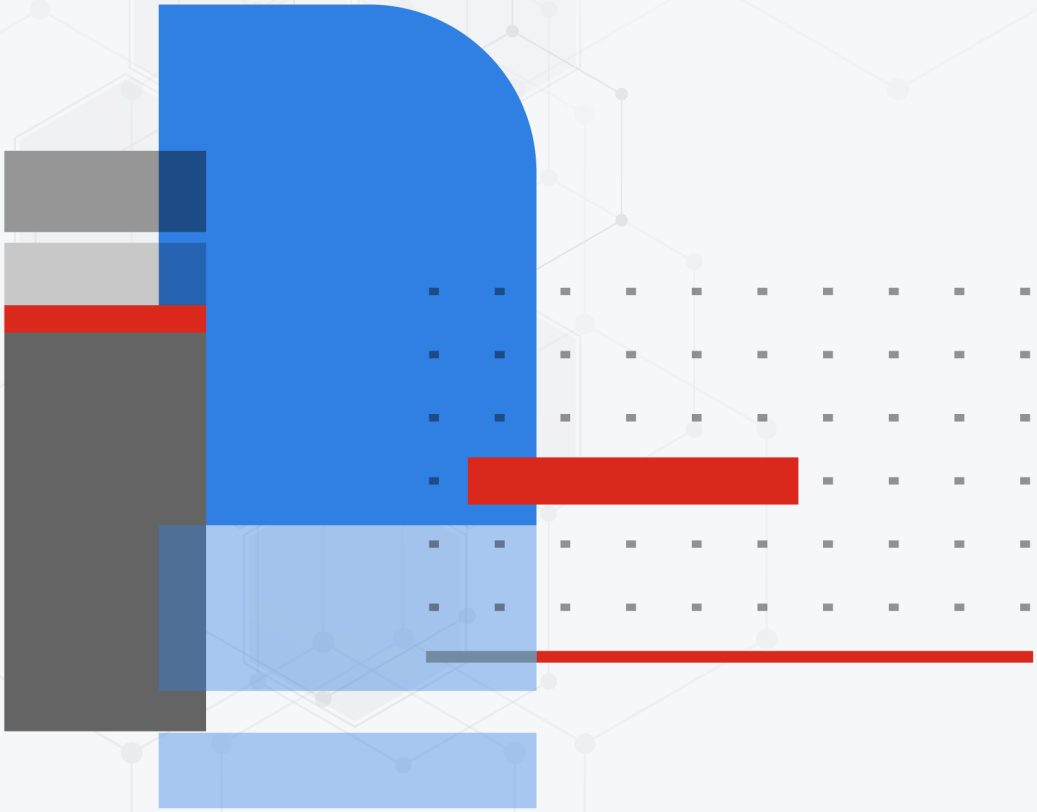
Release Notes

FortiClient (macOS) 7.4.3



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 15, 2025
FortiClient (macOS) 7.4.3 Release Notes
04-743-1105662-20251215

TABLE OF CONTENTS

Change log

Date	Change description
2025-03-20	Initial release.
2025-03-26	Updated Product integration and support on page 13.
2025-04-01	Updated Special notices on page 6.
2025-04-21	Added Common Vulnerabilities and Exposures on page 17.
2025-05-13	Updated Common Vulnerabilities and Exposures on page 17.
2025-05-20	Updated Activating system extensions on page 7.
2025-05-28	Updated Product integration and support on page 13.
2025-12-15	Added FortiClient (macOS) 7.4.3 free VPN-only agent GA update 1 on page 6.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (macOS) 7.4.3 build 1761.

This document includes the following sections:

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

Fortinet uses the following version number format:

<Major version number>.<minor version number>.<patch number>.<build number>

Example: 7.4.3.1761

Release Notes correspond to a certain version and build number of the product.

Licensing

See Windows, macOS, and Linux endpoint licenses.

