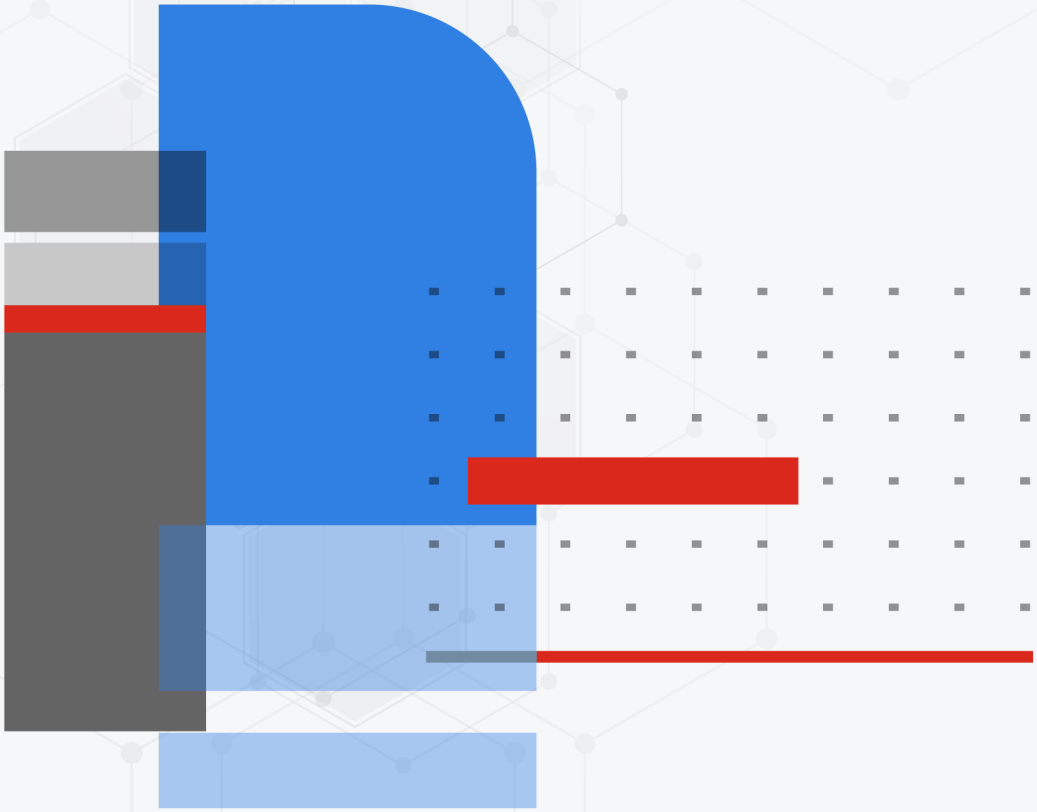
Release Notes

FortiClient (macOS) 7.4.7



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

April 29, 2026
FortiClient (macOS) 7.4.7 Release Notes
04-747-1252789-20260429

TABLE OF CONTENTS

Change log

Date	Change description
2026-04-27	Initial release.
2026-04-29	Updated Activating system extensions on page 8.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (macOS) 7.4.7 build 1928.M.

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: 7.4.7.1928.M

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

Licensing

See Windows, macOS, and Linux endpoint licenses.

Special notices

No IPv6 support for IPsec VPN

FortiClient (macOS) 7.4.4 to 7.4.7 do not support IPv6 for IPsec VPN due to dual VPN changes. Support may be added in future releases.

IPsec VPN support limitation

Due to a macOS limitation, macOS Guest VMs using bridged network connections do not support IPsec VPN tunnels.

Using the same default MTU size for VPN interfaces across all platforms

Starting from 7.4.4, FortiClient (macOS) uses the same default MTU size for SSL and IPsec VPN interfaces as Windows and Linux, which improves connection efficiency. You can modify the MTU size using the `<mtu_size>` XML option. See the XML Reference Guide.

