FORTINET

Release Notes

FortiClient (Windows) 7.2.4

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

March 20, 2024
FortiClient (Windows) 7.2.4 Release Notes
04-724-998650-20240320

TABLE OF CONTENTS

Change log

Date	Change description
2024-03-04	Initial release of 7.2.4.
2024-03-06	Updated Firmware images and tools on page 8.
2024-03-13	Added 1009737 to Remote Access on page 22.
2024-03-20	Added 1008116 to Remote Access on page 22.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 7.2.4 build 0972.

Review all sections prior to installing FortiClient.

FortiClient (Windows) 7.2.4 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 7.2.4 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.

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 failure.

FortiGuard Web Filtering Category v10 Update

Fortinet has updated its web filtering categories to v10, which includes two new URL categories for AI chat and cryptocurrency websites. To use the new categories, customers must upgrade their Fortinet products to one of the versions below:

- FortiManager - Fixed in 6.0.12, 6.2.9, 6.4.7, 7.0.2, 7.2.0, 7.4.0.
- FortiOS - Fixed in 7.2.7 and 7.4.1.
- FortiClient - Fixed in Windows 7.2.3, macOS 7.2.3, Linux 7.2.3.
- FortiClient EMS - Fixed in 7.2.1.
- FortiMail - Fixed in 7.0.7, 7.2.5, 7.4.1.
- FortiProxy - Fixed in 7.4.1.

Please read the following CSB for more information to caveats on the usage in FortiManager and FortiOS:
https://support.fortinet.com/Information/Bulletin.aspx

Installation information

Firmware images and tools

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

File	Description
FortiClientTools_7.2.4.0972.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_ 7.2.4.0972_x64.zip	Fortinet single sign on (FSSO)-only installer (64-bit).
FortiClientVPNSetup_ 7.2.4.0972_x64.exe	Free VPN-only installer (64-bit).

EMS 7.2.4 includes the FortiClient (Windows) 7.2.4 standard installer and zip package containing FortiClient.msi and language transforms.

The following tools and files are available in the FortiClientTools_7.2.4.0972.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.
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_7.2.4.0972_x64.zip	Standard installer package for Windows (64-bit).
FortiClientVPNSetup_7.2.4.xxxx_x64.exe	Free VPN-only installer (64-bit).

Review the following sections prior to installing FortiClient version 7.2.4: 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 7.2.4, do one of the following:

- Deploy FortiClient 7.2.4 as an upgrade from EMS. See Recommended upgrade path.
- Manually uninstall existing FortiClient version from the device, then install FortiClient (Windows) 7.2.4.

FortiClient (Windows) 7.2.4 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) 7.2.4 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 7.2.4 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 7.2.4 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) 7.2.4. 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
VCM engine	• 2.0040
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) 7.2.4. 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) 7.2.4: • 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.

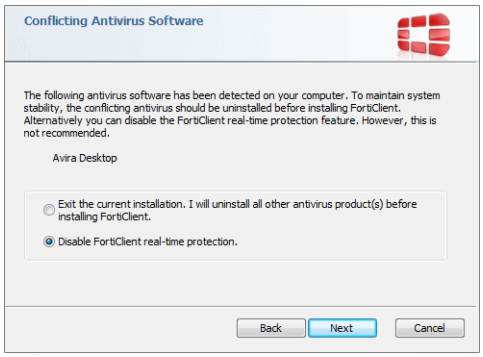
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

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.



Intune product codes

Deploying FortiClient with Intune requires a product code. The product codes for FortiClient 7.2.4 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 7.2.4. For inquiries about a particular bug, contact Customer Service & Support.

ZTNA connection rules

Bug ID	Description
885014	Zero trust network access (ZTNA) fails to resolve FQDN destination hosts with certain domains.
976003	Web access with ZTNA proxy using FQDN fails to work.

Web Filter and plugin

Bug ID	Description
812794	Downloads are canceled in Firefox when Web Filter extension is enabled.
984427	Web Filter traffic logs show that 0 bytes were sent and received.

GUI

Bug ID	Description
975622	GUI does not launch when user clicks EMS invitation link when FortiClient (Windows) is closed.

