FortiClient (macOS) - Release Notes

Version 6.2.3

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

January 27, 2019
FortiClient (macOS) 6.2.3 Release Notes
04-623-597451-20200127

TABLE OF CONTENTS

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (macOS) 6.2.3 build 0707.

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 7 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 6.2.3 supports a 30-day trial license with ten FortiClient seats.

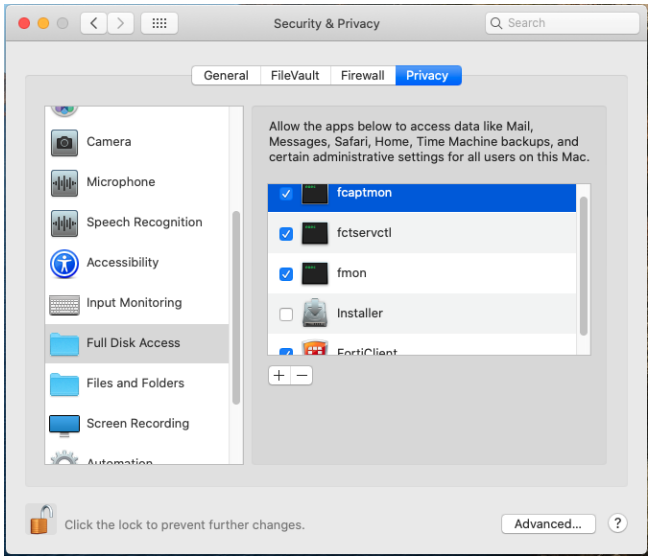
FortiClient 6.2.0 offers a free VPN-only version that can be used for VPN-only connectivity to FortiGate devices running FortiOS 5.6 and later versions. You can download the VPN-only application from FortiClient.com.

Special notices

FortiClient on macOS Catalina (version 10.15)

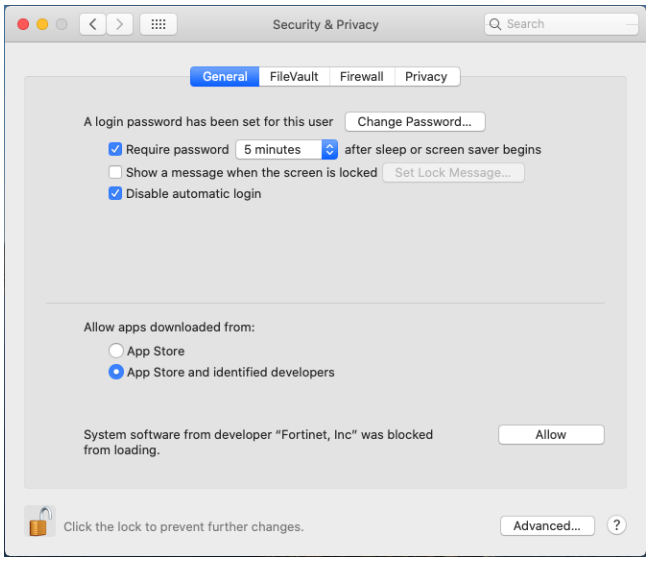
You can install FortiClient (macOS) 6.2.3 on macOS 10.15 Catalina, which Apple released in early October 2019. With this macOS release, however, the antivirus (AV) features in FortiClient will work properly only when you grant permissions to access the full disk in the *Security & Privacy* pane for the following services:

- fcaptmon
- fctservctl
- fmon
- FortiClient



FortiClient 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.


Security & Privacy
Search
General
FileVault
Firewall
Privacy
A login password has been set for this user
Change Password...
Require password
5 minutes
after sleep or screen saver begins
Show a message when the screen is locked
Set Lock Message...
Disable automatic login
Allow apps downloaded from:
App Store
App Store and identified developers
System software from developer "Fortinet, Inc" was blocked from loading.
Allow
Click the lock to prevent further changes.
Advanced...
?

Installation information

Firmware images and tools

The following file is available from the Fortinet support site:

File	Description
FortiClientTools_6.2.3.xxx_macosx.tar.gz	Includes utility tools and files to help with installation.

The following file is available from FortiClient.com:

File	Description
FortiClientVPNOnlineInstaller_6.2.dmg	Free VPN-only installer.

FortiClient EMS 6.2.3 includes the FortiClient (macOS) 6.2.3 standard installer.

Review the following sections prior to installing FortiClient version 6.2.3: Introduction on page 4, and Product integration and support on page 9.

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 6.2.3 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) 6.2.3 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) 6.2.3. 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 6.2.3 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) 6.2.3 product integration and support information:

Desktop operating systems	• macOS Catalina (version 10.15) • macOS Mojave (version 10.14) • macOS High Sierra (version 10.13) • macOS Sierra (version 10.12)
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	• 4.2.1 FortiClient (macOS) does not support FortiToken Mobile push notification for the following versions: • 4.2.0 • 4.1.0 and later • 3.3.0 and later • 3.2.0 and later • 3.1.0 and later • 3.0.0 and later
FortiClient EMS	• 6.2.0 and later
FortiManager	• 6.2.0 and later
FortiOS	• 6.2.0 and later • 6.0.0 and later Telemetry, IPsec VPN, and SSL VPN are supported. See important information in Upgrading from previous FortiClient versions on page 7. • 5.6.0 and later IPsec VPN and SSL VPN are supported. See important information in Upgrading from previous FortiClient versions on page 7.
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) 6.2.3. For inquiries about a particular bug, contact Customer Service & Support.

