FORTINET

Release Notes

FortiClient (macOS) 7.2.7

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

December 12, 2024
FortiClient (macOS) 7.2.7 Release Notes
04-727-1099388-20241212

TABLE OF CONTENTS

Change log

Date	Change description
2024-12-12	Initial release.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (macOS) 7.2.7 build 0976.

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

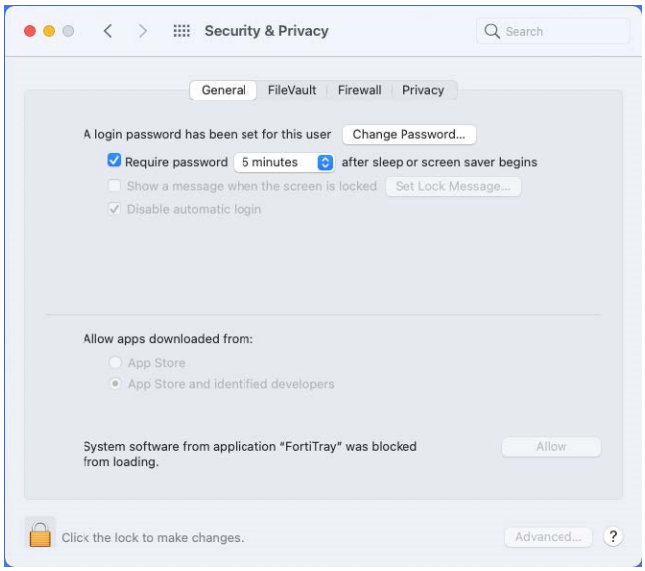
After you initially install FortiClient (macOS), the device prompts you to allow some settings and disk access for FortiClient (macOS) processes. You must have administrator credentials for the macOS machine to configure this change.

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*.

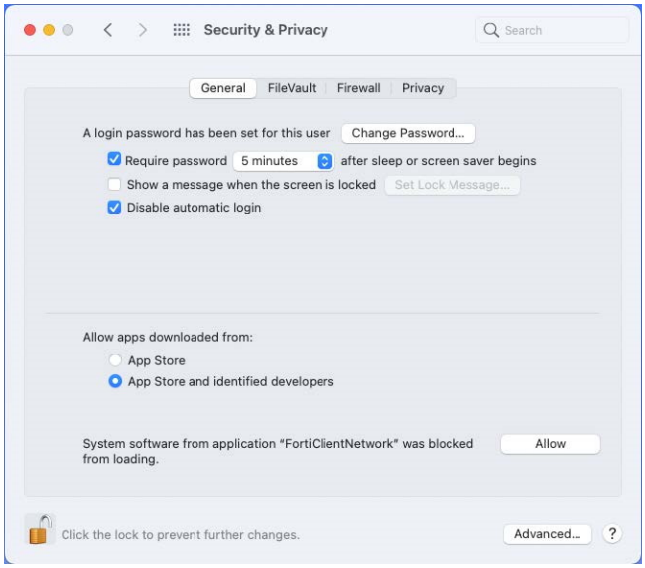


Web Filter and Application Firewall

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 following versions:

- FortiManager - Fixed in 6.0.12, 6.2.9, 6.4.7, 7.0.2, 7.2.0, 7.4.0.
- FortiOS - Fixed in 7.2.8 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

IPsec VPN support limitation

Due to a macOS limitation, FortiClient (macOS) does not support IPsec VPN tunnels on macOS Guest VMs using bridged network connections.

SSL VPN support limitation

SSL VPN with SAML FIDO2 authentication only supports external browser authentication.

Installation information

Firmware images and tools

The following files are available from the Fortinet support site:

File	Description
FortiClientTools_7.2.7.0976_macosx.tar.gz	Includes utility tools and files to help with installation.
FortiClientVPNSetup_7.2.7.0976_macosx.dmg	Free VPN-only installer.

The following files are available from Fortinet.com:

File	Description
FortiClient_OnlineInstaller.dmg	Standard installer for macOS.
FortiClientVPNSetup_7.2.7.0976_macosx.dmg	Free VPN-only installer.

FortiClient EMS 7.2.7 includes the FortiClient (macOS) 7.2.7 standard installer.

