



FortiClient (macOS) - Release Notes

Version 6.0.5

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 COOKBOOK

<https://cookbook.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: techdocs@fortinet.com



January 31, 2019

FortiClient (macOS) 6.0.5 Release Notes

04-605-533968-20190131

TABLE OF CONTENTS

Introduction	4
Licensing	4
Standalone mode	4
Managed mode	4
Special notices	6
Using Web Filter and Real Time Protection with FortiClient (macOS)	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 6.0.5 support information	9
Language support	9
Resolved issues	11
Malware Protection	11
Endpoint control	11
Remote Access	11
GUI	11
Install and upgrade	12
Other	12
Known issues	13
Application Firewall	13
Web Filter	13
Remote Access	13
Endpoint control	13
Other	14
Change log	15

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (macOS) 6.0.5 build 0104.

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 13](#)

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

Using Web Filter and Real Time Protection with FortiClient (macOS)

When using FortiClient (macOS), Web Filter and Real Time Protection may not function properly unless the following steps are taken:

1. Reboot the Mac in recovery mode by holding down the Command and R keys.
2. Go to Utilities and start the Terminal.
3. Issue the following command:
4. Reboot the machine.
5. In the Terminal, enter the following command.

```
spctl kext-consent disable
```

```
kextstat
```

The FortiClient module `com.fortinet.fct.kext.avkern2/fctapnke` should be listed. The Web Filter and Real Time Protection features should function as configured.

For the source of this solution, see [Apple Support](#).

If using MDM with an Enterprise solution, note the FortiClient team ID is AH4XFXJ7DK.

Installation information

Firmware images and tools

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

File	Description
FortiClient_6.0.x.xxx_macosx.dmg	Standard installer for macOS.
FortiClientTools_6.0.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 6.0.5: [Introduction on page 4](#) and [Product integration and support on page 9](#).

Installation options

When installing FortiClient version 6.0.5, 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 6.0.5 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 6.0.5 to previous FortiClient versions is not supported.

Uninstalling FortiClient

To uninstall FortiClient version 6.0.5, 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 6.0.5 support information

The following table lists FortiClient (macOS) 6.0.5 product integration and support information.

Desktop Operating Systems	<ul style="list-style-type: none">• macOS Sierra (version 10.12)• macOS High Sierra (version 10.13)• macOS Mojave (version 10.14)
Minimum System Requirements	<ul style="list-style-type: none">• Intel processor• 256MB of RAM• 20MB 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">• 6.0.0 and later• 5.6.0 and later
FortiAuthenticator	<ul style="list-style-type: none">• 4.2.1 <p>FortiToken Mobile push notification is not supported 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">• 6.0.0 and later
FortiManager	<ul style="list-style-type: none">• 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>Only IPsec VPN and SSL VPN are supported with the following FortiOS versions:</p> <ul style="list-style-type: none">• 5.4.1 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 is not supported by FortiClient, it defaults to English.

Resolved issues

The following issues have been fixed in FortiClient (macOS) 6.0.5. For inquiries about a particular bug, contact [Customer Service & Support](#).

Malware Protection

Bug ID	Description
528525	Daily and monthly Anti Virus scheduled scan not working.
534122	FortiClient (macOS) Anti Virus does not restart after a reboot, need to open the FortiClient (macOS) console.

Endpoint control

Bug ID	Description
535278	Telemetry logging option shows even though Security Fabric Agent was disabled in FortiClient Configurator.

Remote Access

Bug ID	Description
515402	macOS SSL VPN <code><autoconnect_only_when_offnet></code> not working from off-net to on-net.
482160	FortiClient (macOS) SSL VPN split tunneling does not work for DNS resolution. SSL custom DNS replaced system DNS.

GUI

Bug ID	Description
527471	FortiClient (macOS) GUI displays content of any text file.

Install and upgrade

Bug ID	Description
534422	Uninstall of FortiClient from MAC 10.14.2 does not clear all the files.

Other

Bug ID	Description
535979	scanunit not running after shutdown.

Known issues

The following issues have been identified in FortiClient (macOS) 6.0.5. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

Application Firewall

Bug ID	Description
533858	FortiClient (macOS) 6.0.4 for macOS Application Firewall causes slow throughput on 1 Gbps connections.
534000	FortiClient (macOS) 6.0.4 for macOS prevents Apple AirDrop from running.

Web Filter

Bug ID	Description
498203	Exclusion list does not block pages.

Remote Access

Bug ID	Description
533022	Changing VPN tunnel name in EMS GUI can result in partial configuration loss.

Endpoint control

Bug ID	Description
519995	FortiClient (macOS) profile has certificates when EMS profile does not.

Other

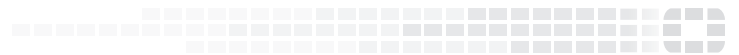
Bug ID	Description
518590	Missed FortiClient macOS non-compliance reason.
526462	Frequent bubble notification from FortiClient (macOS) on macOS devices.
534321	FortiClient failing certificate validation due to ignored intermediate CA.

Change log

Date	Change Description
2019-01-31	Initial release.



FORTINET®



Copyright© 2019 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.