Avatar

Bug ID	Description
589239	FortiClient (macOS) avatar user input camera capture button does not work.

GUI

Bug ID	Description
599243	FortiClient (macOS) crashes when clicking *User Input*.

Malware Protection

Bug ID	Description
569248	FortiClient (macOS) antivirus does not work on macOS Catalina 10.15 beta.
588914	macOS customized manual scan shows no files scanned if the folder has few items.

Sandbox Detection

Bug ID	Description
577852	FortiClient (macOS) Sandbox reports FortiClient (macOS) as unauthorized even if it is registered to an EMS that FortiSandbox has authorized.
586722	FortiClient (macOS) blocks files based on FortiSandbox results that are inconsistent with the FortiSandbox console.

Remote Access

Bug ID	Description
547541	IPsec tray and GUI with certificate do not match.
583944	Obsolete route to the SSL server fails to be deleted.
588103	FortiClient (macOS) should bring back peer in login check request.
590317	NAT-T fails to be negotiated between the FortiGate and FortiClient (macOS).
590402	SSL VPN is stuck on connecting on macOS Catalina.
594271	FortiClient (macOS) blocks native VPN on macOS when Application Firewall or Web Filter is enabled.

Host verification check

Bug ID	Description
578680	User-defined host check error message does not take effect on FortiClient (macOS).

EMS deployment

Bug ID	Description
599965	Deploying FortiClient (macOS) from EMS fails because of leftover fct_uninstall_pipe under /tmp/ folder: • Rebooting the machine cleans up the /tmp/ folder and the fct_uninstall_pipe file. • You can manually delete the fct_uninstall_pipe file from the /tmp/ folder. After above operation, EMS successfully deploys FortiClient (macOS) 6.2.3.

Other

Bug ID	Description
574178	FortiClient (macOS) does not send the correct network interface information in FortiAnalyzer log.
586579	FortiClient (macOS) fails to restart epctrl process when the client machine is booted after abnormal shutdown.
588115	fcconfig high memory usage (less than 1.5 GB) on macOS.

Known issues

The following issues have been identified in FortiClient (macOS) 6.2.3. 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.
586821	Application firewall daemon fails to start itself after registering to EMS.

Avatar

Bug ID	Description
589432	Avatar page is blank after upgrade.

Endpoint control

Bug ID	Description
546973	FortiClient can break quarantined state after system reboot.
567858	FortiClient (macOS) should send all IP addresses to EMS.
582013	FortiClient (macOS) reconnects to EMS after one keep alive interval when EMS deregisters the endpoint.
582706	FortiClient (macOS) does not send AV Cloud Scan quarantine events to EMS endpoint details page.
585896	FortiClient (macOS) shows no IP address and unknown serial number after assigning the non-default profile.
590175	FortiClient GUI shows incorrect EMS connection status for an unreachable EMS.

Malware Protection

Bug ID	Description
582056	Antivirus CloudScan does not detect test EICAR malware when downloaded from email attachment.

Remote Access

Bug ID	Description
582197	macOS endpoints cannot reach local gateway when connected to IPsec VPN with FortiClient (macOS).
600690	EMS provisioning shows invalid configuration for VPN.
602408	Creating a new VPN does not work. Workaround: Close the FortiClient (macOS) GUI and reopen it.

Sandbox

Bug ID	Description
597180	Sandbox remediation action is set to alert but GUI shows that it quarantined the file.

Vulnerability Scan

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

Web Filter

Bug ID	Description
581890	FortiClient GUI cannot retrieve Web Filter violation list from `wf.db` after EMS deregistration.

EMS deployment

Bug ID	Description
586967	FortiSandbox and cloud malware protection are not installed if AV real time protection is excluded in the deployment package.
600744	FortiClient (macOS) deployment does not work because *Install now* prompt shows while user is still downloading the installer.
600753	FortiClient (macOS) deployment status is stuck on endpoint notified after successful deployment.

Update

Bug ID	Description
566085	FortiClient (macOS) updates all signatures after fresh install without a valid license from EMS.
588221	Custom FortiGuard distribution server (FDS) failover to global legacy FDS does not work.
594004	FortiClient (macOS) connects to the wrong legacy U.S. server when EMS is configured for the legacy U.S. FDS.

Change log

Date	Change Description
2019-12-19	Initial release.
2020-01-06	Updated Introduction on page 4. Added 602408 to Remote Access on page 14.
2020-01-27	Added FortiClient Web Filter on page 5.