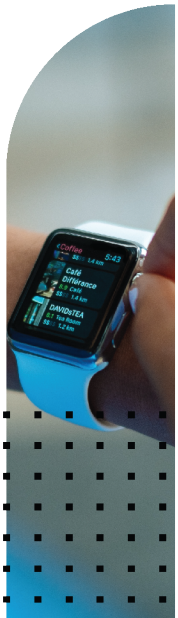
Release Notes

FortiClient (macOS) 7.0.2



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/training-certification

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

November 03, 2021
FortiClient (macOS) 7.0.2 Release Notes
04-702-744815-20211103

TABLE OF CONTENTS

Change log

Date	Change description
2021-10-25	Initial release.
2021-11-03	Updated Endpoint security improvement on page 9.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (macOS) 7.0.2 build 0069.

This document includes the following sections:

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

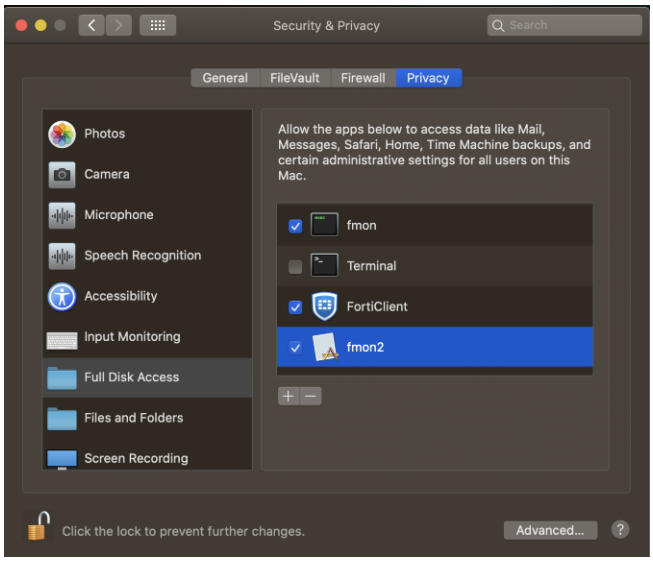
Enabling full disk access

FortiClient (macOS) 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
- FortiGuardAgent

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/FortiGuardAgent.app`

Activating system extensions

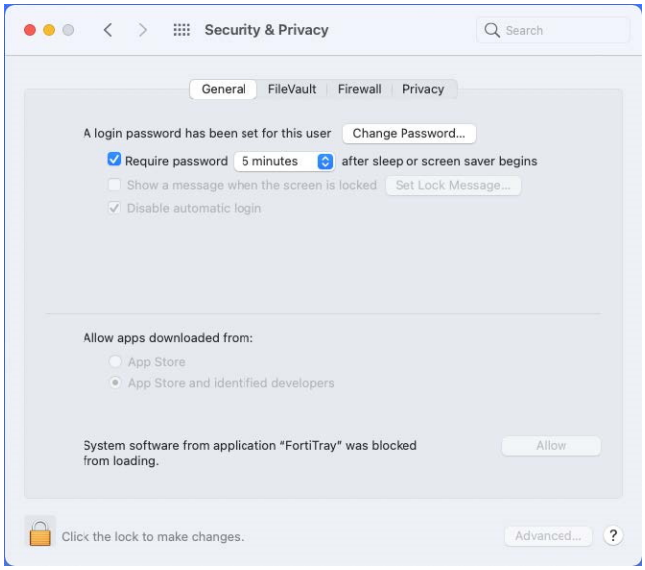
After you perform an initial install of FortiClient (macOS), the device prompts you to allow some settings and disk access for FortiClient (macOS) processes. You must have administrator credentials for the macOS machine to configure this change.

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*.

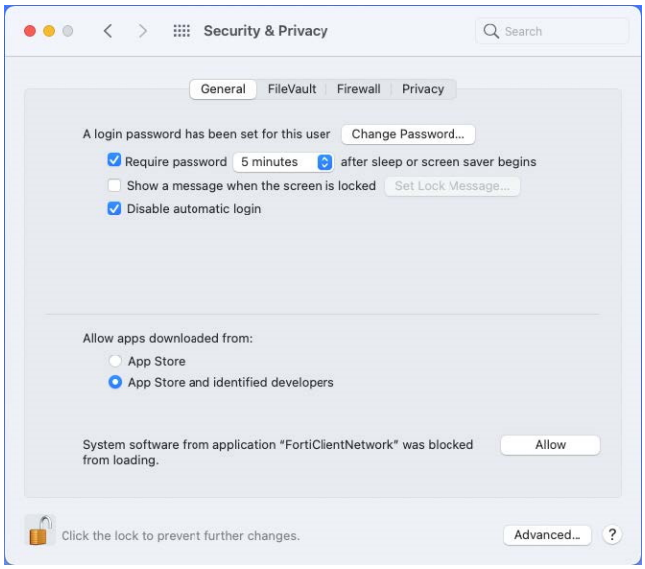


Web Filter and Application Firewall

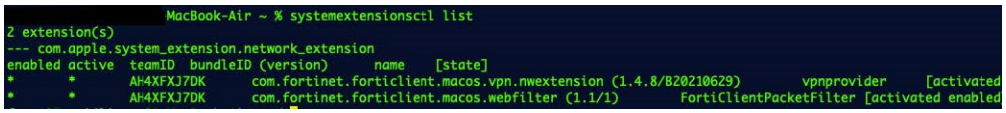
You must enable the FortiClientNetwork extension for Web Filter and Application Firewall to work properly. The FortiClient (macOS) team ID is AH4XFXJ7DK.

