GlobalProtect™ App Release Notes

Release 5.1.1 (Windows, Windows UWP, macOS, iOS, Android, and Linux);
Release 5.1.2 (iOS);
Release 5.1.2 (Windows UWP, Android, and Linux);
Release 5.1.3 (iOS);
Release 5.1.3 (Windows and macOS);
Release 5.1.4 (Windows, Windows UWP, macOS, Linux, Android, and iOS);

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS®

Contact Information

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

About the Documentation

- To ensure you are viewing the most current version of this document, or to access 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

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Last Revised

June 10, 2020

Table of Contents

GlobalProtect App 5.1 Release Information

Review important information about Palo Alto Networks GlobalProtect™ app software, including new features introduced and workarounds for open issues.

To ensure that you are viewing the most current version of these Release Notes, always defer to the web version; do not store or rely on PDFs to be current after you download them.

Features Introduced in GlobalProtect App 5.1

The following table describes the new features introduced in GlobalProtect app 5.1. For additional information on how to use the new features in this release, refer to the GlobalProtect App 5.1 New Features Guide.

New GlobalProtect Feature	Description
macOS System Extensions Support	(GlobalProtect app 5.1.4 and later releases) The GlobalProtect App can now use system extensions on macOS Catalina 10.15.4 endpoints for enabling capabilities such as split tunnel on the GlobalProtect gateway and to enforce GlobalProtect connections for network access without requiring kernel extensions. The GlobalProtect App 5.1.4 replaces kernel extensions with system extensions on macOS Catalina 10.15.4. By enabling system extensions on macOS Catalina 10.15.4 endpoints, you can use a split tunnel based on the destination domain and application and to enforce GlobalProtect connections for network access without requiring kernel extensions.
Consolidated Connectivity Messages for the GlobalProtect App for Windows and macOS	(GlobalProtect app 5.1.1 and later releases) To enable a better user experience, the GlobalProtect App for Windows and macOS are updated to display any connectivity errors directly in the app panel.With this change, the messages displayed when users have connectivity issues are consolidated within the app panel so that the pop-up messages do not interrupt the user.
SAML Authentication for the GlobalProtect App for Linux	The GlobalProtect App for Linux now supports Security Assertion Markup Language (SAML). You can authenticate users through SAML authentication in the GUI version and not in the CLI version. *Due to restrictions for Microsoft Azure support for Ubuntu operating systems, the GlobalProtect App for Linux does not support SAML when Microsoft Azure is used as the SAML identity provider.*
GlobalProtect for Windows 10 UWP for ARM64 Devices	GlobalProtect now extends enterprise security protection to enable enforcement of the same next-generation firewall-based policies that are enforced within the physical perimeter to ARM64 devices running Windows Universal Windows Platform (UWP). You can download the GlobalProtect app directly from the Microsoft Store.
GlobalProtect for IoT Devices	GlobalProtect now extends firewall capabilities such as User-ID, App-ID, and HIP to secure traffic from your IoT devices. GlobalProtect for IoT is available for devices running Windows, Ubuntu, Raspbian, and Android. GlobalProtect for IoT operates in headless mode where no UI is present on the device and seamlessly connects to your GlobalProtect gateways. IoT support is available with a GlobalProtect subscription. Host information collection is available with Content Release version 8196-5685 or later.

