FortiClient (Windows) - Release Notes

Version 5.6.1

November 23, 2017
FortiClient (Windows) 5.6.1 Release Notes
04-561-455040-20171123

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-11-07	Initial release of FortiClient (Windows) 5.6.1.
2017-11-10	Added the following special notice: FortiClient (Windows) 5.6.1 unavailable on page 7.
2017-11-22	Added 0408442 to *Resolved Issues*.
2017-11-23	Updated *Special Notices* by adding *Change in SSL VPN default* and updating *Transition to OS Certificate Store instead of FortiClient's local certificate store* to clarify that FortiClient (Windows) supports certificates.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 5.6.1 build 1115.

- Introduction
- Special Notices
- What’s New in FortiClient (Windows) 5.6.1
- Installation Information
- Product Integration and Support
- Resolved Issues
- Known Issues

Please 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 registered to a FortiGate or Enterprise Management Server (EMS). In this mode, FortiClient is free both 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 register 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

Change in SSL VPN default

Starting with FortiClient 5.4.4, TLS is the default used for SSL VPN when establishing a tunnel connection with FortiGate. Previously with FortiClient 5.4.0 to 5.4.3, DTLS was the default. After you upgrade to FortiClient 5.4.4, you can configure DTLS to be the default by setting the following XML element in the FortiClient configuration file: <prefer_dtls_tunnel>1<prefer_dtls_tunnel>

When <prefer_dtls_tunnel> is set to `0`, FortiClient uses TLS, even if `dtls-tunnel` is enabled on FortiGate.

When <prefer_dtls_tunnel> is set to `1`, FortiClient uses DTLS, if it is enabled on the FortiGate and tunnel establishment is successful. If `dtls-tunnel` is disabled on FortiGate, or tunnel establishment is not successful, TLS is used.

FortiClient (Windows) 5.6.1 unavailable

Due to the discovery of Mantis 0458950, FortiClient (Windows) 5.6.1 is no longer available for installation. Mantis 0458950 is fixed in FortiClient (Windows) 5.6.2. For more information, see Customer Support Bulletin CSB-171110-1 posted on the Customer Service & Support site.

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

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 the performance by up to 20% and provide a stable VPN connection.

Windows notification of AV being disabled

In FortiClient 5.6.1, FortiClient will notify *Windows Security Center Antivirus is Down* only when FortiClient Antivirus has really stopping running.

Transition to OS Certificate Store instead of FortiClient’s local certificate store

FortiClient (Windows) supports certificates using OS certificate store. However, FortiClient (Windows) no longer supports the use of FortiClient’s own local certificate store, and it is recommended that you use Windows Certificates Store instead. If you are currently using FortiClient’s local certificate store, you should transition to Windows Certificates Store before upgrading to FortiClient (Windows) 5.6.1.

Microsoft Windows server support

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

What’s New in FortiClient (Windows) 5.6.1

This section identifies the new features and enhancements in FortiClient (Windows) 5.6.1. For more information, see the *FortiClient Administration Guide*.

Anti-exploit detection

The anti-exploit detection feature helps protect vulnerable endpoints from unknown exploit attacks. FortiClient monitors the behavior of popular applications, such as web browsers (Internet Explorer, Chrome, FireFox, Opera), Java/Flash plug-ins, Microsoft Office applications, and PDF readers, against exploits that use zero-day or unpatched vulnerabilities to infect the endpoint. Once detected, the compromised application process is terminated. The anti-exploit detection feature also helps protect against memory-based attacks and drive-by download attacks. It also detects and blocks unknown and known exploit kits. It is a signature-less solution.

Share endpoint user's social IDs with FortiAnalyzer

When FortiClient is in managed mode, details from cloud applications about endpoint users are sent to FortiAnalyzer. Before the information can be sent, the endpoint user must add the information to FortiClient by logging into a cloud application.

Support for FortiSandbox authorization

Administrators can now enforce that only authorized FortiClient endpoints can connect to their FortiSandbox.

