Release Notes

FortiClient (Windows) 7.2.2

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®

November 06, 2023
FortiClient (Windows) 7.2.2 Release Notes
04-722-935802-20231106

TABLE OF CONTENTS

Change log

Date	Change Description
2023-10-04	Initial release of 7.2.2.
2023-11-06	Updated Installation information on page 9.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 7.2.2 build 0864.

- Special notices on page 7
- What's new in FortiClient (Windows) 7.2.2 on page 8
- Installation information on page 9
- Product integration and support on page 12
- Resolved issues on page 15
- Known issues on page 24

Review all sections prior to installing FortiClient.

Licensing

See Windows, macOS, and Linux endpoint licenses.

FortiClient 7.2.2 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:

- Azure
- 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.

What’s new in FortiClient (Windows) 7.2.2

For information about what's new in FortiClient (Windows) 7.2.2, 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_7.2.2.xxxx.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_7.2.2.xxxx.zip	Fortinet single sign on (FSSO)-only installer (32-bit).
FortiClientSSOSetup_7.2.2.xxxx_x64.zip	FSSO-only installer (64-bit).
FortiClientVPNSetup_7.2.2.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_7.2.2.xxxx_x64.exe	Free VPN-only installer (64-bit).

EMS 7.2.2 includes the FortiClient (Windows) 7.2.2 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 not able 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_7.2.2.xxxx.zip	Standard installer package for Windows (32-bit).
FortiClientSetup_7.2.2.xxxx_x64.zip	Standard installer package for Windows (64-bit).
FortiClientVPNSetup_7.2.2.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_7.2.2.xxxx_x64.exe	Free VPN-only installer (64-bit).

Review the following sections prior to installing FortiClient version 7.2.2: 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 7.2.2, do one of the following:

- Deploy FortiClient 7.2.2 as an upgrade from EMS. See Recommended upgrade path.
- Manually uninstall existing FortiClient version from the device, then install FortiClient (Windows) 7.2.2.

FortiClient (Windows) 7.2.2 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) 7.2.2 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 7.2.2 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 7.2.2 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) 7.2.2. 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 • 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	• 6.00287
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) 7.2.2. 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) 7.2.2: • 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.

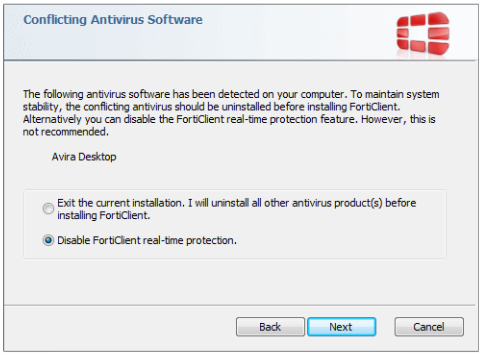
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

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 7.2.2 are as follows:

Version	Product code
Enterprise	{21C1D5EA-CA5E-4625-A8B9-A90CE156CF16}
VPN-only agent	{8DEDB631-3E1D-4DAF-AA5B-A91F8F95A6E9}
Private access management-only agent	{14EABB42-F6A1-4FB9-A019-C57B70665ADE}
Single sign on-only agent	{044EA3E4-58C0-4DFA-8450-423C1A0EB2CB}

See Configuring the FortiClient application in Intune.

Resolved issues

The following issues have been fixed in version 7.2.2. For inquiries about a particular bug, contact Customer Service & Support.

ZTNA connection rules

Bug ID	Description
875254	FortiClient (Windows) cannot finish ZTNA TCP forwarding TFA authentication when FortiClient (Windows) disables *Use external browser...*
883269	FortiClient (Windows) stops logging service portal activities even though new TCP forwarding entries are configured on FortiOS.
914111	ZTNA daemon fortitcs stops updating its log file after running for some time.
918501	Zero trust network access (ZTNA) TCP forwarding (remote desktop protocol) does not work if encryption is enabled and LDAP authentication is used.
919540	ZTNA password can be seen in plain text format in GUI logs with basic authentication enabled.
933690	FortiClient (Windows) does not update Fortitcs logs after a few portal queries or forwarding connection.

