FORTINET

Release Notes

FortiClient (macOS) 7.2.0

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 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

January 31, 2023
FortiClient (macOS) 7.2.0 Release Notes
04-720-832533-20230131

TABLE OF CONTENTS

Change log **5**
Introduction **6**
Licensing 6
Special notices **7**
Enabling full disk access 7
Activating system extensions 8
VPN 8
Web Filter and Application Firewall 8
Proxy mode extension 9
Enabling notifications 10
DHCP over IPsec VPN not supported 10
IKEv2 not supported 10
Running multiple FortiClient instances 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 14
Resolved issues **15**
Install and upgrade 15
GUI 15
ZTNA connection rules 15
Zero trust tags 16
Application Firewall 16
Performance 16
Remote Access 16
Logs 17
Web Filter and plugin 17
Endpoint management 17
Administration 18
Avatar and social login information 18
Endpoint control 18
Deployment and installers 18
Endpoint security 19
Malware Protection and Sandbox 19
Onboarding 19
Zero Trust telemetry 19
Other 19

Common Vulnerabilities and Exposures 20
Known issues **21**
Configuration 21
Endpoint control 21
GUI 21
Remote Access 22
Zero Trust tags 22
Avatar and social login infomration 23
Web Filter and plugin 23
Application Firewall 23
Logs 23
Installation and upgrade 23
FSSOMA 24
Malware Protection and Sandbox 24
Onboarding 24
ZTNA connection rules 25

Change log

Date	Change description
2023-01-31	Initial release.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (macOS) 7.2.0 build 0655.

This document includes the following sections:

- Special notices on page 7
- Installation information on page 11
- Product integration and support on page 13
- Resolved issues on page 15
- Known issues on page 21

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:

- fctservctl2
- FortiClient

The following lists the services and their folder locations:

- Fctservctl2: `/Library/Application\ Support/Fortinet/FortiClient/bin/`
- FortiClient (macOS) application: `/Applications/FortiClient.app`

Activating system extensions

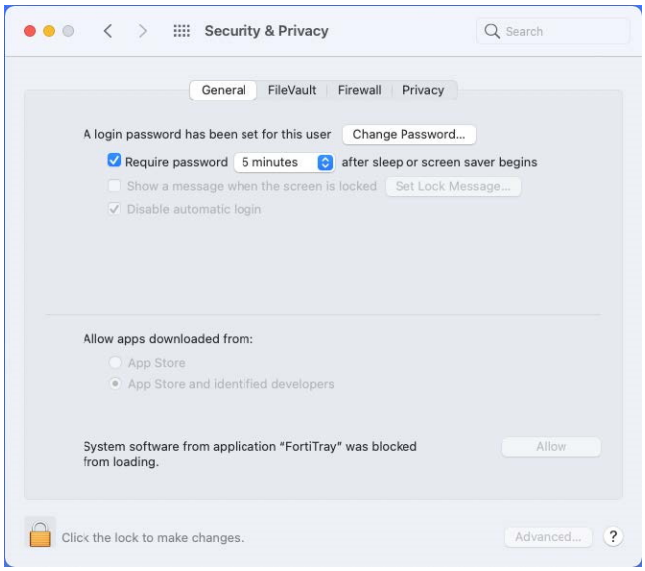
After you initially install FortiClient (macOS), the device prompts you to allow some settings and disk access for FortiClient (macOS) processes. You must have administrator credentials for the macOS machine to configure this change.

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*.

