FortiClient (macOS) - Release Notes

Version 6.2.7

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/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdoc@fortinet.com

September 11, 2020
FortiClient (macOS) 6.2.7 Release Notes
04-627-637107-20200911

TABLE OF CONTENTS

Change log

Date	Change Description
2020-06-02	Initial release.
2020-09-11	Added Common Vulnerabilities and Exposures on page 13.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (macOS) 6.2.7 build 0756.

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 8 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 6.2.7 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.

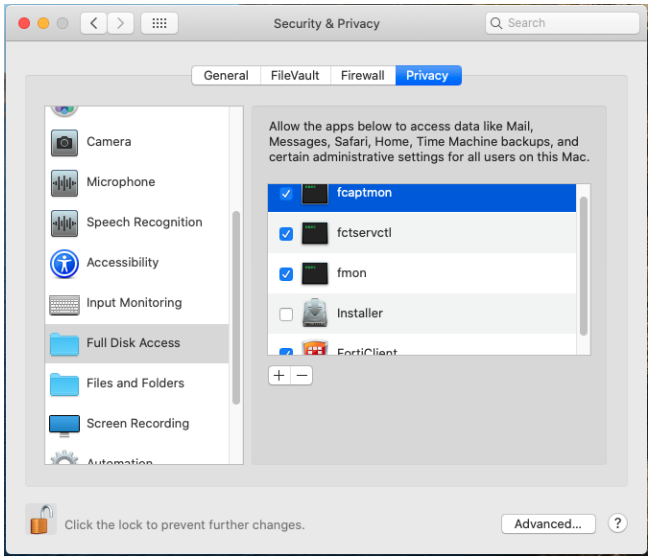
FortiClient 6.2.0 offers a free VPN-only version that can be used for VPN-only connectivity to FortiGate devices running FortiOS 5.6 and later versions. You can download the VPN-only application from FortiClient.com.

Special notices

FortiClient on macOS Catalina (version 10.15)

You can install FortiClient (macOS) 6.2.7 on macOS 10.15 Catalina. With this macOS release, however, FortiClient works properly only when you grant permissions to access the full disk in the *Security & Privacy* pane for the following services:

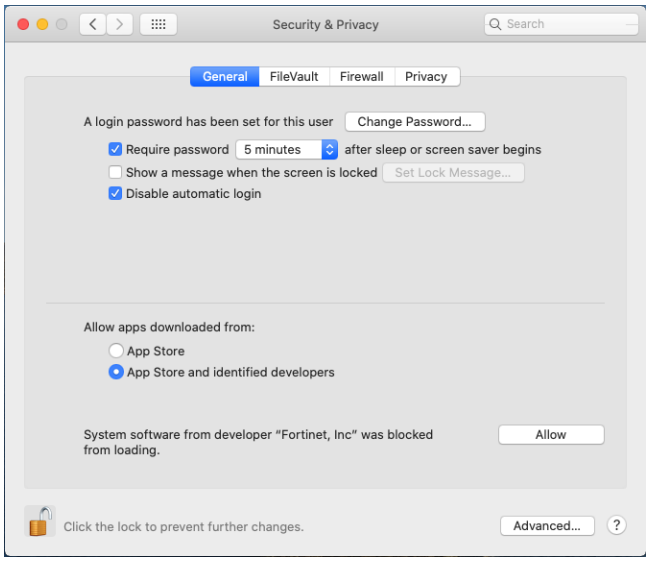
- fcaptmon
- fctservctl
- fmon
- FortiClient



On macOS 10.15 Catalina, the system also displays a reboot prompt following FortiClient installation. Reboot the machine before lauching FortiClient for the first time.

Web Filter

The FortiClient (macOS) Web Filter feature works properly only when you allow system software from Fortinet to load in *Security & Privacy* settings. Go to *System Preferences* > *Security & Privacy* and click the *Allow* button beside *System software from developer "Fortinet, Inc" was blocked from loading*. You must have administrator credentials for the macOS machine to configure this change.



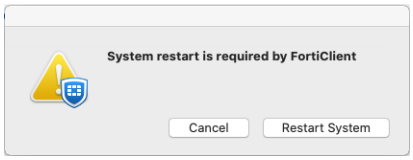
FortiClient (macOS) does not support Web Filter for websites using TLS 1.3.

DHCP over IPsec VPN not supported

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

macOS Catalina (version 10.15) reboot prompt

When using macOS Catalina (version 10.15), 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.

Installation information

Firmware images and tools

The following file is available from the Fortinet support site:

File	Description
FortiClientTools_6.2.7.0756_macosx.tar.gz	Includes utility tools and files to help with installation.

The following file is available from FortiClient.com:

File	Description
FortiClientVPNSetup_6.2.7.0756_ macosx.dmg	Free VPN-only installer.

FortiClient EMS 6.2.7 includes the FortiClient (macOS) 6.2.7 standard installer.

Review the following sections prior to installing FortiClient version 6.2.7: Introduction on page 5, Special notices on page 6, and Product integration and support on page 10.

Installation options

When the administrator creates a FortiClient deployment package in EMS, they choose which setup type and modules to install:

- Secure Remote Access: VPN components (IPsec and SSL) are installed.
- Advanced Persistent Threat (APT) Components: FortiSandbox detection feature is installed.
- Additional Security Features: One or more of the following features is installed: AntiVirus, Web Filtering, Single Sign On, and Application Firewall.

The FortiClient (macOS) installer is available on EMS. You can configure and select installed features and options on EMS.

Upgrading from previous FortiClient versions

FortiClient version 6.2.7 supports upgrade from FortiClient versions 6.0 and later.

