GlobalProtect™ App 4.1 Release Notes

Release 4.1.1

paloaltonetworks.com/documentation

techDOCS paloalto NETWORKS

Contact Information

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

About the Documentation

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

Copyright

Last Revised

April 26, 2018

Table of Contents

GlobalProtect App 4.1 Release Information

Revision Date: April 26, 2018

Review important information about Palo Alto Networks GlobalProtect™ app software, including new features introduced, workarounds for open issues, and issues that are addressed in GlobalProtect app 4.1 releases.

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

Features Introduced in GlobalProtect App 4.1

The following topics describe the new features introduced in GlobalProtect app 4.1. For additional information on how to use the new features in this release, refer to the GlobalProtect App 4.1 New Features Guide.

Feature	Description
GlobalProtect User Experience Enhancements	GlobalProtect app 4.1 for Windows and macOS endpoints introduces an enhanced user experience through a more modern and streamlined user interface and a more intuitive connection process. The new app features simplified workflows that enable end users to view and modify GlobalProtect app settings, manage notifications from a central location, and connect to or disconnect from GlobalProtect more seamlessly.
Optimized Split Tunneling for GlobalProtect	In addition to route-based split tunnel policy, GlobalProtect now supports split tunneling based on destination domain,client process, and HTTP/HTTPS video streaming application. This feature is available on Windows and macOS endpoints and enables you to: • Tunnel enterprise SaaS and public cloud applications for comprehensive SaaS application visibility and control to avoid risks associated with Shadow IT in environments where tunneling all traffic is not feasible. • Send latency-sensitive traffic, such as VoIP, outside the VPN tunnel, while all other traffic goes through the VPN for inspection and policy enforcement by the GlobalProtect gateway. • Exclude HTTP/HTTPS video streaming traffic from the VPN tunnel. Video streaming applications, such as YouTube and Netflix, consume large amount of bandwidth. By excluding lower risk video streaming traffic from the VPN tunnel, you can decrease bandwidth consumption on the gateway. *This enhancement requires a GlobalProtect subscription.*
GlobalProtect App for Linux	The new GlobalProtect app for Linux now extends User-ID and Security policy enforcement to users on Linux endpoints. The GlobalProtect app provides a CLI and functions as an SSL or IPSec VPN client. The GlobalProtect app supports common GlobalProtect features and authentication methods, including certificate and two-factor authentication and both user-logon and on-demand connect methods. The app can also perform internal host detection to determine whether the Linux endpoint is on the internal network and collects host information (such as operating system and operating system version, domain, hostname, host ID, and network interface). Using this information, you can allow or deny access to a specific Linux endpoint based on the adherence of that endpoint to the host policies you define. The GlobalProtect app for Linux is available for the Linux distribution of Ubuntu 14.04, RHEL 7.0, and CentOS 7.0 (and later releases of each) and requires a GlobalProtect subscription.

