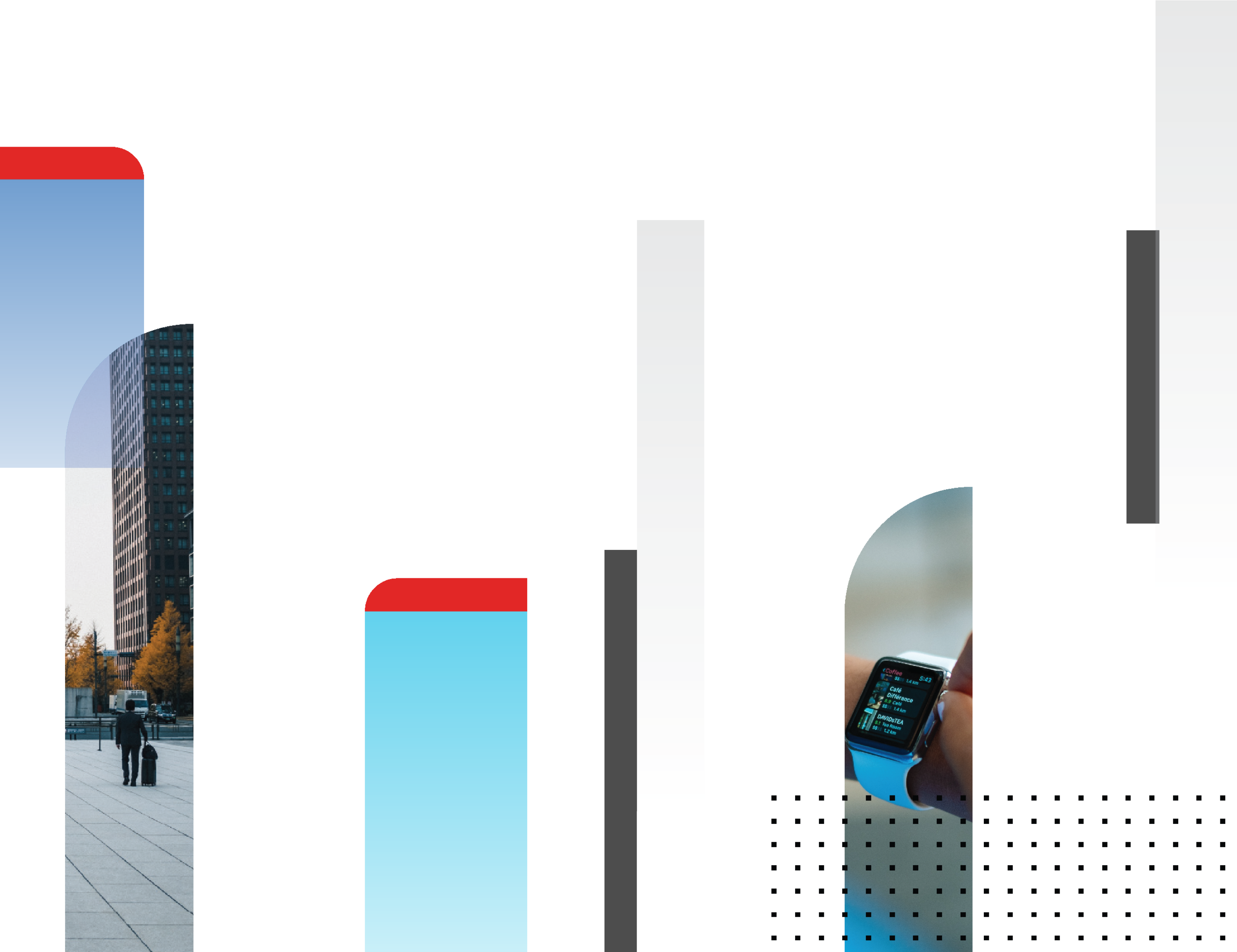
Release Notes

FortiClient (Windows) 7.0.7



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

September 21, 2022
FortiClient (Windows) 7.0.7 Release Notes
04-707-832531-20220921

TABLE OF CONTENTS

Change log

Date	Change Description
2022-08-31	Initial release of 7.0.7.
2022-09-21	Updated Product integration and support on page 9.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 7.0.7 build 0345.

