



FortiClient (macOS) - Release Notes

Version 6.0.9

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



February 21, 2020

FortiClient (macOS) 6.0.9 Release Notes

04-609-593460-20200221

TABLE OF CONTENTS

Introduction	4
Licensing	4
Standalone mode	4
Managed mode	4
Special notices	6
FortiClient on macOS Catalina (version 10.15)	6
Installation information	7
Firmware images and tools	7
Installation options	7
Upgrading from previous FortiClient versions	7
Downgrading to previous versions	8
Uninstalling FortiClient	8
Firmware image checksums	8
Product integration and support	9
FortiClient 6.0.9 support information	9
Resolved issues	11
Remote Access	11
Install and upgrade	11
Known issues	12
Vulnerability Scan	12
Other	12
Change log	13

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (macOS) 6.0.9 build 0162.

This document includes the following sections:

- [Special notices on page 6](#)
- [Installation information on page 7](#)
- [Product integration and support on page 9](#)
- [Resolved issues on page 11](#)
- [Known issues on page 12](#)

Review all sections prior to installing FortiClient. For more information, see the [FortiClient Administration Guide](#).

Licensing

FortiClient offers two licensing modes: standalone mode and managed mode.

Standalone mode

In standalone mode, FortiClient is not connected to a FortiGate or FortiClient Enterprise Management Server (EMS). In this mode, FortiClient is free for private individuals and commercial businesses to use. No license is required.



Support for FortiClient in standalone mode is provided on the [Fortinet Forums](#). Phone support is not provided.

Managed mode

Companies with large installations of FortiClient usually need a means to manage their endpoints. EMS can be used to provision and centrally manage FortiClient endpoints, and FortiGate can be used with FortiClient endpoints for network security. Each FortiClient endpoint can connect to a FortiGate or an EMS. In this mode, FortiClient licensing is applied to the FortiGate or EMS. No separate license is required on FortiClient itself.



When using the ten free trial licenses for FortiClient in managed mode, support is provided on the [Fortinet Technical Discussion Forums](#). Phone support is not provided when using the free trial licenses. Phone support is provided for paid licenses.

FortiClient licenses on the FortiGate

FortiGate 30 series and higher models include a FortiClient free trial license for ten connected FortiClient endpoints. For additional connected endpoints, you must purchase a FortiClient license subscription. Contact your Fortinet sales representative for information about FortiClient licenses.

FortiClient licenses on the EMS

EMS includes a FortiClient free trial license for ten connected FortiClient endpoints for evaluation. For additional connected endpoints, you must purchase a FortiClient license subscription. Contact your Fortinet sales representative for information about FortiClient licenses.

Special notices

FortiClient on macOS Catalina (version 10.15)

You can install FortiClient (macOS) 6.0.9 on macOS 10.15 Catalina, which Apple released in early October 2019. With this macOS release, however, FortiClient works properly only when you grant permissions to access the full disk in the *Security and Privacy* pane for the following services:

- fcaptmon
- fctservctl
- fmon
- FortiClient



Installation information

Firmware images and tools

The following files are available in the firmware image file folder:

File	Description
FortiClient_6.0.9.xxx_macosx.dmg	Standard installer for macOS.
FortiClientTools_6.0.9.x.xxx_macosx.tar	Includes utility tools and files to help with installation.

The following tools and files are available in the FortiClientTools .tar file:

File	Description
OnlineInstaller	Downloads and installs the latest FortiClient file from the public FDS.



Review the following sections prior to installing FortiClient version 6.0.9: [Introduction on page 4](#), [Special notices on page 6](#), and [Product integration and support on page 9](#).

Installation options

When installing FortiClient version 6.0.9, you can choose the setup type that best suits your needs. FortiClient will always install the Fortinet Security Fabric Agent (SFA) feature and enable the Vulnerability Scan feature by default. You can select to install one or more of the following options:

- Secure Remote Access: VPN components (IPsec and SSL) will be installed.
- Additional Security Features: Select one or more of the following to install: AntiVirus, Web Filtering, Single Sign On, Application Firewall

Upgrading from previous FortiClient versions

FortiClient version 6.0.9 supports upgrading from FortiClient versions 5.2 and later.

If you are deploying an upgrade from FortiClient 5.6.2 or earlier versions via FortiClient EMS and the upgrade fails, uninstall FortiClient on the endpoints, then deploy the latest version of FortiClient.

Downgrading to previous versions

Downgrading FortiClient version 6.0.9 to previous FortiClient versions is not supported.

Uninstalling FortiClient

To uninstall FortiClient version 6.0.9, use the *Application > FortiClient > Uninstaller* application.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal located at <https://support.fortinet.com>. 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

FortiClient 6.0.9 support information

Desktop operating systems	<ul style="list-style-type: none">• macOS Catalina (version 10.15)• macOS Mojave (version 10.14)• macOS High Sierra (version 10.13)• macOS Sierra (version 10.12)
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• 6.0.0 and later• 5.6.0 and later
FortiAuthenticator	<ul style="list-style-type: none">• 4.2.1 <p>FortiClient (macOS) does not support FortiToken Mobile push notification for the following versions:</p> <ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 6.2.0 and later• 6.0.0 and later
FortiManager	<ul style="list-style-type: none">• 6.2.0 and later• 6.0.0 and later• 5.6.0 and later
FortiOS	<ul style="list-style-type: none">• 6.0.0 and later• 5.6.0 and later <p>FortiClient (macOS) supports only IPsec VPN and SSL VPN with the following FortiOS versions:</p> <ul style="list-style-type: none">• 6.2.0 and later• 5.4.1 and later

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, FortiClient defaults to English.

Resolved issues

The following issues have been fixed in FortiClient (macOS) 6.0.9. For inquiries about a particular bug, contact [Customer Service & Support](#).

Remote Access

Bug ID	Description
568508	Failure to connect IPsec VPN using certificate authentication.

Install and upgrade

Bug ID	Description
588495	fctservctl crash during EMS deployment of FortiClient macOS to endpoints.

Common Vulnerabilities and Exposures

Bug ID	Description
575641	FortiClient (macOS) 6.0.9 is no longer vulnerable to the following CVE reference: <ul style="list-style-type: none">• CVE-2019-17650

Known issues

The following issues have been identified in FortiClient (macOS) 6.0.9. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

Vulnerability Scan

Bug ID	Description
534567	Vulnerability scan resumes after the user manual stops it.

Other

Bug ID	Description
546973	FortiClient (macOS) can break out of its quarantined state after system reboot.

Change log

Date	Change Description
2019-11-13	Initial release.
2020-02-21	Updated FortiClient on macOS Catalina (version 10.15) on page 6.



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.