paloalto TECHDOCS

GlobalProtect™ App Release Notes

Version 6.2

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2023-2026 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

October 2, 2026

Table of Contents

Changes to Default Behavior 7

Changes to Default Behavior in GlobalProtect App 6.2.8-h7 (6.2.8-c471) 8
Changes to Default Behavior in GlobalProtect App 6.2.8 (Windows) 9
Changes to Default Behavior in GlobalProtect App 6.2.6 10
Changes to Default Behavior in GlobalProtect App 6.2.5 11
Changes to Default Behavior in GlobalProtect App 6.2.4 12
Changes to Default Behavior in GlobalProtect App 6.2.2 13
Changes to Default Behavior in GlobalProtect App 6.2.1 14
Changes to Default Behavior in GlobalProtect App 6.2.0 15

Associated Software and Content Versions 17

GlobalProtect App 6.2 Known Issues 19

GlobalProtect App 6.2.8-h15 (6.2.8-c1084) Windows and macOS Known Issues 20
GlobalProtect App 6.2.8-h13 (6.2.8-c1045) Windows and macOS Known Issues 21
GlobalProtect App 6.2.8-h12 (6.2.8-c1032) Windows and macOS Known Issues 22
GlobalProtect App 6.2.8-h11 (6.2.8-c982) Windows and macOS Known Issues 23
GlobalProtect App 6.2.8-h10 (6.2.8-c948) Windows and macOS Known Issues 24
GlobalProtect App 6.2.8-h9 (6.2.8-c910) Windows and macOS Known Issues 25
GlobalProtect App 6.2.8-h7 (6.2.8-c471) Windows and macOS Known Issues 26
GlobalProtect App 6.2.8-h6 (6.2.8-431) Windows and macOS Known Issues 27
GlobalProtect App 6.2.8-h5 (6.2.8-c416) Windows and macOS Known Issues 29
GlobalProtect App 6.2.8-h4 (6.2.8-c317) Windows and macOS Known Issues 32
GlobalProtect App 6.2.9 Linux Known Issues 34
GlobalProtect App 6.2.8-h3 (6.2.8-c263) Windows and macOS Known Issues 35
GlobalProtect 6.2.8 Linux Known Issues 37
GlobalProtect App 6.2.8-h2 (6.2.8-c243) Windows and macOS Known Issues 38
GlobalProtect App 6.2.7 Linux Known Issues 40
GlobalProtect App 6.2.8-c223 Windows and macOS Known Issues 41
GlobalProtect App 6.2.8 Windows and macOS Known Issues 43
GlobalProtect App 6.2.7 Windows and macOS Known Issues 44
GlobalProtect App 6.2.6-c857 Windows and macOS Known Issues 46
GlobalProtect App 6.2.1-c31 Linux Addressed Issues 48
GlobalProtect App 6.2.6 Windows and macOS Known Issues 49
GlobalProtect App 6.2.5 Windows and macOS Known Issues 51

 ©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.4 Windows and macOS Known Issues..... 53
GlobalProtect App 6.2.3-c287 Windows and macOS Known Issues..... 55
GlobalProtect App 6.2.3 Windows and macOS Known Issues..... 57
GlobalProtect App 6.2.2 Windows and macOS Known Issues..... 59
GlobalProtect App 6.2.1 Linux Known Issues..... 62
GlobalProtect App 6.2.1 Windows and macOS Known Issues..... 65
GlobalProtect App 6.2.0 Linux Known Issues..... 68

Addressed Issues..... 71

GlobalProtect App 6.2.8-h15 (6.2.8-c1084) Windows and macOS Addressed Issues..... 72
GlobalProtect App 6.2.8-h13 (6.2.8-c1045) Windows and macOS Addressed Issues..... 77
GlobalProtect App 6.2.8-h12 (6.2.8-c1032) Windows and macOS Addressed Issues..... 78
GlobalProtect App 6.2.8-h11 (6.2.8-c982) Windows and macOS Addressed Issues..... 83
GlobalProtect App 6.2.8-h10 (6.2.8-c948) Windows and macOS Addressed Issues..... 85
GlobalProtect App 6.2.8-h9 (6.2.8-c910) Windows and macOS Addressed Issues..... 86
GlobalProtect App 6.2.8-h7 (6.2.8-c471) Windows and macOS Addressed Issues..... 89
GlobalProtect App 6.2.8-h6 (6.2.8-c431) Windows and macOS Addressed Issues..... 93
GlobalProtect 6.2.8-h5 (6.2.8-c416) Windows and macOS Addressed issues..... 94
GlobalProtect 6.2.8-h4 (6.2.8-c317) Windows and macOS Addressed issues..... 97
GlobalProtect App 6.2.9 Linux Addressed Issues..... 100
GlobalProtect App 6.2.8-h3 (6.2.8-c263) Windows and macOS Addressed Issues..... 101
GlobalProtect App 6.2.8 Linux Addressed Issues..... 103
GlobalProtect App 6.2.8-h2 (6.2.8-c243) Windows and macOS Addressed Issues..... 104
GlobalProtect App 6.2.7 Linux Addressed Issues..... 106
GlobalProtect App 6.2.8-c223 Windows and macOS Addressed Issues..... 107
GlobalProtect App 6.2.6 Linux Addressed Issues..... 110
GlobalProtect App 6.2.8 Windows and macOS Addressed Issues..... 113
GlobalProtect App 6.2.7 Addressed Issues..... 120
GlobalProtect App 6.2.6-c857 Windows and macOS Addressed Issues..... 121
GlobalProtect App 6.2.1-c31 Linux Addressed Issues..... 123
GlobalProtect App 6.2.6 Windows and macOS Addressed Issues..... 124
GlobalProtect App 6.2.5 Windows and macOS Addressed Issues..... 127
GlobalProtect App 6.2.4 Windows and macOS Addressed Issues..... 133

 ©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.3-c287 Addressed Issues..... 142
GlobalProtect App 6.2.3 Windows and macOS Addressed Issues..... 143
GlobalProtect App 6.2.2 Windows and macOS Addressed Issues..... 152
GlobalProtect App 6.2.1 Linux Addressed Issues..... 154
GlobalProtect App 6.2.1 Windows and macOS Addressed Issues..... 156
GlobalProtect App 6.2.0 Linux Addressed Issues..... 163

 ©2026 Palo Alto Networks, Inc.

©2026 Palo Alto Networks, Inc.

Changes to Default Behavior

The following topics describe changes to default behavior in GlobalProtect app 6.2:

Changes to Default Behavior in GlobalProtect App 6.2.8-h7 (6.2.8-c471)

- Clicking the GlobalProtect icon in the Finder or Applications folder on macOS clients now opens the GlobalProtect client, mirroring the taskbar behavior. This change provides a consistent user experience by ensuring the interface is immediately visible regardless of the launch method. Previously, launching the app via the Applications folder or Spotlight provided no visual feedback if the GlobalProtect app was already running in the background.
- macOS endpoints only When GlobalProtect cannot resolve an IPv6 address for the gateway, it no longer installs any IPv6 routes — including the ::/0 default route — even when the gateway pushes IPv6 access routes, making IPv6 destinations unreachable through the tunnel. This occurs when the endpoint has no usable global IPv6 address (macOS returns no AAAA records to the app in this state), when the gateway FQDN has no AAAA record, or when the gateway is configured by IPv4 address.

  To restore IPv6 route installation, set `split-tunnel-keep-tunnel-ipv6` to `yes` under GlobalProtect > Settings in the plist at `/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`, then restart the endpoint.

©2026 Palo Alto Networks, Inc.

Changes to Default Behavior in GlobalProtect App 6.2.8 (Windows)

(Windows endpoints only; Requires GlobalProtect release 6.2.8-c223 or later or 6.3.3 or later and content version 8966-9398) GlobalProtect now uses an embedded browser for captive portal authentication instead of the system default browser. This change provides improved security and a better user experience:

- **Improved Security**: When captive portal is detected, the Enforce GlobalProtect Connection for Network Access setting no longer needs to be disabled. Embedded browser captive portal traffic is implicitly allowed because the embedded browser runs as a GlobalProtect process. Only GlobalProtect embedded browser traffic is permitted during captive portal authentication, resulting in improved security.
- **Optimized Configuration**: You do not need to define Enforce GlobalProtect Connection for Network Access exceptions (IP-based or FQDN-based) for embedded browser captive portal traffic or associated pages. This preserves the limited number of available exception entries.
- **Better User Experience**: The embedded browser launches as a foreground window, immediately prompting users for authentication. When Captive Portal Exception Timeout (sec) is set to 0 (recommended), there is no risk of timeout expiry because embedded browser traffic is implicitly allowed. If the timeout is set to a value greater than 0 and expires while the embedded browser is open, the embedded browser displays a **Refresh GlobalProtect** option to reset the timeout and restart captive portal detection.

To use the GlobalProtect embedded browser for captive portal authentication, set **Use Default Browser for Captive Portal** to **No**, set **Display Captive Portal Detection Message** to **Yes**, and set **Captive Portal Exception Timeout (sec)** to **0** in the GlobalProtect portal agent configuration. For more information, see Customize the GlobalProtect App.

 ©2026 Palo Alto Networks, Inc.

Changes to Default Behavior in GlobalProtect App 6.2.6

You can now use the new system extension type **Non-removable system extensions from UI** introduced by Jamf Pro for the devices running on macOS 15 Sequoia or later versions to prevent the end users from disabling the GlobalProtect system extensions on the endpoints. GlobalProtect app version 6.2.6 and later supports macOS 15 Sequoia. This functionality is available only for the devices running on macOS 15 Sequoia or later versions.

You can configure this feature to prevent the end users from disabling GlobalProtect system extensions on their endpoints thereby reducing the risks associated with disabled system extensions.

Previously, end users could disable the GlobalProtect system extension through the MDM settings (**General** > **Settings** > **Network Extensions**.) However, with this new feature, the **Non-removable system extensions from UI** system extension type in Jamf Pro restricts users from disabling the GlobalProtect system extension.

To enable this functionality, you must perform the following procedures:

1. Upgrade the GlobalProtect app to version 6.2.6 or later
2. Upgrade the macOS to version 15 Sequoia or later
3. In the mobile device management (MDM), Jamf Pro, set the **System Extension Type** as **Non-removable system extensions from UI** while configuring **Configuration Profile.**

If the GlobalProtect system extensions are disabled by the end-user, the following GlobalProtect features do not work:

- Split-tunnel by domain
- Split-tunnel by app
- Enforcer
- Split-DNS
- Traffic Enforcement

 ©2026 Palo Alto Networks, Inc.

Changes to Default Behavior in GlobalProtect App 6.2.5

The following topics describe changes to default behavior in GlobalProtect app 6.2.5:

- Starting with GlobalProtect 6.2.5, if the saml-browser-order pre-deployment key is not set or set to yes, the user will not be able to bring other windows in front of the saml embedded browser. If the saml-browser-order pre-deployment key is set to no, the user will be able to bring other windows in front of the saml embedded browser.
- When a captive portal is detected on Windows computers, GlobalProtect launches the system default browser (Chrome, Safari, or Firefox).

 ©2026 Palo Alto Networks, Inc.

Changes to Default Behavior in GlobalProtect App 6.2.4

There are no changes to default behavior in GlobalProtect app 6.2.4.

 ©2026 Palo Alto Networks, Inc.

Changes to Default Behavior in GlobalProtect App 6.2.2

If your Prisma Access tenant is IP Optimization enabled (available starting in Prisma Access 5.0.1), the minimum required GlobalProtect app versions are 6.1.4 and later, 6.2.3 and later, or 6.3 and later.

©2026 Palo Alto Networks, Inc.

Changes to Default Behavior in GlobalProtect App 6.2.1

- If your Prisma Access tenant is IP Optimization enabled (available starting in Prisma Access 5.0.1), the minimum required GlobalProtect app versions are 6.1.4 and later, 6.2.3 and later, or 6.3 and later.
- Starting from GlobalProtect Linux version 6.2.1, you must use the following commands to install the CLI or GUI versions of the app.
  - To install the GlobalProtect UI package- **`$ ./gp_install.sh`**
  - To install the GlobalProtect CLI package- **`$ ./gp_install.sh --cli-only`**

  You don't need to run the **`./gp_install.sh`** with **`sudo`** for GlobalProtect app Linux 6.2.1 and later versions. As the script executes, users will be prompted to enter the **`sudo`** password.

 ©2026 Palo Alto Networks, Inc.

Changes to Default Behavior in GlobalProtect App 6.2.0

If you are using PAN-OS 10.x.x or 11.0.x and the **Use Default Browser for SAML Authentication** option is selected in any of the portal agent configurations, the **Use Default Browser** option on the Client Authentication window will be automatically enabled after you upgrade to PAN-OS 11.1.0 or later. Starting from PAN-OS 11.1.0, the default browser behavior is controlled by the client authentication setting. For more information about this feature and upgrade considerations, see Manage Browser Selection for SAML Authentication.

 ©2026 Palo Alto Networks, Inc.

 ©2026 Palo Alto Networks, Inc.

Associated Software and Content Versions

The following minimum Palo Alto Networks software versions are supported with GlobalProtect app 6. 2. 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	Runs on all currently supported PAN-OS versions 11.0 for Extend User Session for GlobalProtect Users.
Prisma Access version	Prisma Access 4.0 for Explicit Proxy Connectivity in GlobalProtect for Always-on Internet Security
XDR Agent version	• 7.9 for GlobalProtect app version 6.2.0 • 8.2 for GlobalProtect app version 6.2.1 • 8.1 and 8.2 for GlobalProtect app version 6.2.2 • 8.3 and 8.4 for GlobalProtect app version 6.2.3

 ©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2 Known Issues

To view the known issues in a release, select the appropriate version from the left navigation bar.

GlobalProtect App 6.2.8-h15 (6.2.8-c1084) Windows and macOS Known Issues

The following table lists the known issues in GlobalProtect app 6.2.8-h15 (6.2.8-c1084) Windows and macOS.

Issue ID	Description
GPC-27907	(Windows only) Connect Before Logon (CBL) does not connect when the GlobalProtect portal uses full-chain certificate verification and the portal and gateways are hosted on Prisma Access. When full-chain-cert-verify is enabled, all gateway connection attempts fail with the error "The network connection is unreachable or the gateway is unresponsive. Check the network connection and reconnect." When full-chain-cert-verify is disabled, a server certificate error prompt appears for the portal on each CBL attempt; after accepting the prompt, users must enter credentials a second time. Workaround: Disable full-chain-cert-verify on the GlobalProtect portal. Note that users will encounter a server certificate error prompt on each CBL attempt and must enter their credentials twice to complete the connection.
GPC-27828	(macOS only) GlobalProtect fails to connect when both the portal and gateway require OTP challenge authentication. After completing the portal OTP challenge, the gateway returns an HTML challenge response instead of the expected XML response, causing the connection to fail with the error "The network connection is unreachable or the gateway is unresponsive. Check the network connection and reconnect."

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.8-h13 (6.2.8-c1045) Windows and macOS Known Issues

The following table lists the known issues in the GlobalProtect app for 6.2.8-h13 (6.2.8-c1045) Windows and Mac devices.

Issue ID	Description
GPC-25294	The reported severity level for the same patch, such as KB5072033, varies depending on the patch management tool used (e.g., Tanium, ManageEngine SCCM, or Windows Update). This inconsistency in severity categorization can result in users losing internet access.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.8-h12 (6.2.8-c1032) Windows and macOS Known Issues

The following table lists known issues in the GlobalProtect app for Windows and Mac devices.

Issue ID	Description
GPC-25294	The reported severity level for the same patch, such as KB5072033, varies depending on the patch management tool used (e.g., Tanium, ManageEngine SCCM, or Windows Update). This inconsistency in severity categorization can result in users losing internet access.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.8-h11 (6.2.8-c982) Windows and macOS Known Issues

The GlobalProtect app 6.2.8-h11 (6.2.8-c) Windows and macOS release includes performance and bug fixes.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.8-h10 (6.2.8-c948) Windows and macOS Known Issues

The GlobalProtect app 6.2.8-h10 (6.2.8-c948) release includes performance and bug fixes.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.8-h9 (6.2.8-c910) Windows and macOS Known Issues

There are no known issues in GlobalProtect app 6.2.8-h9 (6.2.8-c910) Windows and macOS.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.8-h7 (6.2.8-c471) Windows and macOS Known Issues

There are no known issues in the GlobalProtect App 6.2.8-h7 (6.2.8-c471) Windows and macOS release.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.8-h6 (6.2.8-431) Windows and macOS Known Issues

The following table lists the known issues in GlobalProtect app 6.2.8-h6 (6.2.8-431) Windows and macOS.

Issue	Description
GPC-24931	When GlobalProtect app has Enforcer and endpoint traffic policy enforcement enabled, it may fail to connect after a Wi-Fi switch, manual gateway change, or machine reboot. The error message "Could not connect to the authentication server," is displayed even when the device has an active internet connection. Disconnecting the GlobalProtect connection allows browsing, but attempting to reconnect immediately redirects to embedded browser Security Assertion Markup Language (SAML) authentication, which then displays the "Can't reach auth server" error.
GPC-24922	After waking up from modern standby, the GlobalProtect app may get stuck at finding the best available gateway. Disconnecting and reconnecting does not resolve the issue, even though the portal FQDN is reachable.
GPC-24842	(macOS only) GlobalProtect crashes when you click **Change Portal** on setups that include two or more portal entries and have a preferred gateway marked. This issue can corrupt the NSUserDefaults plist file leading to subsequent crashes. **Workaround**: Do one of the following: • Reinstall GlobalProtect. • Remove the corrupted plist file located at `~/Library/Preferences/com.paloaltonetworks.GlobalProtect.client`

©2026 Palo Alto Networks, Inc.

Issue	Description
	• Remove portal entries only from the plist file using the following steps: 1. `$ launchctl unload -S Aqua / Library/LaunchAgents/ com.paloaltonetworks.gp.pangpa.plist` 2. `$ defaults delete com.paloaltonetworks.GlobalProtect.clie PanPortalList` 3. `killall cfprefsd` 4. `launchctl load -S Aqua / Library/LaunchAgents/ com.paloaltonetworks.gp.pangpa.plist`

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.8-h5 (6.2.8-c416) Windows and macOS Known Issues

The following table lists the known issues in GlobalProtect app 6.2.8-h5 (6.2.8-c416) Windows and macOS.

Issue	Description
GPC-24842	(macOS only) GlobalProtect crashes when you click **Change Portal** on setups that include two or more portal entries and have a preferred gateway marked. This issue can corrupt the NSUserDefaults plist file leading to subsequent crashes. **Workaround**: Do one of the following: • Reinstall GlobalProtect. • Remove the corrupted plist file located at `~/Library/Preferences/com.paloaltonetworks.GlobalProtect.client` • Remove portal entries only from the plist file using the following steps: 1. `$ launchctl unload -S Aqua /Library/LaunchAgents/com.paloaltonetworks.gp.pangpa.plist` 2. `$ defaults delete com.paloaltonetworks.GlobalProtect.clie PanPortalList` 3. `killall cfprefsd` 4. `launchctl load -S Aqua /Library/LaunchAgents/com.paloaltonetworks.gp.pangpa.plist`
GPC-23149	Connection via captive portal does not work in agent proxy mode when the captive portal is hosted on a non-local network.
GPC-21694	When the GlobalProtect app is installed on Windows, a Microsoft Defender SmartScreen warning is displayed:. **Workaround:**Click More Info and then click Run to proceed with the installation.

©2026 Palo Alto Networks, Inc.

Issue	Description
GPC-21558	When the GlobalProtect app is installed on devices running on macOS and the end user enable or disable the system extensions, the GlobalProtect Enforcer feature is not working as expected.
GPC-20840	Loading content or text on the SAML embedded browser can take longer than usual. This does not impact authentication.
GPC-17820	Firefox is not supported for proxied traffic in Tunnel and Proxy mode or proxy mode.
GPC-17727	When the GlobalProtect app is connected in Tunnel and Proxy mode or proxy mode, SSH traffic cannot be sent over the proxy.
GPC-17513	When GlobalProtect is configured in Tunnel and Proxy mode or proxy mode, if the admin-defined PAC file has an HTTP URL, the GlobalProtect app will not download the PAC content.
GPC-17447	When the GlobalProtect app is configured in Tunnel and Proxy mode, SSL VPN establishment over the proxy doesn't work.
GPC-17663	In Tunnel and Proxy mode, the GlobalProtect agent tunnel does not work seamlessly when the GlobalProtect app and the third-party VPN are configured to use overlapping IP subnets. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17555	In Tunnel and Proxy mode, the GlobalProtect agent tunnel on macOS does not coexist well with Cisco Anyconnect VPN due to an IP forwarding table issue. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17854	The GlobalProtect app does not prompt the users to extend the login lifetime user

©2026 Palo Alto Networks, Inc.

