Release Notes

FortiClient (Windows) 7.2.1

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

November 18, 2024
FortiClient (Windows) 7.2.1 Release Notes
04-721-904987-20241118

TABLE OF CONTENTS

Change log

Date	Change Description
2023-06-12	Initial release of 7.2.1.
2024-11-18	Added Common Vulnerabilities and Exposures on page 18.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 7.2.1 build 0779.

- What’s new in FortiClient (Windows) 7.2.1 on page 7
- Installation information on page 8
- Product integration and support on page 10
- Resolved issues on page 13
- Known issues on page 19

Review all sections prior to installing FortiClient.

FortiClient (Windows) 7.2.1 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 7.2.1 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.

What’s new in FortiClient (Windows) 7.2.1

For information about what's new in FortiClient (Windows) 7.2.1, 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_7.2.1.xxxx.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_7.2.1.xxxx.zip	Fortinet single sign on (FSSO)-only installer (32-bit).
FortiClientSSOSetup_7.2.1.xxxx_x64.zip	FSSO-only installer (64-bit).
FortiClientVPNSetup_7.2.1.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_7.2.1.xxxx_x64.exe	Free VPN-only installer (64-bit).

EMS 7.2.1 includes the FortiClient (Windows) 7.2.1 standard installer and zip package containing FortiClient.msi and language transforms.

The following tools and files are available in the FortiClientTools_7.2.xx.xxxx.zip file:

File	Description
OnlineInstaller	Installer files that install the latest FortiClient (Windows) version available.
SSLVPNcmdline	Command line SSL VPN client.
SupportUtils	Includes diagnostic, uninstallation, and reinstallation tools.
VPNAutomation	VPN automation tool.
VC_redist.x64.exe	Microsoft Visual C++ 2015 Redistributable Update (64-bit).
vc_redist.x86.exe	Microsoft Visual C++ 2015 Redistributable Update (86-bit).

The following files are available on FortiClient.com:

File	Description
FortiClientSetup_7.2.1.xxxx.zip	Standard installer package for Windows (32-bit).
FortiClientSetup_7.2.1.xxxx_x64.zip	Standard installer package for Windows (64-bit).

File	Description
FortiClientVPNSetup_ 7.2.1.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_ 7.2.1.xxxx_x64.exe	Free VPN-only installer (64-bit).

Review the following sections prior to installing FortiClient version 7.2.1: 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 7.2.1, do one of the following:

- Deploy FortiClient 7.2.1 as an upgrade from EMS. See Recommended upgrade path.
- Manually uninstall existing FortiClient version from the device, then install FortiClient (Windows) 7.2.1.

FortiClient (Windows) 7.2.1 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) 7.2.1 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 7.2.1 product integration and support information:

Desktop operating systems	• Microsoft Windows 11 (64-bit) • Microsoft Windows 10 (64-bit) • Microsoft Windows 7 (64-bit) FortiClient does not support zero trust network access (ZTNA) TCP forwarding on Windows 7.
Server operating systems	• Microsoft Windows Server 2022 • Microsoft Windows Server 2019 FortiClient 7.2.1 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) 7.2.1. 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 512 MB RAM • 600 MB free hard disk space • Native Microsoft TCP/IP communication protocol • Native Microsoft PPP dialer for dialup connections • Ethernet network interface controller (NIC) for network connections • Wireless adapter for wireless network connections • Adobe Acrobat Reader for viewing FortiClient documentation • Windows Installer MSI installer 3.0 or later
AV engine	• 6.00287
FortiAnalyzer	• 7.4.0 • 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 • 7.2.0 and later • 7.0.0 and later
FortiOS	The following FortiOS versions support ZTNA with FortiClient (Windows) 7.2.1. This includes both ZTNA access proxy and ZTNA tags: • 7.4.0 • 7.2.0 and later • 7.0.6 and later The following FortiOS versions support IPsec and SSL VPN with FortiClient (Windows) 7.2.1: • 7.4.0 • 7.2.0 and later • 7.0.0 and later • 6.4.0 and later • 6.2.0 and later • 6.0.0 and later
FortiSandbox	• 4.2.0 and later • 4.0.0 and later • 3.2.0 and later

Language support

The following table lists FortiClient language support information:

Language	GUI	XML configuration	Documentation
English	Yes	Yes	Yes
Chinese (simplified)	Yes		
Chinese (traditional)	Yes		
French (France)	Yes		
German	Yes		
Japanese	Yes		
Korean	Yes		
Portuguese (Brazil)	Yes		
Russian	Yes		
Spanish (Spain)	Yes		

The FortiClient language setting defaults to the regional language setting configured on the client workstation, unless configured in the XML configuration file.

