FortiClient (macOS) - Release Notes

Version 6.2.0

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: techdoc@fortinet.com

May 15, 2019
FortiClient (macOS) 6.2.0 Release Notes
04-620-530290-20190515

TABLE OF CONTENTS

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (macOS) 6.2.0 build 0614.

This document includes the following sections:

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 or on FortiClient EMS 6.2.0.

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

Limitation for remote users

In 6.2.0, FortiClient (macOS) must register to EMS before you can use any features. Remote users may be unable to connect via VPN to their corporate network and register to EMS, since they cannot access the VPN feature until FortiClient (macOS) is registered to EMS.

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

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

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 `spctl kext-consent disable` command.
4. Reboot the machine.
5. In the Terminal, enter the `kextstat` command. The FortiClient module com.fortinet.fct.kext.avkern2/fctapnke should be listed. The Web Filter and RTP features should function as configured.

For the source of this solution, see Apple Support.

If using mobile device management (MDM) with an enterprise solution, note the FortiClient team ID is AH4XFXJ7DK.

What’s new in FortiClient (macOS) 6.2.0

For information about what's new in FortiClient (macOS) 6.2.0, see the *FortiClient & FortiClient EMS 6.2.0 New Features Guide*.

Installation information

Firmware images and tools

The following file is available from the Fortinet support site:

File	Description
FortiClientTools_6.2.0.xxx_macosx.tar	Includes utility tools and files to help with installation.

The following file is available from FortiClient.com:

File	Description
FortiClientVPNSetup_6.2.0.xxx_ macosx.dmg	Free VPN-only installer.

The FortiClient (macOS) 6.2.0 standard installer is included with FortiClient EMS 6.2.0.

Review the following sections prior to installing FortiClient version 6.2.0: Introduction on page 4, Special notices on page 5, and Product integration and support on page 9.

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 6.2.0 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) 6.2.0 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) 6.2.0. 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 6.2.0 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 6.2.0 support

The following table lists FortiClient (macOS) 6.2.0 product integration and support information.

Desktop operating systems	• macOS Sierra (version 10.12) • macOS High Sierra (version 10.13) • macOS Mojave (version 10.14)
Minimum system requirements	• 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	• 6.2.0 and later • 6.0.0 and later
FortiAuthenticator	• 4.2.1 FortiClient (macOS) does not support FortiToken Mobile push notification for the following versions: • 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	• 6.2.0 and later
FortiManager	• 6.2.0 and later • 6.0.0 and later
FortiOS	• 6.2.0 and later • 6.0.0 and later Telemetry, IPsec VPN, and SSL VPN are supported. See important information in Upgrading from previous FortiClient versions on page 8. • 5.6.0 and later Telemetry, IPsec VPN, and SSL VPN are supported. See important information in Upgrading from previous FortiClient versions on page 8.
FortiSandbox	• 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) 6.2.0. For inquiries about a particular bug, contact Customer Service & Support.

Bug ID	Description
482160	FortiClient (macOS) SSL VPN split tunneling does not work for DNS resolution. SSL custom DNS replaced system DNS.
512247	FortiClient (macOS) does not show full details of on-net/online status.
514648	FortiClient (macOS) IPsec cannot reach resource in split tunnel if there is more than one subset.
515402	FortiClient (macOS) SSL VPN `<autoconnect_only_when_offnet>` not working from off-net to on-net.
516394	FortiClient (macOS) freezes on the patching progress screen and also causes the host machine to hang up.
517901	FortiClient (macOS) VPN certificate list shows every available client/system certificate twice.
520016	FortiClient (macOS) only installs one CA certificate.
522372	FortiClient (macOS) tries to connect IPsec even when on-net.
523469	fcconfig crash on install.
523477	SSL error message is unclear when FortiGate web portal disables tunnel mode.
524913	Problem with VPN IPsec profile pushed from EMS to FortiClient (macOS): VPN KO: problem PSK.
525906	Category column for unknown applications is blank in violations list of FortiClient (macOS) Application Firewall.
527471	FortiClient (macOS) GUI displays content of any text file.
528001	FortiClient (macOS) list of VPNs becomes blank.
528525	Daily and monthly AV scheduled scan not working.
528919	If `<save_password>` is enabled it should be enabled in all of the GUI (FortiClient (macOS) GUI and popup) when off-net SSL connection kicks in.
529198	macOS with prepackaged configuration - YouTube restricted mode is set to ON.
529336	Group assignment rules are not honored for macOS clients.
529660	FortiClient (macOS) SSL VPN connect error when RADIUS server sends empty message in a challenge.
530563	All certificates appear in the dropdown list even though the configuration has a filter for just one certificate.
531887	Bubble notifications for component updates show even if *Show Bubble Notifications* is disabled.

