paloalto TECHDOCS

GlobalProtect™ App Release Notes

Version 6.1

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

October 23, 2024

Table of Contents

Features Introduced

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
Embedded Browser Framework Upgrade	Starting with GlobalProtect 6.1.5, the embedded browser framework for SAML authentication has been upgraded to Microsoft Edge WebView2 (Windows) and WebKit (macOS). This provides a consistent experience between the embedded browser and the GlobalProtect client. WebView2 and WebKit are also compatible with FIDO2-based authentication methods. For more information, see the Microsoft Edge WebView2 documentation. By default, tenants using SAML authentication are configured to utilize the embedded WebView2 (Windows) or WebKit (macOS) instead of relying on the system's default browser. With this enhancement, there's no need for end users to configure a SAML landing page, eliminating the necessity to manually close the browser. This streamlines the authentication process. In a Microsoft entra-joined environment with SSO enabled, users are not required to enter their credentials in order to authenticate to Prisma Access using GlobalProtect. This seamless experience is true whether the user is logging in to their environment for the first time or whether they have logged in before. If there is an error during the authentication, it is displayed in the embedded browser. This authentication process works across all device states. In a non entra-joined environment with SSO enabled, users must enter their credentials during the initial login. On subsequent logins, the credentials are auto-filled as long as the SAML identity provider (IdP) session is active and has not timed out.
Share Sheet Support	You can now use the iOS and Android Share Sheet to share GlobalProtect logs. The iOS Share Sheet is supported on GlobalProtect 6.1.0 and later releases and Android Share Sheet is supported on GlobalProtect 6.1.5 (iOS and Android) and later releases.
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)	You can now configure and push the URL for your proxy auto-configuration (PAC) files to your endpoints through the GlobalProtect portal. This feature

New GlobalProtect Feature	Description
Deployment from GlobalProtect	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 manage and deploy the GlobalProtect mobile app for macOS, 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: • 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.

New GlobalProtect Feature	Description
	Both Split DNS and Split-tunnel Domain features for Linux are configurable using existing portal and gateway configuration options
Deploy the GlobalProtect App for iOS using Jamf Pro	You can now use Jamf Pro, one of the most widely used Apple device management platforms, to deploy the GlobalProtect app to iOS endpoints. Administrators can manage and deploy the GlobalProtect app for iOS using Jamf Pro.
Split DNS (iOS) (Requires GlobalProtect app 6.1.6 or later versions)	GlobalProtect now extends Split DNS support to iOS platforms in addition to Linux, Windows, and macOS. With Split DNS , you can configure which domains are resolved by the GlobalProtect gateway assigned DNS servers and which domains are resolved by the local DNS servers.

Changes to Default Behavior

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

Changes to Default Behavior in GlobalProtect App 6.1.6

There are no changes to default behavior in GlobalProtect app 6.1.6.

Changes to Default Behavior in GlobalProtect App 6.1.5

There are no changes to default behavior in GlobalProtect app 6.1.5.

Changes to Default Behavior in GlobalProtect App 6.1.4

(iOS only) Starting with GlobalProtect app 6.1.4, a disclosure notice is displayed when you open the GlobalProtect App for iOS for the first time after installing it. If you already have GlobalProtect in your environment, the notice is displayed the next time you open the GlobalProtect app. Click **Continue** to proceed using the product.

Changes to Default Behavior in GlobalProtect App 6.1.3

There are no changes to default behavior in GlobalProtect app 6.1.3.

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.

Known Issues

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

Issue	Description
GPC-19499	On Linux endpoints, the Firefox browser stops working when you try to connect the GlobalProtect app with the SAML default browser.
GPC-17099 Fixed in GlobalProtect app 6.1.2	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

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

GlobalProtect App 6.1.4-c720 Addressed Issues

This release contains security-related fixes.

GlobalProtect App 6.1.6 Addressed Issues (iOS)

There are no addressed issues in GlobalProtect app 6.1.6 for iOS.

