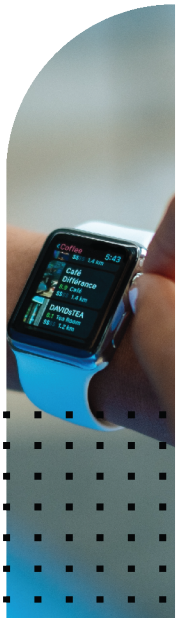
Release Notes

FortiClient (Windows) 7.0.8



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
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

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

February 09, 2024
FortiClient (Windows) 7.0.8 Release Notes
04-708-886312-20240209

TABLE OF CONTENTS

Change log

Date	Change description
2023-03-16	Initial release of 7.0.8.
2024-02-09	Updated Introduction on page 6.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 7.0.8 build 0427.

Review all sections prior to installing FortiClient.

FortiClient (Windows) 7.0.8 components that interact with Microsoft Security Center are signed with an Azure Code Signing certificate, which fulfills Microsoft requirements.

Licensing

See Windows, macOS, and Linux endpoint licenses.

FortiClient 7.0.8 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.

Installation information

Firmware images and tools

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

File	Description
FortiClientTools_7.0.8.0427.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_ 7.0.8.0427.zip	Fortinet single sign on (FSSO)-only installer (32-bit).
FortiClientSSOSetup_ 7.0.8.0427_x64.zip	FSSO-only installer (64-bit).
FortiClientVPNSetup_ 7.0.8.0427.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_ 7.0.8.0427_x64.exe	Free VPN-only installer (64-bit).

EMS 7.0.8 includes the FortiClient (Windows) 7.0.8 standard installer and zip package containing FortiClient.msi and language transforms.

The following tools and files are available in the FortiClientTools_7.0.xx.0427.zip file:

File	Description
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_7.0.8.0427.zip	Standard installer package for Windows (32-bit).
FortiClientSetup_7.0.8.0427_ x64.zip	Standard installer package for Windows (64-bit).

File	Description
FortiClientVPNSetup_ 7.0.8.0427.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_ 7.0.8.0427_x64.exe	Free VPN-only installer (64-bit).

Review the following sections prior to installing FortiClient version 7.0.8: Introduction on page 6 and Product integration and support on page 9.

Upgrading from previous FortiClient versions

To upgrade a previous FortiClient version to FortiClient 7.0.8, do one of the following:

- Deploy FortiClient 7.0.8 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) 7.0.8.

FortiClient (Windows) 7.0.8 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) 7.0.8 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 7.0.8 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 7.0.8 does not support Microsoft Windows XP and Microsoft Windows Vista. FortiClient does not 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 7.0.8 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. Microsoft Windows Server 2016 and 2019 support ZTNA with FortiClient (Windows) 7.0.8. As FortiClient does not support Application Firewall on a Windows Server machine, do not install the Application Firewall module on a Windows Server machine. Doing so may cause performance issues.
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	• 7.2.0 and later

	• 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	• 7.2.0 and later • 7.0.0 and later
FortiManager	• 7.2.0 and later • 7.0.0 and later
FortiOS	The following FortiOS versions support ZTNA with FortiClient (Windows) 7.0.8. This includes both ZTNA access proxy and ZTNA tags: • 7.2.0 and later • 7.0.6 and later The following FortiOS versions support IPsec and SSL VPN with FortiClient (Windows) 7.0.8: • 7.2.0 and later • 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		

Language	GUI	XML configuration	Documentation
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.

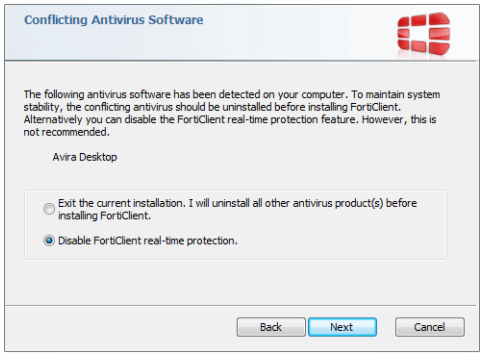
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

Conflicts with third party AV products

The AV feature in FortiClient is known to conflict with other similar products in the market.

- Do 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 FortiClient installation, 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.



