FortiClient (Windows) - Release Notes

Version 6.4.8

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

March 30, 2022
FortiClient (Windows) 6.4.8 Release Notes
04-648-789529-20220330

TABLE OF CONTENTS

Change log

Date	Change Description
2022-03-30	Initial release of 6.4.8.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 6.4.8 build 1755.

Review all sections prior to installing FortiClient.

Licensing

FortiClient 6.2.0+, FortiClient EMS 6.2.0+, and FortiOS 6.2.0+ introduced a new licensing structure for managing endpoints running FortiClient 6.2.0+. See Upgrading from previous FortiClient versions on page 9 for more information on how the licensing changes upon upgrade to 6.2.0+. Fortinet no longer offers a free trial license for ten connected FortiClient endpoints on any FortiGate model running FortiOS 6.2.0+. EMS 6.4 supports a trial license. With the EMS free trial license, you can provision and manage FortiClient on ten Windows, macOS, and Linux endpoints and ten Chromebook endpoints indefinitely.

FortiClient 6.4.8 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. You cannot use the VPN-only client with the FortiClient Single Sign On Mobility Agent (SSOMA). To use VPN and SSOMA together, you must purchase an EMS license.

Special notices

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).

SSL VPN connectivity issues

Latency or poor network connectivity can affect the FortiClient SSL VPN connection. To further help avoid timeouts, increase the login timeout on the FortiGate to 180 seconds using the following CLI command:

```
config vpn ssl settings
   set login-timeout 180
end
```

Microsoft Windows server support

FortiClient (Windows) supports the following features for Microsoft Windows servers:

- Antivirus
- Vulnerability scan
- Web Filter
- SSL VPN

HP Velocity and Application Firewall

When using an HP computer, a conflict between the HP Velocity application and FortiClient Application Firewall can cause a blue screen of death or network issues. If not using HP Velocity, consider uninstalling it.

Split tunnel

In EMS 6.4.1, application-based split tunneling was configured globally and applied to all IPsec or SSL VPN tunnels. In EMS 6.4.2 and later versions, the application-based split tunneling feature was changed to be configured on a per-tunnel basis. Therefore, a global application-based split tunnel configuration made in EMS 6.4.1 no longer functions after

upgrading to 6.4.8. You must complete the per-tunnel configuration after upgrade. See Configuring a profile with application-based split tunnel.

This is unrelated to the FortiOS split tunnel feature.

Installation information

Firmware images and tools

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

File	Description
FortiClientTools_6.4.8.xxxx.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_ 6.4.8.xxxx.zip	FSSO-only installer (32-bit).
FortiClientSSOSetup_ 6.4.8.xxxx_x64.zip	FSSO-only installer (64-bit).
FortiClientVPNSetup_ 6.4.8.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_ 6.4.8.xxxx_x64.exe	Free VPN-only installer (64-bit).

EMS 6.4 includes the FortiClient (Windows) 6.4.8 standard installer and zip package containing FortiClient.msi and language transforms.

The following tools and files are available in the FortiClientTools_6.4.xx.xxxx.zip file:

File	Description
FortiClientVirusCleaner	Virus cleaner.
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).

The following files are available on FortiClient.com:

File	Description
FortiClientSetup_6.4.8.xxxx.zip	Standard installer package for Windows (32-bit).
FortiClientSetup_6.4.8.xxxx_ x64.zip	Standard installer package for Windows (64-bit).

File	Description
FortiClientVPNSetup_ 6.4.8.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_ 6.4.8.xxxx_x64.exe	Free VPN-only installer (64-bit).

Review the following sections prior to installing FortiClient version 6.4.8: Introduction on page 5, Special notices on page 6, and Product integration and support on page 10.

Upgrading from previous FortiClient versions

You must upgrade EMS to one of the following versions before upgrading FortiClient:

- 6.4.7 or later
- 7.0.2 or later

To upgrade a previous FortiClient version to FortiClient 6.4.8, do one of the following:

- Deploy FortiClient 6.4.8 as an upgrade from EMS. With the new endpoint security improvement feature, there are backward compatibility issues to consider while planning upgrades. See Recommended upgrade path.
- Manually uninstall existing FortiClient version from the device, then install FortiClient (Windows) 6.4.8

FortiClient (Windows) 6.4.8 features are only enabled when connected to EMS.

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

Downgrading to previous versions

FortiClient (Windows) 6.4.8 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 Checksums*, enter the image file name, including the extension, and select *Get Checksum Code*.

