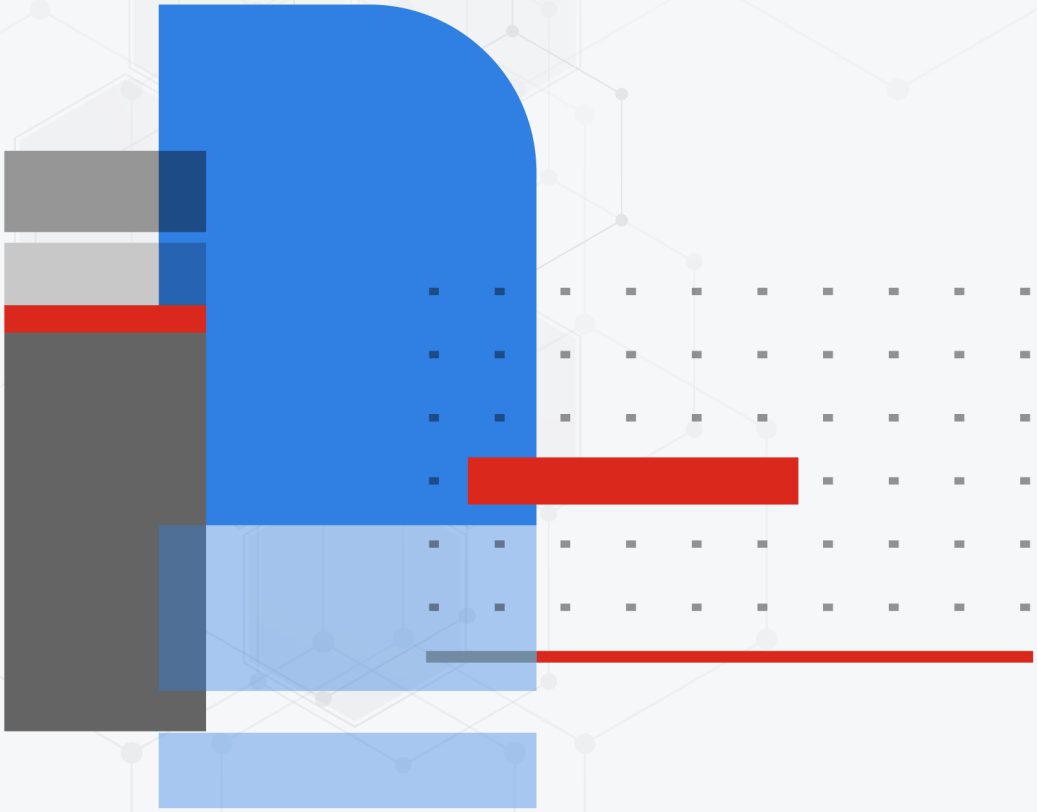
Release Notes

FortiClient (macOS) 7.4.4



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 05, 2026
FortiClient (macOS) 7.4.4 Release Notes
04-744-1147560-20260305

TABLE OF CONTENTS

Change log

Date	Change description
2025-09-09	Initial release.
2025-09-10	Updated: • Special notices on page 7 • New known issues on page 20
2025-09-25	Updated Product integration and support on page 16.
2025-10-09	Updated Special notices on page 7.
2025-10-15	Added Common Vulnerabilities and Exposures on page 19.
2025-10-29	Updated Existing known issues on page 21.
2025-11-14	Updated Special notices on page 7.
2025-11-27	Updated Resolved issues on page 18 and Existing known issues on page 21.
2026-03-03	Added Changes in default behavior on page 12.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (macOS) 7.4.4 build 1831.F.

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: 7.4.4.1831.F

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

Licensing

See Windows, macOS, and Linux endpoint licenses.

