

FortiClient (Windows) - Release Notes

Version 6.2.6

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 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



March 12, 2020

FortiClient (Windows) 6.2.6 Release Notes

04-626-613623-20200312

TABLE OF CONTENTS

Change log	4
Introduction	5
Licensing	5
Special notices	6
Nested VPN tunnels	6
SSL VPN connectivity issues	6
Microsoft Windows server support	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	9
Product integration and support	10
Language support	11
Conflicts with third party AV products	12
Resolved issues	13
GUI	13
Install and deployment	13
Endpoint control	13
Logs	14
Remote Access	14
Sandbox	14
Other	14
Known issues	15
Update	15
Logs	15
Endpoint control	15
GUI	16
Install and deployment	16
Malware Protection	16
Remote Access	16
Sandbox	17
Vulnerability Scan	17
Web Filter	17
Other	17

Change log

Date	Change Description
2020-03-10	Initial release of FortiClient (Windows) 6.2.6.
2020-03-11	Updated Known issues on page 15 .
2020-03-12	Removed 565711 from Resolved issues on page 13 .

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 6.2.6 build 0951.

- [Special notices on page 6](#)
- [Installation information on page 7](#)
- [Product integration and support on page 10](#)
- [Resolved issues on page 13](#)
- [Known issues on page 15](#)

Review all sections prior to installing FortiClient.

Licensing

FortiClient 6.2.0+, FortiClient EMS 6.2.0+, and FortiOS 6.2.0+ introduce a new licensing structure for managing endpoints running FortiClient 6.2.0+. See [Upgrading from previous FortiClient versions on page 8](#) for more information on how the licensing changes upon upgrade to 6.2.0+. Fortinet no longer offers a free trial license for ten connected FortiClient endpoints on any FortiGate model running FortiOS 6.2.0+. EMS 6.2.6 supports a 30-day trial license with ten FortiClient seats.

FortiClient 6.2.6 offers a free VPN-only version that you can use for VPN-only connectivity to FortiGate devices running FortiOS 5.6 and later versions. You can download the VPN-only application from [FortiClient.com](https://forticlient.com). You cannot use the VPN-only client with the FortiClient Single Sign On Mobility Agent (SSOMA). To use VPN and SSOMA together, you must purchase an EMS license.

Special notices

Nested VPN tunnels

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

SSL VPN connectivity issues

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

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

Microsoft Windows server support

FortiClient (Windows) supports the AV and vulnerability scan features for Microsoft Windows servers.

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 from the [Fortinet support site](#):

File	Description
FortiClientTools_6.2.6.xxxx.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_6.2.6.xxxx.zip	FortiClient Single Sign On (FSSO)-only installer (32-bit).
FortiClientSSOSetup_6.2.6.xxxx_x64.zip	FSSO-only installer (64-bit).

The FortiClient (Windows) 6.2.6 standard installer and zip package containing FortiClient.msi and language transforms are included with FortiClient EMS 6.2.6.

The following tools and files are available in the FortiClientTools_6.2.x.xxxx.zip file:

File	Description
FortiClientVirusCleaner	Virus cleaner.
SSLVPNcmdline	Command line SSL VPN client.
SupportUtils	Includes diagnostic, uninstallation, and reinstallation tools.
VPNAutomation	VPN automation tool.

The following file is available from [FortiClient.com](#):

File	Description
FortiClientVPNOnlineInstaller_6.2.exe	Free VPN-only installer. This VPN-only client does not include Fortinet technical support.



Review the following sections prior to installing FortiClient version 6.2.6: [Introduction on page 5](#), [Special notices on page 6](#), and [Product integration and support on page 10](#).

Installation options

When the administrator creates a FortiClient deployment package in EMS, they choose which setup type and modules to install:

- Secure Remote Access: VPN components (IPsec and SSL) are installed.
- Advanced Persistent Threat (APT) Components: FortiSandbox detection and quarantine features are installed.
- Additional Security Features: One or more of the following features are installed: AV, Web Filter, SSO, Application Firewall, and Cloud Based Malware Outbreak Protection.



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



The FortiClient (Windows) installer is available on EMS. You can configure and select installed features and options on EMS.

Upgrading from previous FortiClient versions

FortiClient 6.2.6 supports upgrade from FortiClient 6.0 and later.