- Installation information on page 7
- Product integration and support on page 9
- Resolved issues on page 12
- Known issues on page 16

Review all sections prior to installing FortiClient.

FortiClient (Windows) 7.0.7 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 7.0.7 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.

Installation information

Firmware images and tools

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

File	Description
FortiClientTools_7.0.7.xxxx.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_7.0.7.xxxx.zip	Fortinet single sign on (FSSO)-only installer (32-bit).
FortiClientSSOSetup_7.0.7.xxxx_x64.zip	FSSO-only installer (64-bit).
FortiClientVPNSetup_7.0.7.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_7.0.7.xxxx_x64.exe	Free VPN-only installer (64-bit).

EMS 7.0.7 includes the FortiClient (Windows) 7.0.7 standard installer and zip package containing FortiClient.msi and language transforms.

The following tools and files are available in the FortiClientTools_7.0.xx.xxxx.zip file:

File	Description
FortiClientVirusCleaner	Virus cleaner.
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_7.0.7.xxxx.zip	Standard installer package for Windows (32-bit).
FortiClientSetup_7.0.7.xxxx_x64.zip	Standard installer package for Windows (64-bit).

File	Description
FortiClientVPNSetup_ 7.0.7.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_ 7.0.7.xxxx_x64.exe	Free VPN-only installer (64-bit).

Review the following sections prior to installing FortiClient version 7.0.7: Introduction on page 6 and Product integration and support on page 9.

Upgrading from previous FortiClient versions

To upgrade a previous FortiClient version to FortiClient 7.0.7, do one of the following:

- Deploy FortiClient 7.0.7 as an upgrade from EMS. With the endpoint security improvement feature, there are backward compatibility issues to consider while planning upgrades. See Recommended upgrade path.
- Manually uninstall existing FortiClient version from the device, then install FortiClient (Windows) 7.0.7.

FortiClient (Windows) 7.0.7 features are only enabled when connected to EMS 7.0.

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

You must be running EMS 7.0.2 or later before upgrading FortiClient.

Downgrading to previous versions

FortiClient (Windows) 7.0.7 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 7.0.7 product integration and support information:

Desktop operating systems	• Microsoft Windows 11 (64-bit) • Microsoft Windows 10 (32-bit and 64-bit) • Microsoft Windows 8.1 (32-bit and 64-bit) • Microsoft Windows 7 (32-bit and 64-bit) FortiClient 7.0.7 does not support Microsoft Windows XP and Microsoft Windows Vista. 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 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 FortiClient 7.0.7 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 2016 and 2019 support ZTNA with FortiClient (Windows) 7.0.7. 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.
Embedded system operating systems	Microsoft Windows 10 IoT Enterprise LTSC 2019
Minimum system requirements	• Microsoft Windows-compatible computer with Intel processor or equivalent. FortiClient (Windows) does not support ARM-based processors. • Compatible operating system and minimum 512 MB RAM • 600 MB free hard disk space • Native Microsoft TCP/IP communication protocol • Native Microsoft PPP dialer for dialup connections • Ethernet network interface controller (NIC) for network connections • Wireless adapter for wireless network connections • Adobe Acrobat Reader for viewing FortiClient documentation • Windows Installer MSI installer 3.0 or later
AV engine	• 6.00266
FortiAnalyzer	• 7.0.0 and later

	When using FortiClient with FortiAnalyzer, you should upgrade both to their latest versions. The versions between the two products should match. For example, if using FortiAnalyzer 7.0.5, use FortiClient 7.0.5.
FortiAuthenticator	• 6.4.0 and later • 6.3.0 and later • 6.2.0 and later • 6.1.0 and later • 6.0.0 and later
FortiClient EMS	• 7.0.0 and later
FortiManager	• 7.0.0 and later
FortiOS	The following FortiOS versions support ZTNA with FortiClient (Windows) 7.0.7. This includes both ZTNA access proxy and ZTNA tags: • 7.0.6 and later The following FortiOS versions support IPsec and SSL VPN with FortiClient (Windows) 7.0.7: • 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 • 3.1.0 and later • 3.0.0 and later • 2.5.0 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		

