



# FortiClient (macOS) - Release Notes

Version 6.2.6

**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](mailto:techdoc@fortinet.com)



May 26, 2020

FortiClient (macOS) 6.2.6 Release Notes

04-626-611008-20200526

# TABLE OF CONTENTS

<b>Change log</b>	<b>4</b>
<b>Introduction</b>	<b>5</b>
Licensing	5
<b>Special notices</b>	<b>6</b>
FortiClient on macOS Catalina (version 10.15)	6
FortiClient Web Filter	6
DHCP over IPsec VPN not supported	7
IKEv2 not supported	7
<b>Installation information</b>	<b>8</b>
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
<b>Product integration and support</b>	<b>10</b>
Language support	11
<b>Resolved issues</b>	<b>12</b>
Application Firewall	12
EMS deployment	12
Other	12
<b>Known issues</b>	<b>13</b>
Application Firewall	13
Endpoint control	13
Malware Protection	13
Remote Access	13
Sandbox	14
EMS deployment	14
FortiManager	14

## Change log

Date	Change Description
2020-03-10	Initial release.
2020-03-19	Updated <a href="#">Licensing</a> on page 5.
2020-04-02	Added <a href="#">DHCP over IPsec VPN not supported</a> on page 7.
2020-04-13	Added 582302 to <a href="#">Known issues</a> on page 13.
2020-05-05	Updated <a href="#">FortiClient Web Filter</a> on page 6.
2020-05-26	Added <a href="#">IKEv2 not supported</a> on page 7.

# Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (macOS) 6.2.6 build 0737.

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 13](#)

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 6.2.6 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)

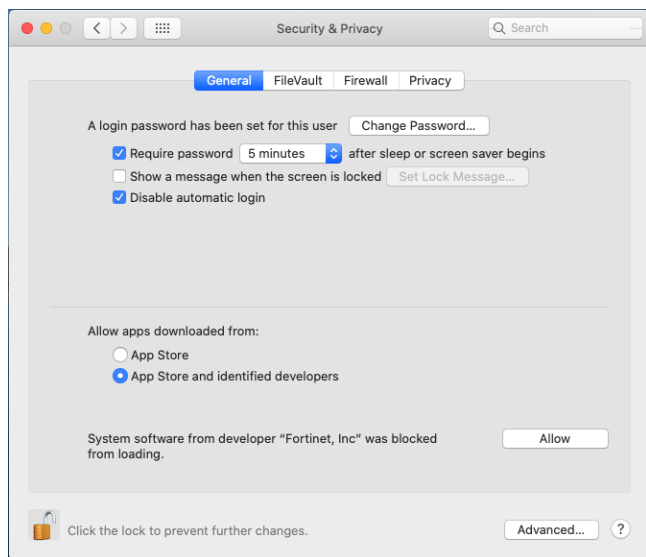
You can install FortiClient (macOS) 6.2.6 on macOS 10.15 Catalina, which Apple released in early October 2019. With this macOS release, however, FortiClient works properly only when you grant permissions to access the full disk in the *Security & Privacy* pane for the following services:

- fcaptmon
- fctservctl
- fmon
- FortiClient



## FortiClient 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.

## 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_6.2.6.0737_macosx.tar.gz	Includes utility tools and files to help with installation.

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

File	Description
FortiClientVPNSetup_6.2.6.0737_macosx.dmg	Free VPN-only installer.

FortiClient EMS 6.2.6 includes the FortiClient (macOS) 6.2.6 standard installer.



Review the following sections prior to installing FortiClient version 6.2.6: [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 6.2.6 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) 6.2.6 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) 6.2.6. 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 6.2.6 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) 6.2.6 product integration and support information:

<b>Desktop operating systems</b>	<ul style="list-style-type: none"><li>• macOS Catalina (version 10.15)</li><li>• macOS Mojave (version 10.14)</li><li>• macOS High Sierra (version 10.13)</li><li>• macOS Sierra (version 10.12)</li></ul>
<b>Minimum system requirements</b>	<ul style="list-style-type: none"><li>• Intel processor</li><li>• 256 MB of RAM</li><li>• 20 MB of hard disk drive (HDD) space</li><li>• TCP/IP communication protocol</li><li>• Ethernet NIC for network connections</li><li>• Wireless adapter for wireless network connections</li><li>• Adobe Acrobat Reader for viewing FortiClient documentation</li></ul>
<b>FortiAnalyzer</b>	<ul style="list-style-type: none"><li>• 6.2.0 and later</li></ul>
<b>FortiAuthenticator</b>	<ul style="list-style-type: none"><li>• 4.2.1</li></ul> <p>FortiClient (macOS) does not support FortiToken Mobile push notification for the following versions:</p> <ul style="list-style-type: none"><li>• 4.2.0</li><li>• 4.1.0 and later</li><li>• 3.3.0 and later</li><li>• 3.2.0 and later</li><li>• 3.1.0 and later</li><li>• 3.0.0 and later</li></ul>
<b>FortiClient EMS</b>	<ul style="list-style-type: none"><li>• 6.2.0 and later</li></ul>
<b>FortiManager</b>	<ul style="list-style-type: none"><li>• 6.2.0 and later</li></ul>
<b>FortiOS</b>	<ul style="list-style-type: none"><li>• 6.2.0 and later</li><li>• 6.0.0 and later</li></ul> <p>Telemetry, IPsec VPN, and SSL VPN are supported. See important information in <a href="#">Upgrading from previous FortiClient versions on page 8</a>.</p> <ul style="list-style-type: none"><li>• 5.6.0 and later</li></ul> <p>IPsec VPN and SSL VPN are supported. See important information in <a href="#">Upgrading from previous FortiClient versions on page 8</a>.</p>
<b>FortiSandbox</b>	<ul style="list-style-type: none"><li>• 3.1.0 and later</li><li>• 3.0.0 and later</li><li>• 2.5.0 and later</li></ul>

## 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) 6.2.6. For inquiries about a particular bug, contact [Customer Service & Support](#).

### Application Firewall

Bug ID	Description
606083	Application Firewall causes network issue on macOS.
607062	Application Firewall performance issues on macOS.

### EMS deployment

Bug ID	Description
610195	FortiClient (macOS) deployment from EMS crashes.

### Other

Bug ID	Description
607249	Pushing CA certificate to macOS disrupts users.
609404	Uninstaller keeps spinning on macOS 10.15.3.

## Known issues

The following issues have been identified in FortiClient (macOS) 6.2.6. 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.

### Endpoint control

Bug ID	Description
600524	FortiClient (macOS) incorrectly or incompletely imports a profile.
601248	EMS randomly fails to deregister FortiClient (macOS).
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.

### Malware Protection

Bug ID	Description
550046	Copying extracted Eicar files does not trigger a virus alert.

### Remote Access

Bug ID	Description
600690	EMS provisioning shows invalid configuration for VPN.

Bug ID	Description
605438	FortiClient (macOS) does not save the username for an SSL VPN tunnel.
614371	SSL VPN does not connect after waking the computer from sleep.

## Sandbox

Bug ID	Description
597180	Sandbox remediation action is set to alert but GUI shows that it quarantined the file.
597278	EMS shows incorrect rating for FortiSandbox result for macOS devices.
592029	Sandbox ignores changing file size limit for device submissions when submissions come from FortiClient (macOS).

## EMS deployment

Bug ID	Description
588656	FortiClient (macOS) EMS deployment fails randomly.

## FortiManager

Bug ID	Description
582302	FortiClient (macOS) cannot get signature from FortiManager using HTTPS due to failed certificate check.



**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.