

Release Notes

FortiClient (macOS) 7.0.1



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://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



August 10, 2021

FortiClient (macOS) 7.0.1 Release Notes

04-701-729341-20210810

TABLE OF CONTENTS

Change log	4
Introduction	5
Licensing	5
Special notices	6
Enabling full disk access on macOS 11 Big Sur and 10.15 Catalina	6
Activating system extensions	7
VPN	7
Web Filter and Application Firewall	8
Enabling notifications	9
DHCP over IPsec VPN not supported	9
IKEv2 not supported	9
What's new in FortiClient (macOS) 7.0.1	10
Installation information	11
Firmware images and tools	11
Upgrading from previous FortiClient versions	11
Downgrading to previous versions	11
Uninstalling FortiClient	12
Firmware image checksums	12
Product integration and support	13
Language support	13
Resolved issues	15
Remote Access	15
Web Filter	15
Endpoint control	15
Performance	15
Known issues	16
Endpoint control	16
Remote Access	16
Web Filter	17
Configuration	17
Multitenancy	17
Performance	17

Change log

Date	Change description
2021-08-10	Initial release.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (macOS) 7.0.1 build 0060.

This document includes the following sections:

- [Special notices on page 6](#)
- [What's new in FortiClient \(macOS\) 7.0.1 on page 10](#)
- [Installation information on page 11](#)
- [Product integration and support on page 13](#)
- [Resolved issues on page 15](#)
- [Known issues on page 16](#)

Review all sections prior to installing FortiClient. For more information, see the [FortiClient Administration Guide](#).

Licensing

See [Windows, macOS, and Linux endpoint licenses](#).

Special notices

Enabling full disk access on macOS 11 Big Sur and 10.15 Catalina

You can install FortiClient (macOS) 7.0.1 on macOS 11 Big Sur and 10.15 Catalina. With these releases, FortiClient works properly only when you grant permissions to access the full disk in the *Security & Privacy* pane for the following services:

- fcaptmon
- fctservctl
- fctservctl2
- fmon
- fmon2
- FortiClient
- FortiClientAgent

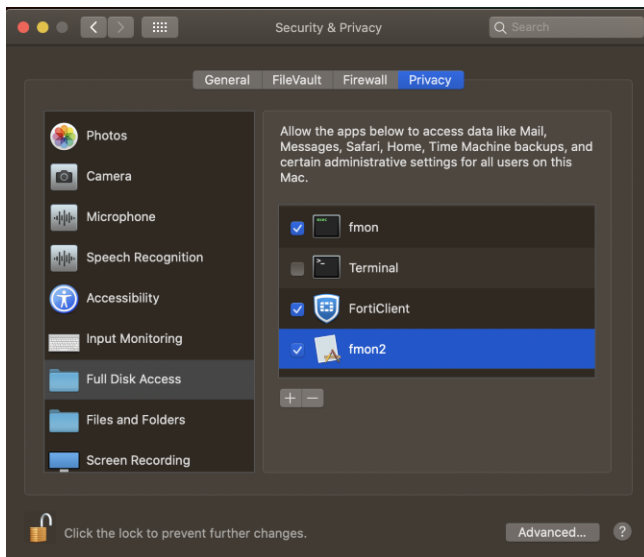


The FortiClient (macOS) free VPN-only client does not include the fcaptmon, fmon, and fmon2 services. If you are using the VPN-only client, you only need to grant permissions for fctservctl and FortiClient.

You may have to manually add fmon2 to the list, as it may not be in the list of applications to allow full disk access to.

Click the + icon to add an application. Browse to `/Library/Application`

`Support/Fortinet/FortiClient/bin/` and select fmon2.



The following lists the services and their folder locations:

- fmon, Fctservctl, Fcaptmon: /Library/Application\ Support/Fortinet/FortiClient/bin/
- FortiClient (macOS) application: /Applications/FortiClient.app
- FortiClient agent (FortiTray):
/Applications/FortiClient.app/Contents/Resources/runtime.helper/FortiClientAgent.ap
p