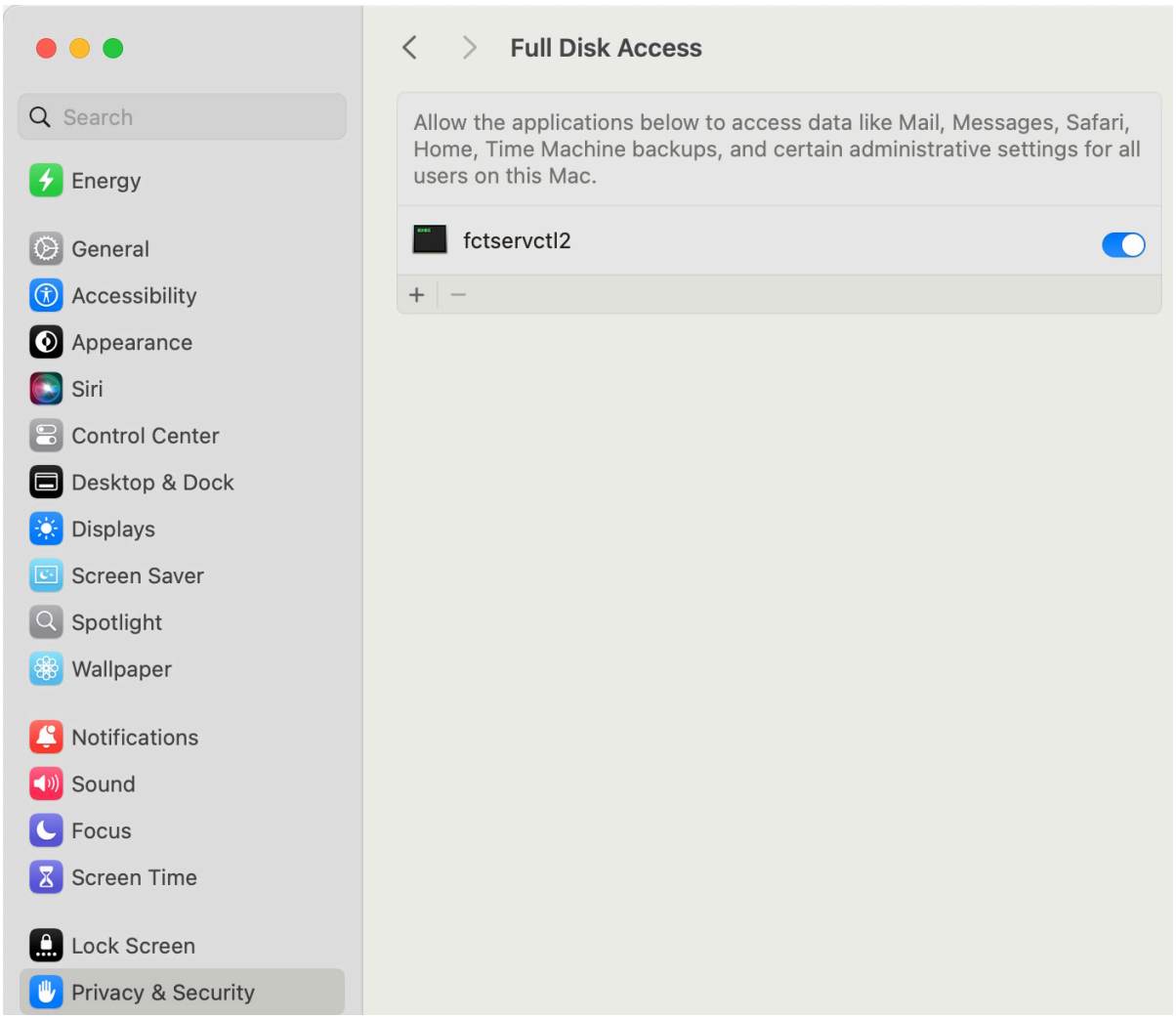
Special notices

DNS root certificate prompt for MDM-managed users with pre-approved certificate

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*.

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.

