FORTINET

Release Notes

FortiClient (Windows) 7.2.0

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

January 31, 2023
FortiClient (Windows) 7.2.0 Release Notes
04-720-848988-20230131

TABLE OF CONTENTS

Change log **5**
Introduction **6**
Licensing 6
What's new in FortiClient (Windows) 7.2.0 ..... **7**
Installation information **8**
Firmware images and tools 8
Upgrading from previous FortiClient versions 9
Downgrading to previous versions 9
Firmware image checksums 9
Product integration and support **10**
Language support 11
Conflicts with third party AV products 12
Intune product code 12
Resolved issues **13**
ZTNA connection rules 13
Web Filter and plugin 13
GUI 14
Endpoint control 14
FSSOMA 15
Install and upgrade 15
Onboarding 15
Zero Trust tags 15
Vulnerability Scan 16
Remote Access 16
Malware Protection and Sandbox 18
Zero Trust telemetry 18
Avatar and social login information 18
Endpoint management 19
Logs 19
Administration 19
Performance 19
Other 19
Common Vulnerabilities and Exposures 20
Known issues **21**
Application Firewall 21
Configuration 21
Endpoint control 21
Endpoint management 22
GUI 22
Install and upgrade 22

Zero Trust tags 23
Malware Protection and Sandbox 23
Remote Access 23
Vulnerability Scan 25
Logs 25
Web Filter and plugin 26
Avatar and social network login 26
License 26
ZTNA connection rules 26
FSSOMA 27
Onboarding 27
Other 27

Change log

Date	Change Description
2023-01-31	Initial release of 7.2.0.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 7.2.0 build 0690.

- What's new in FortiClient (Windows) 7.2.0 on page 7
- Installation information on page 8
- Product integration and support on page 10
- Resolved issues on page 13
- Known issues on page 21

Review all sections prior to installing FortiClient.

FortiClient (Windows) 7.2.0 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 7.2.0 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) 7.2.0

For information about what's new in FortiClient (Windows) 7.2.0, see the *FortiClient & FortiClient EMS 7.2 New Features Guide*.

Installation information

Firmware images and tools

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

File	Description
FortiClientTools_7.2.0.xxxx.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_ 7.2.0.xxxx.zip	Fortinet single sign on (FSSO)-only installer (32-bit).
FortiClientSSOSetup_ 7.2.0.xxxx_x64.zip	FSSO-only installer (64-bit).
FortiClientVPNSetup_ 7.2.0.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_ 7.2.0.xxxx_x64.exe	Free VPN-only installer (64-bit).

EMS 7.2.0 includes the FortiClient (Windows) 7.2.0 standard installer and zip package containing FortiClient.msi and language transforms.

The following tools and files are available in the FortiClientTools_7.2.xx.xxxx.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_7.2.0.xxxx.zip	Standard installer package for Windows (32-bit).
FortiClientSetup_7.2.0.xxxx_ x64.zip	Standard installer package for Windows (64-bit).

File	Description
FortiClientVPNSetup_ 7.2.0.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_ 7.2.0.xxxx_x64.exe	Free VPN-only installer (64-bit).

Review the following sections prior to installing FortiClient version 7.2.0: 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 7.2.0, do one of the following:

- Deploy FortiClient 7.2.0 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) 7.2.0.

FortiClient (Windows) 7.2.0 features are only enabled when connected to EMS 7.2.

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

You must be running EMS 7.2 before upgrading FortiClient.

Downgrading to previous versions

FortiClient (Windows) 7.2.0 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 7.2.0 product integration and support information:

Desktop operating systems	• Microsoft Windows 11 (64-bit) • Microsoft Windows 10 (64-bit) • Microsoft Windows 7 (64-bit) FortiClient 7.2.0 does not support Microsoft Windows XP and Microsoft Windows Vista. FortiClient does not support zero trust network access (ZTNA) TCP forwarding on Windows 7. FortiClient does not support 32-bit platforms such as Windows 10 (32-bit), Windows 8.1 (32-bit), or Windows 7 (32-bit). On those platforms, you can continue to use FortiClient 7.0.
Server operating systems	• Microsoft Windows Server 2022 • Microsoft Windows Server 2019 FortiClient 7.2.0 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 2019 supports ZTNA with FortiClient (Windows) 7.2.0.
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	• 6.00282
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
FortiManager	• 7.2.0 and later • 7.0.0 and later
FortiOS	The following FortiOS versions support ZTNA with FortiClient (Windows) 7.2.0. 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) 7.2.0: • 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

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.