Intune product code

Deploying FortiClient with Intune requires a product code. The product code for full-featured FortiClient 7.0.8 is {12C8C9B7-3C65-4B0E-9DCF-1A1451BABC75}. The product code for the FortiClient 7.0.8 VPN-only agent is {0272F040-0C81-4077-9AA7-82CCD495ADCA}.

See Configuring the FortiClient application in Intune.

Resolved issues

The following issues have been fixed in version 7.0.8. For inquiries about a particular bug, contact Customer Service & Support.

Endpoint control

Bug ID	Description
766241	Endpoint summary reports FortiClient antivirus (AV) software as third party feature.
815384	FortiClient (Windows) has delay in starting Web Filter service after status is off-Fabric.
832627	FortiClient (Windows) to EMS logging does not work as expected after zero trust network access (ZTNA) logging is enabled in System Settings profile.
833848	FortiClient reports incorrect Windows version to EMS.
839197	FortiClient does not reconnect to EMS after deployment over VPN.
839800	Option to hide Application Firewall feature from FortiClient (Windows) does not work with EMS 7.0.7.
841149	Endpoint tries to use ZTNA certificate when ZTNA option is disabled.
842680	FortiClient does not send ADGuid to EMS.
846147	EMS does not display user information details from Active Directory (AD) domain.

GUI

Bug ID	Description
836820	Realtime scan events shows as virus threads detected on German UI.
841355	GUI shows *Remote Access* tab despite being configured to be hidden.
853856	After FortiClient upgrade, Windows clients are stuck at black screen.
864653	FortiClient garbles Chinese name display.

Install and upgrade

Bug ID	Description
839744	FortiClient (Windows) loses telemetry and does not reconnect when administrator moves endpoint between assigned groups with different installers.
848255	Upgrading FortiClient fails with *...when it's registered to administration server* error.
871718	When installed with only AV and ZTNA features, FortiClient failed to sync profile from EMS.
691328	Upgrade does not upgrade AV engine as deployed through an EMS installer.

Vulnerability Scan

Bug ID	Description
811796	Python vulnerability is not excluded for all applications from vulnerability compliance check.
853934	User cannot perform vulnerability scan when EMS enables it as scan option is disabled on GUI.

Web Filter and plugin

Bug ID	Description
804938	All Internet traffic stops when user connects a USB controller (remote network driver interface specification).
826920	Web Filter extension does not work in Microsoft Edge.
829164	Security risk websites violation list are not on *Web Filter* tab.
833506	FortiClient (Windows) registry does not update restriction level value when Web Filter is disabled and reenabled.
836811	Safe Search adds wrong domain addresses such as www.google.n into host file C:\windows\system32\driver\etc.
840993	Upgrading FortiClient (Windows) causes Web Filter to break network connectivity.
851700	User sees popup from FortiClient (Windows) with *Microsoft Edge extension policy anomaly detected, please restart browser* error.
859979	FortiClient blocks web browsing traffic that Web Filter allows.
860560	Web Filter blocks private IP address as unrated.
875001	Firefox extension XPI file must be updated.

Zero Trust tags

Bug ID	Description
704234	Zero Trust tagging rule set syntax to check registry key value is unclear.
832623	AV signature is up-to-date rule does not count days since signature update.

Zero Trust Telemetry

Bug ID	Description
837859	FortiClient (Windows) has issues connecting to EMS after upgrade.
841719	FortiClient cannot connect to FortiClient Cloud.

Remote Access

Bug ID	Description
684913	SAML authentication on SSL VPN with realms does not work.
687765	VPN using SAML authentication gets a certificate warning with a certificate from DigiCert.
706023	FortiClient (Windows) loses DNS settings after restarting computer.
744544	FortiClient (Windows) always saves SAML credentials.
765686	When *autoconnect-only-when-offnet* is enabled, VPN autoconnects when endpoint shifts from off-fabric to on-fabric.
801599	FortiClient opens multiple browser tabs when connecting to SSL VPN via SAML using external browser.
822763	Remote Access *Connect* button does not work when user clicks it.
823350	Autoconnect works intermittently.
824165	SSL VPN does not reconnect when using tunnel-based FortiClient connection vs. PPP method.
825442	ZScaler Client Connector does not work with application-based split tunnel.
826170	FortiClient removes/wipes the SSL VPN password from the GUI if the network interface disconnects then reconnects.
829260	Autoconnect VPN starts unexpectedly without configuration.
829763	With host check enabled, SAML login does not show proper warning message if it failed to connect.
832953	VPN tunnel does not connect automatically always if network disruption or sleep mode occurs even