Product integration and support

The following table lists version 6.4.8 product integration and support information:

Desktop operating systems	• Microsoft Windows 11 (64-bit) • Microsoft Windows 10 (32-bit and 64-bit) • Microsoft Windows 8.1 (32-bit and 64-bit) • Microsoft Windows 7 (32-bit and 64-bit) FortiClient 6.4.8 does not support Microsoft Windows XP and Microsoft Windows Vista.
Server operating systems	• Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 FortiClient 6.4.8 does not support Windows Server Core. For Microsoft Windows Server, FortiClient (Windows) supports the Vulnerability Scan, SSL VPN, Web Filter, and 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.
Embedded system operating systems	Microsoft Windows 10 IoT Enterprise LTSC 2019
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 512 MB RAM • 600 MB 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	• 6.00258
FortiAnalyzer	• 7.0.0 and later • 6.4.0 and later
FortiAuthenticator	• 6.3.0 and later • 6.2.0 and later • 6.1.0 and later • 6.0.0 and later
FortiClient EMS	• 7.0.2 and later

	• 6.4.7 and later
FortiManager	• 6.4.0 and later
FortiOS	The following FortiOS versions support IPsec and SSL VPN with FortiClient (Windows) 6.4.8: • 7.0.0 and later • 6.4.0 and later • 6.2.0 and later • 6.0.0 and later The following FortiOS versions support endpoint control with FortiClient (Windows) 6.4.8: • 6.2.0 and later
FortiSandbox	• 4.0.0 and later • 3.2.0 and later • 3.1.0 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.

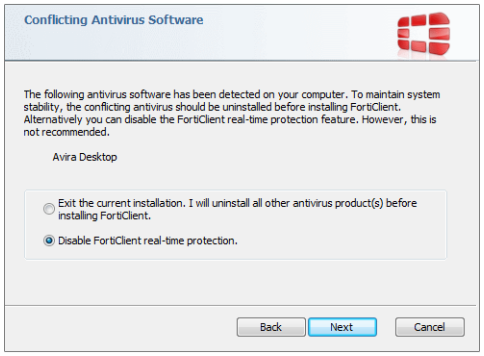
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

Conflicts with third party AV products

The AV feature in FortiClient is known to conflict with other similar products in the market.

- You should not use FortiClient's AV feature with other AV products.
- If not using FortiClient's AV feature, you should exclude the FortiClient installation folder from scanning for the third party AV product.

During a new installation of FortiClient, the installer searches for other registered third party software and, if any is found, warns users to uninstall them before proceeding with the installation. There is also an option to disable FortiClient Real Time Protection (RTP).



Intune product code

Deploying FortiClient with Intune requires a product code. The product code for full-featured FortiClient 6.4.8 is {8C034DB4-951F-4CB3-96E7-251D637F3711}. The product code for the FortiClient 6.4.8 VPN-only agent is {46C4C462-49F3-4A4F-AC87-016D0C4DF672}.

See Configuring the FortiClient application in Intune.

Resolved issues

The following issues have been fixed in version 6.4.8. For inquiries about a particular bug, contact Customer Service & Support.

Install and deployment

Bug ID	Description
716597	FortiClient installation using `norestart` parameter requests reboot.

Endpoint control

Bug ID	Description
751728	FortiClient (Windows) does not automatically connect to EMS after manual FortiClient (Windows) upgrade.
770816	FortiESNAC process consumes a lot of CPU when a particular zero trust network access policy is configured on EMS.
792659	FortiClient (Windows) loses connection to EMS after upgrade.

Application Firewall

Bug ID	Description
749797	Application Firewall decreases network bandwidth while transferring files.

Malware Protection and Sandbox

Bug ID	Description
709729	Realtime_scan log disappears after ten seconds.
759271	FortiClient fails to quarantine a read-only file.

Remote Access

Bug ID	Description
716323	FortiClient (Windows) cannot connect to IPsec VPN and the GUI does not respond.
716952	On connect script for Windows does not execute all the time.
731011	FortiClient (Windows) is stuck at 98% connecting to SSL VPN tunnel when integrated with SAML Azure Active Directory authentication.
731912	FortiClient does not register any interface's IP addresses to the DNS server when IPSec VPN tunnel is up.
740410	FortiClient (Windows) applies `client-cert` to unmatched mapping of SSL VPN.
744945	VPN before logon cannot connect before Windows logon, so the group policy object cannot commit before logon.
745002	FortiClient becomes unusable if it cannot reach EMS after upgrade.
774521	GUI goes blank when using a regular expression type certificate filter for VPN.
785853	SAML SSL VPN tunnel gets stuck at authentication step with some identity providers.
787548	FortiClient (Windows) does not have an option to force DNS queries to private DNS when SSL VPN is connected.

