

FortiClient (Windows) - Release Notes

Version 5.6.6

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



March 29, 2018

FortiClient (Windows) 5.6.6 Release Notes

04-566-475024-20180329

TABLE OF CONTENTS

Change Log	4
Introduction	5
Licensing	5
Standalone mode	5
Managed mode	5
Special Notices	7
Microsoft Windows updates related to CPU security flaw (Meltdown)	7
Nested VPN tunnels	7
SSL VPN 98% issues	7
Windows notification of AV being disabled	7
Local certificate store not supported	7
Microsoft Windows server support	8
User password renewal over SSL VPN with FortiOS 6.0.0	8
Installation Information	9
Firmware images and tools	9
Installation options	10
Upgrading from previous FortiClient versions	10
Downgrading to previous versions	10
Firmware image checksums	10
Product Integration and Support	11
FortiClient 5.6.6 support	11
Language support	12
Conflicts with third party antivirus products	13
Resolved Issues	14
Known Issues	15

Change Log

Date	Change Description
2018-03-08	Initial release of FortiClient (Windows) 5.6.6.
2018-03-12	Added detail in Installation Information on page 9.
2018-03-29	Added special notice about FortiOS 6.0.0 compatibility when using SSL VPN.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 5.6.6 build 1167.

- [Special Notices](#)
- [Installation Information](#)
- [Product Integration and Support](#)
- [Resolved Issues](#)
- [Known Issues](#)

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:

```
config vpn ssl settings
  set login-timeout 180
end
```

Windows notification of AV being disabled

In FortiClient 5.6.6, 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 recommend that 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) 5.6.6.

Microsoft Windows server support

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

User password renewal over SSL VPN with FortiOS 6.0.0

With FortiOS 6.0.0, if the FortiGate local user has a FortiToken assigned and the password is expiring and needs renewal, FortiClient (Windows) will not be able to connect. If FortiGate SSL has the web portal enabled, the user can renew their password over the web portal, then connect with FortiClient.

Installation Information

Firmware images and tools

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

File	Description
FortiClientSetup_5.6.xx.xxxx.exe	Standard installer for Microsoft Windows (32-bit)
FortiClientSetup_5.6.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_5.6.xx.xxxx_x64.exe	Standard installer for Microsoft Windows (64-bit)
FortiClientSetup_5.6.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_5.6.xx.xxxx.zip	A zip package containing miscellaneous tools, including VPN Automation files

The following tools and files are available in the FortiClientTools_5.6.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 5.6.6: [Introduction on page 5](#), [Special Notices on page 7](#), and [Product Integration and Support on page 11](#).

Installation options

When installing FortiClient version 5.6.6, you can choose the setup type that best suits your needs. FortiClient will always install the 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

Upgrading from previous FortiClient versions

FortiClient version 5.6.6 supports upgrade from FortiClient versions 5.2 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 5.6.6 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 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 5.6.6 support

The following table lists version 5.6.6 product integration and support information.

FortiClient 5.6.6 support information

Desktop Operating Systems	<ul style="list-style-type: none">• 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) <p>FortiClient 5.6.6 does not support Microsoft Windows XP and Microsoft Windows Vista.</p>
Server Operating Systems	<ul style="list-style-type: none">• Microsoft Windows Server 2008 R2 or newer <p>FortiClient 5.6.6 does not support Windows Server Core.</p>
Minimum System Requirements	<ul style="list-style-type: none">• Microsoft Internet Explorer version 8 or later• 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 FortiClient documentation• Windows Installer MSI installer version 3.0 or later.
FortiAnalyzer	<ul style="list-style-type: none">• 5.6.0 and later
FortiAuthenticator	<ul style="list-style-type: none">• 4.3.1• 4.3.0• 4.2.1 <p>FortiToken Mobile push notification is not supported for the following versions:</p> <ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 1.2.0 and later
FortiManager	<ul style="list-style-type: none">• 5.6.0 and later

FortiOS

- 5.6.0 and later

Only IPsec VPN and SSL VPN are supported with the following FortiOS versions:

- 5.4.0 and later

FortiSandbox

- 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.

