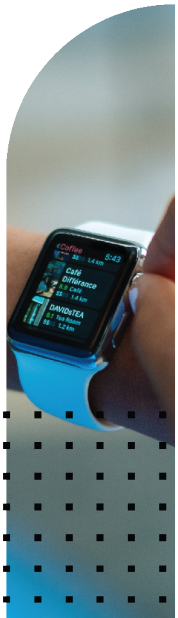
Release Notes

FortiClient (macOS) 7.0.14



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 03, 2026
FortiClient (macOS) 7.0.14 Release Notes
04-7014-1095448-20260303

TABLE OF CONTENTS

Change log

Date	Change description
2024-12-04	Initial release.
2026-03-03	Updated Special notices on page 7 and Existing known issues on page 17.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (macOS) 7.0.14 build 0453.

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

FortiGuard Anycast Certificate Expiration

FortiClient (macOS) 7.0.14 fails to recognize the newly issued April 16, 2026 Digicert CA used by FortiGuard Anycast servers, which results in failed communication for the following updates:

- Web Filter rating
- Video Filter rating
- Split VPN using ISDB
- Signature and engine updates

See CSB-260303-1 for more information.

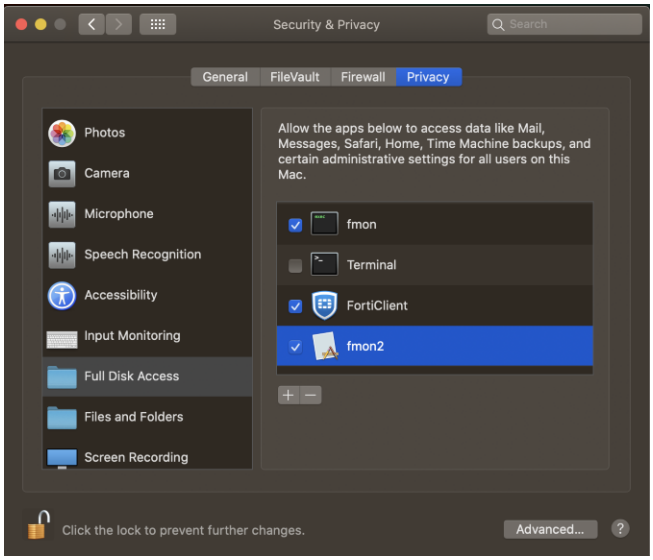
Enabling full disk access

FortiClient (macOS) works properly only when you grant permissions to access the full disk in the *Security & Privacy* pane for the following services:

- fcaptmon
- fctservctl
- fctservctl2
- fmon
- fmon2
- FortiClient
- FortiGuardAgent

The FortiClient (macOS) free VPN-only client does not include the fcaptmon, fmon, and fmon2 services. If you are using the VPN-only client, you only need to grant permissions for fctservctl and FortiClient.

You may have to manually add fmon2 to the list, as it may not be in the list of applications to allow full disk access to. Click the + icon to add an application. Browse to `/Library/Application Support/Fortinet/FortiClient/bin/` and select fmon2.



The following lists the services and their folder locations:

- fmon, Fctservctl, Fcaptmon: `/Library/Application\ Support/Fortinet/FortiClient/bin/`
- FortiClient (macOS) application: `/Applications/FortiClient.app`
- FortiClient agent (FortiTray): `/Applications/FortiClient.app/Contents/Resources/runtime.helper/FortiGuardAgent.app`

Activating system extensions

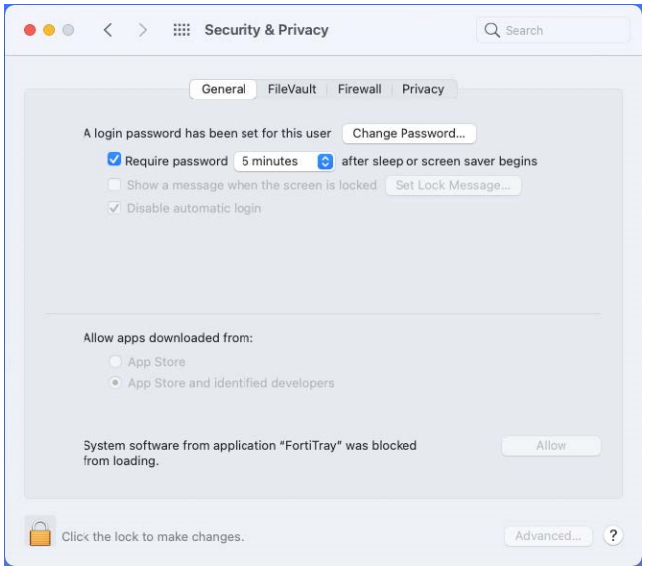
After you initially install FortiClient (macOS), the device prompts you to allow some settings and disk access for FortiClient (macOS) processes. You must have administrator credentials for the macOS machine to configure this change.