Improvements to VPN auto connect

Various improvements and bug fixes have been made to improve the reliability and function of the VPN auto-connect feature

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 5.6.1: Introduction on page 5, Special Notices on page 7, and Product Integration and Support on page 12.

Installation options

When installing FortiClient version 5.6.1, 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 5.6.1 supports upgrade from FortiClient versions 5.2 and later.

Downgrading to previous versions

Downgrading FortiClient version 5.6.1 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 5.6.1 support

The following table lists version 5.6.1 product integration and support information.

FortiClient 5.6.1 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 5.6.1 does not support Microsoft Windows XP and Microsoft Windows Vista.
Server Operating Systems	• Microsoft Windows Server 2008 R2 or newer FortiClient 5.6.1 does not support Windows Server Core.
Minimum System Requirements	• 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	• 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	• 1.2.0 and later
FortiManager	• 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)	✔		

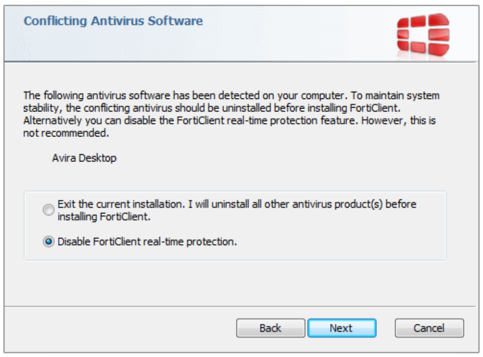
The FortiClient language setting defaults to the regional language setting configured on the client workstation, unless configured in the XML configuration file.

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

Bug ID	Description
0377066	Manually updated software has no chance to get compliance
0384351	Unable to Exclude Microsoft VSS volume
0400439	FortiSandbox will only Respond to Authorized FortiClient
0403544	VPN IPsec auto-connect does not work on FortiClient 5.4.2 and 32-bit Win7
0405106	FortiClient Sandbox status shows *Reachable but Out of Date*"
0409809	FortiClient local privilege escalation with VPN before logon and untrusted certificate
0417707	AV scan history is lost after upgrading FortiClient
0434289	FortiClient b870 with Trendmicro AV causes HTTP websites to fail to load on Windows 10
0435507	FortiClient console displays incorrect number of threats detected
0437125	FortiClient / FortiSandbox integration does not work as expected with Lotus Notes
0437491	b1075: Option to enable wanopt exists on FortiClient after upgrade from 5.4.3
0438790	Windows Defender does not recognize FortiClient RTP
0438999	HTTP upload fails when Web Filter is enabled
0439040	b1075: FortiClient will lose existing registration if trying to register to unlicensed server
0439569	Problems saving Microsoft Word documents (`.DOCX`) with FortiClient RTP in OneDrive
0439625	Botnet did not really block access
0440037	IPS engine categorized many application as storage backup
0440185	b0870: FortiClient loses saved VPN password with weak connection
0441738	`FortiFW.exe` should bypass the EMS webserver
0442752	AV engine gets stuck with 64-bit FortiClient
0443241	B1083: USB and network mapped drives - FortiClient 5.6.0 may not release clean files after FortiSandbox scan
0443321	FortiClient 5.6.0.1075 - Wrong information about FortiClient Configurator in the `Readme_1st.txt` document
0443756	FortiClient SSL VPN tunnel DNS registration