Issue	Description
	session when the device woke up from sleep or hibernation mode.

 ©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.8-h4 (6.2.8-c317) Windows and macOS Known Issues

The following table lists the known issues in GlobalProtect app 6.2.8-h4 (6.2.8-c317) Windows and macOS.

Issue	Description
GPC-24330	Fixed an issue where GlobalProtect app got stuck in a connecting state when using GlobalProtect version 6.2.8-h4. The issue was seen when saml-logout and enforcer was enabled.
GPC-23149	Connection via captive portal does not work in agent proxy mode when the captive portal is hosted on a non-local network.
GPC-21694	When the GlobalProtect app is installed on Windows, a Microsoft Defender SmartScreen warning is displayed:. **Workaround:**Click More Info and then click Run to proceed with the installation.
GPC-21558	When the GlobalProtect app is installed on devices running on macOS and the end user enable or disable the system extensions, the GlobalProtect Enforcer feature is not working as expected.
GPC-20840	Loading content or text on the SAML embedded browser can take longer than usual. This does not impact authentication.
GPC-17820	Firefox is not supported for proxied traffic in Tunnel and Proxy mode or proxy mode.
GPC-17727	When the GlobalProtect app is connected in Tunnel and Proxy mode or proxy mode, SSH traffic cannot be sent over the proxy.
GPC-17513	When GlobalProtect is configured in Tunnel and Proxy mode or proxy mode, if the admin-defined PAC file has an HTTP URL, the GlobalProtect app will not download the PAC content.

©2026 Palo Alto Networks, Inc.

Issue	Description
GPC-17447	When the GlobalProtect app is configured in Tunnel and Proxy mode, SSL VPN establishment over the proxy doesn't work.
GPC-17663	In Tunnel and Proxy mode, the GlobalProtect agent tunnel does not work seamlessly when the GlobalProtect app and the third-party VPN are configured to use overlapping IP subnets. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17555	In Tunnel and Proxy mode, the GlobalProtect agent tunnel on macOS does not coexist well with Cisco Anyconnect VPN due to an IP forwarding table issue. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17854	The GlobalProtect app does not prompt the users to extend the login lifetime user session when the device woke up from sleep or hibernation mode.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.9 Linux Known Issues

Issue	Description
GPC-19339	When the GlobalProtect app is upgraded from version 6.1.4-c1 to 6.2.0-c4 on Linux devices, the GlobalProtect web interface displays the upgraded version only after a system reboot.
GPC-19180	When the GlobalProtect app is installed on Linux devices and the app is upgraded or downgraded, the GlobalProtect web interface and the command-line interface display the new version only after a system reboot.
GPC-17854	The GlobalProtect app does not prompt the users to extend the login lifetime user session when the device woke up from sleep or hibernation mode.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.8-h3 (6.2.8-c263) Windows and macOS Known Issues

The following table lists the known issues in GlobalProtect app 6.2.8-h3 (6.2.8-c263).

Issue	Description
GPC-23149	Connection via captive portal does not work in agent proxy mode when the captive portal is hosted on a non-local network.
GPC-21694	When the GlobalProtect app is installed on Windows, a Microsoft Defender SmartScreen warning is displayed:. **Workaround:**Click More Info and then click Run to proceed with the installation.
GPC-21558	When the GlobalProtect app is installed on devices running on macOS and the end user enable or disable the system extensions, the GlobalProtect Enforcer feature is not working as expected.
GPC-20840	Loading content or text on the SAML embedded browser can take longer than usual. This does not impact authentication.
GPC-17820	Firefox is not supported for proxied traffic in Tunnel and Proxy mode or proxy mode.
GPC-17727	When the GlobalProtect app is connected in Tunnel and Proxy mode or proxy mode, SSH traffic cannot be sent over the proxy.
GPC-17513	When GlobalProtect is configured in Tunnel and Proxy mode or proxy mode, if the admin-defined PAC file has an HTTP URL, the GlobalProtect app will not download the PAC content.
GPC-17447	When the GlobalProtect app is configured in Tunnel and Proxy mode, SSL VPN establishment over the proxy doesn't work.
GPC-17663	In Tunnel and Proxy mode, the GlobalProtect agent tunnel does not work seamlessly when the GlobalProtect app and the third-party

©2026 Palo Alto Networks, Inc.

Issue	Description
	VPN are configured to use overlapping IP subnets. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17555	In Tunnel and Proxy mode, the GlobalProtect agent tunnel on macOS does not coexist well with Cisco Anyconnect VPN due to an IP forwarding table issue. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17854	The GlobalProtect app does not prompt the users to extend the login lifetime user session when the device woke up from sleep or hibernation mode.

©2026 Palo Alto Networks, Inc.

GlobalProtect 6.2.8 Linux Known Issues

The following table lists the known issues in GlobalProtect 6.2.8 Linux.

Issue	Description
GPC-19339	When the GlobalProtect app is upgraded from version 6.1.4-c1 to 6.2.0-c4 on Linux devices, the GlobalProtect web interface displays the upgraded version only after a system reboot.
GPC-19180	When the GlobalProtect app is installed on Linux devices and the app is upgraded or downgraded, the GlobalProtect web interface and the command-line interface display the new version only after a system reboot.
GPC-17854	The GlobalProtect app does not prompt the users to extend the login lifetime user session when the device woke up from sleep or hibernation mode.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.8-h2 (6.2.8-c243) Windows and macOS Known Issues

The following table lists the known issues in GlobalProtect app 6.2.8-h2 (6.2.8-c243).

Issue	Description
GPC-23149	Connection via captive portal does not work in agent proxy mode when the captive portal is hosted on a non-local network.
GPC-21694	When the GlobalProtect app is installed on Windows, a Microsoft Defender SmartScreen warning is displayed:. **Workaround:**Click More Info and then click Run to proceed with the installation.
GPC-21558	When the GlobalProtect app is installed on devices running on macOS and the end user enable or disable the system extensions, the GlobalProtect Enforcer feature is not working as expected.
GPC-20840	Loading content or text on the SAML embedded browser can take longer than usual. This does not impact authentication.
GPC-19339	When the GlobalProtect app is upgraded from version 6.1.4-c1 to 6.2.0-c4 on Linux devices, the GlobalProtect web interface displays the upgraded version only after a system reboot.
GPC-19180	When the GlobalProtect app is installed on Linux devices and the app is upgraded or downgraded, the GlobalProtect web interface and the command-line interface display the new version only after a system reboot.
GPC-17820	Firefox is not supported for proxied traffic in Tunnel and Proxy mode or proxy mode.
GPC-17727	When the GlobalProtect app is connected in Tunnel and Proxy mode or proxy mode, SSH traffic cannot be sent over the proxy.

©2026 Palo Alto Networks, Inc.

Issue	Description
GPC-17513	When GlobalProtect is configured in Tunnel and Proxy mode or proxy mode, if the admin-defined PAC file has an HTTP URL, the GlobalProtect app will not download the PAC content.
GPC-17447	When the GlobalProtect app is configured in Tunnel and Proxy mode, SSL VPN establishment over the proxy doesn't work.
GPC-17663	In Tunnel and Proxy mode, the GlobalProtect agent tunnel does not work seamlessly when the GlobalProtect app and the third-party VPN are configured to use overlapping IP subnets. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17555	In Tunnel and Proxy mode, the GlobalProtect agent tunnel on macOS does not coexist well with Cisco Anyconnect VPN due to an IP forwarding table issue. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17854	The GlobalProtect app does not prompt the users to extend the login lifetime user session when the device woke up from sleep or hibernation mode.

 ©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.7 Linux Known Issues

The following table lists the known issues in GlobalProtect app 6.2.9 Linux.

Issue	Description
GPC-19339	When the GlobalProtect app is upgraded from version 6.1.4-c1 to 6.2.0-c4 on Linux devices, the GlobalProtect web interface displays the upgraded version only after a system reboot.
GPC-19180	When the GlobalProtect app is installed on Linux devices and the app is upgraded or downgraded, the GlobalProtect web interface and the command-line interface display the new version only after a system reboot.
GPC-17854	The GlobalProtect app does not prompt the users to extend the login lifetime user session when the device woke up from sleep or hibernation mode.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.8-c223 Windows and macOS Known Issues

The following table lists the known issues in GlobalProtect app 6.2.8-c223.

Issue	Description
GPC-23149	Connection via captive portal does not work in agent proxy mode when the captive portal is hosted on a non-local network.
GPC-21694	When the GlobalProtect app is installed on Windows, a Microsoft Defender SmartScreen warning is displayed:. **Workaround:**Click More Info and then click Run to proceed with the installation.
GPC-21558	When the GlobalProtect app is installed on devices running on macOS and the end user enable or disable the system extensions, the GlobalProtect Enforcer feature is not working as expected.
GPC-20840	Loading content or text on the SAML embedded browser can take longer than usual. This does not impact authentication.
GPC-19339	When the GlobalProtect app is upgraded from version 6.1.4-c1 to 6.2.0-c4 on Linux devices, the GlobalProtect web interface displays the upgraded version only after a system reboot.
GPC-19180	When the GlobalProtect app is installed on Linux devices and the app is upgraded or downgraded, the GlobalProtect web interface and the command-line interface display the new version only after a system reboot.
GPC-17820	Firefox is not supported for proxied traffic in Tunnel and Proxy mode or proxy mode.
GPC-17727	When the GlobalProtect app is connected in Tunnel and Proxy mode or proxy mode, SSH traffic cannot be sent over the proxy.

©2026 Palo Alto Networks, Inc.

Issue	Description
GPC-17513	When GlobalProtect is configured in Tunnel and Proxy mode or proxy mode, if the admin-defined PAC file has an HTTP URL, the GlobalProtect app will not download the PAC content.
GPC-17447	When the GlobalProtect app is configured in Tunnel and Proxy mode, SSL VPN establishment over the proxy doesn't work.
GPC-17663	In Tunnel and Proxy mode, the GlobalProtect agent tunnel does not work seamlessly when the GlobalProtect app and the third-party VPN are configured to use overlapping IP subnets. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17555	In Tunnel and Proxy mode, the GlobalProtect agent tunnel on macOS does not coexist well with Cisco Anyconnect VPN due to an IP forwarding table issue. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17854	The GlobalProtect app does not prompt the users to extend the login lifetime user session when the device woke up from sleep or hibernation mode.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.8 Windows and macOS Known Issues

The following table lists the known issues in GlobalProtect app 6.2.8 Windows and macOS.

Issue ID	Description
GPC-22028	Fixed an issue where the disconnect reason for macOS users was getting cached.
GPC-21775	Fixed an issue where GlobalProtect users on macOS were disconnected immediately after sending the HIP report.
GPC-21743	Fixed an issue where a user was randomly prompted with a \"Login Successful\" message when connecting to GlobalProtect (GP), even though GP was not connected.
GPC-21639	Fixed an issue where the GlobalProtect macOS client did not extend the session even though the user clicked the Extend Session button.
GPC-21467	Fixed an issue where the Transparent Upgrade with Proxy only mode did not work as expected and no tunnel was established with the gateway.
GPC-21453	Fixed an issue where the GlobalProtect app window displayed "static" instead of the connected gateway name.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.7 Windows and macOS Known Issues

The following table lists the known issues in GlobalProtect app 6.2.7 Windows and macOS .

Issue	Description
GPC-23149	Connection via captive portal does not work in agent proxy mode when the captive portal is hosted on a non-local network.
GPC-21694	When the GlobalProtect app is installed on Windows, a Microsoft Defender SmartScreen warning is displayed:. **Workaround:**Click More Info and then click Run to proceed with the installation.
GPC-21558	When the GlobalProtect app is installed on devices running on macOS and the end user enable or disable the system extensions, the GlobalProtect Enforcer feature is not working as expected.
GPC-20840	Loading content or text on the SAML embedded browser can take longer than usual. This does not impact authentication.
GPC-19339	When the GlobalProtect app is upgraded from version 6.1.4-c1 to 6.2.0-c4 on Linux devices, the GlobalProtect web interface displays the upgraded version only after a system reboot.
GPC-19180	When the GlobalProtect app is installed on Linux devices and the app is upgraded or downgraded, the GlobalProtect web interface and the command-line interface display the new version only after a system reboot.
GPC-17820	Firefox is not supported for proxied traffic in Tunnel and Proxy mode or proxy mode.
GPC-17727	When the GlobalProtect app is connected in Tunnel and Proxy mode or proxy mode, SSH traffic cannot be sent over the proxy.

©2026 Palo Alto Networks, Inc.

Issue	Description
GPC-17513	When GlobalProtect is configured in Tunnel and Proxy mode or proxy mode, if the admin-defined PAC file has an HTTP URL, the GlobalProtect app will not download the PAC content.
GPC-17447	When the GlobalProtect app is configured in Tunnel and Proxy mode, SSL VPN establishment over the proxy doesn't work.
GPC-17663	In Tunnel and Proxy mode, the GlobalProtect agent tunnel does not work seamlessly when the GlobalProtect app and the third-party VPN are configured to use overlapping IP subnets. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17555	In Tunnel and Proxy mode, the GlobalProtect agent tunnel on macOS does not coexist well with Cisco Anyconnect VPN due to an IP forwarding table issue. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17854	The GlobalProtect app does not prompt the users to extend the login lifetime user session when the device woke up from sleep or hibernation mode.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.6-c857 Windows and macOS Known Issues

The following table lists the known issues in GlobalProtect app 6.2.6-c857 Windows and macOS .

Issue	Description
GPC-23149	Connection via captive portal does not work in agent proxy mode when the captive portal is hosted on a non-local network.
GPC-21694	When the GlobalProtect app is installed on Windows, a Microsoft Defender SmartScreen warning is displayed:. **Workaround:**Click More Info and then click Run to proceed with the installation.
GPC-21558	When the GlobalProtect app is installed on devices running on macOS and the end user enable or disable the system extensions, the GlobalProtect Enforcer feature is not working as expected.
GPC-20840	Loading content or text on the SAML embedded browser can take longer than usual. This does not impact authentication.
GPC-19339	When the GlobalProtect app is upgraded from version 6.1.4-c1 to 6.2.0-c4 on Linux devices, the GlobalProtect web interface displays the upgraded version only after a system reboot.
GPC-19180	When the GlobalProtect app is installed on Linux devices and the app is upgraded or downgraded, the GlobalProtect web interface and the command-line interface display the new version only after a system reboot.
GPC-17820	Firefox is not supported for proxied traffic in Tunnel and Proxy mode or proxy mode.
GPC-17727	When the GlobalProtect app is connected in Tunnel and Proxy mode or proxy mode, SSH traffic cannot be sent over the proxy.

©2026 Palo Alto Networks, Inc.

Issue	Description
GPC-17513	When GlobalProtect is configured in Tunnel and Proxy mode or proxy mode, if the admin-defined PAC file has an HTTP URL, the GlobalProtect app will not download the PAC content.
GPC-17447	When the GlobalProtect app is configured in Tunnel and Proxy mode, SSL VPN establishment over the proxy doesn't work.
GPC-17663	In Tunnel and Proxy mode, the GlobalProtect agent tunnel does not work seamlessly when the GlobalProtect app and the third-party VPN are configured to use overlapping IP subnets. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17555	In Tunnel and Proxy mode, the GlobalProtect agent tunnel on macOS does not coexist well with Cisco Anyconnect VPN due to an IP forwarding table issue. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17854	The GlobalProtect app does not prompt the users to extend the login lifetime user session when the device woke up from sleep or hibernation mode.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.1-c31 Linux Addressed Issues

Where Can I Use This?	What Do I Need?
•	❑

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.6 Windows and macOS Known Issues

The following table lists the known issues in GlobalProtect app 6.2.6 Windows and macOS .

Issue	Description
GPC-23149	Connection via captive portal does not work in agent proxy mode when the captive portal is hosted on a non-local network.
GPC-21694	When the GlobalProtect app is installed on Windows, a Microsoft Defender SmartScreen warning is displayed:. **Workaround:**Click More Info and then click Run to proceed with the installation.
GPC-21558	When the GlobalProtect app is installed on devices running on macOS and the end user enable or disable the system extensions, the GlobalProtect Enforcer feature is not working as expected.
GPC-20840	Loading content or text on the SAML embedded browser can take longer than usual. This does not impact authentication.
GPC-19339	When the GlobalProtect app is upgraded from version 6.1.4-c1 to 6.2.0-c4 on Linux devices, the GlobalProtect web interface displays the upgraded version only after a system reboot.
GPC-19180	When the GlobalProtect app is installed on Linux devices and the app is upgraded or downgraded, the GlobalProtect web interface and the command-line interface display the new version only after a system reboot.
GPC-17820	Firefox is not supported for proxied traffic in Tunnel and Proxy mode or proxy mode.
GPC-17727	When the GlobalProtect app is connected in Tunnel and Proxy mode or proxy mode, SSH traffic cannot be sent over the proxy.

©2026 Palo Alto Networks, Inc.

Issue	Description
GPC-17513	When GlobalProtect is configured in Tunnel and Proxy mode or proxy mode, if the admin-defined PAC file has an HTTP URL, the GlobalProtect app will not download the PAC content.
GPC-17447	When the GlobalProtect app is configured in Tunnel and Proxy mode, SSL VPN establishment over the proxy doesn't work.
GPC-17663	In Tunnel and Proxy mode, the GlobalProtect agent tunnel does not work seamlessly when the GlobalProtect app and the third-party VPN are configured to use overlapping IP subnets. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17555	In Tunnel and Proxy mode, the GlobalProtect agent tunnel on macOS does not coexist well with Cisco Anyconnect VPN due to an IP forwarding table issue. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17854	The GlobalProtect app does not prompt the users to extend the login lifetime user session when the device woke up from sleep or hibernation mode.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.5 Windows and macOS Known Issues

The following table lists the known issues in GlobalProtect app 6.2.5 Windows and macOS .

Issue	Description
GPC-26814	Split-tunnel exclusion does not support TURN or QUIC protocols (UDP 443). Due to the protocol behavior of TURN, traffic destined for excluded subnets over UDP 443 is still routed through the GlobalProtect tunnel even when matching exclusion routes are configured. This traffic appears in firewall traffic logs as originating from the tunnel interface, confirming that the GlobalProtect agent encapsulates it rather than routing it directly to the destination.
GPC-23149	Connection via captive portal does not work in agent proxy mode when the captive portal is hosted on a non-local network.
GPC-21694	When the GlobalProtect app is installed on Windows, a Microsoft Defender SmartScreen warning is displayed:. **Workaround:**Click More Info and then click Run to proceed with the installation.
GPC-21558	When the GlobalProtect app is installed on devices running on macOS and the end user enable or disable the system extensions, the GlobalProtect Enforcer feature is not working as expected.
GPC-20840	Loading content or text on the SAML embedded browser can take longer than usual. This does not impact authentication.
GPC-19339	When the GlobalProtect app is upgraded from version 6.1.4-c1 to 6.2.0-c4 on Linux devices, the GlobalProtect web interface displays the upgraded version only after a system reboot.
GPC-19180	When the GlobalProtect app is installed on Linux devices and the app is upgraded or downgraded, the GlobalProtect web interface

©2026 Palo Alto Networks, Inc.

Issue	Description
	and the command-line interface display the new version only after a system reboot.
GPC-17820	Firefox is not supported for proxied traffic in Tunnel and Proxy mode or proxy mode.
GPC-17727	When the GlobalProtect app is connected in Tunnel and Proxy mode or proxy mode, SSH traffic cannot be sent over the proxy.
GPC-17513	When GlobalProtect is configured in Tunnel and Proxy mode or proxy mode, if the admin-defined PAC file has an HTTP URL, the GlobalProtect app will not download the PAC content.
GPC-17447	When the GlobalProtect app is configured in Tunnel and Proxy mode, SSL VPN establishment over the proxy doesn't work.
GPC-17663	In Tunnel and Proxy mode, the GlobalProtect agent tunnel does not work seamlessly when the GlobalProtect app and the third-party VPN are configured to use overlapping IP subnets. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17555	In Tunnel and Proxy mode, the GlobalProtect agent tunnel on macOS does not coexist well with Cisco Anyconnect VPN due to an IP forwarding table issue. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17854	The GlobalProtect app does not prompt the users to extend the login lifetime user session when the device woke up from sleep or hibernation mode.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.4 Windows and macOS Known Issues

The following table lists the known issues in GlobalProtect app 6.2.4 Windows and macOS .