Activating system extensions

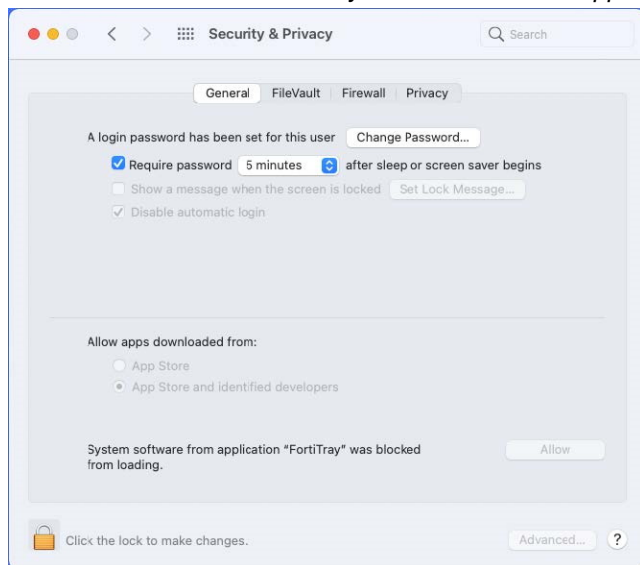
After you perform an initial install of FortiClient (macOS), the device prompts you to allow some settings and disk access for FortiClient (macOS) processes. You must have administrator credentials for the macOS machine to configure this change.

VPN

VPN works properly only when you allow system software from Fortinet to load in *Security & Privacy* settings.

To allow FortiTray to load:

1. Go to *System Preferences > Security & Privacy*.
2. Click the *Allow* button beside *System software from application "FortiTray" was blocked from loading*.

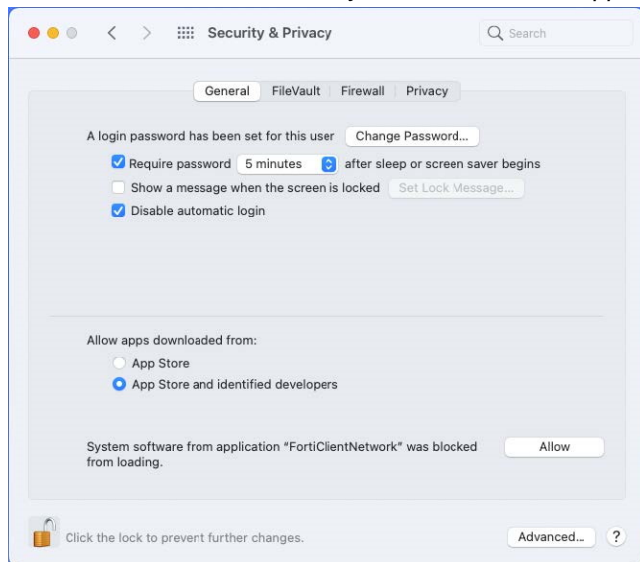


Web Filter and Application Firewall

You must enable the FortiClientNetwork extension for Web Filter and Application Firewall to work properly. The FortiClient (macOS) team ID is AH4XFXJ7DK.

To enable the FortiClientNetwork extension:

1. Go to *System Preferences > Security & Privacy*.
2. Click the *Allow* button beside *System software from application "FortiClientNetwork" was blocked from loading*.



3. Verify the status of the extension by running the `systemextensionsctl list` command in the macOS terminal. The following provides example output when the extension is enabled:

```
MacBook-Air ~ % systemextensionsctl list
2 extension(s)
-- com.apple.system_extension.network_extension
enabled active teamID bundleID (version) name [state]
* * AH4XFXJ7DK com.fortinet.forticlient.macos.vpn.nwextension (1.4.8/B20210629) vpnprovider [activated]
* * AH4XFXJ7DK com.fortinet.forticlient.macos.webfilter (1.1/1) FortiClientPacketFilter [activated enabled]
```

Enabling notifications

After initial installation, macOS prompts the user to enable FortiClient (macOS) notifications.

To enable notifications:

1. Go to *System Preferences > Notifications > FortiClientAgent*.
2. Toggle *Allow Notifications* on.

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.

What's new in FortiClient (macOS) 7.0.1

For information about what's new in FortiClient (macOS) 7.0.1, see the [FortiClient & EMS 7.0 New Features](#).

Installation information

Firmware images and tools

The following files are available from the [Fortinet support site](#):

File	Description
FortiClientTools_7.0.1.xxxx_macosx.tar.gz	Includes utility tools and files to help with installation.
FortiClientVPNSetup_7.0.1.xxxx_macosx.dmg	Free VPN-only installer.

The following files are available from [FortiClient.com](#):

File	Description
FortiClient_7.0.1.xxxx_macosx.dmg	Standard installer for macOS.
FortiClientVPNSetup_7.0.1.xxxx_macosx.dmg	Free VPN-only installer.

FortiClient EMS 7.0.1 includes the FortiClient (macOS) 7.0.1 standard installer.



