FORTINET

Release Notes

FortiClient (Windows) 7.2.3

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

FORTINET®

December 14, 2023
FortiClient (Windows) 7.2.3 Release Notes
04-723-976142-20231214

TABLE OF CONTENTS

Change log

Date	Change Description
2023-12-14	Initial release of 7.2.3.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 7.2.3 build 0929.

- Special notices on page 7
- What’s new in FortiClient (Windows) 7.2.3 on page 8
- Installation information on page 9
- Product integration and support on page 12
- Resolved issues on page 15
- Known issues on page 20

Review all sections prior to installing FortiClient.

Licensing

See Windows, macOS, and Linux endpoint licenses.

FortiClient 7.2.3 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.

FortiClient offers a free standalone installer for the single sign on mobility agent. This agent does not include technical support.

Special notices

SAML IdP Configuration for Save Password

FortiClient provides an option to the end user to save their VPN login password with or without SAML configured. When using SAML, this feature relies on persistent sessions being configured in the identity provider (IdP), discussed as follows:

- Microsoft Entra ID
- Okta

If the IdP does not support persistent sessions, FortiClient cannot save the SAML password. The end user must provide the password to the IdP for each VPN connection attempt.

The FortiClient save password feature is commonly used along with autoconnect and always-up features as well.

FortiClient support for newer Realtek drivers in Windows 11

Issues regarding FortiClient support for newer Realtek drivers in Windows 11 have been resolved. The issue is that Realtek and Qualcomm used the NetAdapterCx structure in their drivers, and Microsoft's API had an error in translating the flags, which may result in IPsec VPN connection to fail.

What’s new in FortiClient (Windows) 7.2.3

For information about what's new in FortiClient (Windows) 7.2.3, 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_7.2.3.xxxx.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_ 7.2.3.xxxx.zip	Fortinet single sign on (FSSO)-only installer (32-bit).
FortiClientSSOSetup_ 7.2.3.xxxx_x64.zip	FSSO-only installer (64-bit).
FortiClientVPNSetup_ 7.2.3.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_ 7.2.3.xxxx_x64.exe	Free VPN-only installer (64-bit).

EMS 7.2.3 includes the FortiClient (Windows) 7.2.3 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).
CertificateTestx64.exe	Test certificate (64-bit).
CertificateTestx86.exe	Test certificate (86-bit).
FCRemove.exe	Remove FortiClient if unable to uninstall FortiClient (Windows) via Control Panel properly.
FCUnregister.exe	Deregister FortiClient (Windows).
FortiClient_Diagnostic_tool.exe	Collect FortiClient diagnostic result.

File	Description
ReinstallINIC.exe	Remove FortiClient SSLVPN and IPsec network adpater, if not uninstall it via control pannel.
RemoveFCTID.exe	Remove FortiClient UUID.

The following files are available on FortiClient.com:

File	Description
FortiClientSetup_7.2.3.xxxx.zip	Standard installer package for Windows (32-bit).
FortiClientSetup_7.2.3.xxxx_x64.zip	Standard installer package for Windows (64-bit).
FortiClientVPNSetup_7.2.3.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_7.2.3.xxxx_x64.exe	Free VPN-only installer (64-bit).

Review the following sections prior to installing FortiClient version 7.2.3: Introduction on page 6 and Product integration and support on page 12.

Upgrading from previous FortiClient versions

To upgrade a previous FortiClient version to FortiClient 7.2.3, do one of the following:

- Deploy FortiClient 7.2.3 as an upgrade from EMS. See Recommended upgrade path.
- Manually uninstall existing FortiClient version from the device, then install FortiClient (Windows) 7.2.3.