Issue	Description
GPC-23149	Connection via captive portal does not work in agent proxy mode when the captive portal is hosted on a non-local network.
GPC-21694	When the GlobalProtect app is installed on Windows, a Microsoft Defender SmartScreen warning is displayed:. **Workaround:**Click More Info and then click Run to proceed with the installation.
GPC-21558	When the GlobalProtect app is installed on devices running on macOS and the end user enable or disable the system extensions, the GlobalProtect Enforcer feature is not working as expected.
GPC-21442	Users running GlobalProtect client with Enforcer enabled may see an "Internet Blocked message" when performing SAML authentication for the nth time (n>1) via embedded web browser. This happens when Webview2 or Edge browser is updated between previous successful authentication and the current unsuccessful authentication attempt.. **Workaround:**Disable webview2 auto update via the group policy. If you still see the error message, restart the device.
GPC-20840	Loading content or text on the SAML embedded browser can take longer than usual. This does not impact authentication.
GPC-19339	When the GlobalProtect app is upgraded from version 6.1.4-c1 to 6.2.0-c4 on Linux devices, the GlobalProtect web interface displays the upgraded version only after a system reboot.

©2026 Palo Alto Networks, Inc.

Issue	Description
GPC-19180	When the GlobalProtect app is installed on Linux devices and the app is upgraded or downgraded, the GlobalProtect web interface and the command-line interface display the new version only after a system reboot.
GPC-17820	Firefox is not supported for proxied traffic in Tunnel and Proxy mode or proxy mode.
GPC-17727	When the GlobalProtect app is connected in Tunnel and Proxy mode or proxy mode, SSH traffic cannot be sent over the proxy.
GPC-17513	When GlobalProtect is configured in Tunnel and Proxy mode or proxy mode, if the admin-defined PAC file has an HTTP URL, the GlobalProtect app will not download the PAC content.
GPC-17447	When the GlobalProtect app is configured in Tunnel and Proxy mode, SSL VPN establishment over the proxy doesn't work.
GPC-17663	In Tunnel and Proxy mode, the GlobalProtect agent tunnel does not work seamlessly when the GlobalProtect app and the third-party VPN are configured to use overlapping IP subnets. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17555	In Tunnel and Proxy mode, the GlobalProtect agent tunnel on macOS does not coexist well with Cisco Anyconnect VPN due to an IP forwarding table issue. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17854	The GlobalProtect app does not prompt the users to extend the login lifetime user session when the device woke up from sleep or hibernation mode.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.3-c287 Windows and macOS Known Issues

The following table lists the known issues in GlobalProtect app 6.2.3-c287 Windows and macOS .

Issue	Description
GPC-23149	Connection via captive portal does not work in agent proxy mode when the captive portal is hosted on a non-local network.
GPC-21694	When the GlobalProtect app is installed on Windows, a Microsoft Defender SmartScreen warning is displayed:. **Workaround:**Click More Info and then click Run to proceed with the installation.
GPC-21558	When the GlobalProtect app is installed on devices running on macOS and the end user enable or disable the system extensions, the GlobalProtect Enforcer feature is not working as expected.
GPC-21442	Users running GlobalProtect client with Enforcer enabled may see an "Internet Blocked message" when performing SAML authentication for the nth time (n>1) via embedded web browser. This happens when Webview2 or Edge browser is updated between previous successful authentication and the current unsuccessful authentication attempt.. **Workaround:**Disable webview2 auto update via the group policy. If you still see the error message, restart the device.
GPC-20840	Loading content or text on the SAML embedded browser can take longer than usual. This does not impact authentication.
GPC-19339	When the GlobalProtect app is upgraded from version 6.1.4-c1 to 6.2.0-c4 on Linux devices, the GlobalProtect web interface displays the upgraded version only after a system reboot.

©2026 Palo Alto Networks, Inc.

Issue	Description
GPC-19180	When the GlobalProtect app is installed on Linux devices and the app is upgraded or downgraded, the GlobalProtect web interface and the command-line interface display the new version only after a system reboot.
GPC-17820	Firefox is not supported for proxied traffic in Tunnel and Proxy mode or proxy mode.
GPC-17727	When the GlobalProtect app is connected in Tunnel and Proxy mode or proxy mode, SSH traffic cannot be sent over the proxy.
GPC-17513	When GlobalProtect is configured in Tunnel and Proxy mode or proxy mode, if the admin-defined PAC file has an HTTP URL, the GlobalProtect app will not download the PAC content.
GPC-17447	When the GlobalProtect app is configured in Tunnel and Proxy mode, SSL VPN establishment over the proxy doesn't work.
GPC-17663	In Tunnel and Proxy mode, the GlobalProtect agent tunnel does not work seamlessly when the GlobalProtect app and the third-party VPN are configured to use overlapping IP subnets. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17555	In Tunnel and Proxy mode, the GlobalProtect agent tunnel on macOS does not coexist well with Cisco Anyconnect VPN due to an IP forwarding table issue. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17854	The GlobalProtect app does not prompt the users to extend the login lifetime user session when the device woke up from sleep or hibernation mode.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.3 Windows and macOS Known Issues

The following table lists the known issues in GlobalProtect app 6.2.3 Windows and macOS .

Issue	Description
GPC-23149	Connection via captive portal does not work in agent proxy mode when the captive portal is hosted on a non-local network.
GPC-21694	When the GlobalProtect app is installed on Windows, a Microsoft Defender SmartScreen warning is displayed:. **Workaround:**Click More Info and then click Run to proceed with the installation.
GPC-21558	When the GlobalProtect app is installed on devices running on macOS and the end user enable or disable the system extensions, the GlobalProtect Enforcer feature is not working as expected.
GPC-21442	Users running GlobalProtect client with Enforcer enabled may see an "Internet Blocked message" when performing SAML authentication for the nth time (n>1) via embedded web browser. This happens when Webview2 or Edge browser is updated between previous successful authentication and the current unsuccessful authentication attempt.. **Workaround:**Disable webview2 auto update via the group policy. If you still see the error message, restart the device.
GPC-20840	Loading content or text on the SAML embedded browser can take longer than usual. This does not impact authentication.
GPC-19339	When the GlobalProtect app is upgraded from version 6.1.4-c1 to 6.2.0-c4 on Linux devices, the GlobalProtect web interface displays the upgraded version only after a system reboot.

©2026 Palo Alto Networks, Inc.

Issue	Description
GPC-19180	When the GlobalProtect app is installed on Linux devices and the app is upgraded or downgraded, the GlobalProtect web interface and the command-line interface display the new version only after a system reboot.
GPC-17820	Firefox is not supported for proxied traffic in Tunnel and Proxy mode or proxy mode.
GPC-17727	When the GlobalProtect app is connected in Tunnel and Proxy mode or proxy mode, SSH traffic cannot be sent over the proxy.
GPC-17513	When GlobalProtect is configured in Tunnel and Proxy mode or proxy mode, if the admin-defined PAC file has an HTTP URL, the GlobalProtect app will not download the PAC content.
GPC-17447	When the GlobalProtect app is configured in Tunnel and Proxy mode, SSL VPN establishment over the proxy doesn't work.
GPC-17663	In Tunnel and Proxy mode, the GlobalProtect agent tunnel does not work seamlessly when the GlobalProtect app and the third-party VPN are configured to use overlapping IP subnets. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17555	In Tunnel and Proxy mode, the GlobalProtect agent tunnel on macOS does not coexist well with Cisco Anyconnect VPN due to an IP forwarding table issue. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17854	The GlobalProtect app does not prompt the users to extend the login lifetime user session when the device woke up from sleep or hibernation mode.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.2 Windows and macOS Known Issues

The following table lists the known issues in GlobalProtect app 6.2.2 Windows and macOS .

Issue	Description
GPC-23149	Connection via captive portal does not work in agent proxy mode when the captive portal is hosted on a non-local network.
GPC-21694	When the GlobalProtect app is installed on Windows, a Microsoft Defender SmartScreen warning is displayed:. **Workaround:**Click More Info and then click Run to proceed with the installation.
GPC-21558	When the GlobalProtect app is installed on devices running on macOS and the end user enable or disable the system extensions, the GlobalProtect Enforcer feature is not working as expected.
GPC-21442	Users running GlobalProtect client with Enforcer enabled may see an "Internet Blocked message" when performing SAML authentication for the nth time (n>1) via embedded web browser. This happens when Webview2 or Edge browser is updated between previous successful authentication and the current unsuccessful authentication attempt.. **Workaround:**Disable webview2 auto update via the group policy. If you still see the error message, restart the device.
GPC-20970	GlobalProtect can have intermittent connectivity issues on Prisma Access IP optimization enabled tenants. **Workaround:** If your Prisma Access tenant is IP Optimization enabled (available starting in Prisma Access 5.0.1), upgrade to GlobalProtect 6.1.4 and later, 6.2.3 and later, or 6.3 and later.

©2026 Palo Alto Networks, Inc.

Issue	Description
GPC-20840	Loading content or text on the SAML embedded browser can take longer than usual. This does not impact authentication.
GPC-19339	When the GlobalProtect app is upgraded from version 6.1.4-c1 to 6.2.0-c4 on Linux devices, the GlobalProtect web interface displays the upgraded version only after a system reboot.
GPC-19180	When the GlobalProtect app is installed on Linux devices and the app is upgraded or downgraded, the GlobalProtect web interface and the command-line interface display the new version only after a system reboot.
GPC-18025	In 6.2.1, after a refresh connection, the HIP patch exclusion isn't visible on the GlobalProtect UI. However, the HIP patch exclusion logs are visible on the `Pangphip.log` file.
GPC-17820	Firefox is not supported for proxied traffic in Tunnel and Proxy mode or proxy mode.
GPC-17727	When the GlobalProtect app is connected in Tunnel and Proxy mode or proxy mode, SSH traffic cannot be sent over the proxy.
GPC-17513	When GlobalProtect is configured in Tunnel and Proxy mode or proxy mode, if the admin-defined PAC file has an HTTP URL, the GlobalProtect app will not download the PAC content.
GPC-17447	When the GlobalProtect app is configured in Tunnel and Proxy mode, SSL VPN establishment over the proxy doesn't work.
GPC-17663	In Tunnel and Proxy mode, the GlobalProtect agent tunnel does not work seamlessly when the GlobalProtect app and the third-party VPN are configured to use overlapping IP subnets. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.

©2026 Palo Alto Networks, Inc.

Issue	Description
GPC-17555	In Tunnel and Proxy mode, the GlobalProtect agent tunnel on macOS does not coexist well with Cisco Anyconnect VPN due to an IP forwarding table issue. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17854	The GlobalProtect app does not prompt the users to extend the login lifetime user session when the device woke up from sleep or hibernation mode.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.1 Linux Known Issues

The following table lists the known issues in GlobalProtect app 6.2.1 Linux.

Issue	Description
GPC-23149	Connection via captive portal does not work in agent proxy mode when the captive portal is hosted on a non-local network.
GPC-21694	When the GlobalProtect app is installed on Windows, a Microsoft Defender SmartScreen warning is displayed:. **Workaround:**Click More Info and then click Run to proceed with the installation.
GPC-21558	When the GlobalProtect app is installed on devices running on macOS and the end user enable or disable the system extensions, the GlobalProtect Enforcer feature is not working as expected.
GPC-21442	Users running GlobalProtect client with Enforcer enabled may see an "Internet Blocked message" when performing SAML authentication for the nth time (n>1) via embedded web browser. This happens when Webview2 or Edge browser is updated between previous successful authentication and the current unsuccessful authentication attempt.. **Workaround:**Disable webview2 auto update via the group policy. If you still see the error message, restart the device.
GPC-20970	GlobalProtect can have intermittent connectivity issues on Prisma Access IP optimization enabled tenants. **Workaround:** If your Prisma Access tenant is IP Optimization enabled (available starting in Prisma Access 5.0.1), upgrade to GlobalProtect 6.1.4 and later, 6.2.3 and later, or 6.3 and later.

©2026 Palo Alto Networks, Inc.

Issue	Description
GPC-20840	Loading content or text on the SAML embedded browser can take longer than usual. This does not impact authentication.
GPC-19339	When the GlobalProtect app is upgraded from version 6.1.4-c1 to 6.2.0-c4 on Linux devices, the GlobalProtect web interface displays the upgraded version only after a system reboot.
GPC-19180	When the GlobalProtect app is installed on Linux devices and the app is upgraded or downgraded, the GlobalProtect web interface and the command-line interface display the new version only after a system reboot.
GPC-18964	The GlobalProtect tunnel disconnects after 10 minutes on app versions 6.0.8 and 6.2.1, when SAML authentication is used and the GlobalProtect app is running on macOS devices.
GPC-18025	In 6.2.1, after a refresh connection, the HIP patch exclusion isn't visible on the GlobalProtect UI. However, the HIP patch exclusion logs are visible on the `Pangphip.log` file.
GPC-17820	Firefox is not supported for proxied traffic in Tunnel and Proxy mode or proxy mode.
GPC-17727	When the GlobalProtect app is connected in Tunnel and Proxy mode or proxy mode, SSH traffic cannot be sent over the proxy.
GPC-17513	When GlobalProtect is configured in Tunnel and Proxy mode or proxy mode, if the admin-defined PAC file has an HTTP URL, the GlobalProtect app will not download the PAC content.
GPC-17447	When the GlobalProtect app is configured in Tunnel and Proxy mode, SSL VPN establishment over the proxy doesn't work.
GPC-17663	In Tunnel and Proxy mode, the GlobalProtect agent tunnel does not work seamlessly when the GlobalProtect app and the third-party

©2026 Palo Alto Networks, Inc.

Issue	Description
	VPN are configured to use overlapping IP subnets. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17555	In Tunnel and Proxy mode, the GlobalProtect agent tunnel on macOS does not coexist well with Cisco Anyconnect VPN due to an IP forwarding table issue. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17854	The GlobalProtect app does not prompt the users to extend the login lifetime user session when the device woke up from sleep or hibernation mode.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.1 Windows and macOS Known Issues

The following table lists the known issues in GlobalProtect app 6.2.1 Windows and macOS.

Issue	Description
GPC-23149	Connection via captive portal does not work in agent proxy mode when the captive portal is hosted on a non-local network.
GPC-21694	When the GlobalProtect app is installed on Windows, a Microsoft Defender SmartScreen warning is displayed:. **Workaround:**Click More Info and then click Run to proceed with the installation.
GPC-21558	When the GlobalProtect app is installed on devices running on macOS and the end user enable or disable the system extensions, the GlobalProtect Enforcer feature is not working as expected.
GPC-21442	Users running GlobalProtect client with Enforcer enabled may see an "Internet Blocked message" when performing SAML authentication for the nth time (n>1) via embedded web browser. This happens when Webview2 or Edge browser is updated between previous successful authentication and the current unsuccessful authentication attempt.. **Workaround:**Disable webview2 auto update via the group policy. If you still see the error message, restart the device.
GPC-20970	GlobalProtect can have intermittent connectivity issues on Prisma Access IP optimization enabled tenants. **Workaround:** If your Prisma Access tenant is IP Optimization enabled (available starting in Prisma Access 5.0.1), upgrade to GlobalProtect 6.1.4 and later, 6.2.3 and later, or 6.3 and later.

©2026 Palo Alto Networks, Inc.

Issue	Description
GPC-20840	Loading content or text on the SAML embedded browser can take longer than usual. This does not impact authentication.
GPC-19339	When the GlobalProtect app is upgraded from version 6.1.4-c1 to 6.2.0-c4 on Linux devices, the GlobalProtect web interface displays the upgraded version only after a system reboot.
GPC-19180	When the GlobalProtect app is installed on Linux devices and the app is upgraded or downgraded, the GlobalProtect web interface and the command-line interface display the new version only after a system reboot.
GPC-18964	The GlobalProtect tunnel disconnects after 10 minutes on app versions 6.0.8 and 6.2.1, when SAML authentication is used and the GlobalProtect app is running on macOS devices.
GPC-18025	In 6.2.1, after a refresh connection, the HIP patch exclusion isn't visible on the GlobalProtect UI. However, the HIP patch exclusion logs are visible on the `Pangphip.log` file.
GPC-17820	Firefox is not supported for proxied traffic in Tunnel and Proxy mode or proxy mode.
GPC-17727	When the GlobalProtect app is connected in Tunnel and Proxy mode or proxy mode, SSH traffic cannot be sent over the proxy.
GPC-17513	When GlobalProtect is configured in Tunnel and Proxy mode or proxy mode, if the admin-defined PAC file has an HTTP URL, the GlobalProtect app will not download the PAC content.
GPC-17447	When the GlobalProtect app is configured in Tunnel and Proxy mode, SSL VPN establishment over the proxy doesn't work.
GPC-17663	In Tunnel and Proxy mode, the GlobalProtect agent tunnel does not work seamlessly when the GlobalProtect app and the third-party

©2026 Palo Alto Networks, Inc.

Issue	Description
	VPN are configured to use overlapping IP subnets. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17555	In Tunnel and Proxy mode, the GlobalProtect agent tunnel on macOS does not coexist well with Cisco Anyconnect VPN due to an IP forwarding table issue. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17854	The GlobalProtect app does not prompt the users to extend the login lifetime user session when the device woke up from sleep or hibernation mode.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.0 Linux Known Issues

The following table lists the known issues in GlobalProtect app 6.2.0 for Linux.

Issue	Description
GPC-23149	Connection via captive portal does not work in agent proxy mode when the captive portal is hosted on a non-local network.
GPC-21694	When the GlobalProtect app is installed on Windows, a Microsoft Defender SmartScreen warning is displayed:. **Workaround:**Click More Info and then click Run to proceed with the installation.
GPC-21558	When the GlobalProtect app is installed on devices running on macOS and the end user enable or disable the system extensions, the GlobalProtect Enforcer feature is not working as expected.
GPC-21442	Users running GlobalProtect client with Enforcer enabled may see an "Internet Blocked message" when performing SAML authentication for the nth time (n>1) via embedded web browser. This happens when Webview2 or Edge browser is updated between previous successful authentication and the current unsuccessful authentication attempt.. **Workaround:**Disable webview2 auto update via the group policy. If you still see the error message, restart the device.
GPC-20970	GlobalProtect can have intermittent connectivity issues on Prisma Access IP optimization enabled tenants. **Workaround:** If your Prisma Access tenant is IP Optimization enabled (available starting in Prisma Access 5.0.1), upgrade to GlobalProtect 6.1.4 and later, 6.2.3 and later, or 6.3 and later.

©2026 Palo Alto Networks, Inc.

Issue	Description
GPC-20840	Loading content or text on the SAML embedded browser can take longer than usual. This does not impact authentication.
GPC-19339	When the GlobalProtect app is upgraded from version 6.1.4-c1 to 6.2.0-c4 on Linux devices, the GlobalProtect web interface displays the upgraded version only after a system reboot.
GPC-19180	When the GlobalProtect app is installed on Linux devices and the app is upgraded or downgraded, the GlobalProtect web interface and the command-line interface display the new version only after a system reboot.
GPC-18964	The GlobalProtect tunnel disconnects after 10 minutes on app versions 6.0.8 and 6.2.1, when SAML authentication is used and the GlobalProtect app is running on macOS devices.
GPC-18025	In 6.2.1, after a refresh connection, the HIP patch exclusion isn't visible on the GlobalProtect UI. However, the HIP patch exclusion logs are visible on the `Pangphip.log` file.
GPC-17820	Firefox is not supported for proxied traffic in Tunnel and Proxy mode or proxy mode.
GPC-17816	After entering CIE SAML authentication credentials to refresh an expired explicit proxy token or cookie when connected in Tunnel and Proxy mode or proxy mode, the GlobalProtect app gets stuck while retrieving the portal configuration. **Workaround:** Refresh the GlobalProtect connection or disconnect and reconnect the GlobalProtect app.
GPC-17727	When the GlobalProtect app is connected in Tunnel and Proxy mode or proxy mode, SSH traffic cannot be sent over the proxy.
GPC-17513	When GlobalProtect is configured in Tunnel and Proxy mode or proxy mode, if the admin-defined PAC file has an HTTP URL, the

 ©2026 Palo Alto Networks, Inc.

Issue	Description
	GlobalProtect app will not download the PAC content.
GPC-17447	When the GlobalProtect app is configured in Tunnel and Proxy mode, SSL VPN establishment over the proxy doesn't work.
GPC-17663	In Tunnel and Proxy mode, the GlobalProtect agent tunnel does not work seamlessly when the GlobalProtect app and the third-party VPN are configured to use overlapping IP subnets. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17555	In Tunnel and Proxy mode, the GlobalProtect agent tunnel on macOS does not coexist well with Cisco Anyconnect VPN due to an IP forwarding table issue. **Workaround:** Use GlobalProtect in proxy mode for better compatibility with third-party VPNs.
GPC-17854	The GlobalProtect app does not prompt the users to extend the login lifetime user session when the device woke up from sleep or hibernation mode.

©2026 Palo Alto Networks, Inc.

Addressed Issues

To view the addressed issues in a release, select the appropriate version from the left navigation bar.

GlobalProtect App 6.2.8-h15 (6.2.8-c1084) Windows and macOS Addressed Issues

The following table lists the issues that are addressed in GlobalProtect app 6.2.8-h15 (6.2.8-c1084) Windows and macOS.