Web Filter and plugin

Bug ID	Description
867483	Web Filter does not give warning message.
915287	Extension does not properly apply safe mode HTTP header restrictions.
919419	Web Filter with FortiGuard Anycast spamming blocks (Unknown) alerts in Notifications.

GUI

Bug ID	Description
913777	Action for cookies should be moved from *Advanced* > *VPN* to *Settings*.
926401	GUI error log should be in info log `Failed to load REG_SSLVPN_SERVICE_PORT`.

Bug ID	Description
943787	Message keeps popping up on endpoint after user acknowledges it.

Endpoint control

Bug ID	Description
900189	Connection media on-fabric detection rule type does not work properly with Windows 10.
921937	FortiClient cannot register to EMS using *Register to EMS* button in invitation email.
922818	FortiESNAC.exe crashes.
927738	EMS shows most endpoints as offline

Application Firewall

Bug ID	Description
853451	FortiClient blocks PIA VPN.
853808	Excluding IPS signatures from Application Firewall (Detect and Block Exploits) is not possible.
876265	Zip Files become corrupt with Application Firewall enabled.
897207	Application Firewall blocks Microsoft 365 Defender device isolation .

FSSOMA

Bug ID	Description
841316	Some FortiClient single-sign on mobility agent (FSSOMA) versions do not present client certificate to FortiAuthenticator.
862021	Local account can access Internet if FSSOMA is logged in and user locks the screen.
888721	SSOMA does not report the domain/user information to FortiAuthenticator in hybrid Azure Active Directory (AD) setup.
893985	FSSOMA creates issue with tenant ID on FortiAuthenticator in standard AD setup.

Configuration

Bug ID	Description
864571	Configuration backup file contains wrong default port of 65535.
897927	FortiClient causes reboot on domain controllers .

Install and upgrade

Bug ID	Description
896152	FortiClient shows *Update failed - Error occurred!* popup after reboot.
905132	Failed to upgrade FSSO 7.2.0 to 7.2.1 with installer that FortiClientSSOConfigurationTool created.
907340	Telemetry connection requires reboot after install.
915493	Reboot popup does not display.
926815	`Host_verification_xml` is missing after upgrading FortiClient 7.2.0 to 7.2.1.

Logs

Bug ID	Description
923245	FortiClient logs do not include time zone .
935428	Frequent log floods other logs in FortiTray and makes debugging difficult.
945992	Diagnostic result is missing FortiClient (Windows) local log.

Zero Trust tags

Bug ID	Description
928574	*Logged in Domain* tags do not work for Azure AD domains.
931490	ZTNA tag is not removed after vulnerability is resolved.
932828	Registry key ZTNA tag does not work when comparing DWORD type data.
911533	AD group ZTNA tag does not calculate on EMS and FortiClient.
919595	ZTNA tag rule does not work for Bitlocker disk encryption.

Vulnerability Scan

Bug ID	Description
908266	FortiClient fails to detect vulnerabilities due to FCM skipping certain VIDs when scanning.
920439	Vulnerability scan reports excluded applications.
944404	Upgrade OpenSSL to 3.1.2: third party component upgrade required for security reasons.

Remote Access

Bug ID	Description
702764	IPsec VPN connection fails with error: *Certificate Was Not Loaded*.
800934	DH group settings are not read-only for tunnel that EMS pushed.
801747	New XML tag `<block_outside_dns>` should be configured per-tunnel.
811458	Connecting to SSL VPN fails after installing Windows update KB5013942.
824165	SSL VPN reconnection does not work when using turn-based FortiClient connection vs. PPP method.
838231	Some users fail when using SAML authentication with SSL VPN.
851093	IPv6 DNS requests do not work.
855836	Remote VPN is visible when on-fabric when it should be hidden.
858696	FortiClient (Windows) cannot connect to SSL VPN with SAML via Satellite ISP.
886928	VPN before logon displays FortiClient credentials prompt if using user@domain.local format for username.
893958	FortiClient (Windows) does not support autoconnect in this session (CREDENTIALPROVIDER).
904923	SSL VPN with external DHCP servers requires DHCP option 12 hostname.
905354	Split tunnel with SSL VPN does not work.
906617	SSL VPN with certificate and token does not work as expected when connecting from tray icon in Windows 10 x64.
907361	IPsec VPN IKE v1 and v2 blocking IPv6 does not work.
907518	FortiClient can connect to VPN without proper remote secure access tag.
909699	Autoconnect only when off-net fails to connect if remote gateway network is down then up.
912255	SSL VPN stays connected even though there is no network connection to the VPN gateway when DTLS is enabled.
914414	When VPN before logon is configured, FortiClient does not initiate SSL VPN when *Use Windows*

