FortiClient (Windows) - Release Notes

Version 6.0.6

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 COOKBOOK
https://cookbook.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

May 16, 2019
FortiClient (Windows) 6.0.6 Release Notes
04-606-554675-20190516

TABLE OF CONTENTS

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 6.0.6 build 0242.

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) 6.0.6 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_6.0.6.xxxx.exe	Standard installer for Microsoft Windows (32-bit)
FortiClientSetup_6.0.6.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_6.0.6.xxxx_x64.exe	Standard installer for Microsoft Windows (64-bit)
FortiClientSetup_6.0.6.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_6.0.6.xxxx.zip	Zip package containing miscellaneous tools, including VPN automation files

The following tools and files are available in the FortiClientTools_6.0.6.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 6.0.6: Introduction on page 4, Special notices on page 6, and Product integration and support on page 9.

Installation options

When installing FortiClient version 6.0.6, 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 6.0.6 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 6.0.6 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

FortiClient 6.0.6 support information

The following table lists version 6.0.6 product integration and support information:

Desktop operating systems	• Microsoft Windows 7 (32-bit and 64-bit) • Microsoft Windows 8, 8.1 (32-bit and 64-bit) • Microsoft Windows 10 (32-bit and 64-bit) FortiClient 6.0.6 does not support Microsoft Windows XP and Microsoft Windows Vista.
Server operating systems	• Microsoft Windows Server 2008 R2 or newer FortiClient 6.0.6 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.

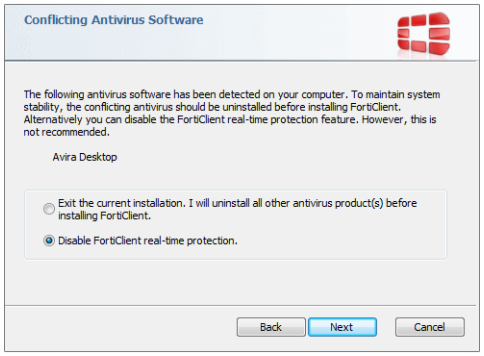
If the client workstation is configured to a regional language setting that FortiClient does not support, FortiClient defaults to English.

Conflicts with third party antivirus products

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

- FortiClient's antivirus feature should not be used with other AV products.
- If not using FortiClient's antivirus 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 6.0.6. For inquiries about a particular bug, contact Customer Service & Support.

Endpoint control

Bug ID	Description
538267	FortiClient (Windows) fails to create a scheduled vcm scan when EMS has enabled the maintenance setting.
553977	FortiClient (Windows) always sends previous avatar image to EMS when using the OS avatar.
554236	FortiClient (Windows) reports that it is connected to the FortiGate after the FortiGate changes the registration port.

Malware Protection

Bug ID	Description
460508	FortiClient does not run AV scan upon USB insertion after reboot.
460980	Sandbox still submits and quarantines files in the Sandbox exclusion list (network drive).
513213	AntiExploit Engine blocks legitimate applications.
516841	Sandbox still holds files with sizes larger than 200 MB until timeout.
548918	FortiClient AV causes high CPU usage on endpoints.
550607	FortiClient AV feature reports back to EMS as enabled when it is hidden.

Web Filter

Bug ID	Description
529450	FortiClient shows *Unrated* for HTTPS sites while it shows the correct category for HTTP sites.
546525	FortiClient (Windows) blocks web traffic due to two FortiProxy services running at the same time.

Application Firewall

Bug ID	Description
526997	Application Firewall blocks web-based applications and lsass.exe and flags them as Psiphon.
538780	FortiClient prevents Google file stream from running properly and causes high CPU and memory usage.

Remote Access

Bug ID	Description
520808	FortiClient fails certificate validation due to an ignored intermediate certificate authority.
525449	A JavaScript error occurs while connecting to VPN. The issue occurs due to an admin roaming profile.
525542	After laptop boot or wakeup, FortiClient (Windows) tries to autoconnect even though it is onnet.
532068	FortiClient cannot see the certificate when the certificate subject contain diacritics.
534650	`<allow_standard_user_use_system_cert>` does not work for SSL IPv6.
534814	FortiClient (Windows) fails to install multiple IPv4 split tunnel routes.
534845	FortiClient (Windows) does not show certificate dropdown after restore.
535114	The user is unable to select a user certificate when reconnecting to a managed SSL VPN profile.
537091	FortiClient (Windows) only allows twelve seconds to key in the token when using a multiple gateway setup and connecting to SSL VPN with 2FA enabled.
537559	Password change does not work for IPsec dialup users with two-factor authentication (2FA) enabled.
539387	VPN autodial does not work when using the domain name to register to EMS.
540588	Windows 10 hosts file gets garbled letters and grows larger with SSL VPN remote traffic.
541420	The user cannot log into Windows after enabling VPN before logon.
541424	VPN *autoconnect only when off-net* issue when EMS packages the installer.
549311	VPN before logon using only LDAP-integrated certificates does not connect.
551236	Default route is missing after connecting IPsec VPN with FortiOS 5.6.X.
551538	Onnet FortiClient triggers VPN autoconnect after system reboot even when *autoconnect only when offnet* is enabled.
551919	Fails to reconnect from FortiTray if username has backslash or domain user format.

Vulnerability Scan

Bug ID	Description
534954	FortiClient fails to use *Install Selected* to patch OS vulnerabilities.
547482	Java Runtime Environment vulnerability exemption does not exempt endpoints from compliance.

Install and upgrade

Bug ID	Description
510748	If FortiClient (Windows) is installed on a different drive (E:\), manual upgrade to 6.0.x completes but FortiClient (Windows) does not work after reboot.
551586	EMS uninstaller fails to remove all FortiClient files and registry in HKCU.
557098	FortiClient (Windows) online installer failed to trigger AV scan on clean system.

Other

Bug ID	Description
450181	FortiClient makes connections to FortiGuard servers even when Web Filter/FortiProxy are disabled.
494257	The user cannot execute FortiClientVirusCleaner in the tool set.
513311	FortiAptFilter causes a blue screen of death.
545427	FortiClient scheduled daily update from Micro-FortiGuard Server for FortiClient communicates to Micro-FortiGuard Server for FortiClient very frequently.
553328	FortiClientOfflineVirusCleaner issue.

Common vulnerabilities and exposures

Bug ID	Description
433685	FortiClient (Windows) is no longer vulnerable to the following CVE reference: • 2019-5589 Visit https://fortiguard.com/psirt for more information.

Known issues

The following issues have been identified in FortiClient (Windows) 6.0.6. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Malware Protection

Bug ID	Description
535604	AntiExploit causes application crashing without block message.

Remote Access

Bug ID	Description
538024	FortiClient (Windows) loses DNS settings after disconnecting IPsec VPN.
551754	*VPN connection failed* error when switching between offnet and onnet networks.

Vulnerability Scan

Bug ID	Description
537016	Vulnerability Scan does not always scan on next startup if off during scheduled scan time.

Install and upgrade

Bug ID	Description
554998	FortiClient (Windows) local records are removed after EMS deploys new FortiClient (Windows).

Other

Bug ID	Description
534194	fcdblog rewrites hosts file without changes.
540455	FortiClient System Tray Controller uses high memory and CPU.

Change log

Date	Change Description
2019-05-15	Initial release.
2019-05-16	Removed 557461 from Known issues on page 15.