Starting with FortiClient 6.2.0, FortiClient EMS 6.2.0, and FortiOS 6.2.0, the FortiClient Endpoint Telemetry license is deprecated. The FortiClient Compliance profile under *Security Profiles* and the *Enforce FortiClient Compliance Check* option on the interface configuration pages have been removed from the FortiOS GUI. Endpoints running FortiClient 6.2.0+ now register only with FortiClient EMS 6.2.0+ and compliance is accomplished through the use of compliance verification rules configured on FortiClient EMS 6.2.0+ and enforced through the use of firewall policies. As a result, there are two upgrade scenarios:

- Customers using only a FortiGate device in FortiOS 6.0 to enforce compliance must install FortiClient EMS 6.2.0+ and purchase a FortiClient Security Fabric Agent License for their FortiClient EMS installation to continue using compliance features.
- Customers using both a FortiGate device in FortiOS 6.0 and FortiClient EMS running 6.0 for compliance enforcement must upgrade the FortiGate device to FortiOS 6.2.0+, FortiClient to 6.2.0+, and FortiClient EMS to 6.2.0+.

FortiClient (Windows) 6.2.6 features are only enabled when connected to EMS 6.2.0+. If FortiClient (Windows) 6.0 was previously running in standalone mode, ensure to install EMS 6.2.0+, apply the license as appropriate, then connect FortiClient (Windows) to EMS before upgrading to FortiClient (Windows) 6.2.6. You should first upgrade any endpoint running a FortiClient (Windows) version older than 6.0.0 to 6.0.5 using existing 6.0 upgrade procedures.

See the [FortiClient and FortiClient EMS Upgrade Paths](#) for information on upgrade paths and the order in which to upgrade Fortinet products.

Downgrading to previous versions

FortiClient (Windows) 6.2.6 does not support downgrading to previous FortiClient (Windows) versions.

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 *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 6.2.6 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 6.2.6 does not support Microsoft Windows XP and Microsoft Windows Vista.
Server operating systems	• Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2016 • Microsoft Windows Server 2019 FortiClient 6.2.6 does not support Windows Server Core. For Microsoft Windows Server, FortiClient (Windows) supports the Vulnerability Scan, SSL VPN, and AV features, including obtaining a Sandbox signature package for AV scanning. To use SSL VPN on a Windows Server machine, you must enable your browser to accept cookies. Otherwise, tunnel connection fails.
Embedded system operating systems	Microsoft Windows 10 IoT Enterprise LTSC 2019
Minimum system requirements	• Microsoft Windows-compatible computer with Intel processor or equivalent. FortiClient (Windows) does not support ARM-based processors. • 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 3.0 or later
FortiAnalyzer	6.2.0 and later
FortiAuthenticator	• 4.3.1 • 4.3.0 • 4.2.1 FortiClient (Windows) does not support FortiToken Mobile push notification for the following FortiAuthenticator 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
FortiManager	6.2.0 and later
FortiOS	6.2.0 and later 6.0.0 and later Telemetry, IPsec VPN, and SSL VPN are supported. See important information in Upgrading from previous FortiClient versions on page 8. 5.6.0 and later IPsec VPN and SSL VPN are supported. See important information in Upgrading from previous FortiClient versions on page 8.
FortiSandbox	3.1.0 and later 3.0.0 and later 2.5.0 and later

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.



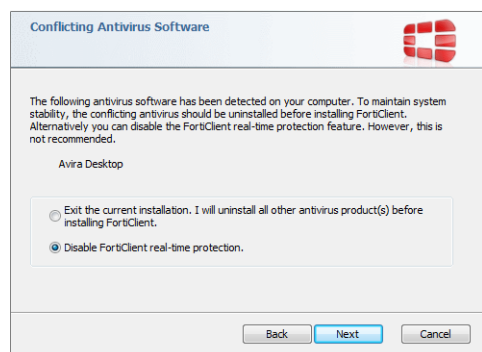
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

Conflicts with third party AV products

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

- You should not use FortiClient's AV feature with other AV products.
- If not using FortiClient's AV feature, you should exclude the FortiClient installation folder from scanning for the third party AV product.

During a new installation of FortiClient, the installer searches for other registered third party software and, if any is found, warns 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 6.2.6. For inquiries about a particular bug, contact [Customer Service & Support](#).