Bug ID	Description
	Credentials is enabled.
918669	Single user mode VPN disconnects if user locks then unlocks Windows.
920805	With multifactor authentication enabled, SSL VPN may fail to work.
920870	GUI does not support encryption as NCSC support defines.
923869	FortiClient retries multiple times to connect to VPN with Azure AD autologin when user belongs to more than 100 groups.
925710	For split tunnel exclusions, local routes are added with incorrect next hop on multihomed devices.
926174	DNS has delays on SSL VPN with *Same as client system DNS* error and DNS server is unreachable over VPN.
926774	Azure SAML VPN fails to autoconnect after machine wakes from hibernation.
927083, 937347	SAML login window does not come up when clicking *SAML Login* button.
927825	Host check for firewall does not work with FortiOS 7.0.12.
929177	IPsec VPN IKE v2 with preshared key or certificate-based with EAP enabled fails to connect.
931326	*Invalid server address or port number.* error occurs during upgrade.
931680	VPN before logon on Windows 11 build 7129 does not work as expected.
938746	Secure remote access with SAML tries to connect when it should be blocked.
943208	FortiClient (Windows) continuously autoconnects after manual disconnection.
945056	FortiClient (Windows) does not save Azure SAML authentication cookies in local storage and is missing SAML_VPN_COOKIES key.
947956	FortisslVPNdaemon.exe indexes the FortiClient installed location on port 8053.
950199	FortiClient (Windows) sends no DTLS encrypted alert to FortiGate when disconnecting SSL VPN DTLS tunnel.
950815	SSL VPN SAML login fails to work when using Okta for initial authentication.
951164	FortiClient (Windows) does not save SAML login credentials when *Save Password* is enabled.
953853	SSL VPN SAML login shows black login page if FortiClient (Windows) cannot reach IdP.

Malware Protection and Sandbox

Bug ID	Description
716547	AV and Sandbox do not support combination of wildcard and path variable exclusions.
875930	FortiClient fails to quarantine a specific malware-infected dll file in Exchange Server.
893530	FortiClient reports the endpoint as not having third-party antivirus when Microsoft Defender is

Bug ID	Description
	active.
893964	FortiClient cannot quarantine files located in a network-shared folder.
894638	FortiClient shows to kill 1426161032.exe twice for W32/Filecoder.CL!tr.ransom.
903614	Number of blocked exploit count is inconsistent with EMS.
907006	FortiClient console closes automatically when FIPS is enabled through CLI or EMS-created installer.
907331	FortiClient cannot create exception for NetSupport Manager.
911335	Removable media blocks duplicate USB device with same `'driverkeyname:' & 'device_property_classguid:'`.
911521	Sandbox Detection shows double count of executed samples.
913701	Antiransomware feature fails to decrypt MSIL/Filecoder.AKJ!tr.ransom.
917941	Sandbox exclusions do not work for shared drives.
919920	FortiClient does not automatically restore previously allowlisted samples when FortiSandbox rescans them.
921366	Recorder device is inaccessible with removable media access (RMA) enabled.
923470	RMA modifies NoDriveTypeAutoRun (sets value 44) registry key.
926335	Sandbox include and exclude lists do not work.
926383	When realtime protection is enabled, logon takes around two to three minutes.
929900	FortiClient does not recognize HP docking station.
930398	USB exception rule with specific vendor ID and PID does not work.
931816	FortiClient (Windows) reports detected ransomware to Sandbox Detection.
934389	Sandbox fails to quarantine or block files in network drive.
937971	Sandbox *Alert & Notify* does not behave correctly.

Zero Trust telemetry

Bug ID	Description
911495	FortiClient fails to autoregister to FortiClient Cloud due to Telemetry key mismatch.
922757	ZTNA registry tag rule crashes FortiNSNAC and causes FortiClient to fail to sync EMS profile and deregister.
953263	FortiESNAC process has memory leak.
953521	Feature shows as hidden when EMS does not configure it being hidden.