Bug ID	Description
	if always up is enabled.
834722	Autoconnect stops working.
834883	On-fabric rule for VPN tunnel name does not work when the tunnel name uses special characters.
835072	FortiClient blocks an internal application's activity to autoopen a saved HTML template.
836148	FortiClient does not attempt to connect to the realmhttps://X.Y:10443/Z if X and Z have same names.
836400	SSL VPN dual stack full tunnel leaks IPv6 access via local NIC.
838380	FortiClient (Windows) removes user credentials to the autoconnect VPN tunnel after a couple of restarts.
840685	Windows does not show the *VPN Before logon* icon in certain conditions.
840720	User cannot modify IPsec VPN advanced settings for personal VPN profile.
842560	FortiClient disables PolicyAgent and IKEEXT services when connecting to dial-up IPsec VPN.
846985	SAML SSL VPN occasionally fails due to failure to launch IPsec VPN service.
852036	FortiClient cannot correctly handle a certificate having Japanese characters in its issuer or subject.
859498	Current connection feature does not work as expected.
860618	FortiClient goes into connect/disconnect loop after authentication timeout expires.
870180	VPN before logon does not work after sleep/hibernation on Windows 10.
870316	Autoconnect does not work until first VPN connect is manually triggered.
871153	FortiClient tries to reuse the same saved password for other VPN connections even if they do not have *Save password* enabled.
872811	VPN before logon does not work.
873488	SSL VPN fails to work when using certificate in local computer.
876062	API connect does not work with certificate authentication.
878291	After registering to EMS using FortiSASE invitation code, FortiClient shows unable to reach tunnel gateway error.
885738	SSL VPN SAML login does not work.
887493	FortiClient fails to autoconnect when using SAML single sign on.

Malware Protection and Sandbox

Bug ID	Description
650383	Number of blocked exploits attempts does not work properly.
730172	FortiClient causes VMware Horizon Agent to disconnect from VMware Connection Server.
758665	Antiexploit protection list does not include Chrome and Firefox.
784126	FortiClient (Windows) shows antiexploit bubble message when option is disabled in EMS profile.
820068	FortiClient on Lenovo notebook with mobile WWAN shows blue screen at login.
826055	FortiDeviceGuard causes blue screen of death (BSOD).
844962	FortiClient (Windows) does not block phone mobile storage when default removable media access is set to block.
857482	FortiClient (Windows) built-in AV engine is not updated to 6.00282.
861296	AV scan exclusion list does not work for shared/network drive files.
863950	FortiClient reports the device as blocked but still allows access to it.
867087	cxwmbclass.sys causes BSOD.

Avatar and social login information

Bug ID	Description
805153	FortiClient (Windows) does not save user-specified *Submit User Identity Information* form.

SSO mobility agent

Bug ID	Description
803213	FSSO fails to send user login information, machine IP address, and other information to FortiAuthenticator.
868524	SSO configuration tool does not generate preshared key and server information in the installer.

Administration

Bug ID	Description
798055	JavaScript error occurs in the main process

Onboarding

Bug ID	Description
864582	After PC reboot, FortiClient repeatedly tries SAML login when disconnected from EMS.

ZTNA connection rules

Bug ID	Description
858271	ZTNA TCP forwarding does not work for SSH protocol.
870138	ZTNA certificate is not installed in personal store when only ZTNA component is installed.
877128	User in different country is unable to connect to ZTNA tunnel.

Other

Bug ID	Description
850528	FortiClient (Windows) does not always get IPv4 address from https://www.ipify.org.
863746	FortiProxy daemon cannot start up properly after machine reboot.

Common Vulnerabilities and Exposures

Bug ID	Description
838208	FortiClient (Windows) 7.0.8 is no longer vulnerable to the following CVE References: • CVE-2022-42470 Visit https://fortiguard.com/psirt for more information.
840897	FortiClient (Windows) 7.0.8 is no longer vulnerable to the following CVE References:

Bug ID	Description
	• CVE-2022-40682 Visit https://fortiguard.com/psirt for more information.
845295	FortiClient (Windows) 7.0.8 is no longer vulnerable to the following CVE References: • CVE-2022-43946 Visit https://fortiguard.com/psirt for more information.