FortiClient (Windows) 7.2.3 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) 7.2.3 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 7.2.3 product integration and support information:

Desktop operating systems	• Microsoft Windows 11 (64-bit) • Microsoft Windows 10 (64-bit)
Server operating systems	• Microsoft Windows Server 2022 • Microsoft Windows Server 2019 FortiClient 7.2.3 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 zero trust network access (ZTNA) with FortiClient (Windows) 7.2.3. 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.
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 2 GB RAM • 1 GB 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	• 6.00287
FortiAnalyzer	• 7.4.0 and later • 7.2.0 and later • 7.0.0 and later
FortiAuthenticator	• 6.5.0 and later • 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
FortiManager	• 7.4.0 and later • 7.2.0 and later

	• 7.0.0 and later
FortiOS	The following FortiOS versions support ZTNA with FortiClient (Windows) 7.2.3. This includes both ZTNA access proxy and ZTNA tags: • 7.4.0 and later • 7.2.0 and later • 7.0.6 and later The following FortiOS versions support IPsec and SSL VPN with FortiClient (Windows) 7.2.3: • 7.4.0 and later • 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	• 4.4.0 and later • 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.

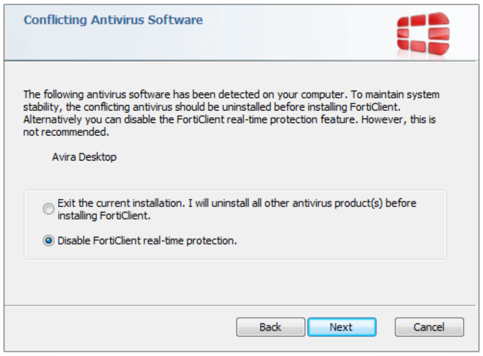
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

Conflicts with third party AV products

The FortiClient antivirus (AV) feature 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.



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.

Intune product codes

Deploying FortiClient with Intune requires a product code. The product codes for FortiClient 7.2.3 are as follows:

Version	Product code
Enterprise	611804A7-F14E-45A2-9F55-345D33EDD28E
VPN-only agent	D6A52B20-063A-4BF6-8228-CDADBF8ACBCF
Private access management-only agent	E28AF72E-B96C-405E-8281-7F1329ADB947
Single sign on-only agent	165D1BE3-2F3D-4E74-8108-74B755371E69

See Configuring the FortiClient application in Intune.

Resolved issues

The following issues have been fixed in version 7.2.3. For inquiries about a particular bug, contact Customer Service & Support.

ZTNA connection rules

Bug ID	Description
926403	Ports list does not work in ZTNA TCP forwarding rule for scenario with EMS rule or scenario with portal, wildcard, and ports list.
957442	Zero trust network access (ZTNA) destination does not work with and without ZTNA tag attached to FortiGate ZTNA rules.
966169	ZTNA does not work when Fortinet Security Fabric connector is connected to FortiGate on FortiOS 7.4.1 with virtual domains.

Web Filter and plugin

Bug ID	Description
812794	Downloads are canceled in Firefox when Web Filter extension is enabled.
932019	*Bypass Private IP* does not work on Edge and Chrome.
967191	YouTube videos do not play if Web Filter extension is enabled.

GUI

Bug ID	Description
795350	Multiple FortiTray icons display in Windows system tray.
949939	JavaScript error occurs in main process.

Endpoint control

Bug ID	Description
821024	FortiClient (Windows) fails to send username to EMS and causes EMS to report it as having a different user.
926631	Duplicate users show in EMS and FortiClient (Windows) does not intermittently send user update.

Application Firewall

Bug ID	Description
848280	Application-based split tunnel does not work.
940481	Antivirus and Firewall features cause network problems.

FSSOMA

Bug ID	Description
935090	Single sign-on mobility agent (SSOMA) stops sending SSO session information to FortiAuthenticator while service runs on host.

Install and upgrade

Bug ID	Description
955824	Free VPN-only agent does not include SSOMA registry value if it was upgraded free VPN-only agent 7.0, which does not include SSOMA.
957228	Status sentence is incomplete on deployment wizard when FortiClient (Windows) requests reboot during deployment.

Logs

Bug ID	Description
811746	FortiClient (Windows) sends duplicated and old logs to FortiAnalyzer.