Feature	Description
Kerberos Authentication Support for macOS	The GlobalProtect app for macOS endpoints (10.10 and later releases) now supports Kerberos V5 single sign-on (SSO) for GlobalProtect portal and gateway authentication. Kerberos SSO, which is primarily intended for internal gateway deployments, provides accurate User-ID information without user interaction and helps enforce user- and HIP-based policies.
SAML SSO for GlobalProtect on Chromebooks	The GlobalProtect app for Chromebooks (Chrome OS) now supports SAML single sign-on (SSO). If you configure SAML as the authentication standard for Chromebooks, end users can authenticate to GlobalProtect by leveraging the same login they use to access their Chromebook applications. This enables users to connect to GlobalProtect without having to re-enter their credentials in the GlobalProtect app. With SSO enabled (default), Google acts as the SAML service provider while the GlobalProtect app authenticates users directly to your organization's SAML identity provider. *GlobalProtect currently supports only the **Post** SAML HTTP binding method.*
Automatic VPN Reconnect for Chromebooks	The GlobalProtect app for Chromebooks can now automatically try to reestablish the connection when any of the following events occur: • The endpoint wakes up from sleep. • The endpoint switches between wireless networks. • The endpoint switches from wired to a wireless or LTE network. • The wireless interface is disabled and re-enabled. This is especially useful for mobile users who encounter these events as part of their day-to-day operations because it reduces disruptions in VPN connectivity as well as the manual steps required to reestablish the connection. This feature is automatically enabled in Chrome OS 51 and later releases and does not require any configuration.
GlobalProtect Credential Provider Pre-Logon Connection Status	The GlobalProtect credential provider logon screen on Windows 7 and Windows 10 endpoints now displays the pre-logon connection status when you configure pre-logon for remote users. The pre-logon connection status indicates the state of the pre-logon VPN connection prior to user logon. By providing more visibility on the pre-logon connection status, this feature allows end-users to determine whether they can access network resources after logon, and therefore avoid logging in prematurely before the connection establishes and network resource become available. If the GlobalProtect app determines that an endpoint is internal (connected to the corporate network), the logon screen displays the GlobalProtect connection status as `Internal`. If the GlobalProtect app determines that an endpoint is external (connected to a remote network), the logon screen displays the GlobalProtect connection status as `Connected` or `Not Connected`.
Active Directory Password Change Using the	End users can now change their Active Directory (AD) password using the GlobalProtect credential provider on Windows 10 endpoints. This enhancement improves the single sign-on (SSO) experience by allowing users to update their AD password and access resources that are secured by GlobalProtect using the GlobalProtect credential provider. Users can change

Feature	Description
GlobalProtect Credential Provider	their AD password using the GlobalProtect credential provider only when their AD password expires or an administrator requires a password change at the next login.
Expired Active Directory Password Change for Remote Users	Remote users can now change their RADIUS or Active Directory (AD) password through the GlobalProtect app when their password expires or a RADIUS/AD administrator requires a password change at the next login. With this feature, users can change their RADIUS or AD password when they can't access the corporate network locally and their only option is to connect remotely using RADIUS authentication. This feature is enabled only when the user authenticates with a RADIUS server using the Protected Extensible Authentication Protocol Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MSCHAPv2).
Multiple Portal Support	End users can now save multiple portals in a list on the GlobalProtect app for Windows and macOS endpoints. This enhancement enables users to manage their deployments more efficiently, as they can switch between different portals without having to re-enter the portal address each time they want to connect. *GlobalProtect does not save separate credentials for each portal.*
Static IP Address Assignment	You can now assign static IP addresses to Windows endpoints by configuring the **reserved-ipv4** or **reserved-ipv6** entries in the Windows Registry during GlobalProtect app deployment. This feature ensures that the GlobalProtect tunnel IP addresses that you assign to your endpoints do not change, which enables you to locate and troubleshoot errors in IP address assignment. The GlobalProtect app can create a tunnel between the endpoint and the gateway only when the gateway returns the same IP address as the reserved tunnel IP address assigned to the endpoint. If the gateway does not return the same IP address, the GlobalProtect app displays the following error message: `Could not connect to the gateway with the specified tunnel IP address. Please contact your IT administrator.`
OPSWAT SDK V4 Support	GlobalProtect is now integrated with OPSWAT SDK V4 to detect and assess the endpoint state and the third-party security applications running on the endpoint. OPSWAT is a security tool leveraged by the Host Information Profile (HIP) to collect information about the security status of the endpoints in the network. GlobalProtect uses this information for policy enforcement on the GlobalProtect gateway. This integration follows the end-of-life (EoL) announcement for OPSWAT SDK V3, which is the OPSWAT SDK version supported by GlobalProtect in PAN-OS 8.0 and earlier releases.
Support for the ARMv7-A Application Binary Interface	(GlobalProtect 4.1.1 and later) The GlobalProtect app for Android endpoints now supports the ARMv7-A Application Binary Interface (ABI).