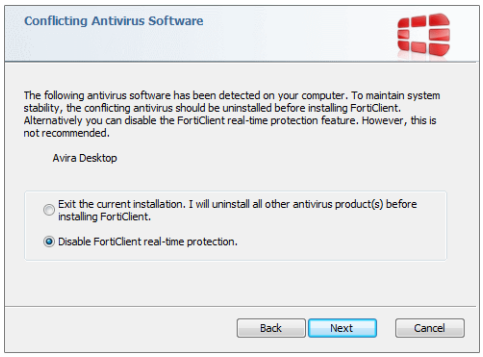
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

Conflicts with third party AV products

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

- 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 FortiClient 7.2.0 is {B4E0AE6E-1C5D-4774-938F-38574804698F}.

See Configuring the FortiClient application in Intune.

Resolved issues

The following issues have been fixed in version 7.2.0. For inquiries about a particular bug, contact Customer Service & Support.

ZTNA connection rules

Bug ID	Description
773956	FortiClient (Windows) cannot show normal webpage of real Internet server (Dropbox) with zero trust network access (ZTNA).
823012	ZTNA TCP forwarding fails to work when FortiClient console is closed.
831895	FortiClient does not send `CERT_REQ` after receiving certificate revoke command from EMS.
875739	ZTNA client certificate is missing in user certificate manager.

Web Filter and plugin

Bug ID	Description
676424	NETIO.SYS causes blue screen of death (BSOD).
784677	Web Filter plugin blocks YouTube comments with *Restricted Mode has hidden comments for this video* message.
804938	All Internet traffic stops when user connects a USB controller (RNDIS).
812794	When Web Filter extension is enabled, downloads in Firefox browser get canceled.
812879	Web Filter blocks Chocolatey installation.
813034	FortiTray keeps notifying user to install Web Filter plugin when Chrome has installed the plugin.
824067	Web Filter blocks HTTP traffic configured as allowed on the exclusion list.
826920	Web Filter extension does not support Edge browser.
829164	Security risk websites violation list is not in Web Filter profile.
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.

Bug ID	Description
839435	Web Filter extension has issues when downloading a PDF from www.gob.mx/curp.
840993	Upgrading FortiClient (Windows) causes Web Filter to break network connectivity.
851700	FortiClient displays *Microsoft Edge extension policy anomaly detected, please restart browser* popup.
860560	Web Filter blocks private IP address as unrated.

GUI

Bug ID	Description
828339	GUI returns blank page after install.
836820	German GUI shows realtime scan events as detected virus threats.
841355	FortiClient (Windows) shows *Remote Access* tab when administrator configured it to be hidden.
863751	GUI becomes blank.
864653	FortiClient (Windows) garbles Chinese name display.

Endpoint control

Bug ID	Description
766241	Endpoint summary reports FortiClient (Windows) antivirus software as third-party feature.
777473	FortiClient Cloud is unaware of UID change when it sends a new UID to FortiClient.
815384	After FortiClient (Windows) status is off-Fabric, Web Filter service start is delayed.
832627	Logging does not work after ZTNA logging is enabled in System Settings profile.
833848	FortiClient reports incorrect Windows version to EMS.
839197	FortiClient (Windows) does not reconnect to EMS after deployment over VPN.
839800	Option to hide Application Firewall in FortiClient (Windows) GUI does not work.
841149	Endpoint tries to use ZTNA certificate when ZTNA option is disabled.
842680	FortiClient (Windows) does not send ADGUID.
846147	EMS does not display user information details from Active Directory (AD) domain.

FSSOMA

Bug ID	Description
868524	Single sign on configuration tool does not generate preshared key and server information in the installer.

Install and upgrade

Bug ID	Description
691328	Upgrade does not upgrade AV engine as deployed through an EMS installer.
839744	FortiClient loses Telemetry connection and does not reconnect when administrator assigns the endpoint to a new group with a different installer.
848255	Upgrading FortiClient from 7.0.6 to 7.0.7 fails when it is registered to EMS.
862161	FortiClient upgrades to include full features when it should not.
875875	FortiClient loses all tags after deployment.

Onboarding

Bug ID	Description
864582	After PC reboot, FortiClient repeatedly tries to log in with SAML when EMS is disconnected.

Zero Trust tags

Bug ID	Description
821391	User in AD group zero trust tag does not tag users in security groups.
704234	Zero trust tagging rule set syntax to check registry key value is unclear.
832623	AV Signature is up-to-date rule not does count days.

Vulnerability Scan

Bug ID	Description
767604	jar file detection does not support YARA rule.
811796	Vulnerability compliance check includes Python vulnerability for all applications.

