FortiClient (Windows) - Release Notes

Version 6.0.2

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
http://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: techdocs@fortinet.com

September 10, 2018
FortiClient (Windows) 6.0.2 Release Notes
04-602-509679-20180910

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-09-07	Initial release of FortiClient (Windows) 6.0.2.
2018-09-10	Added 506334 to Resolved Issues on page 15.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 6.0.2 build 0128.

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 (10) free licenses for FortiClient in managed mode, support is provided on the Fortinet Forums (forum.fortinet.com). Phone support is not provided when using the free licenses. Phone support is provided for paid licenses.

FortiClient licenses on the FortiGate

FortiGate 30 series and higher models include a FortiClient license for ten (10) free, 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 license for ten (10) free, 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

Microsoft Windows updates related to CPU security flaw (Meltdown)

Microsoft Windows updates may not occur due to a CPU security flaw (Meltdown) with anti-virus products installed. Please read the customer service bulletin CSB-180105-1 at https://support.fortinet.com/Information/Bulletin.aspx. A PDF of the bulletin can be downloaded from the firmware download directory of the Fortinet support site at https://support.fortinet.com.

Nested VPN tunnels

Parallel, independent VPN connections to different sites are not supported; however, FortiClient VPN connection may still be established over existing third-party (for example, AT&T Client) VPN connection (nested tunnels).

SSL VPN 98% issues

The new SSL VPN Windows driver, which was first introduced in FortiClient 5.6.0, resolves various SSL VPN connection issues. The new driver will help increase performance by up to 20% and provide a stable VPN connection.

Latency or poor network connectivity can affect the FortiClient SSL VPN connection. To further help avoid timeouts, the login timeout on the FortiGate can be increased to 180 seconds using the following CLI command:

```
configure vpl ssl settings
   set log-in timeout 180
```

Windows notification of AV being disabled

In FortiClient 6.0.2, FortiClient will notify *Windows Security Center Antivirus is Down* only when FortiClient Antivirus has really stopped running.

Local certificate store not supported

FortiClient (Windows) no longer supports the local certificate store, and it is recommended you use Windows Certificates Store instead. If you are currently using the local certificate store, you should transition to Windows Certificates Store before upgrading to FortiClient (Windows) 6.0.2.

Microsoft Windows server support

For Microsoft Windows servers, the AntiVirus and Vulnerability Scan features for FortiClient are supported.

Rebranding tool not supported

FortiClient (Windows) 6.0.2 does not support the FortiClient Rebranding Tool.

Installation Information

Firmware images and tools

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

File	Description
FortiClientSetup_6.0.xx.xxxx.exe	Standard installer for Microsoft Windows (32-bit)
FortiClientSetup_6.0.xx.xxxx.zip	A zip package containing FortiClient.msi and language transforms for Microsoft Windows (32-bit). Some properties of the MSI package can be customized with FortiClient Configurator tool
FortiClientSetup_6.0.xx.xxxx_x64.exe	Standard installer for Microsoft Windows (64-bit)
FortiClientSetup_6.0.xx.xxxx_x64.zip	A zip package containing FortiClient.msi and language transforms for Microsoft Windows (64-bit). Some properties of the MSI package can be customized with FortiClient Configurator tool
FortiClientTools_6.0.xx.xxxx.zip	A zip package containing miscellaneous tools, including VPN Automation files

The following tools and files are available in the FortiClientTools_6.0.xx.xxxx.zip file:

File	Description
FortiClientVirusCleaner	A 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	A VPN automation tool

Please review the following sections prior to installing FortiClient version 6.0.2: Introduction on page 6, Special Notices on page 8, and Product Integration and Support on page 12.

Installation options

When installing FortiClient version 6.0.2, you can choose the setup type that best suits your needs. FortiClient will always install the Fortinet Security Fabric Agent (SFA) feature and enable 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 6.0.2 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 6.0.2 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 located at https://support.fortinet.com. 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 6.0.2 support

The following table lists version 6.0.2 product integration and support information.

FortiClient 6.0.2 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 6.0.2 does not support Microsoft Windows XP and Microsoft Windows Vista.
Server Operating Systems	• Microsoft Windows Server 2008 R2 or newer FortiClient 6.0.2 does not support Windows Server Core.
Minimum System Requirements	• Microsoft Windows compatible computer with Intel processor or equivalent • Compatible operating system and minimum 512MB RAM • 600MB free hard disk space • Native Microsoft TCP/IP communication protocol • Native Microsoft PPP dialer for dial-up 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	• 6.0.0 and later • 5.6.0 and later
FortiAuthenticator	• 4.3.1 • 4.3.0 • 4.2.1 FortiToken Mobile push notification is not supported 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	• 6.0.0 and later

FortiManager	• 6.0.0 and later • 5.6.0 and later
FortiOS	• 6.0.0 and later • 5.6.0 and later Only IPsec VPN and SSL VPN are supported with the following FortiOS versions: • 5.4.0 and later
FortiSandbox	• 3.0.0 • 2.5.0 and later The following version is supported, but may require authorization of FortiClient to be disabled. To disable authorization run the FortiSandbox CLI command: `device-authorization -f` • 2.4.0 and later The following supported versions do not offer authorization of FortiClient: • 2.3.0 and later • 2.2.0 and later • 2.1.0

Language support

The following table lists FortiClient language support information.