New GlobalProtect Feature	Description
Graphical User Interface for GlobalProtect App for Linux	GlobalProtect for Linux is now available with a graphical user interface (GUI). Similar to GlobalProtect for Windows and macOS, you can use the GUI to connect to and disconnect from GlobalProtect portal and gateways; receive notifications and errors; enable or disable the app; and view host, connection, and other information about the app. You can also toggle from the CLI to the GUI version as desired.
User Sign-Out Restriction (Windows, macOS, iOS, Android, and Chrome)	You can now prevent or allow users to log out of GlobalProtect. By default, GlobalProtect allows users to sign-out. To customize this GlobalProtect behavior, configure the Allow user to Sign Out from GlobalProtect App option in the App configuration of your GlobalProtect portal. The new option is available with Content Release Version 8196-5685 or later.
Biometric Sign-In Support (Windows, macOS, iOS, and Android)	For enhanced usability, GlobalProtect now supports biometric sign-in. When biometric sign-on is enabled on an endpoint, GlobalProtect can now authenticate using the saved user credentials when a user supplies a finger-print scan that matches a trusted finger-print template on the endpoint. To enable biometric sign-on, configure Save User Credentials as Only with User Fingerprint in the App configuration of your GlobalProtect portal. The minimum PAN-OS 9.1 or a later release.
Single Sign-On (SSO) for macOS Endpoints	The GlobalProtect app now supports single sign-on for macOS endpoints. Single sign-on improves the user experience by reducing the number of times users must enter credentials when they log in. When a user logs in to macOS, the GlobalProtect app acquires and uses the credentials to authenticate with GlobalProtect portal and gateways. To enable single-sign on, set Use Single Sign-on (macOS) to Yes in the App configuration of your GlobalProtect portal. Available with Content Release Version 8196-5685 or later.
GlobalProtect Gateway Latency Reporting	To help you troubleshoot connection and performance issues for a specific user, GlobalProtect now collects and reports telemetry information for latency between the GlobalProtect gateway and the endpoint. Now, you can easily identify the gateway to which the user is connected, the current stage of the connection, and statistics about the pre-tunnel and post-tunnel network latency. To view logs, see the new Monitor > Logs > GlobalProtect section on PAN-OS 9.1 and later releases.
Proxy Handling for macOS Endpoints	The GlobalProtect app can now automatically detect and inherit proxy settings on macOS endpoints. This enables you to deploy GlobalProtect on macOS endpoints that do not have a direct internet connection and that route traffic through a proxy server. GlobalProtect for macOS supports both the use of PAC files and manual proxy configuration. *GlobalProtect does not monitor changes to the proxy settings of the physical adapter. As a result, if an end user changes the proxy settings of the physical adapter after GlobalProtect is connected, the user must manually disconnect and*

New GlobalProtect Feature	Description
	reconnect to enable GlobalProtect to detect and inherit the new settings.
Exclusions to Allow Traffic to Specified Hosts or Networks When Enforce GlobalProtect Connection for Network Access is Enabled and GlobalProtect Connection is not established (Windows and macOS)	To improve user experience when a GlobalProtect connection is not established, you can now provide exclusions to allow traffic to specified hosts or networks for access to local resources although you Enforce GlobalProtect for Network Connection for all users. With this option that is available as a dynamic app configuration, when GlobalProtect is not connected, you can for example exclude link-local addresses and allow access to a local network segment or broadcast domain. You can configure up to ten IP addresses or network segments for which you want to allow access in the Exceptions to Enforce GlobalProtect field of the App configuration of your GlobalProtect portal. Available with Content Version 8196-5685 or later.
New Linux OS Support for Ubuntu	GlobalProtect is now available for endpoints running the following Linux OS versions for Ubuntu: • Ubuntu 20.04 (CLI-based GlobalProtect app only) • Ubuntu 19.04 (CLI-based GlobalProtect app only) • Ubuntu 18.04.3 LTS • Ubuntu 18.04.2 LTS • Ubuntu 18.04.1 LTS (CLI-based GlobalProtect app only) • Ubuntu 18.04 LTS (Only Ubuntu 18.04.3 LTS and Ubuntu 18.04.2 LTS support the GUI-based version of the GlobalProtect app for Linux) • Ubuntu 16.04 (CLI-based GlobalProtect app only) In addition, on these OS versions you can now create HIP objects for use in security policy enforcement.
New Linux OS Support for Red Hat Enterprise Linux	GlobalProtect is now available for endpoints running the following Linux OS versions for Red Hat Enterprise Linux: • Red Hat Enterprise Linux 7.7 • Red Hat Enterprise Linux 7.6 (CLI-based GlobalProtect app only) • Red Hat Enterprise Linux 7.5 (CLI-based GlobalProtect app only) • Red Hat Enterprise Linux 7.4 (CLI-based GlobalProtect app only) • Red Hat Enterprise Linux 7.3 (CLI-based GlobalProtect app only) • Red Hat Enterprise Linux 7.2 (CLI-based GlobalProtect app only) • Red Hat Enterprise Linux 7.1 (CLI-based GlobalProtect app only) • Red Hat Enterprise Linux 7.0 (CLI-based GlobalProtect app only) • Red Hat Enterprise Linux 6.9 (CLI-based GlobalProtect app only) • Red Hat Enterprise Linux 6.8 (CLI-based GlobalProtect app only) In addition, on these OS versions you can now create HIP objects for use in security policy enforcement.
New Linux OS Support for CentOS	GlobalProtect is now available for endpoints running the following Linux OS versions for CentOS: • CentOS 7.7 (CLI-based GlobalProtect app only)