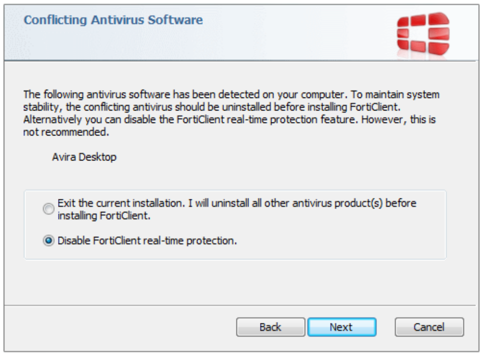
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

Conflicts with third party AV products

The 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 7.2.1 are as follows:

Version	Product code
Enterprise	{CA453742-0693-47F1-88AE-AE30C2A4B31F}
VPN-only agent	{846D8E6C-0CC1-4391-B86C-76CDD29F819B}
Private access management-only agent	{28D401F5-A375-42A9-B528-2CCFA45C12C5}
Single sign on-only agent	{80F9E9CD-7CE9-4E4B-84E7-C7AB5266407D}

See Configuring the FortiClient application in Intune.

Resolved issues

The following issues have been fixed in version 7.2.1. For inquiries about a particular bug, contact Customer Service & Support.

ZTNA connection rules

Bug ID	Description
847299	FortiClient does not support CIRA (default DNS over HTTPS provider) added to Firefox.
862921	FortiClient does not show prompt for zero trust network access (ZTNA) user authentication when form-based method is set under authentication rule/scheme on FortiGate.
870138	ZTNA certificate is not installed in personal store when only ZTNA component is installed.
871342	ZTNA error message that shows on browser is not configurable.
876254	FortiClient fails to delete portal configuration when EMS does not specify and overwrites EMS ZTNA configuration.
877128	User in different country cannot create ZTNA tunnel.
911024	Host keeps requesting new certificates after Windows login.

Web Filter and plugin

Bug ID	Description
826697	Web Filter feature affects ConnectWise automate application.
842966	Web Filter fails to activate when off-fabric.
859979	FortiClient blocks web browsing traffic that Web Filter allows.
868217	firefox_ext.xpi contains unexpected information that should be removed.
870895	Web Filter blocks Docker pull.
885310	When Web Filter blocks Youtube except for a video-specific URL, FortiClient (Windows) allows other videos.
892204	Web Filter blocks traffic for signing into http://login.qiye.ccpiteco.net and http://zwfw.safe.gov.cn/asone/
900083	User has problem accessing HTTP site after upgrading to FortiClient 7.0.8.
907534	FortiClient does not open page/window to enable *Allow in Incognito* option when clicking popup.

GUI

Bug ID	Description
853856	After FortiClient upgrade, Windows client is stuck at black screen.
875712	FortiClient console garbles username after reboot.

Endpoint control

Bug ID	Description
878514	FortiClient (Windows) cannot get tenant ID after deploying FortiClient 7.2.0 over 7.0.7 from EMS.
899960	FortiESNAC process stops after switching between two FortiSASE FortiClient Cloud instances.

FSSOMA

Bug ID	Description
803213	FSSO fails to send user login information, machine IP address, and other information to FortiAuthenticator.
851036	FortiClient (Windows) does not send IP address using mobility agent to FortiAuthenticator when on-premise.
854882	FortiClient single sign on mobility agent (FSSOMA) does not send EMS tenant ID to FortiAuthenticator.

Install and upgrade

Bug ID	Description
791538	EMS 7.0.3 deployments fail if *Require Password to Disconnect from EMS* is enabled.
816531	Signatures do not get updated.
868570	FortiESNAC.exe fails to run after EMS tries to deploy FortiClient (Windows) 7.2.0 to endpoint with interim build installed.
871718	FortiClient (Windows) with only antivirus (AV) and ZTNA features installed fails to sync profile.
872096	FortiClient is missing avatar and *Zero Trust Telemetry* pages after upgrading from free VPN-only client to full FortiClient (Windows).

