paloalto TECHDOCS

GlobalProtect™ App Release Notes

Version 6.1.2

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

July 27, 2023

Table of Contents

Features Introduced in GlobalProtect App 6.1

The following table describes the new features introduced in GlobalProtect app 6.1. For additional information on how to use the new features in this release, refer to the GlobalProtect App 6.1 New Features Guide.

New GlobalProtect Feature	Description
Advanced Internal Host Detection	You can now configure advanced internal host detection through the portal to add an extra security layer during internal host detection by the GlobalProtect app. Enabling advanced internal host detection stops malicious actors from spoofing the reverse DNS server response during the internal host detection and thereby prevents malicious actors from accessing the enterprise network.
Proxy Auto Configuration (PAC) Deployment from GlobalProtect	You can now configure and push the URL for your proxy auto-configuration (PAC) files to your endpoints through the GlobalProtect portal. This feature enables you to manage the proxy settings for your endpoints using the GlobalProtect app.
End-user Notification about GlobalProtect Session Logout	You can now enable and customize end-user notifications about expiry of GlobalProtect app sessions on the gateway. These notifications inform the end users on Windows, macOS and Linux endpoints in advance when their app sessions are about to expire due to inactivity or expiry of the login lifetime and lets them know how much time is left before the app gets disconnected, preventing unexpected and abrupt app logout.
Simplified and Seamless macOS GlobalProtect App Deployment Using Jamf MDM Integration	You can now use Jamf Pro, one of the most widely used Apple device management platforms, to deploy the GlobalProtect app to macOS endpoints to support large-scale GlobalProtect app deployments in on-premises and Prisma Access environments. Administrators can also provide a seamless user experience for macOS end users by deploying Jamf configuration profiles that can automatically load system and network extensions, thus preventing the user from having to respond to notifications on the GlobalProtect app. Administrators can use Jamf Pro to deploy the GlobalProtect mobile app to macOS endpoints and enable system and network extensions on macOS endpoints using Jamf Pro.
New Linux OS Support for Ubuntu	GlobalProtect is now supported on endpoints running the following Linux OS versions for Ubuntu:

New GlobalProtect Feature	Description
	• Ubuntu 20.04 LTS (CLI-based and GUI-based GlobalProtect app) • Ubuntu 22.04 LTS (CLI-based and GUI-based GlobalProtect app)
New Linux OS Support for Red Hat Enterprise Linux (RHEL)	(GlobalProtect app 6.1.1 and later releases) GlobalProtect is now supported on endpoints running the following Linux OS versions for RHEL. • Red Hat Enterprise Linux (RHEL) 8.7 (CLI-based and GUI-based GlobalProtect app) • Red Hat Enterprise Linux (RHEL) 9.1 (CLI-based and GUI-based GlobalProtect app)
Split DNS and Split Domain (Linux OS)	GlobalProtect now extends Split DNS and Split Tunnel Domain support to Linux platforms in addition to Windows and macOS. With Split DNS, you can configure which domains are resolved by the VPN assigned DNS servers and which domains are resolved by the local DNS servers. With Split Tunnel Domain, you can configure traffic for which domains are included over or excluded from the tunnel. Both Split DNS and Split-tunnel Domain features for Linux are configurable using existing portal and gateway configuration options

Changes to Default Behavior in GlobalProtect App 6.1

The following topics describes changes to default behavior in GlobalProtect app 6.1:

Changes to Default Behavior in GlobalProtect App 6.1.2

There are no changes to default behavior in GlobalProtect app 6.1.2.

Changes to Default Behavior in GlobalProtect App 6.1.1

There are no changes to default behavior in GlobalProtect app 6.1.1.

Changes to Default Behavior in GlobalProtect App 6.1.0

Starting with GlobalProtect app 6.1.0, the End-user Notification about GlobalProtect Session Logout feature is introduced and end users will start seeing notifications. To disable or customize the notifications, you must be running GlobalProtect on PAN-OS 11.0 or later, or on a version of Prisma Access running a 11.0 or later dataplane.

Associated Software and Content Versions

The following minimum Palo Alto Networks software versions are supported with GlobalProtect app 6. 1. Refer to the Compatibility Matrix for additional information about endpoint OS compatibility.