Bug ID	Description
876810	FortiClient does not indicate `vpnuser` in logs when connection succeeds.
962704	FortiClient floods FortiAnalyzer with SYN packets.
966018	FortiClient uploads logs more frequently than its configured upload interval.

Zero Trust tags

Bug ID	Description
957469	Zero Trust tag for Windows CA certificate does not work.
976374	CURRENT_USER registry tag does not work.

Vulnerability Scan

Bug ID	Description
956805	FortiClient EMS shows *Scheduled* as patch status for critical FortiClient EMS Microsoft Office Memory Corruption Vulnerability, but it is not fixed with next telemetry communication.

Remote Access

Bug ID	Description
793668	ipsec.exe crashes with split tunnel and application-based exclude configuration.
819279	When using FortiClient with Realtek Windows 11 drivers, FortiClient (Windows) cannot establish an IPsec VPN tunnel.
858806	IKE/IPsec VPN sends the same token code multiple times within a second.
876607	FortiClient (Windows) on Windows 11 cannot connect to IPsec VPN when using Ethernet connection.
884348	DTLS in SSL VPN does not work with SAML.
889638	SSL VPN push prompt does not disappear after push approval.
905443	Race condition between Windows autologin and autoconnect blocks FortiClient from automatically connecting to IPsec VPN.
912980	IPsec VPN fails to connect if `vpn-ems-sn-check` is enabled and FortiClient is registered to custom EMS site.

Bug ID	Description
936354	FortiClient (Windows) cannot connect to SSL VPN with Azure SAML when Microsoft Entra ID (formerly known as Azure Active Directory) autologin is enabled.
942104	Connecting to SSL VPN with multifactor authentication set for user using FortiToken Mobile stops at 98% and does not complete the connection.
945888	When using VPN before logon, there is no one-time password (OTP) token request prompt if using FortiToken Mobile with FortiAuthenticator for OTP.
947381	With `<prefer_sslvpn_dns>` set to 0, when SSL VPN is up, FortiClient adds dns-suffix to all network interfaces.
948611	With customized host check fail warning off and ZTNA tags assigned, FortiClient (Windows) shows empty warning when trying to establish VPN.
949945	Network lockdown blocks FortiClient Cloud telemetry.
953214	FortiClient cannot update from 7.0.7 to 7.2.1 when deployed from EMS.
955248	SSL VPN does not work with local machine certificate-based tunnel when initiated from FortiTray.
956202	FortiClient (Windows) reaches a status that cannot connect after updating a VPN tunnel without a certificate to have a certificate.
960369	When the SSL VPN disconnects, FortiClient (Windows) automatically adds backslash sign to username.
961087	Blue screen of death (BSOD) occurs after installing FortiClient and connecting to SSL VPN.
962287	SSL VPN reaches infinite loop that keeps trying to connect to SSL VPN but fails.
963039	SslvpnAgent: Pipe is broken for writing.
965016	FortiClient does not connect to IPsec VPN when adding a second remote gateway.

Malware Protection and Sandbox

Bug ID	Description
940272	Antivirus and Sandbox settings do no allow user to copy files to a share folder.
946390	Real-time Protection blocks Word and Excel file access from network shared drive (network-attached storage).
952073	Windows notification about virus protection is out -of-date and has a red icon on Windows Security Center.
953905	FortiClient does not display *Malware Protection* tab when installer only includes antiransomware.

Zero Trust telemetry

Bug ID	Description
917708	FortiClient cannot connect to EMS if installed on same machine.
952565	FortiClient does not show error after reconnecting with deleted invitation code.

Other

Bug ID	Description
915119	FortiClient requires further localization into supported languages.
942082	FortiClient causes Windows 10 BSOD ntoskrnl.exe when Cisco AnyConnect VPN is connected.
943967	NETIO.SYS causes BSOD.
964838	FortiClient Cloud French translation for Zero Trust Telemetry is incorrect in FortiClient.
973928	Orchestrator crashes when backing up FA_ESNAC\cloud_client registry values.

