Release Notes

FortiClient (Windows) 7.2.7

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
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

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

December 12, 2024
FortiClient (Windows) 7.2.7 Release Notes
04-727-1099386-20241212

TABLE OF CONTENTS

Change log **5**
Introduction **6**
Licensing 6
Special notices **7**
SAML IdP configuration for Save Password 7
FortiGuard Web Filtering Category v10 Update 7
Nested VPN tunnels 7
Installation information **8**
Firmware images and tools 8
Upgrading from previous FortiClient versions 9
Downgrading to previous versions 9
Firmware image checksums 9
Product integration and support **10**
Language support 11
Conflict with third-party endpoint protection software 12
Intune product codes 12
Resolved issues **13**
Malware Protection and Sandbox 13
Install and upgrade 13
Logs 13
Onboarding 13
Zero Trust tags 14
Vulnerability Scan 14
Remote Access 14
Remote Access - IPsec VPN 14
Remote Access - SSL VPN 15
Deployment and installers 15
Quarantine Management 15
PAM 16
Web Filter and plugin 16
Other 16
Known issues **17**
New known issues 17
Existing known issues 17
Application Firewall 17
Avatar and social network login 17
Deployment and installers 17
Endpoint control 18
Endpoint management 18
Logs 18
Malware Protection and Sandbox 18

Remote Access 18
Remote Access - IPsec 19
Remote Access - SSL VPN 19
Vulnerability Scan 19
Web Filter and plugin 19
Zero Trust tags 20
ZTNA connection rules 20
Onboarding 20
Other 20
Numbering conventions 21

Change log

Date	Change description
2024-12-12	Initial release of 7.2.7.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 7.2.7 build 1116.

- Special notices on page 7
- Installation information on page 8
- Product integration and support on page 10
- Resolved issues on page 13
- Known issues on page 17

Review all sections prior to installing FortiClient.

FortiClient (Windows) 7.2.7 components that interact with Microsoft Security Center are signed with an Azure Code Signing certificate, which fulfills Microsoft requirements.

Licensing

See Windows, macOS, and Linux endpoint licenses.

FortiClient 7.2.7 offers a free VPN-only version that you can use for VPN-only connectivity to FortiGate devices running FortiOS 5.6 and later versions. You can download the VPN-only application from FortiClient.com.

FortiClient offers a free standalone installer for the single sign on mobility agent. This agent does not include technical support.

Special notices

SAML IdP configuration for Save Password

FortiClient provides an option to the end user to save their VPN login password with or without SAML configured. When using SAML, this feature relies on persistent sessions being configured in the identity provider (IdP), discussed as follows:

- Microsoft Entra ID
- Okta

If the IdP does not support persistent sessions, FortiClient cannot save the SAML password. The end user must provide the password to the IdP for each VPN connection attempt.

The FortiClient save password feature is commonly used along with autoconnect and always-up features.

FortiGuard Web Filtering Category v10 Update

Fortinet has updated its web filtering categories to v10, which includes two new URL categories for AI chat and cryptocurrency websites. To use the new categories, customers must upgrade their Fortinet products to one of the following versions:

- FortiManager - Fixed in 6.0.12, 6.2.9, 6.4.7, 7.0.2, 7.2.0, 7.4.0.
- FortiOS - Fixed in 7.2.8 and 7.4.1.
- FortiClient - Fixed in Windows 7.2.3, macOS 7.2.3, Linux 7.2.3.
- FortiClient EMS - Fixed in 7.2.1.
- FortiMail - Fixed in 7.0.7, 7.2.5, 7.4.1.
- FortiProxy - Fixed in 7.4.1.

Please read the following CSB for more information to caveats on the usage in FortiManager and FortiOS:
https://support.fortinet.com/Information/Bulletin.aspx

Nested VPN tunnels

FortiClient (Windows) does not support parallel independent VPN connections to different sites. However, FortiClient (Windows) may still establish VPN connection over existing third-party (for example, AT&T Client) VPN connection (nested tunnels).

Installation information

Firmware images and tools

The following files are available in the firmware image file folder:

File	Description
FortiClientTools_7.2.7.1116.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_ 7.2.7.1116_x64.zip	Fortinet single sign on (FSSO)-only installer (64-bit).
FortiClientVPNSetup_ 7.2.7.1116_x64.exe	Free VPN-only installer (64-bit).

EMS 7.2.7 includes the FortiClient (Windows) 7.2.7 standard installer and zip package containing FortiClient.msi and language transforms.