Language	GUI	XML configuration	Documentation
Russian	Yes		
Spanish (Spain)	Yes		

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

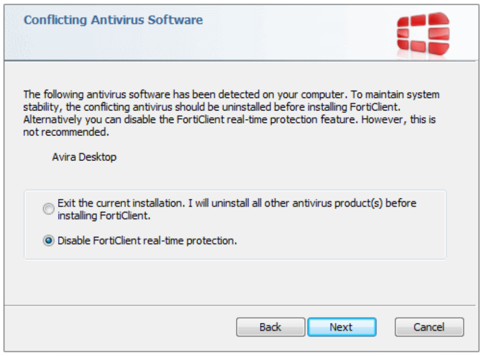
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

Conflicts with third party AV products

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

- Do not use FortiClient's AV feature with other AV products.
- If not using FortiClient's AV feature, exclude the FortiClient installation folder from scanning for the third party AV product.

During a new FortiClient installation, the installer searches for other registered third party software and, if it finds any, warns users to uninstall them before proceeding with the installation. There is also an option to disable FortiClient real time protection.


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 code

Deploying FortiClient with Intune requires a product code. The product code for FortiClient 7.0.7 is {17748981-CA57-4D18-8B08-5685F656221D}.

See Configuring the FortiClient application in Intune.

Resolved issues

The following issues have been fixed in version 7.0.7. For inquiries about a particular bug, contact Customer Service & Support.

Web Filter and plugin

Bug ID	Description
784677	Web Filter plugin blocks YouTube comments with *Restricted Mode has hidden comments for this video* message.
793017	Web Filter disconnects application's underlying connection.
804938	All Internet traffic stops when user connects a USB controller (RNDIS).
812879	Web Filter blocks Chocolatey installation.
813034	FortiTray keeps notifying user to install Web Filter plugin when Chrome has installed the plugin.
823469	Console does not show security risk category as configured on EMS in Web Filter profile when antivirus is enabled.
823477	Web Filter fails to block security risk category URLs when antivirus is enabled.

GUI

Bug ID	Description
773355	FortiClient has display issue with umlauts on the Web Filter tab.
798526	Vulnerability Scan has typo in Spanish.
828339	GUI returns blank page after install.

Endpoint control

Bug ID	Description
777473	FortiClient Cloud is unaware of UID change when it sends a new UID to FortiClient.
821820	FortiClient loses connection from FortiClient Cloud.

Bug ID	Description
823386	FortiClient fails to send correct public IP address to EMS if registered to EMS as a SAML onboarding user.

Install and upgrade

Bug ID	Description
726616	FortiClient (Windows) 6.4.3 cannot upgrade to 6.4.4.

Zero Trust tags

Bug ID	Description
821391	User in Active Directory group zero trust tag does not tag users in security groups.

Remote Access

Bug ID	Description
742279	FortiClient to FortiGate SSL VPN gets stuck during connection with SAML.
776329	IPsec VPN connection from tray fails to launch IPsec VPN service with certificate and ping-based redundant sort method.
801599	FortiClient opens multiple browser tabs when connecting to SSL VPN via SAML using external browser.
802323	VPN before login fails to connect with host check rule configured immediately after reboot.
802809	Routes are missing when using DHCP over IPsec VPN.
807258	VMware Horizon client does not work with application-based split tunnel.
812898	SSL VPN autoconnect does not work and results in IPsec VPN errors.
821395	SAML SSL VPN and autoconnect when off-fabric does not reconnect.
821994	VPN does not disconnect if administrator deregisters FortiClient from the FortiSASE portal GUI.
827612	update_task.exe execution window pops up while connecting to SSL VPN.
830067	Connecting to IPsec VPN displays *Update failed - Error occurred!* error.
832036	VPN autoconnect does not always work with special Azure AD build.

Bug ID	Description
834874	Autoconnect does not work after restart when the Remote Access profile only has an IPsec VPN tunnel and the SSL VPN option disabled.

Malware Protection and Sandbox

Bug ID	Description
784306	FortiClient causes blue screen of death (BSOD) when ACR1281 card reader is plugged in.
820511	Promethean ActivBoard does not work with FortiClient.

