



# FortiClient (Windows) - Release Notes

Version 6.4.6

**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](mailto:techdoc@fortinet.com)



July 13, 2021

FortiClient (Windows) 6.4.6 Release Notes

04-646-731407-20210713

# TABLE OF CONTENTS

<b>Change log</b>	<b>4</b>
<b>Introduction</b>	<b>5</b>
Licensing	5
<b>Special notices</b>	<b>6</b>
Nested VPN tunnels	6
SSL VPN connectivity issues	6
Microsoft Windows server support	6
HP Velocity and Application Firewall	6
Split tunnel	6
<b>Installation information</b>	<b>7</b>
Firmware images and tools	7
Upgrading from previous FortiClient versions	8
Downgrading to previous versions	8
Firmware image checksums	8
<b>Product integration and support</b>	<b>9</b>
Language support	10
Conflicts with third party AV products	11
<b>Resolved issues</b>	<b>12</b>
<b>Known issues</b>	<b>13</b>
Install and deployment	13
Endpoint control	13
GUI	13
Zero Trust Telemetry	14
Malware Protection and Sandbox	14
Remote Access	15
Vulnerability Scan	16
Web Filter	16
Logs	16
Other	17

## Change log

Date	Change Description
2021-07-13	Initial release of 6.4.6.

# Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 6.4.6 build 1658.

- [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 13](#)

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 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 6.4.6 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](https://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 6.4.6. You must complete the per-tunnel configuration after upgrade.

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_6.4.6.xxxx.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_6.4.6.xxxx.zip	FSSO-only installer (32-bit).
FortiClientSSOSetup_6.4.6.xxxx_x64.zip	FSSO-only installer (64-bit).
FortiClientVPNSetup_6.4.6.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_6.4.6.xxxx_x64.exe	Free VPN-only installer (64-bit).

EMS 6.4 includes the FortiClient (Windows) 6.4.6 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://www.fortinet.com):

File	Description
FortiClientSetup_6.4.6.xxxx.zip	Standard installer package for Windows (32-bit).
FortiClientSetup_6.4.6.xxxx_x64.zip	Standard installer package for Windows (64-bit).

File	Description
FortiClientVPNSetup_6.4.6.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_6.4.6.xxxx_x64.exe	Free VPN-only installer (64-bit).



Review the following sections prior to installing FortiClient version 6.4.6: [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 6.4.6, do one of the following:

- Deploy FortiClient 6.4.6 as an upgrade from EMS
- Manually uninstall existing FortiClient version from the device, then install FortiClient (Windows) 6.4.6

FortiClient (Windows) 6.4.6 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) 6.4.6 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 6.4.6 product integration and support information:

<b>Desktop operating systems</b>	<ul style="list-style-type: none"><li>• Microsoft Windows 10 (32-bit and 64-bit)</li><li>• Microsoft Windows 8.1 (32-bit and 64-bit)</li><li>• Microsoft Windows 7 (32-bit and 64-bit)</li></ul> <p>FortiClient 6.4.6 does not support Microsoft Windows XP and Microsoft Windows Vista.</p>
<b>Server operating systems</b>	<ul style="list-style-type: none"><li>• Microsoft Windows Server 2019</li><li>• Microsoft Windows Server 2016</li><li>• Microsoft Windows Server 2012 R2</li><li>• Microsoft Windows Server 2012</li><li>• Microsoft Windows Server 2008 R2</li></ul> <p>FortiClient 6.4.6 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>
<b>Embedded system operating systems</b>	Microsoft Windows 10 IoT Enterprise LTSC 2019
<b>Minimum system requirements</b>	<ul style="list-style-type: none"><li>• Microsoft Windows-compatible computer with Intel processor or equivalent. FortiClient (Windows) does not support ARM-based processors.</li><li>• Compatible operating system and minimum 512 MB RAM</li><li>• 600 MB free hard disk space</li><li>• Native Microsoft TCP/IP communication protocol</li><li>• Native Microsoft PPP dialer for dialup connections</li><li>• Ethernet network interface controller (NIC) for network connections</li><li>• Wireless adapter for wireless network connections</li><li>• Adobe Acrobat Reader for viewing FortiClient documentation</li><li>• Windows Installer MSI installer 3.0 or later</li></ul>
<b>AV engine</b>	<ul style="list-style-type: none"><li>• 6.00258</li></ul>
<b>FortiAnalyzer</b>	<ul style="list-style-type: none"><li>• 7.0.0 and later</li><li>• 6.4.0 and later</li></ul>
<b>FortiAuthenticator</b>	<ul style="list-style-type: none"><li>• 6.3.0 and later</li><li>• 6.2.0 and later</li><li>• 6.1.0 and later</li><li>• 6.0.0 and later</li></ul>
<b>FortiClient EMS</b>	<ul style="list-style-type: none"><li>• 7.0.0 and later</li><li>• 6.4.1 and later</li></ul>

