FortiClient (Windows) - Release Notes

Version 6.2.9

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/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

August 26, 2021
FortiClient (Windows) 6.2.9 Release Notes
04-629-740539-20210826

TABLE OF CONTENTS

Change log

Date	Change Description
2021-08-26	Initial release of FortiClient (Windows) 6.2.9.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 6.2.9 build 1032.

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 6.2.9 supports a trial license. With the EMS free trial license, you can provision and manage FortiClient on ten Windows, macOS, and Linux endpoints and ten Chromebook endpoints indefinitely.

FortiClient 6.2.9 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. 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, vulnerability scan, Web Filter, and SSL VPN 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_6.2.9.xxxx.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_6.2.9.xxxx.zip	FortiClient Single Sign On (FSSO)-only installer (32-bit).
FortiClientSSOSetup_6.2.9.xxxx_x64.zip	FSSO-only installer (64-bit).

FortiClient EMS 6.2.9 includes the FortiClient (Windows) 6.2.9 standard installer and zip package containing FortiClient.msi and language transforms.

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
FortiClientVPNSetup_6.2.9.1032.exe	Free VPN-only installer. This VPN-only client does not include Fortinet technical support.

Review the following sections prior to installing FortiClient version 6.2.9: 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 6.2.9 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) 6.2.9 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) 6.2.9. 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) 6.2.9 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 6.2.9 product integration and support information:

Desktop operating systems	FortiClient supports all versions of the listed OSes. • 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 6.2.9 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 6.2.9 does not support Windows Server Core. For Microsoft Windows Server, FortiClient (Windows) supports the Vulnerability Scan, SSL VPN, Web Filter, 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	• 6.1.0 and later • 6.0.0 and later
FortiClient EMS	• 6.4.0 and later • 6.2.0 and later
FortiManager	6.2.0 and later
FortiOS	The following FortiOS versions support Telemetry and IPsec and SSL VPN with FortiClient (Windows) 6.2.9:

	• 6.2.0 and later • 6.0.0 and later The following FortiOS versions support IPsec and SSL VPN with FortiClient (Windows) 6.2.9: • 6.4.0 and later • 5.6.0 and later
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.

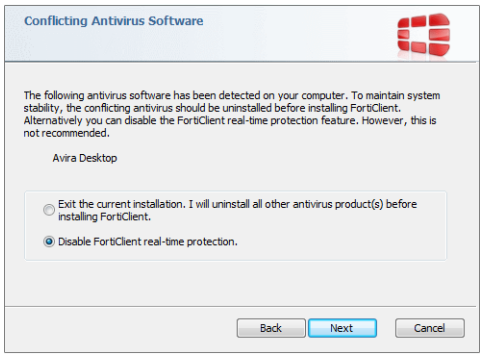
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

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

GUI

Bug ID	Description
606712	Attempts to restore quarantined files from USB drives fail.
670671	Diacritics does not show correctly in EMS endpoint summary detail.

Install and deployment

Bug ID	Description
666024	FortiClientSetup_6.4.2_x64.exe deployment package created in FortiClient Cloud crashes during deployment.

Fabric Telemetry

Bug ID	Description
661107	FortiClient (Windows) sends avatar every keepalive interval.
666649	FortiClient stops attempting to register to EMS when it cannot reach EMS.

Malware Protection and Sandbox Detection

Bug ID	Description
600765	Log shows Sandbox agent receives "`score = 0`" instead of "`score = 4`" for a file that FortiSandbox determines as low risk.
634353	Initial scan ignores `%localappdata%` exclusion.
668719	Real-time protection on Citrix VDA server blocks remote sessions.

Remote Access

Bug ID	Description
671392	Windows restart does not remove SSL VPN tunnel that VPN before logon established.
676554	If user enters incorrect username/password for SSL VPN tunnel, FortiClient (Windows) displays error that it cannot reach the server.

Other

Bug ID	Description
670029	Incorrectly formatted firewall alerts.

Known issues

The following issues have been identified in FortiClient (Windows) 6.2.9. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Application Firewall

Bug ID	Description
579458	Application Firewall decreases throughput on wireless adapters.
700601	fortisniff2.sys triggers blue screens of death.

Logs

Bug ID	Description
676122	Logs show that the number of received bytes is 0 when downloading big files.

Endpoint control

Bug ID	Description
588059	Onnet checked conditions by ESNAC do not match with configuration when only using EMS.
676156	Active Directory group compliance verification rule does not work.
684662	FortiClient cannot install the certificate included in the profile.
688913	FortiClient is missing Telemetry EMS list.
731525	FortiClient (Windows) does not detect compliance verification tag that requires antivirus to not be up-to-date on the endpoint properly.

Sandbox and Malware Protection

Bug ID	Description
623867	FortiClient (Windows) cannot connect to FortiClient Cloud Sandbox despite port 514 being open.
700195	User cannot log in to Windows after waking computer from sleep mode.
730172	FortiClient causes VMware Horizon Agent to disconnect from VMware Connection Server.

Remote Access

Bug ID	Description
680615	FortiClient (Windows) sends DNS queries to wrong servers on SSL VPN.
681399	IPsec VPN autoconnect does not work after an automatic frequency change.
686908	After updating FortiClient, user cannot connect to VPN for the first time.
700060	`/forcerestart` CLI installer option prompts user for reboot.
700499	VPN before login keeps prompting for user credentials even after establishing VPN connection but will not log in to Windows.

Vulnerability Scan

Bug ID	Description
663788	FortiClient (Windows) starts Windows update services upon Vulnerability Scan execution.

Web Filter and plugin

Bug ID	Description
673329	Windows update patch blocks all web traffic.

FSSO

Bug ID	Description
705256	Single sign on mobility agent fails to call WTSQueryUserToken.