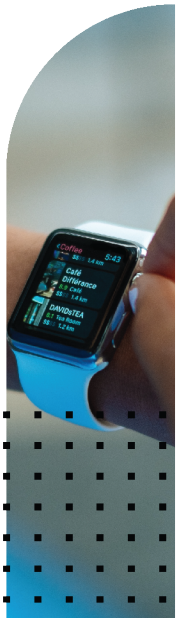
Release Notes

FortiClient (Windows) 7.0.6



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/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

July 05, 2022
FortiClient (Windows) 7.0.6 Release Notes
04-706-805981-20220705

TABLE OF CONTENTS

Change log

Date	Change Description
2022-07-05	Initial release of 7.0.6.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 7.0.6 build 0290.

Review all sections prior to installing FortiClient.

Licensing

See Windows, macOS, and Linux endpoint licenses.

FortiClient 7.0.6 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.

Special notices

Upgrade issue

FortiClient may fail to upgrade to 7.0.6 if the upgrade is attempted using a local upgrade (MSI or FortiClientSetup.exe file), due to FortiShield blocking an update. Use one of the following workarounds:

- Use EMS to deploy FortiClient 7.0.6 to endpoints.
- To run a local FortiClient upgrade, do the following:
  a. Shut down FortiClient.
  b. Stop FortiShield.
  c. Perform the local FortiClient upgrade using MSI or the FortiClientSetup.exe file

Installation information

Firmware images and tools

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

File	Description
FortiClientTools_7.0.6.xxxx.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_ 7.0.6.xxxx.zip	Fortinet Single Sign On (FSSO)-only installer (32-bit).
FortiClientSSOSetup_ 7.0.6.xxxx_x64.zip	FSSO-only installer (64-bit).
FortiClientVPNSetup_ 7.0.6.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_ 7.0.6.xxxx_x64.exe	Free VPN-only installer (64-bit).

EMS 7.0.6 includes the FortiClient (Windows) 7.0.6 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_7.0.6.xxxx.zip	Standard installer package for Windows (32-bit).
FortiClientSetup_7.0.6.xxxx_ x64.zip	Standard installer package for Windows (64-bit).

File	Description
FortiClientVPNSetup_ 7.0.6.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_ 7.0.6.xxxx_x64.exe	Free VPN-only installer (64-bit).

Review the following sections prior to installing FortiClient version 7.0.6: 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 7.0.6, do one of the following:

- Deploy FortiClient 7.0.6 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) 7.0.6.

FortiClient (Windows) 7.0.6 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) 7.0.6 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 Checksum*, enter the image file name, including the extension, and select *Get Checksum Code*.

Product integration and support

The following table lists version 7.0.6 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 7.0.6 does not support Microsoft Windows XP and Microsoft Windows Vista. There is no plan for FortiClient to support zero trust network access (ZTNA) TCP forwarding on Windows 7.
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 7.0.6 does not support Windows Server Core. For Microsoft Windows Server, FortiClient (Windows) supports the Vulnerability Scan, SSL VPN, Web Filter, and antivirus (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
AV engine	• 6.00266
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 (ZTNA) with FortiClient (Windows) 7.0.6. This includes both ZTNA access proxy and ZTNA tags: • 7.0.6 and later The following FortiOS versions support IPsec and SSL VPN with FortiClient (Windows) 7.0.6: • 7.0.0 and later • 6.4.0 and later • 6.2.0 and later • 6.0.0 and later
FortiSandbox	• 4.2.0 and later • 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.

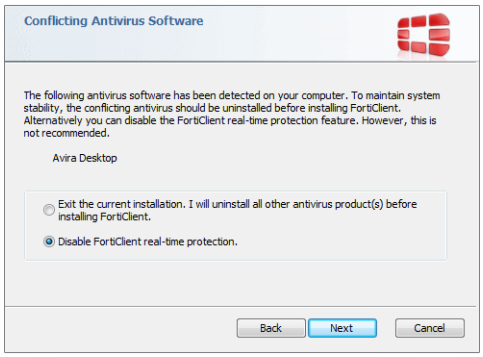
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

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, 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.