GlobalProtect App 6.1.5 Addressed Issues (Android)

The following table lists the issue that is addressed in GlobalProtect app 6.1.5 for Android.

Issue ID	Description
GPC-20071	Resolved an issue where when the GlobalProtect app is installed on Android devices, the Host ID column of the Strata Logging Service (formerly CDL) log did not display the mobile-id setting value.

GlobalProtect App 6.1.5 Addressed Issues (Windows and macOS)

The following table lists the issues that are addressed in GlobalProtect app 6.1.5 for Windows and macOS.

Issue ID	Description
GPC-20562	Resolved an issue where some users are unable to play YouTube videos.
GPC-20243	Fixed an issue where, when the GlobalProtect app was used with an embedded browser, the browser displayed ‘can't reach page’ due to a Windows filter driver issue.
GPC-20091	Fixed an issue where pre-logon failed when the computer was rebooted.
GPC-20080	Fixed an issue where the GlobalProtect logs displayed different event messages for Windows and macOS devices when the **Allow User to Disable GlobalProtect App** was set to **Allow with Passcode** for the GlobalProtect app.
GPC-20060	Fixed an issue where it was possible for the GlobalProtect enforcer to be disabled when there was a network change during portal authentication.
GPC-20040	Resolved an issue where GlobalProtect did not re-check for internal gateways when using cached portal configuration and an external network was previously detected.
GPC-19961	Fixed an issue where the hamburger menu on the GlobalProtect app was disabled and end users were unable to click on the **Report an Issue** option when the GlobalProtect app was disabled in **Always-On** mode.
GPC-19948	Fixed an issue where connection to the GlobalProtect portal failed with the error **Username from CAS SSO response is different from the input**.

Issue ID	Description
GPC-19924	Fixed an issue where the users faced intermittent connection issues while accessing GlobalProtect using an embedded browser.
GPC-19901	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS, the app got disconnected and reconnected intermittently.
GPC-19833	Fixed an issue where, when the GlobalProtect app was installed on Windows devices, the Smart card (Yubikey) authentication did not work when the device woke up from sleep mode.
GPC-19829	Fixed an issue where the manual gateway login failed when users tried to login using their username and password.
GPC-19794	Resolved an issue where users had login issues on MAC devices when the enforcer was enabled.
GPC-19790	Resolved an issue where users running GlobalProtect version 6.0.5-30 had a connection failure when connecting to a hotspot.
GPC-19686	Fixed an issue where translation errors were observed in the GlobalProtect app for French localization.
GPC-19659	Fixed an issue where macOS users were connected to the GlobalProtect app before they agreed to their company's terms of service.
GPC-19630	Fixed an issue where the prelogon connect method failed on the Globalprotect gateway prelogin stage.
GPC-19686	Fixed an issue where translation errors were observed in the GlobalProtect app for French localization.
GPC-19901	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS, the app got disconnected and reconnected intermittently.
GPC-19818	Fixed an issue where, when the GlobalProtect app was installed on devices running macOs and when the Enforcer was enabled, Jamf connect was not

Issue ID	Description
	working after the MacBook was rebooted. Users had to log in manually.
GPC-19712	Fixed an issue where PanGPS did not work on GlobalProtect app version 6.0.4 due to invalid memory reference and users were unable to reconnect to the GlobalProtect app after a system reboot.
GPC-19696	Fixed an issue where, when the GlobalProtect app was installed on endpoints running macOS and the split tunnel was configured based on the application for Zoom, users were unable to access any sites when the split tunnel was disabled for Zoom and moved to full tunnel.
GPC-19659	Fixed an issue where macOS users were connected to the GlobalProtect app before they agreed to their company's terms of service.
GPC-19652	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS, users were unable to access the applications and websites when the app got disconnected and reconnected while switching the medium from wired to wireless and vice versa.
GPC-19610	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS, end users were not prompted to enter a password and the app got stuck in Restoring VPN connection state until the cookie was deleted.
GPC-19605	Fixed an issue where the GlobalProtect app went missing from the endpoints after an upgrade from app version 6.0.5-35 to 6.0.8-601.
GPC-19603	Fixed an issue where the GlobalProtect app displayed a generic SAML login page and not the actual login page for authentication and the connection was not established when cached portal configuration was used.
GPC-19570	Fixed an issue where a hyperlink in a HIP notification opened in the GPO-disabled Internet Explorer 11 browser instead of the default browser.

