FortiClient (Windows) - Release Notes

Version 6.2.2

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

December 05, 2019
FortiClient (Windows) 6.2.2 Release Notes
04-622-579772-20191205

TABLE OF CONTENTS

Introduction **4**
Licensing 4
Special notices **5**
Nested VPN tunnels 5
SSL VPN connectivity issues 5
Microsoft Windows server support 5
HP Velocity and Application Firewall 5
Installation information **6**
Firmware images and tools 6
Installation options 6
Upgrading from previous FortiClient versions 7
Downgrading to previous versions 7
Firmware image checksums 8
Product integration and support **9**
FortiClient 6.2.2 support 9
Language support 10
Conflicts with third party AV products 11
Resolved issues **12**
Avatar 12
Endpoint control 12
Install and upgrade 12
Malware Protection 13
Remote Access 13
Sandbox 13
Vulnerability Scan 14
Web Filter 14
Other 14
Known issues **15**
Avatar 15
Endpoint control 15
GUI 15
Install and upgrade 16
Malware Protection 16
Remote Access 16
Sandbox 17
Vulnerability Scan 17
Web Filter 17
Other 18
Change log **19**

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 6.2.2 build 0877.

- Special notices on page 5
- Installation information on page 6
- Product integration and support on page 9
- Resolved issues on page 12
- 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 7 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 6.2.2 supports a 30-day trial license with ten FortiClient seats.

FortiClient 6.2.2 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.

Installation information

Firmware images and tools

The following files are available from the Fortinet support site:

File	Description
FortiClientTools_6.2.2.xxxx.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_6.2.2.xxxx.zip	FortiClient Single Sign On (FSSO)-only installer (32-bit).
FortiClientSSOSetup_6.2.2.xxxx_x64.zip	FSSO-only installer (64-bit).

The FortiClient (Windows) 6.2.2 standard installer and zip package containing FortiClient.msi and language transforms are included with FortiClient EMS 6.2.2.

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 6.2.2: Introduction on page 4, Special notices on page 5, and Product integration and support on page 9.

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 6.2.2 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) 6.2.2 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) 6.2.2. 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 6.2.2 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 6.2.2 support

The following table lists version 6.2.2 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 6.2.2 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 6.2.2 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.
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 7. • 5.6.0 and later IPsec VPN and SSL VPN are supported. See important information in Upgrading from previous FortiClient versions on page 7.
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.

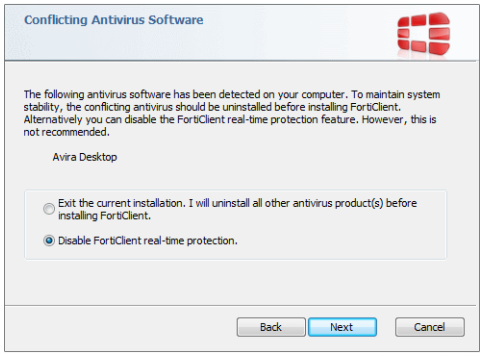
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

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

Avatar

Bug ID	Description
584733	After upgrading FortiClient, the user avatar is missing on both FortiClient and EMS.

Endpoint control

Bug ID	Description
559308	FortiClient does not register to new FortiGate when EMS changes/updates its gateway list.
570558	FortiESNAC causes endpoint to query for domain name.
579194	FortiClient (Windows) fails to register to other reachable EMS in EMS list if current one becomes offline.
580313	FortiClient can get stuck while synchronizing and never receive profile.
581260	FortiClient still reports its state as offline/onnet when unregistered from EMS.
582986	FortiClient fails to connect or disconnect to EMS.

Install and upgrade

Bug ID	Description
552839	Light installer should not work on any clients registered to EMS.
568294	Should remove VPN-only in applications and features after installing full version over free client.