Issue ID	Description
GPC-27851	Fixed an issue where GlobalProtect could not connect after an upgrade, which occurred because the GlobalProtect service sent portal configuration and gateway authentication requests to the portal's connected IP address instead of its fully qualified domain name (FQDN), causing certificate verification to not succeed. Users encountered the error "The network connection is unreachable or the gateway is unresponsive. Check the network connection and reconnect." With this fix, GlobalProtect correctly routes requests to the portal FQDN and connects as expected.
GPC-27846	(macOS devices) Fixed an issue where GlobalProtect authentication did not complete during the portal sign-in process, which caused users to encounter an "Authentication Failed" error. This occurred because the GlobalProtect service stopped unexpectedly during SAML authentication. With this fix, GlobalProtect authenticates and connects as expected.
GPC-27555	Fixed an issue where GlobalProtect user connections were disconnecting after one hour, which occurred when the portal refresh process initiated and the client encountered an error during its network configuration update. With this fix, GlobalProtect connections now refresh as expected without interruption.
GPC-27513	Fixed an issue where GlobalProtect intermittently did not detect the Real-time Protection (RTP) state of Windows Defender, which prevented authorized users from accessing resources when Host Information Profile (HIP) policies were applied. This behavior occurred after an upgrade of Windows Defender. With this fix, GlobalProtect properly detects the RTP state of Windows Defender.
GPC-27403	(GlobalProtect client on Windows devices using SmartCard authentication) Fixed an issue where the GlobalProtect client would unexpectedly terminate and fail to establish a connection, which was caused by inter-process communication issues during the authentication process. With this fix, the client connects as expected.
GPC-27394	Fixed an issue where GlobalProtect gateway certificate verification would fail after a software upgrade, which prevented connections to

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	the gateway. With this fix, gateway certificate verification proceeds as expected.
GPC-27281	Fixed an issue where GlobalProtect Host Information Profile (HIP) checks intermittently failed with an "Invalid authentication cookie" error after machines woke up from modern standby, which caused traffic to incorrectly match policies without HIP requirements or fall through to default rules. With this fix, HIP checks proceed as expected, and traffic correctly matches policies based on HIP requirements.
GPC-27202	Fixed an issue where GlobalProtect log entries for macOS agents that disconnected using ticket were not displayed in the Strata Cloud Manager Log Viewer, which led to an inconsistency in log reporting compared with Windows agents. With this fix, log entries for macOS agents are displayed correctly.
GPC-27149	Fixed an issue where GlobalProtect connections would intermittently stall, preventing internet access. With this fix, GlobalProtect connections establish and maintain properly.
GPC-26994	Fixed an issue where Host Information Profile (HIP) reports were not sent to the gateway intermittently, which resulted in issues with user-IP mapping. With this fix, HIP reports are sent consistently, ensuring accurate user-IP mapping.
GPC-26933	(macOS endpoints only) Fixed an issue where the GlobalProtect app would not connect to the GlobalProtect service after a macOS upgrade and a sleep-wake event. With this fix, the GlobalProtect app connects as expected.
GPC-26928	Fixed an issue where the GlobalProtect client would remain in a connecting state after an initial authentication attempt failed, and would not attempt to connect to alternate gateways. With this fix, the GlobalProtect client now properly transitions out of the connecting state and attempts alternate gateways when authentication fails.
GPC-26808	Fixed an issue where GlobalProtect did not detect a specific version of the Broadcom Endpoint Security Agent (ESA) on macOS endpoints. With this fix, the agent is correctly detected, and administrators can configure policies for it.
GPC-26790	(macOS devices running GlobalProtect) Fixed an issue where GlobalProtect would not connect, which caused users to encounter a "Could not connect to the GlobalProtect service" error after a macOS update or system reboot. This occurred because the GlobalProtect

©2026 Palo Alto Networks, Inc.

Issue ID	Description
	service would not start or would stop unexpectedly. With this fix, GlobalProtect connects successfully.
GPC-26780	(macOS devices only) Fixed an issue where GlobalProtect would get stuck in a connecting state after the device woke from sleep or reconnected to a network, which resulted from GlobalProtect attempting to resolve the gateway's fully qualified domain name (FQDN) using the tunnel's DNS instead of the local internet service provider (ISP) DNS. With this fix, GlobalProtect correctly uses the local ISP DNS for gateway FQDN resolution when disconnected.
GPC-26764	(GlobalProtect app on macOS devices) Fixed an issue where the GlobalProtect app initiated unexpected portal requests after a manual gateway selection. With this fix, the app behaves as expected after a manual gateway selection.
GPC-26699	(macOS only) Fixed an issue where the GlobalProtect user interface popover would not dismiss after a successful connection, which occurred because the GlobalProtect menu bar icon became inaccessible when hidden by the operating system. With this fix, the popover automatically dismisses after a successful connection.
GPC-26682	Fixed an issue where internet connectivity would stop working on macOS when the GlobalProtect client was connected to certain mobile hotspots that assigned IP addresses from a specific reserved range, which occurred because the GlobalProtect client did not properly process this particular IP address range used in some mobile network environments. With this fix, internet connectivity is maintained in these scenarios.
GPC-26657	Fixed an issue where the HIP process repeatedly launched in a rapid-fire loop, which triggered alerts. With this fix, the process launches as expected.
GPC-26619	(GlobalProtect app on macOS only) Fixed an issue where the GlobalProtect app remained in a connecting state for approximately two minutes after a local network-extension or route-change event, which required a restart of the app to recover. With this fix, the GlobalProtect app now connects as expected after such events.
GPC-26618	(GlobalProtect app on macOS) Fixed an issue where the GlobalProtect app would fail to connect to gateways after a manual gateway selection. With this fix, the GlobalProtect app connects successfully to gateways after manual selection.
GPC-26560	Fixed an issue where GlobalProtect app connections experienced a delay when Autonomous Digital Experience Management (ADEM) was

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	disabled in the portal, which occurred because the agent continued to search for the ADEM configuration file. With this fix, the agent no longer attempts to locate the ADEM configuration file when ADEM is disabled.
GPC-26558	Fixed an issue where GlobalProtect App disconnect reason text was truncated in the user interface when the GlobalProtect Portal was configured with a custom disconnect reason, which prevented the full message from being displayed. With this fix, the user interface now properly displays the complete disconnect reason.
GPC-26537	Fixed an issue where an unauthorized user could disconnect a GlobalProtect connection after interrupting Security Assertion Markup Language (SAML) authentication during a connection refresh. With this fix, the Disconnect button no longer appeared for unauthorized users in this scenario.
GPC-26536	Fixed an issue where the GlobalProtect client on macOS would intermittently become stuck in a connecting state after the system resumed from sleep mode, which prevented internet access even after disconnecting the virtual private network (VPN). With this fix, the client now connects as expected and allows proper network access.
GPC-26224	Fixed an issue where the GlobalProtect client stole focus when a user entered a PIN for PINGID/Security Assertion Markup Language (SAML) authentication. With this fix, the GlobalProtect client no longer unexpectedly takes focus during this authentication process.
GPC-26133	Fixed an issue where the `DisplayVersion` registry key for GlobalProtect clients on Windows reported an incomplete version string, which led to other software misidentifying the installed GlobalProtect version. With this fix, the registry key now accurately reflects the full client version.
GPC-26088	Fixed an issue where the GlobalProtect Enforcer did not unblock network traffic after a GlobalProtect connection was established, which resulted in the blocking of traffic not explicitly excluded from enforcement. With this fix, the GlobalProtect Enforcer now correctly unblocks traffic upon successful GlobalProtect connection.
GPC-25840	Fixed an issue where applications configured for split tunneling would not function correctly after a network transition. With this fix, applications would function as expected after network changes.
GPC-25670	Fixed an issue where the GlobalProtect app would intermittently get stuck in a connecting state after a laptop woke up from standby,

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	preventing it from establishing a connection to the gateway. With this fix, the GlobalProtect agent connects successfully.
GPC-25575	(macOS devices only) Fixed an issue where custom Host Information Profile (HIP) checks did not correctly evaluate certain system configuration parameters, which prevented macOS devices from matching the intended HIP objects. With this fix, HIP checks accurately evaluate the system configuration parameters.
GPC-25567	Fixed an issue where the GlobalProtect Client would intermittently not complete Kerberos Single Sign-On (SSO) during pre-login. This occurred when the client did not post the Kerberos token back after receiving an initial authentication challenge from the portal, which prompted users for credentials and displayed an error message indicating an unreachable network or unresponsive portal. With this fix, Kerberos SSO now succeeds consistently.
GPC-25308	Fixed an issue where the GlobalProtect app intermittently stopped transmitting Host Information Profile (HIP) reports, which caused User-ID entries to be cleared and resulted in missing user-to-IP mappings. With this fix, the GlobalProtect app now consistently transmits HIP reports, maintaining accurate user-to-IP mappings.
GPC-25219	Fixed an issue where users were unable to select the GlobalProtect icon from the status bar on macOS.

 ©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.8-h13 (6.2.8-c1045) Windows and macOS Addressed Issues

The following table lists the issues addressed in GlobalProtect app 6.2.8-h13 (6.2.8-c1045) Windows and macOS.

Issue ID	Description
GPC-27179	Fixed an issue where GlobalProtect portal registration was prevented during SAML authentication hand-off, which caused agents to remain disconnected despite successful authentication with an identity provider. This occurred because an internal data buffer became corrupted during the authentication token hand-off, which led to the loss of session identity. With this fix, the authentication token is correctly processed, allowing agents to register with the portal.
GPC-27177	Fixed an issue where GlobalProtect Host Information Profile (HIP) reports had an invalid XML format. With this fix, HIP reports are generated with the correct XML structure.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.8-h12 (6.2.8-c1032) Windows and macOS Addressed Issues

The following table lists the issues that are addressed in GlobalProtect app 6.2.8-h12 Windows and macOS.

Issue ID	Description
GPC-26949	Fixed an issue where the GlobalProtect embedded browser would stall in a connecting state when a macOS device attempted to establish a connection to the identity provider after waking from sleep. With this fix, the connection process completes successfully.
GPC-26946	Fixed an issue where GlobalProtect would skip sending a Host Information Profile (HIP) report after a network change, such as transitioning between wired and Wi-Fi networks. This behavior prevented the firewall from receiving necessary data to maintain the user's session, which resulted in an outage. With this fix, GlobalProtect now properly sends HIP reports after network changes.
GPC-26856	Fixed an issue where GlobalProtect Host Information Profile (HIP) recognition incorrectly reported the Real-Time Protection (RTP) status of a specific antivirus product, which caused endpoints to be marked as non-compliant and resulted in blocked network access. This occurred after an external update and rebranding of the antivirus product. With this fix, GlobalProtect accurately identifies the RTP status, ensuring correct compliance enforcement.
GPC-26275	Fixed an issue where the Traffic Blocking Notification message was not displayed when GlobalProtect Connection for Network Access was enforced and a user connected to a network behind a Captive Portal before completing authentication. With this fix, the notification message "To access the network, you must first connect to GlobalProtect." displays as expected.
GPC-26227	Fixed an issue where your GlobalProtect client connected to a geographically distant GlobalProtect gateway even when a closer, preferred gateway was available. This occurred when your network connection became temporarily unavailable during the GlobalProtect client's attempt to connect to the preferred gateway. With this fix, your GlobalProtect client correctly prioritizes and connects to the optimal gateway after network connectivity is restored.
GPC-26152	Fixed an issue where GlobalProtect users would fail to authenticate when their usernames contained certain special characters, which led to a mismatch in character interpretation during the authentication process. With this fix, GlobalProtect now correctly processes

©2026 Palo Alto Networks, Inc.

Issue ID	Description
	usernames containing these special characters, allowing for successful authentication.
GPC-25996	Fixed an issue where GlobalProtect target gateway selection reverted to the default after a few seconds. With this fix, the target gateway selection now persisted as configured.
GPC-25879	Fixed an issue where GlobalProtect incorrectly detected an internal network over the tunnel, which happened when SAML authentication timed out during a GlobalProtect gateway switch. With this fix, GlobalProtect accurately determines network connectivity.
GPC-25869	(macOS clients only) Fixed an issue where GlobalProtect connections would not establish after a reboot, which occurred because the GlobalProtect agent did not start or connect properly. With this fix, GlobalProtect connections establish as expected after a reboot.
GPC-25866	Fixed an issue where the system did not send a Host Information Profile (HIP) report when real-time protection was detected as enabled after an initial detection of it being disabled immediately following power-on, which occurred because the system created a new HIP report but did not send it. With this fix, the system correctly sends HIP reports when the real-time protection status changes.
GPC-25797	Fixed an issue where GlobalProtect connections would show a connected status but would not pass traffic. Attempts to refresh the connection would also fail, preventing further connection establishment for a period. With this fix, GlobalProtect connections properly pass traffic when showing a connected status.
GPC-25792	Fixed an issue where GlobalProtect would not reconnect when Dynamic Link State Awareness (DLSA) was handling dual Network Interface Cards (NICs) if the gateway IP was not explicitly added to split routing, which occurred because the previous implementation required the gateway IP to be known and configured for split routing in such scenarios. With this fix, DLSA now handles dual NIC scenarios without requiring the gateway IP to be added to split routing.
GPC-25731	Fixed an issue where GlobalProtect split-tunnel configurations did not correctly exclude multicast IP addresses. With this fix, multicast IP addresses are excluded as configured.
GPC-25677	Fixed an issue where, on GlobalProtect deployments with Windows clients configured for "Pre-logon (Always On)" connection, the GlobalProtect App would incorrectly establish an external GlobalProtect gateway tunnel immediately after a user logged into their Windows account, even when the client was connected to the

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	internal network. This behavior occurred when the GlobalProtect Portal agent configuration had the "Enable Cache Portal Configuration in Absence of Pre-logon Tunnel" setting enabled and the "Pre-Logon Tunnel Rename Timeout (sec) (Windows Only)" was set to a positive value, leading to a bypass of internal network discovery during the pre-logon tunnel rename process.
GPC-25512	Fixed an issue where the GlobalProtect Agent (PanGPA) would unexpectedly terminate in a Prisma Access environment, which was related to cryptographic operations. With this fix, the GlobalProtect Agent maintains stable operation.
GPC-25511	Fixed an issue where macOS GlobalProtect clients running version 6.2.8-h7 experienced a failure in IPv6 routing and traffic flow through the VPN tunnel. This occurred because the GlobalProtect client did not correctly install IPv6 routes when the gateway's Fully Qualified Domain Name (FQDN) lacked an AAAA DNS record, leading to an empty remoteHostV6 variable and the IPv6 system configuration being skipped, even when the gateway assigned an IPv6 tunnel IP and provided access routes.
GPC-25484	Fixed an issue where the GlobalProtect Agent software (versions 6.2.8 H4, 6.2.8 H7, and 6.3.3) would crash, disconnect from the VPN, and restart when a user clicked outside the 'Add Portal Address' window while it was open.
GPC-25459	Fixed an issue where GlobalProtect exclude routes were not installed correctly on Windows endpoints. With this fix, exclude routes install as expected.
GPC-25444	Fixed an issue where GlobalProtect clients on macOS would display a "Portal not found" or "Could not connect to Authentication server" error on the first connection attempt to the GlobalProtect portal after an upgrade or system reboot, requiring a second attempt to successfully connect.
GPC-25425	(GlobalProtect client on Windows 11 only) Fixed an issue where the GlobalProtect client window displayed a blank screen, which prevented the connection status from appearing. This issue occurred intermittently, particularly after the computer woke up. With this fix, the client window displays the connection status as expected.
GPC-25396	Fixed an issue where macOS GlobalProtect clients lost internet connectivity after switching between different GlobalProtect portals. This occurred because the client retained incorrect Domain Name System (DNS) server assignments from the previously connected

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	portal, which prevented successful name resolution. With this fix, the client properly updates DNS settings when switching portals.
GPC-25286	Fixed an issue where importing a self-signed root certificate into the user trust store through the GlobalProtect (GP) portal's `Agent -> Trusted Root CA -> install in local root certificate store` option would not complete, which occurred when strict certificate checking options were enabled, even if the GlobalProtect portal's own certificate was trusted. With this fix, the import process completes as expected under these conditions.
GPC-25221	Fixed an issue where the Real Time protection status for Carbon Black Cloud Sensor was displayed as 'n/a', which occurred even after the sensor product was correctly detected. With this fix, the Real Time protection status is now correctly recognized and populated.
GPC-24969	Fixed an issue where on Windows endpoints, the system's proxy AutoConfigURL was not restored to its original value after GlobalProtect disconnected, specifically when GlobalProtect had pushed a different proxy AutoConfigURL during the connection.
GPC-24968	Fixed an issue where GlobalProtect clients failed to correctly parse the internal gateway IP address provided via DHCP option 43 with sub-option 100, causing the client to attempt connection to an incorrect IP address.
GPC-24587	Fixed an issue where GlobalProtect client version 6.2.8, when installed in FIPS-CC mode on client machines with AMD chipsets, failed with an error message indicating that the CPU does not support RDSEED/RDRAND instructions. This occurred because the openssl library was built with the RDCPU flag, leading to an incorrect assessment of CPU capabilities on AMD platforms.
GPC-24138	Fixed an issue where GlobalProtect Portal and Gateway logs (`pan_gp_event.log`) did not provide detailed error messages when client certificate authentication failed during the pre-logon stage, particularly when the private key was stored on a Trusted Platform Module (TPM).
GPC-24065	Fixed an issue where GlobalProtect displayed a connected status, but internet connectivity was interrupted, which led to dropped calls and other service disruptions. This occurred because the GlobalProtect virtual adapter unexpectedly disconnected when an IPSec tunnel failed to gracefully fall back to an SSL tunnel. With this fix, the GlobalProtect virtual adapter maintains its connection and properly transitions between tunnel types.

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
GPC-23848	Fixed an issue where the GlobalProtect client (version 6.2.8-243) on macOS 15.5 (Build 24F74) caused excessive memory consumption, with the GlobalProtect process consuming up to 27 GB of memory, due to improper memory management related to autoreleasepool.
GPC-23551	Fixed an issue where the virtual network adapter retained the static IP address assigned by GlobalProtect even after the GlobalProtect client disconnected. This caused DNS registration conflicts, making workstations unreachable by hostname even after a reboot.
GPC-22392	Fixed an issue where the GlobalProtect client for Windows (Spanish version) displayed an incorrect translation, "Logs ficticios" (Fake logs), for the log collection option in the Settings > Troubleshooting menu.
GPC-17407	Fixed an issue where traffic to loopback addresses within the 127.0.0.0/8 subnet, excluding 127.0.0.1, was dropped when Endpoint Traffic Policy Enforcement was enabled, which prevented applications from using these loopback addresses for internal communication. With this fix, traffic to the entire loopback subnet is handled correctly.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.8-h11 (6.2.8-c982) Windows and macOS Addressed Issues

The following table lists the issues that are addressed in GlobalProtect app 6.2.8-h11 (6.2.8-c982) Windows and macOS.

Issue ID	Description
GPC-24992	Fixed an issue where GlobalProtect users experienced long login delays after rebooting or shutting down their device. This occurred because the PanGPA process spawned multiple `msedgewebview2.exe` processes to facilitate SAML authentication, and these processes entered a frozen state, causing the connection to hang on "Getting Portal Configuration." With this fix, GlobalProtect correctly handles the WebView2 authentication process and connects without delay after a reboot or shutdown.
GPC-26311	Fixed an issue where GlobalProtect users were unable to submit Host Information Profile (HIP) reports, which prevented security rules requiring a HIP match from applying. This occurred when you connected to an NGPA gateway using a dual-stack network, such as a mobile hotspot. With this fix, GlobalProtect successfully submits HIP reports regardless of your network configuration.
GPC-25946	Fixed an issue where your GlobalProtect client did not send Host Information Profile (HIP) check and report messages after you established a connection to the gateway. This occurred even when a HIP report was generated shortly before the connection, which could have impacted security posture assessment. With this fix, your GlobalProtect client now correctly sends HIP check and report messages after establishing a connection.
GPC-25776	Fixed an issue where GlobalProtect clients displayed an incorrect "Connecting" status after a GlobalProtect Portal or Gateway authentication failure, specifically when "Portal auth failed but SAML/CAS auth is successful". This misleading status persisted even though the connection had actually failed, preventing users from understanding the true connection state.
GPC-25541	Fixed an issue where MacOS GlobalProtect client version 6.2.8-416 was unable to connect to the GlobalProtect gateway, getting stuck in a connecting state.
GPC-25490	(MacBook devices) Fixed an issue where your GlobalProtect enabled device lost internet access after returning from hibernation. This occurred when your computer completely lost network connectivity,

©2026 Palo Alto Networks, Inc.

