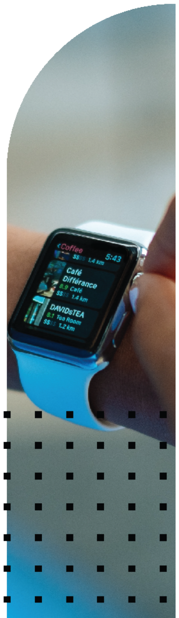
Release Notes

FortiClient (Windows) 7.0.3



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

FORTINET®

February 28, 2022
FortiClient (Windows) 7.0.3 Release Notes
04-703-766527-20220228

TABLE OF CONTENTS

Change log

Date	Change Description
2022-02-28	Initial release of 7.0.3.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 7.0.3 build 0193.

- What's new in FortiClient (Windows) 7.0.3 on page 7
- Installation information on page 8
- Product integration and support on page 10
- Resolved issues on page 13
- Known issues on page 18

Review all sections prior to installing FortiClient.

Licensing

See Windows, macOS, and Linux endpoint licenses.

FortiClient 7.0.3 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.

What’s new in FortiClient (Windows) 7.0.3

For information about what's new in FortiClient (Windows) 7.0.3, see the *FortiClient & FortiClient EMS 7.0 New Features Guide*.

Installation information

Firmware images and tools

The following files are available in the firmware image file folder:

File	Description
FortiClientTools_7.0.3.xxxx.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_7.0.3.xxxx.zip	FSSO-only installer (32-bit).
FortiClientSSOSetup_7.0.3.xxxx_x64.zip	FSSO-only installer (64-bit).
FortiClientVPNSetup_7.0.3.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_7.0.3.xxxx_x64.exe	Free VPN-only installer (64-bit).

EMS 7.0.3 includes the FortiClient (Windows) 7.0.3 standard installer and zip package containing FortiClient.msi and language transforms.

The following tools and files are available in the FortiClientTools_7.0.xx.xxxx.zip file:

File	Description
FortiClientVirusCleaner	Virus cleaner.
OnlineInstaller	Installer files that install the latest FortiClient (Windows) version available.
SSLVPNcmdline	Command line SSL VPN client.
SupportUtils	Includes diagnostic, uninstallation, and reinstallation tools.
VPNAutomation	VPN automation tool.
VC_redist.x64.exe	Microsoft Visual C++ 2015 Redistributable Update (64-bit).
vc_redist.x86.exe	Microsoft Visual C++ 2015 Redistributable Update (86-bit).

The following files are available on FortiClient.com:

File	Description
FortiClientSetup_7.0.3.xxxx.zip	Standard installer package for Windows (32-bit).
FortiClientSetup_7.0.3.xxxx_x64.zip	Standard installer package for Windows (64-bit).

File	Description
FortiClientVPNSetup_ 7.0.3.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_ 7.0.3.xxxx_x64.exe	Free VPN-only installer (64-bit).

Review the following sections prior to installing FortiClient version 7.0.3: Introduction on page 6 and Product integration and support on page 10.

Upgrading from previous FortiClient versions

To upgrade a previous FortiClient version to FortiClient 7.0.3, do one of the following:

- Deploy FortiClient 7.0.3 as an upgrade from EMS. With the endpoint security improvement feature, there are backward compatibility issues to consider while planning upgrades. See Recommended upgrade path.
- Manually uninstall existing FortiClient version from the device, then install FortiClient (Windows) 7.0.3

FortiClient (Windows) 7.0.3 features are only enabled when connected to EMS 7.0.

See the *FortiClient and FortiClient EMS Upgrade Paths* for information on upgrade paths.

You must be running EMS 7.0.2 or later before upgrading FortiClient.

Downgrading to previous versions

FortiClient (Windows) 7.0.3 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 Checksum*, enter the image file name, including the extension, and select *Get Checksum Code*.