Changes to Default Behavior

The following topics describe changes to default behavior in GlobalProtect app 4.1:

Changes to Default Behavior in GlobalProtect App 4.1.1

The following table describes changes to default behavior in GlobalProtect app 4.1.1:

Feature	Description of Change
Local subnet access	The GlobalProtect app on Windows endpoints no longer modifies the endpoint proxy settings after establishing and taking down a VPN tunnel if you configured **No direct access to local network** for the GlobalProtect gateway (**Network** > **GlobalProtect** > **Gateways** > **<gateway** > **Agent** > **Client Settings** > **<client_settings_configuration>** > **Split Tunnel** > **Access Route**). Previously, the app removed and then re-stored the proxy settings when establishing and taking down the tunnel.
GlobalProtect service logs	On Windows UWP endpoints, the GlobalProtect app now stores PanGPS logs in the `%localappdata%\Packages\PaloAltoNetworks.GlobalProtect_rn9aeerfb38dg\LocalState\DiagOutputDir` directory instead of the `%localappdata%\Packages\PaloAltoNetworks.GlobalProtect_rn9aeerfb38dg\LocalState` directory.

Changes to Default Behavior in GlobalProtect App 4.1.0

The following table describes changes to default behavior in GlobalProtect app 4.1.0:

Feature	Description of Change
Help Page Configuration	The GlobalProtect **App Help Page** configuration on the GlobalProtect portal has the following changes (**Network** > **GlobalProtect** > **Portals** > **<portal-config>** > **GlobalProtect Portal Configuration** > **General** > **Appearance**): • If you select **Factory Default** from the **App Help Page** drop-down, the GlobalProtect app displays the default help file that is built in to the app. • If you select **None** (default) from the **App Help Page** drop-down, the **Help** option is removed from the **Settings** menu on the GlobalProtect status panel. • If you select **Import** from the **App Help Page** drop-down, you can upload a custom help file for the GlobalProtect app. The GlobalProtect portal provides the custom help file with the GlobalProtect portal configuration.
Manual-Only Gateways in Always On Mode	When you configure the GlobalProtect **Connect Method** as **User-Logon (Always On)** or **Pre-Logon (Always On)** but configure all external gateways as manual-only gateways, external users do not automatically connect to any of the manual-only gateways. GlobalProtect now remains in the `Not Connected` state until the external user connects to a gateway manually. In

Feature	Description of Change
	addition, GlobalProtect does not perform periodic auto-discovery for external gateways unless a network change occurs. This change to default behavior enables customers to deploy GlobalProtect to derive User-ID when the user is internal and support On-Demand VPN behavior when the user is external.
Endpoint Traffic Handling	If you configure the GlobalProtect app to tunnel all traffic, GlobalProtect drops packets that do not have the source IP address as the tunnel-assigned IP address. This change to default behavior enables applications to re-establish the connection through the tunnel. For example, if a user initiates a connection prior to establishing a GlobalProtect connection on the endpoint, all traffic for that connection is sourced from the IP address of the physical adapter (LAN or WiFi). After the user establishes the GlobalProtect connection, GlobalProtect drops all packets for the previously initiated connections, which have the source IP address as the IP address of the physical adapter.
GlobalProtect Credential Provider Pre-Logon Domain Name Display	When you configure GlobalProtect with the **Pre-Logon** connection method, the GlobalProtect Credential Provider logon screen on Windows 10 endpoints now displays the pre-populated domain name below the editable username field.
Cached Passwords	If you do not enable two-factor authentication for your GlobalProtect portal and gateway, the GlobalProtect service (PanGPS) now clears the following passwords when gateway authentication fails: • Cached single sign-on (SSO) passwords (when SSO is enabled) • Cached GlobalProtect portal passwords • Cached saved user passwords (when **Save User Credentials** is enabled) After authentication fails, users must re-enter their passwords on the GlobalProtect app or portal/gateway authentication prompt (when **Do not prompt user for authentication** is disabled) in order to authenticate and establish a connection to GlobalProtect. If users click **Cancel**, and then initiate a new authentication attempt, the GlobalProtect app prompts them to manually enter their passwords instead of using previously saved passwords.
macOS Version Check	The GlobalProtect app software package for macOS endpoints now includes a minimum OS version check to ensure that end users install the GlobalProtect app only on endpoints running macOS versions that the specific app release supports (such as GlobalProtect app 4.1). If users attempt to install the GlobalProtect app on endpoints running macOS versions that the app release does not support, installation fails. For example, users can install GlobalProtect app 4.1 only on endpoints running macOS 10.10 or later releases. Refer to the GlobalProtect Compatibility Matrix for the complete list of OS versions that each GlobalProtect app release supports.