Issue ID	Description
GPC-19545	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS, users were unable to connect to the GlobalProtect app when they used T-Mobile iPhone hotspot.
GPC-19513	Fixed an issue where the GlobalProtect app was trying to use the old portal's authorization cookie to login instead of the newly migrated portal. This happened when the user changed from secondary portal to primary portal or vice versa without signing out.
GPC-19505	Fixed an issue where the GlobalProtect embedded browser for SAML authentication window obscured the two-factor authentication prompt hindering the users from entering their PIN.
GPC-19492	Fixed an issue where the GlobalProtect app displayed the text incorrectly on the web interface.
GPC-19475	Fixed an issue where users got connection errors in an embedded browser after the computer woke up from sleep or when the user switched gateways.
GPC-19449	Fixed an issue where, when the user used CAS token to authenticate, the system logs incorrectly displayed an error message during the GlobalProtect auto refresh configuration interval.
GPC-19433	Fixed an issue where a small white blank page randomly popped up on the device screen distracting the users. This issue occurred while the device was connected to GlobalProtect app.
GPC-19416	Fixed a GlobalProtect redirection issue in embedded browser. When a user tried to connect to GlobalProtect, an error was displayed while waiting for the SAML response instead of being redirected to the embedded browser.
GPC-19403	Fixed an issue where the GlobalProtect HIP check failed to detect Kaspersky after an upgrade from 21.3.10.391 to 21.15.8.493.

Issue ID	Description
GPC-19391	Fixed an issue where GlobalProtect stayed disconnected even when the device was unlocked by the user.
GPC-19387	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS, the app displayed text incorrectly when the system language was German.
GPC-19314	Fixed an issue where, when the GlobalProtect app is installed on devices running macOS, the app displayed the message, **Downloading in progress** when the GlobalProtect app was upgraded to 6.0.x using the option **Allow Transparently**. The app should not display the message when upgraded using the transparent method.
GPC-19262	Fixed an issue where GlobalProtect 6.2.1 tried to connect automatically after the user restarted their computer even though the connect method was set to **On-Demand**.
GPC-19237	Fixed an issue where the GlobalProtect app did not disconnect when the user used the **Disable** option on the hamburger menu. The tunnel was still up and connected even when the user disconnected the GlobalProtect app.
GPC-19138	Resolved an issue where the exclude for google application was not working for users.
GPC-19098	Resolved an issue where pre-logon setup was not working when GlobalProtect 6.2.1 was deployed via Microsoft Intune.
GPC-18992	Fixed an issue where internet via WiFi connection was unavailable for GlobalProtect users after their computer woke up from sleep because the app WiFi adapter was unable to obtain a DHCP IP address. This issue occurred on devices where Enforce GlobalProtect for Network Access feature was enabled.
GPC-18933	Fixed an issue where the GlobalProtect HIP check incorrectly detected Real Time Protection for Cortex XDR, which caused the device to fail the HIP check.

