



FortiClient (macOS) - Release Notes

Version 6.2.1

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



November 8, 2019

FortiClient (macOS) 6.2.1 Release Notes

04-621-563661-20191108

TABLE OF CONTENTS

Introduction	4
Licensing	4
What's new in FortiClient (macOS) 6.2.1	5
Installation information	6
Firmware images and tools	6
Installation options	6
Upgrading from previous FortiClient versions	7
Downgrading to previous versions	7
Uninstalling FortiClient	7
Firmware image checksums	7
Product integration and support	8
FortiClient 6.2.1 support	8
Language support	9
Resolved issues	10
Known issues	12
Change log	13

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (macOS) 6.2.1 build 0654.

This document includes the following sections:

- [What's new in FortiClient \(macOS\) 6.2.1 on page 5](#)
- [Installation information on page 6](#)
- [Product integration and support on page 8](#)
- [Resolved issues on page 10](#)
- [Known issues on page 12](#)

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 7](#) 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 6.2.1 supports a 30-day trial license with ten FortiClient seats.

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](https://forticlient.com).

What's new in FortiClient (macOS) 6.2.1

For information about what's new in FortiClient (macOS) 6.2.1, see the [FortiClient & FortiClient EMS 6.2.1 New Features Guide](#).

Installation information

Firmware images and tools

The following file is available from the [Fortinet support site](#):

File	Description
FortiClientTools_6.2.1.xxx_macosx.tar	Includes utility tools and files to help with installation.

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

File	Description
FortiClientVPNSetup_6.2.1.xxx_macosx.dmg	Free VPN-only installer.

FortiClient EMS 6.2.1 includes the FortiClient (macOS) 6.2.1 standard installer.



Review the following sections prior to installing FortiClient version 6.2.1: [Introduction on page 4](#), and [Product integration and support on page 8](#).

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 6.2.1 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) 6.2.1 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) 6.2.1. 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 6.2.1 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

FortiClient 6.2.1 support

The following table lists FortiClient (macOS) 6.2.1 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• 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
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 <p>EMS 6.2.2 does not provide backwards host tag compatibility for FortiClient (macOS) 6.2.1. Upgrade FortiClient to 6.2.2 for host tag compatibility with EMS 6.2.2.</p>
FortiManager	<ul style="list-style-type: none">• 6.2.0 and later
FortiOS	<ul style="list-style-type: none">• 6.2.0 and later• 6.0.0 and later <p>Telemetry, IPsec VPN, and SSL VPN are supported. See important information in Upgrading from previous FortiClient versions on page 7.</p> <ul style="list-style-type: none">• 5.6.0 and later <p>IPsec VPN and SSL VPN are supported. See important information in Upgrading from previous FortiClient versions on page 7.</p>
FortiSandbox	<ul style="list-style-type: none">• 3.1.0 and later• 3.0.0 and later

- 2.5.0 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 FortiClient does not support, it defaults to English.

Resolved issues

The following issues have been fixed in FortiClient (macOS) 6.2.1. For inquiries about a particular bug, contact [Customer Service & Support](#).

Bug ID	Description
469778	RTP cannot quarantine grayware.
513095	Inconsistency between macOS and Windows online status on EMS.
533858	Application Firewall causes slow throughput on 1 Gbps connections.
538752	EMS settings for <show_remember_password>, <show_alwaysup>, and <show_autoconnect> should override similar FortiOS settings.
542809	FortiClient does not save the certificate.
544037	User can disconnect FortiClient (macOS) from EMS with a blank password.
547664	Unable to run manual autopatching for OS, web, and third party vulnerabilities.
548238	FortiClient SSL VPN connectivity issue to Cloudflare DNS services 1.1.1.1 when split tunnel is enabled.
549174	IPsec VPN fails to work on macOS Mojave.
549809	VPN certificate filter always chooses the first user info certificate in the list.
552539	FortiClient does not have unique serial number.
553099	FortiClient (macOS) deletes a file in additionally created in directory <i>etc/resolver</i> .
553718	FortiClient forces password change before FortiGate local user password expires.
553824	FortiClient fails to establish IPsec VPN if the wifi network is switched.
555488	FortiClient (macOS) cannot forget or remember the EMS list in the GUI.
557920	IPsec VPN rekey fails for system certificate (XAuth disabled) with Racoon process crash.
566060	FortiClient unlocks settings after registering to EMS.
566611	FortiClient does not prompt for password to disconnect from EMS when EMS profile enables it.
568379	Sandbox unauthorizes FortiClient (macOS) when it is registered to a FortiSandbox-authenticated EMS.
568811	FortiClient status is not connected when it is registered to EMS.
569293	FortiClient sends the FortiGate serial number to FortiAnalyzer in the EMS serial number field when FortiClient is dual registered.

Common Vulnerabilities and Exposures

Bug ID	Description
566262	FortiClient (macOS) 6.2.1 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2019-15704 Visit https://fortiguard.com/psirt for more information.

Known issues

The following issues have been identified in FortiClient (macOS) 6.2.1. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

Bug ID	Description
534567	Vulnerability scan automatically resumes after user manually stops it.
546973	FortiClient can break quarantined state after system reboot.
547253	Incorrect port number appended to remembered EMS IP address list.
549699	FortiClient free VPN does not show certificate dropdown list after SSL VPN is configured.
550046	Copying extracted EICAR files does not trigger a virus alert.
550389	Autoconnect tries to reconnect to corporate VPN even after deregistering from EMS.
550673	FortiClient zero-day Sandbox detection event in notification list shows source as <i>AntiVirus</i> with RTP.
550678	FortiClient displays incorrect Sandbox signatures status and version details.
551282	Sandbox exception for trusted sources does not work when FortiClient (macOS) uploads files sourced from Apple.
553657	FortiClient does not send Sandbox zero day detection to FortiAnalyzer.
553927	FortiClient only uses NAT traversal in VPN tunnel.
562936	FortiClient has no server name extension included in the SSL client hello which causes a load-balanced fail.
563320	<i>Forget/Remember EMS IP</i> button does not work.
563457	Web Filter blocks unrated category websites even when profile action is set to allow or monitor.
564922	FortiClient does not perform vulnerability scan when EMS enables <i>Scan on registration</i> .
565438	FortiClient (macOS) GUI keeps showing vulnerabilities on the scan details page after patching them.
566478	No FortiToken rekey prompt for IPsec VPN.
566762	VPN elapsed timer remains static/frozen in FortiTray.
568085	Remembered EMS list detail box displays :0 after EMS IP address.
568508	FortiClient fails to connect IPsec VPN using certificate authentication.

Change log

Date	Change Description
2019-07-18	Initial release.
2019-08-06	Updated Product integration and support on page 8 .
2019-11-08	Added 566262 to Resolved issues on page 10 .



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.