Palo Alto Networks Software or Content Release Version	Minimum Supported Version
PAN-OS version	9.1 and above. End-user Notification about GlobalProtect Session Logout feature starts with GlobalProtect 6.1 and requires PAN-OS 11.0 and above. You cannot disable End-user Notification about GlobalProtect Session Logout unless the PAN-OS version is 11.0 or above.

GlobalProtect App 6.1 Known Issues

The following table lists the known issues in GlobalProtect app 6.1 for Windows, Windows UWP, Linux, and macOS.

Issue	Description
GPC-17099	When the GlobalProtect app for Windows is upgraded to version 6.1.1, devices with Driver Verifier enabled and configured to monitor the PAN virtual adapter driver (pangpd.sys) display the DRIVER_VERIFIER_DETECTED_VIOLATION Blue Screen error.
GPC-15969	On Windows endpoints, the GlobalProtect app sometimes fails to send the Diagnostic report when the end user uses the option to Report an Issue. The Troubleshooting logs are sent successfully.
GPC-16570	When using the embedded browser for SAML authentication with the GlobalProtect app for Linux while installed on operating systems using OpenSSL 3 as the system version and using a portal or gateway running PAN-OS 10.2 or earlier versions, authentication does not work as expected. **Workaround:** Use the default system browser for SAML authentication.

Addressed Issues in GlobalProtect App 6.1

The following topics describe the issues addressed in GlobalProtect 6.1 for , Windows, Windows UWP, macOS, and Linux.

GlobalProtect App 6.1.2 Addressed Issues

The following table lists the issues that are addressed in GlobalProtect app 6.1.2 for Windows, macOS, and Linux.

Issue ID	Description
GPC-18126	Fixed an issue where devices displayed the `DRIVER_VERIFIER_DETECTED_VIOLATION` Blue Screen error when the GlobalProtect app was upgraded from version 5.2.10 to 6.1.1.
GPC-18116	Fixed an issue where Trend Micro XDR detected packet capture processes randomly via GlobalProtect (PanGPS.exe service).
GPC-18073	Fixed an issue where the GlobalProtect app selected an unexpected gateway due to a latency discrepancy seen between PanGPS and packet capture.
GPC-17921	Fixed an issue where, when the language was set to Japanese, the time to connect was not displayed properly when a **Disconnect Timeout** was configured for the app.
GPC-17896	Fixed an issue where users were unable to connect to GlobalProtect gateway when only one external gateway was added due to the following error: `Cannot Verify Server Certificate of Gateway`.
GPC-17771	Fixed an issue where the GlobalProtect app stopped working abruptly.
GPC-17776	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS and GlobalProtect enforcer was configured with allowed FQDNs, users were still able to access the internet and other public domains.
GPC-17762	Fixed an issue where when the GlobalProtect app **Allow User to Disable GlobalProtect App** setting was set to **Allow with Comment**, the option did not work as expected.
GPC-17754	Fixed an issue where the GlobalProtect app did not detect Smart Card removal every time

Issue ID	Description
	the user removed the card and due to which the app was not getting disconnected in On-Demand tunnel mode.
GPC-17740	Fixed an issue where, when the GlobalProtect app was connected through the Prisma Access gateway, the upload speed of the internet was reduced to 2 Mbps.
GPC-17728	Fixed an issue where users were unable to connect to the GlobalProtect gateway when only one external gateway was added due to the following error: `Cannot Verify Server Certificate of Gateway`.
GPC-17718	Fixed an issue where the GlobalProtect app incorrectly detected the firewall status as disabled while the GlobalProtect HIP check detected the device as Windows firewall enabled.
GPC-17556	Fixed an issue where the GlobalProtect app would get stuck in the `Connecting` state when the user tried to close the browser window for SAML authentication after configuring On-Demand mode for the app.
GPC-17598	Fixed an issue on the GlobalProtect app for Linux where, when the GlobalProtect app was connected and the tunnel was up, the DNS requests were sent to the public DNS servers assigned to the physical interface.
GPC-17554	Fixed an issue where the device displayed a Blue Screen error when users upgraded the GlobalProtect version to 6.1.1-5
GPC-17519	Fixed an issue where, when the GlobalProtect app was installed on Linux devices, the file size of the log file (PanGPUI.log.old) increased without getting log rotated.
GPC-17473	Fixed an issue where the GlobalProtect portal and gateway selection list were displayed in the table format and not as menu items.
GPC-17460	Fixed an issue where, when the GlobalProtect app was installed on Windows 10 or

