FortiClient (Windows) - Release Notes

Version 6.0.10

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://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

December 11, 2020
FortiClient (Windows) 6.0.10 Release Notes
04-6010-659098-20201211

TABLE OF CONTENTS

Introduction **4**
Licensing 4
Standalone mode 4
Managed mode 4
Special notices **6**
Nested VPN tunnels 6
Microsoft Windows Server support 6
FortiClient Rebranding Tool not supported 6
HP Velocity and Application Firewall 6
Installation information **7**
Firmware images and tools 7
Installation options 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 antivirus products 11
Resolved issues **12**
Malware Protection 12
Remote Access 12
Compliance 12
GUI 13
FortiAnalyzer 13
Other 13
Known issues **14**
Endpoint control 14
Application Firewall 14
Remote Access 14
Change log **15**

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 6.0.10 build 0297.

- 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 offers two licensing modes:

- Standalone mode
- Managed mode

Standalone mode

In standalone mode, FortiClient is not connected to a FortiGate or FortiClient Enterprise Management Server (EMS). In this mode, FortiClient is free for private individuals and commercial businesses to use. No license is required.

Support for FortiClient in standalone mode is provided on the Fortinet Forums (forum.fortinet.com). Phone support is not provided.

Managed mode

Companies with large installations of FortiClient usually need a means to manage their endpoints. EMS can be used to provision and centrally manage FortiClient endpoints, and FortiGate can be used with FortiClient endpoints for network security. Each FortiClient endpoint can connect to a FortiGate or an EMS. In this mode, FortiClient licensing is applied to the FortiGate or EMS. No separate license is required on FortiClient itself.

When using the ten free trial licenses for FortiClient in managed mode, support is provided on the Fortinet Forums. Phone support is not provided when using the free trial licenses. Phone support is provided for paid licenses.

FortiClient licenses on the FortiGate

FortiGate 30 series and higher models include a FortiClient free trial license for ten connected FortiClient endpoints. For additional connected endpoints, you must purchase a FortiClient license subscription. Contact your Fortinet sales representative for information about FortiClient licenses.

FortiClient licenses on the EMS

EMS includes a FortiClient free trial license for ten connected FortiClient endpoints for evaluation. For additional connected endpoints, you must purchase a FortiClient license subscription. Contact your Fortinet sales representative for information about FortiClient licenses.

Special notices

Nested VPN tunnels

FortiClient (Windows) does not support parallel, independent VPN connections to different sites. However, you may still establish FortiClient VPN connection over existing third-party (for example, AT&T Client) VPN connection (nested tunnels).

Microsoft Windows Server support

FortiClient (Windows) supports the AV and Vulnerability Scan features for Microsoft Servers.

FortiClient Rebranding Tool not supported

FortiClient (Windows) 6.0.10 does not support the FortiClient Rebranding Tool.

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.

Installation information

Firmware images and tools

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

File	Description
FortiClientSetup_6.0.10.xxxx.exe	Standard installer for Microsoft Windows (32-bit)
FortiClientSetup_6.0.10.xxxx.zip	Zip package containing FortiClient.msi and language transforms for Microsoft Windows (32-bit). You can customize some of the MSI package's properties with FortiClient Configurator Tool.
FortiClientSetup_6.0.10.xxxx_x64.exe	Standard installer for Microsoft Windows (64-bit)
FortiClientSetup_6.0.10.xxxx_x64.zip	Zip package containing FortiClient.msi and language transforms for Microsoft Windows (64-bit). You can customize some of the MSI package's properties with FortiClient Configurator Tool.
FortiClientTools_6.0.10.xxxx.zip	Zip package containing miscellaneous tools, including VPN automation files.

The following tools and files are available in the FortiClientTools_6.0.10.xxxx.zip file:

File	Description
FortiClientVirusCleaner	Virus cleaner
OnlineInstaller	This file downloads and installs the latest FortiClient file from the public FDS.
SSLVPNcmdline	Command line SSL VPN client
SupportUtils	Includes diagnostic, uninstallation, and reinstallation tools
VPNAutomation	VPN automation tool

Review the following sections prior to installing FortiClient 6.0.10: Introduction on page 4, Special notices on page 6, and Product integration and support on page 9.

Installation options

When installing FortiClient version 6.0.10, you can choose the setup type that best suits your needs. FortiClient always installs the Fortinet Security Fabric Agent (SFA) feature and enables the Vulnerability Scan feature by default. You can

select to install one or more of the following options:

- Secure Remote Access: VPN components (IPsec and SSL) will be installed.
- Advanced Persistent Threat (APT) Components: FortiSandbox detection and quarantine features will be installed.
- Additional Security Features: Select one or more of the following to install them: AntiVirus, Web Filtering, Single Sign On, Application Firewall

It is recommended to not install VPN components on Windows Server systems if not required.

Upgrading from previous FortiClient versions

FortiClient version 6.0.10 supports upgrade from FortiClient versions 5.4 and later.

If you are deploying an upgrade from FortiClient 5.6.2 or earlier versions via FortiClient EMS and the upgrade fails, uninstall FortiClient on the endpoints, then deploy the latest version of FortiClient.

Downgrading to previous versions

Downgrading FortiClient version 6.0.10 to previous FortiClient versions is not supported.

