# GlobalProtect App Release Notes

## 4.1 Beta 7

paloaltonetworks.com/documentation

techDOCS

## 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

February 16, 2018

# Table of Contents

# GlobalProtect App 4.1 Release Information

# 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 tunneling, GlobalProtect now supports split tunneling based on destination domain, client process, and HTTP/HTTPS video streaming application.<br>This feature is available on Windows and macOS endpoints and enables you to:<br>• 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.<br>• 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.<br>• 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.<br>*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 command-line interface 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. |

| Feature | Description |
|---|---|
| | 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. |
| **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 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.<br>⚠ *When GlobalProtect and PAN-OS are configured to use the **Redirect** SAML HTTP binding method for SSO requests to the identity provider (IdP), authentication fails. Use the **Post** SAML HTTP binding method instead.* |
| **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:<br>• The endpoint wakes up from sleep.<br>• The endpoint switches between wireless networks.<br>• The endpoint switches from wired to a wireless or LTE network.<br>• The wireless interface is disabled and re-enabled.<br>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 will be able to access network resources upon logon, which prevents them from logging in prematurely before the connection establishes and network resource become available.<br>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**. |

| Feature | Description |
|---|---|
| **Active Directory Password Change Using the GlobalProtect Credential Provider** | 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 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 are unable to 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.<br>*GlobalProtect does not save separate credentials for each portal.* |
| **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.<br>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. |

# Changes to Default Behavior

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

- Changes to Default Behavior in GlobalProtect App 4.1.0

## 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 following changes have been made to the GlobalProtect **App Help Page** configuration on the GlobalProtect portal (**Network** > **GlobalProtect** > **Portals** > **<portal-config>** > **GlobalProtect Portal Configuration** > **General** > **Appearance**):<br>• 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.<br>• 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.<br>• 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 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 addition, GlobalProtect does not perform periodic auto-discovery for external gateways unless a network change occurs.<br>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 Wi-Fi). 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** connect method, the GlobalProtect Credential Provider logon screen on Windows 10 endpoints now displays the pre-populated domain name below the editable username field. |

| Feature | Description of Change |
|---|---|
| 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:<br>• Cached single sign-on (SSO) passwords (when SSO is enabled)<br>• Cached GlobalProtect portal passwords<br>• Cached saved user passwords (when **Save User Credentials** is enabled)<br>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 (such as GlobalProtect app 4.1) supports. 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 Beta 7 release.

| Feature | Limitation |
|---|---|
| GlobalProtect app for Linux | Proxy connections are not supported with the GlobalProtect app for Linux. |

# GlobalProtect App 4.1 Beta Known Issues

The following table includes known issues in GlobalProtect App 4.1 Beta 7.

| Issue ID | Description |
|---|---|
| **GPC-5758** | When GlobalProtect app 4.1 on Windows and macOS endpoints connects to a gateway that is configured on a PAN-OS 8.0.x or earlier firewall, the app displays host information based on OPSWAT SDK V4 categories and values (on the **Host Profile** tab of the GlobalProtect Settings panel) but reports host information to the gateway based on OPSWAT SDK V3 categories and values. |
| **GPC-5614** | If you configure a custom **Authentication Message** for GlobalProtect portal or gateway login (**Network** > **GlobalProtect** > **Portals** or **Gateways** > *<portal-config>* or *<gateway-config>* > **Authentication** > *<client-authentication-config>*), the GlobalProtect status panel and sign-in prompt on Windows endpoints are unable to wrap non-breaking strings that are longer than the width of the authentication message display area (for example, **`credentials_for_Portal_Customized_Authentication_Message_test`**). This issue causes the GlobalProtect status panel and sign-in prompt to display a truncated authentication message. |
| **GPC-5382**<br>This issue is now resolved. See GlobalProtect App 4.1 Addressed Issues. | When users attempt to connect to the GlobalProtect app for Chrome OS using SAML single sign-on (SSO), the app intermittently fails to connect and displays the `Network Connection Error` message.<br>**Workaround**: Delete and re-add the user account, and then reboot the system. |
| **GPC-5381**<br>This issue is now resolved. See GlobalProtect App 4.1 Addressed Issues. | The GlobalProtect app for Chrome OS incorrectly displays the `VPN disconnected` notification message after users successfully authenticate and establish a connection to GlobalProtect using SAML single sign-on (SSO). |
| **GPC-5380**<br>This issue is now resolved. See GlobalProtect App 4.1 Addressed Issues. | After users authenticate and establish a connection to the GlobalProtect app for Chrome OS using SAML single sign-on (SSO), GlobalProtect is unable to reconnect automatically when users switch to a different Wi-Fi connection or turn the Wi-Fi connection off and on. |
| **GPC-5375**<br>This issue is now resolved. See GlobalProtect App 4.1 Addressed Issues. | After end users enter the wrong password at any User Access Control (UAC) prompt on Windows, the GlobalProtect Credential Provider displays in subsequent login attempts. |
| **GPC-5346** | When you connect to a Windows 10 endpoint using the Microsoft Remote Desktop Connection, you cannot authenticate and establish a connection to |

