FORTINET

Release Notes

FortiClient (Windows) 7.2.6

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

November 26, 2024
FortiClient (Windows) 7.2.6 Release Notes
04-726-1095443-20241126

TABLE OF CONTENTS

Change log

Date	Change description
2024-11-25	Initial release of 7.2.6.
2024-11-26	Updated Intune product codes on page 12.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 7.2.6 build 1076.

Review all sections prior to installing FortiClient.

FortiClient (Windows) 7.2.6 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 7.2.6 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_7.2.6.1076.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_ 7.2.6.1076_x64.zip	Fortinet single sign on (FSSO)-only installer (64-bit).
FortiClientVPNSetup_ 7.2.6.1076_x64.exe	Free VPN-only installer (64-bit).

EMS 7.2.6 includes the FortiClient (Windows) 7.2.6 standard installer and zip package containing FortiClient.msi and language transforms.

The following tools and files are available in the FortiClientTools_7.2.6.1076.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_7.2.6.1076_x64.zip	Standard installer package for Windows (64-bit).
FortiClientVPNSetup_7.2.6.1076_x64.exe	Free VPN-only installer (64-bit).

Review the following sections prior to installing FortiClient version 7.2.6: 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 7.2.6, do one of the following:

- Deploy FortiClient 7.2.6 as an upgrade from EMS. See Recommended upgrade path.
- Manually uninstall existing FortiClient version from the device, then install FortiClient (Windows) 7.2.6.

FortiClient (Windows) 7.2.6 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) 7.2.6 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 7.2.6 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 7.2.6 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) 7.2.6. 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	• 7.2.0 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) 7.2.6. 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) 7.2.6: • 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.

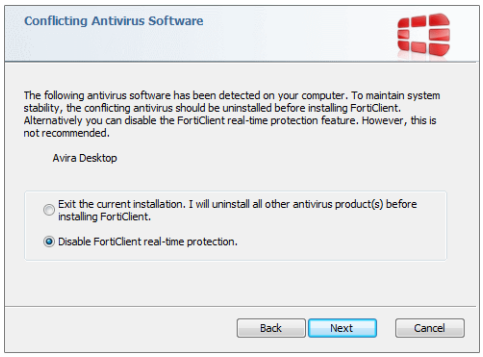
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

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 7.2.6 are as follows:

Version	Product code
Enterprise	EA653D27-8CFF-4242-A378-6859D9E156CA
VPN-only agent	93BAF658-B4AC-4063-83AB-33A3F95C62D0
Private access management-only agent	7CE2BFAC-6430-43B8-AA25-BB75AEBE8A0F
Single sign on-only agent	79F3E2A6-DF5C-48E2-A4B6-9816F3C0068D

See Configuring the FortiClient application in Intune.

Resolved issues

The following issues have been fixed in version 7.2.6. For inquiries about a particular bug, contact Customer Service & Support.

Endpoint control

Bug ID	Description
975704	FortiClient does not report most recent completed scan timestamp due to incorrect last scan time showing on EMS dashboard.
1035687	Action for EMS invalid certificates Warn, then Deny does not work as expected.

Avatar and social login information

Bug ID	Description
1075028	Avatar does not display.

Malware Protection and Sandbox

Bug ID	Description
1060437	FortiClient Cloud Sandbox does not scan downloaded files from Outlook.

Logs

Bug ID	Description
1027844	Unified threat management and system event logs do not appear in FortiAnalyzer.

Remote Access

Bug ID	Description
1010271	When VPN connection name has more than ten Japanese characters, VPN connection fails.
1052284	Per-machine prelogon tunnel does not work by per-user autoconnect configuration.
1060034	VPN before logon uses incorrect tunnel list order.
1065837	In FortiTray, network lockdown terminology is not translated and language needs to be more consistent with macOS.
1066263	Free VPN-only client does not minimize after tunnel established though `<minimize_window_on_connect>=1`.
1090354	VPN before logon always has *Use Windows credentials for VPN* selected even when `<use_windows_credentials>` is disabled.

Remote Access - IPsec VPN

Bug ID	Description
1060130	With redundant gateway list, disclaimer message appears for every time that FortiClient (Windows) attempts to connect to an entry in the gateway list.
1061455	FortiClient (Windows) does not support network ID to differentiate multiple IKEv2 certificate-based phase 1 tunnels.
1078571	When autoconnect is enabled and FortiClient (Windows) cannot reach VPN gateway, it is stuck in a loop.
1079047	FortiClient (Windows) on Windows 11 with Intel WiFi 7 BE200 Wi-Fi network adapter cannot connect to IPsec VPN.
1079575	FortiClient (Windows) uses port 500 for IPsec VPN when `<sase_mode>` is enabled on standard FortiSASE instances and cannot connect.
1081489	With multifactor authentication enabled, FortiClient cannot save credentials when connecting to IPsec VPN via system tray icon.

Remote Access - SSL VPN

Bug ID	Description
920383	FortiClient enables *Turn off smart multi-homed name resolution* on the machine after successful connection.

Bug ID	Description
1007613	`sslvpn-ems-sn-check` error is not descriptive on SAML SSL VPN connections.
1011690	SamlGetResponseUsingWebBrowser cannot start SamlAuthWB.exe.
1040725	VPN before logon cannot connect after sleep until two or three attempts and first attempt always fails.
1063513	Host check error (-7006) occurs after login if *Realtime Antivirus* or *both* is enabled for hostcheck in SSL VPN portal.
1071790	VPN before logon fails with OS host check.
1081068	SSL VPN does not connect on Windows Server 2019.