Known issues

The following issues have been identified in FortiClient (Windows) 7.2.3. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Administration

Bug ID	Description
867818	fortishield.sys and fortimon3.sys are incompatible with HVCI.

Application Firewall

Bug ID	Description
814391	FortiClient Cloud application signatures block allowlisted applications.
827788	Threat ID is 0 on Firewall Events.
842534	After upgrade, Application Firewall blocks internal webpage.
844997	FortiClient loses several packets on different internal resources after connecting telemetry.
860062	Application Firewall slows down opening of Microsoft Active Directory (AD) Users and Computers application.
869671	FortiClient (Windows) bypasses Application Firewall block after matching detection rule.
879985	Application Firewall fails to block Web.Client category HTTPS traffic.
884911	FortiClient detects IntelliJ IDEA Community Edition 2021.2.2 as Java.Debug.Wire.Protocol.Insecure.Configuration.
890001	Application Firewall blocks Tanium application under antiexploit.
891789	Application Firewall blocks CREO management tool software.
902866	Application Firewall does not block Google Drive.
958651	Application Firewall violation list always shows violated programs as the same as applications, which is not as accurate as Windows.

Configuration

Bug ID	Description
730415	FortiClient backs up configuration that is missing locally configured zero trust network access (ZTNA) connection rules.

Deployment and installers

Bug ID	Description
783690	Reboot prompt does not display after user login.
870370	Upgrading FortiClient from FortiClient Cloud uses expired invitation code to register.
953124	FortiClient Orchestrator notification does not appear when upgrade is scheduled.

Endpoint control

Bug ID	Description
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.
820483	EMS device control does not block camera device.
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 FQDN duplicates.
868230	"Connection expiring due to FortiClient Connect license exceeded" error occurs.
880167	FortiClient cannot register with EMS due to selecting wrong interface to connect to EMS.
975391	FortiClient 7.2.1 and later versions report a different user to EMS than 7.0.7 did.
979669	User avatar fails to upload to FortiAnalyzer.

Endpoint management

Bug ID	Description
916566	FortiClient reports USB as blocked but user can access the storage files.

GUI

Bug ID	Description
872634	FortiClient shows blank page when user opens FortiClient console.
874560	GUI becomes blank after receiving EMS-pushed profile.
888185	FortiClient does not minimize after successful VPN connection.
902595	SAML prompt flashes on autoconnect.
955209	GUI has issues after disconnecting from VPN.

Endpoint policy and profile

Bug ID	Description
889517	EMS fails to assign the correct endpoint policy and shows FortiClient as out-of-sync despite the client syncing.
915678	FortiClient does not send acknowledged event to EMS if it disconnects and reconnects to EMS immediately after the user acknowledges the one-way message.

Endpoint security

Bug ID	Description
960595	Some FortiClient (Windows) endpoints cannot reach FortiClient Cloud.
975704	FortiClient does not report most recent completed scan timestamp to EMS and causes last scan time to show incorrectly on EMS dashboard.

Install and upgrade

Bug ID	Description
769639	FortiDeviceGuard is not installed on Windows Server 2022.
955268	User can uninstall FortiClient when it is registered to EMS.
960301	FortiClient fails to install due to orphaned registry key.
982033	Windows application (native launchers) fail to launch after upgrade from previous standalone version.

Malware Protection and Sandbox

Bug ID	Description
828862	FortiClient does not allow virtual CD-ROM device.
831560	GUI shows ransomware quarantined files after restoration via EMS.
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.
863802	FortiClient (Windows) cannot detect SentinelOne when they have product on OS level.
871078	Antiexploit protection blocks Adobe plugin in Chrome.
872970	Bubble notifications do not appear when inserting USB drive in endpoint machine.
874312	Sandbox quarantines files with read-only access permission.
874315	Sandbox scan reports read-only file as quarantined.
874578	Real-time protection does not delete quarantined files after cullage time.
876465	FortiClient does not detect virus in network drive.
876925	Antiexploit protection blocks Microsoft signing application in Chrome.
901065	Logitech driver breaks after installing FortiClient with Malware Protection feature enabled in installer.
915300	FortiClient (Windows) detects file configured as exception as malware.
919007	On-demand scan for mapped drives is not possible.
919499	Windows Security Center shows that FortiClient (Windows) is inactive when FortiClient (Windows) is running and up-to-date.
946756	EMS logs USB events logged when there is an allow rule configured.
948985	update_task downloads AV signature from FDS, but AV engine fails to verify the signature.