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 on *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 6.0.10 product integration and support information:

Desktop operating systems	• Microsoft Windows 10 (32-bit and 64-bit) • Microsoft Windows 8, 8.1 (32-bit and 64-bit) • Microsoft Windows 7 (32-bit and 64-bit) FortiClient 6.0.10 does not support Microsoft Windows XP and Microsoft Windows Vista.
Server operating systems	• Microsoft Windows Server 2008 R2 or newer FortiClient 6.0.10 does not support Windows Server Core.
Minimum system requirements	• Microsoft Windows-compatible computer with Intel processor or equivalent • 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 version 3.0 or later
FortiAnalyzer	• 6.2.0 and later • 6.0.0 and later • 5.6.0 and later
FortiAuthenticator	• 4.3.1 • 4.3.0 • 4.2.1 FortiClient (Windows) does not support FortiToken Mobile push notification for the following versions: • 4.2.0 • 4.1.0 and later • 3.3.0 and later • 3.2.0 and later • 3.1.0 and later • 3.0.0 and later
FortiClient EMS	• 6.2.0 and later • 6.0.0 and later
FortiManager	• 6.2.0 and later • 6.0.0 and later • 5.6.0 and later
FortiOS	• 6.0.0 and later • 5.6.0 and later

	FortiClient (Windows) only supports IPsec VPN and SSL VPN with the following FortiOS versions: • 6.2.0 and later • 5.4.0 and later
FortiSandbox	• 3.1.0 and later • 3.0.0 and later • 2.5.0 and later FortiClient (Windows) does support the following version, but you may need to disable FortiClient authorization. To disable authorization, run the `device-authorization -f` command in the FortiSandbox CLI. • 2.4.0 and later The following supported versions do not offer FortiClient authorization: • 2.3.0 and later • 2.2.0 and later • 2.1.0

Language support

The following table lists FortiClient language support information.

Language	Graphical user interface	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.

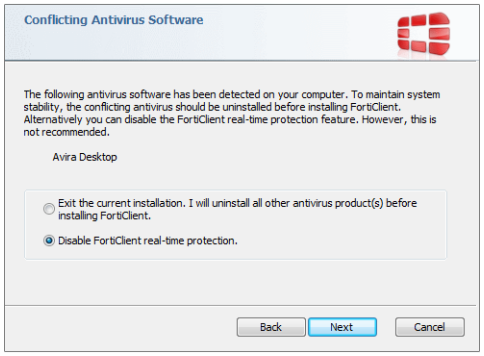
If the client workstation is configured to a regional language setting that FortiClient does not support, FortiClient defaults to English.

Conflicts with third party antivirus products

The antivirus (AV) feature in FortiClient is known to conflict with other similar products in the market.

- FortiClient's AV feature should not be used with other AV products.
- If not using FortiClient's AV feature, the FortiClient installation folder should be excluded from scanning for the third party AV product.

During a new installation of FortiClient, the installer will search for other registered third party software and, if any is found, warn 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 6.0.10. For inquiries about a particular bug, contact Customer Service & Support.

Malware Protection

Bug ID	Description
599118	Virtual machines crash when a third-party application is running and FortiClient real-time scan is enabled.

Remote Access

Bug ID	Description
513932	FortiClient (Windows) does not send CERT payload during IKEv2 certificate authentication.
599924	Certificate-based IKEv2 cannot connect with EAP disabled.
621313	Microsoft Teams cannot make voice calls over FortiClient IPsec VPN full tunnel.
634300	Windows crashes due to fortips.sys process.
634346	DNS queries on LAN interface and dialup interface.
645110	FortiClient (Windows) changes VPN name to primary VPN name in various cases.
658802	IPsec VPN settings do not save correctly.

Compliance

Bug ID	Description
600838	Erratic behavior for compliance enforcement when endpoint connects over SSL VPN.

GUI

Bug ID	Description
557381	FortiClient (Windows) fails to open when clicking the tray icon.

FortiAnalyzer

Bug ID	Description
601725	FortiClient should send full URL, such as - http://www.google.com/maps/, to FortiAnalyzer.

Other

Bug ID	Description
534194	fcdblog rewrites hosts file without any changes.
576632	System processes should not create temp files with predictable names.
611821	FortiClient (Windows) mishandles special character, such as %, in new password.

Common vulnerabilities and exposures

Bug ID	Description
576632	FortiClient (Windows) is no longer vulnerable to the following CVE Reference: • CVE-2020-9291 Visit https://fortiguard.com/psirt for more information.

Known issues

The following issues have been identified in FortiClient (Windows) 6.0.10. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Endpoint control

Bug ID	Description
554998	FortiClient (Windows) local records are removed after EMS deploys new FortiClient (Windows).
586894	FortiESNAC.exe high memory usage.

Application Firewall

Bug ID	Description
593493	fortifws crash in ntdll.

Remote Access

Bug ID	Description
590462	FortiClient (Windows) loses DNS settings after disconnecting SSL VPN.
551183	IPsec VPN autoconnect on reboot does not work on Windows 8.1.

Change log

Date	Change Description
2020-09-08	Initial release.
2020-12-11	Added Common vulnerabilities and exposures on page 13.

Copyright© 2020 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.