Issue ID	Description
GPC-18831	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS, the GlobalProtect app got stuck in the Connecting stage after the device woke up from Modern Standby mode.
GPC-18815	Fixed an issue where the Logon button on the GlobalProtect login screen stopped working after receiving the Microsoft Edge WebView2 runtime, 117.0.2045.36 update on the devices.
GPC-18778	Resolved an issue where devices supporting Modern Standby (Microsoft Learn) crashed when they entered sleep mode while the VPN plugin had an active connection and was sending data over its tunnel.
GPC-18750	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS, the GlobalProtect HIP check did not detect the Total Defense antivirus application, which caused the device to fail the HIP check.
GPC-18728	Fixed an issue where the **I Agree** option on the GlobalProtect app Welcome page did not work as expected when the user selected the option using a keyboard.
GPC-18702	Fixed an issue where, when the GlobalProtect app was installed on Windows devices, the **Allow Manually** upgrade failed when the user tried to upgrade the GlobalProtect app version from 6.0.5 to 6.0.7
GPC-18625	Resolved an issue where the Zoom app intermittently stopped connecting on macOS and displayed an error message.
GPC-18384	Fixed an issue where GlobalProtect app did not connect while Netskope was connected and vice-versa.
GPC-15750	Fixed an issue where a hyperlink in a HIP notification opened in the GPO-disabled Internet Explorer 11 browser instead of the default browser.

GlobalProtect App 6.1.5 Addressed Issues (iOS)

The following table lists the issues that are addressed in GlobalProtect app 6.1.5 for iOS.

Issue ID	Description
GPC-19631	Fixed an issue where when the GlobalProtect app is installed on iOS devices, the GlobalProtect app got disconnected and reconnected intermittently when the user was trying to upload files.

GlobalProtect App 6.1.5 Addressed Issues (Linux)

The following table lists the issues that are addressed in GlobalProtect app 6.1.5 for Linux.

Issue ID	Description
GPC-20193	Fixed an issue where Linux users are disconnected intermittently from GlobalProtect.
GPC-20124	Fixed an issue where GlobalProtect HIP was not working due to a failed OPSWAT library.
GPC-19792	Fixed an issue where an error message was displayed on the GlobalProtect client: "Previous authentication attempt timed out. Please select Connect to initiate authentication once again". Despite this error, the VPN tunnel was established, and traffic was routed successfully through the tunnel.
GPC-19748	Fixed an issue where the GlobalProtect app status was connected but no traffic was passing through. This issue occurred after the GlobalProtect Linux client was upgraded from 6.1.3 to 6.1.4 on Ubuntu Version 22.04.
GPC-19353	Fixed an issue where GlobalProtect was stuck in "Connecting" stage a with "Login Successful!" white page displayed on the default browser instead of the expected Microsoft SAML page.
GPC-19297	Fixed an issue where the Cortex XDR Last full-Scan-Time was not detected on GlobalProtect App for Linux.
GPC-18903	Fixed an issue where when the GlobalProtect app was installed on Linux devices running on Red Hat version 9, the ‘resolv.conf file’ was not getting updated with GlobalProtect DNS servers as expected.
GPC-17378	Fixed an issue where, when the GlobalProtect app was installed on devices running System76 coreboot BIOS, the HIP check failed when the Device ID was empty.

GlobalProtect App 6.1.4 Addressed Issues

The following table lists the issues that are addressed in GlobalProtect app 6.1.4 for Windows, macOS, iOS, Android, and Linux.

Issue ID	Description
GPC-19340	Fixed an issue where the GlobalProtect app failed to send HIP reports hourly.
GPC-19331	Fixed an issue where, when SAML authentication was used to authenticate to the GlobalProtect app, the app used an unknown username SAMLUser which was not configured instead of the actual username of the user, which caused an authentication failure.
GPC-19289	Fixed an issue where, when the GlobalProtect app was installed on Linux devices with Ubuntu 22.04, the app was unable to collect HIP reports.
GPC-19280	Fixed an issue where, when the GlobalProtect app transitions from pre-logon to user-logon tunnel, the app did not display the list of gateways for the users to change the gateway. The gateway list was displayed only when the app was refreshed.
GPC-19193	Fixed an issue where the GlobalProtect app was unable to fetch Windows firewall and antimalware information correctly.
GPC-19187	Fixed an issue where, when the GlobalProtect app version 6.0.8 or 6.0.7 was installed on endpoints running macOS Sonoma 14.1, the PanGPS did not work as expected.
GPC-19162	Fixed an issue where, when the user upgraded the GlobalProtect version to 5.2.13 or later version, the HIP report displayed the DLP Digital Guardian Agent as disabled.
GPC-19153	Fixed an issue where, when the GlobalProtect app was installed on iOS devices, the users had to reconnect to the GlobalProtect app several times in a day. Users were prompted to enter the credentials every time they tried to reconnect.