Zero Trust telemetry

Bug ID	Description
1077673	FortiClient does not connect with FortiClient Cloud due to authentication error.

Deployment and installers

Bug ID	Description
1039041	User cannot open FortiClient after getting a scheduled deployment task.
1076809	Updating from 7.2.4 to 7.2.5 disables FortiESNAC on the Microsoft register key.
1083623	FortiClient shows reboot prompt in a loop after upgrade.

Onboarding

Bug ID	Description
1018839	FortiClient fails to open automatically upon clicking SAML notification.

PAM

Bug ID	Description
797048	Uploaded recorded video shows only part of application window.

Web Filter and plugin

Bug ID	Description
1043986	Web Filter blocks the URL data:application/vnd and you cannot configure an exclusion for it.
1075358	Web Filter extension blocks some websites that have links to different categories.
1083774	Web Filter may block all sites for up to five minutes when rating error occurs.

Other

Bug ID	Description
984763	NETIO.SYS/FortiWF2.sys causes blue screens of death (BSOD) on Windows 10.
1081675	FortiAptFilter.sys causes BSOD when FortiClient upgraded to 7.2.5.

Known issues

Known issues are organized into the following categories:

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

New known issues

The following issues have been identified in version 7.2.6.

Deployment and installers

Bug ID	Description
1075698	FortiClient does not show *FortiClient software upgrade is available* when upgrade deployment is pushed to endpoint.

Install and upgrade

Bug ID	Description
1099284	FortiClient becomes unlicensed after upgrading to 7.2.5.

Malware Protection and Sandbox

Bug ID	Description
1083058	Antiexploit cannot detect and block exploits.

Remote Access

Bug ID	Description
1027199	FortiClient (Windows) does not log in into system when SAML VPN before logon is used.

Remote Access - SSL VPN

Bug ID	Description
997131	FortiClient (Windows) keeps attempting and retaining outdated saved password despite autoconnect failure in SSL VPN.

Web Filter and plugin

Bug ID	Description
1061163	Web Filter plugin blocks some websites after a file download.
1092975	Web Filter blocks Amazon Web Services S3 browser.
1094009	FortiClient (Windows) does not disable Web Filter when switching to on-Fabric state.
1094865	Session becomes unresponsive after downloading the attachment when accessing the internal website.
1097357	Web Filter cannot block https://chromewebstore.google.com in Edge and Chrome.

Existing known issues

The following issues have been identified in a previous version of FortiClient (Windows) and remain in FortiClient (Windows) 7.2.6.

Application Firewall

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

Configuration

Bug ID	Description
1087936	Disconnecting with password with some special characters does not work.
1089575	On Windows 11 24H2, DNS for Ethernet adapter is removed when FortiClient is installed and connected to EMS.

Endpoint control

Bug ID	Description
1012497	FortiClient does not send empty `USER/USER_SID` to EMS when domain/Azure users log out.
1084906	DHCP server on-fabric detection rule does not work with IPsec VPN tunnel on Windows 11.
1086370	Unverified FortiClient does not prompt for verification after upgrade with user verification invite being part of the installer.

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.

Performance

Bug ID	Description
1086957	Network access control (FortiEsNac daemon) causes high CPU on Windows Server 2019.

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.
993280	FortiGate does not answer on the right port during P2 initiation of dialup VPN with NAT-T.
1003308	FortiClient (Windows) attempts to autoconnect Azure autoconnect tunnels when the logged in user is not an Azure user.
1079599	IPsec VPN with *Save Username* makes double slash after disconnection.

Remote Access - SSL VPN

Bug ID	Description
874759	SSL VPN has DNS issues if AWS Route53 is configured for name resolution.
884926	Okta SAML token window popup displays in low resolution.
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.
989864	When network lockdown is enabled in Remote Access profile, signing in to Windows takes longer than usual.
994884	SSL VPN connections get stuck on 40%.
1002294	FortiClient does not reconnect to the VPN until restarted.
1083352	FortiClient does not wait for the On-fabric status check before autoconnect tunnel starts when waking up from sleep.

Vulnerability Scan

Bug ID	Description
1077070	FortiClient (Windows) does not report Windows OS vulnerabilities or security patches.
1092036	Logs for the detected vulnerability shows only UUID code as the detectedpath, instead the application's actual path.

Web Filter and plugin

Bug ID	Description
1083327	Web Filter extension anomaly occurs in Chrome and Edge when downloading PDF.
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.

ZTNA connection rules

Bug ID	Description
839589	ZTNA TCP forwarding not working for GoAnywhere application.

Bug ID	Description
949999	SAML authentication does not work with Azure AD certificate-based authentication.
952888	IPv6 DNS servers bypass inline CASB IPv4 access proxies.
965476	User cannot access website with certificate warning and Forticlient DNS Root certificate signs the certificate.
965630	Windows 11 with FortiClient installed fails to register DNS via secure DDNS.
967199	*No ZTNA client certificate was provided* error occurs when trying to access HTTPS page.
977407	ZTNA TCP forwarding with authentication does not work properly for SaaS and SaaS group applications.
1032986	ZTNA destination-based SMB drive access fails to load for the first time when authentication is enabled.

Numbering conventions

Fortinet uses the following version number format:

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

Example: 7.2.6.15

- 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