HHS Virtual Private Network (VPN) Compliance Requirements

Each time you login to Palo Alto GlobalProtect VPN, the VPN will perform a security compliance check on your device. This will ensure your device meets HHS VPN security requirements.

Table of Contents

Compliance Requirements

Your device must meet the following security requirements. If your device does not meet these requirements, your VPN access will be denied.
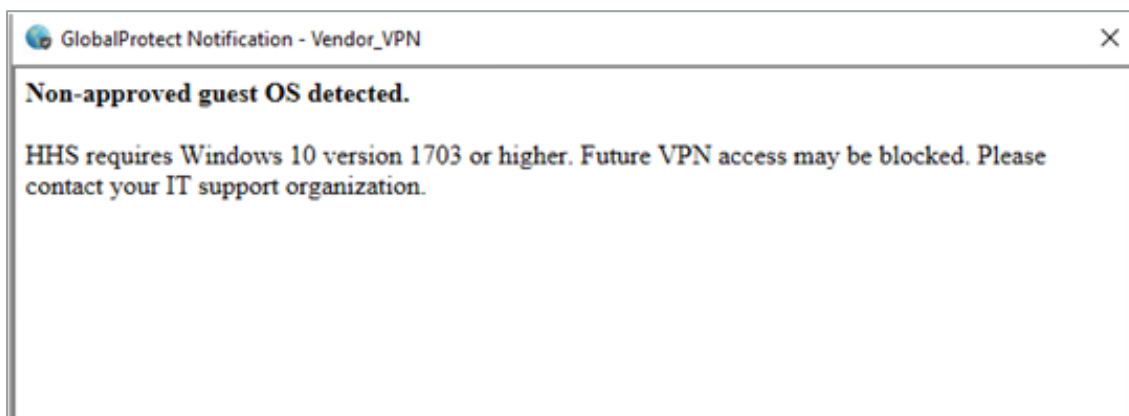
1. **Operating System**:
   - Windows Operating System: At least Windows 10 or greater (includes Windows 11)
   - macOS Operating System: At least macOS 11.7.4 (Big Sur) or greater

2. **Firewall**: You must have any firewall installed and active.

3. **Patch Management**: You must have patch management installed and active on your device.

4. **Antimalware**: You must have any antimalware installed and active on your device. Additionally, signatures should have updated within the past 30 days.

5. **Screensaver**: You must have a screen saver enabled and password protected on your device.
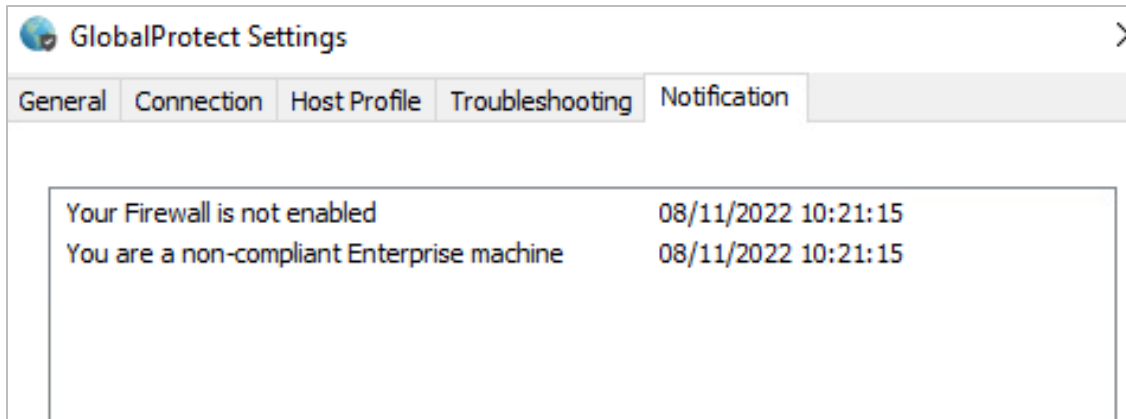
Noncompliance Notifications

You will receive a notification on your device if it is not in compliance with our VPN security requirements.

If you have an IT support organization, we recommend you notify them if you receive a noncompliance notification. They can assist with remediation as some of these requirements may be managed by an IT support organization.

1. You will receive a notification indicating which security requirements your device does not comply with. If your device does not comply with one requirement, it will be listed on the notification. If your device does not comply with multiple requirements, click **More Notifications**.

GlobalProtect Notification - Vendor_VPN   ×

Non-approved guest OS detected.

HHS requires Windows 10 version 1703 or higher. Future VPN access may be blocked. Please contact your IT support organization.

