



FortiClient (Mac OS X) - Release Notes

VERSION 5.4.2

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



March 15, 2017

FortiClient (Mac OS X) 5.4.2 Release Notes

04-542-393398-20170315

TABLE OF CONTENTS

Change Log	4
Introduction	5
Licensing	5
Standalone Mode	5
Managed Mode	5
Special Notices	7
DHCP over IPSec not Supported	7
Upgrade of FortiClient on Mac OS X 10.12	7
SSL VPN Requirements	7
Cooperative Security Fabric Upgrade	7
Change in FortiClient Endpoint Control Default Registration Port	7
What's New in FortiClient (Mac OS X) 5.4.2	9
Installation Information	10
Firmware images and tools	10
Upgrading from previous FortiClient versions	10
Downgrade to previous versions	10
Uninstall FortiClient	10
Firmware image checksums	11
Product Integration and Support	12
FortiClient 5.4.2 support	12
Language support	12
Resolved Issues	14
Known Issues	16

Change Log

Date	Change Description
2016-11-10	Initial release.
2016-11-17	Updated to add special notice about upgrade of FortiClient on Mac OS X 10.12.
2016-11-21	Added 389240 to Resolved Issues
2017-02-02	Added 159366 to Known Issues.
2017-02-03	Added special notice for 159366.
2017-03-15	Removed Mac OS X 10.8 Mountain Lion from the list of supported platforms.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Mac OS X) 5.4.2 build 0523.

This document includes the following sections:

- [Introduction](#)
- [Special Notices](#)
- [What's New in FortiClient \(Mac OS X\) 5.4.2](#)
- [Installation Information](#)
- [Product Integration and Support](#)
- [Resolved Issues](#)
- [Known Issues](#)

Please review all sections prior to installing FortiClient. For more information, see the *FortiClient Administration Guide* in the [Fortinet Document Library](#).

Licensing

FortiClient offers two licensing modes:

- Standalone Mode
- Managed Mode

Standalone Mode

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



Support for FortiClient in standalone mode is provided on the Fortinet Forums (forum.fortinet.com). 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 register 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.

FortiClient Licenses on the FortiGate

FortiGate 30 series and higher models include a FortiClient license for ten (10) free, 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 license for ten (10) free, 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

DHCP over IPSec not Supported

FortiClient (Mac OS X) does not support DHCP over IPSec.

Upgrade of FortiClient on Mac OS X 10.12

On Mac OS X 10.12, when upgrading FortiClient to 5.4.2, you must use the *OnlineInstaller* from the *FortiClient Tools* file. See [Firmware images and tools on page 10](#).

SSL VPN Requirements

When using SSL VPN on Mac OS X 10.8, you must enable SSLv3 in FortiOS.

Cooperative Security Fabric Upgrade

FortiOS 5.4.1 and later greatly increases the interoperability between other Fortinet products. This includes:

- FortiClient 5.4.1 and later
- FortiClient EMS 1.0.1 and later
- FortiAP 5.4.1 and later
- FortiSwitch 3.4.2 and later

The upgrade of the firmware for each product must be completed in a precise order so the network connectivity is maintained without the need of manual steps. Customers must read the following two documents prior to upgrading any product in their network:

- *Cooperative Security Fabric - Upgrade Guide*
This document is available on the Fortinet Document Library on the FortiOS page (docs.fortinet.com/).
- *FortiOS 5.4.x Upgrade Guide for Managed FortiSwitch Devices*
This document is available in the Customer Support Firmware Images download directory for FortiSwitch 3.4.2 (support.fortinet.com/).

Change in FortiClient Endpoint Control Default Registration Port

FortiClient registers to the FortiGate using Endpoint Control (EC). In FortiClient 5.0 and 5.2, the default registration port is TCP port 8010. FortiOS 5.0 and 5.2 both listen on TCP port 8010.

Starting with FortiClient 5.4, EC registration will use port 8013 by default. To register to FortiOS 5.0 or 5.2, the user must specify port 8010 with the IP address, separated by a colon. For example, <ip_address>:8010.

FortiOS 5.4 and later will listen on port 8013. If registering from FortiClient 5.4 and later to FortiOS 5.4 and later, the default ports will match. Specifying the port number with the IP address is then optional.

What's New in FortiClient (Mac OS X) 5.4.2

This section identifies the new features and enhancements in FortiClient (Mac OS X) 5.4.2. For more information, see the *FortiClient Administration Guide*.

- FortiClient (Mac OS X) supports Mac OS X v10.12 Sierra.
- FortiClient in standalone mode no longer includes a banner at the bottom of the console.

Installation Information

Firmware images and tools

When installing FortiClient version 5.4.2, you can choose the setup type that best suits your needs. You can select one of the following options:

- Complete: all Endpoint Security and VPN components will be installed.
- VPN Only: only VPN components (IPsec and SSL) will be installed.

FortiClient includes various tools to help with and customize installations. The following tools and files are available in the *FortiClientTools* file:

- *OnlineInstaller*: downloads and installs the latest FortiClient file from the public FortiGuard Distribution Server (FDS).
- *FortiClientConfigurator*: an installer repackaging tool that can be used to create custom installation packages
- *RebrandingResources*: resources used by the FortiClient Configurator tool for rebranding.