Resolved issues

The following issues have been fixed in version 7.0.6. For inquiries about a particular bug, contact Customer Service & Support.

ZTNA connection rules

Bug ID	Description
798057	Zero trust network access (ZTNA) connection rule issue when FortiClient is on-fabric.

Performance

Bug ID	Description
814057	FortiClient upgrade results in blue screen of death due to DRIVER OVERRAN STACK BUFFER error in FortiShield.

GUI

Bug ID	Description
793577	Disclaimer message is unreadable.

Endpoint control

Bug ID	Description
723599	FortiClient uses FortiSASE egress IP address as the public IP address.
780368	When FortiClient (Windows) requires a password for disconnecting from EMS, *Allow User to Shutdown When Registered to EMS* fails to work.
806052	Surge of DNS and LDAP traffic.
817257	FortiClient GROUP_TAG is empty.

Install and deployment

Bug ID	Description
791538	EMS deployments can fail when requiring FortiClient (Windows) user to enter password to disconnect from EMS.

Application Firewall

Bug ID	Description
654152	Configuring Application Firewall to block *All Other Unknown Applications* blocks allowed categories.
790397	IPv6 traffic is blocked when FortiClient is enabled.

Zero Trust tags

Bug ID	Description
731525	FortiClient (Windows) does not properly detect Zero Trust tag for not having antivirus up-to-date.
782869	Zero Trust tag fails to work for file with environments variable in its file path.
803426	FortiClient reports BitLocker as disabled when it is enabled.

License

Bug ID	Description
776869	FortiClient (Windows) hard codes ZTNA license.

Remote Access

Bug ID	Description
634609	FortiClient credential provider displays the wrong domain when logging in to Windows 10.

Bug ID	Description
684913	SAML authentication on SSL VPN with realms does not work.
711402	FortiClient (Windows) does not establish per-user autoconnect tunnel, and per-machine autoconnect remains connected after logging in to Windows.
714688	IPsec VPN login is not possible when password includes German umlaut.
729610	When a password includes special characters and user enables FortiClient (Windows) to save their username and password, FortiClient (Windows) saves the encrypted password incorrectly.
763611	If dual stack is enabled and user successfully connects to tunnel with IPv6 and tries to access an IPv4 server to upload/download some files, the network speed is slow.
776888	FortiClient does not dynamically display button to disconnect VPN unless you reopen the FortiClient (Windows) window.
782393	Application-based split VPN tunnel has issue when using VipWebAppServer.exe application.
784822	FortiSASE VPN does not automatically reconnect after upgrading FortiClient.
786348	Error code -8 or -14 displays when limiting users to one SSL VPN connection at a time is enabled on FortiOS with SAML authentication.
788765	A password that includes the German characters "" and/or "$" activates the SAML button.
796852	Using application-based split tunnel with an exclusion rule disrupts access to local resources.
798044	Using Finnish front vowels [/] in the SSL VPN password causes issues when FortiClient (Windows) saves the password.
807267	SSL VPN drops when datagram transport layer security and application split tunnel are enabled.
807759	SAML does not prompt for credentials and crashes the GUI.

Malware Protection and Sandbox

Bug ID	Description
584975	Context menu fails to show option to scan with Sandbox when Malware Protection is disabled.
638227	USB detection notifications lack accurate device descriptions.
721038	FortiClient (Windows) fails to block SD cards when configured to block default removable media access.
801161	Antiransomware has false positive on Microsoft Office.

Configuration

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

Installation and upgrade

Bug ID	Description
773219	FortiClient (Windows) allows user to uninstall FortiClient when administrator has locked the setting.

Vulnerability Scan

Bug ID	Description
740061	FortiClient (Windows) only detects and reports one instance of log4net.

Other

Bug ID	Description
658098	FortiShield prevents FortiClient processes from modifying a file or registry settings that FortiClient (Windows) is protecting.