Product integration and support

The following table lists version 7.0.3 product integration and support information:

Desktop operating systems	• Microsoft Windows 11 (64-bit) • Microsoft Windows 10 (32-bit and 64-bit) • Microsoft Windows 8.1 (32-bit and 64-bit) • Microsoft Windows 7 (32-bit and 64-bit) FortiClient 7.0.3 does not support Microsoft Windows XP and Microsoft Windows Vista.
Server operating systems	• Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 FortiClient 7.0.3 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 antivirus (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
AV engine	• 6.00258
FortiAnalyzer	• 7.0.0 and later
FortiAuthenticator	• 6.4.0 and later • 6.3.0 and later • 6.2.0 and later • 6.1.0 and later • 6.0.0 and later

FortiClient EMS	• 7.0.0 and later
FortiManager	• 7.0.0 and later
FortiOS	The following FortiOS versions support Zero Trust Network Access with FortiClient (Windows) 7.0.3. This includes both ZTNA access proxy and ZTNA tags: • 7.0.4 and later The following FortiOS versions support IPsec and SSL VPN with FortiClient (Windows) 7.0.3: • 7.0.0 and later • 6.4.0 and later • 6.2.0 and later • 6.0.0 and later
FortiSandbox	• 4.0.0 and later • 3.2.0 and later • 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	GUI	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.

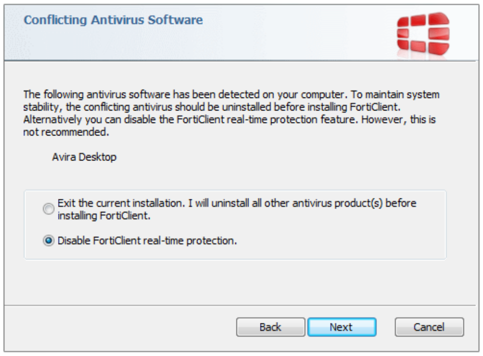
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

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 it finds any, 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 7.0.3. For inquiries about a particular bug, contact Customer Service & Support.

Zero Trust Telemetry

Bug ID	Description
765348	FortiClient (Windows) detects invalid certificate after FortiClient (Windows) upgrade.

GUI

Bug ID	Description
751299	FortiClient (Windows) has empty vulnerability details tab.
765714	FortiClient (Windows) shows encryption as disabled when EMS-pushed rule has encryption enabled.

Endpoint control

Bug ID	Description
742070	FortiClient is stuck syncing and cannot be manually reconnected.
751728	FortiClient (Windows) does not automatically connect to EMS after manual FortiClient (Windows) upgrade.
757985	EMS group assignment rule does not work.

Install and deployment

Bug ID	Description
716597	Install using `norestart` parameter requires reboot.

Bug ID	Description
742508	You can uninstall FortiClient (Windows) using CCleaner when *Require password for Disconnect* is enabled.

Application Firewall

Bug ID	Description
663024	Add VMware Horizon virtual desktop infrastructure agent signature on Application Firewall.

Zero Trust tags

Bug ID	Description
652897	FortiClient (Windows) tags endpoint as vulnerable when EMS has enabled *Exclude Application Vulnerabilities Requiring Manual Update from Vulnerability*.
683099	Host tagging rule for 2019 operating system version does not work.
726729	Windows firewall Zero Trust tagging rule does not tag FortiClient (Windows) when Web Filter is enabled via a group policy object (GPO).

Malware Protection and Sandbox

Bug ID	Description
688725	Add browser support for new antiexploit.
693565	Chrome cannot rename temporary download files because Sandbox agent locks them.
700298	FortiClient (Windows) does not submit zip files larger than 200 MB to FortiSandbox.
700396	FortiClient (Windows) cannot load the device driver (code 38).
709729	Realtime_scan log disappears after ten seconds.
713557	Antiexploit exceptions do not work.
725936	FortiClient compatibility with USB key.
734993	Rule to block removable media (USB drive) stops working.
737561	Files quarantined on client do not sync with FortiClient Cloud.
754593	Removable media access does not work for selected devices.

Bug ID	Description
759271	FortiClient fails to quarantine a read-only file.
759692	Removable media access does not block camera.

FSSO

Bug ID	Description
683213	FortiClient SSO Mobility Agent does not update logon events/IP address changes to FortiAuthenticator and intermittently fails to send information.

