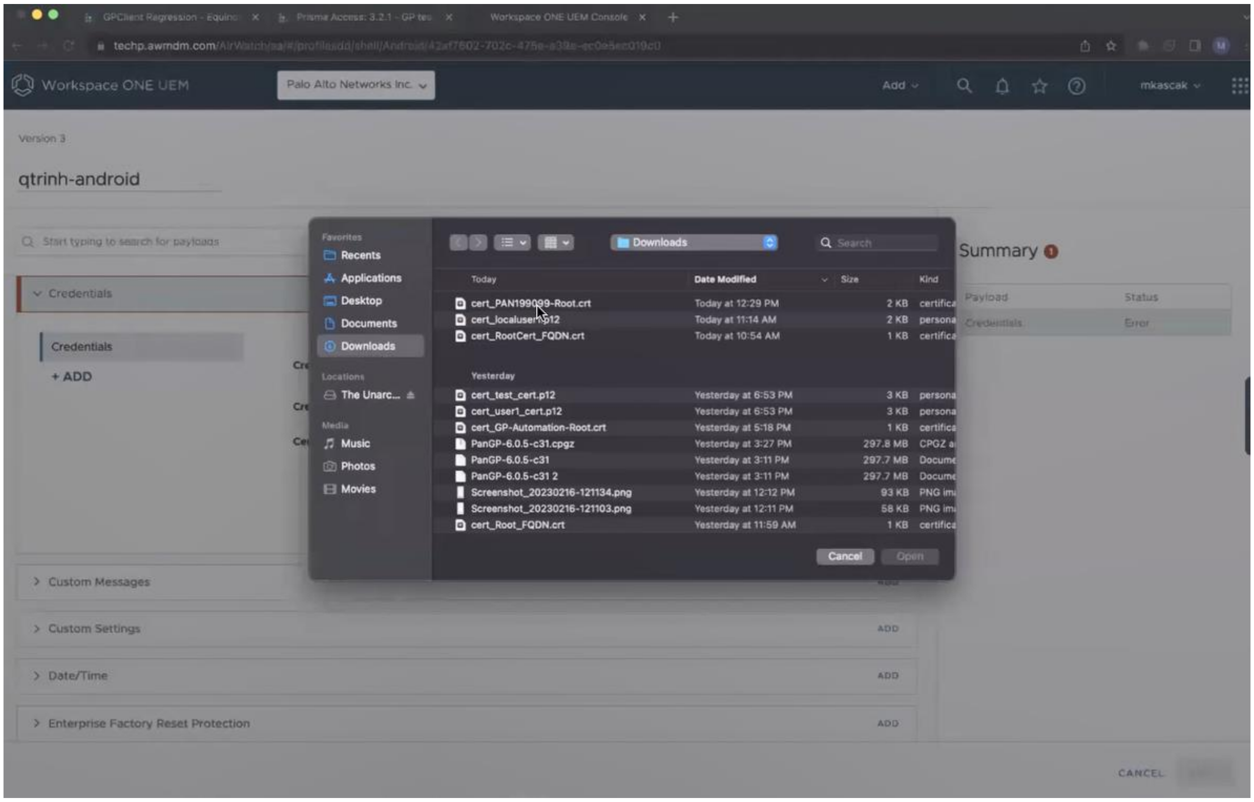
Subject Name CN=GP-Auto-Root, O=P

Thumbprint 1A8542CB471DD0949D:

Summary

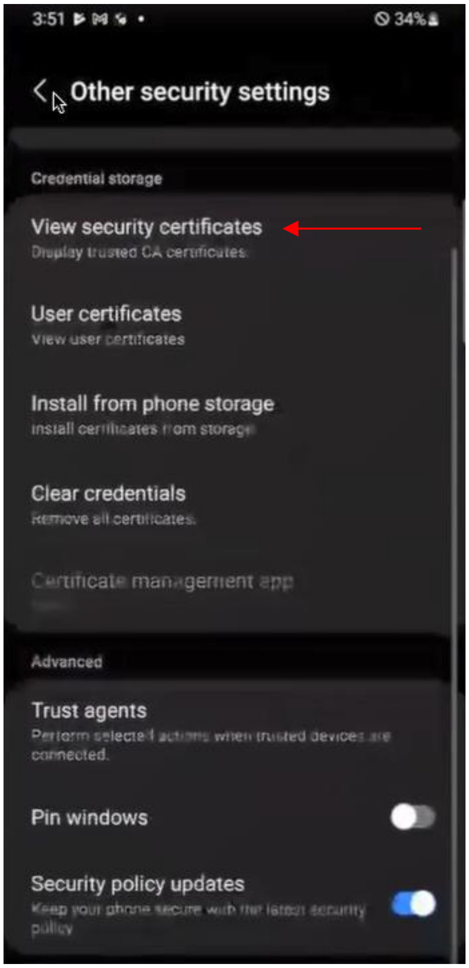
Payload	Status
Credentials	Configured

4. Upload as many CA certificates as needed.
5. To clear, click on Clear button.
6. To add more CA certificates, click on the +Add link.