Bug ID	Description
	FortiClient (Windows) does not keep copy of problem signature.
956963	FortiClient Spoolsv is blocked when Windows antimalware scan is enabled.
966195	Antimalware detects W64/AI.Pallas Suspicious and fails to quarantine.
967202	FortiClient does not receive signature updates.
972036	Sandbox agent uses high CPU/memory/I/O when connecting to external SSD.
972671	If Malware Protection is enabled, Valorant fails to work.
976366	Windows 10 login page is stuck when FortiClient has long AV exclusion list.

Zero Trust tags

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

Software Inventory

Bug ID	Description
737970	Software Inventory on EMS does not properly reflect software changes (adding/deleting) on Windows endpoints.
844392	Software Inventory shows last installation time in future.

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.

Bug ID	Description
762986	FortiClient (Windows) does not use second FortiGate to connect to resilient tunnel from FortiTray if it cannot reach first remote gateway.
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.
815528	If `<allow_local_lan=0>`, per-application split tunnel is enabled, exclude mode is enabled, and a full tunnel is up, FortiClient (Windows) does not block local RDP/HTTPS traffic.
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.
841144	Users disconnect from VPN after screen locks on endpoint.
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.
850494	VPN fails to connect at 98% to hotspot/Wi-Fi when dual stack is enabled.
861231	VPN configured with `<on_os_start>` does not start on Windows Server.
863138	TapiSrv does not run.
869362	FortiClient (Windows) has issues reconnecting to SSL VPN without reauthentication.
869477	If a self-test fails, 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 predefined VPN profiles for corporate or personal VPNs.
870087	Windows feature DeadGatewayDetection bypasses default route via VPN.
871346	FortiClient (Windows) cannot remember username and password for tunnel with SAML login with built-in browser, FortiAuthenticator, and *Save Password* and autoconnect selected.
871374	VPN tunnel with SAML login does not warn user when opening multiple connections with *Limit Users to One SSL-VPN Connection at a Time* enabled.
872315	IPsec VPN resiliency based on ping response does not work.
872339	Per-user autoconnect does not work after restarting FortiClient.
874208	FortiClient (Windows) cannot dial up SSL VPN tunnel with ECDSA certificate.
874298	Always up does not work for SAML SSL VPN tunnel with single FQDN resolved to multiple IP addresses.

Bug ID	Description
874310	Using closest gateway based on ping speed and TCP round trip does not work for SSL VPN resilience if using different ports for the remote gateways.
874669	FortiClient does not attempt to connect with redundant SAML VPN gateway if it cannot reach first gateway.
874759	SSL VPN has DNS issues if AWS Route53 is configured for name resolution.
875631	Dialup IPsec VPN does not allow multiple valid server certificates for client use simultaneously.
875999	FortiClient does not show GUI prompt to enter PIN for SSL VPN certificate stored on USB PKI/SmartCard device.
876429	FortiClient (Windows) ignores `redundant_sort_method=0` configuration option for IPsec VPN IKEv2 tunnel using multiple VPN gateways.
876643	Connecting to an IKEv2 tunnel with EAP disabled from FortiTray with certificate only does not work.
877640	If FortiClient is registered to EMS, IPsec VPN tunnel fails to connect when it is configured to connect on OS start.
878070	After device wakes from sleep, FortiClient intermittently grays out SAML button.
878652	VPN secure remote access notification prompt displays multiple times with cutoff text.
882408	FortiClient (Windows) fails to renew password when user changes password in Windows login screen.
884926	Okta SAML token popup displays in low resolution.
887631	Using closest gateway based on TCP round trip for IPsec VPN resilience does not work if ping is disabled for first gateway.
891202	Autoconnect only when off-fabric does not work properly with user account and multifactor authentication (MFA) (FortiToken) for XAuth.
892314	On-connect script does not execute .
893237	FortiClient (Windows) does not provide opportunity to reinput password during autoconnect after identity provider password change.
893677	Autoconnect and always-up do not work when two gateways are configured for SAML SSL VPN with *Redundancy Sort Method*.
896213	GUI is stuck in VPN connecting status.
896400	VPN autoconnects when endpoint is woken from hibernation.
898873	SSL VPN tries to reconnect after screen is unlocked even when VPN tunnel is up and updated ZTNA tags are not synced to FortiGate.
901247	FortiClient does not exclude Five9 application from VPN.
903159	FortiClient does not save SSL VPN credentials for tunnel with dual stack and *Save Password* enabled.