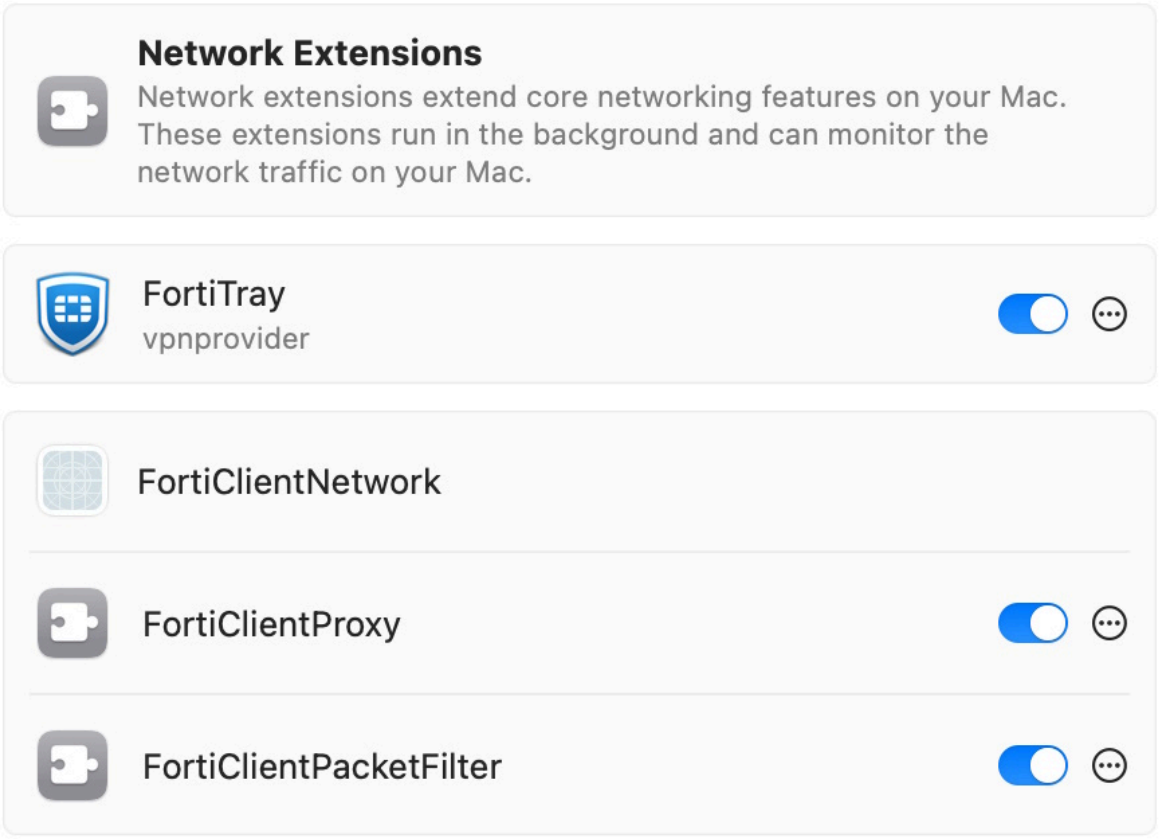
VPN works properly only when you allow FortiTray to load in *Network Extensions* settings. You must enable the FortiClientProxy and FortiClientPacketFilter extensions for Web Filter and Application Firewall, respectively, to work properly. The FortiClient (macOS) team ID is AH4XFXJ7DK.

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 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.

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.

No IKEv1 support for IPsec VPN

FortiClient (macOS) 7.4.4 no longer supports IKEv1 for IPsec VPN. Please migrate to using IKEv2 instead.

No IPv6 support for IPsec VPN

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

No new version of VPN-only agent

FortiClient (macOS) 7.4.4 does not include a new version of the free VPN-only agent as no feature updates were made to the free VPN-only agent between 7.4.3 and 7.4.4. Users can continue to use the FortiClient (macOS) 7.4.3 free VPN-only agent.