Deployment and installers

Bug ID	Description
942984	EMS shows wrong scheduled time under endpoint details page for endpoint user-scheduled FortiClient (Windows) deployment.

Endpoint management

Bug ID	Description
904348	FortiClient (Windows) and EMS detect encrption status as not enabled when only one hard disk has encryption (Bitlocker) enabled.

PAM

Bug ID	Description
864571	Backup configuration contains wrong default port of 65535.
868822	PAM does not support some video parameters such as resolution, color, and so on.
905506	Recording shows black screen for SQL Server Management Services.
908671	PAM doe snot include private HTTP header (x-complete: true) to signal the file is finished uploading.
909164	PAM does not support live streaming.
912655	FortiPAM secret launchers do not launch correctly when accessing FortiPAM via external DNAT.
914874	FortiClient PAM component does not report that video monitoring has stopped.
917230	If some CLI launch (mysql shell) closes quickly, PAM GUI keep loading for 15 seconds , then response error displays.
918352	Client executable integrity check.
918486	No video-Finish received in FortiPAM.
930761	*"Unchecked runtime.lastError: The message port closed before a response was received."* error displays with PAM agent.
931648	FortiClient PAM is not disabled in the MSI MST when it is disabled in the installer package.
939187	PAM session recorded video from extension has incorrect length because information is missing in mpd file.
946105	PAM does not include FortiClient version, OS type, and build number.

FortiSASE

Bug ID	Description
930967	FortiClient (Windows) cannot establish FortiSASE VPN with Azure SAML AD user and Windows Defender blocks FortiClientConsole.exe.

Other

Bug ID	Description
797264	FortiClient (Windows) cannot update signatures from FortiManager.
833661	Blue screen of death (BSOD) occurs with FortiClient installed.
874474	FortiClient does not start update_task as scheduled or update ISDB signature.
893820	Add new Forensics agent to FDS.
896137	DesktipID does not work after installing FortiClient.
900691	Forticlient on Windows Server 2019 causes BSOD when copying files to and from Citrix Share.
909504	Use industry standards in names and labels.
915119	Localization into supported languages.
915168	Memory leak in fcaptmon process.
919027	User cannot shut down FortiClient (Windows) after deregistering from and EMS that has *Require Password to Disconnect From EMS* enabled.
922413	fortitcs.exe thread and handle leak.
931821	Orchestrator.exe pings 1.1.1.1.
932433	FortiClient binds Forensic and VCM features.
933608	FortiAptFilter.sys causes BSOD on Windows 11 with FortiClient.
937175	Windows Firewall shows alert regarding FortiClient.exe.
937215	ftsvnic.sys causes BSOD.
938181	ZTNA daemon takes high CPU and keep switching between its log files.
940025	FortiClient does not have the latest ICDB signature version in the installed build.
948228	FortiShield blocks its own process (fmon).
954687	FortiSSLVPNdaemon crash observed in the auto test system.
955237	FortiSettings crashes when FortiClient Settings configuration is selected/unselected in GUI.

Common Vulnerabilities and Exposures

Bug ID	Description
957936	FortiClient for Windows no longer is vulnerable to exposing sensitive information in the agent log.

Known issues

The following issues have been identified in FortiClient (Windows) 7.2.2. 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.
848280	Application-based split tunnel does not work.
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.
907089	Application Firewall blocks MS.Windows.HTTP.Protocol.Stack.CVE-2022-21907.Code.Execution.
936039	WhatsApp_Web_File.Download and WhatsApp_Web_File.Upload App signatures do not work in FortiClient Firewall.
940481	Antivirus (AV) and Application Firewall cause network problems.

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
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.
821024	FortiClient fails to send username to EMS, causing EMS to report it as different users.
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.
914495	Pinging a public IP address does not work for on-Fabric detection rules.
926631	Windstream hits a condition where duplicate users show in EMS and FortiClient (Windows) intermittently does not send user updates.