Endpoint control

Bug ID	Description
976602	Use the previous resolved IP address when DNS server fails to respond endpoint DNS query.
979593	One-way message GUI is not translated.
979756	FortiClient disconnects from Windows primary EMS after first sync.

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
953124	Orchestrator notification does not appear when upgrade is scheduled.

Logs

Bug ID	Description
811746	FortiClient (Windows) sends duplicated and old logs to FortiAnalyzer.
962704	FortiClient floods FortiAnalyzer with SYN packets.
966018	FortiClient uploads logs more frequently than its configured upload interval.
974960	Log daemon makes connections to FortiAnalyzer when updating or starting VPN.
1001042	FortiClient cannot send SIEM logs to FortiAnalyzer.

Zero Trust tags

Bug ID	Description
976374	CURRENT_USER registry tag does not work.
988269	Using spaces in common name when creating certificate-based ZTNA rules with regular expressions do not pass tags.

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.
987137	vcm.exe 2.0.39.39 crashes.

Remote Access

Bug ID	Description
882408	FortiClient fails to renew password when user changes password after user password expired message appears in Windows login.
890000	FortiClient 7.2.0 configured with `on-os-start-connect` is slow compared to FortiClient (Windows) 7.0.7.
907248	FortiClient cannot connect to FortiSASE SAML VPN using OneLogin as identity provider (IdP) with built-in browser when IdP requires client certificate.
909573	With multifactor authentication enabled and autoconnect, user account password becomes empty after login to Windows.
912980	IPsec VPN fails to connect if `vpn-ems-sn-check` is enabled and FortiClient is registered to custom site.
930740	User cannot set up SSL VPN if password contains Polish characters ł , ą, and ń.
931283	Machine VPN does not work if secure sign-in policy is enabled and users must press `Ctrl+Alt+Delete` to login.
936354	FortiClient (Windows) cannot establish SSL VPN connection with Microsoft Entra ID SAML when Entra ID autologin is enabled.
949945	Network lockdown blocks FortiClient Cloud Telemetry.
951269	SSL VPN logs out immediately after login when application split tunnel is enabled.
954004	FortiClient (Windows) cannot establish DTLS tunnel when handshake packet has a large MTU.
962287	SSL VPN reaches infinite loop that keeps trying to connect to SSL VPN but fails.
963039	SslvpnAgent: Pipe is broken for writing.
966713	User certificate-only tunnels do not autoconnect if user does not connect the tunnel once before logging out of Windows.
970620	SAML SSL VPN still connects to SAML without asking for credentials even if *Save Password* is disabled

Bug ID	Description
974129	Script error occurs while initiating SAML VPN.
976050	FortiClient does not provide Entrust eGRID information so user can put in their 2F grid information.
979166	Black screen appears on VPN before logon.
998146	SSL VPN disconnects every 20-30 minutes.

PAM

Bug ID	Description
982033	Native launchers fail after upgrading standalone FortiClient from previous version.
990358	Browser privilege access management (PAM) extension does not autofill credentials correctly for EMS and password field remains blank.

Other

Bug ID	Description
964456	FortiClient does not allow Windows DNS only secure dynamic updates.
971090	FortiClient daemon (fcaptmon) has memory leak.
982997	FortiShield.sys causes blue screen of death on Windows 10.

Known issues

The following issues have been identified in FortiClient (Windows) 7.2.4. 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.
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.
980803	Image becomes corrupted or damaged with a green patch when trying to view it from a shared location.

Avatar and social network login

Bug ID	Description
878050	FortiClient avatar does not update on FortiOS dashboards and FortiOS cannot show updated information.
943053	FortiClient (Windows) grays out avatar page when uploading image using user input or logging in via LinkedIn or Google.
950503	FortiClient does not use image that user uploaded as their avatar.

Chromebook

Bug ID	Description
997927	On Chromebook, fallback action is to override exclusion list, which is unlike FortiClient (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.
981552	Upgrade through installer from digital experience monitoring (DEM) to non-DEM build does remove or stop DEM agent on endpoint.