The following tools and files are available in the FortiClientTools_7.2.7.1116.zip file:

File	Description
OnlineInstaller	Installer files that install the latest FortiClient (Windows) version available.
SSLVPNcmdline	Command line SSL VPN client.
SupportUtils	Includes diagnostic, uninstallation, and reinstallation tools.
VPNAutomation	VPN automation tool.
VC_redist.x64.exe	Microsoft Visual C++ 2015 Redistributable Update (64-bit).
vc_redist.x86.exe	Microsoft Visual C++ 2015 Redistributable Update (86-bit).
CertificateTestx64.exe	Test certificate (64-bit).
CertificateTestx86.exe	Test certificate (86-bit).
FCRemove.exe	Remove FortiClient if unable to uninstall FortiClient (Windows) via Control Panel properly.
FCUnregister.exe	Deregister FortiClient (Windows).
FortiClient_Diagnostic_tool.exe	Collect FortiClient diagnostic result.
ReinstallINIC.exe	Remove FortiClient SSLVPN and IPsec network adpater, if not uninstall it via control pannel.
RemoveFCTID.exe	Remove FortiClient UUID.

The following files are available on FortiClient.com:

File	Description
FortiClientSetup_7.2.7.1116_x64.zip	Standard installer package for Windows (64-bit).
FortiClientVPNSetup_7.2.7.1116_x64.exe	Free VPN-only installer (64-bit).

Review the following sections prior to installing FortiClient version 7.2.7: Introduction on page 6 and Product integration and support on page 10.

Upgrading from previous FortiClient versions

To upgrade a previous FortiClient version to FortiClient 7.2.7, do one of the following:

- Deploy FortiClient 7.2.7 as an upgrade from EMS. See Recommended upgrade path.
- Manually uninstall existing FortiClient version from the device, then install FortiClient (Windows) 7.2.7.

FortiClient (Windows) 7.2.7 features are only enabled when connected to EMS 7.2.

See the *FortiClient and FortiClient EMS Upgrade Paths* for information on upgrade paths.

You must be running EMS 7.2 before upgrading FortiClient.

Downgrading to previous versions

FortiClient (Windows) 7.2.7 does not support downgrading to previous FortiClient (Windows) versions.

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 *Download* > *Firmware Image Checksum*, enter the image file name, including the extension, and select *Get Checksum Code*.

Product integration and support

The following table lists version 7.2.7 product integration and support information:

Desktop operating systems	• Microsoft Windows 11 (64-bit) • Microsoft Windows 10 (64-bit)
Server operating systems	• Microsoft Windows Server 2022 • Microsoft Windows Server 2019 FortiClient 7.2.7 does not support Windows Server Core. For Microsoft Windows Server, FortiClient (Windows) supports the Vulnerability Scan, SSL VPN, Web Filter, and antivirus (AV) features, including obtaining a Sandbox signature package for AV scanning. To use SSL VPN on a Windows Server machine, you must enable your browser to accept cookies. Otherwise, tunnel connection fails. Microsoft Windows Server 2019 supports zero trust network access (ZTNA) with FortiClient (Windows) 7.2.7. As FortiClient does not support Application Firewall on a Windows Server machine, do not install the Application Firewall module on a Windows Server machine. Doing so may cause performance issues.
Minimum system requirements	• Microsoft Windows-compatible computer with Intel processor or equivalent. FortiClient (Windows) does not support ARM-based processors. • Compatible operating system and minimum 2 GB RAM • 1 GB free hard disk space • Native Microsoft TCP/IP communication protocol • Native Microsoft PPP dialer for dialup connections • Ethernet network interface controller (NIC) for network connections • Wireless adapter for wireless network connections • Adobe Acrobat Reader for viewing FortiClient documentation • Windows Installer MSI installer 3.0 or later
AV engine	• 6.00299
VCM engine	• 2.0040
FortiAnalyzer	• 7.4.0 and later • 7.2.0 and later • 7.0.0 and later
FortiAuthenticator	• 6.5.0 and later • 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
FortiClient EMS	• 7.4.0 and later • 7.2.0 and later

FortiManager	• 7.4.0 and later • 7.2.0 and later • 7.0.0 and later
FortiMonitor agent	24.3.3
FortiOS	The following FortiOS versions support ZTNA with FortiClient (Windows) 7.2.7. This includes both ZTNA access proxy and ZTNA tags: • 7.4.0 and later • 7.2.0 and later • 7.0.6 and later The following FortiOS versions support IPsec and SSL VPN with FortiClient (Windows) 7.2.7: • 7.4.0 and later • 7.2.0 and later • 7.0.0 and later • 6.4.0 and later
FortiSandbox	• 4.4.0 and later • 4.2.0 and later • 4.0.0 and later • 3.2.0 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.