No support for concurrent third-party tunneling or proxy clients

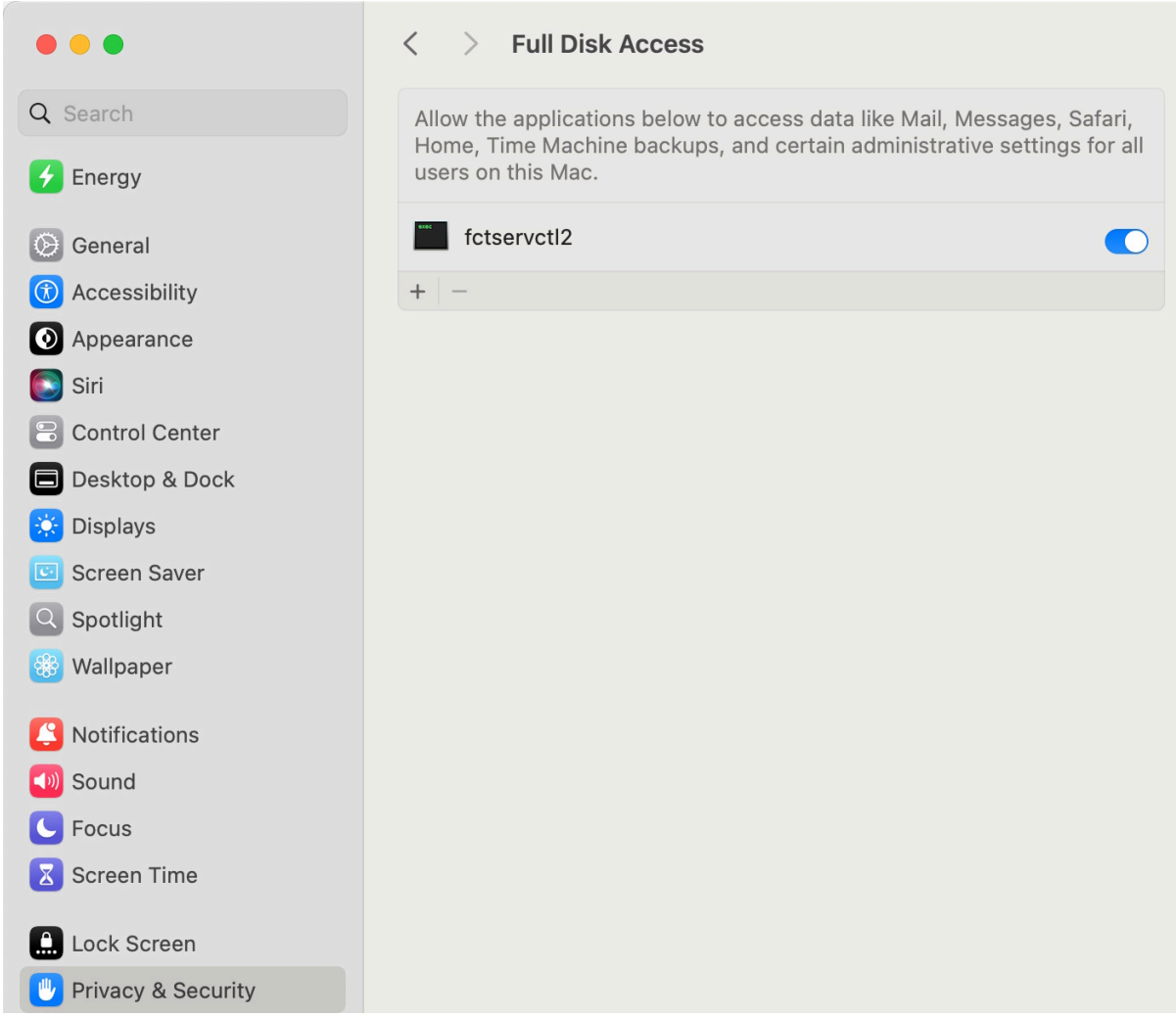
Using third-party tunneling or proxy clients (including VPN, DNS, HTTP(s), SOCKS, ZTNA or PAC files) in parallel or nested combination with FortiClient's VPN, ZTNA or Web Filter is not recommended nor supported.

Enabling full disk access for FortiClient process

To use the following features, you must grant full disk access permission for the fctservctl2 process (located in `/Library/Application Support/Fortinet/FortiClient/bin/`):

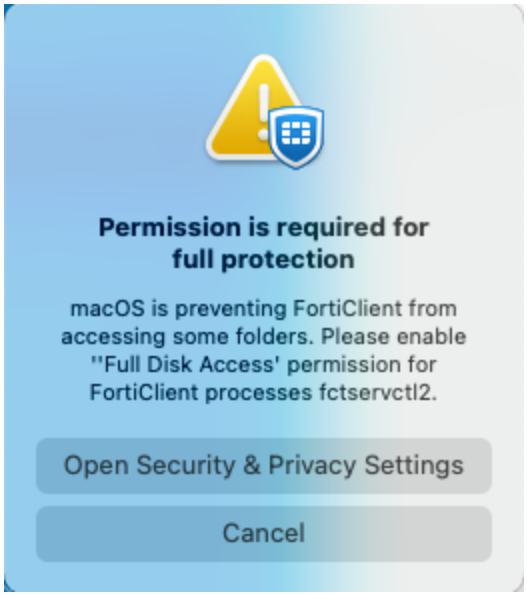
- AV scan
- Sandbox scan
- Importing VPN profile

To do so, go to the *Security & Privacy* pane and toggle on the *fctservctl2* option under *Full Disk Access*.



