



FortiClient (Mac OS X) - Release Notes

Version 5.6.6

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 29, 2018

FortiClient (Mac OS X) 5.6.6 Release Notes

04-566-475025-20180329

TABLE OF CONTENTS

Change Log	4
Introduction	5
Licensing	5
Standalone mode	5
Managed mode	5
Special Notices	7
User password renewal over SSL VPN with FortiOS 6.0.0	7
Installation Information	8
Firmware images and tools	8
Installation options	8
Upgrading from previous FortiClient versions	8
Downgrading to previous versions	9
Uninstall FortiClient	9
Firmware image checksums	9
Product Integration and Support	10
FortiClient 5.6.6 support	10
Language support	11
Resolved Issues	12
Known Issues	13

Change Log

Date	Change Description
2018-03-08	Initial release of FortiClient (Mac OS X) 5.6.6.
2018-03-12	Added detail in Upgrading from previous FortiClient versions on page 8 .
2018-03-29	Added special notice about FortiOS 6.0.0 compatibility when using SSL VPN.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Mac OS X) 5.6.6 build 0755.

This document includes the following sections:

- [Introduction](#)
- [Special Notices](#)
- [Installation Information](#)
- [Product Integration and Support](#)
- [Resolved Issues](#)
- [Known Issues](#)

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 connected to a FortiGate or 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 (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 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 (10) free licenses for FortiClient in managed mode, support is provided on the Fortinet Forums (forum.fortinet.com). Phone support is not provided when using the free licenses. Phone support is provided for paid licenses.

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

User password renewal over SSL VPN with FortiOS 6.0.0

With FortiOS 6.0.0, if the FortiGate local user has a FortiToken assigned and the password is expiring and needs renewal, FortiClient (Mac OS X) will not be able to connect. If FortiGate SSL has the web portal enabled, the user can renew their password over the web portal, then connect with FortiClient.

Installation Information

Firmware images and tools

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

File	Description
FortiClient_5.6.x.xxx_macosx.dmg	Standard installer for Mac OS X
FortiClientTools_5.6.x.xxx_macosx.tar	FortiClient includes various utility tools and files to help with installations

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

File	Description
OnlineInstaller	This file downloads and installs the latest FortiClient file from the public FDS



Review the following sections prior to installing FortiClient version 5.6.6: [Introduction on page 5](#) and [Product Integration and Support on page 10](#).

Installation options

When installing FortiClient version 5.6.6, you can choose the setup type that best suits your needs. FortiClient will always install the 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 5.6.6 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 5.6.6 to previous FortiClient versions is not supported.

Uninstall FortiClient

To uninstall FortiClient version 5.6.6, 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 5.6.6 support

The following table lists FortiClient (Mac OS X) 5.6.6 product integration and support information.

Desktop Operating Systems	<ul style="list-style-type: none">• 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• Mac OS X v10.13 High Sierra
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 FortiClient documentation
FortiAnalyzer	<ul style="list-style-type: none">• 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">• 1.2.0 and later
FortiManager	<ul style="list-style-type: none">• 5.6.0 and later
FortiOS	<ul style="list-style-type: none">• 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	✓	✓	✓
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) 5.6.6. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
458782	FortiClient 5.6.0 and 5.6.1 for Mac unable to connect to IPsec VPN using okta 2 factor authentication.
468105	FortiClient Mac localization issues.

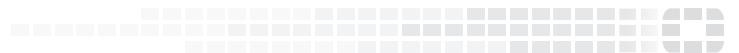
Known Issues

The following issues have been identified in FortiClient (Mac OS X) 5.6.6. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

Bug ID	Description
451605	b0394: EMS reports NPAPI Flash Plug-in vulnerable while not installed.
462791	VPN auto connect value cannot be restored.
462928	FortiClient Mac not sending alerts when registered to FortiGate and monitored by EMS.
463261	Web filter and malicious website in on-net scenario.
467328	b1130: FortiClient log for vulnerability scan should include file path.
467414	b726: SSL VPN issues when connecting to FortiGate in AWS cloud.
467624	b726 iTunes fails to sync with iPhone over wi-fi on FortiClient 5.6.3.
468031	Error shown when scanning a folder using environment variable.
476456	Vulnerability Scan exclusion for applications not working.
476454	Exclusions not being obeyed on FortiClient Mac.
475421	FortiClient for Mac update does not try to contact more than 1 server.
474993	b1150: FortiClient cannot be compliant when AV engine is different on FCT and FOS.
473975	FortiClient managed by Corporate EMS on MAC removes custom VPN profiles upon upgrade.
471379	FortiClient Mac OS VPN split tunneling and DNS.



FORTINET[®]



Copyright© 2018 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.