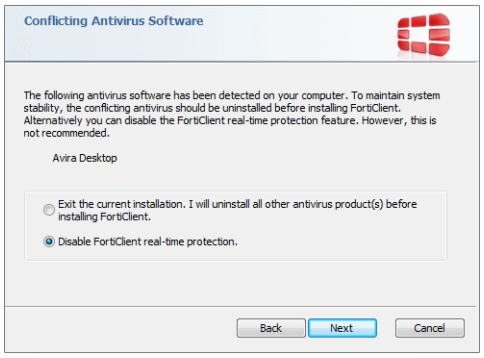
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

Conflict with third-party endpoint protection software

As a Fortinet Fabric Agent that provides protection, compliance, and secure access, FortiClient may conflict with anti-malware products on the market that provide similar AV, web filtering, application firewall, and ransomware protection features as FortiClient. If you encounter a conflict, there are a few steps you can take to address it:

- Do not use other AV products when FortiClient's AV feature is enabled.
- If FortiClient's AV feature is disabled, configure the third party AV product to exclude the FortiClient installation folder from being scanned.

During a new FortiClient installation, the installer searches for other registered third party software and, if it finds any, warns users to uninstall them before proceeding with the installation. There is also an option to disable FortiClient real time protection.



Intune product codes

Deploying FortiClient with Intune requires a product code. The product codes for FortiClient 7.2.7 are as follows:

Version	Product code
Enterprise	8699D5AB-E232-4261-8120-1C6B528DFF11
VPN-only agent	3087498C-B979-48FD-91D1-9EABB6979F67
Private access management-only agent	C81E506E-A586-4632-B280-5B3D76DCFA5F
Single sign on-only agent	B3CADF55-5182-41CE-A40B-1279695B0A99

See Configuring the FortiClient application in Intune.

Resolved issues

The following issues have been fixed in version 7.2.7. For inquiries about a particular bug, contact Customer Service & Support.

Malware Protection and Sandbox

Bug ID	Description
1083058	Antiexploit cannot detect and block exploits.

Install and upgrade

Bug ID	Description
1003200	Silent and version-independent uninstall using CLI has issue.
1080006	FortiClient (Windows) exe installer does not properly handle `v` or `msicl` command line parameters.

Logs

Bug ID	Description
1034892	EMS cannot download diag_logs for FortiClient (Windows) from EMS.

Onboarding

Bug ID	Description
1081547	Authentication dialog is blank when using invitation code with local or LDAP authentication to connect to EMS.

Zero Trust tags

Bug ID	Description
1027851	FortiClient (Windows) sometimes loses Zero Trust tag based on combined rules, with the only way to fix the issue being reinstalling FortiClient.

Vulnerability Scan

Bug ID	Description
1054778	FortiClient displays incorrect detected version on Vulnerability scan report GUI.
1092036	Logs for the detected vulnerability show only UUID code as the detected path instead of the application's actual path.

Remote Access

Bug ID	Description
1027199	FortiClient (Windows) does not log in to system when using SAML VPN before logon.
1065837	In FortiTray, *Network Lockdown* is not translated and is inconsistent with macOS.
1066263	Free VPN-only client does not minimize after it establishes a tunnel that has `<minimize_window_on_connect>` enabled.
1090354	When using VPN before logon, *Use Windows credentials for VPN* is always selected even when `<use_windows_credentials>` is disabled.

Remote Access - IPsec VPN

Bug ID	Description
714023	Dialup IPsec VPN does not come up and shows NAT-T inconsistency.
993280	FortiGate does not answer on the right port during P2 initiation of dialup VPN with NAT-T.
1078571	When autoconnect is enabled and FortiClient (Windows) cannot reach VPN gateway, VPN connection is stuck in a loop.
1079047	When using Windows 11 with Intel WiFi 7 BE200 Wi-Fi network adapter, FortiClient (Windows) cannot connect to IPsec VPN.

Bug ID	Description
1079599	Disconnecting from IPsec VPN with *Save Username* enabled turns \ in username to \\.
1081489	With multifactor authentication enabled, FortiClient cannot save credentials when connecting to IPsec VPN via system tray icon.
1091700	High volume of LDAP traffic occurs when endpoint connected to tunnel.

Remote Access - SSL VPN

Bug ID	Description
1040725	VPN before logon cannot connect after sleep until two or three attempts and first attempt always fails.
1052659	FortiClient (Windows) gets stuck at 98% and cannot reconnect when endpoint is left in standby or sleep for a couple of hours until reboot.
1078689	Internal browser shows script error when connecting to SSL VPN with Okta as SAML identity provider.
1081068	SSL VPN does not connect on Windows Server 2019.
1083352	FortiClient does not wait for the on-fabric status check before autoconnect tunnel starts when waking up from sleep.

Deployment and installers

Bug ID	Description
1083623	FortiClient shows reboot prompt in a loop after upgrade.

Quarantine Management

Bug ID	Description
1006062	FortiClient (Windows) cannot restore files for network share.