New GlobalProtect Feature	Description
	• CentOS 7.6 • CentOS 7.5 (CLI-based GlobalProtect app only) • CentOS 7.4 (CLI-based GlobalProtect app only) • CentOS 7.3 (CLI-based GlobalProtect app only) • CentOS 7.2 (CLI-based GlobalProtect app only) • CentOS 7.1 (CLI-based GlobalProtect app only) • CentOS 7.0 In addition, on these OS versions you can now create HIP objects for use in security policy enforcement.
Uninstall Option for GlobalProtect(Windows only)	To prevent users from uninstalling the GlobalProtect app and thereby bypassing the Always On GlobalProtect configuration, you can now require a password to uninstall GlobalProtect. To get this password, they must work with your IT administrator or Help Desk team that manages access to the password. Requires PAN-OS 9.1 and Content Version 8207-5750 or later.
Seamless Soft-Token Authentication with RSA SecureID	The GlobalProtect app can now automatically generate and retrieve the password for PIN and no-PIN based one-time password for soft-token authentication with RSA SecureID. The user must specify the PIN on first-use only.
SSL Tunnel Enforcement	To ensure reliable connectivity and a better user experience in networks where an IPSec connection is not permitted or is unreliable, you can configure the GlobalProtect app to connect using SSL instead of using IPSec as the default. Available with Content Version 8207-5750 or later.
SAML SSO for the GlobalProtect app for Android on Chromebooks	The GlobalProtect app for Android now supports SAML single sign-on (SSO) for Chromebooks. End users can authenticate to GlobalProtect by leveraging the same login they use to access their Chromebook device or account. This enables users to connect to GlobalProtect without having to re-enter their credentials in the GlobalProtect app. Requires PAN-OS 9.1 or later.

Changes to Default Behavior in GlobalProtect App 5.1

The following topic describes changes to default behavior in GlobalProtect app 5.1:

Changes to Default Behavior in GlobalProtect App 5.1.4

There are no changes to default behavior in GlobalProtect app 5.1.4.

Changes to Default Behavior in GlobalProtect App 5.1.3

There are no changes to default behavior in GlobalProtect app 5.1.3.

Changes to Default Behavior in GlobalProtect App 5.1.2

There are no changes to default behavior in GlobalProtect app 5.1.2.

Changes to Default Behavior in GlobalProtect App 5.1.1

There are no changes to default behavior in GlobalProtect app 5.1.1.

Changes to Default Behavior in GlobalProtect App 5.1.0

There are no changes to default behavior in GlobalProtect app 5.1.0.

Associated Software and Content Versions

The following minimum software versions are supported with GlobalProtect app 5.1.

Palo Alto Networks Software or Content Release Version	Minimum Supported Version
PAN-OS version	8.0

GlobalProtect App 5.1 Known Issues

The following table describes known issues in the GlobalProtect app 5.1 releases.

Issue ID	Description
GPC-10842	When the Enforce GlobalProtect Connections for Network Access feature is enabled on GlobalProtect on macOS client 10.15.4 or later, the GlobalProtect client continued to stay in connecting state after a system reboot. GlobalProtect connected successfully after a Refresh Connection.
GPC-10839	Safari cannot be added to the application-based split tunnel rule on macOS endpoints.
GPC-10603	When the split tunnel settings based on the destination domains are configured on the GlobalProtect gateway and either Chrome or the Edge browser is used to navigate to these domains on macOS endpoints running macOS Catalina 10.15.4 or later, the `connection reset` errors appear for a few seconds before the website launches.
GPC-10356	When the split tunnel settings are configured to exclude application traffic such as Microsoft Teams and Skype, some excluded traffic are still forwarded through the tunnel.
GPC-10339	The GlobalProtect HIP check does not detect real-time protection for Traps version 6.1.4 and 6.1.5 on Windows 10 endpoints. This issue caused the endpoints to fail the HIP check.
GPC-9980	After logging out and logging in when using the GlobalProtect app for Linux in Always On mode, the intermediate page (Not Connected page) displays for more than 1 second before the Connecting page displays.
GPC-9979	When the GlobalProtect app connects to a portal with a connect method as Always On and an authentication type of SAML, the GlobalProtect app does not attempt to reconnect after a system reboot.
GPC-9415	For the GUI version of the GlobalProtect app for Linux, SAML authentication with Microsoft Azure does not work on Ubuntu 1804 or greater versions.
GPC-9353	When you upgrade Red Hat® Enterprise Linux 7 to Red Hat® Enterprise Linux 8, the operating system displays errors for missing GlobalProtect packages (qt5-qtwebkit) during the upgrade.
GPC-9092	On Chromebooks with the GlobalProtect app for Android, after refreshing the configuration or disabling and re-enabling the app, GlobalProtect reports a `portal not found` error. **Workaround**: Refresh the configuration again to trigger the connection.
GPC-9043	On iOS devices where you enable the user to save user credentials after supplying a trusted fingerprint, when you refresh the connection, the GlobalProtect app displays an `Authentication Failed` error.

