FORTINET

# Release Notes

## FortiClient (macOS) 7.2.4

**FORTINET DOCUMENT LIBRARY**
https://docs.fortinet.com

**FORTINET VIDEO LIBRARY**
https://video.fortinet.com

**FORTINET BLOG**
https://blog.fortinet.com

**CUSTOMER SERVICE & SUPPORT**
https://support.fortinet.com

**FORTINET TRAINING & CERTIFICATION PROGRAM**
https://www.fortinet.com/training-certification

**FORTINET TRAINING INSTITUTE**
https://training.fortinet.com

**FORTIGUARD LABS**
https://www.fortiguard.com

**END USER LICENSE AGREEMENT**
https://www.fortinet.com/doc/legal/EULA.pdf

**FEEDBACK**
Email: techdoc@fortinet.com

March 04, 2024
FortiClient (macOS) 7.2.4 Release Notes
04-724-998652-20240304

# TABLE OF CONTENTS

# Change log

| Date | Change description |
|---|---|
| 2024-03-04 | Initial release. |
| | |

# Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (macOS) 7.2.4 build 0850.

This document includes the following sections:



Review all sections prior to installing FortiClient. For more information, see the *FortiClient Administration Guide*.

## Licensing

See Windows, macOS, and Linux endpoint licenses.

# Special notices

## Enabling full disk access

FortiClient (macOS) works properly only when you grant permissions to access the full disk in the *Security & Privacy* pane for the following services:

- fctservctl2
- FortiClient


The following lists the services and their folder locations:

- Fctservctl2: `/Library/Application\ Support/Fortinet/FortiClient/bin/`
- FortiClient (macOS) application: `/Applications/FortiClient.app`

# Activating system extensions

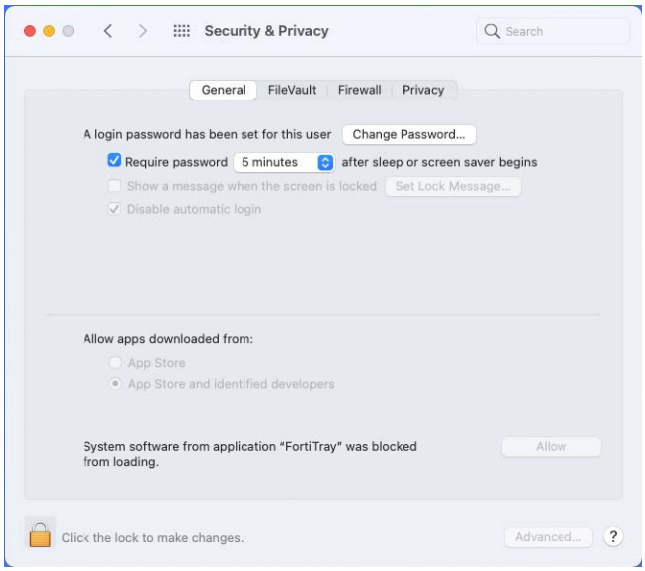
After you initially install FortiClient (macOS), the device prompts you to allow some settings and disk access for FortiClient (macOS) processes. You must have administrator credentials for the macOS machine to configure this change.

## VPN

VPN works properly only when you allow system software from Fortinet to load in *Security & Privacy* settings.

**To allow FortiTray to load:**

1. Go to *System Preferences* > *Security & Privacy*.
2. Click the *Allow* button beside *System software from application "FortiTray" was blocked from loading*.

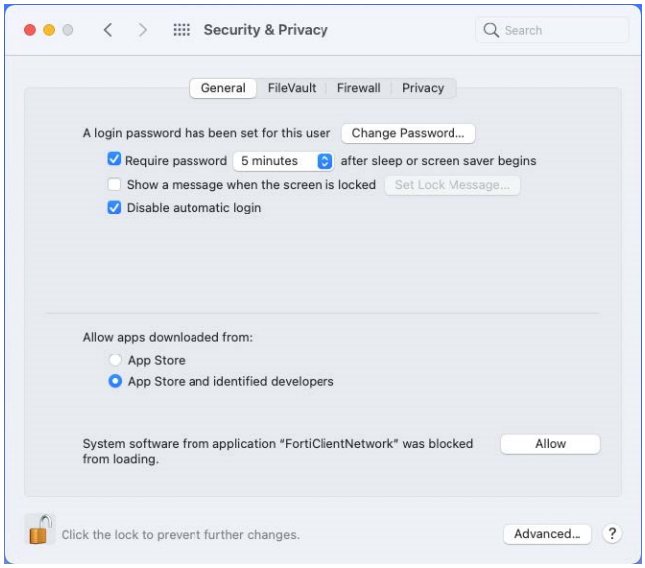



## Web Filter and Application Firewall

You must enable the FortiClientNetwork extension for Web Filter and Application Firewall to work properly. The FortiClient (macOS) team ID is AH4XFXJ7DK.

