FortiClient (Windows) - Release Notes

Version 6.2.1

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

November 12, 2019
FortiClient (Windows) 6.2.1 Release Notes
04-621-563657-20191112

TABLE OF CONTENTS

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 6.2.1 build 0831.

- Special notices on page 5
- What’s new in FortiClient (Windows) 6.2.1 on page 6
- Installation information on page 7
- Product integration and support on page 10
- Resolved issues on page 13
- Known issues on page 16

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 6.2.1 supports a 30-day trial license with ten FortiClient seats.

FortiClient 6.2.1 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 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.

What’s new in FortiClient (Windows) 6.2.1

For information about what's new in FortiClient (Windows) 6.2.1, see the *FortiClient & FortiClient EMS New Features Guide*.

Installation information

Firmware images and tools

The following files are available from the Fortinet support site:

File	Description
FortiClientTools_6.2.1.xxxx.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_6.2.1.xxxx.zip	FortiClient Single Sign On (FSSO)-only installer (32-bit).
FortiClientSSOSetup_6.2.1.xxxx_x64.zip	FSSO-only installer (64-bit).

The FortiClient (Windows) 6.2.1 standard installer and zip package containing FortiClient.msi and language transforms are included with FortiClient EMS 6.2.1.

The following tools and files are available in the FortiClientTools_6.2.xx.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 6.2.1: Introduction on page 4, Special notices on page 5, 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 version 6.2.1 supports upgrade from FortiClient versions 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) 6.2.1 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) 6.2.1. 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

Downgrading FortiClient version 6.2.1 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. 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 6.2.1 support

The following table lists version 6.2.1 product integration and 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 6.2.1 does not support Microsoft Windows XP and Microsoft Windows Vista.
Server operating systems	• Microsoft Windows Server 2008 R2 or newer FortiClient 6.2.1 does not support Windows Server Core. For Microsoft Windows Server, FortiClient (Windows) supports the Vulnerability Scan and AV features, including obtaining a Sandbox signature package for AV scanning.
Minimum system requirements	• Microsoft Windows compatible computer with Intel processor or equivalent • 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 version 3.0 or later
FortiAnalyzer	• 6.2.0 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	• 6.2.0 and later EMS 6.2.2 does not provide backwards host tag compatibility for FortiClient (Windows) 6.2.1. Upgrade FortiClient to 6.2.2 for host tag compatibility with EMS 6.2.2.

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.

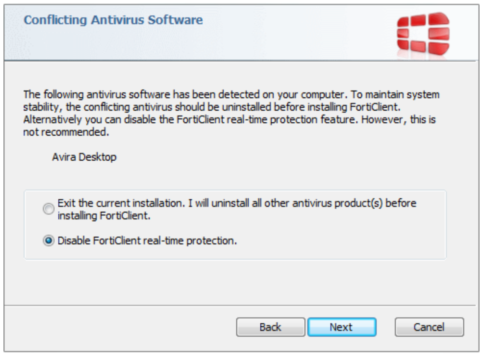
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

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).



Conflicting Antivirus Software

The following antivirus software has been detected on your computer. To maintain system stability, the conflicting antivirus should be uninstalled before installing FortiClient. Alternatively you can disable the FortiClient real-time protection feature. However, this is not recommended.

Avira Desktop

○ Exit the current installation. I will uninstall all other antivirus product(s) before installing FortiClient.

● Disable FortiClient real-time protection.

Resolved issues

The following issues have been fixed in version 6.2.1. For inquiries about a particular bug, contact Customer Service & Support.

Endpoint control

Bug ID	Description
553718	FortiClient forces password change before FortiGate local user password expires.
553977	FortiClient always sends previous avatar image to EMS when configured to send the OS avatar.
554236	FortiClient still reports that it is connected to FortiGate when FortiGate changes the registration port.
550158	FortiClient (Windows) fails to unregister when EMS is not reachable.
563396	FortiClient shows all features when registered to on-premium EMS with Sandbox license only.

Malware Protection

Bug ID	Description
557098	FortiClient online installer fails to trigger AV scan on clean system.
563144	FortiClient registers to Windows security center even if no AV is installed.

Sandbox

Bug ID	Description
563467	Right-clicking a file to select Sandbox scan in the context menu resets the number of files submitted for Sandbox scan.
563697	fortimon3 service does not run when no Sandbox is installed.
564177	FortiClient blocks file access when it reaches the daily count limit.
564363	FortiClient Sandbox Cloud daily count resets when EMS profile switches between physical and cloud Sandbox.

Web Filter

Bug ID	Description
416909	RTP should support blocking malicious webpages and known attack communication channels when only AV is installed.
450181	FortiClient makes connections to FortiGuard servers even when Web Filter and FortiProxy are disabled.
529450	FortiClient shows *Unrated* for HTTPS sites while HTTP shows correct category.
551211	*Client Web Filtering When On-Net* setting in EMS profile fails to work for Chrome plugin.
561788	FortiClient Web Filter plugin blocks any URL as unknown when FortiClient Web Filter is disabled.