Issue ID	Description
	requiring a restart to restore internet access. With this fix, your device maintains network connectivity after resuming from hibernation.
GPC-25394	Fixed an issue where your traffic continued to pass through the GlobalProtect tunnel interface after you disconnected GobalProtect, preventing it from reverting to your local interface. With this fix, your traffic properly reverts to the local interface after GlobalProtect disconnects.
GPC-25320	Fixed an issue where GlobalProtect intermittently appeared in the foreground of your user session. This occurred even when you configured GlobalProtect for on-demand connections and were not actively trying to connect, causing it to overshadow other applications. With this fix, GlobalProtect remains in the background until you actively initiate a connection.
GPC-25280	Fixed an issue where GlobalProtect clients on macOS devices would intermittently get stuck in a "Connecting" state for several minutes after waking from modern standby. This occurred due to a race condition between DNS proxy reconfiguration and the VPN connection process during wake from sleep, where the macOS DNS proxy would temporarily stop and restart, causing the PanGPS service to time out when attempting to send DNS configuration commands. This led to repeated connection failures until the DNS proxy fully stabilized, a condition that was exacerbated by the presence of multiple network extensions on the macOS device.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.8-h10 (6.2.8-c948) Windows and macOS Addressed Issues

The GlobalProtect app 6.2.8-h10 (6.2.8-c948) release includes performance and bug fixes.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.8-h9 (6.2.8-c910) Windows and macOS Addressed Issues

The following table lists the issues that are addressed in GlobalProtect app 6.2.8-h9 (6.2.8-c910) Windows and macOS.

Issue ID	Description
GPC-25324	Fixed an issue where the GlobalProtect client briefly displayed a "Sign-out" option after the application was ended from the task manager and restarted, even when the portal configuration had "Allow users to sign-out" set to "No". This was caused by a race condition during the client's initialization, where the sign-out button was temporarily visible before the portal's configuration to disable it could be loaded.
GPC-25300	Fixed an issue where GlobalProtect clients experienced frequent disconnections from GlobalProtect gateways. After being disconnected, users were often unable to reconnect for extended periods, and connection attempts to designated gateways, including those manually selected or identified as 'Best Available', would incorrectly redirect to other gateways.
GPC-25222	Fixed an issue where GlobalProtect clients failed to detect captive portals on public Wi-Fi networks, even when the captive portal responded with an HTTP 302 Redirect. This occurred because the GlobalProtect agent expected the HTTP response to be terminated by `\r\n\r\n` as per RFC, but some captive portals did not adhere to this, causing the agent to incorrectly report that no data was received from the captive portal server and thus fail to detect the portal.
GPC-25215	Fixed an issue on macOS devices running the GlobalProtect agent and has multiple physical interfaces, when Disable Local Subnet Access (DLSA) feature was active, manually disabling the GlobalProtect agent caused the client to lose routing information. This prevented the client from reaching the GlobalProtect portal or gateway, even though FQDN resolution was successful, resulting in "Network is unreachable" errors and requiring a device reboot to restore connectivity.
GPC-25172	Fixed an issue where, on macOS GlobalProtect clients, exclude routes were not properly removed from the system routing table after a PanGPS (GlobalProtect client) crash. This occurred because the routes remained in the macOS kernel, and upon reconnection, the client's `checkExistingExRts()` function only validated the destination and netmask, not the gateway. As a result, these stale routes, pointing to an old or unreachable gateway, were marked as existing and skipped during the reconnection process, leading to a corrupted routing state

©2026 Palo Alto Networks, Inc.

Issue ID	Description
	and preventing correct route injection, especially after a network change.
GPC-25148	Fixed an issue where GlobalProtect intermittently displayed a large blank rectangle (bottom right side of the screen) on connection failure on macOS 26 (Tahoe).
GPC-25121	Fixed an issue where the GlobalProtect DNS proxy Network Extension on macOS endpoints failed to start due to retaining an incorrect Process ID (PID) for the GlobalProtect app (PanGPA) after PanGPA restarted. This prevented split-tunnel exclude applications from functioning correctly.
GPC-24845	Fixed an issue where GlobalProtect users on Prisma Access intermittently experienced "No user mapping" issues across multiple gateways.
GPC-24659	Fixed an issue where macOS GlobalProtect clients failed to complete transparent upgrades from a GlobalProtect portal because the download of the upgrade package timed out.
GPC-24600	Fixed an issue where macOS GlobalProtect clients (versions 6.2.8 and 6.3.3) were stuck in a connecting state after the macOS device woke up from sleep mode (Modern Standby), particularly when using Certificate or SAML authentication, requiring a manual connection refresh.
GPC-24538	Fixed an issue where the GlobalProtect client, specifically versions 6.2.8 and 6.2.6-857, would crash immediately after installation on Microsoft Windows 11 Pro (64-bit) endpoints. The `PanGPA` process would exit due to a null pointer dereference, preventing the client from launching.
GPC-24300	Fixed an issue where GlobalProtect clients running version 6.2.8-h2, when initially loading a pre-logon configuration, failed to correctly apply traffic exclusion rules for specified FQDNs (such as Avaya VoIP traffic), causing the excluded traffic to be sent through the GlobalProtect tunnel instead of the physical interface. This occurred because an internal driver event reset a flag, preventing additional IP rules from being set, and was resolved after the GlobalProtect connection was refreshed and the default configuration was loaded.
GPC-24006	Fixed an issue where MacOS GlobalProtect clients, when configured for Okta authentication with Prisma Access, intermittently failed to log in after a previous log-off. This failure manifested as an "Okta device not on-line" error, caused by the GlobalProtect client's log-off process

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	not completing gracefully, which resulted in the client service not starting correctly on subsequent login attempts.
GPC-25637	Fixed an issue where on macOS devices, after upgrading macOS to version 26.3 (from 26.2), the GlobalProtect client was unable to connect and displayed the error "Could not connect to the GlobalProtect service.
GPC-25196	Fixed an issue where the GlobalProtect client UI on macOS devices would remain open in the dock and sometimes on top of other applications after the device resumed from hibernation or sleep mode. This behavior, observed in GlobalProtect client versions 6.2.8 and 6.3.2, was caused by the `globalClickMonitor` not being reset after the device woke up, preventing the UI from properly minimizing or closing.
GPC-25702	Fixed an issue where the GlobalProtect service (PanGPS) failed to start after upgrading macOS to version 26.3.1 (Tahoe), displaying the error "Could not connect to the GlobalProtect service. Make sure the GlobalProtect service is running." This occurred because the macOS upgrade disrupted the LaunchAgent registration for the GlobalProtect service. With this fix, the GlobalProtect service starts correctly after a macOS upgrade.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.8-h7 (6.2.8-c471) Windows and macOS Addressed Issues

The following table lists the issues that are addressed in GlobalProtect app 6.2.8-h7 (6.2.8-c471) Windows and macOS.

Issue ID	Description
GPC-25063	Fixed an issue where, in the GlobalProtect app on macOS, keyboard focus did not automatically move to the required "Enter portal Address" field when a user attempted to add a new portal without entering an address. This accessibility issue impacted keyboard-dependent users.
GPC-24961	Fixed an issue where the firewall, when configured to obtain IP addresses from a DHCP server for GlobalProtect clients, sent a MAC address of '00' to the DHCP server specifically for MacOS 26 (Tahoe) clients running GlobalProtect App versions 6.2 or 6.3, which resulted in IP address collisions on the DHCP server.
GPC-24907	Fixed an issue where the GlobalProtect UI unexpectedly appeared a few minutes after a user logged into Windows, even after portal authentication. This occurred when a second instance of the GlobalProtect app was launched, either by a scheduled task or through the Windows Run registry key, causing it to signal the first app instance to display the main UI.
GPC-24897	Fixed an issue where the GlobalProtect Connect Before Logon tunnel disconnected for new users on their first logon. This issue affected GP client versions 6.2.8-hx and 6.3.3-hx.
GPC-24892	Fixed an issue where the GlobalProtect Portal welcome page, when displayed in German, incorrectly presented a button labeled 'Genau' instead of 'Zustimmen' (Accept).
GPC-24880	Fixed an issue where GlobalProtect clients, after upgrading to versions 6.2.8-263, 6.3.3-h2, or 6.3.3-h3, would get stuck in a connecting loop and fail to connect to the portal or gateways. This occurred because the GlobalProtect app crashed when attempting to delete previous SAML user data, specifically when the user data folder path contained non-ANSI characters that the app could not convert to a UTF-16 path.
GPC-24842	(macOS only) GlobalProtect crashed when you clicked **Change Portal** on setups that included two or more portal entries and had a preferred gateway marked.

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
GPC-24835	Fixed an issue where split tunneling domain exclusions on GlobalProtect App version 6.3.3-C711 for Windows clients failed to function as expected after the application disconnected and reconnected. This resulted in traffic for domains configured for exclusion being incorrectly routed through the VPN tunnel instead of directly, because the TTLMap for split tunneling domain rules was not properly cleared when the GlobalProtect App re-established its connection.
GPC-24515	Fixed an issue where GlobalProtect clients on macOS devices, specifically version 6.3.3-h2, were unable to resolve internal IPv6 domains when split tunneling was enabled and the operating system lacked native IPv6 connectivity. This occurred because the client's logic, which was designed to apply IPv6 configuration only when the OS already had native IPv6 connectivity, prevented the GlobalProtect tunnel from properly handling IPv6 traffic, resulting in "Err name not resolved" errors for internal FQDNs.
GPC-24242	Fixed an issue where GlobalProtect portal authentication failed for some macOS users when attempting to use saved credentials. This issue, observed on GlobalProtect client versions 6.2.8 and 6.3.3, resulted in an immediate authentication failure on the client and firewall logs indicating an invalid username or password, even though the credentials were valid for other macOS clients.
GPC-24216	Fixed an issue where the Host Information Profile (HIP) banner was not displayed on Windows 11 client machines running GlobalProtect client versions 6.2.8-h7 and 6.3.3. This occurred due to a timing or race condition where the GlobalProtect client (PanGPA) received an outdated status, preventing the visual display of HIP match or not-match notifications, even though the messages were recorded in the client logs.
GPC-24144	Fixed an issue where, after a client machine regained internet access, Network Discovery was skipped due to the fed-mandate-accept setting, preventing automatic reconnection to the Prisma Access gateway. This occurred when the device switched from a non-internet-accessible Ethernet connection to a 5G connection.
GPC-24083	Fixed an issue where GlobalProtect clients intermittently failed RADIUS authentication due to treating the portal challenge response as a gateway challenge response. This resulted in incorrect handling of the OTP response back to the server.
GPC-23963	Fixed an issue where GlobalProtect Client version 6.2.8 running in Windows 365 environments, would experience PanGPA getting stuck during the tunnel rename process. This prevented successful gateway

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	authentication and registration after users closed and re-opened their Windows 365 session, leading to a pop-up message prompting users to re-authenticate.
GPC-23960	Fixed an issue where the GlobalProtect agent on macOS devices entered a connecting loop when attempting to connect to an IPv6 gateway due to a missing gateway preservation in the original script. This resulted in the tunnel interface capturing the route to the gateway and an infinite retry loop.
GPC-23909	Fixed an issue where AAAA DNS records were not working when connected to GlobalProtect client versions 6.2.8-c243 or 6.2.8-c263, preventing successful IPv6 connections. This issue occurred when split tunnel is not configured, causing the IPv6 DNS settings to be incorrectly set.
GPC-23787	Fixed an issue where GlobalProtect clients on macOS devices, after upgrading to version 6.2.8-h2, were unable to connect to the authentication server. This occurred because incorrect logic in the GlobalProtect Agent code prevented the Webview Process ID from syncing with the Network Extension process, causing the Network Extension to block SAML authentication traffic, resulting in a "Could not connect to the authentication server" error and a blank embedded browser during SAML authentication.
GPC-23723	Fixed an issue where GlobalProtect clients running version 6.2.8-h1 (6.2.8-c223) experienced intermittent connection failures and disconnections, with the client agent getting stuck in a 'connecting' state even when backend logs indicated a successful connection. This occurred because, when conditional connect mode was enabled, the client attempted to impersonate a user and write On-Demand settings to the user's registry hive (HKEY_CURRENT_USER) during pre-logon. As no user was logged in at that stage, user impersonation failed, leading to incorrect registry access or failed registry operations, which caused service instability or misconfiguration.
GPC-22424	Fixed an issue where, on Windows endpoints running GlobalProtect, roaming user profile data was not written or sent to the server shared folder over SMB (TCP/445) during user logoff or system reboot when the GlobalProtect client was connected to the internal corporate network.
GPC-18976	Fixed an issue where GlobalProtect client 6.1.1-5 would select the incorrect Windows tile by default after locking the screen when using Single Sign-On for Smart Card PIN (Windows) with the Yubikey Smart Card Minidriver. When multiple smart cards were present,

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	GlobalProtect incorrectly selected the last enumerated card instead of the currently active one.

 ©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.8-h6 (6.2.8-c431) Windows and macOS Addressed Issues

The following table lists the issues that are addressed in GlobalProtect app 6.2.8-h6 Windows and macOS.

Issue ID	Description
GPC-24859	Fixed an issue where the GlobalProtect HIP check did not detect the Kaspersky signature information which caused the device to fail the HIP check.
GPC-24827	Fixed an issue where, on GlobalProtect client version 6.2.8-h3, HIP checks for CrowdStrike Falcon or Microsoft/Windows Defender intermittently took longer than expected to complete, sometimes exceeding the default 20-second limit. This resulted in partial HIP reports being sent to the gateway, causing connectivity issues for users accessing internal resources or the internet.
GPC-24683	Fixed an issue where Host Information Profile (HIP) matching failed for Anti-Malware criteria on macOS endpoints due to GlobalProtect failing to detect the virus definition version for Kaspersky Anti-Virus.
GPC-23090	Fixed an issue where the GlobalProtect app experienced connectivity issues after the host computer resumed from sleep mode due to a missing self-pointed route. This issue resulted in a delay of 5 to 10 minutes for the GlobalProtect connection to get stabilized.

 ©2026 Palo Alto Networks, Inc.

GlobalProtect 6.2.8-h5 (6.2.8-c416) Windows and macOS Addressed issues

The following table lists the issues that are addressed in GlobalProtect app 6.2.8-h5 (6.2.8-c416) Windows and macOS.

Issue ID	Description
GPC-24581	Fixed an issue where GlobalProtect disable agent messages were not reported to firewall when machine certificate authentication with full chain certificate validation was enabled.
GPC-24332	Fixed an issue where users on trusted networks were incorrectly receiving a captive portal detection message and being redirected to a separate browser tab. This occurred because the GlobalProtect app was not properly handling captive portal detection response.
GPC-24330	Fixed an issue where GlobalProtect app got stuck in a connecting state when using GlobalProtect version 6.2.8-h4. The issue was seen when saml-logout and enforcer was enabled.
GPC-24261	Fixed an issue where GlobalProtect app running on macOS Sequoia 15.6.1 running GP 6.2.8 -c263 that receive both IPv4 and IPv6 addresses were not receiving packets back from the Network Load Balancer (NLB) instances.
GPC-24221	Fixed an issue where the GlobalProtect app experienced a continuous connect-disconnect loop when used on flights. This issue occurred because rapid network wake-ups left network interfaces in an inconsistent state, causing GlobalProtect to attempt tunnel establishment on an unstable network foundation.
GPC-24103	Fixed an issue where the GlobalProtect app running on macOS allowed users to modify or add a new portal address after each device reboot, even when the **Allow users to change portal** setting was configured as **No** in the GlobalProtect app.
GPC-24048	Fixed an issue where GlobalProtect apps installed on on Dell Vostro 15 3515 laptops were unable

©2026 Palo Alto Networks, Inc.

Issue ID	Description
	to connect to the GlobalProtect service with the following error: **Could not connect to the GlobalProtect service. If the issue persists, contact your administrator**.
GPC-24037	Fixed an issue where GlobalProtect app prompted users to log in with SAML through the embedded browser even when the GlobalProtect app was already connected. This occurred when users logged off and then back onto their Cloud PC (Windows Azure PC), and closing the prompt disconnected and reconnected the VPN session.
GPC-24036	Fixed an issue where the HIP check did not correctly detect the status of the ESET firewall on Windows hosts.
GPC-23990	Fixed an issue where the captive portal opened in the embedded browser, but when the user tried to connect to the internet, it redirected to the default browser and was blocked.
GPC-23929	Fixed an issue where, when GlobalProtect app was configured with Enforcer, users could bypass Enforcer restrictions by repeatedly canceling authentication prompts after logging into Windows. This occurred because the cached portal configuration, which contains Enforcer settings, was not loaded when a pre-logon tunnel failed to establish due to a quick user login. This fix ensures that the cached portal configuration is loaded as soon as PanGPA starts and PanGPS learns the username, preventing unrestricted access in scenarios where Enforcer is intended to lockdown the endpoint.
GPC-23730	Fixed an issue where IPv6 traffic on Windows 11 24H2 did not work as expected with GlobalProtect app.
GPC-23689	Fixed an issue where the GlobalProtect app running on macOS devices would stuck in a connecting loop indefinitely if the user did not complete authentication, requiring manual cancellation of the connection.

©2026 Palo Alto Networks, Inc.

Issue ID	Description
GPC-23650	Fixed an issue where the GlobalProtect enforcer blocked network traffic on Windows endpoints even after the tunnel was successfully connected.
GPC-23525	Fixed an issue where on macOS Ventura and Sequoia, GlobalProtect app versions 6.2.6-838, 6.2.7-1047, 6.2.8, and 6.3.3, manually changing the portal address using the GlobalProtect app UI would fail and revert back to the last connected portal. This issue occurred even when **Allow User to Change Portal Address** was enabled in the agent configuration.
GPC-23394	Fixed an issue where GlobalProtect app version 6.2.8-183. running on macOS 15.5 was unable to accurately report the disk encryption status of FileVault, resulting in an `Unknown` status in HIP checks.
GPC-23336	Fixed an issue where agent disable logs were not being logged to Gateway System Logs on the firewall. The GlobalProtect agent reset the authentication code, which falsely indicated that the gateway was not fully authenticated, and the agent did not send the message.
GPC-22683	Fixed an issue where tool tips were not available for the **Add**, **Edit**, and **Delete** buttons on the GlobalProtect application's settings page on Windows devices.
GPC-22572	Fixed an issue where the hamburger menu button was disabled in the Refresh connection screen, which made it inaccessible when using a keyboard.
GPC-22021	Fixed an issue where, when using conditional-connect on macOS Sequoia with GlobalProtect app version 6.2.6, manually switching gateways caused the app to display a `Not Connected` status for approximately 10 seconds while establishing a connection to the second gateway.
GPC-22010	Fixed an issue where loopback connection did not work when Endpoint Traffic Policy Enforcement was enabled.

 ©2026 Palo Alto Networks, Inc.

GlobalProtect 6.2.8-h4 (6.2.8-c317) Windows and macOS Addressed issues

The following table lists the issues that are addressed in GlobalProtect app 6.2.8-h4 (6.2.8-c317) Windows and macOS.

Issue ID	Description
GPC-23839	Fixed an issue that caused the GlobalProtect 6.3.3 HIP report to fail with the error Method: **WAAPI_MID_GET_AGENT_STATE**.
GPC-23786	Fixed an issue where the `agent-msg` log (**Panorama** > **Monitor** > **GlobalProtect**) was not generated when a user disabled the GlobalProtect app and logged out of the gateway.
GPC-23760	GlobalProtect app version 6.3.3 using SAML with the embedded browser loses cursor focus in the password field, requiring users to click in the password field before entering their password.
GPC-23752	Fixed an issue where the GlobalProtect app failed to authenticate to the portal and gateway after a machine certificate was renewed by Intune MDM. A reboot was required to restore the connection.
GPC-23746	Fixed an issue where the GlobalProtect HIP check incorrectly detected status for Symantec Endpoint Protection, which caused the device to fail the HIP check.
GPC-23646	Fixed an issue where the GlobalProtect app ignores the new gateway-generated authentication override cookie and continues to use the old, expired portal cookie when using the cached portal configuration. As a result, the authentication override cookie generated by a successful SAML authentication to a gateway is replaced by the old, expired portal cookie during successive authentications, causing the gateway to prompt for SAML authentication repeatedly.
GPC-23616	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS, the following error **TransparentProxy:**

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	openWithLocalEndpoint failed occurred in `PanNExt.log` when using an IPv6 address.
GPC-23583	Fixed an issue where the pre-login tunnel rename timeout notification would overlay other system tray icons, preventing users from accessing them
GPC-23558	Fixed an issue where GlobalProtect clients using SAML with Ping Federate did not save the SAML token upon reboot or restart of the pangps service, requiring users to re-authenticate even when the token was not expired. This issue affected GlobalProtect app version 6.3.3 when SAML authentication was configured in Prisma Access and not in Cloud Identity Engine.
GPC-23519	Fixed an issue where GlobalProtect HIP reports on MacBooks intermittently failed with an **Invalid client IP** error, preventing users from accessing resources over the GlobalProtect tunnel. This issue occurred after a system network change when GlobalProtect attempted to send the HIP report to an external gateway while the tunnel was disconnected. This issue affected MacBooks running GlobalProtect version 6.2.5.
GPC-23514	Fixed an issue where, when using a screen reader on Windows or macOS, the GlobalProtect app's **Settings** button did not announce the available options for the end users.
GPC-23488	Fixed an issue where the HIP report intermittently detected MacOS XProtect Real Time Protection status as disabled.
GPC-23468	Fixed an issue where the GlobalProtect HIP check failed to detect the correct version of Forticlient Antivirus, which caused the device to fail the HIP check.
GPC-23441	Fixed an issue where the GlobalProtect installation failed after a transparent upgrade automatically uninstalled the previous version.
GPC-23428	Fixed an issue where the username and password fields in the GlobalProtect app had incorrect labels.