Malware Protection

Bug ID	Description
563663	FortiClient AV cannot quarantine files on Remote Desktop Session host with *User profile disk*.
580604	FortiClient AV causes PC to become unusable when opening Microsoft Outlook.
581221	Observed memory leak by `Fortiae.exe`.
584584	FortiClient fails to send avatar to EMS.

Remote Access

Bug ID	Description
498782	Toggling *Prefer SSL VPN DNS* setting from *Enabled* to *Disabled* does not clear the DNS entries for local adapters.
514030	FortiClient does not connect to IPsec VPN if multiple Diffie Hellman groups are selected.
528434	Failed to see VPN before logon option on Windows 10 x64 1803 with fresh FortiClient install.
566012	With proxy server in the middle, SSL VPN tunnel requires that a machine certificate can bypass it.
567908	*User Name* is empty on GUI after VPN is up.
570030	Remote Access cannot display tunnel and related information after disconnecting.
571650	Tunnel with *RegEx* as certificate filter fails to make VPN connection from FortiTray after clicking *Connect first time*.
576712	VPN before login feature does not work on Windows 10 LTSB.
579724	FortiClient (Windows) fails to make VPN connect with certificate in current user or without certificate on Windows 7.
580080	FortiClient (Windows) should not allow VPN connection from FortiTray after free three-day VPN access.

Sandbox

Bug ID	Description
548919	FortiSandbox does not scan attachments opened from Microsoft Outlook 2016.
576869	FortiClient with FortiSandbox setting *Blocking File Access on Mapped Drive* when using PDF 995 application.
588336	FortiClient sends incorrect checksum for detected Sandbox Cloud quarantined files.

Vulnerability Scan

Bug ID	Description
555100	FortiClient fails to patch vulnerability for Java JRE 8.0.1310.11.
568381	FortiClient fails to update vulnerabilities to EMS without starting new VCM scan.

Web Filter

Bug ID	Description
551227	FortiClient Web Filter warning page *Proceed* button does not work.
567677	FortiClient (Windows) treats rated websites as unrated URLs and blocks them.
568863	FortiClient Web Filter marks Lifesize application/URL under hacking and blocks it.
574948	Web Filter does not block http://www.google.com/drive.

Other

Bug ID	Description
478256	Severe network degradation (extremely slow network) on Windows VM when FortiClient is loaded.
512774	FortiClient diagnostic tool does not do anything if FortiClient is not installed.
540455	FortiClient System Tray Controller has memory leak and high CPU.
554911	FortiAnalyzer is missing FortiClient logs.
561015	*Host Tag Monitor* should not tag applications excluded from vulnerability compliance check.
563994	FortiClient does not send assigned policy to FortiAnalzyer.
568767	FortiClient reports to FortiAnalyzer that endpoint quarantine and endpoint control state change every two minutes.
569741	BSOD was observed with FortiClient with crash inside `fortiaptfilter.sys`.
575365	You can delete files in FortiClient folder even if FortiShield is running.
583073	`FCDblog.exe` process keeps crashing on Windows 10 x64 platform when FortiClient is registered to EMS.
585791	FortiClient sends garbled social info to FortiAnalyzer.
587914	FortiTray does not run after EMS deployment.

Known issues

The following issues have been identified in FortiClient (Windows) 6.2.2. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Avatar

Bug ID	Description
586684	FortiClient does not send avatar to FortiAnalyzer.

Endpoint control

Bug ID	Description
529794	EMS and manual upgrade of FortiGate registration statuses differ.
566039	Alert user that FortiClient license is expiring because EMS server is unreachable.
578065	Host tag rule *Exploit Guard* does not work.
582302	FortiClient cannot get signature from FortiManager using HTTPS because certificate check failed.
587689	All FortiClient processes still run after EMS deploys new FortiClient.

GUI

Bug ID	Description
532412	FortiClient malware protection dashboard still displays USB setting when EMS has disabled AV.
568816	GUI becomes blank after VPN is up for a while.

Install and upgrade

Bug ID	Description
570862	FortiClient VPN does not uninstall from AD endpoint after EMS deploys new version of FortiClient.