Bug ID	Description
880132	FortiClient uninstall fails when using msiexec command.
892003	FortiClient allows user to install FortiClient (Windows) with two different installers at the same time on same machine.
907340	Reboot is required after reinstall for telemetry connection.

Vulnerability Scan

Bug ID	Description
853934	User cannot perform vulnerability scan when EMS enables it as scan option is disabled on GUI.

Remote Access

Bug ID	Description
763611	SSL VPN dual stack has slow upload speed.
792131	FortiClient has issues with the *Save Password* feature for SSL VPN profile.
801599	FortiClient opens multiple browser tabs when connecting to SSL VPN via SAML using external browser.
805880	SSLVPNcmdline does not work with SSL VPN connection.
825365	When disconnecting from VPN, FortiClient (Windows) does not restore the *Register this connection's IP to DNS* checkbox.
829084	*Redundant Sort Method* does not work with redundant SAML authentication.
835072	FortiClient blocks an internal application's activity to automatically open a saved HTML template.
840685	The VPN before logon icon does not appear in certain conditions.
842560	FortiClient disables PolicyAgent and IKEEXT services when connecting to dialup IPsec VPN.
847640	SSL VPN client certificate is missing on GUI when user enables SSO.
847990	Network adapter keeps DNS registration disabled after FortiClient disconnects from SSL VPN.
850822	FortiClient does not connect to IPsec VPN if multiple Diffie Hellman groups are selected.
852507	When connecting to SSL VPN using FortiSSLVPNclient.exe, the VPN adapter IP address is incorrect.
856798	When a BitLocker attached drive is locked, EMS reports endpoint as not having disk encryption.
867087	cxwmbclass.sys causes blue screen of death.

Bug ID	Description
868337	IPsec VPN client operating system is Windows 10, but FortiGate IKE debug log shows it as Windows 8.0.
871031	FortiClient (Windows) asks for answer instead of token when using third party multifactor authentication.
874144	FortiClient (Windows) uses client certificates and connects to SSL and IPsec VPN when the certificate filter is applied on the EMS.
874655	IPsec VPN connection fails and ends with unusable status.
876062	API connection does not work with certificate authentication.
877314	EMS-configured autoconnect does not have higher priority than a user's previously selected autoconnect.
877320	Autoconnect on install is not triggered if FortiClient is installed and registered to EMS during the same Windows logon session.
881633	FortiClient (Windows) cannot set two-byte character as VPN name.
884348	DTLS in SSL VPN does not work with SAML.
885541	SSL VPN does not connect when special characters are used in VPN password.
888878	Custom host check fail warning does not show entire notification.
890069	FortiClient (Windows) removes user credentials after reboot, hibernation or suspension.
890352	IPsec VPN for FIPS-enabled FortiClient fails to work when EMS-pushed IPsec or SSL VPN tunnel contains application split tunnel settings.
891164	FortiClient does not handle EMS-pushed IPsec VPN configuration of encryption/authentication/DH group that FortiClient FIPS does not support.
903336	FortiClient does not store SSL VPN connection username.
905346	IPsec VPN autoconnect works after tag or ZTNA tag rule changes.
909103	Toggling *Save Password* in GUI removes IPsec VPN tunnel saved username.
914957	`fortivpn::IEndpointControl::queryState nn_recv` fails.

Malware Protection and Sandbox

Bug ID	Description
833264	Antiexploit detection blocks Chrome without sharing payload details.
844962	FortiClient (Windows) does not block phone mobile storage when default removable media access is set to block.
861296	AV scan exclusion list does not work for shared/network drive files.
863950	FortiClient reports device as blocked but allows access to it.

Zero Trust telemetry

Bug ID	Description
841719	FortiClient does not connect to FortiClient Cloud.
886203	Telemetry is stuck in syncing state.

Avatar and social login information

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

License

Bug ID	Description
904835	FortiClient (Windows) loses license after upgrade.

Administration

Bug ID	Description
846036	FortiClient (Windows) does not send device fields when hostname changes.
869731	scheduler.exe crashes.
869845	Multiple FortiClient (Windows) daemon crashes occur.
909517	FortiESNAC daemon does not notify Fortitcs daemon after certificate update.

PAM

Bug ID	Description
866949	FortiShield blocks FortiPAM from writing files in FortiClient installation directory.
876170	FortiPAM does not work if ZTNA is disabled and client certificate is required.

Other

Bug ID	Description
861070	User can end FortiClient (Windows) processes when FortiShield is running.