Associated Software and Content Versions

The following minimum software versions are supported with the GlobalProtect app 4.1.

Palo Alto Networks Software or Content Release Version	Minimum Supported Version
PAN-OS version	7.1

Limitations

The following table includes limitations associated with the GlobalProtect app 4.1 release.

Issue ID	Description
GPC-5543	On macOS endpoints, native modal notification dialogs (such as the GlobalProtect update installation dialog) open behind the GlobalProtect status panel if they overlap.
GPC-5346	When users connect to Windows 10 endpoints using the Microsoft Remote Desktop Connection, they cannot authenticate and establish a connection to GlobalProtect using single sign-on (SSO) because Remote Desktop Services (RDS)—which enables users to access and run applications on the remote desktop—does not support SSO with non-native Windows credentials. If users initiate a remote desktop connection using credentials from the GlobalProtect Credential Provider, they must manually re-enter their credentials on the GlobalProtect Credential Provider logon screen (when prompted) to access the endpoint and establish the GlobalProtect connection.

GlobalProtect App 4.1 Known Issues

The following table includes known issues in GlobalProtect app 4.1.

Issue ID	Description
GPC-6045	Endpoints can't connect to GlobalProtect after you set the Windows System Display to Chinese and specify Chinese characters for the **Username Label** in the GlobalProtect app login page (**Network** > **GlobalProtect** > **Portals** > <*portal*> > **Agent** > <*agent*> > **Authentication**).
GPC-5909	When you **Allow User to Disable GlobalProtect** and then specify a **Disable Timeout** value to restrict the amount of time for which users can disable the app (**Network** > **GlobalProtect** > **Portals** > <*portal*> > **Agent** > <*agent*> > **App**), the GlobalProtect app for macOS endpoints does not automatically enable after reaching the **Disable Timeout** value. **Workaround**: Users must manually enable the GlobalProtect app.
GPC-5879 This issue is now resolved. See GlobalProtect App 4.1.1 Addressed Issues.	Endpoints running iOS 10.12 and later iOS releases on the T-Mobile LTE network cannot connect to GlobalProtect gateways that are configured with only IPv4 addresses because T-Mobile now assigns only IPv6 addresses to endpoints running iOS 10.12 and later releases. **Workaround**: Configure your GlobalProtect gateway with FQDNs instead of IPv4 addresses.
GPC-5416 This issue is now resolved. See GlobalProtect App 4.1.1 Addressed Issues.	On Windows 10 endpoints, the GlobalProtect app removes DNS suffixes due to an error in the read/rewrite function that directly modifies the DNS suffix search list in the Windows registry key.
GPC-4856	On macOS endpoints, the GlobalProtect app can't detect the following **Anti-Malware** information for the HIP Match log details of the Gatekeeper security feature (**Monitor** > **Logs** > **HIP Match** > <*hip-match-log*>): • **Engine Version** • **Definition Version** • **Date** • **Last Scanned**
GPC-3962	Proxies are disabled after you establish the GlobalProtect connection on macOS endpoints because proxy settings are not copied from the physical network adapter of the endpoint to the virtual network adapter of the endpoint, and the virtual network adapter becomes the primary adapter from which the macOS endpoint receives proxy settings.