Today	Date Modified	Size	Kind
cert_PAN199099-Root.crt	Today at 12:29 PM	2 KB	certifica
cert_localuser1.p12	Today at 11:14 AM	2 KB	persona
cert_RootCert_FQDN.crt	Today at 10:54 AM	1 KB	certifica
Yesterday			
cert_test_cert.p12	Yesterday at 6:53 PM	3 KB	persona
cert_user1_cert.p12	Yesterday at 6:53 PM	3 KB	persona
cert_GP-Automation-Root.crt	Yesterday at 5:18 PM	1 KB	certifica
PanGP-6.0.5-c31.cpgz	Yesterday at 3:27 PM	297.8 MB	CPGZ a
PanGP-6.0.5-c31	Yesterday at 3:11 PM	297.7 MB	Docume
PanGP-6.0.5-c31 2	Yesterday at 3:11 PM	297.7 MB	Docume
Screenshot_20230216-121134.png	Yesterday at 12:12 PM	93 KB	PNG im
Screenshot_20230216-121103.png	Yesterday at 12:11 PM	58 KB	PNG im
cert_Root_FQDN.crt	Yesterday at 11:59 AM	1 KB	certifica

7. When done, click on Next then Save & Publish.
8. On the Samsung phone, verify the CA cert was pushed.
9. Go to Settings > Biometrics and Security > Other Security Settings > View Security Certificates



3:51 ⊘ 34%

Other security settings

Credential storage

View security certificates
Display trusted CA certificates

User certificates
View user certificates

Install from phone storage
Install certificates from storage

Clear credentials
Remove all certificates.

Certificate management app

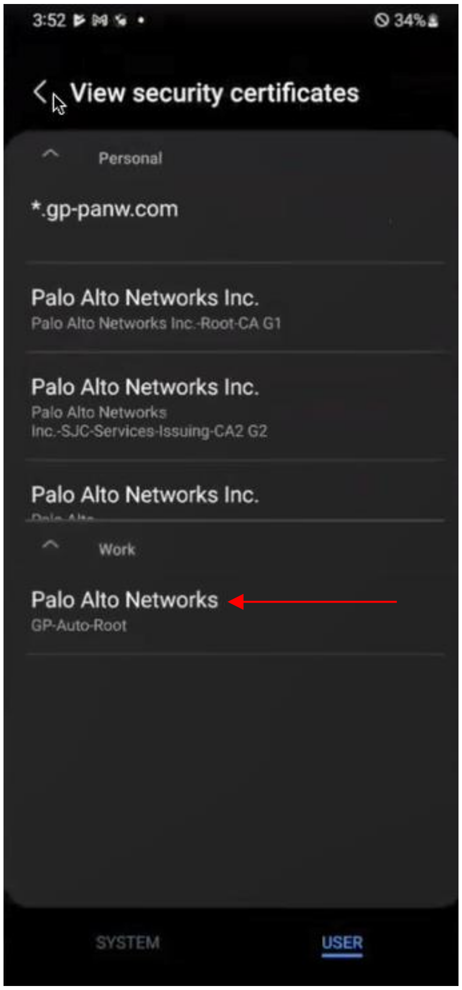
Advanced

Trust agents
Perform selected actions when trusted devices are connected.

Pin windows

Security policy updates
Keep your phone secure with the latest security policy

10. Click on the User tab.
11. Look for your Certificates in the Work section.



View security certificates

Personal

*.gp-panw.com

Palo Alto Networks Inc.
Palo Alto Networks Inc.-Root-CA G1

Palo Alto Networks Inc.
Palo Alto Networks Inc.-SJC-Services-Issuing-CA2 G2

Palo Alto Networks Inc.

Work

Palo Alto Networks
GP-Auto-Root

Deploy the Trusted CA Certificate on the Linux Platform with GlobalProtect

1. Download the certificate to the endpoint and then transfer to the trusted certificate folder
2. sudo cp <CA-Cert.crt> /usr/local/share/ca-certificates
3. sudo cp <CA-Cert.crt> /etc/ssl/certs
4. Perform the following to have the packages be updated with certificates:
    a. sudo dpkg-reconfigure ca-certificates

Or

The Root CAs are stored in Linux keypair (its trust CA anchor store). Extension should be .crt as recommended.

Function	Method
Add	1. Copy your CA to dir /usr/local/share/ca-certificates/[5] Use command: sudo cp foo.crt /usr/local/share/ca-certificates/foo.crt 2. Update the CA store: sudo update-ca-certificates
Remove	1. Remove your CA. 2. Update the CA store: sudo update-ca-certificates --fresh

NOTE: All the CA certificates must be stored in the Linux trust anchor. For example, if the server certificate is signed and issued by Root CA -> Sub CA. Both the CA certificates must be stored in the Linux trust anchor.

[5] On Redhat 8 or later, the directory is /usr/share/pki/ca-trust-source/anchors and the command is “update-ca-trust”