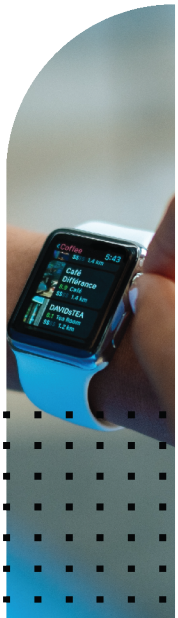
Release Notes

FortiClient (macOS) 7.0.6



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

July 19, 2022
FortiClient (macOS) 7.0.6 Release Notes
04-706-805985-20220719

TABLE OF CONTENTS

Change log

Date	Change description
2022-07-05	Initial release.
2022-07-19	Added Proxy mode extension on page 9.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (macOS) 7.0.6 build 0208.

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

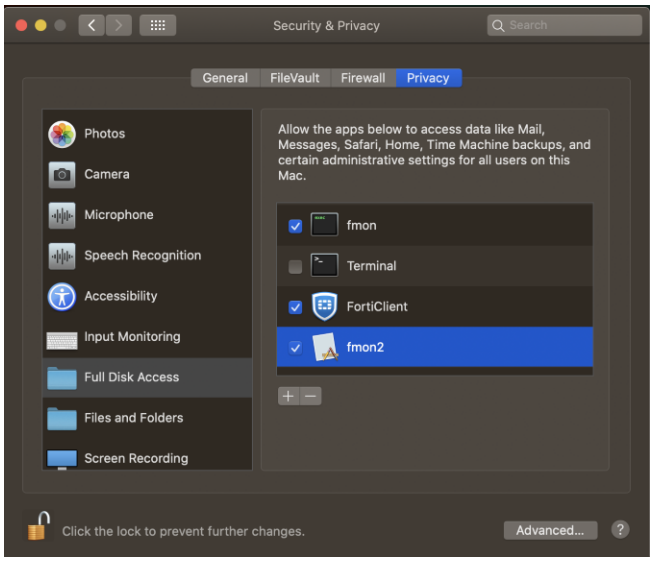
Enabling full disk access

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

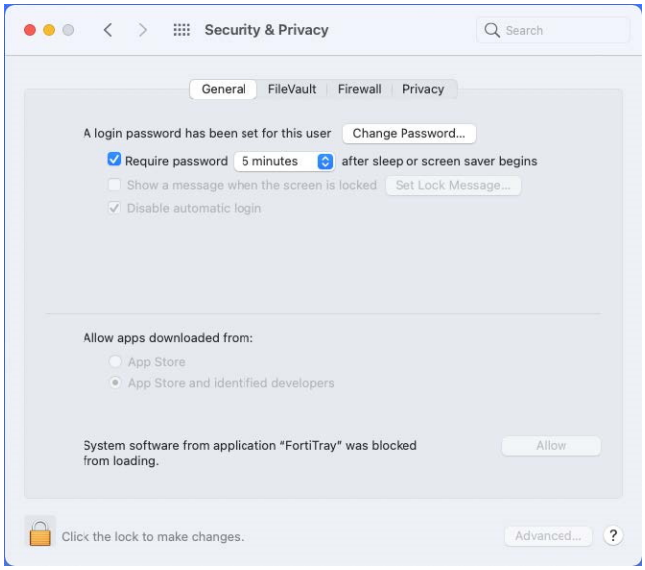
After you perform an initial install of FortiClient (macOS), the device prompts you to allow some settings and disk access for FortiClient (macOS) processes. You must have administrator credentials for the macOS machine to configure this change.

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*.