GlobalProtect App 4.1.1 Addressed Issues

The following table lists the issues that are addressed in GlobalProtect app 4.1.1.

Issue ID	Description
GPC-6154	Fixed an issue on Windows UWP endpoints where the GlobalProtect app intermittently failed to connect to the GlobalProtect gateway when the UWP plugin was set to Always On.
GPC-6150	Fixed an issue on Windows endpoints where, after end users logged in to Windows, the GlobalProtect app stopped running and Windows Error Reporting (WER) displayed the following error: `GlobalProtect client stopped working`.
GPC-6149	Fixed an issue on Windows 8 endpoints where the GlobalProtect login page displayed the password field above the username field after you enabled **Interactive Logon: Do not display last username** in the Windows Local Group Policy Editor (**Local Computer Policy** > **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policy** > **Security Options**).
GPC-6121	Fixed an issue on MacOS endpoints where the GlobalProtect app couldn't detect processes that had more than 16 characters in their names.
GPC-6080	Fixed an issue where remote desktop connections over existing VPN tunnels disconnected after you configured the GlobalProtect portal to use a **Certificate Profile** for authenticating clients (**Network** > **GlobalProtect** > **Portals** > *<portal>* > **Authentication**) and set **Save User Credentials** to **Save Username Only** in the app (agent) configurations (**Network** > **GlobalProtect** > **Portals** > *<portal>* > **Agent** > *<agent>* > **Authentication**).
GPC-6079	Fixed an issue where the GlobalProtect app continuously tried to connect to external GlobalProtect gateways and displayed `connecting` or `still working` status even though the GlobalProtect portal configuration didn't have external gateways defined (**Network** > **GlobalProtect** > **Portals** > *<portal>* > **Agent** > *<agent>* > **External**).
GPC-6076	Fixed an issue on Android endpoints enrolled with AirWatch where Host Information Profile (HIP) checks failed because the manifest file for the GlobalProtect app was missing the mobile_id value.
GPC-6068	Fixed an issue where HIP matching failed because HIP reports included the wrong characters for antivirus software that had Unicode names.
GPC-6052	Fixed an issue where the GlobalProtect app couldn't detect FireEye Endpoint Antivirus software and therefore didn't include it in HIP reports.
GPC-6049	Fixed an issue where, even though you configured **No direct access to local network** in the GlobalProtect gateway, the GlobalProtect app reverted to its local DNS to resolve domain names after the DNS servers that the gateway provided failed to resolve the names (**Network** > **GlobalProtect** > **Gateways** >

Issue ID	Description
	<gateway> > **Agent** > **Client Settings** > *<client_settings_configuration>* > **Split Tunnel** > **Access Route**).
GPC-6040	Fixed an issue where end users who had special characters associated with XML markup (<, >, &, ', ") in their password couldn't connect to the GlobalProtect gateway after an upgrade to GlobalProtect app 4.1.0.
GPC-6037	Fixed an issue where the GlobalProtect app failed to automatically install VPN tunnel routes and the routes then required manual installation.
GPC-6036	Fixed an issue where the GlobalProtect app failed to authenticate to the GlobalProtect portal through the Proxy Login prompt when the endpoint browser used a proxy auto-config (PAC) file to automatically select a proxy server.
GPC-6010	Fixed an issue where the GlobalProtect app displayed an empty dialog instead of the portal detection message after the end user logged into a network through its captive portal and then followed the instructions to log off and reconnect through a pre-logon VPN tunnel.
GPC-6002	Fixed an issue on MacOS endpoints where the GlobalProtect app failed to automatically populate the username in the GlobalProtect gateway authentication prompt.
GPC-5986	Fixed an issue on Windows endpoints where end users could add, modify, or delete GlobalProtect portal addresses even after you set the **Allow User to Change Portal Address** option to **No** (**Network** > **GlobalProtect** > **Portals** > *<portal>* > **Agent** > *<agent>* > **App**).
GPC-5985	Fixed an issue where, after you installed a GlobalProtect app using the Windows Installer (Msiexec), a popup window displayed `Portal not found. Please re-enter or contact an administrator for help`, but the portal connection succeeded when you clicked **OK** to close the popup.
GPC-5952	Fixed an issue in GlobalProtect deployments configured for multi-factor authentication where end users couldn't activate the **Submit** button in the GlobalProtect Login page by pressing the Enter key on their keyboard.
GPC-5946	Fixed an issue where the GlobalProtect login prompt allowed only 24 characters for usernames and 21 characters for passwords. With this fix, you can enter up to 256 characters for usernames and passwords.
GPC-5935	Fixed an issue where, whenever Windows endpoints rebooted and end users logged in, the GlobalProtect app displayed a popup window that users had to click to close even after you configured the app not to **Show System Tray Notifications** or **Display GlobalProtect Icon** (**Network** > **GlobalProtect** > **Portals** > *<portal>* > **Agent** > *<agent>* > **App**).