Endpoint management

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

GUI

Bug ID	Description
795350	Multiple FortiTray icons display in Windows system tray.
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.
949939	JavaScript error occurs in main process.
954711	FortiClient allows entering user personal information when EMS has disabled manually entering user details.
955209	GUI has issues after disconnecting from VPN.
955724	GUI takes around 28 seconds to display when connecting from FortiTray.

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.

Install and upgrade

Bug ID	Description
769639	FortiDeviceGuard is not installed on Windows Server 2022.

Bug ID	Description
783690	Reboot prompt does not display after user login.
870370	Upgrading FortiClient from FortiClient Cloud uses expired invitation code to register.
914498	After deploying FortiClient upgrade through IBM BigFix, on some endpoints, FortiClient does not start or connect to EMS telemetry .
953492	FortiClient cannot be installed on Windows 10 version 20H2 and 22H2.
955268	User can uninstall FortiClient when it is registered to EMS.
955824	Free VPN-only FortiClient (Windows) does not include FSSOMA registry value if user upgraded free VPN-only FortiClient (Windows) from 7.0, which does not have SSOMA.

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.
916958	FortiClient cannot detect a virus-infected file.
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.

Bug ID	Description
935610	Windows context menu popup takes long time to display when AV exclusions are added.
936105	USB media blocks all devices.
940272	AV and Sandbox profiles do not allow copying files to a share folder.
943466	FortiClient deletes suspicious file even though the configurated action in the profile is to quarantine the file.
946390	RTP blocks Word and Excel file access from network shared drive (NAS).
950411	Sandbox exclusions do not work.
950896	FortiClient installed on server blocks PowerShell scripts and causes performance issues.
952073	Windows notification about virus protection is out-of-date and red icon on WSC.
956963	FortiClient Spoolsv is blocked when Windows Antimalware Scan is enabled.

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.
956947	Zero Trust tags disappear from FortiClient (Windows) avatar if a different user logs in to Windows machine.

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.

Zero Trust Telemetry

Bug ID	Description
917708	FortiClient cannot connect to EMS if installed on same machine.

Bug ID	Description
945911	FortiClient is stuck at syncing state after enabling registry tagging rule.
952565	FortiClient does not show error after reconnecting with deleted invitation code.

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.
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.
816826	SAML VPN connection has *"ErrorCode=-6005"* issue when it reaches 31%.
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.
851600	FortiClient fails to connect to SSL VPN with FQDN resolving to multiple IP addresses when it cannot reach resolved IP address.
854237	FortiClient fails to connect at 98% when connecting to hot spot/Wi-Fi when dual stack is enabled on gateway device.

Bug ID	Description
858806	IKE/IPsec VPN sends the same token code multiple times within a second.
859061	Azure autologin des not work.
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.
873490	SSL VPN failover does not show the correct error message when user provides wrong credentials.
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.
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.

Bug ID	Description
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.
885285	SSL VPN network profile is public instead of domain.
887631	Using closest gateway based on TCP round trip for IPsec VPN resilience does not work if ping is disabled for first gateway.
890000	FortiClient 7.2.0 configured with `on-os-start-connect` is slow compared to 7.0.7.
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.
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.
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.
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.

Bug ID	Description
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.
912980	IPsec VPN fails to connect if `vpn-ems-sn-check` is enabled and FortiClient is registered to custom site. **Workaround:** Always establish Fortinet Security Fabric between FortiGate and EMS default site before you attempt IPsec VPN connection if `vpn-ems-sn-check` is enabled and FortiClient is registered to custom site.
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.
922941	Connecting to SSL VPN with FQDN resolved to both IPv4 and IPv6 as remote gateway gets stuck at 98%.
929442	ZTNA TCP forwarding with remote LDAP authentication does not work for SMB.
933603	SSL VPN connection drops intermittently.
933991	FortiClient does not trust SSL VPN gateway that is signed by Internal Intermediate Cert even though the PC trusts it.
938977	SSL VPN throughput degrades with DTLS enabled.
941259	When enabling *Register this connection's addresses in DNS* on the adapter, after a restart, the option is disabled.
942104	SSL VPN with multifactor authentication set for user with FortiToken Mobile process stops at 98% and FortiClient (Windows) does not establish connection.
942668	Split DNS on SSL VPN only resolves the first DNS server.
944266	SAML login always up does not work.
945874	When disconnecting from VPN, FortiClient (Windows) does not restore *Register this connection's IP to DNS* configuration.
945888	VPN before logon does not prompt for one-time password (OTP) token request if using FortiToken Mobile with FortiAuthenticator for OTP.
947381	When `prefer_sslvpn_dns=0` and SSL VPN is up, FortiClient adds dns-suffix to all network