Remote Access

Bug ID	Description
684913	SAML authentication on SSL VPN with realms does not work.
687765	VPN using SAML authentication displays a certificate warning with a DigiCert certificate.
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- to on-fabric.
776329	IPsec VPN connection from tray fails to launch IPsec VPN service with certificate and ping-based redundant sort method.
789669	DNS suffix is not injected when connecting to SSL VPN over IPV6.
802323	VPN before login fails to connect with host check rule configured immediately after reboot.
812898	SSL VPN autoconnect does not work and results in IPsec VPN errors.
821395	SAML SSL VPN and autoconnect when off-fabric does not reconnect.
822763	Remote Access *Connect* button does not work.
824165	SSL VPN does not reconnect when using tunnel-based connection over point-to-point tunneling protocol.
825442	ZScaler client connector does not work with application-based split tunnel.
826170	FortiClient removes the SSL VPN password from the GUI if the network interface is disconnected and reconnected.
827612	update_task.exe execution window pops up while connecting to SSL VPN.
829763	With host check enabled, SAML login does not show proper warning message if it fails to connect.
830067	Connecting to IPsec VPN displays *Update failed - Error occurred!* error.
832036	VPN autoconnect does not always work with special Azure AD build.
832953	VPN tunnel does not always connect automatically if network is disrupted or if the device is in sleep mode even if always up is enabled.

Bug ID	Description
834874	Autoconnect does not work after restart when the Remote Access profile only has an IPsec VPN tunnel and the SSL VPN option disabled.
834883	On-fabric rule for VPN tunnel name does not work when the tunnel name uses special characters.
836148	FortiClient does not try to connect to a realm with name https://X.Y:10443/Z if X and Z are the same values.
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 restarts.
840685	The VPN before logon icon does not show in certain conditions.
840720	User cannot modify IPsec VPN advanced settings for personal VPN profile.
844190	Upon connecting to SAML VPN, FortiClient (Windows) displays *Update failed - Error occurred!* popup.
852036	FortiClient cannot correctly handle a certificate having a Japanese character in the issuer or subject name.
859498	Current connection feature does not work as expected.
864430	Machine SSL VPN does not work with existing user autoconnect configuration.
866494	Certificate-only SSL VPN tunnel fails to connect if it is configured to be a machine autoconnect tunnel.
867202	IPsec VPN with certificate authentication fails to connect if it is configured to be a machine autoconnect tunnel.
868568	VPN before logon feature fails to work with IPsec and SSL VPN tunnel.
868931	If user attempts to connect to SSL VPN using incorrect credentials for the second time, FortiClient (Windows) does not notify the user of incorrect credentials and is stuck in an idle state.
870035	Machine IPsec VPN with signature certificate authentication and user autoconnect IPsec VPN with preshared key does not work.
871091	`tunnel-connect-without-reauth` for SSL VPN does not reconnect automatically.
872132	If FortiClient (Windows) cannot reach the first remote gateway, it fails to connect to the redundant VPN tunnel and the connection is stuck at 10%.
872237	Per-user autoconnect with redundant VPN gateways does not work if *Enable Invalid Server Certificate Warning* is on.

Malware Protection and Sandbox

Bug ID	Description
606634	FortiClient fails to remove quarantined files after days configured with cullage option.
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 the option is disabled in the EMS profile.
784306	FortiClient causes blue screen of death (BSOD) when ACR1281 card reader is plugged in.
817933	Antiransomware fails to recover files that W32/GenKryptik.FQWI!tr.ransom ransomware encrypted.
820068	FortiClient on Lenovo laptop with mobile WWAN results in BSOD at login.
820511	Promethean ActivBoard does not work with FortiClient.
820565	FortiClientVirusCleaner.exe has *Failed to download supporting files* error.
826055	FortiDeviceGuard causes BSOD.
857482	FortiClient (Windows) built-in AV engine is not updated to 6.00282.
859749	Antiransomware feature fails to detect W64/Filecoder.EJ!tr.ransom ransomware.

Zero Trust telemetry

Bug ID	Description
837859	FortiClient (Windows) has issues connecting to EMS after upgrade.

Avatar and social login information

Bug ID	Description
729140	FortiClient (Windows) fails to allow login with Google, LinkedIn, or Salesforce.
802471	`enable_manually_entering` parameter does not work.
825913	FortiClient (Windows) reports system user changes to EMS inconsistently.

Endpoint management

Bug ID	Description
770637	FortiClient (Windows) cannot unquarantine endpoint with one-time access code.

