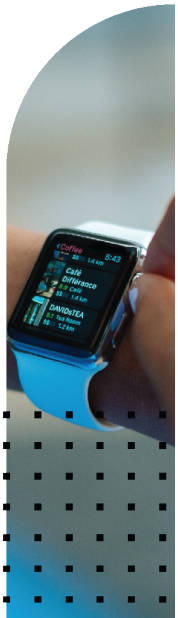
Release Notes

FortiClient (macOS) 7.0.3



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

February 28, 2022
FortiClient (macOS) 7.0.3 Release Notes
04-703-764298-20220228

TABLE OF CONTENTS

Change log

Date	Change description
2022-02-28	Initial release.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (macOS) 7.0.3 build 0131.

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

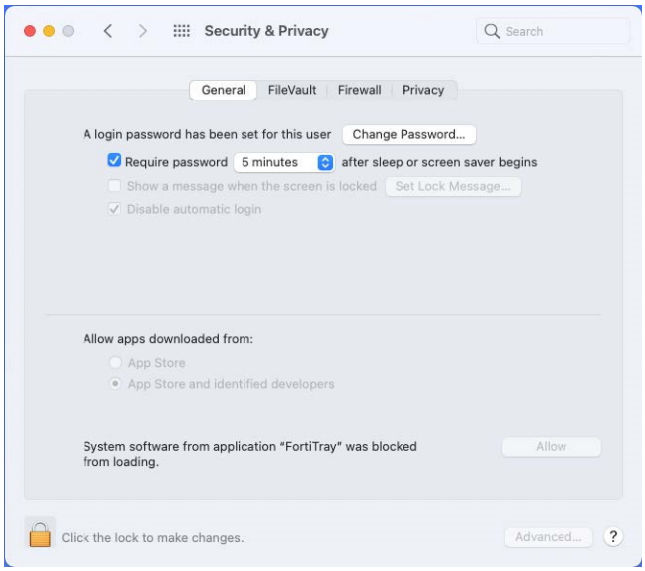
After you perform an initial install of FortiClient (macOS), the device prompts you to allow some settings and disk access for FortiClient (macOS) processes. You must have administrator credentials for the macOS machine to configure this change.

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*.

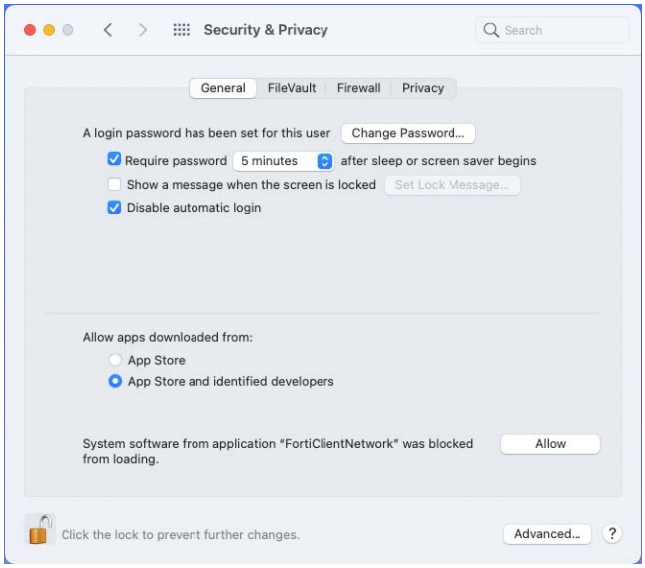


Web Filter and Application Firewall

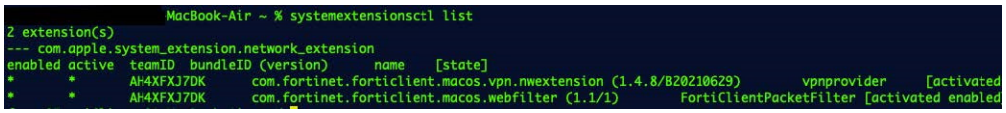
You must enable the FortiClientNetwork extension for Web Filter and Application Firewall to work properly. The FortiClient (macOS) team ID is AH4XFXJ7DK.