**To enable the FortiClientNetwork extension:**

1. Go to *System Preferences* > *Security & Privacy*.
2. Click the *Allow* button beside *System software from application "FortiClientNetwork" was blocked from loading*.




3. Verify the extension status by running `systemextensionsctl list` in the macOS terminal. The following provides example output when the extension is enabled:

```
[redacted]-Mac ~ % systemextensionsctl list
3 extension(s)
--- com.apple.system_extension.network_extension
enabled active  teamID  bundleID (version)      name    [state]
*       *       AH4XFXJ7DK      com.fortinet.forticlient.macos.webfilter (1.6.9/1)      FortiClientPacketFilter [activated enabled]
*       *       AH4XFXJ7DK      com.fortinet.forticlient.macos.vpn.nwextension (7.2.0/0652)     vpnprovider     [activated enabled]
*       *       AH4XFXJ7DK      com.fortinet.forticlient.macos.proxy (1.0.12/1)FortiClientProxy [activated enabled]
```

## Proxy mode extension

The com.fortinet.forticlient.macos.proxy system extension works as a proxy server to proxy a TCP connection. macOS manages the extension's connection status and other statistics. This resolves the issue that Web Filter fails to work when SSL and IPsec VPN are connected.

FortiClient (macOS) automatically installs the extension on an M1 Pro or newer macOS device.

# Enabling notifications

After initial installation, macOS prompts the user to enable FortiClient (macOS) notifications.

**To enable notifications:**

1. Go to *System Preferences* > *Notifications* > *FortiGuardAgent*.
2. Toggle *Allow Notifications* on.

## DHCP over IPsec VPN not supported

FortiClient (macOS) does not support DHCP over IPsec VPN.

## Running multiple FortiClient instances

FortiClient (macOS) does not support running multiple FortiClient instances for different users simultaneously.

## FortiGuard Web Filtering Category v10 Update

Fortinet has updated its web filtering categories to v10, which includes two new URL categories for AI chat and cryptocurrency websites. To use the new categories, customers must upgrade their Fortinet products to one of the versions below:

- FortiManager - Fixed in 6.0.12, 6.2.9, 6.4.7, 7.0.2, 7.2.0, 7.4.0.
- FortiOS - Fixed in 7.2.7 and 7.4.1.
- FortiClient - Fixed in Windows 7.2.3, macOS 7.2.3, Linux 7.2.3.
- FortiClient EMS - Fixed in 7.2.1.
- FortiMail - Fixed in 7.0.7, 7.2.5, 7.4.1.
- FortiProxy - Fixed in 7.4.1.

Please read the following CSB for more information to caveats on the usage in FortiManager and FortiOS:
https://support.fortinet.com/Information/Bulletin.aspx

# Installation information

## Firmware images and tools

The following files are available from the Fortinet support site:

| File | Description |
|---|---|
| FortiClientTools_7.2.4.0850_macosx.tar.gz | Includes utility tools and files to help with installation. |
| FortiClientVPNSetup_7.2.4.0850_macosx.dmg | Free VPN-only installer. |

The following files are available from Fortinet.com:

| File | Description |
|---|---|
| FortiClient_OnlineInstaller.dmg | Standard installer for macOS. |
| FortiClientVPNSetup_7.2.4.0850_macosx.dmg | Free VPN-only installer. |

FortiClient EMS 7.2.4 includes the FortiClient (macOS) 7.2.4 standard installer.

Review the following sections prior to installing FortiClient version 7.2.4: Introduction on page 6, Special notices on page 7, and Product integration and support on page 13.

## Upgrading from previous FortiClient versions

You must upgrade EMS to 7.2 or newer before upgrading FortiClient.