©2026 Palo Alto Networks, Inc.

Issue ID	Description
GPC-23417	Fixed an issue where SAML authentication with Azure AD, using Cisco Duo EAM, failed after upgrading to GlobalProtect version 6.2.8
GPC-23404	Fixed an issue where the Host Information Profile (HIP) check was unable to accurately identify key details from third-party security products.
GPC-23403	Fixed an issue where the GlobalProtect HIP report failed to detect the status of SentinelOne, causing the device to fail the HIP check
GPC-23361	Fixed an issue where the GlobalProtect HIP report did not detect the Status for Zoho corporation - ManageEngine Patch Manager Plus Agent, which caused the device to fail the HIP check.
GPC-23283	Fixed an issue where GlobalProtect was unable to set [exclude/include] 0.0.0.0/netmask routes on Mac endpoint.
GPC-23142	Fixed an issue where an Explicit Proxy token refresh would fail with the message EP TOKEN configuration is NULL, causing the GlobalProtect app to get stuck in a `Connecting` state.
GPC-23095	Fixed and issue where the GlobalProtect HIP report failed to detect the Symantec DLP software, which caused the device to fail the HIP check.
GPC-22353	Fixed an issue where a comment was not visible in the GlobalProtect logs when GlobalProtect was disabled with-comment.
GPC-21745	Fixed an issue where the GlobalProtect HIP check failed to detect Workspace ONE status, which caused the device to fail the HIP check.
GPC-20617	Fixed an issue where a notification appeared on the GlobalProtect app every 10 seconds asking the end-user to re-authenticate. This notification appeared during the pre-logon tunnel rename timeout period.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.9 Linux Addressed Issues

The GlobalProtect 6.2.9 Linux release does not include any bug fixes.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.8-h3 (6.2.8-c263) Windows and macOS Addressed Issues

The following table lists the addressed issues in GlobalProtect app 6.2.8-h3 (6-2-8-c263) Windows and macOS .

Issue ID	Description
GPC-23604	Fixed an issue where GlobalProtect users were not automatically prompted for authentication on public Wi-Fi networks with a captive portal.
GPC-23520	Fixed an issue where new GlobalProtect users were unable to connect to the GlobalProtect app. The app got stuck in **Connecting** stage and stopped working when redirected to the embedded browser.
GPC-23496	Fixed an issue where the GlobalProtect app's **Connect** button did not work as expected preventing users from connecting or changing gateways.
GPC-23440	Fixed an issue where Okta FastPass authentication did not work with GlobalProtect 6.3.3 on macOS 15.5 Sequoia, where the Okta Verify app did not open for the additional authentication prompt.
GPC-23466	Fixed an issue where, when the GlobalProtect app was installed on devices running Windows OS and macOS, the Captive Portal detection message briefly appeared and disappeared when the Captive Portal exception timeout was set to 0.
GPC-23432	Fixed an issue where the GlobalProtect app version 6.3.3 intermittently got stuck on the **finding best gateway** status
GPC-23365	Fixed an issue where, when the GlobalProtect app was installed on Windows machines, the app intermittently disconnected and then reconnected with the error message **Failed to create exclude route**.
GPC-23301	Fixed an issue where, when the GlobalProtect app 6.2.7 and later, was installed on Windows 10 devices, the app deleted the predefined

©2026 Palo Alto Networks, Inc.

Issue ID	Description
	proxy PAC file configuration whenever the app got disconnected regardless of whether the disconnection was initiated manually or occurred automatically due to a timeout.
GPC-23263	Fixed an issue where after upgrading to GlobalProtect app version 6.3.3, the app did not save the username in the embedded browser when "**Save Username** was enabled.
GPC-23218	Fixed an issue where, when using the GlobalProtect app with an embedded browser, interrupting or canceling the SAML authentication prompt terminated the pre-logon tunnel, potentially allowing full internet access even when enforcer was enabled for the user-logon profile. With default browser, the pre-logon tunnel remained active when the SAML authentication prompt was interrupted.
GPC-23125	Fixed an issue where GlobalProtect did not remove older versions of the WebView2 component from the `%LOCALAPPDATA%\Palo Alto Networks \GlobalProtect\GPAEdge` directory, which led to unnecessary disk space consumption over time.
GPC-22989	Fixed an issue where the GlobalProtect app intermittently stopped sending HIP reports while connected to the gateway.
GPC-22979	Fixed an issue where, after upgrading to GlobalProtect app version 6.2.6, the PanGPA application got stuck in **Connecting** 'state and then got terminated unexpectedly.
GPC-22541	Fixed an issue on Windows 11 where the GlobalProtect app (PanGPA) would stop working when the device was locked. The crash occurred when an expired authentication triggered a persistent smartcard login dialog during sleep, leading to excessive memory swapping and a crypt32.dll failure.

 ©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.8 Linux Addressed Issues

The following table lists the addressed issues in GlobalProtect app 6.2.8 Linux.

Issue ID	Description
GPC-23405	Fixed an issue where GlobalProtect version 6.2.7 on Fedora 41 was unable to identify the installed antivirus software, preventing users from connecting to the VPN.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.8-h2 (6.2.8-c243) Windows and macOS Addressed Issues

The following table lists the addressed issues in GlobalProtect app 6.2.8-h2 (6.2.8-c243) Windows and macOS.

Issue ID	Description
GPC-23294	Fixed an issue where GlobalProtect app intermittently disconnected on macOS endpoints even with a stable network connection. This was due to a timeout that was too short for the route system command.
GPC-23270	Fixed an issue where GlobalProtect app version 6.3.3 using SAML with the embedded browser would lose cursor focus in the password field, requiring users to click in the password field before entering their password.
GPC-23191	Fixed an issue where GlobalProtect took almost 2 minutes to reconnect to an already connected gateway after a host reboot.
GPC-23115	Fixed an issue where the hardware token authentication option was intermittently unavailable while using the embedded GlobalProtect browser on Windows machines.
GPC-23044	Fixed an issue where, when a machine was in Modern standby, the GlobalProtect app repeatedly attempted to connect to gateways, even when authentication failed due to SAML timeout. This resulted in GlobalProtect connecting to non-optimal gateway
GPC-22763	Fixed an issue where GlobalProtect prompted for credentials instead of using authoverride cookie when authenticating to the best available gateway.
GPC-22522	Fixed an issue where, after upgrading from GlobalProtect app version 6.1.2 to 6.2.6, external users on Windows 11 computers with multiple Azure Entra accounts were unable to authenticate to the portal using

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	SAML with Azure Entra as the Identity Provider (IdP). The new WebView2 embedded browser automatically used the user's default Windows credential for Single Sign-On (SSO), preventing them from selecting the correct account for authentication.To resolve this issue a new registry key 'entra-sso' has been introduced. You can add the registry key using two methods and set it to no to disable SSO. • For pre-deployment, use **msiexec.exe /i globalprotect64.msi ENTRASSO="no"** • Add key **entra-sso** and set it to **no**under **HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings**. If the **entra-sso** key does not exist under the above path, the GlobalProtect app's default behavior is to **Allow** Entra SSO.
GPC-22066	Fixed an issue where the HIP check detected an incorrect real-time protection status for Windows Defender ATP and CrowdStrike Falcon anti-malware software, which could incorrectly mark non-compliant devices as compliant.
GPC-22029	Fixed an issue where Apple software downloads took longer to complete when using GlobalProtect with split tunneling enabled.

 ©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.7 Linux Addressed Issues

The following table lists the addressed issues in GlobalProtect app 6.2.7 Linux.

Issue ID	Description
GPC-23208	Fixed an issue where traffic was going through via physical interface instead of the tunnel even though GlobalProtect was connected.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.8-c223 Windows and macOS Addressed Issues

The following table lists the addressed issues in GlobalProtect app 6.2.8-c223 Windows and macOS.

Issue ID	Description
GPC-23215	Fixed an issue where, the traffic stopped passing through the GlobalProtect app on macOS devices after upgrading to GP 6.2.8 and when the computer screen was locked.
GPC-23174	Fixed an issue where the GlobalProtect failed to detect DNS during the Network Detection stage, causing the GlobalProtect app to stop working.
GPC-23161	Fixed an issue where the GlobalProtect app stopped working after a session change.
GPC-23088	Fixed an issue where the portal login user authentication failed after cookie expiration.
GPC-21982	Fixed an issue in which IPv6 traffic bypassed the valid route in the rerouting table and instead passed through the physical adapter when the GlobalProtect app was installed on Windows devices.
GPC-23046	Fixed an issue where users experienced connectivity problems when GlobalProtect was used in a WiFi network with captive portal.
GPC-23034	Fixed an issue where the GlobalProtect embedded browser did not display certificate selection pop-up when there were multiple client certificates available.
GPC-23032	Fixed an issue where the GlobalProtect agent restarts when the device wakes up from Modern Standby.
GPC-23011	Fixed an issue wherein wherein the Enforcer intermittently failed to promptly block network access as configured, thereby

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	resulting in delays of 1 to 5 minutes before eventually blocking the traffic flow.
GPC-22800	Fixed an issue where, when the GlobalProtect app was configured with enforcer and Captive Portal, users faced issues in connecting to Captive Portal using GlobalProtect.
GPC-22610	Fixed an issue where, after an upgrade, GlobalProtect restarted and failed to connect to the portal
GPC-22595	Fixed an issue where users were unable to select the correct client certificate when using the GlobalProtect app on Windows devices and connected to the internal network using SAML embedded browse
GPC-22536	Fixed an issue where users faced connectivity issues when the GlobalProtect app version 6.2.6 was installed on devices running macOS 15.3.1
GPC-22365	Fixed an issue where users experienced intermittent issues browsing webpages while connected to the GlobalProtect app.
GPC-22294	. Fixed an issue where intermittent internet access problems occurred when the macOS was upgraded to 15.2 and the GlobalProtect app version to 6.2.6.
GPC-21766	Fixed an issue where the split tunnel excluded routes go missing from routing table on Windows machine at intermittent times.
GPC-21755	Fixed an issue where GlobalProtect users with enforcer enabled were able to access applications that were not in the enforcer exception list.
GPC-21737	Fixed an issue where the SAML redirection page opened up on end user computers even though they did not have internet connectivity.

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
GPC-19024	Fixed an issue where the GlobalProtect app incorrectly used an embedded WebView instead of the system default browser for Captive Portal logins.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.6 Linux Addressed Issues

The following table lists the issues that are addressed in GlobalProtect app 6.2.6 for Linux.

Issue ID	Description
GPC-22950	Fixed an intermittent issue on Linux machines that affected users' ability to perform Web searches on browsers while connected to the GlobalProtect app.
GPC-22872	Fixed an issue while installing the GlobalProtect app version 6.2.1.1-7 on Fedora 41 x86_64 Linux machines by executing gp_install.sh script on command line interface did not work as expected.
GPC-22774	Fixed an issue where GlobalProtect app 6.2.1-7 was installed on Linux Fedora machines, the import certificate failed due to missing /etc/ssl/private/ directory.
GPC-22766	Fixed an issue where, when the GlobalProtect app was installed on Linux machines, hyperlink in the welcome page opened in the embedded browser instead of default browser.
GPC-22390	Fixed an issue where the GlobalProtect app version 6.2.1 did not fetch the portal address from pre-deployed pangps.xml.
GPC-22306	Fixed an issue where the GlobalProtect app tray icon failed to display when the app was installed on devices running Linux Ubuntu 24.04.1 LTS.
GPC-22249	Fixed an issue where some of the third party license files were missing in the GlobalProtect app packages.
GPC-22130	Fixed an issue where the GlobalProtect app displayed the following incorrect error message when there was no internet connectivity: **Could not verify the server of the gateway. If the issue persists, contact your administrator.**

©2026 Palo Alto Networks, Inc.

Issue ID	Description
GPC-22051	Fixed an issue where the GlobalProtect app displayed the following unexpected client certificate error message during portal logon: **Valid client certificate required for authentication**, when **Allow Authentication with User Credentials OR Client Certificate** option was set to **Yes**.
GPC-21951	Fixed an issue where, when the GlobalProtect app was installed on Linux machines, the virtual adapter maintained tunnel IP even when the app was disconnected.
GPC-21920	Fixed an issue where the GlobalProtect app web interface did not display some settings such as portal address when the user manually disconnected the app and then restarted.
GPC-21915	Fixed an issue where, when the GlobalProtect app was installed on Linux Ubuntu LTE 20.04 machines, the GlobalProtect app did not properly display the connection status and the app was incorrectly positioned in the middle of the screen.
GPC-21861	Fixed an issue where, when the GlobalProtect app was installed on Linux devices (Ubuntu 22.04.4 LTS), the tunnel got disconnected intermittently causing connectivity issues.
GPC-21762	Fixed an issue where, when the GlobalProtect app is installed on Linux RHEL 8.9, PanGPA process stopped and failed to recover automatically impacting the functioning of the GlobalProtect app.
GPC-21724	Fixed an issue where the IoT GlobalProtect app connection failed after system reboot with error: **cannot connect to local gpd service**.
GPC-21651	Fixed an issue where, when the GlobalProtect app is installed on Linux RHEL 8.9,the app did not remove the configured DNS even after disabling the app.

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
GPC-21092	Fixed an issue on Linux machines where users were unable to authenticate to the GlobalProtect app using certificate authentication. Despite the certificate being sent to the firewall, the app was defaulting to SAML authentication method.
GPC-21478	Fixed an issue where, when the GlobalProtect app version 6.2.0-265 was installed on Linux machines running Ubuntu 24.04.1 LTS, the app got stuck and users were unable to connect to the app after system reboot.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.8 Windows and macOS Addressed Issues

The following table lists the addressed issues in GlobalProtect app 6.2.8 Windows and macOS.

Issue ID	Description
GPC-22894	Fixed an issue where GlobapProtect did not detect the correct version of Kaspersky Endpoint Security.
GPC-22847	Fixed an issue where GlobalProtect did not detect Qualys for patch management.
GPC-22764	Fixed an issue where wa_3rd_party_host_xx.exe attempted to connect to Microsoft's update servers for information and the patch information was not sent in the HIP report. This occured even though HIP Exceptions for patch management were configured to exclude Windows updates agent.
GPC-22740	Fixed an issue where macOS computers displayed both the new and old versions of the GlobalProtect welcome page.
GPC-22688	Fixed an issue for proxy-only mode where customers were unable to access websites when the computer woke up from sleep.
GPC-22638	Fixed an issue where Global Protect HIP did not detect the drive state when using Trellix Drive Encryption 8.0.
GPC-22620	Fixed an issue where GlobalProtect was not working correctly and blocked internet access.
GPC-22589	Fixed an issue where the Report an Issue functionality did not send the troubleshooting log to the administrator's Strata Logging Service instance.
GPC-22544	Fixed an issue where the GlobalProtect client did not send the HIP report causing user-IP

©2026 Palo Alto Networks, Inc.

Issue ID	Description
	mapping to be cleared and resulting in traffic drop.
GPC-22542	Fixed an issue where the embedded browser shown as part of SAML authentication was blank.
GPC-22487	Fixed an issue where Norton 360 was not compatible with GlobalProtect causing the device to fail the HIP check.
GPC-22443	Fixed an issue where the GlobalProtect agent showed as connected even when the virtual adapter was down.
GPC-22437	Fixed an issue where the GlobalProtect macOS client experienced a keep-alive timeout, preventing the tunnel from connecting.
GPC-22412	Fixed an error where virtual adapter is not set correctly during tunnel creation.
GPC-22297	Fixed an issue where the Customer was getting "A valid client certificate is required for authentication" even though they had a valid client certificate installed. In order to access the fix, you must do one of the following: • uninstall the previous release (to remove all registry entries). • manually delete the registry value "ext-key-usage-oid-for-client-cert" under "HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings" as it may contain a corrupted value.
GPC-22264	Fixed an issue where the GlobalProtect HIP report did not detect the last full scan time for Avast antivirus software.
GPC-22245	Fixed an issue where transparent upgrade from GlobalProtect version 6.2.4 or 6.2.5 to version 6.2.6 failed on some Windows endpoints with error 1618.

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
GPC-22237	Fixed an issue where GlobalProtect shut down unexpectedly on Windows 11 devices running multiple versions of GlobalProtect 6.3. The issue was caused by the firewall sending invalid IPv6 packets to GlobalProtect, which did not have a validation method before processing.
GPC-22235	Fixed an issue where users were unable to connect to the app after the system woke up from sleep mode.
GPC-22233	Fixed an issue where the users were unable to connect the GlobalProtect app after performing the resolution of CVE-2024-5921. The app displayed the following error, “The certificate CN name mismatch.”
GPC-22126	Fixed an issue where GlobalProtect version 6.2.6-838 was stuck intermittently during the connection process.
GPC-22123	Fixed an issue where the GlobalProtect app got stuck and users faced connection issues after the system woke up from sleep mode even though the internet connection was stable.
GPC-22092	Fixed an issue where the GlobalProtect app failed to validate the server certificate when the portal or gateway sent only the leaf certificate.
GPC-22061	Fixed an issue where the GlobalProtect client displayed an error when using an ECDSA certificate with explicit EC parameters in FIPS mode.
GPC-22043	Fixed an issue where Okta push notification shows incorrect Windows OS, when Okta SAML authentication is enabled in GlobalProtect.
GPC-22036	Resolved an issue where GlobalProtect did not populate the internal routes in the user's routing table.

©2026 Palo Alto Networks, Inc.

Issue ID	Description
GPC-22028	Fixed an issue where the disconnect reason for macOS users was getting cached.
GPC-21988	Fixed an issue where the GlobalProtect Client displayed a download prompt or was updated even with an "upgrade disallow" configuration.
GPC-21979	Fixed an issue where the included domain traffic was routed through the physical interface when split tunnel was configured.
GPC-21961	Fixed an issue where, after upgrading to GlobalProtect version 6.2.5, the app triggered authentication and opened multiple browser tabs when the computer woke from sleep.
GPC-21960	Fixed an issue where the HIP check failed to detect the Norton anti-malware version 24.11.9615.0.
GPC-21955	Fixed an issue where the HIP notification pop-up on macOS looked different from that on Windows.
GPC-21938	Fixed an issue where, when the GlobalProtect app version 6.3.x was installed on devices running macOS, the HIP check failed to detect ESET Endpoint Security version 8.
GPC-21918	Fixed an issue where, when the patch management category was excluded for HIP checks, HIP checks were still happening for missing patches which consumed CPU resources on users' machine.
GPC-21938	Fixed an issue where, when the GlobalProtect app version 6.3.x was installed on devices running macOS, the HIP check failed to detect ESET Endpoint Security version 8.
GPC-21775	Fixed an issue where GlobalProtect users on macOS were disconnected immediately after sending the HIP report.
GPC-21771	Fixed an issue where the GlobalProtect HIP check incorrectly detected Malware

©2026 Palo Alto Networks, Inc.