Review the following sections prior to installing FortiClient version 7.2.7: 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 7.2.7 supports upgrade from FortiClient 6.2, 6.4, and 7.0.

FortiClient (macOS) 7.2.7 features are only enabled when connected to EMS 7.2.

See Recommended upgrade path for information on upgrading FortiClient (macOS) 7.2.7.

Downgrading to previous versions

FortiClient 7.2.7 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) 7.2.7 product integration and support information:

Desktop operating systems	• macOS Sequoia (version 15) • macOS Sonoma (version 14) • macOS Ventura (version 13) • macOS Monterey (version 12)
Minimum system requirements	• Intel processor or M1 or M2 chip • 1 GB of RAM • 1 GB of free hard disk drive (HDD) space • TCP/IP communication protocol • Ethernet NIC for network connections • Wireless adapter for wireless network connections • Adobe Acrobat Reader for viewing FortiClient documentation
AV engine	• 6.00287
FortiAnalyzer	• 7.4.0 and later • 7.2.0 and later • 7.0.0 and later
FortiAuthenticator	• 6.5.0 and later • 6.4.0 and later • 6.3.0 and later • 6.2.0 and later • 6.1.0 and later • 6.0.0 and later
FortiClient EMS	• 7.4.0 and later • 7.2.0 and later
FortiOS	The following versions support zero trust network access: • 7.4.0 and later • 7.2.0 and later • 7.0.6 and later The following versions support IPsec and SSL VPN: • 7.4.0 and later • 7.2.0 and later • 7.0.0 and later • 6.4.0 and later
FortiManager	• 7.4.0 and later • 7.2.0 and later • 7.0.0 and later
FortiMonitor agent	2024.2.10

FortiSandbox	• 4.4.0 and later • 4.2.0 and later • 4.0.0 and later • 3.2.0 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.

Conflict with third-party endpoint protection software

As a Fortinet Fabric Agent that provides protection, compliance, and secure access, FortiClient may conflict with anti-malware products on the market that provide similar AV, web filtering, application firewall, and ransomware protection features as FortiClient. If you encounter a conflict, there are a few steps you can take to address it:

- Do not use other AV products when FortiClient's AV feature is enabled.
- If FortiClient's AV feature is disabled, configure the third party AV product to exclude the FortiClient installation folder from being scanned.

During a new FortiClient installation, the installer searches for other registered third party software and, if it finds any, warns users to uninstall them before proceeding with the installation. There is also an option to disable FortiClient real time protection.

Resolved issues

The following issues have been fixed in FortiClient (macOS) 7.2.7. For inquiries about a particular bug, contact Customer Service & Support.

Endpoint control

Bug ID	Description
1031812	User can turn off autoconnect on FortiClient when it is pushed from EMS.
1035687	Setting *Action* for EMS invalid certificates as *Warn*, then *Deny* does not work as expected.

Install and upgrade

Bug ID	Description
975336	Deployment fails if installer has space in name.

Logs

Bug ID	Description
750703	IPsec and SSL VPN events are not logged on FortiAnalyzer correctly.

Remote Access

Bug ID	Description
1075772	VPN Unity features are not consistent with FortiClient (Windows).

Remote Access - SSL VPN

Bug ID	Description
1089916	Horizontal scaled instance with realm configuration does not connect on macOS but can connect on Windows.
1102807	SAML authentication popup has issue if the operating system is not in English.

Known issues

Known issues are organized into the following categories:

To inquire about a particular bug or to report a bug, contact Customer Service & Support.

New known issues

No new issues have been identified in version 7.2.7.

Existing known issues

The following issues have been identified in a previous version of FortiClient (macOS) and remain in FortiClient (macOS) 7.2.7.

Application Firewall

Bug ID	Description
834839	Web Filter does not block traffic when proxy mode and Application Firewall are disabled.
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.

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.
954273	After FortiClient upgrades through script, avatar page does not load properly and shows a blank page.

Deployment and installers

Bug ID	Description
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.
975804	*FortiClientUninstaller is damaged* error occurs during FortiClient (macOS) deployment.

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.
1029889	ffconfig leaves behind zombie processes.

Endpoint management

Bug ID	Description
891264	EMS creates duplicate records for domain-joined Ubuntu endpoints.
1106089	FortiClient fails to open with syntax error prompt if compliance.json file is empty.

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.
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.