Issue ID	Description

GPC-5933	Fixed an issue on Linux endpoints where certificate imports failed when you ran the GlobalProtect CLI command in prompt mode:
	`user@linuxhost:~$ globalprotect`
	`>>import-certificate --location <file-path>`

GPC-5925	Fixed an issue where GlobalProtect endpoints failed to authenticate to the GlobalProtect gateway on the first connection attempt (subsequent attempts succeeded) after you configured cookie authentication for the GlobalProtect portal and gateway.
GPC-5922	Fixed an issue where Windows endpoints failed the HIP check after you upgraded Norton Internet Security to version 22.12.x.x.
GPC-5879	Fixed an issue on T-Mobile LTE networks where endpoints running iOS 10.12 or a later iOS release couldn't connect to GlobalProtect gateways that were configured with only IPv4 addresses because T-Mobile now assigns only IPv6 addresses to those endpoints.
GPC-5866	Fixed an issue on Windows endpoints where users couldn't upgrade the GlobalProtect app using the Windows Installer (Msiexec) because the GlobalProtect setup file couldn't overwrite existing GlobalProtect app software packages when the GlobalProtect service (PanGPS) was running.
GPC-5865	Fixed an issue on Windows endpoints where the GlobalProtect app incorrectly reported server certificate warnings for unknown errors. With this fix, the app displays the following message for unknown errors: `GlobalProtect has encountered an internal error. Please contact your IT administrator`.
GPC-5629	Fixed an issue where GlobalProtect apps that you installed in a non-default location couldn't connect to the GlobalProtect portal after you set **Enforce GlobalProtect Connection for Network Access** to **Yes** (**Network** > **GlobalProtect** > **Portals** > *<portal>* > **Agent** > *<agent>* > **App**).
GPC-5416	Fixed an issue where DNS suffixes were removed from Windows 10 endpoints due to an error in the read/rewrite function that directly modified the DNS suffix search list in the Windows registry key.
GPC-5286	Fixed an issue on Windows 10 endpoints where GlobalProtect apps with the **Connect Method** set to **User-logon (Always On)** didn't automatically connect to the GlobalProtect portal after network availability went from down to up (**Network** > **GlobalProtect** > **Portals** > *<portal>* > **Agent** > *<agent>* > **App**).

GlobalProtect App 4.1.0 Addressed Issues

The following table lists the issues that are addressed in GlobalProtect app 4.1.0.

Issue ID	Description
GPC-5784	Fixed an issue on Windows 10 UWP endpoints where the certificate key access prompt for VPN connections displayed automatically when newly added GlobalProtect VPN connections were in the `Action Needed` state. In addition, the prompt redisplayed each time users clicked **Cancel**.
GPC-4839	Fixed an issue where the GlobalProtect app for Android endpoints incorrectly displayed the **Secure ID** field when users attempted to log in to GlobalProtect using Duo two-factor authentication.

Getting Help

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

Related Documentation

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

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

Requesting Support

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

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

Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

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

Palo Alto Networks, Inc.

www.paloaltonetworks.com