FortiClient (Windows) - Release Notes

Version 6.4.4

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/support-and-training/training.html

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

June 02, 2021
FortiClient (Windows) 6.4.4 Release Notes
04-644-717036-20210602

TABLE OF CONTENTS

Change log

Date	Change Description
2021-06-02	Initial release of 6.4.4.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 6.4.4 build 1655.

- Special notices on page 6
- Installation information on page 8
- Product integration and support on page 10
- Resolved issues on page 13
- Known issues on page 16

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 6.4.4 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 6.4.4 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

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 will no longer function after upgrading to 6.4.4. You must complete the per-tunnel configuration after upgrade.

This is unrelated to the FortiOS split tunnel feature.

What’s new in FortiClient (Windows) 6.4.4

For information about what's new in FortiClient (Windows) 6.4.4, see the *FortiClient & FortiClient EMS 6.4 New Features Guide*.

Installation information

Firmware images and tools

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

File	Description
FortiClientTools_6.4.4.xxxx.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_ 6.4.4.xxxx.zip	FSSO-only installer (32-bit).
FortiClientSSOSetup_ 6.4.4.xxxx_x64.zip	FSSO-only installer (64-bit).
FortiClientVPNSetup_ 6.4.4.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_ 6.4.4.xxxx_x64.exe	Free VPN-only installer (64-bit).

EMS 6.4.4 includes the FortiClient (Windows) 6.4.4 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_6.4.4.xxxx.zip	Standard installer package for Windows (32-bit).
FortiClientSetup_6.4.4.xxxx_ x64.zip	Standard installer package for Windows (64-bit).

File	Description
FortiClientVPNSetup_6.4.4.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_6.4.4.xxxx_x64.exe	Free VPN-only installer (64-bit).

Review the following sections prior to installing FortiClient version 6.4.4: Introduction on page 5, Special notices on page 6, and Product integration and support on page 10.

Upgrading from previous FortiClient versions

To upgrade a previous FortiClient version to FortiClient 6.4.4, do one of the following:

- Deploy FortiClient 6.4.4 as an upgrade from EMS
- Manually uninstall existing FortiClient version from the device, then install FortiClient (Windows) 6.4.4

FortiClient (Windows) 6.4.4 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) 6.4.4 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 6.4.4 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 6.4.4 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 6.4.4 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	• 7.0.0 and later • 6.4.1 and later

FortiManager	• 6.4.0 and later
FortiOS	The following FortiOS versions support IPsec and SSL VPN with FortiClient (Windows) 6.4.4: • 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) 6.4.4: • 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.

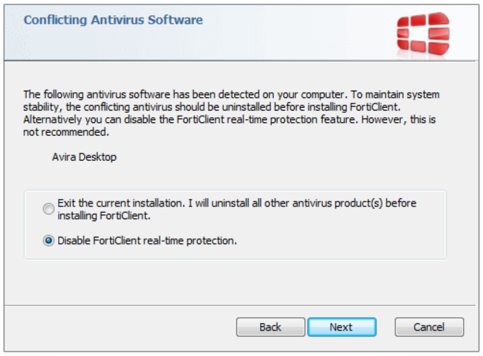
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

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).



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 6.4.4. For inquiries about a particular bug, contact Customer Service & Support.

GUI

Bug ID	Description
685756	FortiClient (Windows) does not respond after entering invitation code and clicking *Connect* to register to EMS.
686139	Console fails to open when double-clicking tray icon.
689936	GUI issue when connecting to IPsec VPN using tray.
690769	FortiClient (Windows) cannot start VPN connection with `Enter` key.
691647	Real-time protection event button does not open logs.

Logs

Bug ID	Description
656318	Diagnostic tool has high CPU usage, takes forever to run, and does not finish.

Malware Protection and Sandbox

Bug ID	Description
705452	Sandbox agent crashes when trying to submit network files to FortiSandbox from Windows Explorer context menu.
717417	FortiClient (Windows) could not get FortiSandbox Cloud IP address list. FortiClient (Windows) fails to connect to the aptgwserver in some situation.
718343	Ransomware detection for DarkSide ransomware.

Remote Access

Bug ID	Description
617420	Support remote access VPN with prelogon without user interaction.
645174	FortiClient (Windows) sometimes does not use the `remoteauthtimeout` value configured on FortiGate for SSL VPN.
649426	IPsec and SSL VPN per-application VPN split tunnel does not work properly.
671392	Windows restart does not remove SSL VPN tunnel established by VPN before logon.
677766	When VPN tunnel goes down, the single-host route for the VPN server stays.
682249	SSL VPN DNS split tunnel issues slow down the DNS request process.
682675	SSL VPN RSA token (for example new PIN mode) does not work properly if the RADIUS server message contains double quotes.
688043	VPN before logon does not request FortiToken.
689176	IPsec VPN failover to SSL VPN with VPN before logon does not work properly.
695133	DNS resolution is inconsistent when split DNS is enabled.
702965	SSL VPN host check interval does not work as expected, after PC has gone to sleep mode previously.
703939	VPN client does not send UID to SSL VPN daemon.
706023	Restarting computer loses DNS settings.
710603	VPN resets with each EMS push.
713909	If VPN before Windows logon is enabled and there are multiple tunnels configured, there is a long delay before Windows login prompt.
717448	VPN before Windows logon fails to list certificate when `disable_internet_check` is 1.