Bug ID	Description
	interfaces.
948611	With customize host check fail warning off and ZTNA tags assigned, FortiClient (Windows) show warning box with empty message when trying to establish VPN.
949977	FortiClient disclaimer does not work for IPsec VPN.
950787	Domain filter cannot block access to specific server FQDN.
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.
953693	Special characters in password incorrectly change VPN *Connect* button to *SAML Login*.
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.
955248	SSL VPN does not work with local machine certificate-based tunnel when initiated from FortiTray.
955674	FortiClient (Windows) showing *IPsec VPN connection down* GUI notification while autoconnecting.
955887	SAML login VPN tunnel does not showing *Save Password* if using external browser for authentication.
956202	FortiClient (Windows) reaches a state where it cannot connect after updating a VPN tunnel without a certificate to have a certificate.
956729	Web Filter blocks FortiClient itself imitated URL when trying to connect to SSL VPN with SAML login.
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.

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.
947921	Vulnerability scan shows false positive for Adobe Acrobat 2020 v 20.005.30514.10514.
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.
811746	FortiClient sends duplicated and old logs to FortiAnalyzer.
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.
876810	FortiClient does not indicate VPN user in logs when connection succeeds.
948156	Excessive logging causes high I/O.
948887	FortiClient does not send Windows log of Exchange Server logon failure (Event ID 4625).

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.
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.
932019	*Bypass Private IP* does not work on Edge and Chrome.
939986	Web Filter blocks LUXTRUST middleware.
943046	FortiClient web access is blocked after EMS server firmware is rolled back from 7.0.9 to 7.0.8.

Bug ID	Description
943103	Web Filter prevents Slack from launching.
951738	FortiClient (Windows) throws JavaScript error when clicking *Launch FortiClient* in SSL VPN web portal.
951749	Web Filter incognito mode spams notification.
952715	FortiClient (Windows) blocks access to internal website after receiving EMS profile.

Avatar and social network login

Bug ID	Description
878050	FortiClient avatar does not update on FortiOS dashboards and FortiOS cannot show updated information.

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.

Bug ID	Description
874290	PowerShell with .NET framework 5, 6, or 7 does not work with TCP ZTNA.
885014	ZTNA fails to resolve FQDN destination hosts with certain domains.
913267	FortiClient (Windows) fails to export ZTNA web portal settings.
918045	FortiClient (Windows) requests ZTNA certificate when switching between user accounts.
919134	ZTNA works if `<disallow_invalid_server_certificate>` is enabled and server certificate is invalid.
919832	ZTNA stops working after days with the error message *No ZTNA client certificate was provided*.
926403	Ports list does not work in ZTNA TCP forwarding rule for scenario with EMS rule or scenario with portal, wildcard, and ports list.
943921	ZTNA is disabled but device keeps prompting for ZTNA certificate when accessing internal website.
949507	FortiClient (Windows) has ZTNA multiple client certificates in certificate store.
949701	FortiClient (Windows) has duplicate ZTNA Destinations when using EMS 7.2.1.
949999	SAML authentication does not work with Azure AD certificate-based authentication.
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.

FSSOMA

Bug ID	Description
900953	SSOMA does not send SSO sessions information to FortiAuthenticator.
909844	FSSO sessions drop earlier than expected.
935090	SSOMA stops sending SSO session information to FortiAuthenticator while service is running on host.

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, 943567	NETIO.SYS causes BSOD.
919017	FortiClient changes the checksum hash of the installer for Baramundi Management Agent.
942082	FortiClient causes Windows 10 BSOD ntoskrnl.exe when Cisco AnyConnect VPN is connected.
952737	FortiTray has high CPU usage.
955861	FortiClient (Windows) fails to send complete video to PAM if launching Windows-native application when maximum duration is reached.

FORTINET®

www.fortinet.com