Avatar and social login information

Bug ID	Description
729140	FortiClient (Windows) fails to allow login with Google, LinkedIn, or Salesforce.
825913	FortiClient (Windows) reports system user changes to EMS inconsistently.

Endpoint management

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

Logs

Bug ID	Description
713287	FortiClient (Windows) does not generate local logs for ZTNA.

Administration

Bug ID	Description
798055	JavaScript error occurs in the main process

Performance

Bug ID	Description
676424	NETIO.SYS causes BSOD.
827743	Corporate endpoints experience BSOD after FortiClient installation. Non-corporate endpoints do not experience BSOD.

ZTNA connection rules

Bug ID	Description
823012	Zero trust network access (ZTNA) TCP forwarding fails to work when FortiClient console is closed.

Common Vulnerabilities and Exposures

Bug ID	Description
820903	FortiClient (Windows) 7.0.7 is no longer vulnerable to the following CVE References: • CVE-2022-33877 Visit https://fortiguard.com/psirt for more information.

Known issues

The following issues have been identified in FortiClient (Windows) 7.0.7. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Install and upgrade

Bug ID	Description
749331	Windows Security setting in Windows displays *FortiClient is snoozed* when FortiEDR is installed.
769639	FortiDeviceGuard is not installed on Windows Server 2022.
820672	ZTNA driver FortiTransCtrl.sys fails to start up on Windows Server 2016.

Application Firewall

Bug ID	Description
717628	Application Firewall causes issues with Motorola RMS high availability client.
776007	Application Firewall conflict with Windows firewall causes issues updating domain group policies.
814391	FortiClient Cloud application signatures block allowlisted applications.
817932	Application Firewall fails to allow application signatures added under Application Overrides as allow.
823292	FortiClient cannot connect to JVC wireless display.
827788	Threat ID is 0 on Firewall Events.

GUI

Bug ID	Description
767998	Free VPN-only client includes *Action for invalid EMS certificate* in settings.
811742	FortiClient (Windows) does not hide software update options when registered to EMS (regression).
826895	FortiClient ignores the listing order of the configured VPN connections in the GUI and tray.

Bug ID	Description
827394	FortiClient does not report profile change update in *Notifications*.

Zero Trust tags

Bug ID	Description
704234	Zero Trust tagging rule set syntax does not check registry key values.
782394	ZTNA user identity tags do not work.
819120	Zero trust tag rule for Active Directory group does not work when registering FortiClient to EMS with onboarding user.
831981	On-Fabric detection rule for local IP address/subnet) fails to identify secondary Ethernet adapter IPv4 address.

Endpoint control

Bug ID	Description
753151	Updating endpoint status from endpoint notified to deployed takes a long time.
765686	When autoconnect only when offnet is enabled, VPN autoconnects when endpoint shifts from off-Fabric to on-Fabric.
798090	FortiClient (Windows) incorrectly recognizes on-fabric status.
804552	FortiClient shows all feature tabs without registering to EMS after upgrade.
808880	FortiClient fails to synchronize with EMS on Windows 7 x86 platform for long time.
815037	After administrator selects *Mark All Endpoints As Uninstalled*, FortiClient (Windows) connected with verified user changes to unverified user.
815384	FortiClient (Windows) delays starting Web Filter service after status is off-fabric.
816751	Administrator cannot restore a quarantined file through EMS quarantine management if FortiClient (Windows) registered as onboarding user.
817061	Redeploying from another EMS server causes FortiClient (Windows) to not reconnect to EMS automatically.
819552	After upgrading FortiClient with EMS local onboarding user with LDAP, FortiClient (Windows) prompts for registration authentication.
821024	FortiClient fails to send username to EMS, causing EMS to report it as different users.
827200	EMS displays no user for some devices.

Bug ID	Description
833717	EMS shows endpoints as offline, while they show their own status as online.
833848	FortiClient reports incorrect Windows version to EMS.
834162	LDAP query for Active Directory group check does not execute.
836239	FortiClient does not update off-Fabric features automatically.

Endpoint management

Bug ID	Description
760816	Group assignment rules based on IP addresses do not work when using split tunnel.

Configuration

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

Endpoint policy and profile

Bug ID	Description
774890	FortiClient (Windows) does not receive updated profile after syncing imported Web Filter profile from EMS.

