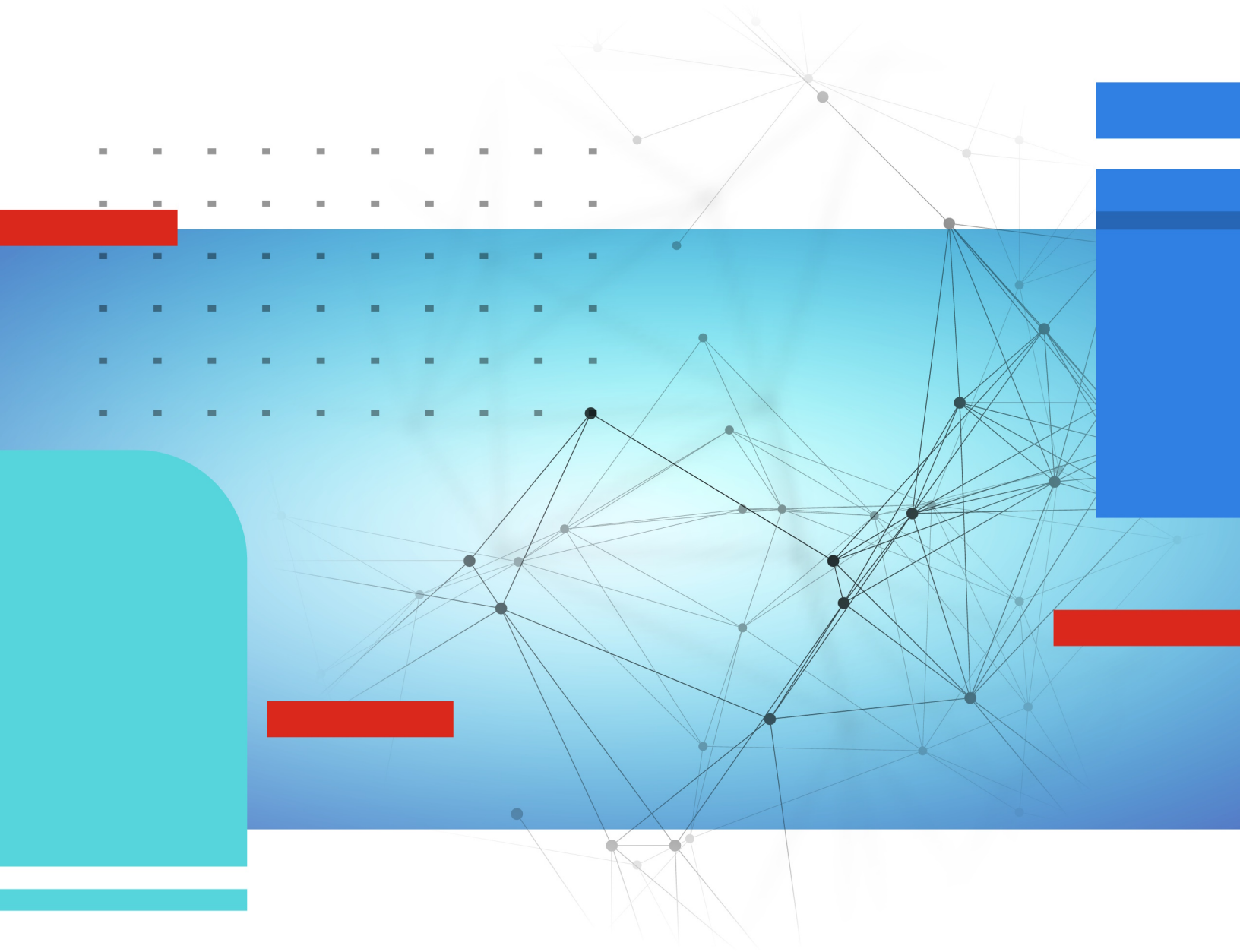
(macOS) Release Notes

FortiClient 7.4.8



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



November 12, 2026
FortiClient 7.4.8 (macOS) Release Notes

TABLE OF CONTENTS

Change log **4**
Introduction **5**
Licensing 5
Special notices **6**
IPsec VPN support limitation 6
Using the same default MTU size for VPN interfaces across all platforms 6
No support for concurrent third-party tunneling or proxy clients 6
DHCP over IPsec VPN not supported 6
Running multiple FortiClient instances 6
What's new in FortiClient (macOS) 7.4.8 ..... **7**
Installation information **8**
Firmware images and tools 8
Upgrading from previous FortiClient versions 8
Downgrading to previous versions 8
Uninstalling FortiClient 9
Firmware image checksums 9
Product integration and support **10**
Language support 11
Resolved issues **12**
Deployment and installers 12
Endpoint control 12
Remote Access 12
Remote Access - IPsec VPN 12
Web filter and plugin 13
Vulnerabilities and Exposures 13
Known issues **14**
New known issues 14
Remote Access - IPsec VPN 14
Existing known issues 14
Deployment and installers 14
Endpoint control 15
GUI 15
Sandbox Protection 15
Remote Access - IPsec VPN 15
Remote Access - SSL VPN 16
Third-party compatibility 16
Vulnerability Scan 16
ZTNA TCP/UDP Forwarding 16
Other 17