Issue ID	Description
	Definition Date for Trend Micro Deep Security Agent, which caused the device to fail the HIP check.
GPC-21743	Fixed an issue where a user was randomly prompted with a \"Login Successful\" message when connecting to GlobalProtect (GP), even though GP was not connected.
GPC-21695	Fixed an issue where the GlobalProtect embedded browser could not utilize a new PIV certificate for SAML authentication if multiple certificates were available.
GPC-21677	Fixed an issue where GlobalProtect configured for Always-on Pre-logon may not display the captive portal page if there is a delay with network access or Internet connectivity.
GPC-21653	Fixed an issue where the GlobalProtect virtual adapter was not set up correctly.
GPC-21639	Fixed an issue where the GlobalProtect macOS client did not extend the session even though the user clicked the Extend Session button.
GPC-21627	Fixed an issue where the Report an Issue feature failed to work for a specific user whose username contained Japanese character.
GPC-21615	Fixed an issue where the GlobalProtect agent (wa_3rd_party_host_64.exe) modified the __PSLockDownPolicy registry key from 4 (secure language mode) to 0 (full language mode) after a reboot.
GPC-21571	Fixed an issue where the hyperlink in HIP notification opened up in Webview2 instead of the default browser.
GPC-21565	Fixed an issue where the SAML embedded browser did not remember the username after sign-out, even when the user had selected

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	the check box “Remember Me" on the SAML embedded browser,
GPC-21527	Fixed an issue where the firewall did not exclude the APIPA (169.254.0.0/16) range from GlobalProtect when the Endpoint Traffic Policy Enforcement feature was enabled with the exclude option. As a result, traffic to the APIPA range was sent over GlobalProtect instead of the local interface.
GPC-21467	Fixed an issue where the Transparent Upgrade with Proxy only mode did not work as expected and no tunnel was established with the gateway.
GPC-21453	Fixed an issue where the GlobalProtect app window displayed "static" instead of the connected gateway name.
GPC-21222	Fixed an issue where the GlobalProtect HIP check incorrectly detected the Real Time Protection Status and Last Full Scan for Avast application, which caused the device to fail the HIP check.
GPC-21090	Fixed an issue where GlobalProtect only displayed ADEM information for approximately 120 users even though more than 600 ADEM users were connected to GlobalProtect.
GPC-20967	Fixed an issue where, when the GlobalProtect app was installed with the Conditional Connect method, users had to click the Connect button twice to connect to an external gateway after a system reboot.
GPC-20632	Fixed an issue where GLobalProtect was stuck in connecting mode after the customer manually selected a gateway that hit the maximum user limit. This was a multi-gateway environment with SAML/CAS authentication method.
GPC-20621	Fixed an issue where users from overseas locations were disconnected from

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	GlobalProtect due to the HIP report not being sent with manual gateway selection.
GPC-18587	Fixed an issue where, when the GlobalProtect was installed on Windows devices and Connect Before Logon was deployed, users were unable to log in to the device using the User Principal Name (UPN). This issue occurred when the GlobalProtect credential provider was selected and the device was offline.

 ©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.7 Addressed Issues

Transparent upgrade between two GlobalProtect releases in the same release train is currently not supported. For example, you cannot do a transparent upgrade from GlobalProtect 6.2.6-c700 to 6.2.6-c857. To enable easier transparent upgrades, we have re-packaged 6.2.6-c857 as GlobalProtect 6.2.7. Customers looking to upgrade to 6.2.6-c857 can use 6.2.7.

GlobalProtect 6.2.7 includes no additional bug fixes compared to GlobalProtect 6.2.6-c857.

 ©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.6-c857 Windows and macOS Addressed Issues

Transparent upgrade between two GlobalProtect releases in the same release train is currently not supported. For example, you cannot do a transparent upgrade from GlobalProtect 6.2.6-c700 to 6.2.6-c857. To enable easier transparent upgrades, we have re-packaged 6.2.6-c857 as GlobalProtect 6.2.7. Customers looking to upgrade to 6.2.6-c857 can use 6.2.7.

If you plan to upgrade the GlobalProtect app on your Windows endpoints to 6.2.6-c857, review the GlobalProtect upgrade best practices.

The following table lists the issues that are addressed in GlobalProtect app 6.2.6-c857 hotfix for Windows and macOS.

Issue ID	Description
GPC-22107	Fixed an issue where the GlobalProtect agent was unable to validate the server certificate after the CVE-2024-5921 remediation was applied.
GPC-22104	Fixed an issue where the GlobalProtect HIP report failed to detect the Seqrite Endpoint Protection application, when the application was upgraded to a higher version 18.00 (14.0.0.1)
GPC-22082	Fixed an issue where GlobaProtect did not validate certificates with 3rd parties or PKI and displayed a FIPS error.
GPC-22079	Fixed an issue where users were unable to connect to the GlobalProtect app due to Captive Portal connectivity issues.
GPC-22046	Fixed an issue where when the GlobalProtect app was installed on devices running macOS and the app version was upgraded to 6.2.5, end users were unable to connect the app. The app got stuck in the Connecting state and displayed the following message, “You are redirected to an embedded browser to authenticate and connect.”
GPC-22010	Fixed an issue where loopback connection did not work when Endpoint Traffic Policy Enforcement was enabled.

©2026 Palo Alto Networks, Inc.

Issue ID	Description
GPC-21950	Fixed an issue where the GlobalProtect connection on MacOS Sequoia 15+ was unstable.
GPC-21778	Fixed an issue where the GlobalProtect IPSec tunnel got disconnected on GlobalProtect app version 6.2.5 when the `gpupdate /force` command was used to update a policy.
GPC-21284	Fixed an issue where the GlobalProtect gateway did not receive the HIP reports from the user correctly due to which the end users were unable to access the resources even when the sessions were active.
GPC-20592	Fixed an issue where the GlobalProtect app could not establish the tunnel and the app got stuck in the tunnel creation stage. The app displayed the following error, " The virtual adapter was not set up correctly due to a delay."

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.1-c31 Linux Addressed Issues

Where Can I Use This?	What Do I Need?
•	❑

 ©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.6 Windows and macOS Addressed Issues

The following table lists the issues that are addressed in GlobalProtect app 6.2.6 Windows and macOS.

Issue ID	Description
GPC-21774	Fixed an issue where the GlobalProtect ARM64 installers for 6.2.5 version did not display **Digital Signatures** tab.
GPC-21721	Fixed an issue, where the GlobalProtect app got stuck in Connecting status when the device woke up from sleep mode.
GPC-21731	Fixed an issue where the GlobalProtect app is stuck in the `Connecting` status when upgraded to 6.2.5-788 version and the users had to reboot the system to resolve the issue.
GPC-21665	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS and the app was used with Trellix Proxy Agent, the web browser displayed the following error, **ERR_SOCKET_NOT_CONNECTED**.
GPC-21636	Fixed an issue where the users were unable to login Windows 11 using the User Principal Name (UPN) when GPCP was selected with GlobalProtect app version 6.2.4 and **Interactive logon: Don't display last signed-in** was enabled in their Entra ID - group policy.
GPC-21604	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS and were connected to the internal gateway, the app did not display the **Disconnect** option under **Settings**.
GPC-21413	Fixed an issue where the GlobalProtect Credential Provider did not reset focus on the password field when the user entered the wrong password.

©2026 Palo Alto Networks, Inc.

Issue ID	Description
GPC-21375	Fixed an issue where the Windows SSO did not work when the SAML authentication method was used to authenticate to the app. The username retrieved from SAML was not matching configuration selection criteria causing authentication issues.
GPC-21332	Fixed an issue where the GlobalProtect HIP check incorrectly detected Real Time Protection status for Avast and XProtect, which caused the device to fail the HIP check.
GPC-21320	Fixed an issue where the GlobalProtect HIP check did not detect Kaspersky Endpoint Security antimalware application which caused the device to fail the HIP check.
GPC-21281	Fixed an issue where the GlobalProtect app got stuck in the `Connecting` status when the user refreshed the connection.
GPC-21267	Fixed an issue where, when the user installed the GlobalProtectARM installer from the Customer Support Portal (CSP) and the user opened GlobalProtect using the Start menu, the icon file (PanGPA.ico) was opened instead of the executable (PanGPA.exe) file.
GPC-21247	Fixed an issue where GlobalProtect HIP set the Filevault encryption status to unencrypted on macOS running devices, which denied access to the end-point machines.
GPC-21240	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS Sonoma 14.5, the app used the old FQDN names and got stuck in the `Connecting` status instead of prompting the user to enter the portal FQDN name.
GPC-21222	Fixed an issue where the GlobalProtect HIP check incorrectly detected the Real Time Protection Status and Last Full Scan for Avast application, which caused the device to fail the HIP check.

©2026 Palo Alto Networks, Inc.

Issue ID	Description
GPC-21811	Fixed an issue where the PanGPS stopped working soon after the GlobalProtect was installed on the endpoint and the GlobalProtect app got stuck in the `Connecting` stage.
GPC-21174	Fixed an issue where the GlobalProtect HIP check did not detect Real time protection status for Acronis Cyber Protection Agent, which caused the device to fail the HIP check.
GPC-21131	Fixed an issue where the users were unable to access the Advanced Logging Settings screen of the GlobalProtect app using the **ctrl + tab** key combination on the keyboard. The screen reader did not announce the keyboard options correctly.
GPC-21106	Fixed an issue where the GlobalProtect HIP check did not detect 'Real Time Protection' status for Malwarebytes anti-malware application, which caused the device to fail the HIP check.
GPC-20783	Fixed an issue where the password field was not automatically selected for typing when using the embedded browser, requiring users to click inside the field before entering their password
GPC-20779	Fixed an issue where Windows regional settings are not respected by Webview 2 on SAML embedded browser resulting in regional language(French, German, Chinese, Spanish, and Japanese) not loading properly in embedded browser.
GPC-20674	Fixed an issue where all GlobalProtect portals except for the currently connected portal were deleted during the upgrade from 6.2.2 to 6.2.3 or from 6.2.3 to 6.3.0.
GPC-18647	Fixed an issue with GlobalProtect App Log Collection feature where the user reported an issue using **Report an Issue** option on the GlobalProtect app and the issue was not reported as expected.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.5 Windows and macOS Addressed Issues

The following table lists the issues that are addressed in GlobalProtect app 6.2.5 Windows and macOS.

Issue ID	Description
GPC-21656	Fixed an issue where an unexpected extra string was added to the end of the MFA prompt.
GPC-21533	Fixed an issue where GlobalProtect connected and disconnected in a loop
GPC-21483	Fixed an issue where users are intermittently unable to connect to GlobalProtect and get stuck at the connecting stage.
GPC-21465	Fixed an issue where GlobalProtect is stuck in "Connecting... Finding the Best Available Gateway".
GPC-21442	Fixed an issue where there was a delay in GlobalProtect restoring connectivity after the Windows host woke up from modern standby.
GPC-21443	Fixed an issue where GlobalProtect crashed when the PanGPS service was stopped.
GPC-21414	Fixed an issue where GlobalProtect using SAML authentication gets stuck in a connecting loop upon the expiration of the authentication cookie.
GPC-21392	Fixed an issue where GlobalProtect is stuck in the connecting state for 2-3 minutes during Windows Pre-logon.
GPC-21387	Fixed an issue that prevented users from connecting to Wi-Fi networks when GlobalProtect was disconnected.
GPC-21355	Fixed an issue where GlobalProtect was incorrectly showing as connected during Windows pre-logon.

©2026 Palo Alto Networks, Inc.

Issue ID	Description
GPC-21301	Fixed an issue where after upgrading to GlobalProtect 6.2.4, users were unable to connect to GlobalProtect intermittently when Enforcer is enabled.
GPC-21247	Fixed an issue where HIP checks for Disk Encryption status were failing after Windows and Mac hosts were rebooted, on low power mode or were resuming from standby.
GPC-21206	Fixed an issue where GlobalProtect intermittently does not restore connection after the user logs back in or wakes a Windows host.
GPC-21172	Fixed an issue where the GlobalProtect agent gets disconnected right after successful connection when SAML embedded browser authentication is used along with "Enforce GlobalProtect for Network Access".
GPC-21161	Fixed an issue where the notifications prior to 'Login Lifetime Expiration' and 'Notify Before Lifetime Expires' were not displayed even when enabled.
GPC-21101	Fixed an issue where the embedded browser pop-up with "Login Successful" was displayed for each SAML authentication.
GPC-21057	Fixed an issue where HIP checks for Disk Encryption status were failing on Windows during modern standby.
GPC-21035	Fixed an issue where GlobalProtect HIP did not identify the definition version of the SentinelOne Agent.
GPC-21024	Fixed an issue where a HIP notification configured as "pop-up-message" for pre-logon does not show up. The pop up window is blank.
GPC-21005	Fixed an issue where after submitting the SAML credentials, a blank screen was displayed and GlobalProtect got stuck in that stage.

©2026 Palo Alto Networks, Inc.

Issue ID	Description
GPC-20991	Fixed an issue where the 'Extended Key Usage OID' value for certificate selection was deleted during an upgrade of the GlobalProtect agent. This forces users to have to manually select the correct certificate tp be used for authentication.
GPC-20988	Fixed an issue where GlobalProtect failed to resolve DNS queries when the 'Allow traffic to specified FQDN when Enforce GlobalProtect Connection for Network Access is enabled and GlobalProtect Connection is not established' configuration is set.
GPC-20983	Fixed an issue where the GlobalProtect app remains stuck in the connecting stage when Windows computer resumes from sleep.
GPC-20943	Fixed an issue where the GlobalProtect enforcer blocked DHCP packets.
GPC-20895	Fixed an issue where GlobalProtect users on macOS were able to add and modify the portal address even when portal agent configuration was "Allow User to Change Portal Address = NO".
GPC-20884	Fixed an issue where users get disconnected a few seconds after logging in to VDI when GlobalProtect connects. They are unable to reconnect after that.
GPC-20864	Fixed an issue where the GlobalProtect embedded browser login window did not stay pinned to the front of all open windows on Windows and MAC computers.
GPC-20839	Fixed an issue where system extensions on MacBooks were not updated upon GlobalProtect app upgrade.
GPC-20838	Fixed an issue where the HIP report generation was taking longer than the 'Max Wait Time' on Windows devices when anti-malware and disk encryption checks are configured.

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
GPC-20771	Fixed an issue where GlobalProtect 6.2 users on Windows 11(ARM & Intel) devices cannot connect to GlobalProtect due to "The Parameter is incorrect" error.
GPC-20770	Fixed an issue where certain GlobalProtect HIP checks on Windows devices failed when there was no internet connectivity.
GPC-20741	Fixed an issue where the GlobalProtect app intermittently disconnects from the gateway when using the embedded browser for SAML authentication.
GPC-20736	Fixed an issue where users are being logged out from GlobalProtect when the device wakes up from modern standby and network discovery happens.
GPC-20700	Fixed an issue where macOS users had to enter the SAML username and password each time they refreshed or rebooted their computer especially when using Safari or Embedded browser.
GPC-20692	Fixed an issue where GlobalProtect 6.2.3 with SAML authentication (via Okta) opens the embedded browser page in the background instead of the foreground.
GPC-20645	Fixed an issue where GlobalProtect app in macOS is stuck in connecting state when the device wakes up from sleep.
GPC-20626	Fixed an issue where the GlobalProtect client overwrites valid authentication override cookie with empty authentication override cookie from portal when using cached portal configuration.
GPC-20601	Fixed an issue where macOS users are unable to connect to GlobalProtect after upgrading from version 6.2.2 to 6.2.3 via JAMF.
GPC-20595	Fixed an issue where GlobalProtect users were unable to connect after upgrading to 6.2.3-270 and received a "Your internet

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	access is blocked" error during SAML authentication using the embedded browser.
GPC-20550	Fixed an issue where Zoom and Outlook apps intermittently stop connecting on macOS with an error "You are unable to connect to Zoom. Please check your network connection and try again" when the apps are excluded under both domains and applications.
GPC-20466	Fixed an issue where when the tunnel is broken on Windows computers in modern standby mode, the Enforcer does not work even when it is enabled.
GPC-20442	Fixed an issue on appliances running PanOS 10.1.11-h1 and GlobalProtect 6.0.10-811 where the tunnel status failed to update to connected immediately after establishment. This problem was specific to IPv4-only clients connecting to dual-stack (IPv4 + IPv6) GlobalProtect gateways or portals.
GPC-20441	Fixed an issue where HIP reports are sometimes not available on the firewall for newly connected users.
GPC-20416	Fixed an issue where there is no network discovery once the laptop came out of standby.
GPC-20360	Fixed an issue where the GlobalProtect app is stuck in the connecting status after authentication and does not connect until the app is restarted or the computer is rebooted.
GPC-20292	Fixed an issue where RDP to Azure VDI clients disconnects when GlobalProtect is enabled on the VDI client with SAML authentication and with 'Enforce GlobalProtect for Network Access' enabled
GPC-20191	Fixed an issue where PanGPA.exe crashes on Windows clients
GPC-20114	Fixed an issue where GlobalProtect on MacOS was incorrectly selecting client

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	certificates without a private key for certificate authentication.
GPC-20112	Fixed an issue where the GlobalProtect HIP check incorrectly detected Real time protection status for Kaspersky Endpoint Security, which caused the device to fail the HIP check.
GPC-20072	Fixed an issue where domain-based split tunneling was not working on MAC with Edge Chromium or Google Chrome browser though it was working on Safari.
GPC-19819	Fixed an issue where SAML default browser IDP traffic is blocked during a refresh connection when GlobalProtect is connected to the internal network with 'Enforce GlobalProtect for Network Access' enabled.
GPC-19269	Fixed an issue where GlobalProtect would show as "connecting" but never actually connect until the user restarted GlobalProtect on their Windows machine.
GPC-18943	Fixed an issue where GlobalProtect would fail to connect on Windows hosts that were woken up from modern standby by initiating an RDP to the host.

 ©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.4 Windows and macOS Addressed Issues

The following table lists the issues that are addressed in GlobalProtect app 6.2.4 Windows and macOS.

Issue ID	Description
GPC-20741	Fixed an issue where the GlobalProtect app intermittently disconnected from the gateway when the user was using the embedded browser for SAML authentication.
GPC-20640	Fixed an issue where the GP App graphical interface on macOS does not close on pressing the ESC key.
GPC-20585	Fixed an issue where the GlobalProtect app could not connect to the GlobalProtect portal when configured with certificate authentication and SAML authentication using an embedded browser
GPC-20571	Fixed an issue where the Report an Issue option was not visible in the GlobalProtect app version 6.2.3.
GPC-20542	Fixed an issue where, when the GlobalProtect app was installed on Windows devices, the GlobalProtect logs did not display the username correctly.
GPC-20537	Fixed an issue where the Login page got redirected twice and opened two separate tabs for GlobalProtect portal and gateway, when the user tried to connect the GlobalProtect app using the SAML authentication method.
GPC-20531	Fixed an issue where, when the user was using Remote Desktop with GlobalProtect, the RDP sessions got disconnected because the GlobalProtect on RDP station got disconnected with a grace period end message.
GPC-20527	Fixed an issue where the Conditional Connect method configured for the GlobalProtect

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	app did not work as expected when the user shifted from external network (home) to an internal network (office). Users had to reboot the system to resolve this issue.
GPC-20514	Fixed an issue where the remote users using GlobalProtect with Connect Before Logon (CBL) were unable to reset their password when using the app with an embedded browser.
GPC-20455	Fixed an issue where the GlobalProtect app intermittently got stuck on the 'Connecting' status when the computer resumed from sleep and a new authentication was needed or authentication cookies had expired.
GPC-20445	Fixed an issue where the GlobalProtect app got stuck in Connecting state after upgrading from PAN-OS 10.1.11-h5 version to PAN-OS 10.1.13
GPC-20444	Fixed an issue where, when the GlobalProtect app was used with the SAML authentication method, the app displayed two pop-up messages; one with a successful authentication message and the other with an authentication failure message.
GPC-20426	Fixed an issue where a new HIP report was not generated when the user disabled AV on an end-user device.
GPC-20381	Fixed an issue where the Windows defender Real Time Protection state and agent version is incorrectly identified in GlobalProtect app version 6.0.8 and 6.2.3.
GPC-20378	Fixed an issue where the GlobalProtect app was used with the SAML authentication method with the embedded browser, the app got stuck while redirecting to the SAML authentication page.
GPC-20374	Fixed an issue where users were unable to connect to GlobalProtect if they accidentally clicked decline on the Terms of Service page.

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
GPC-20370	Fixed an issue where the Real Time Protection state from SentinelOne was displayed as true even when the app was disabled.
GPC-20366	Fixed an issue where, when the GlobalProtect app was installed on Windows devices and the users tried to authenticate to the app, the screen displayed both authentication success and failed message even when the authentication was successful.
GPC-20320	GlobalProtect unable to authenticate with SAML IdP using embedded browser (webview2) when "Enforce GlobalProtect for Network Access" is enabled
GPC-20279	Fixed an issue where users were presented with suggested user names during SAML authentication after upgrading to GlobalProtect 6.2.3.
GPC-20263	Fixed an issue where the correct label was not associated with the GlobalProtect icon so voice over was unable to read the icon name.
GPC-20262	Fixed an issue where users were unable to select the GlobalProtect icon from the status bar on macOS.
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-20242	Fixed an issue where the GlobalProtect app displayed gibberish text on the app.
GPC-20241	Resolved an issue where the GlobalProtect app did not detect HIP information for HP Wolf Security software.
GPC-20178	Resolved an issue where the Certificate Revocation List was sent to a URI that was not an exact match with the URI in the certificate.

©2026 Palo Alto Networks, Inc.