Bug ID	Description
904871	IPsec VPN connection takes long time to connect and shows *Connect* button when connection is in progress.
905651	FortiSASE VPN always up has issues when shifting endpoints from one public network to another.
907248	FortiClient (Windows) cannot connect to FortiSASE SAML VPN tunnel that uses OneLogin as identity provider (IdP) with built-in browser when IdP requires client certificate.
909145	Secure remote access tunnel default host tag message for prohibited connection is empty.
909244	SSL VPN split DNS name resolution stops working.
909573	With MFA and autoconnect enabled, user account password becomes empty after logging in to Windows.
909702	Saved username and password disappear while testing autoconnect only when offnet.
909755	SSL VPN split tunnel does not work for Microsoft Teams.
910533	When a tunnel has two gateways, SAML login is configured, and FortiClient (Windows) can reach the first FortiGate, built-in browser for XAuth failover to second FortiGate does not work.
912110	*A network error prevented updates from being downloaded.* pops up when FortiClient (Windows) establishes SSL VPN.
912703	Deregistered FortiClient (Windows) can connect with tunnel that has ZTNA tag assigned.
913217	*Cancel* button fails to work with IPsec VPN connection.
914018	SSL VPN SAML login fails to work if using YubiKey for MFA.
914987	Windows 10 cannot connect when AES and strong crypto is used in FortiGate.
916240	User from India cannot connect to SSL VPN using SAML authentication while same user can connect from the U.S.
916581	Static DNS entry is registered when on-fabric.
918322	FortiShield blocks FortiClient (Windows) application due to registry issue.
920383	FortiClient always enables *Turn off smart multi-homed name resolution* on Windows after successful connection.
930740	FortiClient (Windows) does not allow setting up SSL VPN tunnel if password contains Polish characters: ł , ą, and ń.
933991	FortiClient does not trust SSL VPN gateway that is signed by Internal Intermediate Cert even though the PC trusts it.
941259	When enabling *Register this connection's addresses in DNS* on the adapter, after a restart, the option is disabled.
942668	Split DNS on SSL VPN only resolves the first DNS server.
949977	FortiClient disclaimer does not work for IPsec VPN.
950787	Domain filter cannot block access to specific server FQDN.