Performance

Bug ID	Description
749348	Performance issues after upgrade.
778651	Large downloads and speed tests result in high latency, packet loss, and poor performance.

Zero Trust Telemetry

Bug ID	Description
683542	FortiClient (Windows) fails to register to EMS if registration key contains a special character: " !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~".
792703	FortiClient (Windows) cannot connect to FortiClient Cloud.
837859	FortiClient does not use invitation code to register after upgrade.

Malware Protection and Sandbox

Bug ID	Description
606634	FortiClient fails to remove quarantined files after number of days configured with cullage option.
650383	Number of blocked exploits attempts does not work properly.
730054	*Allow Admin Users to Terminate Scheduled and On-Demand Scans from FortiClient Console* feature does not work as expected.
760073	FortiClient (Windows) compatibility with USB.
762125	fortimon3.sys causes blue screen of death during Slack calls.
777582	Antiransomware kills FCBLog.exe when exporting debug logs.
793926	FortiShield blocks spoolsv.exe on Citrix virtual machine servers.
820098	Sandbox does not release blocked file.
825732	SIM-card-slot UEFI feature slows down Windows logon when connected to VPN.
828862	FortiClient does not allow virtual CD-ROM device.
831560	GUI shows ransomware quarantined files after restoration via EMS.

Remote Access

Bug ID	Description
727695	FortiClient (Windows) on Windows 10 fails to block SSL VPN when it has a prohibit host tag applied.
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.

Bug ID	Description
730756	For SSL VPN dual stack, GUI only shows IPv4 address.
736353	Multigateway failover does not go back to check previous gateways when failing over to see if they are up.
743106	IPsec VPN XAuth does not work with ECDSA certificates.
744544	FortiClient (Windows) always saves SAML credentials.
744597	SSL VPN disconnects and returns hostcheck timeout after 15 to 20 minutes of connection.
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.
755482	Free VPN-only client does not show token box on rekey and GUI open.
758424	Certificate works for IPsec VPN tunnel if put it in current user store but fails to work if in local machine.
762986	FortiClient (Windows) does not use second FortiGate to connect to resilient tunnel from FortiTray if it cannot reach first remote gateway.
764863	Dialup IPsec VPN over IPv6 drops packets on inbound direction once FortiClient (Windows) establishes tunnel.
767947	SMS verification code/answer code overwrites IPsec VPN saved password.
772108	When `no_dns_registration=1`,*Register This Connection's Address in DNS* of NW IP properties is not selected after VPN is up.
773060	When connected to VPN on wireless connection, Surface Pro cannot access SSRS report (software hosted on internal server).
775633	Priority based IPSec resiliency tunnel, auto failover to second remote gateway doesn't work
789821	IPsec VPN failover to SSL VPN does not work when remote gateway is unreachable due to an invalid FQDN.
790021	Multifactor authentication using Okta with email notification does not work.
792131	FortiClient (Windows) users report issues with the *Save Password* feature for SSL VPN.
793893	FortiClient search domains transfer incorrectly to endpoints.
794110	VPN before logon does not work with Okta multifactor authentication and enforcing acceptance of the disclaimer message.
795334	Always up feature does not work as expected when trying to connect to VPN from tray.
797816	SAML connection with external browser authentication and single sign on port 8020 is busy, with FortiClient returning a JavaScript error.
800453	SSL VPN with certificate authentication fails to connect on OS start.
801674	SAML internal browser authentication prompt does not show up when redirection to external browser is disabled.