GUI

Bug ID	Description
525021	FortiClient fails to find avatar when logged in as domain user.
588965	Avatar fails to display on FortiClient avatar page on Windows 7 x86.
606378	FortiClient avatar page shows avatar icon but fails to display avatar picture.

Install and deployment

Bug ID	Description
606830	Manual FortiClient installation without AV option displays "Conflicting AntiVirus Software" popup.
607620	Free VPN-only installer should not allow installation of multiple versions on same machine.
612209	EMS fails to deploy new FortiClient because FortiClientSetup_<version>_x64.exe crashes.

Endpoint control

Bug ID	Description
583223	Compliance verification using Active Directory group does not work.
607258	EMS software inventory does not update.

Logs

Bug ID	Description
502225	EMS shows message details for AV that convey no information about the event.
546111	FCDBLog.exe process crashes on all platforms.
586798	FortiClient does not generate logs for Cloud Sandbox events, signatures, and submitted files.
596206	Feature logs fill the disk.
601725	FortiClient should send full URL to FortiAnalyzer.
612229	FortiClient debug log can be unlimited when upgrading.

Remote Access

Bug ID	Description
537299	FortiClient (Windows) does not use correct SSL VPN split DNS server.
577346	Every time FortiClient (Windows) synchronizes with EMS, FortiClient creates a duplicate VPN profile when a special character is used.
603321	Saving a password that contains double quotation marks wipes VPN configuration from GUI.
611333	If xAuth is disabled, a tunnel that requires a certificate should not show username/password.

Sandbox

Bug ID	Description
598815	FortiClient Cloud Sandbox status displays incorrectly.

Other

Bug ID	Description
607507	Inconsistent token obfuscation across Windows and macOS FortiClient.

Known issues

The following issues have been identified in FortiClient (Windows) 6.2.6. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

Update

Bug ID	Description
501877	update_task.exe fails to update AV signature from command line.

Logs

Bug ID	Description
587179	No log for removable device control.
587261	Endpoint sends wrong "Endpoint Quarantine Status changed - Unquarantined" logs.
604914	FortiClient real-time logs show random old log, with no actual real-time logs for FortiClient.
609252	FortiClient (Windows) fails to send software inventory to FortiAnalyzer.
612952	Exporting logs specifies Sandbox as <i>Other</i> category.

Endpoint control

Bug ID	Description
588059	On-net checked conditions by ESNAC do not match with configuration when only using EMS.
599807	FortiClient did not register to EMS after deployment.
604742	FortiClient (Windows) connected to FortiClient Cloud EMS shows no vulnerability feature.
606466	"FortiClient registration was blocked by Endpoint Management Server (EMS)" message occurs when FortiGate is in Telemetry list.
608200	FortiClient (Windows) loses EMS registration information after installation.

GUI

Bug ID	Description
616700	FortiClient fails to show avatar from OS for Windows 7 platform for domain user.
612697	About page displays as updating forever.

Install and deployment

Bug ID	Description
555541	Endpoint may reached a state where EMS deployment always fails.
590987	EMS fails to deploy FortiClient (Windows) when deploying FortiClient with a different feature set over the same FortiClient (Windows) version deployed.
607954	EMS deployment issues.

Malware Protection

Bug ID	Description
596388	Realtime protection on RDS server blocks remote sessions.
606534	AV scan fails to scan network folder when folder name contains space.
606712	FortiClient should not allow restoring quarantined files from USB drives when managed by EMS.

Remote Access

Bug ID	Description
601074	Connecting VPN from FortiTray with two-factor authentication leads FortiClient to show FortiClient GUI instead of connecting instantly.
604546	IPsec VPN tunnel with certificate authentication fails to automatically connect when it cannot reach resilience FortiGate.
612885	FortiClient (Windows) fails to delete the selected tunnel for personal VPN with FortiClient registered.

Sandbox

Bug ID	Description
606272	FortiClient (Windows) does not send MSI installers saved on network shares to FortiSandbox.

Vulnerability Scan

Bug ID	Description
600349	Vulnerability Scan does not pick up some vulnerabilities.

Web Filter

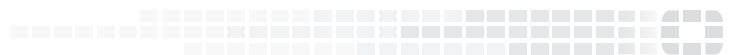
Bug ID	Description
615616	FortiClient keeps prompting to install web extension when Web Filter is disabled.

Other

Bug ID	Description
611821	FortiClient (Windows) mishandles special character, such as %, in new passwords.



FORTINET®



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.