Change log

Date	Change description
2026-07-29	Initial release.
2026-08-28	Updated Special notices on page 6.
2026-11-05	Updated Existing known issues on page 14.
2026-11-12	Added CVE-2026-121529 to Resolved issues on page 12.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (macOS) 7.4.8 build 1977.M.

This document includes the following sections:

- Special notices on page 6
- What's new in FortiClient (macOS) 7.4.8 on page 7
- Installation information on page 8
- Product integration and support on page 10
- Resolved issues on page 12
- Known issues on page 14

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: 7.4.8.1977.M

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

Licensing

See Windows, macOS, and Linux endpoint licenses.

Special notices

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.

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.

What’s new in FortiClient (macOS) 7.4.8

For information about what's new in FortiClient 7.4.8, 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_7.4.8.1977.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 7.4.8 includes the FortiClient (macOS) 7.4.8 standard installer.



Review the following sections prior to installing FortiClient version 7.4.8: Introduction on page 5, Special notices on page 6, and Product integration and support on page 10.

Upgrading from previous FortiClient versions



You must upgrade EMS to 7.2 or later before upgrading FortiClient to 7.4.8.

FortiClient (macOS) 7.4.8 features are only enabled when connected to EMS 7.2 and later.

See Recommended upgrade path for information on upgrading FortiClient (macOS) 7.4.8.

Downgrading to previous versions

FortiClient 7.4.8 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) 7.4.8 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	• 7.4.8 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	7.0.54
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) 7.4.8. For inquiries about a particular bug, contact Customer Service & Support.

Deployment and installers

Bug ID	Description
1260580	Cannot deploy FortiClient (macOS) using the FortiEndpoint unified installer via JAMF.

Endpoint control

Bug ID	Description
1213829	When [User verification period] is toggled OFF in EMS, 'auth_period' FCT registry is not set to 0.

Remote Access

Bug ID	Description
1301371	When multiple VPN tunnels are connected, DNS traffic fails after switching WiFi. The issue is resolved after reboot and no DNS stuck.

Remote Access - IPsec VPN

Bug ID	Description
1196063	FortiClient fails to connect to IPsec IPv6 IKEv2 tunnels when multiconnect is enabled in EMS.

Bug ID	Description
1210851	Suffixes from dns-suffix-search in IKEv2 dialup VPN are not used for DNS resolution on macOS.
1224468	Pinned VPN Tunnel on tray is removed after FortiClient (macOS) upgrade.
1272887	SASE tunnel with UDP-fallback-TCP and auto-connect-only-when-offnet reconnects when switching from off-net to on-net.

Web filter and plugin

Bug ID	Description
1291248	Inconsistent block page observed on macOS with web filter deep inspection enabled.

Vulnerabilities and Exposures

FortiClient (macOS) 7.4.8 is no longer vulnerable to the following CVE reference. Visit https://fortiguard.com/psirt for more information.

Bug ID	Description
1288048	CVE-2026-121529

Known issues

Known issues are organized into the following categories:

- New known issues on page 14
- Existing known issues on page 14

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

New known issues

The following issue has been identified in FortiClient (macOS) 7.4.8.

Remote Access - IPsec VPN

Bug ID	Description
1283704	IKEv2 dual stack over IPv6 gateway fails to work for full tunnel.

Existing known issues

The following issues have been identified in a previous version of FortiClient (macOS) and remain in FortiClient (macOS) 7.4.8.

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*.
1203069	IPdec VPN connection with ECDSA certificate fails to establish.
1222838	FortiClient should use Subject Alternative Name instead of (or in addition to) Common Name when providing peer ID.

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	When the Sandbox feature is enabled, FortiClient conflicts with Microsoft Defender 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.

1219486	FortiClient IPsec IKEv2 VPN connection is terminated unexpectedly on macOS when Sophos EDR/XDR is installed.
	Workaround: Configure the tunnel to allow concurrent running with other tunnels using the following XML options:
	`<enable_multi_vpn>1</enable_multi_vpn>`
	`<allow_concurrent>1</allow_concurrent>`

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

Copyright© 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.