Issue ID	Description
GPC-19143	Fixed an issue where the users were unable to choose the correct certificate for the app as the configured registry value previousCertificate did not work as expected.
GPC-19104	Fixed an issue where the GlobalProtect HIP report failed to detect the Real Time Protection status for Cortex XDR, which caused the device to fail the HIP check.
GPC-19083	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS, the **Connection** tab under app **Settings** did not display the connection status and the refresh connection did not work when the **Settings** window was opened.
GPC-19061	Fixed an issue where GlobalProtect detected an incorrect Real-Time Protection status for Crowdstrike Falcon during HIP checks for antimalware.
GPC-19060	Fixed an issue where when the GlobalProtect app was installed on devices running macOS, the **Connection** tab under app **Settings** did not display the connection status when the app was changed from a non-tunneled gateway to a tunneled gateway.
GPC-19044	Fixed an issue where, when the GlobalProtect app was installed on Windows devices and the user changed the network from wired to wireless within the organization, the device displayed a blue screen.
GPC-19023	Fixed an issue where, when the GlobalProtect app version 5.2.13 was installed on devices running macOS, the users were unable to connect to the Zoom application.
GPC-19009	Fixed an issue where, when SAML authentication was used to authenticate to the GlobalProtect app and the user changed the gateway to a manual gateway, the app stayed in the Connecting stage.
GPC-18983	Fixed an issue where the Central Authentication Service (CAS) authentication did not work when

Issue ID	Description
	the GlobalProtect app was connected to an internal gateway and the app repeatedly opened the SAML authentication page.
GPC-18968	Fixed an issue where the GlobalProtect app displayed, **You are on the internal corporate network** message when users were on a public network. Users had to reboot the system to resolve this issue.
GPC-18903	Fixed an issue where, when the GlobalProtect app was installed on Linux devices running on Red Hat version 9, the resolv.conf file was not getting updated with GlobalProtect DNS servers as expected. Users should install/uninstall GlobalProtect app using p_install.shand gp_uninstall.shto fix resolve this issue.
GPC-18703	Fixed an issue where the GlobalProtect HIP check did not detect the Trellix Endpoint Security application, which caused the device to fail the HIP check.
GPC-18854	Fixed an issue where users were prompted twice to authenticate using SAML authentication when used with CAS authentication and authentication override cookie, the GlobalProtect app got stuck in the Connecting stage while trying to connect.
GPC-18828	Fixed an issue where split tunnel CNAME records were created before the GlobalProtect tunnel was established.
GPC-18525	Fixed an issue where, when the GlobalProtect app was installed on Linux devices running on Ubuntu 22.04, the app got disconnected intermittently with the error message: **Failed to read notify event buffer, error: Resource temporarily unavailable.**
GPC-16975	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS, the screen reader did not announce the name of the GlobalProtect gateway when the gateway was marked with the star symbol.

Issue ID	Description
GPC-16597	Fixed an issue where the GlobalProtect app stopped working when the app was upgraded from version 5.2.8 to 6.0.3.

GlobalProtect App 6.1.3 Addressed Issues

The following table lists the issues that are addressed in GlobalProtect app 6.1.3 for Windows, macOS, and Linux.