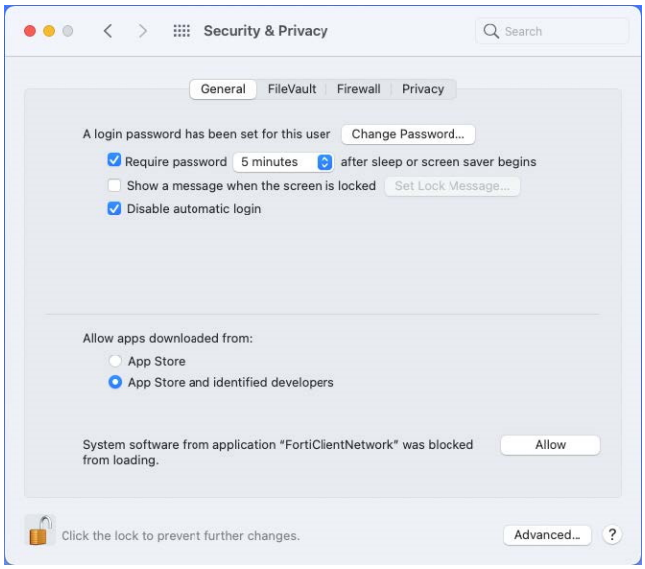


Web Filter and Application Firewall

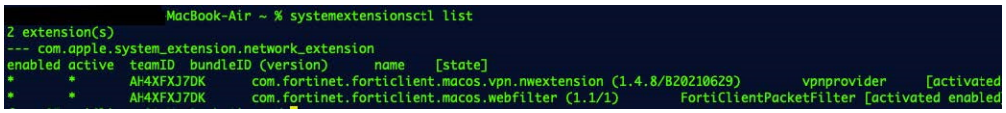
You must enable the FortiClientNetwork extension for Web Filter and Application Firewall to work properly. The FortiClient (macOS) team ID is AH4XFXJ7DK.

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:



Proxy mode extension

A new system extension, com.fortinet.forticlient.macos.proxy, works as a proxy server to proxy a TCP connection. macOS manages the extension's connection status and other statistics. This resolves the issue that Web Filter fails to work when SSL and IPsec VPN are connected.

FortiClient (macOS) automatically installs the extension on an M1 Pro or newer macOS device. For a macOS device with Intel or M1 chip, you can do the following:

To enable proxy mode on macOS devices with an Intel or M1 chip:

1. Add following XML configuration:
```
<forticlient_configuration>
   <webfilter>
      <use_transparent_proxy>1</use_transparent_proxy>
   <webfilter>
<forticlient_configuration>
```
2. Manually create an empty file: `sudo touch /Library/Application\Support/Fortinet/FortiClient/conf/use_transparent_proxy`

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.

Installation information

Firmware images and tools

The following files are available from the Fortinet support site:

File	Description
FortiClientTools_7.0.6.xxxx_macosx.tar.gz	Includes utility tools and files to help with installation.
FortiClientVPNSetup_7.0.6.xxxx_macosx.dmg	Free VPN-only installer.

The following files are available from FortiClient.com:

File	Description
FortiClient_7.0.6.xxxx_macosx.dmg	Standard installer for macOS.
FortiClientVPNSetup_7.0.6.xxxx_macosx.dmg	Free VPN-only installer.

FortiClient EMS 7.0.6 includes the FortiClient (macOS) 7.0.6 standard installer.

Review the following sections prior to installing FortiClient version 7.0.6: Introduction on page 5, Special notices on page 6, and Product integration and support on page 12.

Upgrading from previous FortiClient versions

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

FortiClient 7.0.6 supports upgrade from FortiClient 6.2, 6.4, and 7.0.

FortiClient (macOS) 7.0.6 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) 7.0.6.

Downgrading to previous versions

FortiClient 7.0.6 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) 7.0.6 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	• 6.00266
FortiClient EMS	• 7.0.0 and later
FortiOS	The following versions support zero trust network access: • 7.0.6 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	• 4.2.0 and later • 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) 7.0.6. For inquiries about a particular bug, contact Customer Service & Support.

Deployment and installers

Bug ID	Description
782213	Upgrade fails and user cannot extract install file.

Remote Access

Bug ID	Description
684913	SAML authentication on SSL VPN with realms does not work.
723935	FortiClient does not support always on connections when using SAML single sign on.
767596	FortiClient does not connect over SSL VPN.
776888	FortiClient does not dynamically display button to disconnect from VPN unless you reopen the FortiClient (macOS) window.
785147	FortiSASE VPN does not automatically reconnect after upgrade.
820439	If *Save Password* is enabled on both the FortiClient and FortiGate, FortiTray stores the password in clear view.

Web Filter and plugin

Bug ID	Description
757920	Web Filter does not become enabled when FortiClient is off-fabric.
758472	Web Filter does not work when SSL VPN is connected.

Endpoint control

Bug ID	Description
723599	FortiClient uses FortiSASE egress IP address as the public IP address.

Other

Bug ID	Description
798251	FortiClient (macOS) cannot register to EMS using button in registration email.

