FortiClient (macOS) - Release Notes

Version 6.4.10

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

April 03, 2023
FortiClient (macOS) 6.4.10 Release Notes
04-6410-894593-20230403

TABLE OF CONTENTS

Change log

Date	Change description
2023-04-03	Initial release.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (macOS) 6.4.10 build 1481.

This document includes the following sections:

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

Licensing

FortiClient 6.2.0, FortiClient EMS 6.2.0, and FortiOS 6.2.0 introduce a new licensing structure for managing endpoints running FortiClient 6.2.0+. See Upgrading from previous FortiClient versions on page 9 for more information on how the licensing changes upon upgrade to 6.2.0+. Fortinet no longer offers a free trial license for ten connected FortiClient endpoints on any FortiGate model running FortiOS 6.2.0+. EMS 6.4 supports a trial license. With the EMS free trial license, you can provision and manage FortiClient on ten Windows, macOS, and Linux endpoints and ten Chromebook endpoints indefinitely.

FortiClient 6.4.10 offers a free VPN-only version that can be used for VPN-only connectivity to FortiGate devices running FortiOS 5.6 and later versions. You can download the VPN-only application from FortiClient.com.

Special notices

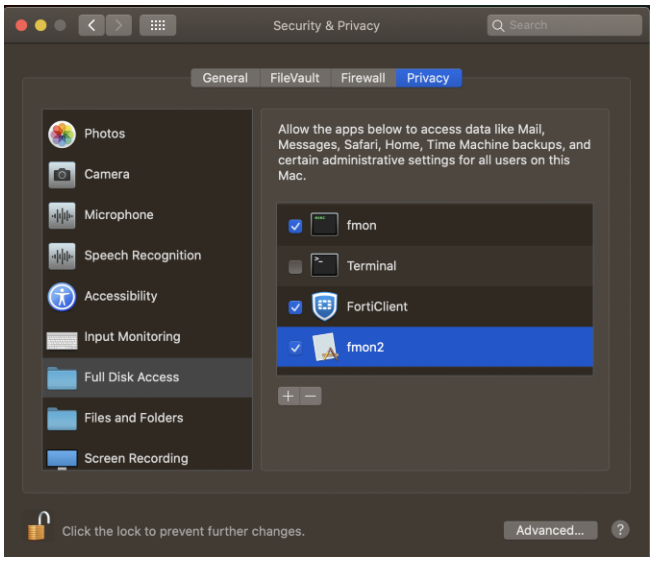
Enabling full disk access on macOS 11 Big Sur and 10.15 Catalina

You can install FortiClient (macOS) 6.4.10 on macOS 11 Big Sur and 10.15 Catalina. With these releases, FortiClient works properly only when you grant permissions to access the full disk in the *Security & Privacy* pane for the following services:

- fcaptmon
- fctservctl
- fmon2
- FortiClient

The FortiClient (macOS) free VPN-only client does not include the fcaptmon and fmon2 services. If you use 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`

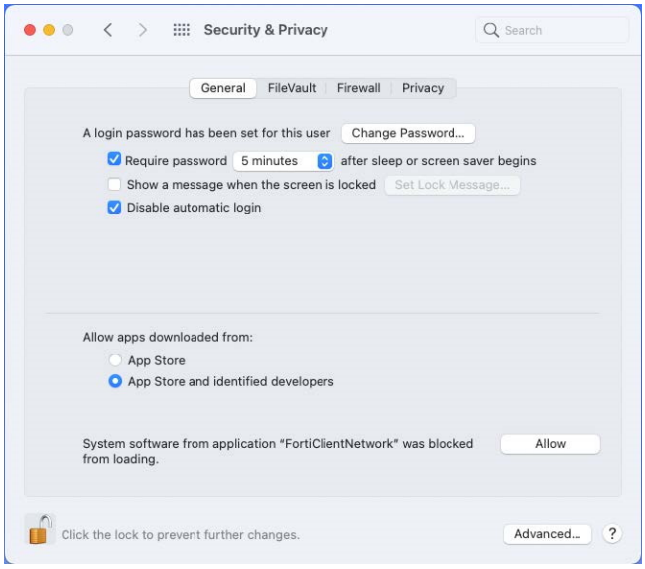
Activating system extensions

After you perform an initial install of 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.

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 the *Allow* button beside *System software from application "FortiClientNetwork" was blocked from loading*.



3. Verify the status of the extension by running the `systemextensionsctl list` command in the macOS terminal. The following provides example of output when the extension is enabled:

```
1 extension(s)
--- com.apple.system_extension.network_extension
enabled active  teamID  bundleID (version)      name    [state]
*       *       AH4XFXJ7DK      com.fortinet.forticlient.macos.webfilter (1.1/1)       FortiClientPacketFilter [activated enabled]
```

Enabling notifications

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

To enable notifications:

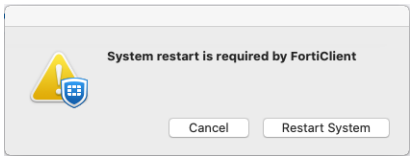
1. Go to *System Preferences* > *Notifications* > *FortiClientAgent*.
2. Toggle *Allow Notifications* on.