Known issues

The following issues have been identified in FortiClient (Windows) 7.0.8. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

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.
814391	FortiClient Cloud application signatures block allowlisted applications.
844997	FortiClient sees several packet losses on different internal resources after connecting telemetry.
823292	FortiClient cannot connect to JVC wireless display.
827788	Threat ID is 0 on Firewall Events.
853451	FortiClient blocks PIA VPN.
853808	FortiClient (Windows) blocks Veeam with messages related to Remote.CMD.Shell and VeeamAgent.exe.
860062	Application Firewall slows down opening Microsoft Active Directory (AD) Users and Computers application.

Endpoint control

Bug ID	Description
753151	Updating endpoint status from endpoint notified to deployed takes a long time.
779267	FortiClient (Windows) does not get updated profile and does not sync.
780130	FortiClient (Windows) fails or takes long time to get updated Endpoint Control profile from EMS.
804552	FortiClient shows all feature tabs without registering to EMS after upgrade.
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.

Bug ID	Description
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.
827200	EMS displays no user for some devices.
833717	EMS shows endpoints as offline, while they show their own status as online.
834162	LDAP query for AD group check does not execute.
841764	EMS does not show third party features in endpoint information.
855851	EMS remembered list shows many FQDN duplicates.
868230	*Connection expiring due to FortiClient Connect license exceeded* error occurs.
880167	FortiClient (Windows) cannot register with EMS due to selecting wrong interface to connect to EMS.
899960	FortiESNAC process may stop after switching between two FortiSASE Endpoint Management Services.

Endpoint management

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

GUI

Bug ID	Description
767998	Free VPN-only client includes *Action for invalid EMS certificate* in settings.
811742	FortiClient (Windows) does not hide software update options when registered to EMS (regression).
826895	FortiClient ignores the listing order of the configured VPN connections in the GUI and tray.
827394	FortiClient does not report profile change update in *Notifications*.
847903	Console stops working on Citrix servers with ntdll.dll crash.
871005	GUI has display issue with certificates that contains non ASCII characters.

Install and upgrade

Bug ID	Description
749331	Windows Security setting in Windows displays *FortiClient is snoozed* when FortiEDR is installed.
769639	FortiDeviceGuard is not installed on Windows Server 2022.
820672	Zero trust network access (ZTNA) driver FortiTransCtrl.sys fails to start on Windows Server 2016.
867982	Blank certificate pops up when upgrading.
900228	On Windows 11 22H2, FortiClient upgrade deployment reboots immediately without asking user when to schedule upgrade regardless of EMS configuration.

Zero Trust tags

Bug ID	Description
782394	ZTNA user identity tags do not work.
819120	Zero trust tag rule for AD group does not work when registering FortiClient to EMS with onboarding user.
872794	AD group tag *Evaluate on FortiClient* feature does not work.

Configuration

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

User and authentication

Bug ID	Description
765184	RADIUS authentication failover between two servers for high availability does not work well.

Performance

Bug ID	Description
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: " !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~".
792703	FortiClient (Windows) cannot connect to FortiClient Cloud.

Malware Protection and Sandbox

Bug ID	Description
760073	FortiDeviceGuard could not be installed on Windows Server through installer.
793926	FortiShield blocks spoolsv.exe on Citrix virtual machine servers.
825732	SIM-card-slot UEFI feature slows down Windows logon when connected to VPN.
828862	FortiClient does not allow virtual CD-ROM device.
831560	GUI shows ransomware quarantined files after restoration via EMS.
833264	Antiexploit blocks Chrome browser without sharing payload details.
837638	Identifying malware and exploits using signatures received from FortiSandbox does not work.
844988	FortiClient (Windows) does not block USB drive if attempting to copy contents even if WPD/USB is set to be blocked in profile.
857041	Windows 10 security center popup shows both FortiClient and Windows Defender are turned off.
863802	EMS and FortiClient (Windows) cannot detect SentinelOne even if they have product on operating system level.
872970	Bubble notifications do not appear when inserting USB drive in endpoint machine.
876925	Antiexploit protection blocks Microsoft Signing application in Chrome.