Issue ID	Description
GPC-8934	The GlobalProtect app for Linux GUI does not display the network name when GlobalProtect is disconnected as it does for other GlobalProtect app versions.
GPC-7017	When users run the GlobalProtect app for Android on their Chromebooks, the app cannot connect to GlobalProtect gateways based on the source IP address of the user because it runs within the Android container on Chrome OS. The Android container uses a network bridge to connect the app to the network, so it is assigned a different IP address from the source IP address of the Chromebook user. **Workaround**: Ensure that gateway selection for the Android operating system is not based on the source IP address of the user by leaving both the Region and IP Address fields empty in the config selection criteria for your client settings configuration (Network > GlobalProtect > Gateways > <*gateway-config*> > Agent > Client Settings > <*client-settings-config*> > Config Selection Criteria).
GPC-6878	When users run the GlobalProtect app for Android on their Chromebooks, the app cannot connect to GlobalProtect portals using IPv6 because it runs within the Android container in Chrome OS, which does not currently support IPv6. **Workaround**: Set the IP Address Type for your GlobalProtect portal to IPv4 Only (Network > GlobalProtect > Portals > <<*portal-config*> > General).
GPC-6792	The GlobalProtect app does not support portal hostnames with non-English characters.
GPC-6456	When users establish a GlobalProtect connection for the first time on iPads running iOS 11.1, and they Don’t Allow GlobalProtect to send them notifications, the Settings -> GlobalProtect link on subsequent notification permission reminders does not open. **Workaround**: Upgrade your iPad to iOS 11.3 or a later version. If you remain on iOS 11.1, you can enable GlobalProtect to send you notifications by going to the GlobalProtect notification settings on your iPad (Settings > Notifications > GlobalProtect) and then selecting Allow Notifications.
GPC-4856	On macOS endpoints, the GlobalProtect app can’t detect the following Anti-Malware information for the HIP Match log details of the Gatekeeper security feature (Monitor > Logs > HIP Match > <*hip-match-log*>): • Engine Version • Definition Version • Date • Last Scanned
GPC-3794	When a user first logs in to a GlobalProtect VPN that uses SAML authentication with pre-logon enabled, the tunnel rename (from pre-logon to user logon) fails, the pre-logon tunnel is disconnected, and the user is prompted to re-authenticate.

Issue ID	Description
PAN-109759	The firewall does not generate a notification for the GlobalProtect app when the firewall denies an unencrypted TLS session due to an authentication policy match.

Addressed Issues in GlobalProtect App 5.1

The following topic describes the issues addressed in GlobalProtect app 5.1 for Android, iOS, Chrome, Windows, Windows 10 UWP, macOS, and Linux.

GlobalProtect App 5.1.4 Addressed Issues (Windows, macOS, Windows 10 UWP, Linux, Android, and iOS)

The following table lists the issues that are addressed in GlobalProtect app 5.1.4 for Windows, Windows 10 UWP, macOS, Linux, Android, and iOS.

