FortiClient (macOS) - Release Notes

Version 6.4.7

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

November 25, 2021
FortiClient (macOS) 6.4.7 Release Notes
04-647-758986-20211125

TABLE OF CONTENTS

Change log

Date	Change description
2021-11-25	Initial release.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (macOS) 6.4.7 build 1405.

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 10 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 6.4.7 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

Endpoint security improvement

EMS 6.4.7 adds an improvement to endpoint security that impacts compatibility between FortiClient and EMS, and the recommended upgrade path. The FortiClient 6.4.7 installer is not available on FortiGuard Distribution Servers (FDS). To install the FortiClient 6.4.7 installer, you must download it from Customer Service & Support. See Endpoint security improvement.

If the EMS server certificate is invalid, and FortiClient is upgraded to 6.4.7, by default, FortiClient displays a warning message on the GUI when trying to connect to the EMS. The end user should click *allow* to complete the connection. FortiClient does not connect to the EMS if the end user selects *deny*. If the end user selects *deny*, FortiClient retries connecting to the EMS after a system reboot. The same warning message displays while trying to connect to the EMS. The end user should click *allow* to complete the connection.

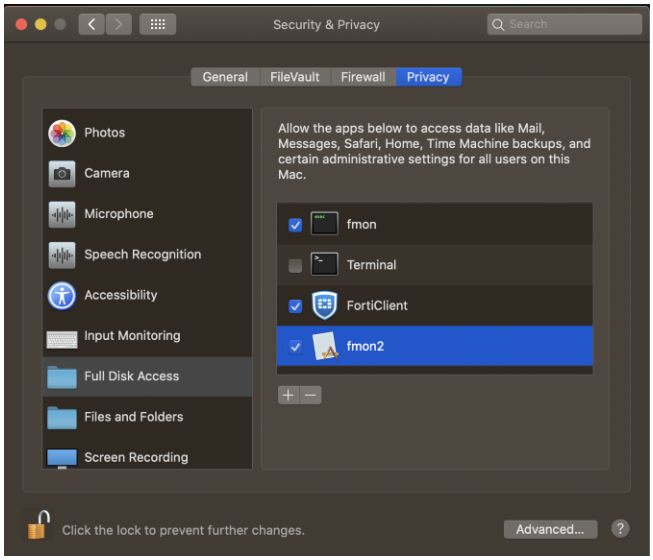
Enabling full disk access on macOS 11 Big Sur and 10.15 Catalina

You can install FortiClient (macOS) 6.4.7 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
- fmon
- fmon2
- FortiClient
- FortiClientAgent

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/FortiClientAgent.app`

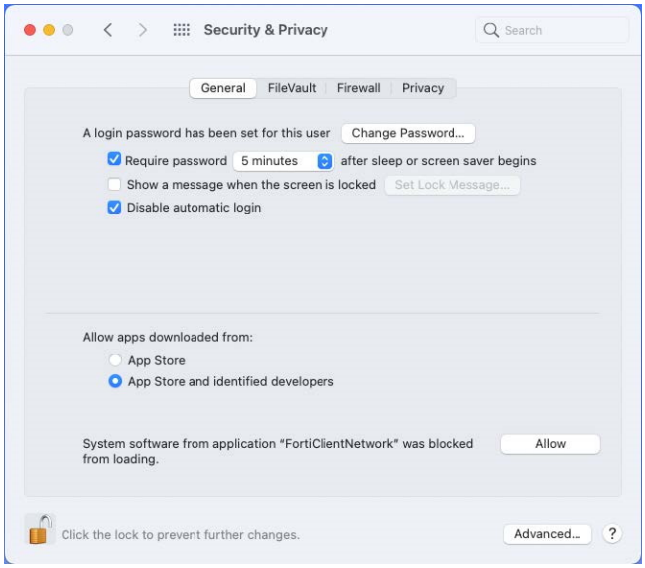
Activating system extensions

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:

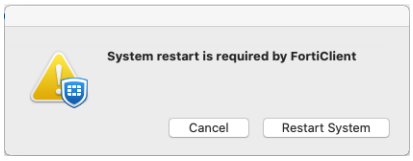
1. Go to *System Preferences* > *Notifications* > *FortiClientAgent*.
2. Toggle *Allow Notifications* on.