Logs

Bug ID	Description
713287	FortiClient (Windows) does not generate local logs for ZTNA.
873945	FortiClient (Windows) logs disconnecting from SSL VPN to FortiAnalyzer as a connection in security event logging.

Administration

Bug ID	Description
798055	JavaScript error occurs in the main process

Performance

Bug ID	Description
827743	Corporate endpoints experience BSOD after FortiClient installation. Non-corporate endpoints do not experience BSOD.

Other

Bug ID	Description
850528	FortiClient (Windows) does not always get IPv4 address from https://ipify.org.

Common Vulnerabilities and Exposures

Bug ID	Description
838208	FortiClient (Windows) 7.2.0 is no longer vulnerable to the following CVE References: • CVE-2022-42470 Visit https://fortiguard.com/psirt for more information.
840897	FortiClient (Windows) 7.2.0 is no longer vulnerable to the following CVE References: • CVE-2022-40682 Visit https://fortiguard.com/psirt for more information.
845295	FortiClient (Windows) 7.2.0 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) 7.2.0. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Application Firewall

Bug ID	Description
814391	FortiClient Cloud application signatures block allowlisted applications.
827788	Threat ID is 0 on Firewall Events.
844997	FortiClient loses several packets on different internal resources after connecting telemetry.
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 of Microsoft Active Directory Users and Computers application.

Configuration

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

Endpoint control

Bug ID	Description
753151	Updating endpoint status from endpoint notified to deployed takes a long time.
804552	FortiClient shows all feature tabs without registering to EMS after upgrade.
815037	After administrator selects *Mark All Endpoints As Uninstalled*, FortiClient (Windows) connected with verified user changes to unverified user.
821024	FortiClient fails to send username to EMS, causing EMS to report it as different users.

Bug ID	Description
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 Active Directory group check does not execute.
841764	EMS does not show third-party features in endpoint information.
855851	EMS remembered list shows FQDN duplicates.
878514	FortiClient cannot get tenant ID after EMS administrator deploys FortiClient 7.2.0 over 7.0.7 from the EMS server.
879108	EMS considers the endpoint as on-Fabric when it does not meet all rules in an on-Fabric detection rule set.
899960	FortiESNAC process may stop after switching between two FortiSASE Endpoint Management Services.

Endpoint management

Bug ID	Description
836134	Inverse selection with ! does not work for deployment package, profile, and features under All Endpoints view.

GUI

Bug ID	Description
847903	Console stops working on Citrix servers with ntdll.dll crash.

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.

Zero Trust tags

Bug ID	Description
819120	Zero trust tag rule for Active Directory group does not work when registering FortiClient to EMS with onboarding user.

Malware Protection and Sandbox

Bug ID	Description
820098	Sandbox does not release blocked file.
828862	FortiClient does not allow virtual CD-ROM device.
831560	GUI shows ransomware quarantined files after restoration via EMS.
833264	Antiexploit blocks Chrome without sharing payload details.
844962	FortiClient (Windows) does not block phone mobile storage when default removable media access is set to block.
844988	FortiClient (Windows) does not block USB drive with attempt to copy contents even if WPD/USB is set to block in profile.
857041	Windows 10 security center popup shows FortiClient and Windows Defender are off.
861296	AV scan exclusion list does not work for shared/network drive files.
863802	FortiClient (Windows) cannot detect SentinelOne when they have product on OS level.
876925	Antiexploit protection blocks Microsoft signing application in Chrome.

Remote Access

Bug ID	Description
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.
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.
762986	FortiClient (Windows) does not use second FortiGate to connect to resilient tunnel from FortiTray if it cannot reach first remote gateway.