Common Vulnerabilities and Exposures

Bug ID	Description
821860	FortiClient (Windows) 7.2.1 is no longer vulnerable to the following CVE References: • CVE-2023-37939 Visit https://fortiguard.com/psirt for more information.

Known issues

The following issues have been identified in FortiClient (Windows) 7.2.1. 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.
844997	FortiClient loses several packets on different internal resources after connecting telemetry.
853451	FortiClient blocks PIA VPN.
853808	FortiClient (Windows) blocks Veeam with messages related to Remote.CMD.Shell and VeeamAgent.exe.
860062	Application Firewall slows down opening of Microsoft Active Directory (AD) Users and Computers application.
749797	Application Firewall decreases network bandwidth while transferring files.
842534	After upgrade, Application Firewall blocks internal webpage.
869671	FortiClient (Windows) bypasses Application Firewall block after matching detection rule.
876265	Zip files become corrupt when Application Firewall is enabled.
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.
897207	Application Firewall blocks Microsoft 365 Defender device isolation.

Bug ID	Description
902866	Application Firewall does not block Google Drive.
907089	Application Firewall blocks MS.Windows.HTTP.Protocol.Stack.CVE-2022-21907.Code.Execution.

Configuration

Bug ID	Description
730415	FortiClient backs up configuration that is missing locally configured zero trust network access (ZTNA) connection rules.
897927	FortiClient causes reboot on domain controllers.

Endpoint control

Bug ID	Description
753151	Updating endpoint status from endpoint notified to deployed takes a long time.
804552	FortiClient shows all feature tabs without registering to EMS after upgrade.
815037	After administrator selects *Mark All Endpoints As Uninstalled*, FortiClient (Windows) connected with verified user changes to unverified user.
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.
827200	EMS displays no user for some devices.
833717	EMS shows endpoints as offline, while they show their own status as online.
834162	LDAP query for AD group check does not execute.
841764	EMS does not show third-party features in endpoint information.
855851	EMS remembered list shows FQDN duplicates.
868230	"Connection expiring due to FortiClient Connect license exceeded" error occurs.
879108	EMS considers the endpoint as on-Fabric when it does not meet all rules in an on-Fabric detection rule set.
880167	FortiClient cannot register with EMS due to selecting wrong interface to connect to EMS.
915074	FortiClient (Windows) cannot register to EMS using Azure LDAP invitation when application ID configured in Azure redirect URL are not all lower case letters.

Bug ID	Description
	Workaround: Ensure that application ID configured in Azure redirect URL only includes lower case letters.
921937	FortiClient cannot register to EMS using *Register to EMS* button in invitation email.

Endpoint management

Bug ID	Description
786738	*Anti-Ransomware Events* tab is visible after disabling the feature from *Feature Select*.
904348	FortiClient (Windows) and EMS detect encryption status as not enabled when only one hard disk has encryption (Bitlocker) enabled.
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.

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.
893883	FortiClient opens infinite loop of browser and Command Prompt windows when certain profile combination is used.
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.
783690	Reboot prompt does not display after user login.
870370	Upgrading FortiClient from FortiClient Cloud uses expired invitation code to register.
896152	FortiClient shows *"Update failed - Error occurred!"* popup after reboot.
898429	Deployment reboot prompt in Windows 11 does not work.
905132	FSSO fails to upgrade from 7.2.0 to 7.2.1 with installer that FortiClientSSOConfigurationTool created.
915493	Reboot popup does not show to user.

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.
837638	Identifying malware and exploits using signatures received from FortiSandbox does not work.
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.
875930	FortiClient (Windows) fails to quarantine a specific malware-infected dll file in Exchange Server.
876465	FortiClient does not detect virus in network drive.
876925	Antiexploit protection blocks Microsoft signing application in Chrome.
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.

Bug ID	Description
901065	Logitech driver breaks after installing FortiClient with Malware Protection feature enabled in installer.
903614	Number of blocked exploit counts does not match between FortiClient (Windows) and EMS.
907331	User cannot create exception for NetSupport Manager.
913701	Antiransomware feature fails to decrypt MSIL/Filecoder.AKJ!tr.ransom.
915300	FortiClient (Windows) detects file configured as exception as malware.
916958	FortiClient cannot detect a virus-infected file.
917941	Sandbox exclusions do not work for shared drives.
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.