| Issue ID | Description |
|---|---|
| | GlobalProtect using single sign-on (SSO) because Remote Desktop Services (RDS)-which enables you to access and run application on the remote desktop-does not support SSO with non-native Windows credentials.<br>**Workaround**: If you initiate a remote desktop connection using credentials from the GlobalProtect Credential Provider, you must manually re-enter your credentials on the GlobalProtect Credential Provider logon screen (when prompted) to access the endpoint and establish the GlobalProtect connection. |
| **GPC-5217**<br>This issue is now resolved. See GlobalProtect App 4.1 Addressed Issues. | After excluding Webex video traffic from the VPN tunnel, Webex cannot connect to audio/video when GlobalProtect is connected to the gateway. |
| **GPC-5038**<br>This issue is now resolved. See GlobalProtect App 4.1 Addressed Issues. | If a user attempts to log in to a Windows 10 endpoint for the first time using the GlobalProtect Credential Provider, and their password has expired, the logon screen does not automatically trigger the password change workflow. |
| **GPC-5021**<br>This issue is now resolved. See GlobalProtect App 4.1 Addressed Issues. | The GlobalProtect app for Linux cannot connect to the GlobalProtect portal or gateway through a proxy connection. |
| **GPC-4856** | OPSWAT SDK is unable to detect the following **Anti-Malware** information for the HIP Match log details (**Monitor** > **Logs** > **HIP Match** > **<hip-match-log>**) of the Gatekeeper security feature on macOS endpoints:<br>• **Engine Version**<br>• **Definition Version**<br>• **Date**<br>• **Last Scanned** |
| **GPC-4837** | The GlobalProtect app for Windows 10 UWP does not allow you to change users.<br>**Workaround**: Reinstall the GlobalProtect app for Windows 10 UWP and configure it for a new user. |
| **PAN-90223**<br>This issue is now resolved. See GlobalProtect App 4.1 Addressed Issues. | The firewall cannot generate HIP Match reports because the **Disk Encryption** states and locations (**Objects** > **GlobalProtect** > **HIP Objects** > **<hip-object>**) are different between OPSWAT SDK V3 and OPSWAT SDK V4. OPSWAT SDK V3 uses state options such as **Full** and **None** but does not include any location options. OPSWAT SDK V4 uses state options such as **Encrypted** and **Not Encrypted** and location options such as **Physical** and **Virtual**. |