Malware Protection

Bug ID	Description
525034	FortiClient does not do AV scan on next startup if off during scheduled scan time.
535604	AntiExploit causes application crashes without blocking message.
554026	Fixing `AntiExploitEngine` false positives.
577642	FortiClient Windows removable media access feature does not block iOS (mobile devices).
587229	*Exclude Files from Trusted Sources* fails to work for cloud-based malware detection.
586444	FortiClient cloud-based malware protection fails to update threats detected statistics.

Remote Access

Bug ID	Description
452476	FortiClient registers all interfaces' IP addresses to the DNS server when SSL VPN tunnel is up.
504291	FortiClient with IPv6-only configuration fails to connect with remote IKE2 IPv6 IPsec tunnel.
537299	FortiClient Windows does not use correct SSL VPN split DNS server.
538024	FortiClient (Windows) loses DNS settings after disconnecting IPsec VPN.
551754	*VPN connection failed* error displays when switching between offnet and onnet networks.
569461	FortiClient fails to connect the IPsec VPN tunnel if using FortiToken 2FA.
571989	FortiClient display issues when connecting to the VPN tunnel.
571992	FortiClient cannot connect to the VPN tunnel with *Save username*.
578168	FortiClient (Windows) cannot connect to VPN tunnel or dismiss the page when *save password/always-up/auto-connect* is enabled.
581149	VPN client did not learn all routes specified in SSL portal with split tunnel or SSL VPN IPv4 policies (pushing approx 1000 routes).

Bug ID	Description
583921	SSL VPN autoconnect does not work reliably.
584953	Split tunnel does not work when manual IP address is chosen.
587910	When FortiClient establishes IPsec/SSL VPN tunnel with FortiGate, it cannot get the FortiGate's tunnel interface as gateway via FortiTelemetry.
588287	FortiClient provide SHA1 cipher only for SSL VPN.
588760	Inappropriate message before FortiGate local user password expires.

Sandbox

Bug ID	Description
576613	FortiClient should use the timezone value from EMS profile to query cloud server list.
584965	FortiClient Sandbox fails to apply new sandbox detection level after EMS updates sandbox detection level.
584969	FortiClient Sandbox fails to detect office files directly opened in Web Outlook mail.

Vulnerability Scan

Bug ID	Description
510597	FortiClient fails to patch OS vulnerabilities on Windows 10 x64 platform when a Windows update is outstanding.
525603	FortiClient reports the same vulnerabilities after EMS triggers patching of all high and critical vulnerabilities.
537016	Vulnerability Scan does not always scan on next startup if off during scheduled scan time.
548614	FortiClient VCM logs have no limit and consume a lot of disk space.

Web Filter

Bug ID	Description
510462	FortiClient does not show correct block message for Unknown category.
579458	On Dell XPS 15 7590, laptop throughput goes down when FortiClient is installed.
584947	Web Filter plugin for Chrome browser fails to show customized block page for blacklisted URL.

Other

Bug ID	Description
534383	FortiClient *Settings* page fails to preserve *Disable Fortiproxy* setting after switching FortiClient tabs.
566084	FortiClient downloads all signature updates after fresh install without registering to EMS to receive a valid license.
571597	GPO update fails due to FortiClient FortiShield blocking the modification of a registry key.
578532	FortiClient has no event log when FortiGuard server `sfctwf.fortinet.net` is not reachable.
579772	FortiClient cannot get signature from FortiManager using HTTPS due to failed certificate check.
585107	FortiClient will not trust certificate trusted by Windows.
587789	CEF standard violation.
087179	No log for removable device control.

Change log

Date	Change Description
2019-10-15	Initial release of FortiClient (Windows) 6.2.2.
2019-10-16	Updated Product integration and support on page 9.
2019-10-28	Updated Product integration and support on page 9.
2019-12-05	Updated Product integration and support on page 9.