Issue ID	Description
GPC-10843	Fixed an issue where, when the GlobalProtect app was installed on iOS endpoints, the app did not automatically reconnect to the external gateway when users moved from the internal network to the external network.
GPC-10818	Fixed an issue where, when the GlobalProtect app was installed on macOS devices, the HIP process restarted multiple times.
GPC-10785	Fixed an issue where the Only with User Fingerprint option was enabled on the GlobalProtect client even though this option was not configured on the portal.
GPC-10745	Fixed an issue where authentication to the GlobalProtect gateway failed as the challenge response for multi-factor authentication was sent to the portal and not to the gateway. This issue occurred when the pre-logon tunnel was not renamed to the user tunnel and the user tried to authenticate to the gateway. With this fix, GlobalProtect authentication is now successful.
GPC-10736	Fixed an issue where the GlobalProtect client on macOS endpoints did not select the client certificate when the certificate did not have the client authentication enabled for the Extended Key Usage.
GPC-10682	Fixed an issue where, when the GlobalProtect app was installed on Linux, **domain.com** was sent in the HIP profile instead of the correct domain.
GPC-10679	Fixed an issue where, when the GlobalProtect app was installed on macOS, the GlobalProtect client tried to connect to the portal after the installation when the On-Demand connect method was defined in the property list (plist).
GPC-10665	Fixed an issue where, when the GlobalProtect app was installed on Windows using Security Assertion Markup Language (SAML) authentication and the Allow user to Sign

Issue ID	Description
	Out from GlobalProtect App option was set to Yes, the username and Sign Out button were not displayed on the app even when the Save User Credentials option was set to No.
GPC-10649	Fixed an issue where, when the GlobalProtect app was installed on Linux, GlobalProtect failed to send an XML compliant HIP report to the firewall.
GPC-10619	Fixed an issue where the GlobalProtect Refresh Connection window displayed the wrong French characters when the system language was French.
GPC-10591	Fixed an issue where, when the GlobalProtect app was installed on Windows, the app failed to download the software from the portal when the proxy auto-configuration files were used.
GPC-10590	Fixed an issue where, when the GlobalProtect app was installed on Windows UWP, the app failed to connect to the portal or gateway when multi-factor authentication (MFA) was used.
GPC-10580	Fixed an issue where the GlobalProtect client failed to authenticate to the Prisma Access gateway when multi-factor authentication was used.
GPC-10575	Fixed an issue where, when the GlobalProtect app was installed on macOS devices running macOS Catalina 10.15.4, the app restarted multiple times and was not able to connect to the gateway.
GPC-10566	Fixed an issue where, when the GlobalProtect app was installed on Windows, the Pre-logon then On-demand connect method did not work properly. When you set the Pre-logon Tunnel Rename Timeout value to 0, GlobalProtect established a user tunnel after users logged in to the endpoint instead of remaining disconnected (On-Demand mode).
GPC-10565	Fixed an issue where, when the GlobalProtect app was installed on Linux, the app did not send the complete HIP report due to many missing patch management entries and caused parsing issues on the gateway.
GPC-10553	Fixed an issue where, when the GlobalProtect app was installed on Windows in On-Demand mode, the app was disconnected from the tunnel, and the HIP report was not sent to the gateway even when the gateway was selected manually after the device reboot.
GPC-10542	Fixed an issue where users were prompted to enter their credentials on the GlobalProtect app 5.0.9 every time their macOS device running macOS Catalina 10.15.3 reboots.
GPC-10477	Fixed an issue where the GlobalProtect HIP check did not detect real-time protection for Traps version 7.0.1 on Windows 10 endpoints, which caused the endpoints to fail the HIP check.
GPC-10469	Fixed an issue on Windows endpoints where, if the GlobalProtect app is configured with the Pre-logon (Always On) Connect Method and users disable the app and reboot their endpoint, the pre-logon tunnel is up after they login.

Issue ID	Description
GPC-10454	Fixed an issue where the firewall failed to parse HIP reports when the file synchronization tool was installed on macOS endpoints.
GPC-10338	Fixed an issue where, after you upgraded the GlobalProtect app from 5.0.x release to 5.1.1 release on Windows endpoints, the username displayed Chinese characters instead of English characters.
GPC-10295	Fixed an issue where, when a split tunnel based on the destination domain was configured on macOS Catalina 10.15.4 endpoints, all Safari-based traffic and all Mac App Store-based traffic that were defined in the split tunnel configuration were dropped. The same issue also occurred when you configured a split tunnel based on the applications downloaded from the Mac App Store. All traffic that was created for the configured applications were dropped. With this fix, traffic defined in the split tunnel configuration will not be dropped using Safari.
GPC-10241	Fixed an issue where the grace period decreased and GlobalProtect is disconnected even after gateway authentication was successful for the switch to the new user.
GPC-10200	Fixed an issue where, when the GlobalProtect app was installed on Android devices, the app failed to reconnect and continued to stay in connecting state. Users had to close and launch the app to establish the connection.
GPC-9992	Fixed an issue where the GlobalProtect HIP process (PanGpHip) on Windows endpoints caused high CPU usage on the endpoint even when users remain idle.