Known issues

The following issues have been identified in FortiClient (Windows) 7.0.6. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Install and upgrade

Bug ID	Description
726616	FortiClient may fail to upgrade to 7.0.6 if the upgrade is attempted using a local upgrade (MSI or FortiClientSetup.exe file), due to FortiShield blocking an update. **Workaround**: Do one of the following: • Use FortiClient EMS to do the deployment. • To run a local FortiClient upgrade, do the following: **a.** Shut down FortiClient. **b.** Stop FortiShield. **c.** Perform the local FortiClient upgrade using MSI or the FortiClientSetup.exe file.
749331	Windows Security setting in Windows displays *FortiClient is snoozed* when FortiEDR is installed.
820672	ZTNA driver FortiTransCtrl.sys fails to start up on Windows Server 2016.

Application Firewall

Bug ID	Description
717628	Application Firewall causes issues with Motorola RMS high availability client.
776007	Application Firewall conflict with Windows firewall causes issues updating domain group policies.
817932	Application Firewall fails to allow application signatures added under Application Overrides as allow.

GUI

Bug ID	Description
767998	Free VPN-only client includes *Action for invalid EMS certificate* in settings.
773355	FortiClient has display issue with umlauts on the Web Filter tab.

Zero Trust tags

Bug ID	Description
704234	Zero Trust tagging rule set syntax does not check registry key values.
726835	FortiOS cannot get the updated VPN IP address in firewall dynamic EMS tag address when FortiClient establishes the VPN tunnel.
782394	ZTNA user identity tags do not work.
802261	FortiClient does not trigger tag message for network event changes.
819120	Zero trust tag rule for Active Directory group does not work when registering FortiClient to EMS with onboarding user.
821391	Zero trust tag rule for Active Directory group does not tag user in security group.

Endpoint control

Bug ID	Description
738813	FortiESNAC process causes high CPU.
753663	When using off-net profile with antivirus protection enabled, FortiClient (Windows) does not show Malware Protection in navigation bar.
779267	FortiClient does not get updated profile and does not sync with EMS.
804552	FortiClient shows all feature tabs without registering to EMS after upgrade.
808880	FortiClient fails to synchronize with EMS on Windows 7 x86 platform for long time.
811951	After EMS license expires, FortiClient (Windows) still shows ZTNA and Application Firewall tabs.
815037	After administrator selects *Mark All Endpoints As Uninstalled*, FortiClient (Windows) connected with verified user changes to unverified user.
816751	Administrator cannot restore a quarantined file through EMS quarantine management if FortiClient (Windows) registered as onboarding user.
817061	Redeploying from another EMS server causes FortiClient (Windows) to not reconnect to EMS automatically.
819552	After upgrading FortiClient with EMS local onboarding user with LDAP, FortiClient (Windows) prompts for registration authentication.
821024	FortiClient fails to send username to EMS, causing EMS to report it as different users.
823386	FortiClient fails to send correct public IP address to EMS if registered to EMS as a SAML onboarding user.

Endpoint management

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

Configuration

Bug ID	Description
730415	FortiClient backs up configuration that is missing locally configured ZTNA connection rules.

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
676424	NETIO.SYS causes blue screen of death on FortiClient endpoints.
749348	Performance issues after upgrade.
778651	Large downloads and speed tests result in high latency, packet loss, and poor performance.

Zero Trust Telemetry

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

Malware Protection and Sandbox

Bug ID	Description
730054	*Allow Admin Users to Terminate Scheduled and On-Demand Scans from FortiClient Console* feature does not work as expected.
760073	FortiClient (Windows) compatibility with USB.
762125	fortimon3.sys causes blue screen of death during Slack calls.
774010	FortiClient does not block access to removable media.
793926	FortiShield blocks spoolsv.exe on Citrix virtual machine servers.
802576	Bluetooth device class access and HID do not work as expected.

Remote Access

Bug ID	Description
649426	IPsec/SSL VPN per-app VPN split tunnel does not work.
727695	FortiClient (Windows) on Windows 10 fails to block SSL VPN when it has a prohibit host tag applied.
728240	SSL VPN negate split tunnel IPv6 address does not work.
728244	Negate split tunnel IPv4 address does not work for dual stack mode using IPv6 access.
730756	For SSL VPN dual stack, GUI only shows IPv4 address.
731127	Configuring SSL VPN tunnel with SAML login displays *Empty username is not allowed* error.
742279	FortiClient to FortiGate SSL VPN gets stuck during connection with SAML.
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.
755105	When VPN is up, changes for *IP properties-> Register this connection's IP to DNS* are not restored after VM reboot from power off.
755482	Free VPN-only client does not show token box on rekey and GUI open.
758424	Certificate works for IPsec VPN tunnel if put it in current user store but fails to work if in local machine.
762986	FortiClient (Windows) does not use second FortiGate to connect to resilient tunnel from FortiTray if it cannot reach first remote gateway.
764863	Dialup IPsec VPN over IPv6 drops packets on inbound direction once FortiClient (Windows)