Special notices

FortiClient (macOS) 7.4.3 free VPN-only agent GA update 1

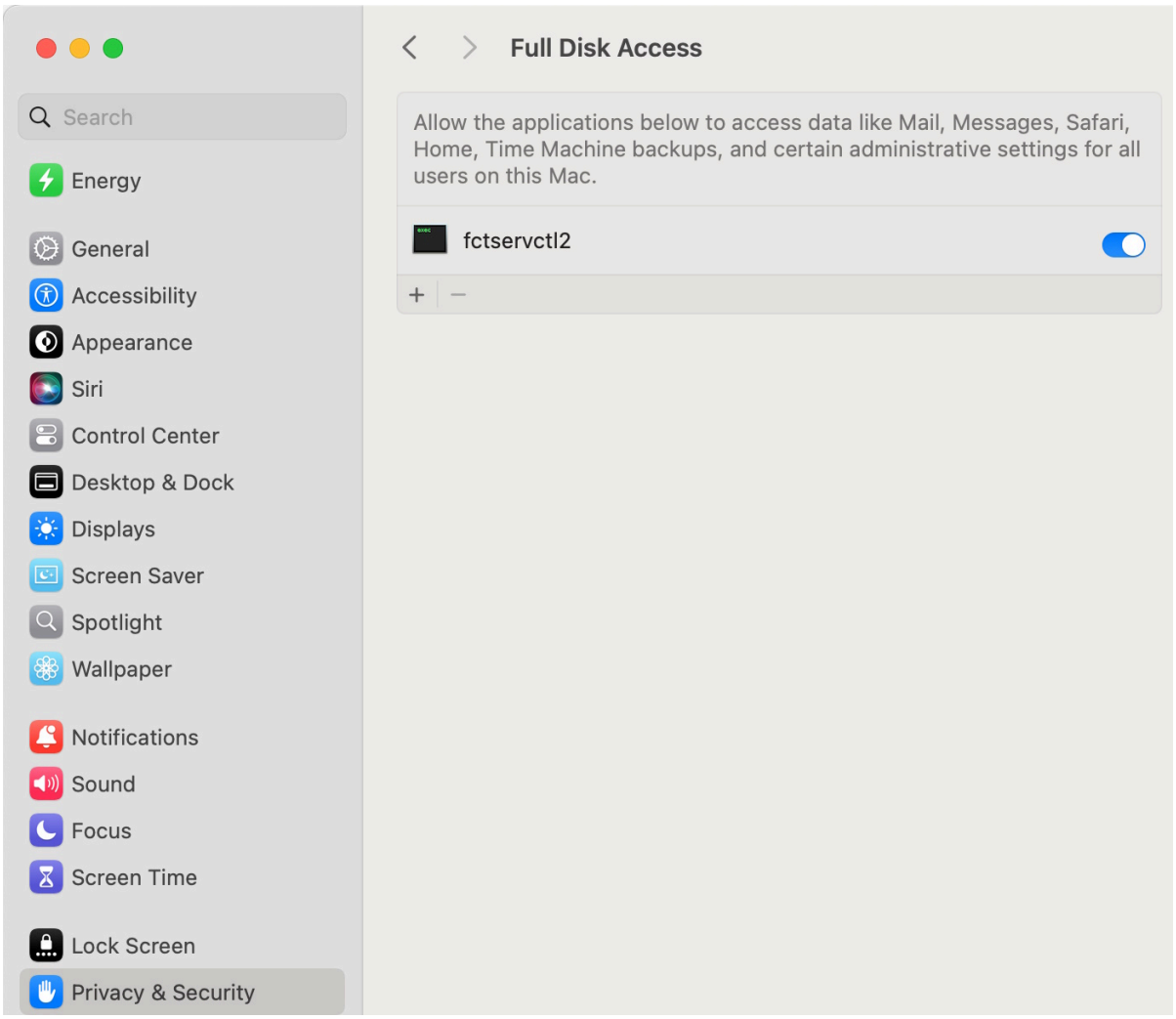
FortiClient (macOS) 7.4.3 free VPN-only agent GA update 1 (7.4.3.6667) was released on December 15, 2025 to address the following vulnerabilities:

Bug ID	Description
1188353	CVE-2025-57741
1125778	CVE-2025-31365
1133162	CVE-2025-46774

To install the update, download the latest FortiClient VPN-only agent installation file for macOS from FortiClient.com and double-click it to complete the installation. To verify the installation is successful, make sure the FortiClient version is *7.4.3.6667* in the *About* page of the FortiClient GUI.

Enabling full disk access

FortiClient works properly only when you grant permissions to access the full disk in the *Security & Privacy* pane for the fctservctl2 service. You can find this service in `/Library/Application\ Support/Fortinet/FortiClient/bin/`.



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.