Bug ID	Description
0444427	b1075: improper endpoint compliance warning prevents web browsing
0444776	[FCT] B1075: BSOD when connecting SSL VPN using WiFi on Surface Pro 4
0445175	B1083: Local drive - FortiClient 5.6.0 may not release clean files after FortiSandbox scan
0445380	[WF] add option to show blocked message from FortiClient Bubble pop-up for HTTPS site
0445532	Localized images display incorrectly
0445692	b1075: Unable to receive WINS via SSL VPN
0446214	1075: FortiClient shortens user passwords to 40 characters when connecting to IPsec tunnel
0446244	SSO Mobility Agent not logging correct users across multiple domains
0446262	SSL VPN option to stop connecting on server certificate issue without warning
0446665	`MSVCP140.dll` missing in Win10x32 installer
0446847	Keep prompting *Unable to reach tunnel/gateway policy server* causes FortiTray crash
0446886	b1075: EMS shows incorrect FortiClient state if EMS is configured as both notification and management in IP list
0447019	b1075: FortiClient SSL VPN unable to connect when using certificate
0447310	b1075: FortiClient FortiSandbox online interval too short - should be configurable from EMS profile or XML
0447391	FortiClient exclusion configuration should support VSS format
0448304	b1075: The number of routes accepted when SSL-VPN-connected is significantly lower then it was in 5.4.1
0448404	[B1075] FortiClient fails to renegotiate SPI after three FortiGate HA failovers
0448849	FortiClient sent loopback IP as FSSOMA requests to FAC after HA cluster failover
0450214	FortiClient Sandbox Detection feature doesn't work on RDP - cannot get user token
0450277	Windows Variable `%USERPROFILE%` not working in exclusion list
0450604	Windows Server 2016 upgrade from 0890 to 1093 keeps prompting reboot after reboot
0451823	FortiClient Sandbox Detection feature corrupts Microsoft Excel files for Microsoft Office 2016
0456662	When opening attachments from inside Microsoft Outlook 2016, they are not scanned by FortiSandbox

Common Vulnerabilities and Exposures

Bug ID	Description
0408442	FortiClient (Windows) 5.6.1 is no longer vulnerable to the following CVE Reference: • CVE-2017-14184 Visit https://fortiguard.com/psirt for more information.

Known Issues

The following issues have been identified in FortiClient (Windows) 5.6.1. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Bug ID	Description
0251589	Fortiproxy certificate is unknown and untrusted
0389712	User unable to establish SSL VPN connection (Windows 10 Build 1607)
0400261	Send supported files received from P2P to FortiSandbox
0404746	b860: SSL VPN with certificate auth doesn't work from FortiTray, but works from FortiClient console
0409656	FortiClient removed default route of LTE card after connecting to IPsec VPN
0411137	Cannot exclude UNC paths from scans
0414476	AV network scan slowing down applications that rely on network resources
0415585	b0126: Redeployment from EMS will reboot servers as no users logged in
0421900	High CPU usage with `fmon.exe`
0422025	`scan_on_insertion =1` would skip scan removal media when inserting USB and AV scan was in progress
0424102	b0870: FortiProxy causes issues with Citrix HTML5
0439903	Web Filter settings from EMS are lost after some time
0440844	B1075 - FCT SSL VPN connection fails at 98% - Works after the 1st attempt
0441590	FortiClient 5.6.0 Application Firewall is blocking access to certain HTTPS websites
0442732	Mdare quick & full scan does not work in 64-bit FortiClient
0443832	High CPU and freeze due to AV exclusions
0444108	Files are getting blocked/quarantined while it is white listed
0444535	FortiClient 5.6 slows PC down when we enable *Scan Files as they are Downloaded of Copied to System*"
0445329	Fortiproxy causing website to fail to display properly
0448485	b1075: Change on-net/off-net status discovery for dual registration case
0449279	b1075: Fortiproxy blocks/prevents in-house software from working
0449330	Verifying FortiClient installer downloads during deployment from EMS

Bug ID	Description
0449596	FortiClient does not follow the same remediation action taken by FortiSandbox for low-risk files
0450200	b1075: FortiClient Connection screen text cut off
0450225	b1075: FortiClient blocking DNS when Application Firewall enabled
0451605	b0394: EMS reports NPAPI Flash Plugin vulnerable while not installed
0451976	FortiClient 5.6.0 Application Firewall is slowing down file transfers
0456320	b0890 also b1075 - SSL VPN saving password after delsecting *Always Up*"
0457244	B890 - GUI option to enable DTLS
0458138	On-net status not being reported correctly on FortiClient when the EMS is offline