Issue ID	Description
	11 devices, and when the user tried to authenticate using SAML authentication, the app did not display the Terms of Use pop-up on the Welcome page properly.
GPC-17436	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS, the upload speed of the internet was reduced after a version upgrade.
GPC-17406	Fixed an issue where GlobalProtect HIP check did not detect the new version of Trellix Drive Encryption correctly, which caused the device to fail the HIP check.
GPC-17404	Fixed an issue where, when the GlobalProtect app was installed on Windows devices and the app was upgraded from version 5.2.12 to 6.0.5, the device displayed the `DRIVER_VERIFIER_DETECTED_VIOLATION` Blue Screen error.
GPC-17398	Fixed an issue where the **Settings** > **Connection** tab in the GlobalProtect add did not display the **Assigned IP Address(es)** and **Gateway IP Address** properly.
GPC-17393	Fixed an issue where, when the GlobalProtect app was installed on Windows 10 devices and the language was set to Japanese, `IpConfig.txt` and `Systeminfo.txt` in the `GlobalProtectLogs.zip` did not work properly.
GPC-17337	Fixed an issue where the GlobalProtect app disconnected due to a HIP reporting error that prevented the app from sending HIP reports to the gateway.
GPC-17335	Fixed an issue where the user interface of the GlobalProtect app was going oversized when the system woke up from the sleep mode.
GPC-17299	Fixed an issue where the GlobalProtect app did not display LDAP password expiration notification on consecutive connection

Issue ID	Description
	attempts when the user tried to authenticate using the LDAP authentication method.
GPC-17227	Fixed an issue where the tunnel was still up and connected even when the user disconnected the GlobalProtect app.
GPC-17205	Fixed an issue where GlobalProtect failed to decrypt HipPolicy.dat on endpoints, which caused the device to fail the HIP check for anti-malware.
GPC-17137	Fixed an issue where, when the user clicked the Network sign-in icon on the Windows login page, an icon with the name 'image' was displayed instead of the portal IP address/ URL.
GPC-17011	Fixed an issue where the GlobalProtect app tried to send HIP reports even when the device was on Modern Standby mode.
GPC-17000	Fixed an issue where the GlobalProtect app got stuck in the `Connecting` state when the user tried to authenticate with SAML authentication using the embedded browser and clicked Cancel on the certificate prompts.
GPC-16978	Fixed an issue where the GlobalProtect app took a long time to establish a connection due to an erroneous packet capture process.
GPC-16959	Fixed an issue where the Endpoint Traffic Policy Enforcement feature was causing the GlobalProtect app to drop Slack WebSocket outbound traffic on macOS endpoints.
GPC-16851	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS, the app did not try to auto-connect to the gateway after exceeding the **Disable Timeout** value.
GPC-16837	Fixed an issue where the GlobalProtect app (PANGP Virtual Ethernet Adapter) was intermittently disconnected after a system

Issue ID	Description
	reboot though the gateway status displayed it as Connected.
GPC-16662	Fixed an issue where the GlobalProtect app sent the Intermediate Certificate instead of the Server Certificate for OCSP check while performing Certificate authentication on GlobalProtect.
GPC-16655	Fixed an issue where, when configured with the pre-logon connect method, the GlobalProtect app indicated that it was connected, but the tunnel was not established and users were unable to access resources.
GPC-16645	Fixed an issue where the GlobalProtect app couldn't display the Verify text box when using the full 255 characters for Radius DUO Authentication on Windows devices.
GPC-16631	Fixed an issue where GlobalProtect logs forwarded from CDL to syslog-ng and Splunk were arriving in multiline and single line mode randomly.
GPC-16575	Fixed an issue where GlobalProtect users were intermittently unable to log in to the gateway when using the user logon connect method because Enforce GlobalProtect Connection for Network Access was enabled immediately after portal login, blocking access to the gateway login URL.
GPC-16504	Fixed an issue where, when the GlobalProtect app was installed on the Windows devices, the GlobalProtect app failed to send the Diagnostic report when the end user used the option to **Report an Issue**.
GPC-16489	Fixed an issue where the GlobalProtect HIP check did not detect the Chinese anti-malware applications, which caused the device to fail the HIP check.
GPC-16267	Fixed an issue where the portal status did not show as `Connected` even when the portal was accessible after a reboot and the portal status was `Using cached portal`