FortiClient 7.2.4 supports upgrade from FortiClient 6.2, 6.4, and 7.0.

FortiClient (macOS) 7.2.4 features are only enabled when connected to EMS 7.2.

See Recommended upgrade path for information on upgrading FortiClient (macOS) 7.2.4.

## Downgrading to previous versions

FortiClient 7.2.4 does not support downgrading to previous FortiClient versions.

# Uninstalling FortiClient

The EMS administrator may deploy uninstall to managed FortiClient (macOS) endpoints.

# Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal. After logging in, click on *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

# Product integration and support

The following table lists FortiClient (macOS) 7.2.4 product integration and support information:

| | |
|---|---|
| **Desktop operating systems** | • macOS Sonoma (version 14)<br>• macOS Ventura (version 13)<br>• macOS Monterey (version 12)<br>• macOS Big Sur (version 11) |
| **Minimum system requirements** | • Intel processor or M1 or M2 chip<br>• 1 GB of RAM<br>• 1 GB of free hard disk drive (HDD) space<br>• TCP/IP communication protocol<br>• Ethernet NIC for network connections<br>• Wireless adapter for wireless network connections<br>• Adobe Acrobat Reader for viewing FortiClient documentation |
| **AV engine** | • 6.00287 |
| **FortiClient EMS** | • 7.2.0 and later |
| **FortiOS** | The following versions support zero trust network access:<br>• 7.4.0 and later<br>• 7.2.0 and later<br>• 7.0.6 and later<br>The following versions support IPsec and SSL VPN:<br>• 7.4.0 and later<br>• 7.2.0 and later<br>• 7.0.0 and later<br>• 6.4.0 and later<br>• 6.2.0 and later<br>• 6.0.0 and later |
| **FortiAnalyzer** | • 7.4.0 and later<br>• 7.2.0 and later<br>• 7.0.0 and later |
| **FortiManager** | • 7.4.0 and later<br>• 7.2.0 and later<br>• 7.0.0 and later |
| **FortiSandbox** | • 4.4.0 and later<br>• 4.2.0 and later<br>• 4.0.0 and later<br>• 3.2.0 and later |
| **FortiAuthenticator** | • 6.5.0 and later<br>• 6.4.0 and later |

| | |
|---|---|
| | • 6.3.0 and later<br>• 6.2.0 and later<br>• 6.1.0 and later<br>• 6.0.0 and later |

# Language support

The following table lists FortiClient language support information:

| Language | GUI | XML configuration | Documentation |
|---|---|---|---|
| English | Yes | Yes | Yes |
| Chinese (simplified) | Yes | | |
| Chinese (traditional) | Yes | | |
| French (France) | Yes | | |
| German | Yes | | |
| Japanese | Yes | | |
| Korean | Yes | | |
| Portuguese (Brazil) | Yes | | |
| Russian | Yes | | |
| Spanish (Spain) | Yes | | |

The FortiClient language setting defaults to the regional language setting configured on the client workstation unless configured in the XML configuration file.

If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

# Resolved issues

The following issues have been fixed in FortiClient (macOS) 7.2.4. For inquiries about a particular bug, contact Customer Service & Support.

## Remote Access

| Bug ID | Description |
|---|---|
| 927712 | FortiClient (macOS) does not disable and hide always up when off-net-only autoconnect is enabled. |
| 951344 | VPN cannot recognize certificate with diacritics. |
| 954004 | FortiClient (macOS) cannot establish DTLS tunnel when handshake packet has a large MTU. |
| 966377 | FortiGate does not see zero trust network access tag for macOS users when connected to SSL VPN. |
| 966405 | With FortiGate `tunnel-connect-without-reauth` enabled and `auth-timeout` is reached, FortiClient (macOS) continues to reconnect to VPN and ask for token. |
| 971633 | SSL VPN fails with certificate authentication when certificate CN is in Chinese. |
| 977245 | FortiClient for macOS 13 fails to autoconnect when endpoint wakes from sleep. |
| 979780 | FortiTray crashes when user manually types FortiToken code from FortiToken Mobile for SSL VPN. |
| 981320 | SSL VPN tunnel disconnects when `off-net-only-autoconnect` is enabled and endpoint shifts from off- to on-net. |
| 981749 | FortiClient does not autoconnect to FortiSASE secure Internet access when it is off-Fabric. |
| 987457 | FortiOS tunnel timeout maximum value does not affect FortiClient. |
| 990135 | FortiClient fails to reconnect to SSL VPN after network disruption with FortiGate `tunnel-connect-without-reauth` enabled. |
| 999361 | FortiClient (macOS) *Remote Access* tab displays *SAML Login* button for VPN tunnels with SAML authentication while FortiClient (Windows) displays *Connect* button. |
| 999674 | IKEv2 connection fails with a *connection was terminated unexpectedly* error. |
| 1000591 | SSL VPN tunnel with `tunnel-connect-without-reauth` and always-up enabled fails to reconnect. |
| 1001252 | FortiClient (macOS) includes external browser single sign on toggle for IPsec VPN when it does not support it. |

