



FortiClient (Windows) - Release Notes

Version 6.4.9

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



September 22, 2022

FortiClient (Windows) 6.4.9 Release Notes

04-649-836871-20220922

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	8
Firmware images and tools	8
Upgrading from previous FortiClient versions	9
Downgrading to previous versions	9
Firmware image checksums	9
Product integration and support	10
Language support	11
Conflicts with third party AV products	12
Resolved issues	13
GUI	13
Install and upgrade	13
Application Firewall	13
Malware Protection and Sandbox	13
FSSO	14
Remote Access	14
Web Filter and plugin	14
Deployment and installers	15
Other	15
Known issues	16
Install and upgrade	16
Application Firewall	16
Endpoint control	16
Logs	16
Zero Trust Telemetry	17
Malware Protection and Sandbox	17
Remote Access	17
Performance	18
Web Filter	18
Zero Trust tags	18
Other	18

Change log

Date	Change Description
2022-09-22	Initial release of 6.4.9.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 6.4.9 build 1797.

- [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 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 6.4.9 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 6.4.9. 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_6.4.9.xxxx.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_6.4.9.xxxx.zip	FSSO-only installer (32-bit).
FortiClientSSOSetup_6.4.9.xxxx_x64.zip	FSSO-only installer (64-bit).
FortiClientVPNSetup_6.4.9.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_6.4.9.xxxx_x64.exe	Free VPN-only installer (64-bit).

EMS 6.4 includes the FortiClient (Windows) 6.4.9 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](https://fortinet.com):

File	Description
FortiClientSetup_6.4.9.xxxx.zip	Standard installer package for Windows (32-bit).
FortiClientSetup_6.4.9.xxxx_x64.zip	Standard installer package for Windows (64-bit).

File	Description
FortiClientVPNSetup_6.4.9.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_6.4.9.xxxx_x64.exe	Free VPN-only installer (64-bit).



Review the following sections prior to installing FortiClient version 6.4.9: [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 6.4.9, do one of the following:

- Deploy FortiClient 6.4.9 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) 6.4.9

FortiClient (Windows) 6.4.9 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) 6.4.9 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 6.4.9 product integration and support information:

Desktop operating systems	<ul style="list-style-type: none">• 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) <p>FortiClient 6.4.9 does not support Microsoft Windows XP and Microsoft Windows Vista.</p>
Server operating systems	<ul style="list-style-type: none">• 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 <p>FortiClient 6.4.9 does not support Windows Server Core.</p> <p>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.</p>
Embedded system operating systems	Microsoft Windows 10 IoT Enterprise LTSC 2019
Minimum system requirements	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 6.00258
FortiAnalyzer	<ul style="list-style-type: none">• 7.0.0 and later• 6.4.0 and later
FortiAuthenticator	<ul style="list-style-type: none">• 6.3.0 and later• 6.2.0 and later• 6.1.0 and later• 6.0.0 and later
FortiClient EMS	<ul style="list-style-type: none">• 7.0.2 and later

	<ul style="list-style-type: none"> • 6.4.7 and later
FortiManager	<ul style="list-style-type: none"> • 6.4.0 and later
FortiOS	<p>The following FortiOS versions support IPsec and SSL VPN with FortiClient (Windows) 6.4.9:</p> <ul style="list-style-type: none"> • 7.0.0 and later • 6.4.0 and later • 6.2.0 and later • 6.0.0 and later <p>The following FortiOS versions support endpoint control with FortiClient (Windows) 6.4.9:</p> <ul style="list-style-type: none"> • 6.2.0 and later
FortiSandbox	<ul style="list-style-type: none"> • 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.



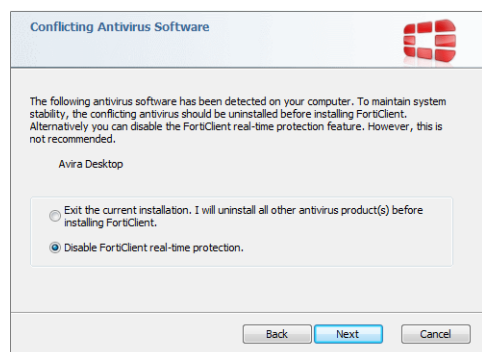
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

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 6.4.9. For inquiries about a particular bug, contact [Customer Service & Support](#).