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

FortiClient (macOS) 7.4.4 now 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.

Changes in default behavior

FortiClient (macOS) 7.4.4 includes the following change in default behavior. For inquiries about a particular change, contact Customer Service & Support.

ID	Description
1078170	The `utun40` virtual interface used to be active only when FortiClient (macOS) is connected to EMS. Starting from 7.4.4, the interface is active as long as FortiClient (macOS) is up and running, regardless of EMS connection status. See FortiClient (macOS) processes for more information.

What’s new in FortiClient (macOS) 7.4.4

For information about what's new in FortiClient 7.4.4, 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_7.4.4.1831.F_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 7.4.4 includes the FortiClient (macOS) 7.4.4 standard installer.

Review the following sections prior to installing FortiClient version 7.4.4: Introduction on page 6, Special notices on page 7, and Product integration and support on page 16.

Upgrading from previous FortiClient versions

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

FortiClient 7.4.4 supports upgrade from FortiClient 6.4 and 7.0.

FortiClient (macOS) 7.4.4 features are only enabled when connected to EMS 7.2 and later.

See Recommended upgrade path for information on upgrading FortiClient (macOS) 7.4.4.

Downgrading to previous versions

FortiClient 7.4.4 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) 7.4.4 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 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	• 7.4.0 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	7.0.43
VCM engine	2.0026
IPS engine	7.1.165
FortiEDR for macOS	6.0.10.1022
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) 7.4.4. For inquiries about a particular bug, contact Customer Service & Support.

Install and upgrade

Bug ID	Description
1147336	Upgrade is triggered twice even when the first upgrade was successful.

Remote Access

Bug ID	Description
1120710	VPN tunnel disconnects after the user locks screen.
1101223	FortiClient retains incorrect password value when attempting to establish VPN tunnel when "Save Password" is selected.

Remote Access - SSL VPN

Bug ID	Description
1012003	When connecting to FortiOS 7.4.3, saved password is not cleared after SSL VPN connection failure due to wrong credentials.
1104958	FortiClient macOS GUI does not display client certificate name for certain certificate regu;ar expression matches.

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.
1142079	FortiClient AV randomly blocks uploading files to web server and Outlook.

ZTNA connection rules

Bug ID	Description
1155036	Forticlient ZTNA TCP forward SAML session should not start redirect with TCP forward path.
1156635	ztagent not running after installed/registration on Mac OS 15.2 and higher version

Common Vulnerabilities and Exposures

FortiClient (macOS) 7.4.4 is no longer vulnerable to the following CVE references. Visit https://fortiguard.com/psirt for more information.

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

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) 7.4.4.

Deployment and installers

Bug ID	Description
1187125	FortiClient DNS root certificate changes from static to dynamic, breaking MDM profile pre-approval on the certificate and causing unwanted popups.

Endpoint security

Bug ID	Description
1190471	Significant delay for Teams app when *Network Lockdown* is enabled with *Excluded SaaS Applications: ms-teams*.

GUI

Bug ID	Description
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.

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*.
1182982	Split-DNS not working as expected for IPsec VPN when multivpn enabled.
1196063	FortiClient fails to connect to IPsec IPv6 IKEv2 tunnels when multiconnect is enabled in EMS.
1197511	FortiClient does not try the remaining gateways if the first gateway's FQDN cannot be resolved.
1201068	When using IPsec IKEv2 with SAML authentication, tunnel reconnection fails if triggered by *Always-Up* after network disruption.

Remote Access - SSL VPN

Bug ID	Description
1197514	SSLVPN auto_connected EMS deployment shows success but the GUI does not change to connected status.

ZTNA connection rules

Bug ID	Description
1196265	Packet Filter firewall rules created by FortiClient's ZTNA are not removed after FortiClient disconnects from EMS.

Existing known issues

The following issues have been identified in a previous version of FortiClient (macOS) and remain in FortiClient (macOS) 7.4.4.

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

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