## Logs

| Bug ID | Description |
|---|---|
| 987780 | FortiAnalyzer does not see logs from FortiClient (macOS). |

## Web Filter and plugin

| Bug ID | Description |
|---|---|
| 977148 | FortiClient does not use Web Filter rating URL provided using XML tag on EMS. |
| 962343 | FortiClient (macOS) does not block unrated sites when it cannot access FortiGuard servers. |

## Zero Trust telemetry

| Bug ID | Description |
|---|---|
| 930029 | FortiClient disconnects after reboot. |

# Known issues

The following issues have been identified in FortiClient (macOS) 7.2.4. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

## Application Firewall

| Bug ID | Description |
|---|---|
| 814391 | When connected to FortiClient Cloud, application signatures block allowlisted applications. |
| 834500 | FortiClient fails to block Application Firewall categories when web client category is set to monitor. |
| 834839 | Web Filter does not block traffic when proxy mode and Application Firewall are disabled. |
| 866711 | SSL VPN with SAML and FIDO2 authentication does not work with built-in browser. |
| 879985 | Application Firewall fails to block Web.Client category HTTPS traffic. |
| 943703 | Application firewall block/allow/monitor based on individual applications does not work as expected. |
| 948718 | Block count for Application Firewall is not accurate. |
| 957984 | Application Firewall reports violations for network service protocols when it is set to monitor in EMS. |
| 958651 | Application Firewall violation list shows violated programs as the same as applications, which is not as accurate as Windows. |
| 958651 | Application Firewall violation list shows violated programs as same as applications, which is not as accurate as Windows. |
| 986928 | FortiClient shows *Blocked (Unknown.Application)* notification every few minutes. |
| 1002892 | Application Firewall blocks OpenVPN when proxy category is set to *Monitor*. |

## Avatar and social login information

| Bug ID | Description |
|---|---|
| 777013 | Avatar, whether changed or existing, does not show on FortiAnalyzer. |
| 857857 | Avatar page goes blank if user logs in with LinkedIn account. |
| 878050 | Avatar does not update on FortiOS dashboards and FortiOS cannot show updated |

| Bug ID | Description |
|---|---|
| | information. |
| 954273 | After FortiClient upgrades through script, avatar page does not load properly and shows a blank page. |

## Configuration

| Bug ID | Description |
|---|---|
| 730415 | FortiClient (macOS) backs up configuration that is missing locally configured zero trust network access (ZTNA) connection rules. |

## Deployment and installers

| Bug ID | Description |
|---|---|
| 764672 | FortiClient (macOS) displays deployment popup for user when EMS admin configured unattended installation. |
| 882705 | EMS deployment fails if endpoint reboots during deployment package installation process. |
| 935387 | Installer downloaded from EMS is not deleted when EMS is changed. |
| 967007 | FortiClient (macOS) installed through mobile device management displays certificate trust prompt. |
| 981552 | Upgrade through installer from FortiClient (macOS) digital experience monitoring (DEM) to non-DEM build does not remove or stop DEM agent on endpoint. |

## Endpoint control

| Bug ID | Description |
|---|---|
| 958511 | FortiClient (macOS) does not support Microsoft Entra ID (formerly known as Azure Active Directory) verification when joining EMS. |
| 967008 | Revoking client certificate from EMS also revokes the EMS CA certificate, which causes unnecessary keychain prompt. |

## Endpoint management

| Bug ID | Description |
|---|---|
| 891264 | EMS creates duplicate records for domain-joined Ubuntu endpoints. |