Bug ID	Description
	establishes tunnel.
767947	SMS verification code/answer code overwrites IPsec VPN saved password.
771090	Save username function on IPsec VPN tunnel does not work.
772108	When `no_dns_registration=1`,*Register This Connection's Address in DNS* of NW IP properties is not selected after VPN is up.
773060	When connected to VPN on wireless connection, Surface Pro cannot access SSRS report (software hosted on internal server).
778738	IPsec VPN IPv6 remote gateway is missing.
778822	When *Limit Users to One SSL-VPN Connection at a Time* is enabled on FortiOS, FortiClient displays error code -8.
782698	IPsec VPN on OS start with SSL VPN failover on Wi-Fi cannot connect.
787123	FortiClient disconnects from IPsec VPN tunnel with *SA hard expired* error right after connecting.
790021	Multifactor authentication using Okta with email notification does not work.
793893	FortiClient search domains transfer incorrectly to endpoints.
794110	VPN before logon does not work with Okta multifactor authentication and enforcing acceptance of the disclaimer message.
794658	FortiClient does not use second FortiGate to make VPN connection when IPsec VPN resilience with VPN is up and first remote gateway becomes offline.
795334	Always up feature does not work as expected when trying to connect to VPN from tray.
797816	SAML connection with external browser authentication and single sign on port 8020 is busy, with FortiClient returning a JavaScript error.
801599	FortiClient opens multiple browser tabs when connecting to SSL VPN via SAML using external browser.
801674	SAML internal browser authentication prompt does not show up when redirection to external browser is disabled.
802809	Routes are missing when using DHCP over IPsec VPN.
807258	VMware Horizon client does not work with application-based split tunnel.
815528	If `allow_local_lan=0` and per-application split tunnel with exclude mode and full tunnel are configured, FortiClient (Windows) should block local RDP/HTTPS traffic.
821994	VPN does not disconnect if user deregisters FortiClient from the FortiSASE GUI.

Vulnerability Scan

Bug ID	Description
741241	FortiClient (Windows) finds vulnerabilities for uninstalled software.

Logs

Bug ID	Description
713287	FortiClient does not generate local logs for ZTNA.

Web Filter and plugin

Bug ID	Description
776089	FortiClient (Windows) does not block malicious sites when Web Filter is disabled.
789017	Web Filter is enabled on FortiSASE profile on EMS when Web Filter is already enforced on the FortiGate.
812207	Blocked web client shows dropped connection message instead of URL blocked message.
812879	Web Filter blocks Chocolatey installation.
813034	FortiTray keeps notifying user to install Web Filter plugin even when Chrome has already installed the plugin.
823469	FortiClient console does not show security risk category as configured on EMS under Web Filter profile.
823477	Web Filter fails to block security risk category URLs when antivirus is enabled.

Avatar and social network login

Bug ID	Description
729140	FortiClient (Windows) fails to work when attempting to log in with Google, LinkedIn, or Salesforce.

Multitenancy

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

ZTNA connection rules

Bug ID	Description
735494	Windows 7 does not support TCP forwarding feature.
773956	FortiClient (Windows) cannot show normal webpage of Internet real server (Dropbox) with ZTNA.
814953	Using an external browser for SSH ZTNA requires restarting FortiClient on Windows 11.
823012	ZTNA TCP forwarding fails to work when FortiClient console is closed.

Administration

Bug ID	Description
798055	Javascript error occurs in the main process.

Other

Bug ID	Description
780651	FortiClient (Windows) does not update signatures on expected schedule.
812778	FortiShield fails to prevent user from killing FortiClient running processes.

www.fortinet.com