Issue ID	Description
GPC-19336	Fixed an issue where the ADEM portal did not display user information such as User-ID when the ADEM portal was changed from on-premises to Prisma Access.
GPC-18964	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS and the user upgraded the GlobalProtect version from 6.0.5 to 6.2.1, the app got disconnected after 10 minutes.
GPC-18913	Fixed an issue where the GlobalProtect app changed the connection status to **Not Connected** even though the app was connected to the internal gateway.
GPC-18907	Fixed an issue where the GlobalProtect app on macOS endpoints did not query the secondary DNS (when primary DNS is not responding) when the domain was part of the exclude domain list (both network and DNS).
GPC-18822	Fixed an issue where, when the GlobalProtect app was installed on Windows devices and the device was reset using the Microsoft Recovery tool, the GlobalProtect app was not properly displayed.
GPC-18788	Fixed an issue where the GlobalProtect HIP check did not detect McAfee Total Protection as an anti-malware application, which caused the device to fail the HIP check.
GPC-18733	Fixed an issue where the hyperlinks with the URLs containing the = character in the HIP notification message did not work as expected and the page did not open when the user clicked the URL.
GPC-18728	Fixed an issue where the **I Agree** option on the GlobalProtect app Welcome page did not work as

Issue ID	Description
	expected when the user selected the option using a keyboard.
GPC-18720	Fixed an issue where the GlobalProtect app became unresponsive when the user clicked the **ESC** button during authentication using a hard token.
GPC-18599	Fixed an issue where Linux endpoints could not resolve FQDNs when the GlobalProtect tunnel was connected because the host stopped listening to UDP/53 on the loopback IP address.
GPC-18598	Fixed an issue where the GlobalProtect SSO tile was selected instead of the Windows Password tile in the Windows Login screen even though the registry key **MakeGPCPDefault** was set to **No**.
GPC-18594	Fixed an issue where the GlobalProtect app was unable to send HIP reports when the app was connected using IPv6 address.
GPC-18566	Fixed an issue where the GlobalProtect app incorrectly displayed the gateway as internal when it was connected to an external gateway.
GPC-18528	Fixed an issue where the GlobalProtect HIP check incorrectly detected the version for KES 12 (Kaspersky Endpoint Security), which caused the device to fail the HIP check.
GPC-18512	Fixed an issue where, when the GlobalProtect app was installed on Linux devices running Ubuntu 22.04 or REHL 9.1, the app got disconnected periodically.
GPC-18471	Fixed an issue where, when multiple wa_3rd_party_host_64.exe processes persisted even after the HIP check was performed, the GlobalProtect app stopped working.
GPC-18426	Fixed an issue where, when the GlobalProtect app was configured with the '**Disable GlobalProtect** option set to **Allow With Ticket**, the app did not display the correct Disable Duration time.

Issue ID	Description
GPC-18383	Fixed an issue where the GlobalProtect app failed to connect on Windows 11 endpoints with error Could not connect to the GlobalProtect service.
GPC-18379	Fixed an issue where, when the IP address type was set to IPv4 and IPv6, the GlobalProtect app could connect only to the manual gateway instead of connecting to the best available gateway.
GPC-18367	Fixed an issue where, when pre-logon was configured for the GlobalProtect app, the GlobalProtect portal displayed the FQDN or IP address of the gateway and not the gateway name. With this fix, the portal displays the gateway name instead of FQDN or IP address.
GPC-18336	Fixed an issue where, when the GlobalProtect app got automatically connected after a system reboot even though the connection method configured was On-Demand.
GPC-18318	Fixed an issue where, when the GlobalProtect app was connected to the internal gateway, the app displayed the message : **Connected - Inter....** instead of **Connected**.
GPC-18251	Fixed an issue where the GlobalProtect HIP check did not detect McAfee LiveSafe as an anti-malware application, which caused the device to fail the HIP check.
GPC-18230	Fixed an issue where, when the user entered credentials during SAML authentication after the set internal login timer, the app displayed an authentication failed message without providing the reason. The **Retry** button on the app web interface did not work properly when using an embedded browser for authentication. The **Retry** button was not fully visible on the embedded browser.
GPC-18223	Fixed an issue where GlobalProtect experienced a prolonged connection time when IPv6 was disabled on Windows devices.
GPC-18200	Fixed an issue where the GlobalProtect HIP check did not detect McAfee LiveSafe as an antivirus