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.
996850	FortiClient sends different username to EMS when user logs on to computer with SmartCard.
1002476	Disconnecting from EMS using password does not work.
1003435	FortiClient (Windows) shows Sandbox, Web Filter, and Vulnerability Scan profiles when unregistered from EMS due to expired license.

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.
990496	FortiClient flickers and opens.

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.
989640	FortiClient does not follow EMS profile after EMS updates feature selecting setting.

Endpoint security

Bug ID	Description
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.
982747	FortiPAM password filter extension is not removing automatically from Firefox when FortiClient (Windows) is uninstalled.
997337	User cannot upgrade FortiClient (Windows) from 7.0.1 to 7.0.9.
993353	FortiClient is missing telemetry pages after upgrading from 7.2.2 to 7.2.3.

License

Bug ID	Description
1003493	FortiClient (Windows) does not show license expiry alert message on telemetry page when offline.

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 (RTP) 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	FortiClient (Windows) cannot scan mapped drives on-demand.
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. 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.
972036	Sandbox agent uses high CPU/memory/I/O when connecting to external SSD.
972671	If Malware Protection is enabled, Valorant fails to work.
984972	RTP fails to detect ransomware Lockbit.K!tr.ransom.
991539	FortiClient (Windows) cannot open AV logs on the scan result page after performing on-demand or scheduled scan.
996029	fmon blocks shared directory that sumidero SNC SQL Tool uses due to suspicious virus that FortiClient (Windows) detects in bitacora.exe.

Bug ID	Description
996431	FortiClient (Windows) cannot block remote NDIS device when the net class device is set to block in removable media access function.
998905	FortiClient cannot detect a malicious file, PowerISO6.exe.
1004611	FortiClient removable media access does not scan USB drive.

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.
1002079	Security Zero Trust tagging rule to tag endpoints where automatic updates are enabled does not work as expected.

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.
991892	Windows 11 clients do not populate Software Inventory in EMS.

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.
758424	Certificate works for IPsec VPN tunnel if put it in local computer but fails to work if same certificate is in current user store.

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.
837391	FortiClient does not send public IP address for SAML, which leads to 0.0.0.0 displaying on FortiOS and FortiSASE.
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 Microsoft Entra ID and Duo (multifactor authentication (MFA)).
851600	FortiClient fails to connect to SSL VPN with FQDN resolving to multiple IP addresses while resolved IP address is unreachable.
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.
872339	Per-user autoconnect does not work after restarting FortiClient.
874208	FortiClient (Windows) cannot dial up SSL VPN tunnel with ECDSA certificate.

Bug ID	Description
874298	Always up does not work for SAML SSL VPN tunnel with single FQDN resolved to multiple IP addresses.
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.
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.
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 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.
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.
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.
909244	SSL VPN split DNS name resolution stops working.

Bug ID	Description
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.
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.
920908	IPsec VPN password renew prompt differs from SSL VPN prompt.
920912	Gateway selection logic for SAML SSL VPN with resilience to FortiVPN needs refactoring.
922941	Connecting to SSL VPN with FQDN resolved to IPv4 and IPv6 as remote gateway gets stuck at 98%.
942668	Split DNS on SSL VPN only resolves the first DNS server.
950787	Domain filter cannot block access to specific server FQDN.
953160	SAML token reuse does not work for SSL VPN if *Disable Connect/Disconnect* option is enabled in EMS Remote Access profile.
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.
961079	Application-based split tunnel needs clarification on how it supports the new Microsoft Teams.
962411	SSL VPN resiliency tunnel with multiple remote gateways with first gateway unreachable does not work if using certificate in local machine.

Bug ID	Description
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.
967051	Initial autoconnect of IPsec VPN on machine reboot fails.
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.
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.
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.
974478	IPsec VPN with split tunnel and network address group with IP address range does not work.
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.
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.
979646	FortiClient cannot connect to VPN [-7200] or [-6006] while using SAML and external browser.
982319	For IPsec VPN phase 2, GUI does not support selecting multiple DH groups.
982354	DH Group module size compatibility requires enhancement for improved IPsec VPN security.
982497	FortiClient fails to establish IPsec VPN with multiple DH groups configured in phase 1.
984454	Since upgrade to 7.2, FortiClient does not remember password when connecting SSL VPN.