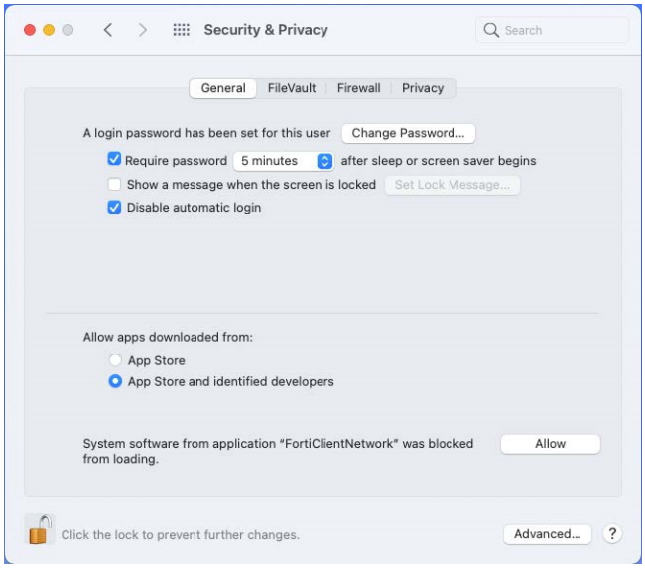


Web Filter and Application Firewall

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:

```
[redacted]-Mac ~ % systemextensionsctl list
3 extension(s)
--- com.apple.system_extension.network_extension
enabled active  teamID  bundleID (version)      name    [state]
*       *       AH4XFXJ7DK      com.fortinet.forticlient.macos.webfilter (1.6.9/1)      FortiClientPacketFilter [activated enabled]
*       *       AH4XFXJ7DK      com.fortinet.forticlient.macos.vpn.nwextension (7.2.0/0652)     vpnprovider     [activated enabled]
*       *       AH4XFXJ7DK      com.fortinet.forticlient.macos.proxy (1.0.12/1)FortiClientProxy [activated enabled]
```

Proxy mode extension

The com.fortinet.forticlient.macos.proxy system extension 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`

This XML element does not affect Windows endpoints.

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.

Running multiple FortiClient instances

FortiClient (macOS) does not support running multiple FortiClient instances for different users simultaneously.

Installation information

Firmware images and tools

The following files are available from the Fortinet support site:

File	Description
FortiClientTools_7.2.0.xxxx_macosx.tar.gz	Includes utility tools and files to help with installation.
FortiClientVPNSetup_7.2.0.xxxx_macosx.dmg	Free VPN-only installer.

The following files are available from FortiClient.com:

File	Description
FortiClient_7.2.0.xxxx_macosx.dmg	Standard installer for macOS.
FortiClientVPNSetup_7.2.0.xxxx_macosx.dmg	Free VPN-only installer.

FortiClient EMS 7.2.0 includes the FortiClient (macOS) 7.2.0 standard installer.

Review the following sections prior to installing FortiClient version 7.2.0: Introduction on page 6, Special notices on page 7, and Product integration and support on page 13.

Upgrading from previous FortiClient versions

You must upgrade EMS to 7.2 or newer before upgrading FortiClient.

FortiClient 7.2.0 supports upgrade from FortiClient 6.2, 6.4, and 7.0.

FortiClient (macOS) 7.2.0 features are only enabled when connected to EMS 7.2.

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) 7.2.0.

Downgrading to previous versions

FortiClient 7.2.0 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) 7.2.0 product integration and support information:

Desktop operating systems	• macOS Ventura (version 13) • macOS Monterey (version 12) • macOS Big Sur (version 11)
Minimum system requirements	• Intel processor or M1 or M2 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	• 6.00282
FortiClient EMS	• 7.2.0
FortiOS	The following versions support zero trust network access: • 7.2.0 and later • 7.0.6 and later The following versions support IPsec and SSL VPN: • 7.2.0 and later • 7.0.0 and later • 6.4.0 and later • 6.2.0 and later • 6.0.0 and later
FortiAnalyzer	• 7.2.0 and later • 7.0.0 and later
FortiManager	• 7.2.0 and later • 7.0.0 and later
FortiSandbox	• 4.2.0 and later • 4.0.0 and later • 3.2.0 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) 7.2.0. For inquiries about a particular bug, contact Customer Service & Support.

Install and upgrade

Bug ID	Description
754722	Uninstall deployment from EMS does not work on FortiClient (macOS).
755309	FortiClient triggers installation of Web Filter system extension only if custom.conf contains all features for the installer.
811001	Intune deployment script does not checks installed version.
833058	Full disk access permission guidance is not proper/accurate on macOS Ventura 13.0 beta with M1 chip.

GUI

Bug ID	Description
763681	EMS cannot update VPN current connection in FortiClient.
828283	Chinese warning message for EMS certificate is empty.
845597	GUI becomes inactive after connecting to VPN.

ZTNA connection rules

Bug ID	Description
832631	After switching to Wi-Fi, ztagent daemon does not run and ZTNA feature does not work.
845674	When registering FortiClient, ZTNA certificate should be installed in keychain silently if CA certificate is already trusted and imported in system.
869648	On macOS 12.6 with M2 chip, fmon2 and ztagent use 65% of CPU, which affects machine performance.

Zero trust tags

Bug ID	Description
805201	FileVault disk encryption is enabled tag does not update dynamically when the encryption status changes.

Application Firewall

Bug ID	Description
827917	Macbook Pro network connectivity issue.

Performance

Bug ID	Description
829658	FortiClient (macOS) overconsumes CPU and memory.