GlobalProtect App 5.1.3 Addressed Issues (Windows and macOS)

The following table lists the issues that are addressed in GlobalProtect app 5.1.3 for Windows and macOS.

Issue ID	Description
GPC-10574	Fixed an issue where, when the GlobalProtect app was installed on Windows with a different language other than English (for example, Spanish), the GlobalProtect agent was continuously restarted.
GPC-10535	Fixed an issue where, after you upgraded the GlobalProtect app from 5.0.x release to 5.1.1 release on a macOS device, users were prompted to re-enter their password even when the saved password was set to **Yes**. With this fix, users will not be prompted to re-enter their password after the upgrade. For GlobalProtect to access user credentials from the login keychain, the following Keychain Pop-Up message will appear: `GlobalProtect wants to use your confidential information stored in "GlobalProtect" in your keychain.` Users are prompted to enter their password and then select Always Allow so that the Keychain Pop-Up prompt does not appear again.

Issue ID	Description
GPC-10468	Fixed an issue where, when the GlobalProtect app was installed on Windows, two OpenSSL DLL files in 64-bit were not signed by a Palo Alto Networks certificate. This issue caused a problem for some endpoint protection applications.
GPC-10403	Fixed an issue where the GlobalProtect app for macOS was disabled and the Disable Timeout (min) value expired, GlobalProtect could reconnect and user credentials were not preserved.
GPC-10395	Fixed an issue where the GlobalProtect app for macOS version 5.1.1 could not be properly installed because the GlobalProtect service failed to launch.

GPC-10380	Fixed an issue where the GlobalProtect app on macOS displayed the following error message when all the gateways were configured as **Manual Only** priority:
	`Could not connect to Gateway, Contact your IT administrator`
	With this fix, the app now displays the following message:
	`Please select a gateway to connect manually`

GPC-10341	Fixed an issue on Windows endpoints where, after the endpoint woke up from sleep mode, the GlobalProtect app was disconnected and then attempted to reconnect to the portal or gateway.
GPC-10311	Fixed an issue where, when the GlobalProtect app was installed on macOS and Windows, cookie authentication was successful even when the wrong password was used and GlobalProtect was still connected after users sign out of the app. With this fix, authentication cookies are now deleted from the system when users sign out of the app.
GPC-10288	Fixed an issue where, when GlobalProtect was installed using the Windows Installer (Msiexec) with on-demand as the connect method, GlobalProtect automatically tried to connect to the portal.
GPC-10261	Fixed an issue where the GlobalProtect app displayed the customized Captive Portal Detection Message in the wrong format when a different language was used other than English.
GPC-10227	Fixed a connectivity issue where, when the GlobalProtect app was installed for macOS Catalina, the GlobalProtect connection was periodically lost.
GPC-10228	Fixed an issue where the GlobalProtect app detected the presence of a captive portal even though it was not present.
GPC-10118	Fixed a periodic issue where the GlobalProtect tunnel failed to be restored after waking up from sleep mode. This issue occurred when on-demand was used as the connect method.
GPC-10024	Fixed an issue where, after upgrading to GlobalProtect 5.0.6, the GlobalProtect HIP check did not detect that Symantec Endpoint Protection 14.2 real-time protection was enabled, which caused the device to fail the HIP check.

Issue ID	Description
GPC-10190	Fixed an issue where the GlobalProtect app on macOS failed to find the correct certificate for authentication to the gateway, when the object identifier (OID) was specified in the plist. With this fix, when you provide the Key Usage OID in the plist, the GlobalProtect app uses the correct certificate.
GPC-9913	Fixed an issue where the portal configuration selection criteria failed when the certificate was signed with the version 2 template.
GPC-9779	Fixed an issue that caused the GlobalProtect app to install a default route with the same metric as the system default route, when split-tunneling based on access route and destination domain was enabled. This issue caused some excluded traffic to go through the tunnel.
GPC-9730	Fixed an issue where GlobalProtect failed to connect to the external gateway when the proxy was not reachable outside of the corporate network until the GlobalProtect service or the desktop was restarted.
GPC-9500	Fixed an issue in GlobalProtect for macOS endpoints where installing or upgrading the package using a Mobile Device Management (MDM) solution such as JAMF Pro resulted in a GlobalProtect app initialization failure.