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_6.4.7.xxxx_macosx.tar.gz	Includes utility tools and files to help with installation.
FortiClientVPNSetup_6.4.7.xxxx_macosx.dmg	Free VPN-only installer.

The following files are available from FortiClient.com:

File	Description
FortiClient_6.4.7.xxxx_macosx.dmg	Standard installer for macOS.
FortiClientVPNSetup_6.4.7.xxxx_macosx.dmg	Free VPN-only installer.

FortiClient EMS 6.4 includes the FortiClient (macOS) 6.4.7 standard installer.

Review the following sections prior to installing FortiClient version 6.4.7: Introduction on page 5, Special notices on page 6, and Product integration and support on page 12.

Upgrading from previous FortiClient versions

You must upgrade EMS to 6.4.7 before upgrading FortiClient.

FortiClient version 6.4.7 supports upgrade from FortiClient 6.2.

FortiClient (macOS) 6.4.7 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 6.4.7 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) 6.4.7 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	• 7.0.0 and later • 6.4.1 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) 6.4.7. For inquiries about a particular bug, contact Customer Service & Support.

Remote Access

Bug ID	Description
664285	VPN connection terminates unexpectedly with error code -121.
684913	SAML authentication on SSL VPN with realms does not work
725855	FortiClient fails to autoconnect to FortiSASE VPN.

Web Filter

Bug ID	Description
613833	Web Filter blocks TLS 1.3 webpages inconsistently across different macOS versions.

Endpoint control

Bug ID	Description
675953	FortiClient cannot store the Telemetry connection key
713082	After disconnecting and reregistering to EMS, FortiClient displays wrong on-Fabric status and receives the wrong profile. This occurs after deployment as well.
717650	FortiClient (macOS) cannot automatically connect to EMS.
719193	IP address Zero Trust tagging rule does not work when endpoint IP address changes.
719766	FortiClient does not reconnect to original EMS if migrated to an unreachable EMS.
725828	FortiClient (macOS) features on tabs do not match endpoint's assigned profile's features.

Known issues

The following issues have been identified in FortiClient (macOS) 6.4.7. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Upgrade

Bug ID	Description
705952	Upgrading VPN-only client using online installer fails.

Endpoint control

Bug ID	Description
664634	FortiClient cannot register with FortiClient Cloud if the connection key has a hyphen.
706496	Deep inspection does not work and the certificate is not downloaded on the endpoint.
717493	FortiClient loses EMS connection and asks for Telemetry key if EMS FQDN resolution changes.

GUI

Bug ID	Description
705518	FortiTray does not differentiate between corporate and personal VPNs.
714853	Unlock button not visible after deregistering from EMS.

Malware Protection

Bug ID	Description
725379	FortiClient does not quarantine files in macOS Mail application folder.

Remote Access

Bug ID	Description
678564	FortiClient (macOS) does not honor `remoteauthtimeout` or `login-timeout` from FortiGate with SAML authentication.
690432	GUI fails to import XML VPN configuration.
697099	Traffic bypasses the web filter when it goes through the IPsec VPN tunnel.
723304	User information does not update when switching users.
723935	FortiClient does not support always-on connections when using SAML SSO.
725444	EMS displays incorrect SSL VPN IP address for macOS endpoint. EMS shows the endpoint's local IP address instead after SSL VPN connection.
726590	FortiClient does not connect using DTLS as configured.

Application Firewall

Bug ID	Description
718657	FortiClient (macOS) does not show error prompt when registration to unreachable FortiClient Cloud fails.
718957	Application Firewall does not work after rebooting macOS machine.

Other

Bug ID	Description
762132	FortiClientAgent and FortiTray names display as "Placeholder Developer" on some macOS devices. This is a known macOS bug for third-party products.