Remote Access

Bug ID	Description
684913	SAML authentication on SSL VPN with realms does not work.
765621	FortiClient has network connection issue after waking from sleep mode.
767596	FortiClient does not connect over SSL VPN.
773519	Free VPN-only client cannot save password for SSL and IPsec VPN.
779797	FortiClient fails to establish SSL VPN with FQDN resolving to multiple gateways.
791930	Autoconnect only when off-net setting fails to trigger autoconnect when endpoint is off-Fabric and logging off and logging into the system.
797559	SSL VPN host check validation does not work, including SAML users.
800918	Autoconnect is triggered and fails after system reboot with IPsec VPN tunnel profile using certificate authentication.
812540	FortiClient does not respect exclusive routing option.
813039	User cannot visit local services after FortiSASE connection.

Bug ID	Description
813241	FortiClient cannot reconnect to SSL VPN without credentials.
840710	VPN autoconnect has issue when there is network error.
840789	VPN autoconnect has issue when EMS is offline.
840816	epctrl takes long time before it sends message to FortiTray to connect VPN.
861923	FortiClient fails to autoconnect to IPsec VPN with certificate.

Logs

Bug ID	Description
713287	FortiClient does not generate local logs for zero trust network access.
801134	FortiClient (macOS) does not generate SSL VPN logs for uploading to FortiAnalyzer when tunnel is established.

Web Filter and plugin

Bug ID	Description
771853	Web Filter does not work as expected on macOS 12 Monterey.
807880	Web Filter proxy fails to connect socket and operation times out.
819138	*Display In-Browser Message* shows blank page and bubble notification but no message.
829164	Security risk websites violation list is not on *Web Filter* tab.
834104	On macOS 11.6 and 12 with M1 chip and on macOS 12.5 with M2 chip, FortiClient (macOS) has no network access when EMS sets `use_transparent_Proxy=1`.
835652	Web Filter has issue when all categories are blocked.
839694	Upgrade procedure installs Web Filter extension on proxy-enabled endpoints.

Endpoint management

Bug ID	Description
773440	Domain-joined macOS endpoints result in duplicate endpoint entries in EMS.

Administration

Bug ID	Description
798055	JavaScript error occurs in the main process.

Avatar and social login information

Bug ID	Description
825913	FortiClient (macOS) reports system user changes to EMS inconsistently.

Endpoint control

Bug ID	Description
777473	FortiClient Cloud is unaware of UID change when EMS sends a new UID to FortiClient (macOS).
816209	FortiClient (macOS) endpoint should be counted as on-Fabric only when all the rules are met in an on-Fabric detection rule set.
828019	Some on-net detection rules do not detect correct on/off fabric status for FortiClient (macOS).
829923	On-fabric status flip-flops when ping rule and different web filter enabled status for on-/off-fabric status.
841149	Endpoint tries to use ZTNA certificate when ZTNA option is disabled.
841737	EMS does not report endpoint VPN IP addresses to FortiOS if they are connected with IPsec VPN.

Deployment and installers

Bug ID	Description
721823	Deployment status always shows as Endpoint Notified in EMS GUI.

Endpoint security

Bug ID	Description
829258	FortiClient (macOS) loses EMS connectivity after changing EMS SSL certificate.

Malware Protection and Sandbox

Bug ID	Description
857482	FortiClient (macOS) built-in AV engine is not updated to 6.00282.

Onboarding

Bug ID	Description
833090	EMS shows wrong user account after switching device user on endpoint and registering with EMS IP address/FQDN.

Zero Trust telemetry

Bug ID	Description
754345	FortiClient does not automatically register to FortiClient Cloud after reboot when user manually disconnects FortiClient from FortiClient Cloud.

Other

Bug ID	Description
850528	FortiClient does not always get IPv4 address from https://ipify.org.

Common Vulnerabilities and Exposures

Bug ID	Description
848892	FortiClient (macOS) 7.2.0 is no longer vulnerable to the following CVE Reference: • CVE-2023-22635 Visit https://fortiguard.com/psirt for more information.

Known issues

The following issues have been identified in FortiClient (macOS) 7.2.0. 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 (ZTNA) connection rules.

Endpoint control

Bug ID	Description
821379	macOS clients do not show up in *Software Inventory* > *Hosts*.
878514	FortiClient cannot get tenant ID after EMS administrator deploys FortiClient 7.2.0 over 7.0.7 from the EMS server.
879108	EMS counts an endpoint as on-Fabric when it does not meet all rules in an on-Fabric detection rule set.

GUI

Bug ID	Description
832758	GUI shows realtime protection as off when the feature is enabled and quarantines files effectively on endpoint.
857148	GUI shows duplicate FortiClient consoles.