PAM

Bug ID	Description
912655	FortiPAM secret launchers do not launch correctly when accessing FortiPAM via external DNAT.
922734	Proxy is enabled but RDP traffic does not go through ZTNA tunnel in privilege access management standalone agent.
922764	Launching WebApp with Edge for use case where video recording and proxy are enabled does not work.

Quarantine management

Bug ID	Description
894510	Quarantine management with EMS 7.2 and FortiClient does not work.
896689	After upgrade, FortiClient (Windows) does not restore quarantined file after it is allowlisted.

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.
793033	ZTNA LDAP group rule does not work.
919595	ZTNA tag rule does not working for BitLocker disk encryption.
872794	AD group tag *Evaluate on FortiClient* feature does not work. If the Windows login user is a local user while the FortiClient onboarding user is a domain user, FortiClient behaves differently for the AD group tag based on the *Evaluate on FortiClient* setting. The AD group tag is applied if EMS does the evaluation and not applied if FortiClient (Windows) does the evaluation.

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
911495	FortiClient (Windows) fails to autoregister to FortiClient Cloud due to Telemetry key mismatch.

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.

Bug ID	Description
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.
800934	DH group settings are not read-only for tunnel that EMS pushed to FortiClient (Windows).
801747	XML tag `<block_outside_dns>` is not per-tunnel .
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.
838231	Users fail to connect when using SAML authentication with SSL VPN.
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.
851093	IPv6 DNS requests do not work.
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.
855836	EMS remote VPN is visible when on-fabric when it should be hidden.
858696	FortiClient cannot connect to SSL VPN with SAML via Satelite ISP.
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.

Bug ID	Description
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.
871153	FortiClient (Windows) tries to reuse the same saved password for other VPN connections even if they have *Save Password* disabled.
871346	FortiClient (Windows) cannot remember username and password for tunnel with SAML login with built-in browser, FortiAuthenticator, and *Save Password* and autoconnect selected.
871374	VPN tunnel with SAML login does not warn user when opening multiple connections with *Limit Users to One SSL-VPN Connection at a Time* enabled.
872315	IPsec VPN resiliency based on ping response does not work.
872339	Per-user autoconnect does not work after restarting FortiClient.
874208	FortiClient (Windows) cannot dial up SSL VPN tunnel with ECDSA certificate.
874298	Always up does not work for SAML SSL VPN tunnel with single FQDN resolved to multiple IP addresses.
874310	Using closest gateway based on ping speed and TCP round trip does not work for SSL VPN resilience if using different ports for the remote gateways.
874669	FortiClient does not attempt to connect with redundant SAML VPN gateway if it cannot reach first gateway.
874759	SSL VPN has DNS issues if AWS Route53 is configured for name resolution.
875631	Dialup IPsec VPN does not allow multiple valid server certificates for client use simultaneously.
875999	FortiClient does not show GUI prompt to enter PIN for SSL VPN certificate stored on USB PKI/SmartCard device.
876429	FortiClient (Windows) ignores `redundant_sort_method=0` configuration option for IPsec VPN IKEv2 tunnel using multiple VPN gateways.
876643	Connecting to an IKEv2 tunnel with EAP disabled from FortiTray with certificate only does not work.
877640	If FortiClient is registered to EMS, IPsec VPN tunnel fails to connect when it is configured to connect on OS start.
878070	After device wakes from sleep, FortiClient intermittently grays out SAML button.
878652	VPN secure remote access notification prompt displays multiple times with cutoff text.

Bug ID	Description
881278	FortiClient (Windows) does not save the username for IPsec VPN with client certificate and XAuth enabled.
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.
886928	VPN before logon displays FortiClient (Windows) credentials prompt if user@domain.local format is used for username.
887631	Using closest gateway based on TCP round trip for IPsec VPN resilience does not work if ping is disabled for first gateway.
891202	Autoconnect only when off-fabric does not work properly with user account and multifactor authentication (MFA) (FortiToken) for XAuth.
892314	On-connect script does not execute .
893237	FortiClient (Windows) does not provide opportunity to reinput password during autoconnect after identity provider password change.
893677	Autoconnect and always-up do not work when two gateways are configured for SAML SSL VPN with *Redundancy Sort Method*.
893958	FortiClient (Windows) logs include `auto-connect is not supported in this session (CREDENTIALPROVIDER)` error.
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.
906617	SSL VPN with certificate and token do not work as expected when connecting from tray icon in Windows 10 x64.
907361	IPsec VPN IKE v1 and v2 block IPv6 do not work when enabled.
907518	FortiClient connects to VPN without proper remote secure access tag.
909145	Secure remote access tunnel default host tag message for prohibited connection is empty.
909573	With MFA and autoconnect enabled, user account password becomes empty after logging in to Windows.