Bug ID	Description
801875	FortiClient cannot connect to VPN when there are two gateways listed using SAML.
802957	Dialup IPsec VPN does not come up and shows NAT-T inconsistency.
811458	FortiClient (Windows) cannot connect to SSL VPN after installing Windows update KB5013942.
814488	SSL VPN with `<on_os_start_connect>` enabled does not work when the machine is put into sleep mode and changes networks.
815528	If `allow_local_lan=0` and per-application split tunnel with exclude mode and full tunnel are configured, FortiClient (Windows) should block local RDP/HTTPS traffic.
816826	FortiClient (Windows) has issue with SAML with *ErrorCode=-6005* when it reaches 31%.
818155	FortiClient (Windows) sends SAML response to a different IP address than the request it received from.
821879	VPN autoconnect does not work with IKEv2 IPsec VPN and user certificates.
822763	Remote access *Connect* button does not work.
823350	Autoconnect works intermittently.
824298	SSL VPN with certificates cannot connect to VPN on Elitebook 850 G5/Elitebook 850 G3 laptops.
825365	Disconnecting from VPN does not restore *Register this connection's IP to DNS*.
825442	ZScaler Client Connector does not work with application-based split tunnel.
826170	FortiClient removes the SSL VPN password from the GUI if the network interface is disconnected and reconnected.
829763	With host check enabled, SAML login does not show proper warning message when it fails to connect.
830899	FortiClient (Windows) becomes unlicensed when connected to SSL VPN.
830944	SAML SSL VPN fails when Duo is the multifactor authentication provider.
834604	Upgrading FortiClient (Windows) free VPN-only client to the latest build removes VPN tunnels.
834883	On-fabric rule for VPN tunnel name does not work when the tunnel name uses special characters.
835042	After upgrading FortiClient (Windows), OpenVPN connection fails while FortiClient (Windows) VPN runs with application-based split tunnel enabled.
835436	FortiClient (Windows) does not save or reuse SAML credentials and shows credentials prompt when VPN autoconnects.
836148	FortiClient does not try to connect to the realm https://X.Y:10443/Z if X and Z have the same name.
837479	FortiClient ignores secure remote access feature if used with VPN before logon.
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.
838380	FortiClient removes autoconnect VPN tunnel user credentials after a couple system restarts.

Vulnerability Scan

Bug ID	Description
741241	FortiClient (Windows) finds vulnerabilities for uninstalled software.
795393	EMS does not remove vulnerability events after successful patch.
811796	FortiClient (Windows) does not exclude Python vulnerability for all applications from vulnerability compliance check.

Logs

Bug ID	Description
820067	FortiClient forwards logs despite being completely disabled.

Web Filter and plugin

Bug ID	Description
776089	FortiClient (Windows) does not block malicious sites when Web Filter is disabled.
812207	Blocked web client shows dropped connection message instead of URL blocked message.
825633	Error revokes certificate accessing outlook.office365.com using Web Filter.
826697	Web Filter affects ConnectWise Automate.
829164	Security risk websites violation list is not on Web Filter tab.
829674	Web Filter does not work with *Only when endpoint is off-fabric* option.
833506	FortiClient (Windows) registry does not update restriction level value when Web Filter is disabled and reenabled.
834135	FortiClient does not remove Web Filter plugin from browser when Web Filter is disabled.
834751	Registry policy value fails to update to new value if Web Filter plugin is enabled on EMS.

Avatar and social network login

Bug ID	Description
802471	`<enable_manually_entering>` parameter does not work.

Bug ID	Description
805153	FortiClient (Windows) does not save user-specified *Submit User Identity Information*.
830117	EMS fails to update email address for endpoint from personal information form in FortiClient (Windows).
831366	EMS does not show correct username if user logs in with Google or Linkedin cloud service or chooses user input.

Multitenancy

Bug ID	Description
780308	EMS automatically migrates endpoints to default site.

ZTNA connection rules

Bug ID	Description
735494	Windows 7 does not support TCP forwarding feature.
773956	FortiClient (Windows) cannot show normal webpage of Internet real server (Dropbox) with ZTNA.
814953	Using an external browser for SSH ZTNA requires restarting FortiClient on Windows 11.
830135	Hosts file becomes empty after disconnecting/reconnecting to EMS multiple times and with fresh install of FortiClient (Windows).
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.

Onboarding

Bug ID	Description
766311	FortiClient (Windows) does not send Windows user information to EMS after user account switching.
811976	FortiClient (Windows) may prioritize using user information from authentication user registered to EMS.
819989	FortiClient (Windows) does not show login prompt when installed with installer using LDAP/local verification.

Other

Bug ID	Description
780651	FortiClient (Windows) does not update signatures on expected schedule.
812778	FortiShield fails to prevent user from killing FortiClient running processes.

www.fortinet.com