On macOS Tahoe (26.1/26.2), the *fctservctl2* option does not appear in the *Full Disk Access* list due to an OS bug. You can drag the process to the list or click the *Add* icon to manually add the process. While the process still does not show up in the list after being added (due to the OS bug), the necessary permission has been granted.

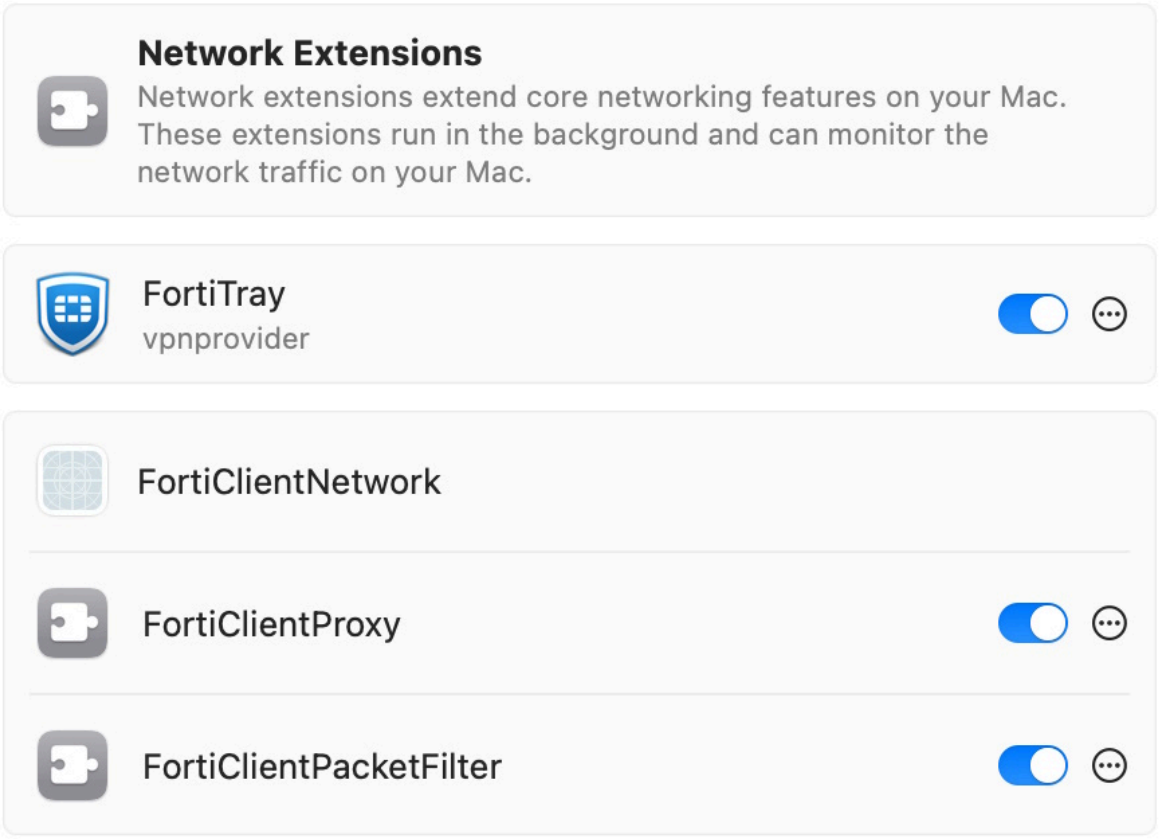
If any of these features are used while full disk access is not enabled for *fctservctl2*, FortiClient (macOS) prompts the user to enable full disk access permission.



Activating system extensions

After you perform an initial install of FortiClient (macOS), you must enable the system extensions for some FortiClient (macOS) processes. The FortiClient (macOS) team ID is AH4XFXJ7DK.

1. Ensure you have administrator credentials for the macOS machine.
2. - **(macOS Tahoe (version 26)** Go to *System Settings > General > Login Items & Extensions > By Category > Network Extensions*.
   - **(macOS Sequoia (version 15)** Go to *System Settings > General > Login Items & Extensions > Network Extensions*.
   - **(macOS Sonoma (version 14)** Click *Some system software requires your attention before it can be used*.
3. Toggle on the following options to enable the extensions:
   - *FortiTray* (for VPN to work properly)
   - *FortiClientProxy* (for Web Filter to work properly)
   - *FortiClientPacketFilter* (for Application Firewall to work properly)



4. 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 an external DHCP server to assign IP addresses to IPsec VPN clients.

Running multiple FortiClient instances

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

Installation information

Firmware images and tools

The following files are available from the Fortinet support site:

File	Description
FortiClientTools_7.4.7.1928.M_macosx.tar.gz	Includes utility tools and files to help with installation.