<b>FortiManager</b>	<ul style="list-style-type: none"> <li>6.4.0 and later</li> </ul>
<b>FortiOS</b>	<p>The following FortiOS versions support IPsec and SSL VPN with FortiClient (Windows) 6.4.6:</p> <ul style="list-style-type: none"> <li>7.0.0 and later</li> <li>6.4.0 and later</li> <li>6.2.0 and later</li> <li>6.0.0 and later</li> </ul> <p>The following FortiOS versions support endpoint control with FortiClient (Windows) 6.4.6:</p> <ul style="list-style-type: none"> <li>6.2.0 and later</li> </ul>
<b>FortiSandbox</b>	<ul style="list-style-type: none"> <li>4.0.0 and later</li> <li>3.2.0 and later</li> <li>3.1.0 and later</li> </ul>

## 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.



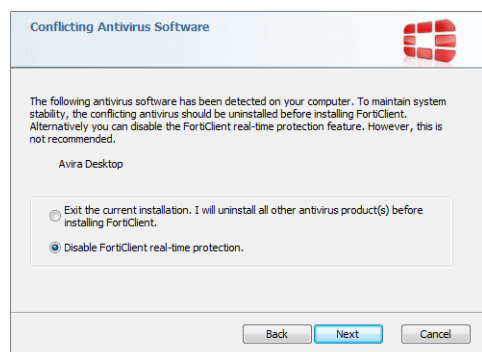
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

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

Bug ID	Description
727224	FortiClient (Windows) stays in syncing state forever and fails to disconnect after manual in-place upgrade.
728114	Telemetry status is stuck on syncing after in-place upgrade.

## Known issues

The following issues have been identified in FortiClient (Windows) 6.4.6. 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 <code>norestart</code> parameter requests reboot.

## Endpoint control

Bug ID	Description
723495	FortiClient loses connectivity to EMS when invitation code used for initial registration is deleted from FortiClient Cloud.
724038	Zero Trust tagging rule does not work properly for Active Directory (AD) joined devices.
728739	Client receives <code>ERROR   5  </code> on default site and disconnects unexpectedly.
731525	FortiClient (Windows) does not properly detect Zero Trust tag that requires endpoint to not have up-to-date antivirus (AV).

## GUI

Bug ID	Description
665426	SAML SSL VPN in tunnel mode is broken when using AD Federation Services and Duo multifactor authentication solution.
689744	FortiClient (Windows) only displays VPN tunnel name after FortiClient (Windows) adds new IPsec VPN tunnels.
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 <i>Endpoints</i> table.
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 does not register to EMS after silent installation.

## Malware Protection and Sandbox

Bug ID	Description
516704	AV 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.
729210	Sandbox statistics accumulate over time.
729457	AV feature causes task windows issue.
730172	FortiClient causes VMware Horizon Agent to disconnect from VMware Connection Server.
730725	Antiransomware feature fails to detect Sodinokibi Kaseya ransomware virus.

## Remote Access

Bug ID	Description
637303	Certificate-only SSL VPN tunnel displays popup with <i>Empty username is not allowed</i> 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 <i>Failed to launch IPsec service</i> .
709001	SSL VPN host check validation does not work for SAML user.
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.
723465	Profiles do not sync when using IPsec VPN phase 2 configuration.
723632	VPN icon does not display lock after connecting to IPsec VPN tunnel.
724092	<code>match_type</code> does not work when using VPN before logon.
725630	Upgrade converts wildcard certificate filter to simple certificate filter.
727098	FortiClient (Windows) appears disconnected when trying to connect to SSL VPN.

Bug ID	Description
727695	On Windows 10, FortiClient (Windows) fails to block SSL VPN when it is applicable for the prohibit host tag.
729610	FortiClient (Windows) incorrectly saves encrypted password when customer uses Spanish characters and save username and password are enabled.
729634	Issues in resolving internal sites when connected to SSL VPN.

## 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.
725852	FortiClient (Windows) does not block malicious websites when real-time protection is enabled but Web Filter is disabled.
729753	FortiClient (Windows) sends Web Filter traffic to FortiGuard server continuously.

## 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.
725631	Network interfaces on Windows 10 laptops stay unavailable after hibernation or sleep.
725710	FortiSSOMA does not send user identities to FortiAuthenticator.



**FORTINET®**



Copyright© 2021 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.