PAM

Bug ID	Description
1099622	FortiPAM fails to automatically fill password for proxy mode enabled secret when FortiClient (Windows) fails to add FortiPAM zero trust network access rules in time.
1101380	*This site can't be reached* error occurs on first attempt through web launcher in FortiPAM.

Web Filter and plugin

Bug ID	Description
1083774	Web Filter may block all sites for up to five minutes when rating error occurs.
1069196	Web Filter does not block access to unauthorized site with Web Filter enabled.

Other

Bug ID	Description
984763	NETIO.SYS/FortiWF2.sys causes blue screens of death on Windows 10.

Known issues

Known issues are organized into the following categories:

- New known issues on page 17
- Existing known issues on page 17

To inquire about a particular bug or to report a bug, contact Customer Service & Support.

New known issues

No new issues have been identified in version 7.2.7.

Existing known issues

The following issues have been identified in a previous version of FortiClient (Windows) and remain in FortiClient (Windows) 7.2.7.

Application Firewall

Bug ID	Description
1069197	Application Firewall does not block peer-to-peer torrent traffic.

Avatar and social network login

Bug ID	Description
1106444	User identity information popup does not allow entering username, email address, and phone number.

Deployment and installers

Bug ID	Description
1104334	Deployment message displays in English when PC local language is not set to English.

Endpoint control

Bug ID	Description
1012497	FortiClient does not send empty `USER/USER_SID` to EMS when domain/Azure users log out.
1086370	Unverified FortiClient does not prompt for verification after upgrade with user verification invite being part of the installer.

Endpoint management

Bug ID	Description
1100822	FortiClient (Windows) reports same user twice in EMS.

Logs

Bug ID	Description
1103313	FortiAnalyzer is missing some Web Filter log entries.

Malware Protection and Sandbox

Bug ID	Description
1039172	Non-manual files sent for scanning to on-premise Sandbox do not show advanced threat protection scan popup.
1103310	German message on reboot prompt does not show completely.
1108242	On-demand scan fails to quarantine Eicar files from C drive root folders.

Remote Access

Bug ID	Description
999139	Laptop Wi-Fi DNS setting gets stuck in unknown DNS server after FortiClient (Windows) connects to and disconnects from VPN.

Remote Access - IPsec

Bug ID	Description
971554	FortiClient (Windows) sends access request for IPsec VPN when password renewal is canceled.
1070788	IPsec VPN disconnects immediately after tunnel is up when working remotely using Wi-Fi.

Remote Access - SSL VPN

Bug ID	Description
909244	SSL VPN split DNS name resolution stops working.
909755	SSL VPN split tunnel does not work for Microsoft Teams.
950787	Domain filter cannot block access specific server FQDN.
994884	SSL VPN connections get stuck on 40%.
997131	FortiClient (Windows) continuously attempts connection and retains outdated saved password despite autoconnect failure for SSL VPN.
1091993	With *Disable Connect/Disconnect* on, FortiClient (Windows) loses saved VPN user credentials when waking from sleep.

Vulnerability Scan

Bug ID	Description
1077070	FortiClient (Windows) does not report Windows OS vulnerabilities or security patches.

Web Filter and plugin

Bug ID	Description
1061163	Web Filter plugin blocks some websites after file download.
1084513	Windows 10 users cannot access internal and external websites due to Web Filter rating lookup errors.
1090048	Web Filter plugin blocks embedded Google Maps.
1092975	Web Filter blocks Amazon Web Services S3 browser.
1101902	Letsignit application cannot authenticate while connected to EMS telemetry.
1103205	FortiClient blocks some websites due to Web Filter category being unknown.
1106128	FortiClient cannot block or warn unauthorized websites when Web Filter extension is disabled.

Zero Trust tags

Bug ID	Description
1101903	Zero Trust tag for Windows automatic update check does not work.
1103074	If Zero Trust tag Tag_C is configured as applying to endpoints that are tagged with Tag_A and Tag_B, endpoint that is tagged with Tag_A and Tag_B is missing Tag_C.
1104084	*OS system last update is within 60 days* tag does not work as expected.

ZTNA connection rules

Bug ID	Description
965630	Windows 11 with FortiClient installed fails to register DNS via secure DDNS.

Onboarding

Bug ID	Description
1104465	FortiClient (Windows) cannot connect to telemetry through SAML authentication due to authorization failing on EMS.

Other

Bug ID	Description
1082299	UID has duplicate entries when deployed on VMware or Citrix.

Numbering conventions

Fortinet uses the following version number format:

<First number>.<Second number>.<Third number>.<Fourth number>

Example: 7.2.7.15

- First number = major version
- Second number = minor version
- Third number = maintenance version
- Fourth number = build version

Release Notes pertain to a certain version of the product. Release Notes are revised as needed.

www.fortinet.com

Copyright© 2024 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 Chief Legal Officer, 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.