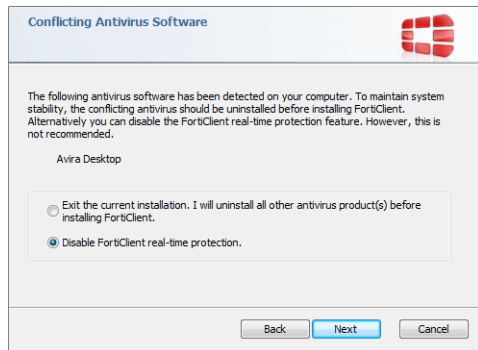


If the client workstation is configured to a regional language setting that is not supported by FortiClient, it defaults to English.

Conflicts with third party antivirus products

The antivirus feature in FortiClient is known to conflict with other similar products in the market. Consider removing other antivirus programs before installing FortiClient.

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

Bug ID	Description
411137	Cannot exclude UNC paths from scans .
421900	High CPU usage with fmon.exe.
443832	High CPU and freeze due to AV exclusions.
457439	AV real-time protection exclusion list with variables does not exclude all login users in terminal server.
457445	fmon high CPU and big latency in Citrix server.

Known Issues

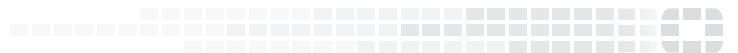
The following issues have been identified in FortiClient (Windows) 5.6.6. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

Bug ID	Description
414476	AV network scan slowing down applications that rely on network resources.
439903	Webfilter settings from EMS are lost after some time.
440844	B1075 - FortiClient SSL VPN connection fails at 98% - Works after the 1st attempt.
444108	Could not whitelist quarantined files while registered to EMS.
445504	The <i>Show VPN before Logon</i> menu may fail to appear before logon. Workaround: Reboot the computer after the option is enabled.
448485	b1075: Change onnet/offnet status discovery for dual registration case.
449596	FortiClient does not follow the same remediation action taken by FortiSandbox for low risk files.
450245	Need to add a switch for the number of auto-connect retries.
451605	b0394: EMS reports NPAPI Flash Plug-in vulnerable while not installed.
451976	FortiClient 5.6.0 FW is slowing down file transfers AV with "block known communication channels" and application firewall enable.
458489	Sandbox scanning is not working properly scanning files on Edge and IE (overlap bypass folder and missing dynamic bypass).
458793	Error messages presented by office and outlook when sandbox scanning is enabled.
460245	[Profiles][Antivirus] Split Block Malicious Websites into subcategories.
460315	FortiClient 98% failure recurring. If using FortiOS 5.6, consider increasing SSL VPN login-timeout as follows: <pre>config vpn ssl settings set login-timeout 180 end</pre>
461136	FortiClient can cause BSOD on Win10 when NIC configured with multiple VLANs.
462162	File sent to FortiSandbox - but no info in FortiClient.
464572	When FortiClient blocks a file for FortiSandbox inspection, the user get misleading error messages; messages show the file is corrupted.
465912	b1075: endpoints disconnect randomly from EMS, still reporting themselves as being connected.

Bug ID	Description
467095	FortiClient b1130 Wi-fi adapter failing to obtain an IP address after installing FortiClient.
467328	b1130: FortiClient log for vulnerability scan should include file path.
467525	FortiClient is causing WMI problems.
469103	SSL VPN disconnects.
469549	FortiAnalyzer is not receiving logs if SSL enabled option is selected in FortiClient.
472617	b1150 - View Details can cause issue with console GUI.
472619	b1150 - View details phone number keeps displaying "invalid characters" after correction.
472624	b1117: BSOD caused by NETIO.SYS.
473018	SSO Mobility Agent Problem.
474472	Saving images to OneDrive using Snipping Tool triggers AV detection on transient file.
474993	b1150: FortiClient cannot be compliant when AV engine is different on FCT and FOS.
475082	Microsoft direct access not detecting on-net status when VPN is connected.
475744	IPsec VPN keep running does not reconnect across network changes.
476249	Closing laptop lid while SSL VPN is connected leads to DNS servers last assigned to interfaces after VPN connection is timed out.
477139	B1150: No translation at windows login.
477140	FortiClient SSL VPN Certificate can't be changed after save password.



FORTINET®



Copyright© 2018 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.