Release Notes

FortiClient (Windows) 7.2.12

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

September 29, 2025
FortiClient (Windows) 7.2.12 Release Notes
04-7212-1200010-20250929

TABLE OF CONTENTS

Change log

Date	Change description
2025-09-29	Initial release of 7.2.12.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 7.2.12 build 1269.

Review all sections prior to installing FortiClient.

FortiClient (Windows) 7.2.12 components that interact with Microsoft Security Center are signed with an Azure Code Signing certificate, which fulfills Microsoft requirements.

Fortinet uses the following version number format:

<Major version number>.<minor version number>.<patch number>.<build number>

Example: 7.2.12.1269

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

Licensing

See Windows, macOS, and Linux endpoint licenses.

FortiClient 7.2.12 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

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 does not support parallel independent VPN connections to different sites. However, FortiClient 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_7.2.12.1269.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_7.2.12.1269_x64.zip	Fortinet single sign on (FSSO)-only installer (64-bit).
FortiClientVPNSetup_7.2.12.1269_x64.exe	Free VPN-only installer (64-bit).

EMS 7.2.12 includes the FortiClient (Windows) 7.2.12 standard installer and zip package containing FortiClient.msi and language transforms.

The following tools and files are available in the FortiClientTools_7.2.12.1269.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_7.2.12.1269_x64.zip	Standard installer package for Windows (64-bit).
FortiClientVPNSetup_7.2.12.1269_x64.exe	Free VPN-only installer (64-bit).

Review the following sections prior to installing FortiClient version 7.2.12: Introduction on page 5 and Product integration and support on page 9.

Upgrading from previous FortiClient versions

To upgrade a previous FortiClient version to FortiClient 7.2.12, do one of the following:

- Deploy FortiClient 7.2.12 as an upgrade from EMS. See Recommended upgrade path.
- Manually uninstall existing FortiClient version from the device, then install FortiClient (Windows) 7.2.12.

FortiClient (Windows) 7.2.12 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) 7.2.12 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 7.2.12 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 7.2.12 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) 7.2.12. 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	• 6.00301
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) 7.2.12. 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) 7.2.12: • 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.

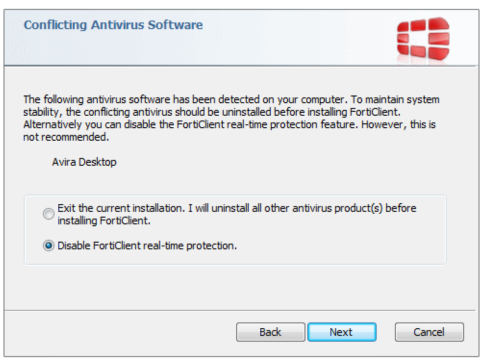
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

Conflict with third-party endpoint protection software

As a Fortinet Fabric Agent that provides protection, compliance, and secure access, FortiClient may conflict with antimalware 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 7.2.12 are as follows:

Version	Product code
Enterprise	B34BA2F5-7F43-481E-90A7-B343A70F2947
VPN-only agent	CEAB81B8-1682-456F-A385-9FDA68C6361D

Version	Product code
Private access management-only agent	E6A3800D-EB2E-4CF1-938F-D25DB72B92FA
Single sign on-only agent	BC5AE9F7-1BE3-4C2B-9BA9-D141F31C6DE2

See Configuring the FortiClient application in Intune.

Resolved issues

The following issues have been fixed in version 7.2.12. For inquiries about a particular bug, contact Customer Service & Support.

Endpoint control

Bug ID	Description
1160546	FortiClient (Windows) cannot detect DHCP server for on-Fabric rule when server is reachable.

Remote Access - IPsec VPN

Bug ID	Description
1160309	Unable to send DHCP requests while connected to IPsec VPN.
1189946	SAML authentication error with *Network Lockdown* enabled.

Remote Access - SSL VPN

Bug ID	Description
1144236	BSODs while loading the webpage business.apple.com while connected to the FortiSASE SSL VPN.
1162957	AutoConnect fails when "AutoConnect only when Off-fabric" is enabled at the Fabric State determination stage.
1166065	Blank SAML screen while connecting to the VPN on user logon.
1179323	Killing the `fortitray.exe` process disconnects the VPN even if VPN is configured as always-on.
1181998	BSOD occurs when connecting to FortiSASE via VPN on FortiClient.

Zero trust network access (ZTNA) connection rules

Bug ID	Description
1094370	FortiClient ZTNA redundant gateway failure.
1170309	Unable to send DHCP requests while connected to IPsec VPN.

Known issues

Known issues are organized into the following categories:

- New known issues on page 15
- Existing known issues on page 15

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 7.2.12.

Existing known issues

The following issues have been identified in a previous version of FortiClient (Windows) and remain in FortiClient (Windows) 7.2.12.

Avatar and social network login

Bug ID	Description
777013	Avatar image change or existing does not show on FortiAnalyzer.

Malware Protection and Sandbox

Bug ID	Description
1103310	Message in German on reboot prompt does not show completely.

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
946059	With VPN up, after signing out from the OS, tunnel disconnects whether <disconnect_on_log_off> is enabled or disabled.

Remote Access - SSL VPN

Bug ID	Description
994884	SSL VPN connections get stuck on 40%.
1091993	With *Disable Connect/Disconnect* on, FortiClient (Windows) loses saved VPN user credentials when waking from sleep.
1160975	SSL VPN does not respect FortiToken authentication timeout if user was canceling or disconnecting from prior connection.

Zero Trust tags

Bug ID	Description
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.

ZTNA connection rules

Bug ID	Description
1114766	Zero trust network access (ZTNA) bypasses all TCP traffic from FortiESNAC process.
1155036	ZTNA TCP forwarding SAML session starts redirect with TCP forwarding path.

www.fortinet.com

Copyright© 2025 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.