Remote Access

Bug ID	Description
599924	Certificate-based IKEv2 cannot connect with extensible authentication protocol disabled.
637303	Configuring certificate-only SSL VPN tunnel displays *Empty username is not allowed* error.
639981	SAML login on FortiClient (Windows) does not work when PKI group and SAML group are assigned to SSL VPN policy together.
684913	SAML authentication on SSL VPN with realms does not work.
685959	When Windows starts, machine IPsec VPN does not connect.
692823	Split DNS tunnel has resolution time of more than 30 seconds.
693611	FortiClient (Windows) fails to show correct current connection.
698713	You can update an SSL VPN user's password without entering the same password to confirm it.
700440	Application-based split tunnel does not work.
707882	IPsec VPN fails to autoconnect with *Failed to launch IPsec service* error.
710877	SSL VPN with SAML (Azure Active Directory (AD)) and two gateways does not work.
716323	FortiClient (Windows) cannot connect to IPsec VPN and shows no response from GUI.
716952	On connect script for Windows does not always execute.
717100	MTU issues when DTLS is enabled and client network tunnels IPv4 over IPv6.
721651	When connected to a full VPN to FortiGate, FortiClient sends virtual IP and MAC addresses to EMS.
724092	`match_type` does not work when using VPN before logon.
726249	FortiClient (Windows) cannot exempt the trusted fully qualified domain names and trusted local

Bug ID	Description
	applications effectively from FortiSASE VPN.
726680	VPN client takes 20 seconds to disconnect.
727967	FortiClient (Windows) should not resend authentication request after SAML login.
731011	FortiClient (Windows) gets stuck at 98% connecting to SSL VPN tunnel when integrated with SAML (Azure AD) authentication.
732594	SSL VPN `redundant_sort_method` does not work with realms.
735096	Remove old SSL VPN driverpppop64.sys.
740410	FortiClient (Windows) applies `client-cert` to unmatched SSL VPN mapping.
742833	Machine VPN before logon does not connect anymore after update from 7.0.0 to 7.0.1.
744945	VPN before logon cannot connect before Windows logon, so the GPO cannot commit before logon.
750008	FortiClient caches username for VPN tunnel when it is configured not to.
751430	Split tunnel, split DNS, and remote DNS server resolution do not work.
754820	Host check *Enable for Firewall only* does not work.
764730	FortiClient cannot enable the dual-stack IPv4/IPv6 from EMS using `<dual_stack>`.
771369	SSL VPN autoconnect does not work sometimes.

Web Filter and plugin

Bug ID	Description
647955	FortiClient (Windows) is involved in traffic when Web Filter is enabled.
740802	Web Filter has many unknown category denylist results.
760972	Chrome pauses file download until user manually resumes it.

Other

Bug ID	Description
722624	Windows 10 21H1 upgrade causes blue screen of death (BSOD) (`SYSTEM_SCAN_AT_RAISED_IRQL_CAUGHT_IMPROPER_DRIVER_UNLOAD`) FortiTransCtrl.sys.
725631	Network interfaces on laptops with Windows 10 stay unavailable after hibernation or sleep.

Bug ID	Description
733704	BSOD Fortips.sys.
737917	FortiClient support for Windows 11.
772310	Shutting down FortiTray from command prompt does not work.
749458	When logging in to FortiClient (Windows) using a Google account, FortiClient (Windows) shows a specific unofficial email address.

Common Vulnerabilities and Exposures

Bug ID	Description
637256	FortiClient (Windows) 7.0.3 is no longer vulnerable to the following CVE Reference: • CVE-2021-36183 Visit https://fortiguard.com/psirt for more information.
721745	FortiClient (Windows) 7.0.3 is no longer vulnerable to the following CVE Reference: • CVE-2021-41028 Visit https://fortiguard.com/psirt for more information.

Known issues

The following issues have been identified in FortiClient (Windows) 7.0.3. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Install and upgrade

Bug ID	Description
749094	FortiClient (Windows) does not display prompt when downloading an installer fails due to an invalid certificate.
749331	Windows Security setting in Windows displays *FortiClient is snoozed* when FortiEDR is installed.
773219	FortiClient (Windows) should not allow user to uninstall it if settings are unlocked.
774278	`/quiet` installer option does not work with FortiClientVPNOnlineInstaller.
784992	Failed to install FortiClient (Windows) with repackaged installer with FIPS feature.