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.

MacBook Pro with M1X chip conflict

The FortiClient Application Firewall and Web Filter features conflict with the SSL VPN feature that is included on new MacBook Pro models that use the new M1X chip. This conflict does not occur on other macOS devices.

FortiClient (macOS) and mobile device management

See the FortiClient Intune Deployment Guide.

What’s new in FortiClient (macOS) 7.0.3

For information about what's new in FortiClient (macOS) 7.0.3, see the *FortiClient & FortiClient EMS 7.0 New Features Guide*.

Installation information

Firmware images and tools

The following files are available from the Fortinet support site:

File	Description
FortiClientTools_7.0.3.xxxx_macosx.tar.gz	Includes utility tools and files to help with installation.
FortiClientVPNSetup_7.0.3.xxxx_macosx.dmg	Free VPN-only installer.

The following files are available from FortiClient.com:

File	Description
FortiClient_7.0.3.xxxx_macosx.dmg	Standard installer for macOS.
FortiClientVPNSetup_7.0.3.xxxx_macosx.dmg	Free VPN-only installer.

FortiClient EMS 7.0.3 includes the FortiClient (macOS) 7.0.3 standard installer.

Review the following sections prior to installing FortiClient version 7.0.3: Introduction on page 6, Special notices on page 7, and Product integration and support on page 14.

Upgrading from previous FortiClient versions

You must upgrade EMS to 7.0.2 or newer before upgrading FortiClient.

FortiClient 7.0.3 supports upgrade from FortiClient 6.2, 6.4, and 7.0.

FortiClient (macOS) 7.0.3 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) 7.0.3.

Downgrading to previous versions

FortiClient 7.0.3 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) 7.0.3 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) 7.0.3. For inquiries about a particular bug, contact Customer Service & Support.

Install and upgrade

Bug ID	Description
729828	Rename FortiClientUpdate to FortiClientInstaller in popup when executing VPN online installer.
760969	FortiClient (macOS) requires Rosetta on macOS Monterey.

GUI

Bug ID	Description
719103	FortiClient (macOS) should show macOS extension permission status.
751299	FortiClient (macOS) has empty vulnerability details tab.

Zero Trust tags

Bug ID	Description
710512	Zero Trust tagging rule for Active Directory-joined macOS devices.

Application Firewall

Bug ID	Description
736534	Application Firewall does not block certain applications in macOS Big Sur and Catalina.

Malware Protection and Sandbox Detection

Bug ID	Description
747879	Malware endpoint summary shows no scans have been completed for macOS endpoints.
748165	FortiClient (macOS) does not perform malware scan after missing scheduled date.

Remote Access

Bug ID	Description
659249	Improve VPN DNS management.
684913	SAML authentication on SSL VPN with realms does not work.
700028	IPsec VPN disconnects with errors -111 and -104.
721651	When connected to a full VPN to FortiGate, FortiClient (macOS) sends virtual IP and MAC addresses to EMS.
754177	When connecting to VPN via FortiTray, FortiClient (macOS) cannot retrieve saved password from keychain, affecting autoconnect/always up.
759551	SSL VPN fails to load local certificate: `keychainRead`.

Vulnerability Scan

Bug ID	Description
749161	FortiClient (macOS) does not detect critical macOS vulnerabilities: CVE-2021-30858 and CVE-2021-30860.

Web Filter and plugin

Bug ID	Description
738770	FortiClient (macOS) blocks all network traffic including the EMS keepalive, until the user manually stops the Web Filter system extension.

Endpoint control

Bug ID	Description
736759	FortiClient (macOS) displays incorrect on-Fabric status when on-Fabric detection rule is set to a specific public IP address.
738582	On macOS Big Sur, FortiClient (macOS) does not change to off-Fabric profile.
757985	Group assignment rule does not work.