Known issues

The following issues have been identified in FortiClient (macOS) 7.0.6. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Configuration

Bug ID	Description
730415	FortiClient (macOS) backs up configuration that is missing locally configured Zero Trust Network Access connection rules.
817546	FortiClient (macOS) does not point to usforticlient.fortinet.net for signature update setting when Location-US | Server-FortiGuard.

Zero Trust Network Access connection rules

Bug ID	Description
761497	macOS displays security confirmation popup twice on Monterey 12.0.1 when user starts, registers, unregisters, or shuts down FortiClient.

GUI

Bug ID	Description
763681	EMS cannot update current VPN connection on FortiClient (macOS).
794215	GUI displays server name indication through EMS Telemetry info when connected to FortiClient Cloud.

Endpoint control

Bug ID	Description
706496	Deep inspection does not work and the endpoint does not download the certificate.
735589	Non-default site shows incorrect deployment state.
753663	When using off-net profile that has antivirus protection enabled, GUI does not show *Malware Protection* tab.
784738	FortiClient console and invalid certificate prompt do not show automatically after installation.
805088	When ztagent process is accidentally terminated, FortiClient cannot get new configuration profile from EMS.
814351	Endpoint information page incorrectly displays device user's domain information after user switches on macOS device.
816209	EMS should only count endpoint as on-fabric when all the rules are met in an on-fabric detection rule set.

Remote Access

Bug ID	Description
736245	IPsec VPN does not work when multiple remote gateways are configured in a priority-based list.
738425	SSL VPN GUI and tray mismatch in unity features.
765621	Network connection issue after waking from sleep mode.
768818	After connecting to SSL VPN main or full tunnel, user cannot access corporate internal network, while Internet works fine.
783439	SAML SSL VPN is stuck at authentication step with some identity providers.
783502	SSL VPN connection fails when fully qualified domain name is set for remote gateway.
790392	FortiClient blocks the network when Wi-Fi is changed.
790733	FortiClient cannot resolve DNS suffix after connecting to SSL VPN.
793893	Search domains do not transfer correctly to endpoints.
794730	Auto connect and always up options appear as enabled after disconnecting from VPN when they are disabled on the XML profile.
800923	Customized host check failure message for SSL VPN does not work.
800978	Autoconnect is triggered twice when both on-fabric and off-fabric profiles are configured.

Bug ID	Description
801134	FortiClient (macOS) does not generate or replicate SSL VPN logs for uploading to FortiAnalyzer when tunnel is established.
813039	User cannot visit local services after FortiSASE connection.
821705	SSL VPN tunnel does not show *Bytes Received* and *Bytes Sent* correctly.

Zero Trust tags

Bug ID	Description
793033	ZTNA LDAP group rule does not work.
805201	*Security > File Vault Disk Encryption is enabled* tag does not update dynamically when the encryption status changes.
816183	On-Fabric detection VPN tunnel rule type does not work properly with FortiClient (macOS).

Vulnerability Scan

Bug ID	Description
786011	Vulnerability feature does not autopatch macOS Monterey 12.2.1 after it detects operating system (OS) vulnerability on macOS Monterey 12.1.
790288	Vulnerability scan does not detect OS vulnerabilities.

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 speed test is run.
788799	Web Filter does not block websites based on configured exclusions.
795631	Web Filter does not block the selected categories.
823469	FortiClient console does not show security risk category as configured on EMS Web Filter profile.

Application Firewall

Bug ID	Description
718957	Application Firewall does not work after reboot.
800344	You can remotely access quarantined endpoints using VNC protocol.

Endpoint management

Bug ID	Description
770364	Disable third party features for macOS endpoints.
773440	Domain-joined macOS endpoints register as duplicates to EMS.

Performance

Bug ID	Description
778651	Large downloads and speed tests result in high latency, packet loss, and poor performance.

Installation and upgrade

Bug ID	Description
820245	While using online installer, upgrading from free VPN-only client to the full version of FortiClient (macOS) fails.

Logs

Bug ID	Description
713287	FortiClient does not generate local logs for zero trust network access.
750703	IPsec and SSL VPN events are not logged on FortiAnalyzer appropriately.
801134	FortiClient (macOS) does not generate or replicate SSL VPN logs for upload to FortiAnalyzer when it establishes a tunnel.

www.fortinet.com