DHCP over IPsec VPN not supported

FortiClient (macOS) does not support DHCP over IPsec VPN.

macOS Mojave (version 10.14) reboot prompt

When using macOS Mojave (version 10.14), you must reboot the macOS device after installing FortiClient (macOS). FortiClient (macOS) displays the following prompt after installation:



IKEv2 not supported

FortiClient (macOS) does not support IPsec VPN IKEv2.

FortiClientAgent only starts after login

FortiClientAgent can only start after the user logs in to macOS. FortiClient only starts its other services after FortiClientAgent is running.

Installation information

Firmware images and tools

The following files are available from the Fortinet support site:

File	Description
FortiClientTools_6.4.10.xxxx_macosx.tar.gz	Includes utility tools and files to help with installation.
FortiClientVPNSetup_6.4.10.xxxx_macosx.dmg	Free VPN-only installer.

The following files are available from FortiClient.com:

File	Description
FortiClient_6.4.10.xxxx_macosx.dmg	Standard installer for macOS.
FortiClientVPNSetup_6.4.10.xxxx_macosx.dmg	Free VPN-only installer.

FortiClient EMS 6.4 includes the FortiClient (macOS) 6.4.10 standard installer.

Review the following sections prior to installing FortiClient version 6.4.10: Introduction on page 5, Special notices on page 6, and Product integration and support on page 11.

Upgrading from previous FortiClient versions

You must upgrade EMS to one of the following versions before upgrading FortiClient:

- 6.4.7 or later
- 7.0.2 or later

FortiClient version 6.4.10 supports upgrade from FortiClient 6.2.

FortiClient (macOS) 6.4.10 features are only enabled when connected to EMS. With the new endpoint security improvement feature, there are backward compatibility issues to consider while planning upgrades. See Recommended upgrade path.

See the *FortiClient and FortiClient EMS Upgrade Paths* for information on upgrade paths.

Downgrading to previous versions

FortiClient 6.4.10 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) 6.4.10 product integration and support information:

Desktop operating systems	• macOS Monterey (version 12) • macOS Big Sur (version 11) • macOS Catalina (version 10.15) • macOS Mojave (version 10.14)
Minimum system requirements	• Intel processor or M1 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	• 6.00258
FortiClient EMS	• 7.0.2 and later • 6.4.7 and later
FortiOS	The following versions support IPsec and SSL VPN: • 7.0.0 and later • 6.4.0 and later • 6.2.0 and later • 6.0.0 and later The following versions support endpoint control: • 6.2.0 and later
FortiAnalyzer	• 7.0.0 and later • 6.4.0 and later
FortiManager	• 6.4.0 and later
FortiSandbox	• 4.0.0 and later • 3.2.0 and later • 3.1.0 and later
FortiAuthenticator	• 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) 6.4.10. For inquiries about a particular bug, contact Customer Service & Support.

Malware Protection and Sandbox Detection

Bug ID	Description
790166	Antivirus scan does not show quarantined files.

Known issues

The following issues have been identified in FortiClient (macOS) 6.4.10. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Avatar and social login information

Bug ID	Description
690354	Phone number and email address that a domain user account manually specified changes when user logs in with service account.

Install and upgrade

Bug ID	Description
754722	Uninstall deployment from EMS 7.0.2 does not work on FortiClient (macOS).
755309	FortiClient triggers installation of Web Filter system extension only if custom.conf contains all installer features.
810176	Upgrading FortiClient removes macOS certificate.

Endpoint control

Bug ID	Description
723599	FortiClient (macOS) uses FortiSASE egress IP address as public IP address.

Logs

Bug ID	Description
742102	Clearing logs from FortiClient GUI does not clear all logs.

Malware Protection and Sandbox Detection

Bug ID	Description
551282	Sandbox exception for trusted sources does not work. FortiClient uploads files sourced from Apple Inc.
630205	About page shows incorrect cloud FortiSandbox signature status as not configured.
719920	FortiClient cannot submit files downloaded from Thunderbird to Cloud Sandbox.
813376	Antivirus (AV) logs shows AV as disabled even though all features are enabled and fully licensed EMS is managing FortiClient.
888356	User can stop AV quick/full scan that EMS triggered.
894699	User must manually add fmon2 process to grant permission under security settings.

Remote Access

Bug ID	Description
694070	FortiClient (macOS) connected to IPsec VPN cannot get ems-tag in firewall dynamic address list.
813239	VPN disconnects intermittently and cannot reconnect on macOS 12.
826381	SAML autoconnect and always up do not work.
826938	Split tunnel does not work properly.

Application Firewall

Bug ID	Description
718957	Application Firewall does not work after reboot.

Web Filter and plugin

Bug ID	Description
771853	Web Filter does not work as expected on macOS Monterey (version 12).
772332	External Ethernet adapter dongle disconnects when running speed test.

Bug ID	Description
857879	Web Filter exclusion list URLs do not work properly.

Zero Trust tags

Bug ID	Description
697655	Zero trust network access tag for FileVault detection disappears after a few seconds.
726818	IP addresses are not populated on FortiGate for Zero Trust tags assigned to macOS clients.

Performance

Bug ID	Description
778651	Large downloads and speed tests result in high latency, packet loss, and poor performance.