The following files are available from Fortinet.com:

File	Description
FortiClient_OnlineInstaller.dmg	Standard installer for macOS.

FortiClient EMS 7.4.7 includes the FortiClient (macOS) 7.4.7 standard installer.

Review the following sections prior to installing FortiClient version 7.4.7: 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 7.4.7 supports upgrade from FortiClient 6.4 and 7.0.

FortiClient (macOS) 7.4.7 features are only enabled when connected to EMS 7.2 and later.

See Recommended upgrade path for information on upgrading FortiClient (macOS) 7.4.7.

Downgrading to previous versions

FortiClient 7.4.7 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) 7.4.7 product integration and support information:

Desktop operating systems	• macOS Tahoe (version 26) • macOS Sequoia (version 15) • macOS Sonoma (version 14)
Minimum system requirements	• Intel processor or Apple silicon 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	• 7.4.7 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
AV engine	7.0.43
VCM engine	2.0026
IPS engine	7.1.165
FortiEDR for macOS	6.1.0.1459
FortiAnalyzer	• 7.6.0 and later • 7.4.0 and later • 7.2.0 and later
FortiAuthenticator	• 8.0.0 and later • 6.6.0 and later • 6.5.0 and later
FortiManager	• 7.6.0 and later • 7.4.0 and later • 7.2.0 and later
FortiSandbox	• 5.0.0 and later • 4.4.0 and later • 4.2.0 and later

Language support

The following table lists FortiClient language support information:

Language	GUI	XML configuration	Documentation
English	Yes	Yes	Yes
Chinese (simplified)			
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) 7.4.7. For inquiries about a particular bug, contact Customer Service & Support.

Remote Access - IPsec VPN

Bug ID	Description
1210851	IKEv2 VPN ignores dns-suffix-search, causing hostname resolution failure without FQDN.
1272887	SASE tunnel with UDP-fallback-TCP and auto-connect-only-when-offnet reconnects when switching from off-net to on-net.

Other

Bug ID	Description
1284931	Security best practice: remove weak cipher support.

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 FortiClient (macOS) 7.4.7.

Existing known issues

The following issues have been identified in a previous version of FortiClient (macOS) and remain in FortiClient (macOS) 7.4.7.

Deployment and installers

Bug ID	Description
1187125	FortiClient DNS root certificate changes from static to dynamic in 7.4.4, which breaks MDM profile pre-approval on the certificate. As a result, MDM-managed users with a pushed official Fortinet mobileconfig file will now see a prompt for "FortiClient DNS Root" certificate on fresh installation or upgrade to 7.4.4. Non-admin users can bypass this prompt by entering the password and clicking "Update Settings".

Endpoint control

Bug ID	Description
949324	Re-authentication error for verified registered FortiClient endpoints with the SAML or Entra ID user verification type when *User Verification Period* is enabled in EMS.
1023729	When detecting Fortinet Security Fabric status via DHCP code, local subnet does not work as expected after connecting to VPN.

GUI

Bug ID	Description
1268450	False error message "Failed to import VPN configuration, please try again!" after successful import of the personal VPN XML configuration.
1188195	Slow response for VPN options checkboxes.
1191168	Renderer crash when the GUI is left open for 2 days.
1193127	VPN connection status frequently blinks with all information showing 0.
1193526	Saving the password for a VPN tunnel while autoconnect option is enabled resets the FortiClient autoconnect configuration.

Sandbox Protection

Bug ID	Description
1138535	FortiSandbox does not detect files downloaded by any other browser or application except Google Chrome.

Remote Access - IPsec VPN

Bug ID	Description
1163586	Unable to connect to FortiOS TCP tunnel when the IPsec IKEv 2 tunnel has encapsulation set to *auto*.
1196063	FortiClient fails to connect to IPsec IPv6 IKEv2 tunnels when multiconnect is enabled in EMS.

Remote Access - SSL VPN

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

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.
1235179	Conflict when trying to connect to AWS VPN while FortiClient ZTNA is running. **Workaround**: Disable ZTNA on the *ZTNA DESTINATION* tab in the FortiClient GUI.

Vulnerability Scan

Bug ID	Description
1230594	FortiClient does not performs vulnerability scan when EMS set scheduled scan on "Weekly Scan at 00:00:00".

ZTNA TCP/UDP Forwarding

Bug ID	Description
1269678	On macOS 26.3.1, ZTNA TCP forwarding using IP with port 22 destinations fails in non-proxy mode. **Workaround**: Use FQDN (instead of IP) with port 22 for ZTNA TCP forwarding in non-proxy mode on macOS 26.3.1.

Other

Bug ID	Description
1205335	During network lockdown, the captive portal always pops up even if the captive portal detection toggle is disabled.
1218936	Diagnostic tool is damaged after upgrade.

www.fortinet.com