When creating a custom FortiClient 5.4.2 installer using the FortiClient Configurator tool, you can choose which features to install. You can also enable or disable software updates, configure SSO, and rebrand FortiClient .

Upgrading from previous FortiClient versions

FortiClient version 5.4.2 supports upgrading from FortiClient 5.2.0 or later.

When FortiClient endpoints are registered to FortiGate, you must upgrade endpoints to FortiClient 5.4.1 before you upgrade FortiGate to 5.4.1. See [Cooperative Security Fabric Upgrade on page 7](#).



Please review the following sections prior to installing FortiClient version 5.4.2: [Introduction on page 5](#), [Special Notices on page 7](#), and [Product Integration and Support on page 12](#).

Downgrade to previous versions

Downgrading FortiClient version 5.4.2 to previous FortiClient versions is not supported.

Uninstall FortiClient

To uninstall FortiClient version 5.4.2, 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 5.4.2 support

The following table lists FortiClient (Mac OS X) 5.4.2 product integration and support information.

Desktop Operating Systems	• Mac OS X v10.9 Mavericks • Mac OS X v10.10 Yosemite • Mac OS X v10.11 El Capitan • Mac OS X v10.12 Sierra
Minimum System Requirements	• 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 FortiClient documentation
FortiAnalyzer	• 5.4.1 and later
FortiAuthenticator	• 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	• 1.0.0 and later
FortiManager	• 5.4.1 and later
FortiOS	• 5.4.1 and later Some FortiClient features are dependent on specific FortiOS versions.

Language support

The following table lists FortiClient language support information.

Language	GUI	XML Configuration	Documentation
English	✓	✓	✓
Chinese (Simplified)	✓		
Chinese (Traditional)	✓		
French (France)	✓		
German	✓		
Japanese	✓		
Korean	✓		
Portuguese (Brazil)	✓		
Russian	✓		
Spanish (Spain)	✓		

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 (Mac OS X) 5.4.2. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
0271427	Host CPU spikes when using type-ahead feature in Eclipse Luna on Mac OS when FortiClient is registered on FortiGate.
0271427	Host CPU spikes when using type-ahead feature in Eclipse Luna on Mac OS when FortiClient is registered on FortiGate.
0290797	FortiClient Mac online installer shall download or install the latest available version
0290797	FortiClient (Mac OS X) online installer shall download or install the latest available version
0297330	Kernel panic related to SSL VPN on Mac OS X v10.11 El Capitan
0373610	FortiClient (Mac OS X) experience kernel panic
0374189	IPSec VPN not working when firewall is enabled
0377283	<i>Compliance</i> page shows as <i>Application Firewall</i> on <i>FortiClient > Preferences > Default</i> tab
0379463	AV kernel extension causing Mac kernel panic
0379946	FortiClient (Mac OS X) 5.4.1 causing OSX to crash
0380124	FortiClient (Mac OS X) - <i>Show Bubble Notification</i> field not activating
0380661	Changes to EC to support disabled compliance rules
0381439	Mac OS X v10.12 -- avkern
0383002	Hostname for Mac users is site visited in event logs
0385141	FortiClient console CPU 40%
0386879	Change priorities for FortiClient registration
0388206	Some Mac OS X devices from Active Directory show as <i>Other Endpoints</i>
0388377	FortiClient should send KA message immediately after receiving compliance rules or configuration

Bug ID	Description
0389433	FortiClient (Mac OS X) online installer does not work on Mac OS X v10.12
0390095	Sending Avatar image should be enabled by default
0390095	Sending Avatar image should be enabled by default
0391098	User initiated logs are not generated using Firefox
0391699	FortiClient crashes on Mac OS X Sierra (10.12)
0393369	FortiClient logs alert but not action taken

Common Vulnerabilities and Exposures

Bug ID	Description
389240	FortiClient (Mac OS X) 5.4.2 is no longer vulnerable to the following CVE-References: • 2016-2177 • 2016-2178 • 2016-2179 • 2016-2181 • 2016-2182 • 2016-2183 • 2016-6302 • 2016-6303 • 2016-6304 • 2016-6305 • 2016-6306 • 2016-6307 • 2016-6308 Visit https://fortiguard.com/psirt for more information.

Known Issues

The following issues have been identified in FortiClient (Mac OS X) 5.4.2. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

Bug ID	Description
0159366	FortiClient (Mac OS X) does not support DHCP over IPSec
0374648	FortiClient DNS and split tunneling
0378259	FortiClient (Mac OS X) 5.4.0.507 AV Scan runs for hours
0380323	Upgrading FortiClient (Mac OS X) with multiple users from 5.4.0 to 5.4.1 fails
0384501	Application Firewall would stop running
0387811	FortiClient error -111 with 2FA
0392902	Different OTP challenge window for IPsec and SSL VPN
0395499	FortiClient (Mac OS X) can't handle the large packets over SSL VPN connection



FORTINET®

High Performance Network Security



Copyright© 2017 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.