Issue ID	Description
	application, which caused the device to fail the HIP check.
GPC-18173	Fixed an issue where the vertical scroll bar on the GlobalProtect app web interface did not work properly when users tried to select the certificate from the drop-down.
GPC-18171	Fixed an issue where users were unable to select the external gateway manually when connected to the internal network. The GlobalProtect stayed in Connecting state and users had to manually disconnect the connection and connect to the internal network to exit the Connecting state.
GPC-18167	Fixed an issue where the GlobalProtect app displayed the Prisma Access gateways that were not set for manual selection.
GPC-18157	Fixed an issue where the GlobalProtect app displayed the Credential Provider language in English when the system language was German.
GPC-18155	Fixed an issue where, when the GlobalProtect app was installed on Linux devices, the app displayed the text in an incorrect format and the users were unable to read the information displayed on the app.
GPC-18146	Fixed an issue where, when the GlobalProtect app was installed on Windows devices, the GlobalProtect HIP check did not detect the correct details for Cortex XDR, which caused the device to fail the HIP check.
GPC-18135	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS, the GlobalProtect HIP check detected the WithSecure antivirus software as XProtect, which caused the device to fail the HIP check.
GPC-18107	Fixed an issue where the GlobalProtect HIP check did not detect McAfee LiveSafe – Internet Security, which caused the device to fail the HIP check.

Issue ID	Description
GPC-18092	Fixed an issue where GlobalProtect connected to an internal gateway got automatically disconnected after a certain period of time.
GPC-18060	Fixed an issue where the GlobalProtect HIP check did not detect McAfee Total Protection, which caused the device to fail the HIP check.
GPC-18039	Fixed an issue where the GlobalProtect HIP check did not detect the Definition Date correctly for the CrowdStrike application, which caused the device to fail the HIP check.
GPC-17914	Fixed an issue where, when the GlobalProtect app was installed on macOS endpoints and split tunnel was configured based on the application, the Zoom app got disconnected intermittently.
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-17640	Fixed an issue where, when the upgrade script update_tmp.bat was used, the error message did not display the correct exit timeout for the PanGPS uninstall process.
GPC-17518	Fixed an issue where the GlobalProtect app displayed the status as Connected-Internal even when the app was not connected.
GPC-17492	Fixed an issue where, when the traffic enforcer setting was applied for pre-logon and the GlobalProtect app was disconnected, the new user setting did not get updated and the pre-logon setting was still applicable.
GPC-17204	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS, the certificate information was not accessible even though the GlobalProtect app had full access to the certificate store.
GPC-17161	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS, the GlobalProtect app failed to reconnect and

Issue ID	Description
	continued to stay in the Connecting state after the device woke up from **Modern Standby** mode.
GPC-17001	Fixed an issue where, when the GlobalProtect app was installed on devices running on macOS, the app did not display the **Connect** button and **Refresh Connection** button properly.
GPC-16609	Fixed an issue where, when the GlobalProtect app was installed on Windows devices and the screen displayed GlobalProtect app connection status incorrectly when the device was locked.
GPC-16597	Fixed an issue where the GlobalProtect app stopped working when the app was upgraded from version 5.2.8 to 6.0.3.
GPC-16441	Fixed an issue where the GlobalProtect app connection failed when both GlobalProtect Enforcer and Endpoint Traffic Policy Enforcement were enabled.
GPC-16397	Fixed an issue where the GlobalProtect app was installed on devices running macOS, a blank GlobalProtect app user interface was displayed instead of the correct page.
GPC-15697	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS, users were able to select All Gateways heading on the page which was not an option for the users to select. This issue happened on the app interface with a non-English language.