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:



Enabling notifications

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

To enable notifications:

1. Go to *System Preferences* > *Notifications* > *FortiGuardAgent*.
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.

Endpoint security improvement

7.0.2 adds an improvement to endpoint security that impacts compatibility between FortiClient and EMS, and the recommended upgrade path. The FortiClient 7.0.2 installer is not available on FortiGuard Distribution Servers (FDS). To use the FortiClient 7.0.2 installer, you must download it from Customer Service & Support. See Endpoint security improvement.

If the EMS server certificate is invalid, and FortiClient is upgraded to 7.0.2, by default, FortiClient displays a warning message on the GUI when trying to connect to the EMS. The end user should click *allow* to complete the connection. FortiClient does not connect to the EMS if the end user selects *deny*. If the end user selects *deny*, FortiClient retries connecting to the EMS after a system reboot. The same warning message displays while trying to connect to the EMS. The end user should click *allow* to complete the connection.

What’s new in FortiClient (macOS) 7.0.2

FortiClient 7.0.2 adds an improvement to endpoint security to follow industry standards. See Endpoint security improvement.

Installation information

Firmware images and tools

The following files are available from the Fortinet support site:

File	Description
FortiClientTools_7.0.2.xxxx_macosx.tar.gz	Includes utility tools and files to help with installation.
FortiClientVPNSetup_7.0.2.xxxx_macosx.dmg	Free VPN-only installer.

The following files are available from FortiClient.com:

File	Description
FortiClient_7.0.2.xxxx_macosx.dmg	Standard installer for macOS.
FortiClientVPNSetup_7.0.2.xxxx_macosx.dmg	Free VPN-only installer.

FortiClient EMS 7.0.2 includes the FortiClient (macOS) 7.0.2 standard installer.

Review the following sections prior to installing FortiClient version 7.0.2: Introduction on page 5, Special notices on page 6, and Product integration and support on page 13.

Upgrading from previous FortiClient versions

You must upgrade EMS 7.0.2 before upgrading FortiClient.

FortiClient 7.0.2 supports upgrade from FortiClient 6.2, 6.4, and 7.0.

FortiClient (macOS) 7.0.2 features are only enabled when connected to EMS 7.0.

With the new endpoint security improvement feature, there are backward compatibility issues to consider while planning upgrades. See Recommended upgrade path for information on upgrading FortiClient (macOS) 7.0.2.

You cannot upgrade FortiClient (macOS) 6.4.7 to 7.0.2.

Downgrading to previous versions

FortiClient 7.0.2 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) 7.0.2 product integration and support information:

Desktop operating systems	• macOS Monterey (version 12) • macOS Big Sur (version 11) • macOS Catalina (version 10.15)
Minimum system requirements	• 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	• 6.00258
FortiClient EMS	• 7.0.0 and later
FortiOS	The following versions support ZTNA: • 7.0.0 and later The following versions support IPsec and SSL VPN: • 7.0.0 and later • 6.4.0 and later • 6.2.0 and later • 6.0.0 and later
FortiAnalyzer	• 7.0.0 and later
FortiManager	• 7.0.0 and later
FortiSandbox	• 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	• 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) 7.0.2. For inquiries about a particular bug, contact Customer Service & Support.

Remote Access

Bug ID	Description
729828	Rename FortiClientUpdate to FortiClientInstaller in popup upon executing OnlineInstaller.

Endpoint control

Bug ID	Description
684302	FortiClient keeps registering after deregistering from FortiClient Cloud.

Common Vulnerabilities and Exposures

Bug ID	Description
723081	FortiClient (macOS) 7.0.2 is no longer vulnerable to the following CVE Reference: • CVE-2021-41028 Visit https://fortiguard.com/psirt for more information.

Known issues

The following issues have been identified in FortiClient (macOS) 7.0.2. 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 information 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.
708932	macOS devices get stuck and/or in disconnected state from EMS.
714853	GUI unlock button is not visible after disregistering from EMS.
754532	EMS deployment considerations when *Invalid Certificate Action* is *Warn* in FortiClient installer created on EMS.

Remote Access

Bug ID	Description
678564	FortiClient (macOS) does not honor `remoteauthtimeout` or `login-timeout` 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.
738888	Save password feature does not work if prompt for login is enabled.
755805	Unity features disabled in EMS-created VPN profile are visible in Remote Access GUI.

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.

Install and deployment

Bug ID	Description
756715	EMS defaults *Invalid Cert Action* to *Warn* for created FortiClient installer. Workaround: EMS administrator to select *Allow* for *Invalid Cert Action* when creating FortiClient installer.

www.fortinet.com