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 *Allow* beside *System software from application "FortiTray" was blocked from loading*.

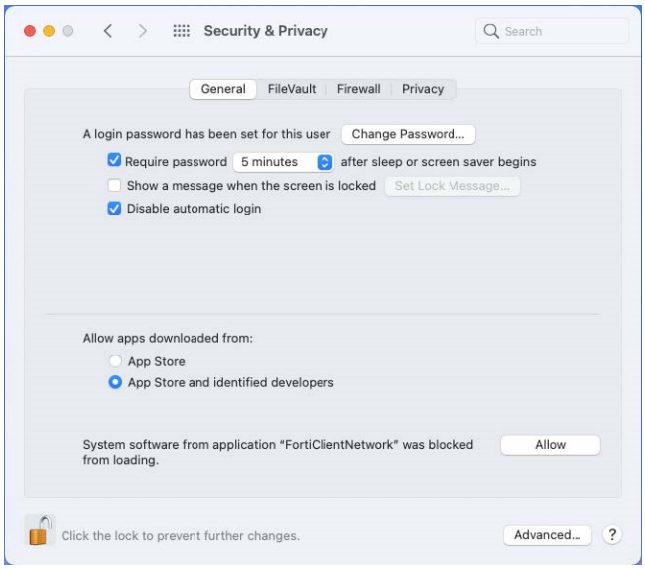


Web Filter and Application Firewall

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 *Allow* 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:

```
MacBook-Air ~ % systemextensionsctl list
2 extension(s)
--- com.apple.system_extension.network_extension
enabled active  teamID  bundleID (version)      name    [state]
*       *       AH4XFXJ7DK      com.fortinet.forticlient.macos.vpn.nwextension (1.4.8/B20210629)        vpnprovider     [activated
*       *       AH4XFXJ7DK      com.fortinet.forticlient.macos.webfilter (1.1/1)        FortiClientPacketFilter [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. For a macOS device with Intel or M1 chip, you can do the following:

To enable proxy mode on macOS devices with an Intel or M1 chip:

1. Add the following XML configuration:

```
<forticlient_configuration>
   <webfilter>
      <use_transparent_proxy>1</use_transparent_proxy>
   <webfilter>
<forticlient_configuration>
```

2. Manually create an empty file: `sudo touch /Library/Application\Support/Fortinet/FortiClient/conf/use_transparent_proxy`

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.

IKEv2 not supported

FortiClient (macOS) does not support IPsec VPN IKEv2.

Running multiple FortiClient instances

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

IPsec VPN support limitation

Due to a macOS limitation, IPsec VPN tunnels are not supported on macOS Guest VMs using bridged network connections.

Installation information

Firmware images and tools

The following files are available from the Fortinet support site:

File	Description
FortiClientTools_7.0.14.0453_macosx.tar.gz	Includes utility tools and files to help with installation.
FortiClientVPNSetup_7.0.14.0453_macosx.dmg	Free VPN-only installer.

The following files are available from Fortinet.com:

File	Description
FortiClient_7.0.14.xxxx_macosx.dmg	Standard installer for macOS.
FortiClientVPNSetup_7.0.14.0453_macosx.dmg	Free VPN-only installer.

FortiClient EMS 7.0.14 includes the FortiClient (macOS) 7.0.14 standard installer.

Review the following sections prior to installing FortiClient version 7.0.14: Introduction on page 6, Special notices on page 7, and Product integration and support on page 14.

Upgrading from previous FortiClient versions

You must upgrade EMS to 7.0.2 or newer before upgrading FortiClient.

FortiClient 7.0.14 supports upgrade from FortiClient 6.2, 6.4, and 7.0.

FortiClient (macOS) 7.0.14 features are only enabled when connected to EMS 7.0 or 7.2.

With the new endpoint security improvement feature, there are backward compatibility issues to consider while planning upgrades. See Recommended upgrade path for information on upgrading FortiClient (macOS) 7.0.14.

Downgrading to previous versions

FortiClient 7.0.14 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) 7.0.14 product integration and support information:

Desktop operating systems	• macOS Sequoia (version 15) • macOS Sonoma (version 14) • macOS Ventura (version 13) • macOS Monterey (version 12) • macOS Big Sur (version 11) • macOS Catalina (version 10.15)
Minimum system requirements	• Intel processor or M1 or M2 chip • 256 MB of RAM • 20 MB of 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
FortiClient EMS	• 7.2.0 and later • 7.0.0 and later
FortiOS	The following versions support zero trust network access: • 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 • 6.2.0 and later
FortiAnalyzer	• 7.4.0 and later • 7.2.0 and later • 7.0.0 and later
FortiManager	• 7.4.0 and later • 7.2.0 and later • 7.0.0 and later
FortiSandbox	• 4.2.0 and later • 4.0.0 and later • 3.2.0 and later • 3.1.0 and later
FortiAuthenticator	• 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

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.

Resolved issues

The following issues have been fixed in FortiClient (macOS) 7.0.14. For inquiries about a particular bug, contact Customer Service & Support.

GUI

Bug ID	Description
1042686	Docker icon keeps jumping and blank page displays when opening console.

Remote Access - SSL VPN

Bug ID	Description
1089916	Horizontal scaled instance with realm configuration does not connect on macOS but connection works on Windows.

Known issues

Known issues are organized into the following categories:

- New known issues on page 17
- Existing known issues on page 17

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 7.0.14.

Existing known issues

The following issues have been identified in a previous version of FortiClient (macOS) and remain in FortiClient (macOS)7.0.14.

Configuration

Bug ID	Description
959285	Using wrong configuration for certificate filter in EMS causes config crash and FortiClient (macOS) cannot sync to EMS anymore.

Dashboard

Bug ID	Description
993484	User-specified information does not update in EMS dashboard properly when switching between different users.
993524	User-specified information does not update in EMS dashboard after uninstalling and installing FortiClient.

Endpoint control

Bug ID	Description
814351	Endpoint information page incorrectly displays device user's domain information after user switches on macOS device.
925823	FortiClient does not send the empty domain when switching to local user.
927357	FortiClient (macOS) has connectivity problems when connected over VPN.

Remote Access

Bug ID	Description
800529	*Do not Warn Invalid Server Certificate* flag in *Settings > VPN Options* has GUI issue.
800923	Custom host check failure message for SSL VPN does not work.
800978	Autoconnect is triggered twice when EMS has both on- and off-fabric profile configured.
864515	Endpoint fails to receive packets from FortiGate over IPsec VPN tunnel on macOS guest VM using bridged network connection.
968070	FortiClient (macOS) does not parse `<disallow_invalid_server_certificate>` correctly.
977725	Split tunnel has limitation.

Remote Access - IPsec VPN

Bug ID	Description
736245	IPsec VPN does not work when multiple remote gateways are configured in a priority-based list.
929577	When VPN is up, for redundant remote gateway, FortiClient fails to use next online gateway to connect if active one is down.
952987	FortiClient 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.