GlobalProtect 6.1.0 Addressed Issues (iOS & Android)

The following table lists the issues that are addressed in GlobalProtect app 6.1.0 for iOS and Android.

Issue ID	Description
GPC-19030	Fixed an issue where GlobalProtect 6.1.0 on iOS 17 cannot connect gateways successfully.
GPC-18672	Fixed an issue where, when the customer upgraded from 5.2.12-26 to 6.1.1-6 on several devices, several devices received blue screen error messages. To fix the problem, the customer completely uninstalled the 5.x version of GlobalProtect before upgrading to 6.1.1.
GPC-18207	Fixed an issue where, when the GlobalProtect app was installed on Android devices and the block list was configured through mobile device management (MDM), the block list did not work as expected and the traffic was not blocked as per the configuration.
GPC-17875	Fixed an issue where,when the GlobalProtect app was installed on iOS devices, the app got stuck in the Connecting state and users had to restart the device to connect to the app.
GPC-17635	Fixed an issue where, when the GlobalProtect app was installed on iOS devices, users were unable to send logs (**Help** > **Send Logs**) through apps other than iOS Mail Client. Users can now share the logs using any file sharing app (e.g. Gmail) so that administrators can analyze the logs.
GPC-17435	Fixed an issue where, when the GlobalProtect app was installed on iOS devices and configured with On-Demand mode, the app displayed the following erroneous pop-up message: **GlobalProtect Always-On mode is enabled. Please sign in to continue.**
GPC-16741	Fixed an issue where, when the GlobalProtect app was installed on iOS devices, users could not connect the iOS device to a manual gateway even though the GlobalProtect portal was configured with two external manual gateways.

Issue ID	Description
GPC-15137	Fixed an issue where, when the GlobalProtect app was installed on Android devices, the users could not connect to the app due to the following error: ANDROID_ACTION_START_VNIC, ret=failed.

GlobalProtect App 6.1.2 Addressed Issues

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

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-17831	Fixed an issue where the GlobalProtect app reported the computer name differently from the computer name displayed in Autonomous DEM causing a data discrepancy.
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.

Issue ID	Description
GPC-17754	Fixed an issue where the GlobalProtect app did not detect Smart Card removal every time 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.

Issue ID	Description
GPC-17460	Fixed an issue where, when the GlobalProtect app was installed on Windows 10 or 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-17419	Fixed an issue where the GlobalProtect system tray icon continued to stay in Connecting state even when the app was connected and had access to internal resources.
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-17339	Fixed an issue where the device could not reconnect to the internet when endpoint traffic policy enforcement was enabled and when the

Issue ID	Description
	user switched networks. Users had to reboot the system to connect to the internet.
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-17326	Fixed an issue where, when the GlobalProtect app was installed on Windows devices, the device displayed a blue screen when users tried to download files larger than 5GB.
GPC-17299	Fixed an issue where the GlobalProtect app did not display LDAP password expiration notification on consecutive connection 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-17099	Fixed an issue where devices with Driver Verified enabled and configured to monitor the PAN virtual adapter driver (pangpd.sys) displayed the DRIVER_VERIFIER_DETECTED_VIOLATION Blue Screen error.
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.

Issue ID	Description
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 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

Issue ID	Description
	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-16346	Fixed an issue where, when the GlobalProtect app was installed on Windows devices, the GlobalProtect HIP check took longer than expected to collect the HIP information and also displayed HIP pop-up error messages for antivirus software, 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 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.

Issue ID	Description
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 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

Issue ID	Description
	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.
GPC-15991	Fixed an issue where the GlobalProtect app installer was displaying the wrong Palo Alto Networks logo.

Issue ID	Description
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.