

FortiClient (macOS) - Release Notes

Version 6.2.8

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



October 13, 2020

FortiClient (macOS) 6.2.8 Release Notes

04-628-665673-20201013

TABLE OF CONTENTS

Change log	4
Introduction	5
Licensing	5
Special notices	6
FortiClient on macOS Catalina (version 10.15)	6
Web Filter	6
DHCP over IPsec VPN not supported	7
macOS Catalina (version 10.15) reboot prompt	7
IKEv2 not supported	7
Installation information	8
Firmware images and tools	8
Installation options	8
Upgrading from previous FortiClient versions	8
Downgrading to previous versions	9
Uninstalling FortiClient	9
Firmware image checksums	9
Product integration and support	10
Language support	10
Resolved issues	12
GUI	12
Install and upgrade	12
Sandbox Detection	12
Remote Access	12
Vulnerability Scan	13
Web Filter	13
Other	13
Known issues	14
Application Firewall	14
Install and upgrade	14
Endpoint control	14
Malware Protection	14
Remote Access	15
Sandbox Detection	15
Vulnerability Scan	15
Web Filter	15
Other	15

Change log

Date	Change Description
2020-10-13	Initial release.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (macOS) 6.2.8 build 0774.

This document includes the following sections:

- [Special notices on page 6](#)
- [Installation information on page 8](#)
- [Product integration and support on page 10](#)
- [Resolved issues on page 12](#)
- [Known issues on page 14](#)

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 6.2.8 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) 6.2.8 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:

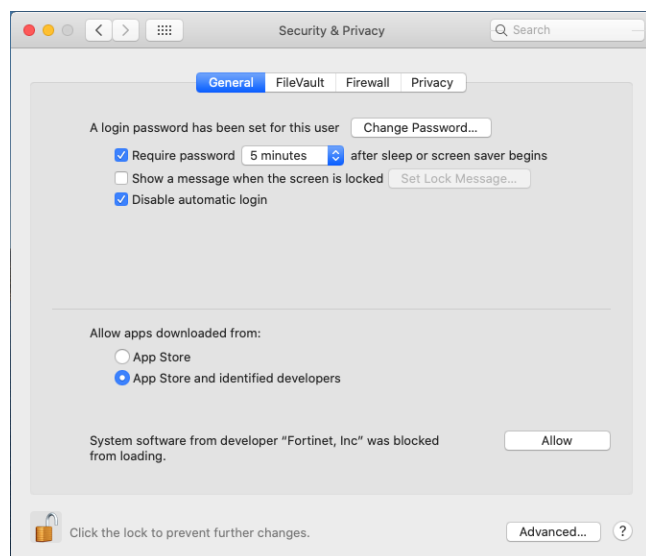
- fcaptmon
- fctservctl
- fmon
- FortiClient



On macOS 10.15 Catalina, the system also displays a reboot prompt following FortiClient installation. Reboot the machine before launching 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.



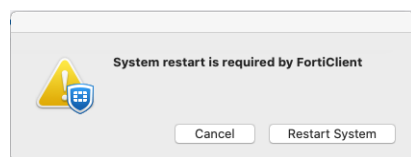
FortiClient (macOS) does not support Web Filter for websites using TLS 1.3.

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_6.2.8.0774_macosx.tar.gz	Includes utility tools and files to help with installation.

The following file is available from [FortiClient.com](#):

File	Description
FortiClientVPNSetup_6.2.8.0774_macosx.dmg	Free VPN-only installer.

FortiClient EMS 6.2.8 includes the FortiClient (macOS) 6.2.8 standard installer.



Review the following sections prior to installing FortiClient version 6.2.8: [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 6.2.8 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) 6.2.8 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) 6.2.8. 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 6.2.8 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) 6.2.8 product integration and support information:

Desktop operating systems	<ul style="list-style-type: none">• macOS Catalina (up to and including version 10.15.3)• macOS Mojave (version 10.14)• macOS High Sierra (version 10.13)
Minimum system requirements	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 6.2.0 and later
FortiAuthenticator	<ul style="list-style-type: none">• 6.1.0 and later• 6.0.0 and later
FortiClient EMS	<ul style="list-style-type: none">• 6.4.0 and later• 6.2.0 and later
FortiManager	<ul style="list-style-type: none">• 6.2.0 and later
FortiOS	<p>The following FortiOS versions support Telemetry and IPsec and SSL VPN with FortiClient (macOS) 6.2.8:</p> <ul style="list-style-type: none">• 6.2.0 and later• 6.0.0 and later <p>The following FortiOS versions support IPsec and SSL VPN with FortiClient (macOS) 6.2.8:</p> <ul style="list-style-type: none">• 6.4.0 and later• 5.6.0 and later
FortiSandbox	<ul style="list-style-type: none">• 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) 6.2.8. For inquiries about a particular bug, contact [Customer Service & Support](#).

GUI

Bug ID	Description
650443	Cannot change GUI language with <culture_code>.

Install and upgrade

Bug ID	Description
655953	FortiClientVPN_OnlineInstaller fails to download any free VPN image from FDS.

Sandbox Detection

Bug ID	Description
592029	Changing filesize limit for device submissions is ignored when submissions come from FortiClient (macOS).

Remote Access

Bug ID	Description
614371	SSL VPN does not connect after waking from sleep.
634037	Preshared key length causes FortiClient to fail to connect to IPsec VPN.

Vulnerability Scan

Bug ID	Description
614425	EMS action fails to remotely patch critical and high vulnerabilities.

Web Filter

Bug ID	Description
634667	Web Filter slows down Resilio file share application performance on macOS.

Other

Bug ID	Description
607904	FTGDAGENT memory leak.
632087	fmon process crashes.

Known issues

The following issues have been identified in FortiClient (macOS) 6.2.8. 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.
615633	macOS freezes when FortiClient (macOS) and Google File Stream are installed.

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.

Malware Protection

Bug ID	Description
628153	macOS devices fail to detect plugged in iOS devices when real-time protection is enabled.

Remote Access

Bug ID	Description
579768	FortiClient (macOS) does not display bubble notification for VPN disconnection.
605438	FortiClient (macOS) does not save the username for an SSL VPN tunnel.
627962	IP address shows local address on EMS while connected via tunnel instead of tunnel address.
634608	IPsec VPN gets stuck on connecting when using preshared key with special characters.
634973	VPN connection fails - error 104.
662105	FortiClient (macOS) does not load all 1000 routes from FortiGate SSL VPN.

Sandbox Detection

Bug ID	Description
597278	EMS shows incorrect rating for FortiSandbox result for macOS devices.

Vulnerability Scan

Bug ID	Description
635014	FortiClient detects some office products as vulnerable when latest update is installed.

Web Filter

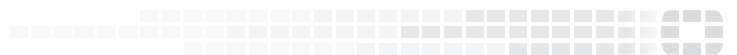
Bug ID	Description
643707	Web Filter affects browsing and Internet usage.

Other

Bug ID	Description
626322	macOS client does not use DNS suffixes configured in OS.
628843	Approximately four hours after bootup, FortiClient consumes up to 5 GB RAM.



FORTINET®



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.