2. You can review all noncompliance notifications in the Notifications tab of GlobalProtect settings.


3. **You will continue to receive noncompliance notifications until all security requirements are met.**

4. Once you believe you have resolved all noncompliance issues, you can confirm your device meets the requirements.

5. While signed into Palo Alto GlobalProtect VPN, open the application. You can use the search feature on your Windows taskbar. Type GlobalProtect, then click **Open**.
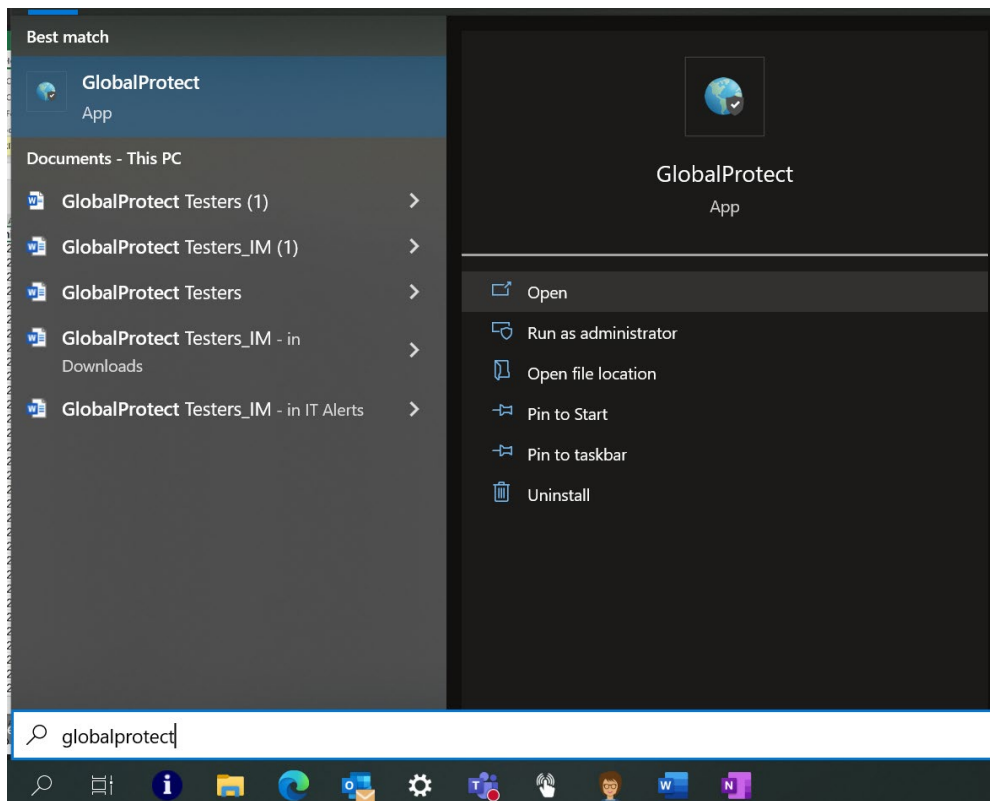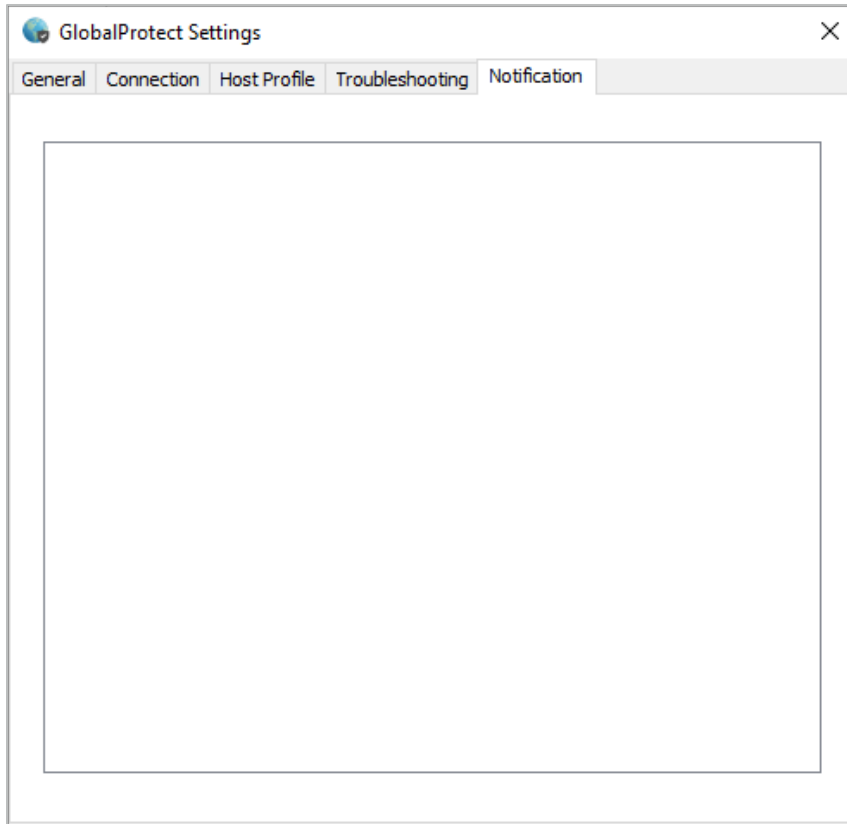