970489	Application Firewall decreases Internet speed when connecting to IPsec VPN.

Remote Access - SSL VPN

Bug ID	Description
772247	SAML authentication times out with SSL VPN.
790392	FortiClient blocks the network when Wi-Fi is changed.
854265	SSL VPN connects after sleep.
870585	When using Okta as SAML VPN to authenticate VPN, save password and autoconnect fail to work.
927290	VPN on free client does not work as expected in macOS 13.
956036	FortiClient (macOS) console does not update GUI when it establishes SSL VPN with SAML-authenticated tunnel.
994191	Autoconnect after reboot does not work for FortiSASE SIA when using Okta as SAML authentication IdP.
1007613	`sslvpn-ems-sn-check` error is not descriptive on SAML SSL VPN connections.

Vulnerability Scan

Bug ID	Description
786011	Vulnerability feature does not autopatch macOS Monterey 12.2.1 after it detects operating system (OS) vulnerability on macOS Monterey 12.1.
790288	Vulnerability Scan does not detect OS vulnerabilities.

Web Filter and plugin

Bug ID	Description
1255625	FortiClient (macOS) 7.0.14 fails to recognize the newly issued April 16, 2026 Digicert CA used by FortiGuard Anycast servers, which results in failed communication for the following updates: • Web Filter rating • Video Filter rating • Split VPN using ISDB • Signature and engine updates See CSB-260303-1 for more information.
755055	When action set for site categories is warn, browser does not show the customized webpage, which allows user to bypass blocking.

Bug ID	Description
772332	External Ethernet adapter dongle gets disconnected when speed test is run.
795631	Web Filter does not block the selected categories.
886326	Web Filter cannot filter URL with URI pathway.
919522	Web Filter extension causes socket hangup for Docker-hosted Linux containers.
956872	Transparent proxy causes issues with Adobe Creative Cloud and OneDrive applications.
984294	Web Filter exclusion list fails to execute expected allow and block actions.

Zero Trust tags

Bug ID	Description
793033	ZTNA LDAP group rule does not work.
794385	FortiClient detects third party antivirus tag.

Application Firewall

Bug ID	Description
800344	You can remotely access quarantined endpoints using VNC protocol.
834839	Web Filter does not block traffic when proxy mode is disabled and Application Firewall is disabled.
927564	FortiTray does not start after system restart.

Avatar and social login information

Bug ID	Description
777013	Avatar changes do not show on FortiAnalyzer.

License

Bug ID	Description
889767	License expiration shows unwanted +0000 at the end in the warning message.

Deployment and installers

Bug ID	Description
935387	FortiClient does not delete installer downloaded from EMS when it connects to a different EMS.
993140	Install log error is present for FortiMonitor agent in Apple silicon macOS VM.

Installation and upgrade

Bug ID	Description
827939	*FortiTray is not open anymore* prompt shows when deploying FortiClient using script through mobile device management.
828781	Behavior is inconsistent when uninstalling FortiClient through command in terminal and FortiClientUninstaller GUI tool.
929219	FortiClient is upgradable from full to free version.

FSSOMA

Bug ID	Description
962067	FSSO mobility agent (FSSOMA) does not work with Apple local account type.

Logs

Bug ID	Description
750703	IPsec and SSL VPN events are not logged on FortiAnalyzer appropriately.
801134	FortiClient (macOS) does not generate or replicate SSL VPN logs for upload to FortiAnalyzer when it establishes a tunnel.
872875	Disabling *Client-Based Logging When On-Fabric* in EMS does not work.
979395	fctinstallpost.log gets overwritten, causing loss of meaningful content.

Malware Protection and Sandbox

Bug ID	Description
719920	FortiClient cannot submit files to FortiClient Cloud Sandbox (SaaS) when downloaded from Thunderbird.
829415	When next-generation antivirus is enabled, real-time protection shows as disabled.
855555	When RTP is enabled and `block_removable_media` is set to `1`, FortiClient (macOS) fails to block USB device.
859241	FortiSandbox sends files to or queries for results from FortiSandbox when EMS is unauthorized.
921370	User cannot stop manually triggered AV scan.
941623	FortiClient does not submit network drive files to Sandbox when copied or executed from mapped network drive.

Endpoint management

Bug ID	Description
891264	EMS creates duplicate records for domain-joined Ubuntu endpoints.
930560	FortiClientAgent/FortiTray do not quit some backend services when shutting down FortiClient.

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. **Workaround**: enable passive mode on Microsoft Defender.

ZTNA connection rules

Bug ID	Description
853281	FortiClient (macOS) does not show ICDB signatures on the About page.
905880	ZTNA certificate prompt displays when deploying FortiClient (macOS) with Jamf Pro configuration profiles.

Bug ID	Description
	Workaround: enable ZTNA in both on- and off-Fabric profile if you are using both on- and off-Fabric profiles.
938962	FortiClient keeps prompting *ztagent wants to sign using key "Imported Private Key"* even when selecting *always trust*.
956351	*ZTNA Destination* GUI does not show detailed prompt for destination rules that EMS pushed.
961800	When ZTNA is enabled, pfctl rules affect DNS traffic.

www.fortinet.com