GUI

Bug ID	Description
751299	FortiClient has empty vulnerability detail tab.
752084	GUI for Sandbox exclusion list is not blocked completely and scrolling is impossible.

Install and upgrade

Bug ID	Description
726616	FortiClient cannot upgrade to 6.4.4.
812010	Users can uninstall FortiClient (Windows) if it was installed via .msi from the group policy object.

Application Firewall

Bug ID	Description
654152	<i>All Other Unknown Applications</i> blocks allowed categories in Application Firewall.

Malware Protection and Sandbox

Bug ID	Description
721038	FortiClient (Windows) does not block SD cards when it is configured to block default removable media access.
758665	FortiClient (Windows) does not update antiexploit protection list to have Chrome and Firefox.

Bug ID	Description
784306	FortiClients causes blue screen of death when ACR1281 card reader is plugged in.
820511	Promethean Active Board does not work.

FSSO

Bug ID	Description
683213	FortiClient single sign on mobility agent does not update logon events or IP address changes to FortiAuthenticator and fails to send information intermittently.

Remote Access

Bug ID	Description
634609	Credential provider displays the wrong domain when logging in to Windows 10.
729610	FortiClient (Windows) saves encrypted password incorrectly when save username and password are activated and the password includes special characters.
788765	German characters "" and/or "\$" in the end user password activates the <i>SAML</i> button in the GUI.
798044	Using Finnish front vowels [/] in the SSL VPN password causes issues when FortiClient (Windows) saves the password.
802323	VPN before login fails to connect with host check rule configured immediately after reboot.
839443	Always up option becomes deselected after user manually disconnects VPN tunnel.
840720	User cannot modify IPsec VPN advanced settings for personal VPN profile.

Web Filter and plugin

Bug ID	Description
804938	All Internet traffic stops when user connects a USB controller (RNDIS).

Deployment and installers

Bug ID	Description
836491	EMS 6.4.8 or later deployments can fail when <i>Require Password to Disconnect from EMS</i> is enabled.

Other

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

Known issues

The following issues have been identified in FortiClient (Windows) 6.4.9. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

Install and upgrade

Bug ID	Description
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
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.
723599	FortiClient uses SASE egress IP address as the public IP address.
789922	FortiClient (Windows) does not reattempt to register to EMS after license assignment until user shuts down or restarts FortiClient (Windows).

Logs

Bug ID	Description
820067	FortiClient forwards logs despite being completely disabled.

Zero Trust Telemetry

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

Malware Protection and Sandbox

Bug ID	Description
606634	FortiClient fails to remove quarantined files after days configured with cullage option.
650383	Number of blocked exploits attempts does not work properly.
760073	FortiClient (Windows) affects USB operation.

Remote Access

Bug ID	Description
743106	IPsec VPN XAuth does not work with ECDSA certificates.
758424	Certificate works for IPsec VPN tunnel if put in current user store but fails to work if it is on the local machine.
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.
780938	SAML connection does not work for international connections.
782393	Application-based split VPN tunnel has issue when using VipWebAppServer.exe application.
786348	FortiClient shows error code -8 or -14 when <i>Limit Users to One SSL-VPN Connection at a Time</i> is enabled on FortiOS with SAML authentication.
790404	GUI is missing SAML button.
795334	Always up feature does not work as expected when trying to connect to VPN form tray.
841970	GUI gets stuck while connecting with SAML to SSL VPN with Azure Active Directory and Duo for multifactor authentication.

Performance

Bug ID	Description
778651	Large downloads and speed tests result in high latency, packet loss, and poor performance.

Web Filter

Bug ID	Description
781874	Website does not load with <code>ERR_CONTENT_LENGTH_MISMATCH</code> error.
793017	Web Filter option disconnects an application's underlying connection.
825633	Error occurs when revoking certificate accessing outlook.office365.com using Web Filter.

Zero Trust tags

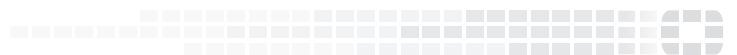
Bug ID	Description
704234	Zero Trust tagging rule set syntax to check registry key value is unclear.
731525	FortiClient (Windows) does not properly detect Zero Trust tag for not having antivirus up-to-date.

Other

Bug ID	Description
749458	FortiClient (Windows) displays specific email address related to social network login using Gmail account.



FORTINET®



Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.