GlobalProtect App 5.1.3 Addressed Issues (iOS Only)

The following table lists the issues that are addressed in GlobalProtect app 5.1.3 for iOS.

Issue ID	Description
GPC-10334	Fixed an issue with the GlobalProtect app on iOS that occurred when two VPN profiles (one device-level VPN profile and one per-app VPN profile) were pushed from the mobile device management (MDM) server. This issue occurred when users initiated the per-App VPN connection using one iOS app that was whitelisted. The GlobalProtect app displayed the status as “Disconnected” and the app did not respond to TAP TO CONNECT. This prevented users from disconnecting from the per-App tunnel and establishing a device-level VPN tunnel.
GPC-10303	Fixed an issue where, when GlobalProtect was installed on iOS endpoints, the GlobalProtect app displayed the `Can’t end Background Task` error message from the GlobalProtect agent logs. This issue occurred periodically when TAP TO CONNECT was used to establish the GlobalProtect connection from the home screen.
GPC-10229	Fixed an issue where, when GlobalProtect was installed on iOS endpoints, the GlobalProtect app failed to perform a successful network discovery when there was a region mismatch between the portal and the gateway.
GPC-9135	Fixed an issue where, when GlobalProtect was installed on iOS devices, the GlobalProtect app did not display a specific notification message when the GlobalProtect session has timed out.

GlobalProtect App 5.1.2 Addressed Issues (Android, Windows 10 UWP, and Linux)

The following table lists the issues that are addressed in GlobalProtect app 5.1.2 for Android, Windows 10 UWP, and Linux.

Issue ID	Description
GPC-10444	Fixed an issue where, when the GlobalProtect Android app was installed on Chromebooks, the GlobalProtect app failed to connect to the tunnel because GlobalProtect was not running.
GPC-10370	Fixed an issue where, when the GlobalProtect app was installed on Android endpoints, the app hangs and the VPN connection failed to be restored. This issue occurred when users switch from an external network to an internal network after the Automatic Restoration of VPN Connection Timeout option was set to **Yes**.
GPC-10362	Fixed an issue where client certificate authentication was failing on Android 10 devices even when the certificate was manually selected.
GPC-10348	Fixed an issue where, when the GlobalProtect app was upgraded to 5.1.1 on an Android device, the client could no longer connect to the gateway with the custom port configuration.
GPC-9135	Fixed an issue where, when GlobalProtect was installed on Android devices, the GlobalProtect app did not display a specific notification message when the GlobalProtect session has timed out.

GlobalProtect App 5.1.2 Addressed Issues (iOS Only)

The following table lists the issues that are addressed in GlobalProtect app 5.1.2 for iOS.

Issue ID	Description
GPC-10011	Fixed a graphical user interface issue with the GlobalProtect app that occurred when the device-level VPN profile and the per-app VPN profile were pushed from the mobile device management (MDM) server. This issue occurred when users initiated the VPN connection from the iOS VPN settings (Settings > General > VPN), and the GlobalProtect app automatically transitioned to “Connected”. After a VPN connection was established and the app was launched, the graphical user interface still displayed “Disconnected” even though the VPN connection was actually running in the background.
GPC-10173	Fixed an issue where, when GlobalProtect was installed for iOS and Security Assertion Markup Language (SAML) was used to authenticate mobile users, the GlobalProtect app did not send information about the mobile device such as the operating system and the browser User-Agent string.

GlobalProtect App 5.1.1 Addressed Issues

The following table lists the issues that are addressed in GlobalProtect app 5.1.1 for Android, macOS, iOS, Windows, Windows 10 UWP, and Linux.