Application Firewall

Bug ID	Description
717628	Application Firewall causes issues with Motorola RMS high availability client.
749797	Application Firewall decreases network bandwidth while transferring files.
776007	Application Firewall conflict with Windows firewall causes issues updating domain group policies.

GUI

Bug ID	Description
752084	FortiClient (Windows) GUI does not completely block Sandbox exclusion list and scrolling is impossible.
773355	FortiClient has display issue with umlauts on the Web Filter tab.

Zero Trust tags

Bug ID	Description
726835	FortiOS cannot get the updated VPN IP address in firewall dynamic EMS tag address when FortiClient establishes the VPN tunnel.
740708	FortiClient (Windows) does not tag Windows 7 endpoint as having its antivirus signature up-to-date.
763868	FortiClient cannot identify domain/local users if they have the same username.
770636	FortiClient (Windows) does not remove Zero Trust Network Access (ZTNA) tag for antivirus signature being up-to-date.
775396	User-specified tag fails to work.
778435	FortiClient (Windows) only shows Zero Trust tags in avatar page.
782394	ZTNA user identity tags do not work.
782869	Zero trust tag fails to work for file with environments variable in its file path.

Endpoint control

Bug ID	Description
738813	FortiESNAC process causes high CPU.
770637	User cannot remove endpoint from quarantine with one-time access code.
779267	FortiClient does not get updated profile and does not sync.
780450	FortiClient (Windows) fails to apply log setting.
783186	FortiESNAC.exe CLI `-m` option does not work.

Endpoint management

Bug ID	Description
760816	Group assignment rules based on IP addresses do not work when using split tunnel.

Configuration

Bug ID	Description
762303	FortiClient (Windows) cannot restore the backup file when the backup file's file path contains a multibyte character.

Endpoint policy and profile

Bug ID	Description
774890	FortiClient (Windows) does not receive updated profile after syncing imported Web Filter profile from EMS.

Performance

Bug ID	Description
749348	Performance issues after upgrade.

Zero Trust Telemetry

Bug ID	Description
683542	FortiClient (Windows) fails to register to EMS if registration key contains a special character: " !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~".
763957	FortiClient (Windows) prompts for telemetry key when telemetry key has changed on EMS.

Malware Protection and Sandbox

Bug ID	Description
721038	FortiClient (Windows) fails to block SD cards when default removable media access is blocked.
730054	*Allow Admin Users to Terminate Scheduled and On-Demand Scans from FortiClient Console* feature does not work as expected.

Bug ID	Description
732497	Updating signatures from GUI does not work.
753672	FortiClient (Windows) logs do not indicate threat level.
754098	Antiransomware detects and stops original sample but replica keeps executing at regular intervals.
758665	Antiexploit protection list should be updated to have Chrome and Firefox.
760073	FortiClient (Windows) compatibility with USB.
762125	fortimon3.sys causes blue screen of death during Slack calls.
764558	Quarantine suspected ransomware files after process detection or termination.
780393	FortiClient (Windows) does not block USB access when default rule is to block.

Remote Access

Bug ID	Description
649426	IPsec/SSL VPN per-app VPN split tunnel does not work.
710783	With per-machine and user autoconnect configured, per-machine tunnel drops in minutes before logging onto Windows.
711402	Per-user autoconnect does not establish and per-machine autoconnect remains connected after logging onto Windows.
724452	IPsec VPN with multiple gateways does not connect to the second gateway if the first one is inaccessible when the certificate is used.
724632	SAML logout does not work.
727695	FortiClient (Windows) on Windows 10 fails to block SSL VPN when it has a prohibit host tag applied.
729610	When using Spanish characters, saving username and password are activated, but FortiClient (Windows) saves encrypted password incorrectly.
730398	Always-up feature does not work for IPsec VPN when connecting from tray.
731127	Configuring SSL VPN tunnel with SAML login displays *Empty username is not allowed* error.
731912	FortiClient does not register any interface's IP addresses to the DNS server when IPsec VPN tunnel is up.
734866	Per-machine autotunnel before OS start keeps trying to connect after failing to connect to VPN.
743106	IPsec VPN XAuth does not work with ECDSA certificates.
744544	FortiClient (Windows) always saves SAML credentials.
744597	SSL VPN disconnects and returns hostcheck timeout after 15 to 20 minutes of connection.