Remote Access

Bug ID	Description
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.
736353	Multigateway failover does not go back to check previous gateways when failing over to see if they are up.
743106	IPsec VPN XAuth does not work with ECDSA certificates.
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) establishes tunnel.
772108	When `no_dns_registration=1`,*Register This Connection's Address in DNS* of NW IP properties is not selected after VPN is up.
773920	Endpoint switches network connection after IPsec VPN connection and causes VPN to disconnect.
775633	Automatic failover to second remote gateway does not work when using priority-based IPsec VPN resiliency tunnel.
783412	Browser traffic goes directly to ZTNA site when SSL VPN is connected.
790021	Multifactor authentication using Okta with email notification does not work.
792131	FortiClient (Windows) users report issues with the *Save Password* feature for SSL VPN.
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.
795334	Always up feature does not work as expected when trying to connect to VPN from tray.
800453	SSL VPN with certificate authentication fails to connect on OS start.

Bug ID	Description
801875	FortiClient cannot connect to VPN when there are two gateways listed using SAML.
814488	SSL VPN with `<on_os_start_connect>` enabled does not work when the machine is put into sleep mode and changes networks.
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.
816826	FortiClient (Windows) has issue with SAML with *ErrorCode=-6005* when it reaches 31%.
818155	FortiClient (Windows) sends SAML response to a different IP address than the request it received from.
821879	VPN autoconnect does not work with IKEv2 IPsec VPN and user certificates.
824298	SSL VPN with certificates cannot connect to VPN on Elitebook 850 G5/Elitebook 850 G3 laptops.
824674	After connecting to VPN tunnel with VPN before logon enabled, FortiClient tray icon menu shows *Connect to [VPN name]* instead of *Disconnect*.
825365	Disconnecting from VPN does not restore *Register this connection's IP to DNS*.
829084	Redundant sort method does not work with redundant SAML authentication.
835042	After upgrading FortiClient (Windows), OpenVPN connection fails while FortiClient (Windows) VPN runs with application-based split tunnel enabled.
838030	Citrix application shows blank pages on SSL VPN tunnel.
838231	Users cannot connect to VPN when using SAML authentication with SSL VPN.
841144	Users disconnect from VPN after screen locks on endpoint.
841641	File/print server stops replying to pings.
841970	GUI gets stuck while connecting SAML SSL VPN with Azure AD and Duo multifactor authentication.
843122	Daily error (-6005) occurs with SAML SSL VPN.
847990	Network adapter keeps DNS registration disabled after FortiClient disconnects from SSL VPN.
848389	FortiClient fails to autoconnect to VPN for personal VPN profile.
850494	VPN fails to connect at 98% to hotspot/Wi-Fi when dual stack is enabled.
851093	IPv6 DNS requests do not work.
851600	FortiClient fails to connect to SSL VPN with FQDN resolving to multiple IP addresses when it could not reach resolved IP address.
852507	When connecting to SSL VPN using FortiSSLVPNclient.exe, the VPN adapter IP address is incorrect.
853368	The assigned SSL VPN IP address appears in GUI but is not assigned to SSL VPN FortiClient virtual interface.
854237	FortiClient fails to connect at 98% when connecting to hot spot/Wi-Fi when dual stack is enabled

Bug ID	Description
	on gateway device.
858696	FortiClient cannot connect to SSL VPN with SAML via satellite Internet service provider.
858806	IKE/IPsec VPN sends the same token code multiple times within a second.
859061	Azure autologin does not work.
861231	VPN tunnel with `on_os_start` enabled does not start on Windows Server.
863138	TapiSrv does not run.
869362	FortiClient (Windows) has issues with multiple reconnections without reauthentication.
869477	When it fails a self test, FortiClient (Windows) does not enter FIPS error mode and shut down completely.
869577	FortiClient only adds FQDN route every second or third disconnect/reconnect.
869862	FortiSSLVPNclient.exe does not correctly use predfined VPN profiles for corporate or personal VPNs.
870087	Windows feature DeadGatewayDetection does bypass default route via VPN.
871346	When using SAML login with built-in browser, FortiAuthenticator, saved password and autoconnect selected, FortiClient (Windows) cannot remember username and password.
871374	SAML login does not display user warning when opening multiple connection with *Limit Users to One SSL-VPN Connection at a Time*.
874208	FortiClient cannot dial up SSL VPN tunnel with ECDSA certificate.
877640	If FortiClient is registered to EMS, option to connect to IPsec VPN on OS start fails to work.
877917	FortiClient Cloud SSL VPN is stuck at 40% to connect with FortiProxy enabled.
878070	FortiClient (Windows) intermittently grays out SAML button after device wakes from sleep.
878880	VPN drops between FortiClient and FortiGate if *Dead Peer Detection* is selected.
885285	SSL VPN network profile is public instead of domain.
887631	Using closest gateway based on TCP round trip time for IPsec VPN resilience does not work if ping is disabled for first gateway.
888602	Autoconnect does not work when based on ping speed/TCP round trip to choose closest FortiGate if FortiClient cannot reach first gateway.
890293	FortiClient cannot trigger self-test when connecting to SSL VPN in FIPS error mode.
890352	IPsec VPN for FIPS-enabled FortiClient fails to work when EMS-pushed IPsec/SSL VPN tunnel contains application split tunnel settings.
891164	FortiClient does not handle EMS-pushed IPsec VPN configuration of encryption/authentication/DH group that FortiClient FIPS does not support.