Review the following sections prior to installing FortiClient version 7.0.1: [Introduction on page 5](#), [Special notices on page 6](#), and [Product integration and support on page 13](#).

Upgrading from previous FortiClient versions

FortiClient version 7.0.1 supports upgrade from FortiClient 6.2, 6.4, and 7.0.

FortiClient (macOS) 7.0.1 features are only enabled when connected to EMS 7.0.

See the [FortiClient and FortiClient EMS Upgrade Paths](#) for information on upgrade paths.

Downgrading to previous versions

FortiClient 7.0.1 does not support downgrading to previous FortiClient versions.

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) 7.0.1 product integration and support information:

Desktop operating systems	<ul style="list-style-type: none">• macOS Big Sur (version 11)• macOS Catalina (version 10.15)
Minimum system requirements	<ul style="list-style-type: none">• Intel processor or M1 chip• 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
AV engine	<ul style="list-style-type: none">• 6.00258
FortiClient EMS	<ul style="list-style-type: none">• 7.0.0 and later
FortiOS	<p>The following versions support ZTNA:</p> <ul style="list-style-type: none">• 7.0.0 and later <p>The following versions support IPsec and SSL VPN:</p> <ul style="list-style-type: none">• 7.0.0 and later• 6.4.0 and later• 6.2.0 and later• 6.0.0 and later
FortiAnalyzer	<ul style="list-style-type: none">• 7.0.0 and later
FortiManager	<ul style="list-style-type: none">• 7.0.0 and later
FortiSandbox	<ul style="list-style-type: none">• 4.0.0 and later• 3.2.0 and later• 3.1.0 and later• 3.0.0 and later• 2.5.0 and later
FortiAuthenticator	<ul style="list-style-type: none">• 6.4.0 and later• 6.3.0 and later• 6.2.0 and later• 6.1.0 and later• 6.0.0 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) 7.0.1. For inquiries about a particular bug, contact [Customer Service & Support](#).

Remote Access

Bug ID	Description
608810	SSL VPN fails to connect. Log shows <code>unknown:0 store cookie failed</code> .
639466	FortiClient (macOS) disconnects from SSL VPN due to host check timeout.

Web Filter

Bug ID	Description
646019	Web Filter blocks connections to locally hosted web server.

Endpoint control

Bug ID	Description
675953	FortiClient cannot store the Telemetry connection key.
721647	EMS should prevent installation and upgrade to unsupported OS versions.

Performance

Bug ID	Description
703785	<code>com.fortinet.forticlient.macos.webfilter</code> crash.

Known issues

The following issues have been identified in FortiClient (macOS) 7.0.1. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

Endpoint control

Bug ID	Description
641503	FortiClient (macOS) cannot get EMS serial number.
646115	Endpoint running process and netstat info is not visible on EMS.
655449	FortiClient (macOS) has Telemetry connection issue to FortiClient Cloud when gateway list is assigned.
664634	FortiClient cannot register with FortiClient Cloud if the connection key has a hyphen.
684302	FortiClient keeps registering after deregistering from FortiClient Cloud.
708932	macOS devices get stuck and/or in disconnected state from EMS.
714853	GUI unlock button is not visible after disregistering from EMS.

Remote Access

Bug ID	Description
664285	VPN connection terminates unexpectedly with error code -121.
678564	FortiClient (macOS) does not honor <code>remoteauthtimeout</code> or <code>login-timeout</code> from FortiGate with SAML authentication.
684913	SAML authentication on SSL VPN with realms does not work.
690432	GUI fails to import XML VPN configuration.
705518	FortiTray does not differentiate between corporate and personal VPNs.
726590	FortiClient does not connect using DTLS.
729828	Rename FortiClientUpdate to FortiClientInstaller in popup upon executing OnlineInstaller.
732973	SSL VPN connectivity problems and disconnection due to sslvpnd crash.
738888	Save password feature does not work if prompt for login is enabled.

Web Filter

Bug ID	Description
661231	Move the Web Filter block to the FortiAnalyzer Event section.
738547	Web Filter browser extension blocks random sites.

Configuration

Bug ID	Description
650334	Feature lists for log setting are inconsistent between EMS and FortiClient (macOS).
714584	Rebooting automatically deletes Zero Trust Network Access-related certificates from certificate store.

Multitenancy

Bug ID	Description
647428	FortiClient (macOS) does not send software inventory to custom site.

Performance

Bug ID	Description
704524	FortiClient causes system to run out of resources due to excessive fcconfig errors.
714620	FortiAgent and fcconfig crash when saving VPN tunnel configuration.



www.fortinet.com

Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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. 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.