Bug ID	Description
952808	FIPS-CC SSL VPN FortiClient (Windows) use MD5 to generate share key to encrypt login post data.
953160	SAML token reuse does not work for SSL VPN if *Disable Connect/Disconnect* option is enabled in EMS Remote Access profile.
954004	DTLS tunnel cannot establish when handshake packet has a large MTU.
954352	DNS servers do not display on the virtual adapter with IPsec VPN. CLI shows the IP address.
955674	FortiClient (Windows) showing *IPsec VPN connection down* GUI notification while autoconnecting.
956472	FortiClient fails to resolve SRV records with split DNS.
956729	Web Filter blocks FortiClient itself imitated URL when trying to connect to SSL VPN with SAML login.
956949	FortiClient endpoint traffic is blocked when connecting to SSL VPN full tunnel.
956967	FortiSandbox exclusions path with wildcard does not work for cache files/folders such as Chrome.
957175	With external browser for SSL VPN SAML login authentication, FortiClient (Windows) cannot save user password when logging off, logging in, or rebooting.
962995	FortiSASE Secure Internet Access VPN frequently disconnects and requires user to log in again.
963554	Lookup by name to internal resources fails when IPv6 is enabled on NIC.
964036	Gateway selection (e.g. saml-login) based on ping speed or TCP round trip does not work.
966713	Certificate-only tunnels do not autoconnect if user does not connect the tunnel once before logging out of Windows.
968151	SAML-login resilience tunnel automatic failover to second remote gateway after first one is unreachable does not work.
969587	VPN disconnects periodically when power mode is set to *Recommended*.
969600	FortiGSLB SAML SSL VPN connection has -6005 error.
969601	Launching the FortiClient GUI from the system tray takes more than 30 seconds and sometimes does not open.
969995	Autoconnect does not work reliably with IPsec VPN using username/password with OTP and client certificate.
970005	DNS over TCP does not work with FortiClient (Windows) connected to FortiSASE and split DNS configured.
970620	SAML SSL VPN still connects to SAML without asking for credentials even save password is disabled.
971554	When connected to IPsec VPN, FortiClient sends access request when password renewal was canceled.
971698	FortiClient disconnects VPN when screen is locked but the user is not logged out.

Bug ID	Description
972004	*Enable Invalid Server Certificate Warning* does not work for IPsec VPN with SAML-based authentication.
972089	VPN is stuck at 98% when connected to iPhone hotspot.
972387	SSLVPNCmdLine tool has error using PSExec and SYSTEM account.
973808	Non-English OS, such as Spanish, on a non-compliant endpoint fails to show warning when trying to connect to VPN.
974129	Script has error while initiating SAML VPN.
974756	FortiClient (Windows) fails to access Azure databases if using defined cloud-based"Microsoft-Office365" for the application-based split tunnel.
976194	If always up is enabled and device switches from Azure user to local user, IPsec VPN autoconnects.
976343	FortiClient sends the same MAC address of different network adapters with IPsec VPN.
977196	Prelogon VPN causes Windows login to take long time.
977214	If local and remote destination networks are the same, when exclusive routing is disabled, traffic to remote destination can go through VPN tunnel.
978155	Application Firewall behaves incorrectly with Epic browser.
979166	Black screen displays on VPN before logon.
979646	FortiClient cannot connect to VPN [-7200] or [-6006] while using SAML and external browser.

Vulnerability Scan

Bug ID	Description
795393	Vulnerability events are not removed from EMS after successful patch.
849485	FortiClient wrongly detects AnyDesk vulnerabilities CVE-2021-44426 and CVE-2021-44425.
869253	FortiClient (Windows) detects vulnerability when the required KB is installed.
955762	FortiClient does not detect known vulnerable software.

Logs

Bug ID	Description
716803	When logged in to Windows as domain user, avatar does not show properly on FortiAnalyzer 7.0.

Bug ID	Description
849043	SSL VPN add/close action does not show on FortiGate *Endpoint Event* section.
874835	FortiClient (Windows) repeatedly logs security event logging - IPsec VPN "Disconnect" to FortiAnalyzer.
948156	Excessive logging causes high I/O.
948887	FortiClient does not send Windows log of Exchange Server logon failure (Event ID 4625).
965729	FortiClient (Windows) does not send Web Filter monitor and block categories logs to FortiAnalyzer.
979323	FortiClient does not send any logs to FortiAnalyzer unless *Log All URLs* is enabled.

