FortiClient (Windows) - Release Notes

Version 6.4.7

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

February 22, 2022
FortiClient (Windows) 6.4.7 Release Notes
04-647-731407-20220222

TABLE OF CONTENTS

Change log

Date	Change Description
2021-11-25	Initial release of 6.4.7.
2022-02-22	Added 779930 to Remote Access on page 16.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 6.4.7 build 1713.

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 6.4.7 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

Endpoint security improvement

EMS 6.4.7 adds an improvement to endpoint security that impacts compatibility between FortiClient and EMS, and the recommended upgrade path. The FortiClient 6.4.7 installer is not available on FortiGuard Distribution Servers (FDS). To install the FortiClient 6.4.7 installer, you must download it from Customer Service & Support. See Endpoint security improvement.

If the EMS server certificate is invalid, and FortiClient is upgraded to 6.4.7, by default, FortiClient displays a warning message on the GUI when trying to connect to the EMS. The end user should click *allow* to complete the connection. FortiClient does not connect to the EMS if the end user selects *deny*. If the end user selects *deny*, FortiClient retries connecting to the EMS after a system reboot. The same warning message displays while trying to connect to the EMS. The end user should click *allow* to complete the connection.

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 6.4.7. 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_6.4.7.xxxx.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_ 6.4.7.xxxx.zip	FSSO-only installer (32-bit).
FortiClientSSOSetup_ 6.4.7.xxxx_x64.zip	FSSO-only installer (64-bit).
FortiClientVPNSetup_ 6.4.7.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_ 6.4.7.xxxx_x64.exe	Free VPN-only installer (64-bit).

EMS 6.4 includes the FortiClient (Windows) 6.4.7 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_6.4.7.xxxx.zip	Standard installer package for Windows (32-bit).
FortiClientSetup_6.4.7.xxxx_ x64.zip	Standard installer package for Windows (64-bit).

File	Description
FortiClientVPNSetup_6.4.7.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_6.4.7.xxxx_x64.exe	Free VPN-only installer (64-bit).

Review the following sections prior to installing FortiClient version 6.4.7: 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 6.4.7 before upgrading FortiClient.

To upgrade a previous FortiClient version to FortiClient 6.4.7, do one of the following:

- Deploy FortiClient 6.4.7 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) 6.4.7

FortiClient (Windows) 6.4.7 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) 6.4.7 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 6.4.7 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 6.4.7 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 6.4.7 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) 6.4.7: • 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) 6.4.7: • 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.

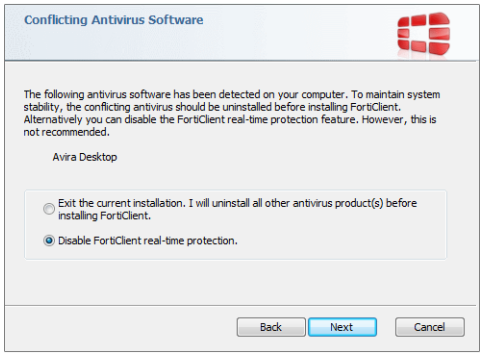
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

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).



Resolved issues

The following issues have been fixed in version 6.4.7. For inquiries about a particular bug, contact Customer Service & Support.

GUI

Bug ID	Description
725854	Antivirus (AV) scan displays scan progress popup.

Install and deployment

Bug ID	Description
742508	FortiClient is uninstalled using CCleaner with *Require password for Disconnect* enabled.

Endpoint control

Bug ID	Description
675889	Improve endpoint modification management behavior.
728114	Telemetry status gets stuck on syncing.

Malware Protection and Sandbox

Bug ID	Description
516704	AV should recognize Windows- signed files.
674454	FortiClient on Windows 7 does not block USB drive.
689248	After upgrading FortiClient, user cannot create, save, delete, or rename *C:\Backup* folder.
693565	Chrome cannot rename temporary download files because Sandbox agent locks them.

Bug ID	Description
700298	FortiClient (Windows) does not submit zip files larger than 200 MB to FortiSandbox.
700396	The device driver cannot be loaded (code 38).
705761	FortiClient (Windows) does not block USB drives despite removable media access being configured to block Windows portable devices.
710899	Excel file save fails.
713557	AntiExploit exceptions do not work.
722597	Keyboards and mouses can be allowed or denied based on human interface device rule.
725936	USB key compatibility.
734993	Rule to block removable media such as a USB drive stops working.

Remote Access

Bug ID	Description
599924	Certificate-based IKEv2 cannot connect without enabling the extensible authentication protocol (EAP).
613868	Always up and autoconnect do not work for SAML SSL VPN connection.
637303	Certificate-only SSL VPN tunnel displays *Empty username is not allowed.* error.
684913	SAML authentication on SSL VPN with realms does not work.
685959	On booting up the operating system, machine IPsec VPN does not connect.
692822	Token popup has six character limit.
692823	Split DNS has resolution time of more than 30 seconds.
693687	FortiClient does not register any interfaces' IP addresses to the DNS server when SSL VPN tunnel is up.
693913	Username and password become blank on console when connecting to second remote gateway with SSL VPN.
698407	VPN before logon does not work with IKEv2 and EAP.
700440	Application-based split tunnel does not work.
702764	IPsec VPN connection fails with error that certificate was not loaded.
707882	IPsec VPN fails to autoconnect with *Failed to launch IPsec service* error (ref.0490188,0555131,0550604).
718178	FortiClient does not support always-on connections when using SAML SSO.
718737	FortiClient is intermittently missing SSL VPN user credentials after Windows logon.

Bug ID	Description
719828	FortiClient fails to allow SSL VPN when it does not have prohibit host tag.
724092	`match_type` does not work when using VPN before logon.
732594	SSL VPN `redundant_sort_method` does not work with realms.
750008	FortiClient caches VPN tunnel username when it is configured not to.
751430	Split tunnel, split DNS, and remote DNS server resolution do not work.

Web Filter and plugin

Bug ID	Description
731982	Web rating overrides behavior between FortiClient Web Filter and FortiOS Web Filter differs.

Zero Trust tags

Bug ID	Description
652897	FortiClient (Windows) tags endpoint as vulnerable when EMS has enabled excluding application vulnerabilities requiring manual update from vulnerabilities
726729	Windows Firewall ZTR does not tag FortiClient when Web Filter is enabled via a group policy object.

Other

Bug ID	Description
737917	Windows 11 support.

Known issues

The following issues have been identified in FortiClient (Windows) 6.4.7. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Install and deployment

Bug ID	Description
716597	Installation using `norestart` parameter requests reboot.
726616	FortiClient 6.4.3 cannot upgrade to 6.4.4.

Endpoint control

Bug ID	Description
751728	FortiClient does not automatically connect to EMS after FortiClient upgrade.

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.

Remote Access

Bug ID	Description
710877	SSL VPN with SAML (Azure Active Directory (AD)) and two gateways does not work.
729610	Save username and password are enabled but FortiClient incorrectly saves encrypted password when user enters Spanish characters.
731011	FortiClient gets stuck at 98% connecting to SSL VPN tunnel when integrated with SAML (Azure AD) authentication.

Bug ID	Description
779930	SAML SSL VPN gets stuck when using CNAME DNS record as remote gateway.

Web Filter

Bug ID	Description
657715	FortiProxy fails to start.
729127	Web Filter affects manufacturing execution system software.

Zero Trust tags

Bug ID	Description
759235	Zero Trust Network Access Bitlocker (BL) policy is not matched despite FortiClient (Windows) having BL protection enabled.

Other

Bug ID	Description
725631	Network interfaces on Windows 10 laptops stay unavailable after hibernation or sleep.