Bug ID	Description
533022	Changing VPN tunnel name in EMS GUI can result in partial configuration loss.
534000	FortiClient (macOS) prevents Apple AirDrop from running.
534122	FortiClient (macOS) AV does not restart after a reboot. FortiClient (macOS) console needs to be opened.
534321	FortiClient fails certificate validation due to ignored intermediate CA.
534422	Uninstalling FortiClient from macOS 10.14.2 does not clear all files.
535065	*Compliance & Telemetry* tab shows even though Security Fabric Agent was disabled in FortiClient Configurator.
535278	Telemetry logging option shows even though Security Fabric Agent was disabled in FortiClient Configurator.
535767	*Save Passwords/Credentials* checkbox for SSL VPN only checked if *Always Up* is enabled.
535774	Consistency between FortiClient console and FortiClient popup from taskbar.
535979	scanunit not running after shutdown.
537290	Incorrect source name for IPsec VPN notifications.
537663	FortiClient (macOS) connects to IP address instead of host when using proxy.
538085	Compliance cannot work correctly due to the same MAC address reported by all devices.
538664	FortiClient (macOS) automatically reconnects SSL VPN with *Auto Connect* disabled.
542616	Web Filter shows enabled when *Client Web Filtering When On-Net* disabled and onnet.
543464	FortiGate routes injected form IPsec on macOS PC remain after disconnecting VPN.
545283	FortiClient (macOS) Sandbox GUI icon reporting incorrect connection status.
545975	FortiClient (macOS) features still visible even after EMS profile has corresponding tags `<endpoint_control><ui><display_ ..>` set to `0`.
546989	Personal information does not get updated in the FortiClient (macOS) GUI.
547664	Unable to run manual autopatching for OS, web, and third party vulnerabilities.
548226	FortiClient (macOS) can disconnect from EMS when EMS profile requires a password to disconnect from EMS.
548986	FortiClient (macOS) can register to EMS when its system date is out of sync for more than two days from EMS system date.
549695	Cannot get back to VPN connection page in the GUI after clicking *Settings*.

Known issues

The following issues have been identified in FortiClient (macOS) 6.2.0. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Bug ID	Description
489370	Email alerts are incomplete for AV events.
498203	Exclusion list does not block pages.
505768	FortiClient EMS does not show VPN and Application Firewall events.
506505	FortiClient fails to allow for any customizations to the IKE proposal for phase 2.
524864	FortiClient (macOS) sends wrong most recent Vulnerability Scan time to EMS.
526346	FortiClient (macOS) *Lock Settings* button appears after FortiGate-EMS dual registration with EMS UI settings are disabled.
526357	*View Compliance Rules page* is blank after dual registered FortiClient (macOS) is deregistered from EMS only.
527452	FortiClient (macOS) detects test Eicar attachments but does not quarantine them if downloaded from the macOS Mail application.
533848	FortiClient (macOS) may fail to transmit multicast requests through an SSL VPN tunnel.
534567	Vulnerability Scan resumes after being manually stopped.
536677	FortiClient (macOS) sends uninstalled applications as part of the software inventory list.
538752	EMS settings for `<show_remember_password>`, `<show_alwaysup>`, `<show_autoconnect>` should override similar FortiOS settings.
542809	FortiClient (macOS) fails to save the certificate when VPN advanced options are enabled.
542895	Application firewall does not block categories enabled from EMS.
544037	FortiClient (macOS) can be disconnected from EMS with a blank password.
544274	FortiClient (macOS) causes SSL error when accessing internal websites when Web Filter is enabled.
546260	User is able to stop AV scan triggered from EMS.
546375	EMS needs FortiClient (macOS) to provide service and download from information for Sandbox event.
546526	FortiGate IP list is not used after reregistration.
546915	Enforce minimum OS version when installing FortiClient.
546973	FortiClient (macOS) is able to break quarantined state after system reboot.
547253	Incorrect port number appended to remembered EMS IP list.

Bug ID	Description
547541	IPsec tray and GUI with certificate.
548234	FortiClient (macOS) on macOS 10.12.6 Sierra is recognized as unknown device.
548238	FortiClient (macOS) SSL VPN connectivity Issue to Cloudflare DNS services 1.1.1.1 when split tunnel enabled.
548517	FortiClient (macOS) GUI shows host tags as clickable.
548744	FortiClient should kill the related process for a Sandbox-detected malicious file.
549174	Unable to open IPsec tunnel, file not found.
549699	FortiClient free VPN is not showing certificate dropdown list after configuring SSL VPN.
549809	FortiClient (macOS) VPN certificate filter always chooses the first user info certificate in the list.
549860	*Auto connect* and *Always up* settings are not visible when using machine certificate (without XAuth).
550046	Copying extracted Eicar files does not trigger virus alert.
550049	Support Sandbox hold file and auto submit on macOS.
550168	FortiClient (macOS) VPN client: unable to select a system certificate from VPN certificate filter.
550389	Autoconnect tries to reconnect to VPN even after deregistering from EMS.

Change log

Date	Change Description
2019-04-16	Initial release.
2019-04-29	Updated Firmware images and tools on page 7.
2019-05-03	Added Limitation for remote users on page 5.
2019-05-15	Updated Firmware images and tools on page 7 and Introduction on page 4.