FortiClient (Windows) - Release Notes

Version 6.4.3

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 18, 2021
FortiClient (Windows) 6.4.3 Release Notes
04-643-690109-20210318

TABLE OF CONTENTS

Change log 4
Introduction 5
Licensing 5
Special notices 6
Nested VPN tunnels 6
SSL VPN connectivity issues 6
Microsoft Windows server support 6
HP Velocity and Application Firewall 6
Split tunnel 6
Installation information 7
Firmware images and tools 7
Upgrading from previous FortiClient versions 8
Downgrading to previous versions 8
Firmware image checksums 8
Product integration and support 9
Language support 10
Conflicts with third party AV products 10
Resolved issues 12
GUI 12
Endpoint control 12
Malware Protection and Sandbox 12
Remote Access 13
Web Filter and plugin 13
Known issues 14
Install and deployment 14
GUI 14
Zero Trust Telemetry 14
Malware Protection and Sandbox 15
Remote Access 15
Web Filter 16
Logs 16
Other 16

Change log

Date	Change Description
2021-02-09	Initial release of 6.4.3.
2021-03-18	Added Split tunnel on page 6.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 6.4.3 build 1608.

- Special notices on page 6
- Installation information on page 7
- Product integration and support on page 9
- Resolved issues on page 12
- Known issues on page 14

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 8 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 6.4.3 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 6.4.3 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 AV, vulnerability scan, Web Filter, and SSL VPN features for Microsoft Windows servers.

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

A split tunnel configuration that functioned in FortiClient (Windows) 6.4.1 no longer works after upgrading to 6.4.3, unless the administrator has configured a per-tunnel configuration in EMS.

Installation information

Firmware images and tools

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

File	Description
FortiClientTools_6.4.3.xxxx.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_ 6.4.3.xxxx.zip	FSSO-only installer (32-bit).
FortiClientSSOSetup_ 6.4.3.xxxx_x64.zip	FSSO-only installer (64-bit).
FortiClientVPNSetup_ 6.4.3.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_ 6.4.3.xxxx_x64.exe	Free VPN-only installer (64-bit).

EMS 6.4.3 includes the FortiClient (Windows) 6.4.3 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_6.4.3.xxxx.zip	Standard installer package for Windows (32-bit).
FortiClientSetup_6.4.3.xxxx_ x64.zip	Standard installer package for Windows (64-bit).

File	Description
FortiClientVPNSetup_ 6.4.3.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_ 6.4.3.xxxx_x64.exe	Free VPN-only installer (64-bit).

Review the following sections prior to installing FortiClient version 6.4.3: Introduction on page 5, Special notices on page 6, and Product integration and support on page 9.

Upgrading from previous FortiClient versions

To upgrade a previous FortiClient version to FortiClient 6.4.3, do one of the following:

- Deploy FortiClient 6.4.3 as an upgrade from EMS
- Manually uninstall existing FortiClient version from the device, then install FortiClient (Windows) 6.4.3

FortiClient (Windows) 6.4.3 features are only enabled when connected to EMS 6.4.0.

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

Downgrading to previous versions

FortiClient (Windows) 6.4.3 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 6.4.3 product integration and support information:

Desktop operating systems	• 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 6.4.3 does not support Microsoft Windows XP and Microsoft Windows Vista.
Server operating systems	• Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 FortiClient 6.4.3 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	• 6.00253
FortiAnalyzer	• 6.4.0 and later
FortiAuthenticator	• 6.1.0 and later • 6.0.0 and later
FortiClient EMS	• 6.4.1 and later
FortiManager	• 6.4.0 and later
FortiOS	The following FortiOS versions support IPsec and SSL VPN with FortiClient (Windows) 6.4.3: • 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) 6.4.3: • 6.2.0 and later
FortiSandbox	• 3.2.0 and later • 3.1.0 and later • 3.0.0 and later • 2.5.0 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.

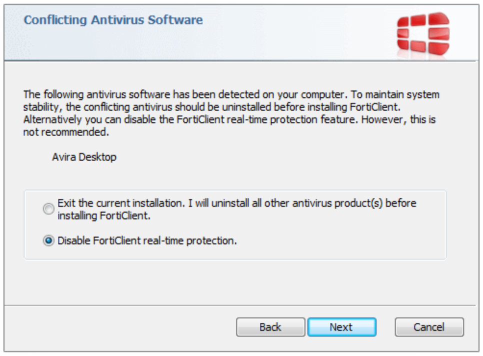
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

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).



Conflicting Antivirus Software

The following antivirus software has been detected on your computer. To maintain system stability, the conflicting antivirus should be uninstalled before installing FortiClient. Alternatively you can disable the FortiClient real-time protection feature. However, this is not recommended.

Avira Desktop

○ Exit the current installation. I will uninstall all other antivirus product(s) before installing FortiClient.

● Disable FortiClient real-time protection.

Resolved issues

The following issues have been fixed in version 6.4.3. For inquiries about a particular bug, contact Customer Service & Support.

GUI

Bug ID	Description
666708	Add error message when FortiClient tries to connect to FortiClient Cloud 6.2.
675451	GUI displays incorrect logs settings compared to EMS profile logs settings.
677473	Rename Security Fabric Agent to Zero Trust Fabric Agent.
679004	Two tokens are delivered via email when moving cursor with `Tab` key and clicking *Connect* button.
685344	FortiClient should show SASE tunnel under SASE SIA heading, not Corporate VPN.