## Endpoint policy and profile

| Bug ID | Description |
|---|---|
| 906951 | GUI does not reflect profile changes unless user manually restarts the FortiClient (macOS) console. |

## FSSOMA

| Bug ID | Description |
|---|---|
| 956538 | FortiClient (macOS) does not support multiple FortiAuthenticator server addresses. |

## GUI

| Bug ID | Description |
|---|---|
| 786779 | About page version infomation is cut off when displaying with copyright information. |
| 857148 | GUI shows duplicate FortiClient consoles. |
| 902595 | SAML prompt flashes on autoconnect. |
| 954876 | *Backup Comments* option does not work. |
| 967169 | GUI is stuck on blank screen. |
| 968068 | FortiClient responds slowly and shows blank page when opening GUI. |
| 971233 | FortiClient does not have GUI option to clear internal browser cookies. |
| 1003447 | *-1* and *-2* display under the Web Filter violation list category column for unknown and denylisted URLs. |

## Installation and upgrade

| Bug ID | Description |
|---|---|
| 827939 | *FortiTray is not open anymore* prompt shows when deploying FortiClient using script through mobile device management. |
| 828781 | FortiClient (macOS) behaves inconsistently when uninstalling it through commands in terminal and the FortiClientUninstaller GUI tool. |
| 929219 | FortiClient is upgradable from full to free version. |
| 951945 | Uninstaller shows *Install Now* prompt instead of *Remove now*. |
| 955448 | Manual upgrade from 7.2.0 removes manually added VPN tunnels. |
| 976951 | FortiClient allows downgrade from full to free VPN-only client, which results in disordered GUI. |

## License

| Bug ID | Description |
|---|---|
| 889767 | License expiration shows unwanted +0000 at end of warning message. |

## Logs

| Bug ID | Description |
|---|---|
| 711763 | FortiClient does not point to usfgd1.fortigate.com for EMS web profile setting:Location-US \| Server-Fortiguard (Legacy). |
| 716803 | When logged in as domain user, avatar does not show properly on FortiAnalyzer 7.0. |
| 742124 | Sandbox events are not replicated on FortiAnalyzer. |
| 872875 | Disabling *Client-Based Logging When On-Fabric* in EMS does not work for macOS endpoints. |
| 951917 | The device MAC address field for FortiClient (macOS)-related events under FortiAnalyzer shows 00:00:00:00:00:00 instead of device MAC address. |
| 998917 | FortiClient fails to report security events to FortiAnalyzer Cloud. |
| 1002118 | fctlogupload causes CPU to spike to 100%. |

## Malware Protection and Sandbox

| Bug ID | Description |
|---|---|
| 551282 | Sandbox exception for trusted sources does not work and FortiClient (macOS) uploads files sourced from Apple Inc. |
| 719920 | FortiClient cannot submit files downloaded from Thunderbird to FortiClient Cloud Sandbox (PaaS). |
| 755198 | FortiClient (macOS) does not submit files downloaded using Edge to Sandbox or Sandbox Cloud. |
| 829415 | When next generation antivirus is enabled, FortiClient (macOS) shows real time protection (RTP) as disabled. |
| 837638 | Identifying malware and exploits using signatures received from FortiSandbox does not work. |
| 855555 | Enabling real-time protection and setting `<block_removable_media>` to `1` causes FortiClient (macOS) to fail to block a USB device. |
| 855570 | Real-time protection (RTP) scans files regardless of the maximum file size setting for scanning files. |
| 888356 | User can stop AV quick/full scan triggered from EMS. |
| 921370 | User cannot stop manually triggered AV scan in FortiClient. |
| 949187 | Cloud Sandbox fails to work and treats EICAR file as clean. |
| 949258 | GUI shows no events under *Realtime Protection events*. |
| 951380 | RTP creates folder when Word and Excel files are saved on network shared drive (NAS). |
| 961542 | Enabling Sandbox freezes system. |
| 995835 | Files submitted to Sandbox intermittently timing out. |
| 1000935 | Sandbox feature *Deny Access to File When There is No Sandbox Result* does not work properly. |

## Onboarding

| Bug ID | Description |
|---|---|
| 811976 | FortiClient (macOS) may prioritize using user information from authentication user registered to EMS. |
| 872136 | User verification period option under User verification does not work as configured. |