Bug ID	Description
763611	If dual stack is enabled and user connects tunnel with IPv6 and tunnel is established successfully, then the user tries to access IPv4 server to upload/download files, the network speed is slow.
773920	Endpoint switches network connection after IPsec VPN connection, causing VPN to disconnect.
775633	Priority based IPSec resiliency tunnel, auto failover to second remote gateway doesn't work
783412	Browser traffic goes directly to ZTNA site when SSL VPN is connected.
795334	Always up feature does not work as expected when trying to connect to VPN from tray.
811458	FortiClient (Windows) cannot connect to SSL VPN after installing Windows update KB5013942.
814488	SSL VPN with `<on_os_start_connect>` enabled does not work when the machine is put into sleep mode and changes networks.
821879	VPN autoconnect does not work with IKEv2 IPsec VPN and user certificates.
824674	After connecting to VPN with VPN before logon option, FortiClient tray icon menu shows *Connect to [VPN name]* instead of *Disconnect*.
834604	Upgrading FortiClient (Windows) free VPN-only client to the latest build removes VPN tunnels.
835042	After upgrading FortiClient (Windows), OpenVPN connection fails while FortiClient (Windows) VPN runs with application-based split tunnel enabled.
837861	Always up fails to keep SSL VPN connection up when endpoint is left idle overnight.
838030	Citrix application shows blank pages on SSL VPN tunnel.
838231	Users fail to connect 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).
842560	FortiClient disables PolicyAgent and IKEEXT services when connecting to dial-up IPsec VPN.
843122	Daily error (-6005) occurs with SAML SSL VPN.
847990	Network adapter keeps DNS registration disabled after FortiClient (Windows) disconnects from SSL VPN.
850494	VPN fails to connect at 98% to hotspot/Wi-Fi when dual stack is enabled.
850822	FortiClient cannot connect to IPsec VPN if multiple Diffie-Hellman groups are selected.
851093	IPv6 DNS requests do not work.
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 (Windows) virtual interface.

Bug ID	Description
854237	FortiClient fails to connect at 98% when connecting to hot spot/Wi-Fi when dual stack is enabled on gateway device.
858696	FortiClient cannot connect to SSL VPN with SAML via Satelite ISP.
859061	Azure autologin des not work.
859703	FortiClient (Windows) cannot reconnect to SSL VPN without credentials.
861231	VPN configured with `<on_os_start>` does not start on Windows Server.
863138	TapiSrv does not run.
877314	EMS-configured autoconnect tunnel does not have higher priority than a user's previously selected autoconnect tunnel.
877320	Autoconnect on install is not triggered if FortiClient is installed and registered to EMS during the same Windows logon session.
877640	If FortiClient is registered to EMS, IPsec VPN tunnel fails to connect when it is configured to connect on OS start.
877917	FortiClient Cloud SSL VPN is stuck at 40% to connect with FortiProxy enabled.
878070	After device wakes from sleep, FortiClient intermittently grays out SAML button.
878291	After registering to EMS using FortiSASE invitation code, FortiClient shows unable to reach tunnel gateway error.
878652	VPN secure remote access notification prompt displays multiple times with cutoff text.
878880	VPN drops between FortiClient and FortiGate if *Dead Peer Detection* is selected.

Vulnerability Scan

Bug ID	Description
849485	FortiClient wrongly detects AnyDesk vulnerabilities CVE-2021-44426 and CVE-2021-44425.
859508	FortiClient detects wrong vulnerability in patched AutoCAD software.

Logs

Bug ID	Description
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.
825633	Error revokes certificate accessing outlook.office365.com using Web Filter.
829265	Endpoint displays Microsoft Teams offline error.
836906	After FortiClient install, extended uptime results in audio cracking.
842966	Web Filter fails to activate when off-fabric.
859979	FortiClient blocks web browsing traffic which Web Filter allows.

Avatar and social network login

Bug ID	Description
830117	EMS fails to update email address for endpoint from personal information form in FortiClient (Windows).
831366	EMS does not show correct username if user logs in with Google or Linkedin cloud service or chooses user input.
878050	FortiClient avatar does not update on FortiOS dashboards and FortiOS cannot show updated information.

License

Bug ID	Description
830899	FortiClient (Windows) loses license.

ZTNA connection rules

Bug ID	Description
814953	Using an external browser for SSH ZTNA requires restarting FortiClient on Windows 11.
831943	ZTNA client certificate is not removed from user certificate store after FortiClient uninstall.

Bug ID	Description
836246	Going from off-Fabric to on-Fabric does not stop the ZTNA service and keeps endpoint from connecting.
839589	ZTNA TCP forwarding not working for GoAnywhere application.
860430	ZTNA web server displays certificate error when browsing inside of application.
871342	Allow ZTNA error message showing on browser to be configurable.
877128	User in different country cannot create a ZTNA tunnel.

FSSOMA

Bug ID	Description
854882	FortiClient (Windows) does not send EMS tenant ID to FortiAuthenticator.
861953	Single sign-on mobility agent (SSOMA) does not send ID to FortiAuthenticator.
862021	Local account can access Internet if FortiClient SSOMA logged-in 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.

Other

Bug ID	Description
834389	FortiClient has incompatibility with Fuji Nexim software.
835743	Windows does not boot up after Windows updates.
865938	FortiClient causes *RPC service unavailable* error and blank screen when trying to connect via RDP to the server.

www.fortinet.com