Starting with FortiClient 6.2.0, FortiClient EMS 6.2.0, and FortiOS 6.2.0, the FortiClient Endpoint Telemetry license is deprecated. The FortiClient Compliance profile under *Security Profiles* and the *Enforce FortiClient Compliance Check* option on the interface configuration pages have been removed from the FortiOS GUI. Endpoints running FortiClient 6.2.0 now register only with FortiClient EMS 6.2.0 and compliance is accomplished through the use of compliance verification rules configured on FortiClient EMS 6.2.0 and enforced through the use of firewall policies. As a result, there are two upgrade scenarios:

- Customers using only a FortiGate device in FortiOS 6.0 to enforce compliance must install FortiClient EMS 6.2.0 and purchase a FortiClient Security Fabric Agent License for their FortiClient EMS installation to continue using compliance features.
- Customers using both a FortiGate device in FortiOS 6.0 and FortiClient EMS running 6.0 for compliance enforcement must upgrade the FortiGate device to FortiOS 6.2.0, FortiClient to 6.2.0, and FortiClient EMS to 6.2.0.

FortiClient (macOS) 6.2.7 features are only enabled when connected to EMS 6.2.0. If FortiClient (macOS) 6.0 was previously running in standalone mode, ensure to install EMS 6.2.0, apply the license as appropriate, then connect FortiClient (macOS) to EMS before upgrading to FortiClient (macOS) 6.2.7. You should first upgrade any endpoint running a FortiClient (macOS) version older than 6.0.0 to 6.0.5 using existing 6.0 upgrade procedures.

See the *FortiClient and FortiClient EMS Upgrade Paths* for information on upgrade paths and order in which to upgrade Fortinet products.

Downgrading to previous versions

Downgrading FortiClient version 6.2.7 to previous FortiClient versions is not supported.

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) 6.2.7 product integration and support information:

Desktop operating systems	• macOS Catalina (version 10.15) • macOS Mojave (version 10.14) • macOS High Sierra (version 10.13)
Minimum system requirements	• Intel processor • 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
FortiAnalyzer	• 6.2.0 and later
FortiAuthenticator	• 6.1.0 and later • 6.0.0 and later
FortiClient EMS	• 6.4.0 and later • 6.2.0 and later
FortiManager	• 6.2.0 and later
FortiOS	The following FortiOS versions support Telemetry and IPsec and SSL VPN with FortiClient (macOS) 6.2.7: • 6.2.0 and later • 6.0.0 and later The following FortiOS versions support IPsec and SSL VPN with FortiClient (macOS) 6.2.7: • 6.4.0 and later • 5.6.0 and later
FortiSandbox	• 3.1.0 and later • 3.0.0 and later • 2.5.0 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) 6.2.7. For inquiries about a particular bug, contact Customer Service & Support.

Install and upgrade

Bug ID	Description
620102	FortiClient (macOS) loses features.
623519	macOS 10.15.4 and later versions require system reboot for newly installed FortiClient.

Malware Protection

Bug ID	Description
550046	Copying extracted Eicar files does not trigger virus alert.
572620	RTP detection prompt detail section is blank in macOS 10.14.6.

Sandbox Detection

Bug ID	Description
597180	Sandbox remediation action differs from remediation action that the GUI reports.
611763	FortiClient (macOS) cannot update Sandbox signatures.

Remote Access

Bug ID	Description
619898	fctctld does not exit after VPN disconnects.

Vulnerability Scan

Bug ID	Description
565438	GUI keeps showing vulnerabilities on the scan details page after patching them.

EMS deployment

Bug ID	Description
588656	FortiClient (macOS) deployment from EMS may fail.

Endpoint control

Bug ID	Description
601248	EMS fails to deregister FortiClient (macOS).

Other

Bug ID	Description
618242	Antivirus evasion via malformed RAR file.

Common Vulnerabilities and Exposures

Bug ID	Description
618242	FortiClient (macOS) 6.2 running AV engine version 6.00243 or later is no longer vulnerable to the following CVE Reference: • CVE-2020-9295 Visit https://fortiguard.com/psirt for more information.

Known issues

The following issues have been identified in FortiClient (macOS) 6.2.7. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Application Firewall

Bug ID	Description
578810	FortiClient blocks traffic between Xcode software and Apple TV.

Install and upgrade

Bug ID	Description
634010	FortiClient (macOS) sync issue in Mojave.

Endpoint control

Bug ID	Description
605831	FortiClient (macOS) does not become quarantined when it is dually registered to EMS and FortiOS.
609245	FortiClient cannot register to EMS if a registration key is enabled.
632117	FortiClient (macOS) does not send virtual adapter interface IP address to EMS.

Remote Access

Bug ID	Description
605438	FortiClient (macOS) does not save the username for an SSL VPN tunnel.
614371	SSL VPN does not connect after waking the computer from sleep.

Bug ID	Description
634037	Preshared key (PSK) length causes FortiClient to fail to connect to IPsec VPN.
634608	IPsec VPN gets stuck on connecting when using PSK with special characters.
634973	VPN connection fails.

Sandbox

Bug ID	Description
597278	EMS shows incorrect rating for FortiSandbox result for macOS devices.
592029	Sandbox ignores changing file size limit for device submissions when submissions come from FortiClient (macOS).

Vulnerability Scan

Bug ID	Description
614425	EMS fails to remotely patch critical and high vulnerabilities on FortiClient (macOS).

Performance

Bug ID	Description
632087	FortiClient (macOS) fmon process crashes.

Other

Bug ID	Description
607904	FTGDAGENT memory leak.