## Quarantine management

| Bug ID | Description |
|---|---|
| 868798 | Custom quarantine message does not work. |

## Remote Access

| Bug ID | Description |
|---|---|
| 720236 | FortiClient (macOS) does not support DH groups 19-21. |
| 738425 | SSL VPN GUI and tray have mismatch in unity features. |
| 772247 | SAML authentication times out with SSL VPN. |
| 800529 | GUI has issue with *Settings* > *VPN Options* > *Do not Warn Invalid Server Certificate*. |
| 821660 | FortiClient (macOS) behaves inconsistently with LDAP user login and autoconnect. |
| 833001 | When using FortiAuthenticator as SAML identity provider, autoconnect fails after user logout/relogin. |
| 834198 | On an AWS virtual machine, autoconnect does not work and FortiClient displays an *Initialize VPN system extension was failed* error. |
| 835096 | FortiClient (macOS) cannot establish SAML single sign on VPN after Wi-Fi drops or disconnects and user reconnects manually. |
| 837391 | FortiClient does not send public IP address for SAML, which leads to 0.0.0.0 displaying on FortiOS and FortiSASE. |
| 851600 | SSL VPN connection fails with FQDN resolving to multiple IP addresses when FortiClient (macOS) cannot reach resolved IP address. |
| 854265 | SSL VPN connects after sleep. |
| 864515 | Endpoint fails to receive packets from FortiGate over IPsec VPN tunnel on macOS guest VM using bridged network connection. |
| 866971 | *System Preferences* for FortiClient (macOS) network extension is under different name compared to 7.0.7. |
| 870585 | When using Okta for SAML VPN authentication, saving password and autoconnect fail to work. |
| 893237 | FortiClient (macOS) does not provide chance to reinput password during autoconnect after identity provider password change. |
| 894027 | FortiClient on macOS Ventura system proxy with proxy autoconfiguration file does not work with IPsec VPN, but works with SSL VPN. |
| 898971 | SSL VPN with SAML drops with *Login error. Remote denied the request.* error. |

| Bug ID | Description |
|---|---|
| 917898 | Host check policy works as AND operation instead of OR operation. |
| 920908 | IPsec VPN password renew prompt differs from SSL VPN prompt. |
| 921191 | After VPN is up, FortiClient (macOS) fails to access internal websites. |
| 929577 | Resilient SSL VPN connection fails after VPN is up and the first gateway goes down. |
| 941513 | *DH Group* option is mandatory when PFS is disabled. |
| 944870 | FortiClient on macOS Ventura breaks DNS when connected to VPN after short period of time. |
| 948566 | Enabling local LAN option does not work as expected. |
| 952987 | FortiClient (macOS) does not clear IPsec VPN tunnel saved password if connection fails due to wrong credentials. |
| 954632 | IPsec VPN fails to update password in keychain store when trying to renew expired AD password with autoconnect enabled. |
| 961800 | When zero trust network access is enabled, pfctl rules affect DNS traffic. |
| 963586 | SSL VPN does not support network lockdown. |
| 967173 | Monterey - Sonoma system proxy does not work with IPsec VPN. |
| 968070 | FortiClient (macOS) does not parse `<disallow_invalid_server_certificate>` attribute. |
| 970489 | Application Firewall decreases Internet speed when connecting to IPsec VPN. |
| 972089 | VPN is stuck at 98% when connected to iPhone hotspot. |
| 974123 | VPN does not automatically disconnect when secure compliance is enforced after host tag has been removed or mismatched. |
| 975879 | IPsec VPN phase 2 setting NO PFS should not configure/show the DH groups for phase 2. |
| 976220 | FortiClient (macOS) does not warn user before starting to connect if user provided empty username and/or password. |
| 976852 | IPsec VPN redundancy based on ping speed or TCP RTT sorting method does not work. |
| 977725 | FortiClient split tunnel has limitation. |
| 978147 | DHCP option 12 - hostname needed in the scenario of SSL VPN with external DHCP servers. |
| 978270 | DNS fails to apply to IPsec VPN tunnel interface after disabling mode_config in IPsec VPN IKEv1 and setting manual mode. |
| 978321 | FortiToken input prompt GUI shows *Password* instead of *FortiToken Code* for IPsec VPN IKEv2 tunnel. |
| 978792 | GUI is stuck in VPN connecting page when VPN is connected. |
| 979345 | FortiClient stays connected to IPsec VPN IKEv2 tunnel despite DH group mismatch in phase 2. |
| 982319 | For IPsec VPN phase2, GUI does not support selecting multiple DH groups. |