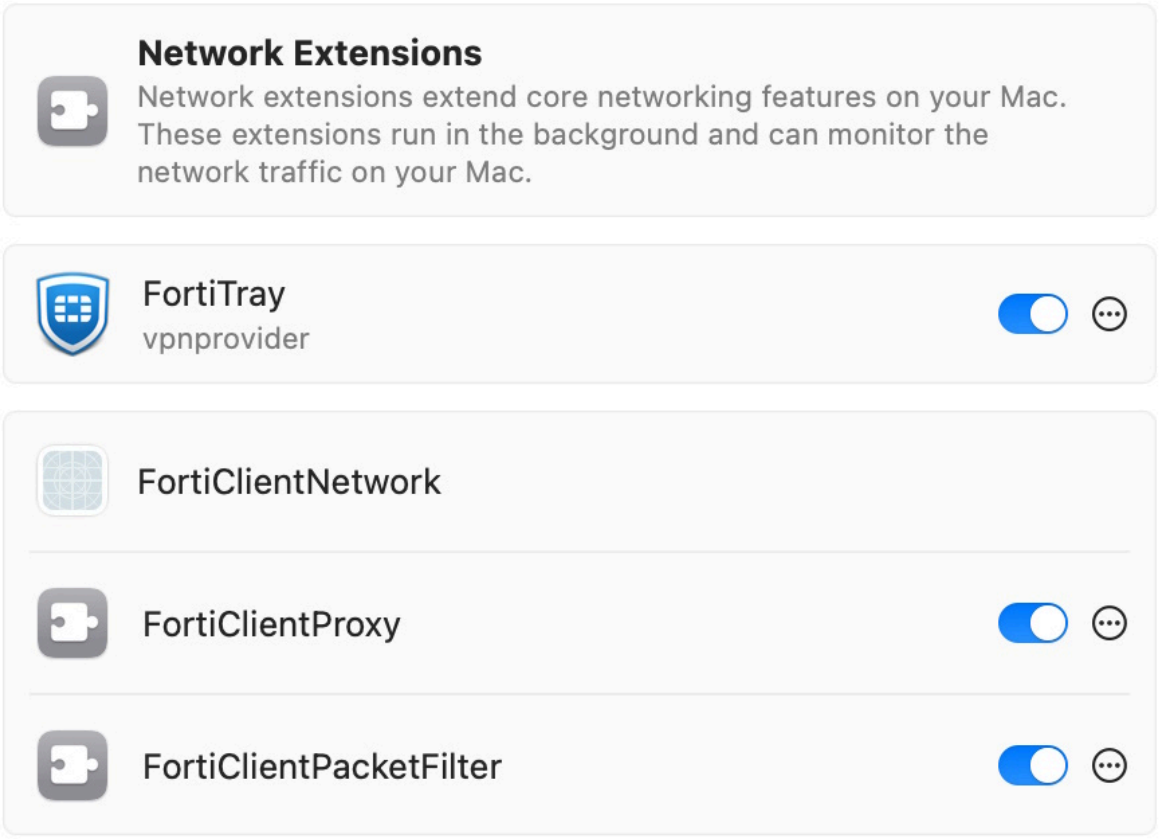
VPN works properly only when you allow FortiTray to load in *Network Extensions* settings. You must enable the FortiClientProxy and FortiClientPacketFilter extensions for Web Filter and Application Firewall, respectively, to work properly. The FortiClient (macOS) team ID is AH4XFXJ7DK.

The following provides instructions for macOS Sequoia (version 15).

For macOS Sonoma (version 14) and older, there is no *Network Extensions* section. You must click *Some system software requires your attention before it can be used*. You can then activate the extensions in *Privacy & Security* settings after the FortiClient prompts redirect you there.

To activate system extensions:

1. Go to *System Settings* > *General* > *Login Items & Extensions* > *Network Extensions*.
2. Toggle on the following to enable the extensions:
   - *FortiTray*
   - *FortiClientProxy*
   - *FortiClientPacketFilter*



3. Click *Done*.

Enabling notifications

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

To enable notifications:

1. Go to *System Settings* > *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, macOS Guest VMs using bridged network connections do not support IPsec VPN tunnels.

What’s new in FortiClient (macOS) 7.4.3

For information about what's new in FortiClient 7.4.3, see the FortiClient & FortiClient EMS 7.4 New Features Guide.

Installation information

Firmware images and tools

The following files are available from the Fortinet support site:

File	Description
FortiClientTools_7.4.3.1761_macosx.tar.gz	Includes utility tools and files to help with installation.
FortiClientVPNSetup_7.4.3.1761_macosx.dmg	Free VPN-only installer.

The following files are available from Fortinet.com:

File	Description
FortiClient_OnlineInstaller.dmg	Standard installer for macOS.
FortiClientVPNSetup_7.4.3.1761_macosx.dmg	Free VPN-only installer.

FortiClient EMS 7.4.3 includes the FortiClient (macOS) 7.4.3 standard installer.

Review the following sections prior to installing FortiClient version 7.4.3: Introduction on page 5, Special notices on page 6, and Product integration and support on page 13.

Upgrading from previous FortiClient versions

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

FortiClient 7.4.3 supports upgrade from FortiClient 6.4 and 7.0.

FortiClient (macOS) 7.4.3 features are only enabled when connected to EMS 7.2 and later.