Bug ID	Description
986732	After upgrade, the IPsec IKEv2 VPN tunnel does not work.
987400	Autoconnect checkbox grayout behavior is inconsistent.
988053	IPsec VPN connection IKE negotiation displays a Windows popup, but it appears in the background.
989595	IPsec VPN IKEv2 tunnel shows SSL VPN username when using only PKI authentication with only certificate and EAP disabled.
989864	When network lockdown is enabled in Remote Access profile, sign in to the operating system takes longer than usual.
991178	IPsec VPN routes traffic through VPN-FortiGate tunnel even if local LAN is disabled on EMS.
992814	Disclaimer acceptance box always pops up when VPN always on is configured.
994884	FortiShield blocks FortiSSLVPNsys.exe and causes SSL VPN connection failure.
995323	Third-party software Lisec throws Java error and drops database connection when endpoint is connected to SSL VPN.
995612	Negative split tunnel metric setting results in loop.
995970	FortiTray has issues depending on FortiClient (Windows) default tab.
996877	ManageEngine ADSelfService installed endpoint causes issue on other user screen when VPN before logon is enabled.
997131	FortiClient retains saved password despite autoconnect failure in SSL VPN connection with changed client password.
997151	IPsec VPN connection with RADIUS user (NPS with MFA) fails to connect using previously saved password.
997277	FortiClient autoconnects when autoconnect is not configured.
997279	FortiClient drops VPN connection after executing taskkill command.
997662	With password saved, clicking *Connect* results in a flash during VPN connection.
997718	When FortiClient (Windows) enables autoconnect, it behaves like always up is enabled.
997860	Reverse DNS queries cause issues in FortiSASE secure private access environment due to split DNS not supporting PTR records.
998022	Split DNS implementation is ineffective in SSL tunneling.
998144	FortiClient (Windows) cannot use network lockdown and Entra ID together.
998406	GUI does not respond when connected to IPsec VPN IKEv2 tunnel with enable LAN option disabled.
999089	When user only saves username, connecting from FortiTray does not cause the GUI to pop up.
1000261	IPsec VPN is not triggered after successful SAML authentication if authentication is delayed for more than 60 seconds.

Bug ID	Description
1000589	VPN is stuck on connecting and error 6005 occurs if SAML takes longer than 60 seconds.
1000706	VPN before Windows logon requires second attempt due to CachedLogonsCount issue.
1000952	IPsec VPN SAML does not validate certificate for untrusted certificate on FortiAuthenticator.
1001405	When connecting to IPsec VPN IKEv2 with SAML, if user clicks *No* on security alert, connection continues.
1001770	After attempting wrong password multiple times, SSL VPN with Entra ID authentication is not triggered after clicking *Connect*.
1002294	FortiClient does not reconnect to VPN until restarted.
1002375	IPsec VPN disclaimer message does not work.
1002424	Remote Access page gets stuck if user clicks *Disconnect* for SSL VPN tunnel using Entra ID SAML with realms before VPN connects.
1002456	After upgrade, customize host check fail warning does not appear when tag is on device.
1002528	FortiClient gets stuck on connecting screen if user closes authentication window without providing credentials.
1002837	GUI shows that tunnel is connected when it is not for IPsec VPN autoconnect using Azure logon session information.
1003277	User autoconnect does not work until user manually triggers first VPN connection.
1003308	FortiClient attempts to autoconnect to Azure autoconnect tunnels when logged-in user is not an Azure user.
1003436	IPsec VPN disconnects or freezes.
1003737	IPsec VPN connection drops a few seconds after connecting multiple times, before being able to successfully establish connection.
1003780	IPsec VPN IKEv2 with certificate authentication has issues with connection when off-net.
1004039	IPsec VPN IKEv2 with SAML and always up does not work on some VMs with latest Windows updates installed.
1005121	SSL VPN frequently disconnects after upgrading FortiClient (Windows).
1006295	FortiClient fails to consistently connect (40%) with DNS round robin of FortiGates for FortiSASE.
1008116	SAML VPN is stuck at 0% with error (-6005) after upgrade to 7.2.4.
1009737	SSL VPN SAML *Connect* button becomes disabled after closing SAML authentication window or reaching timeout displayed in GUI.