Endpoint control

Bug ID	Description
684618	FortiClient does not report error message when it fails to register to FortiClient Cloud with invitation code.
691573	FortiClient (Windows) keeps reregistering to EMS with a different UID and generates duplicated record in EMS.

Malware Protection and Sandbox

Bug ID	Description
582302	FortiClient cannot get signature from FortiManager using HTTPS due to certificate check failure.
606712	Attempts to restore quarantined files from USB drives fail.
686937	Antiransomware feature causes DNS queries to fail, affecting several applications.
690782	Antivirus does not register to Windows Security Center on Windows 10.

Remote Access

Bug ID	Description
659906	IPsec VPN-connected client registers local adapter IP address to DNS server, causing FSSO and client traffic to fail.
664272	FortiClient (Windows) cannot connect SSL VPN tunnel using Azure identity provider for SAML.
671392	Windows restart does not remove SSL VPN tunnel established by VPN before logon.
674145	When registering FortiClient (Windows) to 6.4.2 EMS, IPsec VPN tunnel that EMS pushed does not work properly.
685186	*Auto-Connect only when Off-Fabric* does not work.
686368	Application-based split tunnel only works on Windows 10.
688851	Autoconnect and always up features do not work.
689100	Autoconnect does not work properly.

Web Filter and plugin

Bug ID	Description
676892	Web FIlter violations table only lists last blocked URL.

Known issues

The following issues have been identified in FortiClient (Windows) 6.4.3. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Install and deployment

Bug ID	Description
687647	After upgrading EMS with a remote SQL database, FortiClient cannot register to EMS.
691328	FortiClient upgrade does not upgrade AV engine when deployed through an EMS installer.

GUI

Bug ID	Description
686052	Add EMS connect/disconnect event information.

Zero Trust Telemetry

Bug ID	Description
587327	Device detection/VPN autoconnect frequency is too often.
673183	FortiClient needs to properly handle trying to register to FortiClient Cloud with invitation code with errors.
676923	DNS server on-Fabric detection rule does not work.
678388	Active Directory user logoff does not trigger tag message.
683097	FortiClient shows incorrect connection details.
689111	Changed username, phone number, and email in avatar page do not show in EMS endpoint details page.
689727	Zero Trust tag for Windows Defender does not work on Windows 7.
690457	FortiClient (Windows) fails to migrate from one site to another within the same EMS.
690679	EMS cannot tag endpoint based on nested Active Directory groups.

Bug ID	Description
691966	EMS doe snot assign profile to endpoint after user switches from local to domain user account.
693618	On-/off-fabric calculations do not work with some conditions upon endpoint reboot.

Malware Protection and Sandbox

Bug ID	Description
667964	Protected files may already have been encrypted and fail to be restored when FortiClient detects and suspends the suspicious process.
668719	Realtime protection on Citrix VDA server blocks remote sessions.

Remote Access

Bug ID	Description
617420	Support remote access VPN with prelogon without user interaction.
627339	FortiClient (Windows) fails to establish VPN connection with SAML login if FortiOS *SSL VPN Require Client Certificate* setting is enabled.
637303	Certificate-only SSL VPN tunnel displays popup with *Empty username is not allowed* error.
643083	Dual SSL VPN certs with the same name.
649426	IPsec/SSL VPN per-app VPN split tunnel does not work properly.
649688	Website with HTTP defined in `<fqdn>` does not work properly with per-app VPN split tunnel.
665426	SAML SSL-VPN in Tunnel Mode broken when using ADFS+DUO 2FA solution
671091	IPsec VPN stops traffic to internal network immediately after connecting to a Citrix workspace or RDP.
677766	When VPN tunnel goes down, the single-host route for the VPN server stays.
681399	IPsec VPN autoconnect does not work after an automatic frequency change.
682675	SSL VPN users cannot set new PIN after it expires with RSA RADIUS authentication.
684913	SAML authentication on SSL VPN with realms does not work.
685951	FortiClient (Windows) does not use fallback server IP address when *Show VPN before Logon* is enabled.
686908	After updating FortiClient, users cannot connect to VPN.
688043	VPN before logon does not display FortiToken request prompt.

Bug ID	Description
688844	FortiClient (Windows) drops SSL VPN connection after enabling EMS tag authentication on SSL VPN.
689163	IPsec VPN RSA token rekey does not work.
689176	IPsec VPN failover to SSL VPN when VPN before logon does not work properly.
689936	FortiClient (Windows) displays GUI issue when connecting to IPsec VPN using tray.
690057	FortiClient (Windows) does not display *Error: Wrong Credentials* message for IKEv2.
693687	FortiClient does not register any interface IP addresses to the DNS server when SSL VPN tunnel is up.
714688	User cannot log in to IPSec VPN when password includes umlaut.

Web Filter

Bug ID	Description
689182	FortiClient (Windows) blocks access to Office 365 or Microsoft sites.

Logs

Bug ID	Description
671461	FortiClient (Windows) does not have debug logs about FortiSandbox file submission.

Other

Bug ID	Description
649168	Windows crashes when Safetica DLP 9.6.55 and FortiClient are installed together.
673671	fmon.exe locks with writers some files stored in excluded folders.
686139	Console fails to open when double-left-clicking the tray icon.
691564	FortiShield causes third party application performance issues.