Issue ID	Description
GPC-20163	Fixed an issue where the GlobalProtect app was unable to connect to the gateway via IPv6.
GPC-20162	Fixed an issue where the GlobalProtect enforcer blocked some DHCPv6 packets on Windows computers.
GPC-20157	Fixed an issue where the gateway location was not correctly displayed in the Connections panel.
GPC-20143	Fixed an issue where the user was redirected to the Authentication page twice on the default browser for both portal and gateway authentication when SAML was configured.
GPC-20091	Fixed an issue where pre-logon failed when the computer was rebooted, when the machine store had an expired and active certificate.
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-20028	Fixed an issue where macOS users, despite having 'Allow User to Change Portal Address' set to No, were able to choose a different portal from the existing list.
GPC-20005	Fixed an issue where, when the GlobalProtect app was installed on Windows devices, users were able to select the manual gateway and

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	connect to the app even when the regional or global fall back gateway was not configured.
GPC-20004	Fixed an issue where both certificates with and without the specified OID were incorrectly being selected as potential machine certificates.
GPC-20003	Fixed an issue where GlobalProtect users with certificates were unable to connect a gateway on version 6.0.9.
GPC-19991	Fixed an issue where client certificate authentication between embedded browser and IdP (SAML) failed.
GPC-19972	Fixed an issue where users were unable to connect to Prisma Access after a break and had to reboot their computer.
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 Alway-On mode.
GPC-19930	Fixed an issue where the HIP check did not detect the BitLocker disk encryption correctly during windows update, causing the device to fail the HIP check.
GPC-19918	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS, the HIP check did not detect CrowdStrike antivirus software correctly, causing the device to fail the HIP check.
GPC-19889	Fixed an issue where, when the GlobalProtect app was installed on Windows machine and Connect Before Logon (CBL) was configured for the app, the app did not start properly when the user logged on to the device.
GPC-19878	Fixed an issue where a typo in the IP address exclusion list was not marked as invalid by the GlobalProtect enforcer, resulting in all IP addresses in the range being allowed.

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
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 user name and password.
GPC-19751	Fixed an issue where the programmatic and visual label for the GlobalProtect form field was not announced.
GPC-19740	Fixed an issue where, when the GlobalProtect app was installed on VDI devices running Windows OS, the GlobalProtect app got disconnected without displaying any message.
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-19660	Fixed an issue where the "Check for Updates" button on GlobalProtect app version 6.2.2 did not work when the activated GlobalProtect version on the firewall was earlier than 6.2.2.
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-19629	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS, the split tunnel feature did not work as expected when Jamf was used to push the configuration policy rules.
GPC-19610	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS, end users were not prompted to enter a

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	password and the app got stuck in Restoring VPN connection state until the cookie was deleted.
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-19436	Fixed an issue where the screen reader could not identify the image in the GlobalProtect app tray on the devices running macOS causing accessibility issues.
GPC-19532	Fixed an issue where, after upgrading GlobalProtect via the portal prompt, all traffic except DNS was being dropped because the new GlobalProtect extensions were not being loaded.
GPC-19373	Fixed an issue where the HIP remediation pop up is displayed even when the user is disconnected.
GPC-19373	Fixed an issue where the HIP remediation pop up is displayed even when the user is disconnected.
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-19279	Fixed an issue where the GlobalProtect client was not displayed during the upgrade from version 6.0.5-35 to 6.0.8-601.
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.

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
GPC-19098	Resolved an issue where pre-logon setup was not working when GlobalProtect 6.2.1 was deployed via Microsoft Intune.
GPC-19043	Fixed an issue where the GlobalProtect app did not add all routes configured in the access route to the route table.
GPC-19011	Fixed an issue where the GlobalProtect app on a Windows computer was unable to connect to an IPv4 gateway behind a NAT64 device.
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.
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-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	Fixed an issue where the Zoom app intermittently stopped connecting on macOS and displayed an error message.
GPC-18385	Fixed an issue where, when the GlobalProtect app got reconnected after the user changed the network access from Wi-Fi (IPv4 only) to Ethernet connection (Dual Stack IPv4 + IPv6), the IPv6 ip-user mapping was missing on the firewall and only IPv6 ip-user mapping was available. The user had to refresh the connection to resolve this issue.

©2026 Palo Alto Networks, Inc.

Issue ID	Description
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.
GPC-14714	Fixed an error where the screen reader does the announce the status when the radio button is selected for Network configuration, Routing table, Sockets, and "Logs".

 ©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.3-c287 Addressed Issues

The following table lists the issues that are addressed in GlobalProtect app 6.2.3-c287.

Issue ID	Description
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-20157	Fixed an issue where the gateway location was not correctly displayed in the Connections panel.
GPC-20143	Fixed an issue where the user was redirected to the Authentication page twice on the default browser for both portal and gateway authentication when SAML was configured.
GPC-19991	Fixed an issue where client certificate authentication between embedded browser and IdP (SAML) failed.

 ©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.3 Windows and macOS Addressed Issues

The following table lists the issues that are addressed in GlobalProtect app 6.2.3 Windows and macOS.

Issue ID	Description
GPC-20970	Fixed an issue where GlobalProtect had intermittent connectivity issues on Prisma Access IP optimization enabled tenants.
GPC-19968	Fixed an issue where the GlobalProtect agent failed to detect Bitdefender Antivirus Plus on the Windows ARM64 platform during the HIP check.
GPC-19924	Resolved intermittent connection issues for users accessing GlobalProtect via an embedded browser.
GPC-19901	Fixed an issue where the GlobalProtect client for Mac users was intermittently disconnecting and reconnecting.
GPC-19840	Fixed an issue where Mac computers did not display all gateways in the Search Gateway tab.
GPC-19818	Fixed an issue where when the Enforcer was enabled, Jamf connect was not working after the MacBook was rebooted. Users had to log in manually.
GPC-19784	Fixed an issue where the HIP check did not detect McAfee Premium individual.
GPC-19753	Fixed an issue where the GlobalProtect icon could not be selected using the keyboard.
GPC-19712	Fixed an issue where PanGPS crashed on 6.0.4 caused by invalid memory reference. GlobalProtect did not run correctly after the system was rebooted.
GPC-19686	Fixed an issue where translation errors were observed in the GlobalProtect app for French localization.

©2026 Palo Alto Networks, Inc.

Issue ID	Description
GPC-19664	Fixed an issue where users were able to deploy GlobalProtect from JAMF on Mac Sonoma, but the connection to the portal was stuck.
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-19656	Resolved an issue where connecting to a GlobalProtect gateway with IPv6 from macOS resulted in the tunnel connection dropping every 45 seconds when Endpoint Traffic Policy Enforcement was set to All Traffic.
GPC-19630	Fixed an issue where the prelogon connect method failed on the gateway prelogin stage.
GPC-19587	Fixed an issue where the user could not login with Okta on macOS when Endpoint Traffic Policy Enforcement was set to **All traffic**.
GPC-19581	Fixed an issue where GlobalProtect indicated that Windows firewall was not enabled in the HIP report even though it was enabled.
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-19524	Fixed an issue where the GlobalProtect app connection failed when the user used CAS authentication to authenticate to the app. The app displayed the error message, "Username from CAS SSO response is different from the input".
GPC-19513	Fixed an issue where the GlobalProtect client 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.

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
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 the GlobalProtect client was trying to use the old portal's authorization cookie to login instead of the newly migrated portal. This happened when the user changed the portal from secondary to primary or vice versa without signing out.
GPC-19433	Fixed an issue where a small white blank page randomly popped up on the user's screen and the focus shifted to this blank page. This issue occurs while the computer is connected to Global Protect.
GPC-19431	Fixed an issue where interactive components in the session tray on Windows did not receive keyboard focus and were not keyboard operable.
GPC-19418	Fixed an issue where GlobalProtect users randomly experienced issues connecting to the gateway after their computer woke up. This occurred when Enforce GlobalProtect for Network Access was enabled and Tunnel and Proxy was set to agent mode.
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-19414	Fixed an issue where GlobalProtect Always-On connect method was not triggered after a reboot when the connect-method setting was set to on-demand in the Windows Registry.
GPC-19403	Fixed an issue where OPSWAT was unable to detect Kaspersky after an upgrade from 21.3.10.391 to 21.15.8.493.
GPC-19400	Fixed an issue where the GlobalProtect HIP check did not detect the Definition Date for

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	Bitdefender Virus Scanner, which caused the device to fail the HIP check.
GPC-19391	Fixed an issue where GlobalProtect stayed disconnected even after being unlocked.
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-19374	Fixed an issue where the GlobalProtect debug logs displayed information, which was not supposed to display in the logs.
GPC-19359	Fixed an issue where system extensions on MacBook were not updated after the GlobalProtect client was upgraded.
GPC-19340	Fixed an issue where the GlobalProtect app failed to send HIP reports hourly.
GPC-19337	Fixed an issue where the Captive Portal functionality of the GlobalProtect app did not work as expected when the users used public Wi-Fi hotspots.
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-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-19284	Fixed an issue where GlobalProtect was unable to extend user session.
GPC-19280	Fixed an issue where, when the GlobalProtect app transitioned from pre-logon to user-

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	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-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-19193	Fixed an issue where the GlobalProtect app was unable to fetch Windows firewall and antimalware information correctly.
GPC-19162	Fixed an issue where, when the user upgraded the GlobalProtect version to 5.2.13 or later, the HIP report displayed the DLP 'Digital Guardian Agent' as disabled.
GPC-19107	Fixed an issue where some log files were missing from the GlobalProtect bundle when downloaded from the Explore app.
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 refresh connection did not work when the Settings window was opened.
GPC-19074	Fixed an issue where Login Lifetime was incorrectly translated on the French version of the GlobalProtect 6.2.1 app.
GPC-19060	Fixed an issue where the app Settings -> Connection tab 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

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	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-18992	Fixed an issue where internet via WiFi connection was unavailable for GlobalProtect users after their computer woke up from sleep because the client WiFi adapter was unable to obtain a DHCP IP address. This issue occurred on computers where Enforce GlobalProtect for Network Access was enabled.
GPC-18983	Fixed an issue where the Central Authentication Service (CAS) authentication did not work when the GlobalProtect app was connected to an internal gateway and the app repeatedly opened the SAML authentication page.
GPC-18913	Fixed an issue where the GlobalProtect app displayed the connection status as 'Not Connected' even though the app was connected to the internal gateway.
GPC-18907	Fixed an issue where the GlobalProtect app running 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-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.

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
GPC-18845	Fixed an issue, where the GlobalProtect app was installed manually and the user clicked the ‘Get Started’ button, the app displayed the incorrect message, "Oops! Slow or No Network Connection" instead of the actual message "Not Connected" window where they can input their portal address.
GPC-18828	Fixed an issue where split tunnel CNAME records were created before the GlobalProtect tunnel was established.
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-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-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-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-18720	Fixed an issue where the GlobalProtect app became unresponsive when the user clicked the ESCbutton during authentication using a hard token.
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-18598	Fixed an issue where the GlobalProtect SSO tile was selected instead of the

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	Windows Password tile in the Windows Login screen even though the registry key MakeGPCPDefault was set to No.
GPC-18384	Fixed an issue where GlobalProtect did not connect while Netskope was connected and vice-versa.
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-18223	Fixed an issue where GlobalProtect experienced a prolonged connection time when IPv6 was disabled on Windows devices.
GPC-18157	Fixed an issue where the GlobalProtect app displayed the Credential Provider language in English when the system language was German.
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-18025	In 6.2.1, after a refresh connection, the HIP patch exclusion isn't visible on the GlobalProtect UI. However, the HIP patch exclusion logs are visible on the `Pangphip.log` file.
GPC-17640	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-17518	Fixed an issue where the GlobalProtect app displayed the status as 'Connected-Internal' even when the app was not connected.
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.

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
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-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.
GPC-16584	Fixed an issue where the GlobalProtect HIP check did not detect the CrowdStrike antivirus software correctly, causing the device to fail the HIP check.
GPC-15123	Fixed an issue where users were unable to collapse the Change Portal and Change Gateway menus using the Escape key.

©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.2 Windows and macOS Addressed Issues

The following table lists the issues that are addressed in GlobalProtect app 6.2.2 Windows and macOS.

Issue ID	Description
GPC-19116	Fixed an issue where the user faced authentication issues while the GlobalProtect app was attempting to refresh the explicit proxy token.
GPC-19049	Fixed an issue where, when the GlobalProtect app was configured in hybrid mode with internal host detection, the app failed to connect and continued to stay in the `Connecting` state when users tried to connect using SAML authentication.
GPC-19007	Fixed an issue where users were unable to connect to the GlobalProtect portal and gateway after upgrading the app version to 6.2.1.
GPC-19002	Fixed an issue where the GlobalProtect app did not display the **Connect** button when the user clicked the **Get Started** button after the app installation through Jamf.
GPC-18991	Fixed an issue where the proxy auto-configuration (PAC) files were not restored as expected after a system reboot or when the user disconnected the GlobalProtect app.
GPC-18964	Fixed an issue where the GlobalProtect tunnel got disconnected after 10 minutes on the app versions 6.0.8 and 6.2.1, when the GlobalProtect app was running on macOS devices and SAML authentication was used to authenticate.
GPC-18861	Fixed an issue where the GlobalProtect MSI download was getting stuck at 27%.
GPC-18471	Fixed an issue where, when multiple `wa_3rd_party_host_64.exe` processes

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	persisted even after the HIP check, the GlobalProtect app stopped working.

 ©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.1 Linux Addressed Issues

The following table lists the issues that are addressed in GlobalProtect app 6.2.1 for Linux.

Issue ID	Description
GPC-21151	Fixed an issue where, when the option **Allow Authentication with User Credentials OR Client Certificate** was set to **Yes** in the portal configuration, and no valid client certificate was installed on the endpoint, the connection failed with the error: **Connection Failed. A valid client certificate is required for authentication** without prompting the user for their credentials.
GPC-20945	Fixed an issue where, when the GlobalProtect app was installed on Linux endpoints, users were unable to access ephemeral URLs.
GPC-20605	Fixed an issue where, when the GlobalProtect app was installed on Linux endpoints with the connect method pre-deployed, the connect method failed to get updated with the portal configuration after the first successful connection.
GPC-20574	Fixed an issue where, when the GlobalProtect app was installed on Linux (Fedora 38 version) endpoints, the GlobalProtect HIP check did not detect the SentinelOne application, which caused the device to fail the HIP check.
GPC-20544	Fixed an issue where the GlobalProtect app on Linux endpoints was displaying confusing error messages when the user would connect to manual gateways.
GPC-20525	Fixed an issue where, when the GlobalProtect app 6.1.4 version was installed on Linux endpoints and the **Allow User to Change Portal Address** option was set to **No** in the app settings of the portal configuration, the app did not retain the portal name after a system reboot.
GPC-20449	Fixed an issue where the GlobalProtect HIP check incorrectly detected the date for

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	ClamAV virus definition update, which caused the endpoint to fail the HIP check.
GPC-20398	Fixed an issue where, when the GlobalProtect app was installed on Linux endpoints, the app could not resolve the DNS queries containing capital letters.
GPC-20340	Fixed an issue where, when the GlobalProtect app was installed on Linux endpoints, end users had to reboot the system to reconnect the app when the GlobalProtect got disconnected.
GPC-19973	Fixed an issue where, when the GlobalProtect app was installed on Linux endpoints (Ubuntu 22.04.4 LTS) and SAML authentication was used to authenticate to the app, a blank page appeared during the first attempt at SAML authentication every time.
GPC-19297	Fixed an issue where the GlobalProtect HIP check did not detect the Last Full Scan Time for Cortex XDR, which caused the device to fail the HIP check.
GPC-18105	Fixed an issue where the user was unable to cancel out of SAML authentication in on-demand mode while the GlobalProtect app was in connecting state.
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.

 ©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.1 Windows and macOS Addressed Issues

The following table lists the issues that are addressed in GlobalProtect app 6.2.1 for Windows and macOS.

Issue ID	Description
GPC-18789	Fixed an issue where the GlobalProtect app took a long time to connect to the gateway when the include domain list was used, while the enhanced split-tunnel feature was not used.
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-18594	Fixed an issue where the GlobalProtect app was unable to send HIP reports when the app was connected using IPv6.
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-18509	Fixed an issue where, when the GlobalProtect app was configured with the Internal Host Detection and Conditional Connect method, the app did not connect to the internal network when the network was changed from external to internal as it should have with the Conditional Connect method enabled.
GPC-18452	Fixed an issue where, when the GlobalProtect app was installed on Windows devices the app did not start right away after a system reboot.

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
GPC-18426	Fixed an issue where when the GlobalProtect app was configured with the **Disable GlobalProtect** set to **Allow with Ticket**, the app did not display the correct Disable Duration time.
GPC-18336	Fixed an issue where 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 as **Connected - Inter....** instead of **Connected - Internal**.
GPC-18281	Fixed an issue where the MSI install logs showed mutiple messages for Autonomous DEM installation.
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-18175	Fixed an issue where users were prompted to enter their credentials even when the GlobalProtect app was configured for authenticating with either Authentication Profile /Cookie or Client Certificate.
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

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	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 are not set for manual selection.
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.
GPC-18092	Fixed an issue where GlobalProtect connected to an internal gateway got automatically disconnected after a certain period of time.
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-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-18036	Fixed an issue where, when the **No direct access to local network** option was enabled on the GlobalProtect app with access routes excluded from the GlobalProtect VPN tunnel, the feature did not work as expected when

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	Endpoint Traffic Policy Enforcement was enabled.
GPC-17936	Fixed an issue where the Conditional Connect method did not work as expected and users had to manually connect the app when they changed their network.
GPC-17921	Fixed an issue where, when the language was set to Japanese, the time to connect was not displayed properly when **Disconnect Timeout** for the app was configured.
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-17816	Fixed an issue ehere after entering CIE SAML authentication credentials to refresh an expired explicit proxy token or cookie when connected in Tunnel and Proxy mode or proxy mode, the GlobalProtect app got stuck while retrieving the portal configuration.
GPC-17795	Fixed an issue where the GlobalProtect HIP check did not detect the Xcitium Enterprise, the Endpoint Protection Platform by COMODO, which caused the device to fail the HIP check.
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 when the GlobalProtect app was configured with the option **Allow User to Disable GlobalProtect App** with comment, the option did not work as expected.
GPC-17748	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.

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
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 GlobalProtect gateway when only one external gateway was added due to the following error: **Cannot Verify Server Certificate of Gateway**.
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 **Term of Use** pop-up on the **Welcome** page properly.
GPC-17398	Fixed an issue where the GlobalProtect app **Settings** > **Connection** tab did not display the **Assigned IP Address(es)** and **Gateway IP Address** properly.
GPC-17206	Fixed an issue where, when Internal Host Detection (IHD) was enabled but failed to detect the internal network properly, the app failed to switch to the external gateway when users switched from an internal network to an external network.
GPC-17161	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS, the GlobalProtect app failed to reconnect and continued to stay in the **Connecting** state after the device woke up from Modern Standby mode.
GPC-17099	When the GlobalProtect app for Windows is upgraded to version 6.0.5, 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-17001	Fixed an issue where, when the GlobalProtect app was installed on devices running on macOS, the app did not display the **Connect**

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	button and **Refresh Connection** button properly.
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-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-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-16126	Fixed an issue where the GlobalProtect app did not display the certificate name in the Client Certificate selection field properly.
GPC-16003	Fixed an issue where, when the GlobalProtect app was installed on devices running macOS, the app was not connected when the proxy was configured for Safari or Chrome.
GPC-15968	Fixed an issue where the GlobalProtect app was stuck in **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-15262	Fixed an issue where when single sign-on (SSO) for Smart Cards was used for authentication, users were prompted to enter a PIN instead of a password on the Windows login screen.
GPC-15234	Fixed an issue where the app would get stuck at Connecting state while trying to connect to a gateway.
GPC-15080	Fixed an issue where when the split tunnel was configured based on the destination domain, split tunneling did not work as

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	expected when IPv6 traffic exclusion was configured.

 ©2026 Palo Alto Networks, Inc.

GlobalProtect App 6.2.0 Linux Addressed Issues

The following table lists the issues that are addressed in GlobalProtect app 6.2.0 for Linux.

Issue ID	Description
GPC-19792	Fixed an issue where an error message was displayed on the GlobalProtect app: **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 app 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-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-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-18820	Fixed an issue where some users were unable to connect to GlobalProtect after disconnecting the app.
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-18155	Fixed an issue where the GlobalProtect main panel was displayed on the bottom right

 ©2026 Palo Alto Networks, Inc.

Issue ID	Description
	instead of its usual location at the top right. This occurred when an NVidia Graphics GPU driver was installed in the environment,
GPC-17598	Fixed an issue where, when the GlobalProtect app was installed on Linux devices and 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-16980	Fixed an issue where users were unable to upgrade GlobalProtect app from 5.3 to 6.0.x or 6.1.x due to file conflicts between packages.

 ©2026 Palo Alto Networks, Inc.