See Recommended upgrade path for information on upgrading FortiClient (macOS) 7.4.3.

Downgrading to previous versions

FortiClient 7.4.3 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) 7.4.3 product integration and support information:

Desktop operating systems	• macOS Sequoia (version 15) • macOS Sonoma (version 14) • macOS Ventura (version 13)
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
FortiClient EMS	• 7.4.0 and later • 7.2.0 and later
FortiOS	• 7.6.0 and later. FortiOS 7.6.3 and later versions do not support SSL VPN tunnel mode. See Migrating from SSL VPN tunnel mode to IPsec VPN. • 7.4.0 and later • 7.2.0 and later • 7.0.0 and later • 6.4.0 and later
AV engine	7.0.38
IPS engine	7.6.1040
FortiEDR for macOS	6.0.9.1028
FortiAnalyzer	• 7.6.0 and later • 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
FortiManager	• 7.6.0 and later • 7.4.0 and later • 7.2.0 and later • 7.0.0 and later
FortiSandbox	• 4.4.0 and later • 4.2.0 and later • 4.0.0 and later

Language support

The following table lists FortiClient language support information:

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

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) 7.4.3. For inquiries about a particular bug, contact Customer Service & Support.

Endpoint control

Bug ID	Description
1031812	User can turn off autoconnect on FortiClient when setting is pushed from EMS.
1100661	FortiClient (macOS) does not send SNI when connecting to on-premise EMS.
1105523	FortiClient (macOS) does not have option to use invitation code from new upgrade installer.

Endpoint management

Bug ID	Description
1091756	Endpoint one-way message does not work after system sleep or wakeup.
1106089	FortiClient fails to open with syntax error prompt if compliance.json file is empty.

Endpoint policy and profile

Bug ID	Description
1092879	Deselecting *Save Password* updates vpn.plist and removes existing IPv4SplitExcludeNetworks configuration.

Install and upgrade

Bug ID	Description
975336	macOS deployment fails if installer name has space.

Logs

Bug ID	Description
750703	IPsec and SSL VPN events do not log to FortiAnalyzer appropriately.

Quarantine management

Bug ID	Description
1091718	FortiClient (macOS) fails to upload quarantine file list to EMS.

Remote Access

Bug ID	Description
1075772	VPN features are in consistent with FortiClient (Windows).

Remote Access - IPsec VPN

Bug ID	Description
948566	*Enable Local LAN* option does not work as expected.

Remote Access - SSL VPN

Bug ID	Description
1089916	Horizontal scaled instance with realm configuration does not connect on macOS.
1102807	SAML authentication popup has issue with non-English OS languages.
1110157	Client hangs on connecting when user closes SAML external browser without authenticating.

ZTNA connection rules

Bug ID	Description
1104481	FortiClient (macOS) does not update `/etc/hosts` with FQDN containing hyphens.

Common Vulnerabilities and Exposures

Bug ID	Description
993833	FortiClient (macOS) 7.4.3 is no longer vulnerable to the following CVE Reference: • CVE-2024-35281 Visit https://fortiguard.com/psirt for more information.
1053898	FortiClient (macOS) 7.4.3 is no longer vulnerable to the following CVE Reference: • CVE-2024-3661 Visit https://fortiguard.com/psirt for more information.
1123431	FortiClient (macOS) 7.4.3 is no longer vulnerable to the following CVE Reference: • CVE-2025-25251 Visit https://fortiguard.com/psirt for more information.

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

The following issues have been identified in FortiClient (macOS) 7.4.3.

Endpoint control

Bug ID	Description
1023729	When detecting Fortinet Security Fabric status via DHCP code, local subnet does not work as expected after connecting to VPN.

Remote Access - SSL VPN

Bug ID	Description
1126363	FortiClient (macOS) fails to shut down during automatic test for autoconnect-related cases.

Existing known issues

The following issues have been identified in a previous version of FortiClient (macOS) and remain in FortiClient (macOS) 7.4.3.

Endpoint control

Bug ID	Description
958511	FortiClient (macOS) does not support Microsoft Entra ID verification when joining EMS.
1029889	FortiClient ffconfig leaves behind many zombie processes.

Malware Protection and Sandbox

Bug ID	Description
1087180	Real-time protection does not detect or quarantine when downloading Eicar sample files through Safari and only works when accessing files.

Third-party compatibility

Bug ID	Description
961542	FortiClient and Microsoft Defender conflict due to system processes used in overlapping real-time protection features. **Workaround**: enable passive mode on Microsoft Defender.
1085782	Cisco Umbrella does not work when zero trust network access is enabled.

www.fortinet.com