GlobalProtect™ App Release Notes

Release 5.1.1 (Windows, Windows UWP, Mac, iOS, Android, and Linux);

Release 5.1.2 (iOS)

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

- 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

Last Revised

February 27, 2020

Table of Contents

GlobalProtect App 5.1 Release Information

Revision Date: February 27, 2020

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
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.
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

New GlobalProtect Feature	Description
	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 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	GlobalProtect is now available for endpoints running the following Linux OS versions: • Ubuntu 19.04 (CLI-based GlobalProtect app only)

New GlobalProtect Feature	Description
	• 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) • 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) • CentOS 7.7 (CLI-based GlobalProtect app only) • 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	The GlobalProtect app for Android now supports SAML single sign-on (SSO) for Chromebooks. End users can authenticate to GlobalProtect by leveraging

New GlobalProtect Feature	Description
for Android on Chromebooks	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 5.1.1
- Changes to Default Behavior in GlobalProtect App 5.1.0

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-10252	After the client upgrades the GlobalProtect app to 5.1.1 on a Mac device, the predefined GlobalProtect portals are removed except for the active portal.
GPC-10006	After the client upgrades the GlobalProtect app to 5.1.0 on an iOS device, the GlobalProtect service (PanGPS) restarts during portal or gateway authentication.
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.
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 >

Issue ID	Description
	<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.
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, Mac, and Linux.

- GlobalProtect App 5.1.1 Addressed Issues
- GlobalProtect App 5.1.0 Addressed Issues (Android Only)

GlobalProtect App 5.1.2 Addressed Issues

The following table lists the issues that are address 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 the complete information about the mobile device such as the operating system and the browser User-Agent string. With this fix, the GlobalProtect app can now send the device information while performing SAML authentication.

GlobalProtect App 5.1.1 Addressed Issues

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

Issue ID	Description
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.

Issue ID	Description
GPC-10162	Fixed an issue where, when GlobalProtect was installed for Mac, 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 Mac. 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-10133	Fixed a network connectivity issue where GlobalProtect would open the modal dialog if the portal was down or unreachable. With this fix, the connectivity error message is now displayed in the GlobalProtect app window.
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 the GlobalProtect service (PanGPS) 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.
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 Mac 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 (Mac 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 (Mac Only)” app setting is set to “Yes” in the portal agent configuration.

Issue ID	Description
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-9230	Fixed an issue where the Network Location Awareness (NLA) service detected the GlobalProtect interface as public instead of domain.
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