6. Click the Settings button in the top right corner, then click **Settings**.
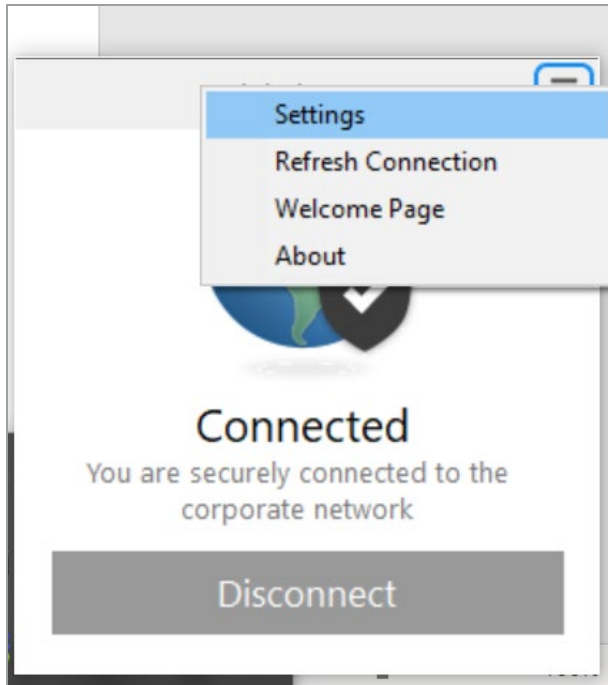
7. Click the Host Profile tab, then click **Resubmit Host Profile**.
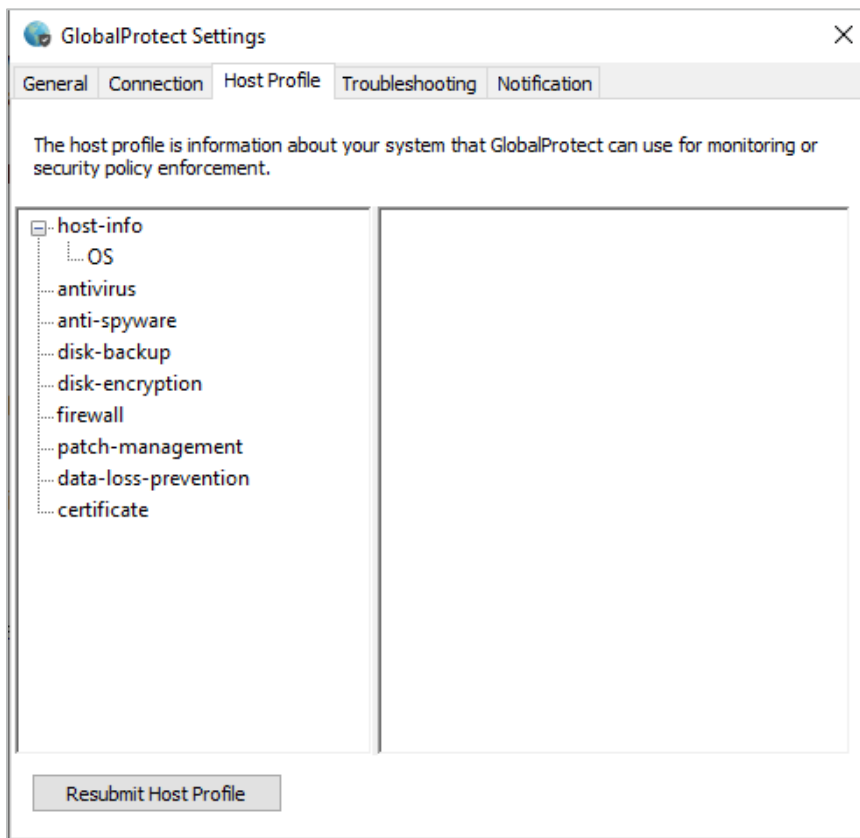
8. If the Notifications tab is now blank, you have resolved all noncompliance issues.

Need help?

Contact your IT support organization for technical support or assistance. For any additional questions, call the HHS IT Help Desk at 855-435-7181 (toll-free) or 512-438-4720, 7 a.m. to 7 p.m. CST, Monday-Friday.