FortiClient language support

Language	Graphical user interface	XML configuration	Documentation
English	✔	✔	✔
Chinese (simplified)	✔		
Chinese (traditional)	✔		
French (France)	✔		
German	✔		
Japanese	✔		
Korean	✔		
Portuguese (Brazil)	✔		
Russian	✔		
Spanish (Spain)	✔		

The FortiClient language setting defaults to the regional language setting configured on the client workstation, unless configured in the XML configuration file.

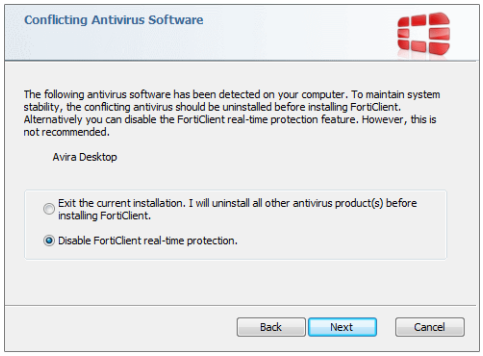
If the client workstation is configured to a regional language setting that is not supported by FortiClient, it defaults to English.

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 6.0.2. For inquiries about a particular bug, please contact Customer Service & Support.

Endpoint Control

Bug ID	Description
501452	Vulnerability scanner/patch does not work if triggered from EMS.

Malware Protection

Bug ID	Description
462163	Scheduled AV scan consumes a lot of resources.

Application Firewall

Bug ID	Description
503650	Unable to add Edonkey key signature in Application Firewall.

Remote Access

Bug ID	Description
468288	Randomly after IPsec VPN is disconnected, the DNS setting will not change back to the original setting in the adapter.
471234	Some inconvenience with current per user password design for both SSL and IPSec.
479236	FortiClient has issue with two factor authentication using Yubikey as 2FA for IPsec.
495325	FortiClient 6.0.0 VPN auto-connect feature not working properly.

Bug ID	Description
504708	Improve implementation for *Always Up*, *Auto connect*, and *Save Password*.
505191	Remote Access (IPsec) loses saved username/password when upgrading to 6.0.0.
506334	FortiClient console opens constantly when connected to VPN.
507024	Microsoft Visual C++ Runtime error when logging into FortiClient using FTM push.
507516	Resolve *Save Password*, *Auto Connect*, and *Always Up* issues.

Vulnerability Scan

Bug ID	Description
467328	FortiClient log for vulnerability scan should include file path.

GUI

Bug ID	Description
498527	GUI does not show IP address for IPSec VPN when it is connected.
506713	FortiClient windows stay open in taskbar after connecting to VPN.

Install and upgrade

Bug ID	Description
479229	After upgrading FortiClient (Windows) from 5.6.4 to 5.6.6, AV scan history is lost.
496895	When using EMS to upgrade FortiClient (Windows) from 5.6 to 6.0.0, installer waits until someone logs in to start.
496895	When using EMS to upgrade FortiClient (Windows) from 5.6 to 6.0.0, installer creates lots of empty folders in C:\Windows\TEMP\.

Other

Bug ID	Description
492704	FortiAnalyzer-VM64-AWS does not show all FortiClient logs.

Known Issues

The following issues have been identified in FortiClient (Windows) 6.0.2. For inquiries about a particular bug or to report a bug, please contact Customer Service & Support.

Malware Protection

Bug ID	Description
481003	FortiClient causing longer logon time to terminal server(Citrix) for first user.
483523	Black screen for a few minutes after login/logoff.
489052	Memory leak caused by FortiAptFilter.sys.
495880	Non-admin domain users can stop/pause USB media scans enforced by EMS configuration.
496084	AV exclusion list does not work in on-demand scan if %windir% or %systemroot% variables are used.
496326	FortiClient is sending intermittently files from local disk to the FortiSandbox for analysis.
499891	Scan on insertion does not work all the time.
509624	Newly installed FortiClient with RTP enabled does not disable Windows Defender's Real Time Protection on Windows 7.

Web Filter

Bug ID	Description
489821	FortiClient 5.6.6 and Windows 8.1 SSL error.

Application Firewall

Bug ID	Description
482920	FortiClient blocking DF set response.
509128	FortiClient 6.0.1 Application Firewall is blocking Avaya.

Remote Access

Bug ID	Description
450245	Need to add a switch for the number of auto-connect retries.
472223	Unable to select certificate for SSL VPN.
486362	FortiClient 5.6.6 disables Windows IKE and AuthIP IPsec keying modules when connecting the VPN which effects MS direct access.
491407	FortiClient AutoConnect when Offnet not working (IPsec certificate).
510060	*Save password*, *Auto-connect*, *Always up* checkboxes do not display after IPsec VPN is disconnected.
510735	6.0.2 RC1 fails to connect to VPN from task tray with user cert authentication - it prompts for certificate
510748	If FortiClient 5.6.x is installed on a different drive (E:\) manual upgrade to 6.0.x will complete but FortiClient does not work after reboot.
511291	FortiClient reports signature to be out of date if it updated to the signature more than x days ago, regardless of version.

GUI

Bug ID	Description
492890	FortiClient malware GUI says malware is quarantined when in fact it is not.
510945	Right-click is not working for Username and Password VPN fields.

Install and upgrade

Bug ID	Description
497115	GUI is blank after installation on certain locales (localisation issues).
497387	FortiClient Configurator should support automatic group assignment.
505191	Remote Access (IPsec VPN) loses saved username/password when upgrading to 6.0.0

Other

Bug ID	Description
488842	Total uninstall 6.22.1 completely removing managed FortiClient.