| Issue ID | Description |
|---|---|
| **PAN-89611** | The GlobalProtect App displays the `Your password could not be changed. Please contact the administrator.` error message when users that match the following conditions attempt to change their RADIUS or Active Directory (AD) password through the app:<br>• The user authenticates to the portal and gateway with a RADIUS server using the Protected Extensible Authentication Protocol Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MSCHAPv2).<br>• The user's password has expired, or an administrator requires a password change at the next login.<br>• The user does not have dial-in network access permissions in Active Directory.<br>Without dial-in network access permissions, users cannot connect to GlobalProtect. This causes the GlobalProtect app to trigger the error message every time a user attempts to change his or her password. However, if users enter their password information correctly, their passwords are updated in Active Directory even though the app still displays the error message.<br>**Workaround**: Enable Active Directory dial-in network access permissions for the user. |
| **PAN-89456**<br>This issue is now resolved. See GlobalProtect App 4.1 Addressed Issues. | When using PAN-OS 8.1.0 Beta 4, remote users are unable to change their RADIUS or Active Directory (AD) passwords on the GlobalProtect app if they are authenticated with a RADIUS server using the Protected Extensible Authentication Protocol Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MSCHAPv2). When users attempt to change their password, the following error message appears:<br>`Authentication failed: Invalid username or password.`<br>**Workaround**: Use this feature with PAN-OS 8.1.0 Beta 3. |
| **PAN-89202** | If you upgrade your firewall from PAN-OS 8.0.6 to PAN-OS 8.1, web applications are intermittently unreachable when end users open the applications from a Clientless VPN portal. |
| **PAN-85621**<br>This issue is now resolved. See GlobalProtect App 4.1 Addressed Issues. | When users try to connect to a portal or gateway using an Active Directory/Radius server for authentication and unsuccessfully change their password, GlobalProtect displays a generic authentication failure message instead of a more descriptive message indicating the password could not be changed. |

# GlobalProtect App 4.1 Beta Addressed Issues

The following table lists the issues that are addressed in GlobalProtect App 4.1 Beta 7.

| Issue ID | Description |
|---|---|
| GPC-5382 | Fixed an issue where the app intermittently failed to connect and displayed the `Network Connection Error` message when users attempted to connect to the GlobalProtect app for Chrome OS using SAML single sign-on (SSO). |
| GPC-5381 | Fixed an issue where the GlobalProtect app for Chrome OS incorrectly displayed the `VPN disconnected` notification message after users successfully authenticated and established a connection to GlobalProtect using SAML single sign-on (SSO). |
| GPC-5380 | Fixed an issue where after users authenticated and established a connection to the GlobalProtect app for Chrome OS using SAML single sign-on (SSO), GlobalProtect was unable to reconnect automatically when users switched to a different Wi-Fi connection or turned the Wi-Fi connection off and on. |
| GPC-5375 | Fixed an issue where after end users entered the wrong password at any User Access Control (UAC) prompt on Windows, the GlobalProtect Credential Provider displays in subsequent login attempts. |
| GPC-5217 | Fixed an issue where after excluding Webex video traffic from the VPN tunnel, Webex could not connect to audio/video when GlobalProtect was connected to the gateway. |
| GPC-5038 | Fixed an issue where the logon screen did not automatically trigger the password change workflow when users attempted to log in to a Windows 10 endpoint for the first time using the GlobalProtect Credential Provider, and their password expired. |
| GPC-5021 | Fixed an issue where the GlobalProtect app for Linux could not connect to the GlobalProtect portal or gateway through a proxy connection. |
| GPC-4271 | Fixed an issue where users could not connect to manual-only gateways for the first time using the **User-Logon (Always On)** connect method if all external gateways were manual-only. |
| PAN-90223 | Fixed an issue where the firewall could not generate HIP Match reports because the **Disk Encryption** states and locations (**Objects** > **GlobalProtect** > **HIP Objects** > **<hip-object>**) were different between OPSWAT SDK V3 and OPSWAT SDK V4. |
| PAN-89456 | Fixed an issue where remote users were unable to change their RADIUS or Active Directory (AD) passwords on the GlobalProtect app if they were authenticated with a RADIUS server using the Protected Extensible Authentication Protocol Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MSCHAPv2). When users attempted to change their password, the following error message appeared: |

| Issue ID | Description |
|---|---|
| | `Authentication failed: Invalid username or password.` |
| PAN-85621 | Fixed an issue where when users attempted to connect to a portal or gateway using an Active Directory/Radius server for authentication and unsuccessfully changed their password, GlobalProtect displayed a generic authentication failure message instead of a more descriptive message indicating that the password could not be changed. |

# Getting Help

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

- > Related Documentation
- > Requesting Beta Support

# Related Documentation

For more detailed information on how to use the GlobalProtect app, refer to the GlobalProtect App 4.1 New Feature Guide.

# Requesting Beta Support

To get support during the GlobalProtect app beta, visit the beta forum at:

https://live.paloaltonetworks.com/t5/Pine/ct-p/BetaPine.

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

February 15, 2018