Bug ID	Description
891202	Autoconnect only when off-fabric does not work properly with user account and MFA with FortiToken for xAuth.
892581	Right click to connect to SSL VPN shows host check error.

Vulnerability Scan

Bug ID	Description
741241	FortiClient (Windows) finds vulnerabilities for uninstalled software.
795393	EMS does not remove vulnerability events after successful patch.
849485	FortiClient wrongly detects AnyDesk vulnerabilities CVE-2021-44426 and CVE-2021-44425.
859508	FortiClient detects wrong vulnerability in patched AutoCAD software.
869253	FortiClient detects vulnerability when the required KB is installed.

Logs

Bug ID	Description
820067	FortiClient forwards logs despite being completely disabled.
849043	SSL VPN add/close action does not show on FortiGate *Endpoint Event* section.
857784	FortiClient (Windows) cannot send OS logs/system events to FortiAnalyzer.

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 it is already enforced through FortiOS.
812207	Blocked web client shows dropped connection message instead of URL blocked message.
825633	Error revokes certificate accessing outlook.office365.com using Web Filter.
826697	Web Filter affects ConnectWise Automate.
829265	Microsoft Teams offline error occurs in SB 6211.

Bug ID	Description
836906	After FortiClient install, extended uptime results in audio cracking.
870895	Web Filter blocks Docker pull.
871325	Web Filter breaks DW Spectrum.

Avatar and social network login

Bug ID	Description
802471	`<enable_manually_entering>` parameter does not work.
830117	EMS fails to update email address for endpoint from personal information form in FortiClient (Windows).
878050	Avatar does not update on FortiGate dashboards and FortiGate cannot show updated information.

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.
830135	Hosts file becomes empty after disconnecting/reconnecting to EMS multiple times and with fresh install of FortiClient (Windows).
831943	ZTNA client certificate is not removed from user certificate store after FortiClient uninstall.
836246	Going from off-Fabric to on-Fabric does not stop the ZTNA service and keeps endpoint from connecting.
839589	ZTNA TCP forwarding does not work for Goanywhere application.
860430	ZTNA web server displays certificate error when browsing inside of application.

FSSOMA

Bug ID	Description
851036	FortiClient (Windows) does not send IP address using mobility agent to FortiAuthenticator when on-premise.
861953	FortiClient single-sign on mobility agent (FSSOMA) does not send ID to FortiAuthenticator.
862021	Local account can access Internet if FSSOMA is logged in and AD user locks the screen.

Onboarding

Bug ID	Description
811976	FortiClient (Windows) may prioritize using user information from authentication user registered to EMS.
819989	FortiClient (Windows) does not show login prompt when installed with installer using LDAP/local verification.

License

Bug ID	Description
830899	FortiClient connected to EMS loses license.
874676	EMS tags endpoint with existing ZTNA host tags for vulnerability and AV after EMS administrator updates EMS license from Endpoint Protection Platform to Remote Access.

Other

Bug ID	Description
780651	FortiClient (Windows) does not update signatures on expected schedule.
834389	FortiClient (Windows) has incompatibility with Fuji Nexim software.
861070	FortiClient (Windows) allows user to end FortiClient (Windows) processes when FortiShield is running/
865938	FortiClient causes *RPC service unavailable* error and blank screen when trying to use Remote Desktop Protocol connection to the server.

www.fortinet.com