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.
989431	Vulnerability Scan recognizes Windows 10 as Windows 11.

Logs

Bug ID	Description
716803	When logged in to Windows as domain user, avatar does not show properly on FortiAnalyzer 7.0.
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.
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.
984729	Traffic logs do not populate on FortiAnalyzer.
985044	FortiClient log level does not change from debug and user cannot delete log files from "%AppData%".
988706	Web Filter log in FortiAnalyzer does not have URL information.
993163	FortiClient (Windows) does not generate fcdblog log file in the trace logs folder.
996345	Disabling logging from EMS profile still results in it being enabled.
996767	FortiAnalyzer does not show endpoint logs after endpoint upgrade from 7.0.9 to 7.2.3.
999900	Exporting log from GUI does not include IPsec VPN IKEv2 connected log line.

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.
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.
914636	Web Filter exclusion list does not include Warn action support.
939986	Web Filter blocks LUXTRUST middleware.
948500	Video Filter does not block YouTube channel if channel ID case changes in the URL.
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.
996420	Web Filter has issue with resolved IP addresses in multiple ISDB objects such as cloud applications.
997118	Web Filter extension does not apply DNS restrictions when Safe Search is enabled on Web Filter profile.
997519	Web Filter does not block all subdomains when domain URL is set to Block in the exclusion list and *Wildcard Match Root Domain* is enabled.
998747	FortiClient does not block Gmail when using Gmail link in Chrome browser.
999256	FortiClient (Windows) blocks some HTTP exclusions that it should allow.
999261	Web Filter blocks WSL-vpnkit connection on Windows 11.
1002532	FortiClient does not take exceptions set on Web Filter profile and blocks download of RDP plugin, blocking access to server.

ZTNA connection rules

Bug ID	Description
814953	Using an external browser for SSH ZTNA requires restarting FortiClient on Windows 11.
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.
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*.
921406	ZTNA destination rule using hostname does not work.
931275	ZTNA destination rules stop working.
942413	Issue occurs when trying to reach a ZTNA destination added to FortiClient manually from public IP address as it does not resolve.
949999	SAML authentication does not work with Azure AD certificate-based authentication.
952888	IPv6 DNS servers bypass inline CASB IPv4 access proxies.
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.
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.
976028	ZTNA feature driver fortitransctrl fails to start and causes ZTNA TCP forwarding to not work as expected.
977407	ZTNA TCP forwarding with authentication does not work properly for SaaS and SaaS group applications.

Bug ID	Description
990864	With SAML for ZTNA authentication, after closing the first session, the second session continues to request credentials.
992649	User cannot create FortiGate tunnel if FortiGate works as both VPN and ZTNA proxy server.
995677	ZTNA TCP forwarding fails to prompt for SAML authentication with external browser after closing and reattempting the connection.
1001116	FortiClient requests SAML credentials after network change in ZTNA connections.

FSSOMA

Bug ID	Description
900953	SSOMA does not send SSO sessions information to FortiAuthenticator.
909844	FSSO sessions drop earlier than expected.
995379	FSSOMA does not properly install on CIS hardened Windows 10 and 11 image.

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.
982079	FortiClient Cloud invitation with LDAP verification type to Entra ID fails with *Azure Token Required* error.

PAM

Bug ID	Description
993068	Firefox FortiPAM launch secret does not record screen for newly opened tabs. It only records the first tab opened from launch secret.
1001231	FortiPAM extension does not support Firefox.

Other

Bug ID	Description
834389	FortiClient has incompatibility with Fuji Nexim software.
897741	Virus cleaner does not scan PC.
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.
984763	NETIO.SYS/FortiWF2.sys causes blue screen of death on Windows 10.
998183	FortiESNAC.exe crashes and fails to update signatures.
999139	Laptop Wi-Fi DNS setting gets stuck in unknown DNS server after FortiClient connects to and disconnects from IPsec or SSL VPN.

www.fortinet.com