Bug ID	Description
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.
912255	SSL VPN stays connected when there is no network connection to the VPN gateway when DTLS is enabled.
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.

Vulnerability Scan

Bug ID	Description
849485	FortiClient wrongly detects AnyDesk vulnerabilities CVE-2021-44426 and CVE-2021-44425.
869253	FortiClient (Windows) detects vulnerability when the required KB is installed.

Logs

Bug ID	Description
811746	FortiClient sends duplicated and old logs to FortiAnalyzer.
849043	SSL VPN add/close action does not show on FortiGate *Endpoint Event* section.

Bug ID	Description
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.

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.
867483	Web Filter does not give warning message.
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.
915287	Extension does not properly apply safe mode HTTP header restrictions.
919419	When Web Filter with FortiGuard Anycast *Allow websites when rating error occurs* is set to *Block*, blocked message should not spam FortiClient (Windows) notifications.

Avatar and social network login

Bug ID	Description
830117	EMS fails to update email address for endpoint from personal information form in FortiClient (Windows).

Bug ID	Description
878050	FortiClient avatar does not update on FortiOS dashboards and FortiOS cannot show updated information.
922816	FortiClient fails to show avatar after user login with Google, LinkedIn, or Salesforce.

License

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

ZTNA connection rules

Bug ID	Description
814953	Using an external browser for SSH ZTNA requires restarting FortiClient on Windows 11.
831943	ZTNA client certificate is not removed from user certificate store after FortiClient uninstall.
836246	Going from off-Fabric to on-Fabric does not stop the ZTNA service and keeps endpoint from connecting.
839589	ZTNA TCP forwarding not working for GoAnywhere application.
857909	FortiClient (Windows) does not support enabling encryption for ZTNA TCP forwarding rules acquired from ZTNA service portal.
857999	FortiClient does not support use of external browser for SAML authentication for ZTNA rules acquired through service portal.
872153	Old certificate is not deleted when FortiClient is uninstalled or upgraded.
874290	PowerShell with .NET framework 5, 6, or 7 does not work with TCP ZTNA.
875254	FortiClient cannot finish ZTNA TCP forwarding TFA authentication when *Use external browser...* is disabled.
913267	FortiClient (Windows) fails to export ZTNA web portal settings.
914111	ZTNA daemon fortitcs stops updating its log file after running for some time.
918045	FortiClient (Windows) requests ZTNA certificate when switching between user accounts.
918501	ZTNA TCP forwarding (RDP) does not work if encryption is enabled and LDAP is used for authentication.
919134	ZTNA works if `<disallow_invalid_server_certificate>` is enabled and server certificate is invalid.

Bug ID	Description
919832	ZTNA stops working after days with the error message *No ZTNA client certificate was provided*.

FSSOMA

Bug ID	Description
862021	Local account can access Internet if FortiClient SSOMA logged-in AD user locks the screen.
893985	FortiClient SSOMA creates issue with tenant ID on FortiAuthenticator in regular/normal AD.
900953	SSOMA does not send SSO sessions information to FortiAuthenticator.
909844	FSSO sessions drop earlier than expected.

Onboarding

Bug ID	Description
811976	FortiClient (Windows) may prioritize using user information from authentication user registered to EMS.
819989	FortiClient (Windows) does not show login prompt when installed with installer using LDAP/local verification.
872136	User verification period option does not work as configured.

Other

Bug ID	Description
834389	FortiClient has incompatibility with Fuji Nexim software.
874474	`update_task` does not start as scheduled and ISDB signature is not updated.
896137	DesktipID app does not working after installing FortiClient.
897741	Virus cleaner does not scan PC.
900691	FortiClient on Windows Server 2019 shows blue screen of death (BSOD) when copying files to/from Citrix Share.
901972	NETIO.SYS causes BSOD.
907006	FortiClient console closes automatically when FIPS is enabled through CLI or EMS-created

Bug ID	Description
	installer.
919017	FortiClient changes the checksum hash of the installer for Baramundi Management Agent.

www.fortinet.com