| Bug ID | Description |
|---|---|
| 982354 | DH group module size compatibility needs enhancement for improved IPsec VPN security. |
| 984150 | SAML login window does not appear on the first attempt after clicking *Disconnect*. |
| 985070 | SSL VPN connection with SAML and Keycloak redirect does not close but connection is up. |
| 985277 | Split tunnel VPN macOS client does not connect to local LAN. |
| 987299 | Multifactor authentication prompt does not show for external RADIUS users with token authentication enabled. |
| 998022 | Split DNS implementation is ineffective in SSL VPN tunneling. |
| 999205 | FortiClient (macOS) allows users to accept invalid certificate and internal browser does not inform user of invalid certificate. |
| 999358 | FortiClient does not hide *Save Password*, *Always up*, and *Auto-connect* checkboxes when disallowed in EMS Remote Access profile. |
| 1000595 | User cannot disable SAML authentication in personally created IPsec VPN tunnel. |

## Software Inventory

| Bug ID | Description |
|---|---|
| 737970 | Software Inventory may not properly reflect software changes (adding/deleting) on macOS endpoints. |
| 860954 | Sending software inventory list or updates to EMS does not happen in real time. |

## Vulnerability Scan

| Bug ID | Description |
|---|---|
| 771833 | FortiClient tags endpoint as vulnerable when EMS administrator has enabled *Exclude Application Vulnerabilities Requiring Manual Update from Vulnerability*. |

## Web Filter and plugin

| Bug ID | Description |
|---|---|
| 873803 | In-browser message does not show after switching device user without system reboot. |

| Bug ID | Description |
|---|---|
| 875298 | Exclusion list does not work properly with regular expressions. |
| 878055 | Web access does not work. |
| 898303 | Web Filter does not work when administrator pushes extensions through Jamf in mobile device management platform. |
| 918616 | Video meetings have lag. |
| 937125 | Ping drops when clicking *About* to update signature. |
| 950119 | FortiClient (macOS) does not include ability to sign certificate for Web Filter. |
| 955529 | Teams and other applications that use video crash and fail to work. |
| 971067 | FortiClient with Web Filter enabled does not allow login to Netflix account. |
| 998541 | Web Filter on *Only when Endpoint is Off-Fabric* does not work properly. |
| 1002798 | Web Filter (proxy) prevents webpage elements from loading. |

## Zero Trust tags

| Bug ID | Description |
|---|---|
| 794385 | FortiClient detects third-party antivirus tag. |

## Zero Trust Telemetry

| Bug ID | Description |
|---|---|
| 951597 | If the endpoint is bound to Active Directory, FortiClient (macOS) does not sync with EMS while on VPN. |

## ZTNA connection rules

| Bug ID | Description |
|---|---|
| 853281 | FortiClient (macOS) does not show the inline CASB database signatures on the *About* page. |
| 857909 | FortiClient (macOS) does not support enabling encryption for ZTNA TCP forwarding rules acquired form ZTNA service portal. |

| Bug ID | Description |
|---|---|
| 857999 | FortiClient does not support using external browser for SAML authentication for ZTNA rules acquired through service portal. |
| 862921 | FortiClient does not show prompt for ZTNA  user authentication when form-based method is set under authentication rule/scheme on FortiGate. |
| 864821 | ZTNA does not have proper logging for SaaS portals. |
| 905880 | ZTNA certificate prompt displays when deploying FortiClient (macOS) with Jamf Pro configuration profiles.<br>**Workaround:** enable ZTNA in both on-fabric and off-fabric profile if using both. |
| 938962 | FortiClient keeps prompting *ztagent wants to sign using key Imported Private Key* when selecting *Always trust*. |
| 975845 | FortiClient (macOS) does not notify end user that certificate is not trusted for ZTNA connection when `<disallow_invalid_server_certificate>` is enabled. |

## Other

| Bug ID | Description |
|---|---|
| 950099 | Non-admin users cannot trust new Web Filter certificate generated in the system keychain. |

www.fortinet.com