Issue ID	Description
GPC-10006	Fixed an issue where the GlobalProtect app was upgraded to 5.1.0 on an iOS device. This issue occurred because the GlobalProtect was restarted during portal or gateway authentication.
GPC-10239	Fixed an issue where, when GlobalProtect was installed for Android 10, the GlobalProtect app was not able to use the client certificate for authentication. This issue occurred when the client certificate was created with an algorithm other than RSA.
GPC-10260	Fixed an issue where, when GlobalProtect was installed for Windows UWP, the GlobalProtect app crashed when traffic was sent through the IPSec tunnel.
GPC-10174	Fixed an issue where, when GlobalProtect was installed for Android and Security Assertion Markup Language (SAML) was used to authenticate mobile users, the GlobalProtect app did not send the complete information about the mobile device such as the User-Agent string for the web browser. With this fix, the GlobalProtect app can now send the device information while performing SAML authentication.
GPC-10162	Fixed an issue where, when GlobalProtect was installed for macOS, the GlobalProtect client used the expired certificate instead of the new certificate for portal authentication. This issue occurred when both expired and new certificates were installed for macOS. With this fix, the GlobalProtect client will no longer use the expired certificate for authentication.
GPC-10140	Fixed an issue where, when GlobalProtect was installed on CentOS, the GlobalProtect portal or gateway authentication prompt did not display the customized authentication messages that were configured in the portal configuration. With this fix, the customized authentication messages are now displayed correctly.
GPC-10136	Fixed a connectivity issue where GlobalProtect failed to reconnect to the network. This issue occurred when different portal configurations were pushed from a mobile device management (MDM) system one at a time.
GPC-10110	Fixed an issue where the GlobalProtect client was not enabled automatically after a reboot even when the duration timer has expired. This issue occurred when the GlobalProtect client was disabled and your system was rebooted. With this fix, the GlobalProtect client will now be enabled automatically even after a reboot.
GPC-10108	Fixed an issue where GlobalProtect crashed on macOS devices when the Automatic Proxy Configuration was enabled.
GPC-10100	Fixed an issue where, when the GlobalProtect Android app was installed on Chromebooks with **On-Demand** mode, the GlobalProtect app failed to connect to the tunnel after the device was in “sleep” mode.

Issue ID	Description
GPC-10037	Fixed an issue where the IPSec connection failed on a dual stack environment. This issue occurred when the IPv6 preferred option was set to No.
GPC-10023	Fixed an issue where, when the GlobalProtect Android app was installed on Chromebooks with **Always On** mode and managed using the Google Admin console, the device did not reconnect after a reboot.
GPC-9959	Fixed an issue where macOS users could not connect to the GlobalProtect gateway during manual gateway selection. This issue occurred because the portal and gateway were configured to authenticate users through Security Assertion Markup Language (SAML) authentication with the On-Demand connect method. With this fix, users can now connect to the manual gateway upon the first attempt.
GPC-9855	Fixed an issue where the GlobalProtect App for macOS did overwrite the local DNS search domains with the tunnel DNS search domains. This occurred when the "Append Local Search Domains to Tunnel DNS Suffixes (macOS Only)" app setting was set to "No" in the portal agent configuration. With this fix, the tunnel DNS search domains are now appended with the local DNS search domains when the "Append Local Search Domains to Tunnel DNS Suffixes (macOS Only)" app setting is set to "Yes" in the portal agent configuration.
GPC-9463	Fixed an issue where Ubuntu 19.04 did not display the GlobalProtect system tray icon or the app could not be launched by clicking the system tray icon.
GPC-8743	Fixed an issue where the GlobalProtect app was frequently generating the pop-up dialog to request that you change your password even when the password was not set to expire.

GlobalProtect App 5.1.0 Addressed Issues (Android Only)

The following table lists the issues that are addressed in GlobalProtect app 5.1.0 for Android.

Issue ID	Description
GPC-10099	Fixed an issue where GlobalProtect app for Android could not be properly connected with two-factor authentication due to a change in the default value for the TCP Receive Timeout (sec) option. With this fix, the default is now 30 seconds.

Getting Help

The following topics provide information on where to find more about this release and how to request support:

- Related Documentation
- Requesting Support

Related Documentation

Refer to the following documents on the Technical Documentation portal for more information on our products:

- For more information on GlobalProtect™, refer to the GlobalProtect Administrator’s Guide.
- For other related content, including Knowledge Base articles and videos, search the Technical Documentation portal.

Requesting Support

To contact support, get information on support programs, manage your accounts or devices, or open a support case, visit the Palo Alto Networks Support site.

To provide feedback on the documentation, please write to us at: **documentation@paloaltonetworks.com**.

Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

https://www.paloaltonetworks.com/company/contact-support

Palo Alto Networks, Inc.

www.paloaltonetworks.com