Web Filter and plugin

Bug ID	Description
519066	User cannot print to WSD network printer when FortiProxy is enabled.
776089	FortiClient (Windows) does not block malicious sites when Web Filter is disabled.
836906	After FortiClient install, extended uptime results in audio cracking.
871325	Web Filter breaks DW Spectrum.
875298	Exclusion list does not work properly with regular expressions.
876273	Restricted mode has issue in Edge when moving from off- to on-fabric.
883568	Web Filter causes Docker pull command to fail and connectivity issues afterward.
884420	Web Filter extension does not categorize sites properly.
890433	Firefox extension is stuck on older version.
903426	User cannot access internal application with Web Filter enabled. **Workaround**: Add a simple rule to allow HTTP/HTTPS server IP addresses.
904840	When a user is performing a device recovery in iTunes, error 3500 occurs.
909060	User cannot update information on internal portal with Web Filter active.
911410	Safe Search restriction level does not apply properly if it is enabled for both Web and Video Filters.
939986	Web Filter blocks LUXTRUST middleware.
952715	FortiClient (Windows) blocks access to internal website after receiving EMS profile.
962343	FortiClient does not block unrated sites when it cannot reach FortiGuard servers.
962502	Web Filter does not respect exclusion list when imported from FortiGate with web category overrides.

Avatar and social network login

Bug ID	Description
878050	FortiClient avatar does not update on FortiOS dashboards and FortiOS cannot show updated information.
950503	FortiClient does not use image that user uploaded as their avatar.

License

Bug ID	Description
874676	EMS tags endpoint with existing ZTNA host tags for vulnerabilities and AV after license is updated from Endpoint Protection Platform to Remote Access.

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.
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.
857909	FortiClient (Windows) does not support enabling encryption for ZTNA TCP forwarding rules acquired from ZTNA service portal.
857999	FortiClient does not support use of external browser for SAML authentication for ZTNA rules acquired through service portal.
872153	Old certificate is not deleted when FortiClient is uninstalled or upgraded.
874290	PowerShell with .NET framework 5, 6, or 7 does not work with TCP ZTNA.
913267	FortiClient (Windows) fails to export ZTNA web portal settings.
918045	FortiClient (Windows) requests ZTNA certificate when switching between user accounts.
919832	ZTNA stops working after days with the error message *No ZTNA client certificate was provided*.
949999	SAML authentication does not work with Azure AD certificate-based authentication.
952888	IPv6 DNS servers bypass inline CASB IPv4 access proxies.

Bug ID	Description
954563	TFAP ZTNA SAML authentication popup does not show up if user closes it without authenticating.
954946	ZTNA TCP forwarding does not show the untrusted certificate prompt warning with SAML authentication.
955377	FortiClient (Windows) blocks ZTNA because *device is offline*.
955437	With multiple browsers installed and external browser used for SAML authentication, choosing browser option does not show up if user does not choose any.
955570	FortiClient switches to default site.
965476	User cannot access website with certificate warning and Forticlient DNS Root certificate signs the certificate.
967199	*No ZTNA client certificate was provided* error occurs when trying to access HTTPS page.
975845	FortiClient must notify end user that certificate is not trusted for ZTNA connection when `disallow_invalid_server_certificate` is enabled.
976003	Web access with ZTNA proxy using FQDN fails to work.
976028	ZTNA feature driver fortitransctrl fails to start and causes ZTNA TCP forwarding to not work as expected.

FSSOMA

Bug ID	Description
900953	SSOMA does not send SSO sessions information to FortiAuthenticator.
909844	FSSO sessions drop earlier than expected.

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.
872136	User verification period option does not work as configured.

Other

Bug ID	Description
834389	FortiClient has incompatibility with Fuji Nexim software.
897741	Virus cleaner does not scan PC.
901972	NETIO.SYS causes BSOD.
919017	FortiClient changes the checksum hash of the installer for Baramundi Management Agent.
952013	FortiClient (Windows) cannot access YouTube channel when channel_id is set to *Warning* in EMS.
952737	FortiClient FortiTray has high CPU usage.
964456	FortiClient does not allow Windows DNS only secure dynamic updates.

www.fortinet.com