Remote Access

Bug ID	Description
538722	VPN-only free client shows always-up/auto-connect.
538752	EMS settings for `<show_remember_password>`, `<show_alwaysup>`, and `<show_autoconnect>` should override similar FortiOS settings.
551538	Onnet FortiClient triggers VPN autoconnect after system reboot even when autoconnect only when offnet is enabled.
551919	Fails to reconnect from FortiTray if username has "\" or domain user format.
554014	When using local machine certificate, SSL VPN resilience is stuck and does not try next available remote gateway.
555676	Dialup IPsec VPN with DHCP over IPsec VPN has no Internet access with split tunneling.
558488	SSL VPN always_up does not work when connecting from tray.
559907	IPsec VPN cannot connect if started from tray with GUI open.
561826	SSL VPN with FortiToken two-factor authentication (2FA) does not automatically reconnect when network connection reestablishes after network failure.
563257	FortiClient (Windows) cannot save phase 2 DH group properly.
563263	PFS DH group is 1 on GUI, but IPsec daemon sent 5 to FortiOS.
565074	VPN before logon does not work properly.
566503	With FortiClient registered to EMS, always up does not work properly with FortiToken 2FA.
567911	FortiToken 2FA fails to make VPN connection.
568019	Client certificate is empty on GUI when connecting from FortiTray when tunnel requires a certificate.

Vulnerability Scan

Bug ID	Description
394362	FortiClient requests reboot even if automatic patching is disabled.
538267	FortiClient fails to create scheduled vcm scan when EMS enables maintenance setting.

Install and upgrade

Bug ID	Description
566360	.exe installer fails to run except on US-English Windows.

Other

Bug ID	Description
534194	fcdblog rewrites hosts file without any changes.
545427	FortiClient scheduled daily update from MFGD communicates with MFGD very frequently.
548918	FortiClient AV causes high CPU usage on endpoints.
552481	Standalone FSSO fails to work after installation with FortiClientSSOSetup_6.2.0.0780_x64.zip.
565128	FortiClient (Windows) should automatically update avatar page based on EMS settings.
566703	FortiTray crashes randomly.

Common Vulnerabilities and Exposures

Bug ID	Description
433685	FortiClient (Windows) is no longer vulnerable to the following CVE reference: • CVE-2019-5589
559607	FortiClient (Windows) is no longer vulnerable to the following CVE reference: • CVE-2019-6692

Known issues

The following issues have been identified in FortiClient (Windows) 6.2.1. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Endpoint Control

Bug ID	Description
550165	EMS is missing Cloud Malware Protection feature state.
551878	FortiClient registration state stays in syncing state forever if EMS is not reachable.
552101	EMS reports endpoint notified state after EMS deploys FortiClient successfully.
559308	FortiClient does not register to new FortiGate when EMS changes or updates its gateway list.
564681	EMS sometimes fails to deploy to endpoints.
565172	FortiClient (Windows) fails to push updated avatar to EMS.
568381	FortiClient (Windows) fails to update vulnerabilities to EMS without starting new VCM scan.

Malware Protection

Bug ID	Description
535604	AntiExploit causes application to crash without block message.
541953	FortiClient gives an error if restoring configuration when third party AV is installed.
550154	FortiClient fails to show *Malware Protection* tab when installer does not contain AV feature.
553361	Cloud-based threat detection event should display on *AntiVirus Events* tab.
563663	FortiClient AV cannot quarantine files on Remote Desktop Session host. 0 0 0 0 0
567993	FortiClient AV scan for removable media stops prematurely.

Sandbox

Bug ID	Description
548919	FortiSandbox does not scan attachments opened from inside Outlook 2016.

Web Filter

Bug ID	Description
547614	Chrome plugin does not use customized warning page.
550021	Web Filter plugin blocks URL accessed in incognito mode when Web Filter is disabled.
551227	*Proceed* button on warning page does not work.
567677	FortiClient (Windows) blocks rated websites as unrated URLs.

Application Firewall

Bug ID	Description
564595	Application Firewall does not block BitTorent peer-to-peer traffic.
579458	Application Firewall decreases throughput on wireless adapters.

Remote Access

Bug ID	Description
537299	FortiClient (Windows) does not use correct SSL VPN split DNS server.
538024	FortiClient (Windows) loses DNS settings after disconnecting IPsec VPN.
546487	IPsec VPN IKEv2 error after disconnecting from and reconnecting to network.
547456	FortiClient (Windows) GUI does not display bytes sent and received when connecting from FortiTray.
549011	After renewing the saved LDAP user password, GUI does not show correct tunnel if connected from FortiTray.
549122	IPv6 tunnel requiring certificate fails to make VPN connection with new PIN.
550601	Resiliency ping-based method does not work properly.
551754	FortiClient reports *VPN connection failed* error when switching between offnet and onnet networks.
563083	When registered to EMS, IPsec new PIN/next token mode does not work properly.
565449	SSL VPN resilience does not try the last remote gateway.
566012	When a proxy server is in the middle, an SSL VPN tunnel that requires a machine certificate can bypass it.

Bug ID	Description
566698	For always-up with FortiToken 2FA, GUI does not auto-popup for token code when network is down then up.
567908	Username is empty on GUI after VPN is up.

Install and upgrade

Bug ID	Description
543034	EMS-deployed FortiClient fails to show message on active logged-on user when multiple users are logged on.

Other

Bug ID	Description
540455	FortiClient System Tray Controller causes high memory and CPU usage
547731	FortiClient does not warn the user about third party RTP when enabling FortiClient (Windows) RTP via the GUI.
549289	User details reset after new FortiClient deployment.
557410	High memory usage for fcappdb on Windows Servers.
568328	FortiClient crashes and stops AV updates.
568767	FortiClient reports to FortiAnalyzer that endpoint quarantine and endpoint control states change every two minutes.

Change log

Date	Change Description
2019-07-18	Initial release of FortiClient (Windows) 6.2.1.
2019-08-06	Updated Product integration and support on page 10.
2019-08-16	Updated Product integration and support on page 10.
2019-08-22	Added 559607 to Resolved issues on page 13.
2019-09-04	Updated Installation information on page 7.
2019-11-12	Added 579458 to Known issues on page 16.