Web Filter and plugin

Bug ID	Description
696581	Web plugin causes Gmail attachment downloads to pause and lock up the browser.

Zero Trust Telemetry

Bug ID	Description
696230	On-Fabric detection based on public IP address does not recognize IP address change.
697795	FortiClient fails to calculate On-Fabric result.
698008	Disconnection from Telemetry also disconnects SSL VPN.
699686	EMS does not receive Software Inventory from FortiClient (Windows).
700915	FortiClient (Windows) fails to disconnect from FortiClient Cloud when FortiClient Cloud is unreachable.
715320	FortiClient fails to update state when FortiClient Cloud is unreachable.

Known issues

The following issues have been identified in FortiClient (Windows) 6.4.4. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Install and deployment

Bug ID	Description
691328	FortiClient upgrade does not upgrade AV engine when deployed through an EMS installer.
716597	Installation using `norestart` parameter requests reboot.

GUI

Bug ID	Description
665426	SAML SSL VPN in tunnel mode is broken when using Active Directory Federation Services and Duo multifactor authentication solution.
689744	FortiClient (Windows) only displays VPN tunnel name after FortiClient (Windows) adds new IPsec VPNs.
717476	EMS tag does not appear in FortiClient (Windows) GUI.

Zero Trust Telemetry

Bug ID	Description
652647	FortiClient fails to upload large diagnostic tool result file to EMS.
687611	FortiClient (Windows) should calculate AD group-based policy rule for tags.
690679	EMS cannot tag endpoint based on nested AD groups.
692385	After disconnecting from EMS, FortiClient should keep the EMS hostname/IP address in the GUI.
693928	After FortiClient (Windows) migrates to new EMS successfully, it does not remove original EMS from EMS list.
702660	Switching to a new AD user does not modify user details in EMS GUI Endpoints table.

Bug ID	Description
705010	EMS shows endpoint with incorrect username.
714131	Migrating FortiClient to different server fails when connection key is enabled.
717482	FortiClient IPsec VPN client does not appear in dynamic address list on FortiGate.
718995	FortiClient is not registered to EMS after silent installation.

Malware Protection and Sandbox

Bug ID	Description
516704	Antivirus should recognize Windows-signed files.
590688	FortiClient says that FortiSandbox scan does not support file type when extension is supported and enabled on FortiSandbox.
700396	FortiClient causes DVD driver to fail to load (code 38).
705761	FortiClient (Windows) does not block USB drives despite removable media access being configured to block Windows portable devices.
709238	Building Java projects takes twice as long when real-time protection is enabled.
710899	Saving an Excel file fails.
713557	Exceptions do not work for antiexploit module.

Remote Access

Bug ID	Description
637303	Certificate-only SSL VPN tunnel displays popup with *Empty username is not allowed* error.
671091	IPsec VPN stops traffic to internal network immediately after connecting to a Citrix workspace or RDP.
693687	FortiClient does not register any interface IP addresses to the DNS server when SSL VPN tunnel is up.
698407	VPN before logon does not work with IKEv2 and Extensible Authentication Protocol.
700092	VPN does not connect when in domain user account.
701552	SASE SIA tunnel reconnection issues after SASE SIA portal removes VPN user.
707882	IPsec VPN fails to automatically connect with *Failed to launch IPsec service*.
709001	SSL VPN host check validation does not work for SAML user.

Bug ID	Description
710877	SSL VPN with SAML (Azure AD) and two gateways does not work.
711227	Per-user autoconnect starts to automatically connect before logging onto Windows.
711402	Per-user autoconnect is not established after logon and per machine autoconnect still keeps up.
714564	SAML connection stays in connecting state and never returns with error when FortiGate gateway is inaccessible.
714688	IPsec VPN login is impossible when password includes German umlauts.
716323	FortiClient (Windows) cannot connect to IPsec VPN with no response from GUI after machine wakeup.
716924	Azure multifactor authentication fails when redundant sort method is configured as ping or TCP round trip time.
717512	VPN disclaimer does not show during IPsec VPN connection.
717913	FortiSASE SIA VPN fails to reestablish after FortiSASE SIA-related components are upgraded.
718737	FortiClient is intermittently missing SSL VPN user credentials after Windows logon per user tunnel.
720559	When connecting to IPsec VPN through FortiTray, after inputting username/password in GUI, there is a 30 second delay before asking for user token.

Vulnerability Scan

Bug ID	Description
630202	Vulnerability Scan cannot detect Zoom.exe installer.

Web Filter

Bug ID	Description
708855	GUI shows site is unavailable when blocked.

Logs

Bug ID	Description
638227	Improve USB detections notifications.
716495	FortiClient does not log tag assigned/unassigned event.
717452	Diagnostic result does not display after diagnostic tool completes exporting the files.

Other

Bug ID	Description
716803	When logging into Windows as domain user, avatar does not show properly on FortiAnalyzer.