Configuration

Bug ID	Description
704524	FortiClient (macOS) stops functioning after system runs out of resources due to fcconfig's *ERR:socketpair failed 24-Too may files open*.

Other

Bug ID	Description
742462	FortiClient (macOS) cannot shut down while connected to EMS.

Common Vulnerabilities and Exposures

Bug ID	Description
723081	FortiClient (macOS) 7.0.3 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) 7.0.3. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Avatar

Bug ID	Description
763109	User cannot submit user-specified information and cannot log in with cloud services.

Zero Trust Network Access connections

Bug ID	Description
736561	TCP forwarding does not work effectively for macOS while trying to RDP and SSH over IPsec or SSL VPN tunnel.
786340	ZTNA traffic not routed to ZTNA Access Proxy when connected to SSLVPN. A workaround in 7.0.3 is to use a physical macOS device and disconnect thunderbolt.

GUI

Bug ID	Description
763681	EMS cannot update current VPN connection on FortiClient (macOS).

Malware Protection and Sandbox Detection

Bug ID	Description
753672	FortiClient (macOS) logs do not indicate threat level.
763603	Removable media access does not block devices.
774268	Sandbox test button on GUI shows invalid network IP address and Sandbox status remains unreachable after configuring valid IP address.

Bug ID	Description
784572	EMS doesn't have USB monitor event tab for USB monitor logs sent from FortiClient (macOS) when tested on masOS endpoints.

Remote Access

Bug ID	Description
697099	Traffic bypasses the Web Filter when it goes through IPsec VPN tunnel.
730348	Unity features for save password, autoconnect, and always up are missing in GUI.
738425	SSL VPN GUI and tray mismatch in Unity features.
755199	Button to launch FortiClient from SSL VPN web portal does not work.
761729	IPsec VPN stays in connecting stage with wrong preshared key.
764104	FortiClient (macOS) does not forward traffic via SSL VPN tunnel.
768818	After connecting to SSL VPN main or full tunnel, user cannot access corporate internal network, while Internet works fine.
776888	FortiClient (macOS) does not dynamically display *Disconnect* VPN button unless the user reopens the console.
781422	IPsec VPN rekey does not work with FortiToken.
782048	You must disable Application Firewall and Web Filter on new Macbook Pros 14 and 16 to avoid conflict with SSL VPN.
785147	FortiSASE VPN doesn't automatically connect back after FortiClient (macOS) is upgraded from 6.4.6 GA to 7.0.3 latest build.
786011	Vulnerability feature does not auto-patch OS 12.2.1 after OS vulnerability is detected on Monterey 12.1.
786029	After SASE EMS is upgraded from 6.4.4 to 7.0.3, the FortiClient (macOS) OS status shows not connected.

Zero Trust tags

Bug ID	Description
762199	FortiClient (macOS) fails to report user identity tag.

Vulnerability Scan

Bug ID	Description
770605	GUI does not display the correct information about the scheduled scan time for weekly and monthly vulnerability scheduled scans.
785166	Many installed apps are not displaying under Software Inventory on EMS.

Web Filter and plugin

Bug ID	Description
755055	When action set for site categories is warn, browser does not show the customized webpage, which allows user to bypass blocking.
772332	External Ethernet adapter dongle gets disconnected when running speed test.

Application Firewall

Bug ID	Description
718957	Application Firewall does not work after reboot.
768897	Application Firewall does not take effect unless FortiClient (macOS) disconnects and reconnects to EMS.

Endpoint management

Bug ID	Description
770364	Disable third party features for macOS endpoints.

Logs

Bug ID	Description
777013	Change/existing avatar image does not show on FortiAnalyzer.

Install and deployment

Bug ID	Description
754722	Uninstall deployment from EMS does not work.
764672	FortiClient (macOS) displays deployment popup for user when EMS configured an unattended installation.

Bug ID	Description
784738	The FortiClient (macOS) console and invalid certificate prompt are not showing automatically after FortiClient (macOS) installation.

www.fortinet.com