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).
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.
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).
829415	When next generation antivirus is enabled, FortiClient (macOS) shows real time protection (RTP) as disabled.
855555	Enabling real-time protection and setting `<block_removable_media>` to `1` causes FortiClient (macOS) to fail to block a USB device.
921370	User cannot stop manually triggered AV scan in FortiClient.
949187	Cloud Sandbox fails to work and treats EICAR file as clean.

Quarantine management

Bug ID	Description
868798	Custom quarantine message does not work.

Remote Access

Bug ID	Description
800529	GUI has issue with *Settings* > *VPN Options* > *Do not Warn Invalid Server Certificate*.
818359	FortiClient (macOS) does not instantly clear saved password when user deselects *Save Password* for VPN tunnel.
866971	*System Preferences* for FortiClient (macOS) network extension is under different name compared to 7.0.7.
977725	FortiClient split tunnel has limitation.

Remote Access - IPsec VPN

Bug ID	Description
720236	FortiClient does not support DH groups 19-21.
894027	FortiClient on macOS Ventura system proxy with PAC does not work with IPsec VPN but works with SSL VPN.
948566	*Enable Local LAN* does not work as expected.

Bug ID	Description
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.
975879	IPsec VPN phase 2 setting NO PFS configures or shows the DH groups for phase 2.
976852	IPsec VPN redundancy based on ping speed or TCP RTT sorting method does not work.
978270	DNS fails to apply to the IPsec VPN tunnel interface after disabling `<mode_config>` in IPsec VPN IKEv1 and setting manual mode.
987299	Multifactor authentication prompt does not show for external RADIUS users with token authentication enabled.

Remote Access - SSL VPN

Bug ID	Description
772247	SAML authentication times out with SSL VPN.
854265	SSL VPN connects after sleep.
866711	SSL VPN with SAML and FIDO2 authentication does not work with built-in browser.
870585	When using Okta for SAML VPN authentication, saving password and autoconnect fail to work.
898971	SSL VPN with SAML drops with *Login error. Remote denied the request.* error.
978147	DHCP Option 12 - hostname needed if using SSL VPN with external DHCP servers.
978792	GUI is stuck in VPN connecting page when VPN connected successfully.
985277	When connected to a split tunnel VPN, FortiClient (macOS) does not connect to local LAN.

Software Inventory

Bug ID	Description
860954	Sending software inventory list or updates to EMS does not happen in real time.

Third-party compatibility

Bug ID	Description
961542	Conflict occurs between FortiClient and Microsoft Defender due to the system processes used in overlapping real-time protection features.

Bug ID	Description
	Workaround: enable passive mode on Microsoft Defender.
1085782	Cisco Umbrella does not work when ZTNA is enabled.

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.
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.
950119	FortiClient (macOS) does not have the 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.
1019409	Web Filter HTTP mode does not work properly.
1022664	When FortiClient (macOS) blocks all Web Filter categories, exclusions do not work properly.
1026797	Web Filter *Proceed* button does not work properly.

Real-time protection

Bug ID	Description
855570	RTP scans files regardless of the maximum file size setting for scanning files.
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).

Zero Trust tags

Bug ID	Description
794385	FortiClient (macOS) detects third party antivirus tag.

ZTNA connection rules

Bug ID	Description
807827	FortiClient is missing external browser support for SAML authentication for ZTNA.
853281	FortiClient (macOS) does not show the inline CASB database signatures on the *About* page.
864821	ZTNA does not have proper logging for SaaS portals.
905880	ZTNA certificate prompt displays when deploying FortiClient with Jamf Pro configuration profiles. **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*.
961800	When ZTNA is enabled, pfctl rules affect DNS traffic.
994025	ZTNA fails to work when no port number is specified on the destination rule.
1032986	ZTNA destination-based SMB drive access fails to load for the first time when authentication is enabled.
1094278	ZTNA fails to process when destination rule is configured with port range.
1099562	ZTNA wildcard FQDN fails to work.

Numbering conventions

Fortinet uses the following version number format:

<First number>.<Second number>.<Third number>.<Fourth number>

Example: 7.2.7.15

- First number = major version
- Second number = minor version
- Third number = maintenance version
- Fourth number = build version

Release Notes pertain to a certain version of the product. Release Notes are revised as needed.

www.fortinet.com