Issue ID	Description
	`config`, which did not trigger the transparent upgrade.
GPC-16148	Fixed an issue where GlobalProtect notifications were displayed in HTML code instead of formatted text.
GPC-16135	Fixed an issue where the GlobalProtect app connection failed when Windows 10 21H2 users tried to switch to another Windows user account on the device
GPC-16074	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS with SAML authentication, users were unable to connect to the app after the system woke up from sleep mode. The app stayed in `Connecting` state for a long time and users had to refresh the connection.
GPC-16056	Fixed an issue where GlobalProtect HIP check did not detect the name of the Trellix Agent correctly, which caused the device to fail the HIP check.
GPC-16002	Fixed an issue where the GlobalProtect HIP check detected the device as Windows firewall enabled even though the firewall was disabled on the device.
GPC-15976	Fixed an issue where, when the GlobalProtect app was installed on Windows devices, the device displayed a Blue Screen error due to a faulty GlobalProtect app driver.
GPC-15968	Fixed an issue where the GlobalProtect app was stuck in the Connecting state when users failed to authenticate with SAML and using an embedded browser. Users were unable to disconnect the app and had to reboot the device.
GPC-15922	Fixed an issue where, when Connect Before Logon using Security Assertion Markup Language (SAML) authentication was used to log in to the endpoint, the Use Default Browser for SAML Authentication did not

Issue ID	Description
	work as expected with the configured Connect Before Logon option.
GPC-15485	Fixed an issue where the GlobalProtect HIP check did not detect the Real-Time Protection status for the FireEye Endpoint Agent, which caused the device to fail the HIP check.
GPC-15262	Fixed an issue where single sign-on (SSO) for Smart Card were used for authentication, users were prompted to enter PIN instead of password on the Windows login screen.
GPC-15234	Fixed an issue where the app would get stuck at the Connecting state while trying to connect to a gateway.
GPC-15111	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS, the screen reader repeatedly announced tabs, **Add** button, and portals table on the user interface. The screen reader must announce the user interface elements only once.
GPC-15105	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS, the app Home page displayed text in an incorrect color contrast ratio causing readability issues for users.
GPC-15080	Fixed an issue where the split tunnel was configured based on the destination domain, split tunneling did not work as expected when IPv6 traffic exclusion was configured.

GlobalProtect App 6.1.1 Addressed Issues

The following table lists the issues that are addressed in GlobalProtect app 6.1.1 for Windows, macOS, and Linux.

Issue ID	Description
GPC-16324	Fixed an issue where Endpoint Traffic Policy Enforcement dropped IPv6 ICMP neighbor discovery packets causing the IPv6 tunnel to drop.
GPC-16029	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS, users were prompted for certificate selection even when the **Extended Key Usage OID for Client Certificate'** was configured in the App Configurations area of the GlobalProtect portal configuration.
GPC-15989	Fixed an issue where, when the Default System Browser is used for SAML, the GlobalProtect app kept displaying `Connecting` when connected to an internal gateway.
GPC-15994	Fixed an issue where Endpoint Traffic Policy Enforcement interaction with Windows Filter Platform (WFP) and third-party vendors caused intermittent user tunnel drops.
GPC-15972	Fixed an issue where the GlobalProtect HIP check did not detect the Real-Time Protection status correctly for the CrowdStrike Falcon application, which caused the device to fail the HIP check.
GPC-15834	Fixed an issue where the GlobalProtect app got disconnected after HIP check.
GPC-15677	Fixed an issue where, when the GlobalProtect app was installed on macOS, users were prompted for login when the app was installed using the property list (plist) with **On-Demand** connect method.

Issue ID	Description
GPC-15991	Fixed an issue where the GlobalProtect app installer was displaying the wrong Palo Alto Networks logo.
GPC-15534	Fixed an issue where the proxy credential pop-up window did not show when connecting to the GlobalProtect portal after upgrading the GlobalProtect app to version 5.2.5 and above.
GPC-15167	Fixed an issue where when the GlobalProtect app was installed on devices running macOS, the GlobalProtect enforcer continued to block network access even after connecting to the internal gateway.

GlobalProtect App 6.1.0 Addressed Issues

There are no addressed issues in the 6.1.0 release.