Web Filter and plugin

Bug ID	Description
729753	FortiClient sends Web Filter traffic to FortiGuard server continuously.

Zero Trust Telemetry

Bug ID	Description
765348	Invalid certificate detected after FortiClient upgrade.

Other

Bug ID	Description
772310	FortiTray shutdown from Command Prompt does not work.

Known issues

The following issues have been identified in FortiClient (Windows) 6.4.8. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Install and upgrade

Bug ID	Description
726616	FortiClient 6.4.3 cannot upgrade to 6.4.4.
749331	Windows Security settings show that FortiClient is snoozed when FortiEDR is installed.
773219	FortiClient (Windows) should not allow the user to uninstall it if settings are locked.

Application Firewall

Bug ID	Description
663024	Application Firewall does not include VMware Horizon VDI Agent signature.
776007	Application Firewall conflicts with Windows firewall, causing issues updating domain group policies.

Endpoint control

Bug ID	Description
693928	After FortiClient migrates to new EMS successfully, it does not remove original EMS from EMS list.
738813	FortiESNAC process causes high CPU.
764664	FortiClient falls out of sync with EMS.
789922	FortiClient (Windows) does not reattempt to register to EMS after license assignment until user shuts down or restarts FortiClient (Windows).

GUI

Bug ID	Description
752084	GUI for Sandbox exclusion list is not blocked completely and scrolling is impossible.
773355	Web Filter tab has display issue with German umlauts.

Zero Trust Telemetry

Bug ID	Description
683542	FortiClient (Windows) fails to register to EMS if registration key contains special character, such as " !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~" .
763957	FortiClient prompts for Telemetry key when Telemetry key changes on EMS.

Malware Protection and Sandbox

Bug ID	Description
721038	Customized access rule to allow USB, camera, and Bluetooth devices fails when default removable media access is blocked.
730054	*Allow Admin Users to Terminate Scheduled and On-Demand Scans from FortiClient Console* feature does not work as expected.
759834	FortiClient does not bypass keyboard and mouse device by default when default removable media access action is block.
760073	FortiClient (Windows) affects USB operation.
762125	fortimon3.sys causes blue screen of death during Slack calls.

Remote Access

Bug ID	Description
710877	SSL VPN with SAML (Azure Active Directory (AD)) and two gateways does not work.
711402	Per-user autoconnect does not establish and per-machine autoconnect remains connected after logon to Windows.
729610	Save username and password are enabled but FortiClient incorrectly saves encrypted password

Bug ID	Description
	when user enters Spanish characters.
731127	SSL VPN with SAML tunnel displays error that empty username is not allowed.
743106	IPsec VPN XAuth does not work with ECDSA certificates.
744544	FortiClient (Windows) always saves SAML credentials.
758424	Certificate works for IPsec VPN tunnel if put it is in current user store, but fails to work if it is in local machine.
759138	FortiSASE VPN traffic inconsistently goes through the FortiSASE tunnel when trusted traffic is enabled.
762986	If FortiClient (Windows) cannot reach the first remote gateway when connecting to a resilient tunnel from FortiTray, FortiClient does not use the second FortiGate to connect.
771090	Saving username for IPsec VPN tunnel does not work.
773060	Microsoft Surface Pro connected to VPN on wireless connection cannot access SQL Server Reporting Services report, software hosted on internal server.
790404	GUI is missing SAML button.
794110	VPN before logon does not work with Okta as multifactor authentication and disclaimer message acceptance is enforced.
794658	If the first remote gateway becomes offline with IPsec VPN resilience when VPN is up, FortiClient does not use the second FortiGate to connect to VPN.

Web Filter

Bug ID	Description
781874	Website does not load with `ERR_CONTENT_LENGTH_MISMATCH` error.
793017	Web Filter option disconnects an application's underlying connection.

Zero Trust tags

Bug ID	Description
731525	FortiClient (Windows) does not properly detect Zero Trust tag for not having antivirus up-to-date.
759235	Zero Trust Network Access Bitlocker (BL) policy is not matched despite FortiClient (Windows) having BL protection enabled.

Other

Bug ID	Description
725631	Windows 10 laptop network interfaces stay unavailable after hibernation or sleep.
749458	FortiClient (Windows) displays specific email address related to social network login using Gmail account.