Bug ID	Description
754665	Resilient IPSec VPN tunnel is stuck in connection when failing over from first FortiGate to second if user password is not saved.
763611	Slow upload speed on `ssl-vpn dual-stack`.
764863	Dialup IPsec VPN over IPv6 drops packets on inbound direction once FortiClient (Windows) establishes tunnel.
765184	RADIUS authentication failover between two servers.
767947	SMS verification code/answer code overwrites IPsec VPN saved password.
768829	GUI shows incorrect tunnel name after VPN is up.
771090	Save username function on IPsec VPN tunnel does not work.
773060	When connected to VPN on wireless connection, Surface Pro cannot access SSRS report (software hosted on internal server).
776888	FortiClient (Windows) does not dynamically display *Disconnect* button unless user reopens console.
778738	IPsec VPN IPv6 remote gateway is missing from GUI.
779670	FortiClient (Windows) shows SSL VPN password as expired when the password has not expired.
782201	With an always-up VPN connection with multifactor authentication enabled, FortiClient fails to display popup for entering token code when reconnecting.
782352	FortiClient fails to perform XAuth with RSA certificates being used
782698	IPsec VPN on OS start with SSL VPN failover on Wi-Fi cannot connect.
784822	FortiSASE VPN doesn't automatically connect back after FortiClient (Windows) is upgraded from 6.4.6 GA to 7.0.3 latest Interim build.
785709	FortiClient (Windows) ipv6 site will not work after disconnect ipsec if the app firewall is enabled.
785853	FortiClient (Windows) SAML SSL VPN is stuck at authentication step with Okta.
786210	FortiClient (Windows) tries to connect to two FortiGate units and fails.

Vulnerability Scan

Bug ID	Description
741241	FortiClient (Windows) finds vulnerabilities for uninstalled software.
780815	Scheduled scan does not work.

Web Filter and plugin

Bug ID	Description
729127	Web Filter affects manufacturing execution system software.
757886	Internet connection issue after adding extension to the browser.
760182	Web Filter plugin does not work on x86 Windows 7 and Windows 8.1.
776089	FortiClient (Windows) does not block malicious sites when Web Filter is disabled.
784677	Web Filter plugin blocking YouTube comments with "Restricted Mode has hidden comments for this video".

Avatar and social network login

Bug ID	Description
729140	FortiClient (Windows) fails to work when attempting to log in with Google, LinkedIn, or Salesforce.
779387	FortiClient fails to set avatar and user information using Google social login.

Multitenancy

Bug ID	Description
780308	EMS automatically migrates endpoints to default site.

ZTNA connections

Bug ID	Description
742103	ZTNA connection rule deletion does not take effect immediately.
778612	FortiClient (Windows) routes ZTNA traffic via FortiSASE FortiGate instead of directly to ZTNA FortiGate.

License

Bug ID	Description
776869	FortiClient (Windows) should not hard code ZTNA license.

FIPS

Bug ID	Description
766616	Entering FIPS error mode does not shut down FortiClient (Windows) including GUI.
766623	If self-test fails during VPN connection, FortiClient (Windows) does not enter FIPS error mode.
766945	FortiClient does not send statistics to FortiGuard Distribution Servers for FIPS features.
769107	With FIPS enabled, FortiClient (Windows) imports unsupported encryption or authentication algorithm.
769191	FIPS allow use of 1024 bit certificate.

Logs

Bug ID	Description
778988	FortiClient (Windows) cannot report features to FortiAnalyzer.
776001	FortiClient (Windows) generates security information and event management log after deregistering.

Other

Bug ID	Description
780651	FortiClient (Windows) does not update signatures on expected schedule.
782630	User cannot open GUI via tray or desktop shortcut.

www.fortinet.com