Remote Access

Bug ID	Description
772247	SAML authentication times out with SSL VPN.
794380	FortiClient does not work with overlapping subnet when connected to SSL VPN.
799332	FortiClient for macOS 12.3.1 cannot connect to VPN when there are two gateways listed using SAML.
800529	GUI has issue with *Settings* > *VPN Options* > *Do not Warn Invalid Server Certificate*.
801555	FortiClient has SSL VPN throughput issue.
821660	FortiClient (macOS) behaves inconsistently with LDAP user login and autoconnect.
825009	VPN with SAML displays *ErrorCode=-6005* when it reaches 31%.
826763	FortiClient (macOS) console does not show VPN username for SAML when SSL VPN tunnel establishes connection.
827685	FortiClient connects to VPN when a tag is assigned and the configuration should block access to the VPN tunnel for endoints with the tag.
833001	When using FortiAuthenticator as SAML identity provider, autoconnect fails after user logout/relogin.
835096	FortiClient (macOS) cannot establish SAML single sign on VPN after Wi-Fi drops or disconnects and user reconnects manually.
850246	User cannot enable iCloud private relay due to VPN system extension.
863431	On macOS 13, FortiClient does not use internal DNS for SSL VPN tunnel.
864632	DNS inconsistency exists for FortiClient and macOS 13 Ventura.
870198	FortiClient system keychain has issue while connecting to SSL VPN with system keychain certificate. **Workaround options**: • Move the FortiClient system keychain to the login keychain. • Right-click the private key, select *Access Control*, then +, then `Command + Shift + g`. Enter the following path: `"/Applications/FortiClient/Contents/Resources/runtime.helper/FortiTray.app"`. This disables user prompts needed when using the certificate.
874669	FortiClient does not attempt to connect with redundant SAML VPN gateway if it cannot reach first gateway.

Zero Trust tags

Bug ID	Description
793033	ZTNA LDAP group rule does not work.
794385	FortiClient detects third-party antivirus tag.

Avatar and social login infomration

Bug ID	Description
878050	Avatar does not update on FortiOS dashboards and FortiOS cannot show updated information.

Web Filter and plugin

Bug ID	Description
856060	Web Filter with proxy mode does not work on macOS 13.0 Ventura.
872607	FortiClient does not support Web Filter custom messages.

Application Firewall

Bug ID	Description
814391	When connected to FortiClient Cloud, application signatures block allowlisted applications.
834500	FortiClient fails to block Application Firewall categories when web client category is set to monitor.
834839	Web Filter does not block traffic when proxy mode and Application Firewall are disabled.

Logs

Bug ID	Description
872875	Disabling *Client-Based Logging When On-Fabric* in EMS does not work for macOS endpoints.

Installation and upgrade

Bug ID	Description
827939	*FortiTray is not open anymore* prompt shows when deploying FortiClient using script through mobile device management.

Bug ID	Description
828781	FortiClient (macOS) behaves inconsistently when uninstalling it through commands in terminal and the FortiClientUninstaller GUI tool.

FSSOMA

Bug ID	Description
854882	FortiClient (macOS) does not send EMS tenant ID to FortiAuthenticator.

Malware Protection and Sandbox

Bug ID	Description
829415	When next generation antivirus is enabled, FortiClient (macOS) shows real time protection (RTP) as disabled.
833845	FortiClient (macOS) does not submit .zip files to Cloud Sandbox if Malware Protection is enabled and .zip is under RTP exclusion list.
855570	Real-time protection scans files regardless of the maximum file size setting for scanning files.
860065	FortiClient does not report the last AV scan time.

Onboarding

Bug ID	Description
811976	FortiClient (macOS) may prioritize using user information from authentication user registered to EMS.
869657	FortiClient (macOS) 7.0.5 and 7.0.7 upgraded with EMS-created user authentication (local/LDAP/SAML) installer does not show authentication prompt after upgrade to 7.2.0.
872136	User verification period option under User verification does not work as configured.

ZTNA connection rules

Bug ID	Description
831943	FortiClient (macOS) uninstall does not remove ZTNA client certificate is not removed from user certificate store.
838075	ztagent daemon still runs after FortiClient (macOS) deregisters from EMS and ZTNA rules still work.
857999	FortiClient does not support using external browser for SAML authentication for ZTNA rules acquired through service portal.
862273	ZTNA breaks intranet connection and ZTNA destination after running a custom macOS application.
871342	ZTNA error message that shows on browser is not configurable.

www.fortinet.com