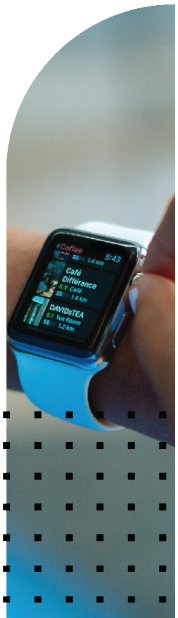
Release Notes

FortiClient (Windows) 7.0.12



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

April 04, 2024
FortiClient (Windows) 7.0.12 Release Notes
04-7012-1012260-20240404

TABLE OF CONTENTS

Change log

Date	Change description
2024-04-04	Initial release of 7.0.12.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 7.0.12 build 0572.

Review all sections prior to installing FortiClient.

FortiClient (Windows) 7.0.12 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 7.0.12 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
Chrome_Extension_Debug.7.0.12.0572.zip	Web Filter extension build for Google Chrome, unminified and minified.
Chrome_Extension_Release.7.0.12.0572.zip	
Edge_Extension_Debug.7.0.12.0572.zip	Web Filter extension build for Microsoft Edge, unminified and minified.
Edge_Extension_Release.7.0.12.0572.zip	
fct_log_def_7.0.12.0572.xml	Log definition file.
Firefox_Extension_Debug.7.0.12.0572.zip	Web Filter extension build for Mozilla Firefox, unminified and minified.
Firefox_Extension_Release.7.0.12.0572.zip	
FortiClientOnlineInstaller_7.0.12.0572.exe	Minimal installer for 32-bit and 64-bit Windows.
FortiClientSetup_7.0.12.0572.zip	Zip package containing FortiClient.msi and language transforms for 32-bit Windows.
FortiClientSetup_7.0.12.0572_x64.zip	Zip package containing FortiClient.msi and language transforms for 64-bit Windows.
FortiClientSSOConfigurationTool_7.0.12.0572.zip	Zip package containing FortiClient single sign on (FSSO) configurator tool.
FortiClientSSOSetup_7.0.12.0572.zip	FSSO-only installer (32-bit).
FortiClientSSOSetup_7.0.12.0572_x64.zip	FSSO-only installer (64-bit).
FortiClientTools_7.0.12.0572.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientV5SHA256_build0572.sum	SHA256 hashes for files in the image file folder.
FortiClientVPNOnlineInstaller_7.0.12.0572.exe	Minimal FortiClientVPN installer for 32-bit and 64-bit Windows.
FortiClientVPNSetup_7.0.12.0572.exe	Free VPN-only installer (32-bit)
FortiClientVPNSetup_7.0.12.0572.zip	
FortiClientVPNSetup_7.0.12.0572_x64.exe	Free VPN-only installer (64-bit)
FortiClientVPNSetup_7.0.12.0572_x64.zip	

File	Description
md5sum.txt	MD5 hashes for files in the image file folder.
Readme_1st.txt	Read me file that explains files available in the image file folder.
sha512sum.txt	SHA5 hashes for files in the image file folder.

EMS 7.0.12 includes the FortiClient (Windows) 7.0.12 standard installer and zip package containing FortiClient.msi and language transforms.

The following tools and files are available in the FortiClientTools_7.0.12.0572.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.
VC_redist.x64.exe	Microsoft Visual C++ 2015 Redistributable Update (64-bit).
vc_redist.x86.exe	Microsoft Visual C++ 2015 Redistributable Update (86-bit).
VPNAutomation	VPN automation tool.

The following files are available on FortiClient.com:

File	Description
FortiClientSetup_7.0.12.0572.zip	Standard installer package for Windows (32-bit).
FortiClientSetup_7.0.12.0572_x64.zip	Standard installer package for Windows (64-bit).
FortiClientVPNSetup_7.0.12.0572.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_7.0.12.0572_x64.exe	Free VPN-only installer (64-bit).

Review the following sections prior to installing FortiClient version 7.0.12: 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 7.0.12, do one of the following:

- Deploy FortiClient 7.0.12 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) 7.0.12.

FortiClient (Windows) 7.0.12 features are only enabled when connected to EMS 7.0 or 7.2.

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) 7.0.12 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 7.0.12 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)
Server operating systems	• Microsoft Windows Server 2022 • Microsoft Windows Server 2019 FortiClient 7.0.12 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 and 2022 support zero trust network access (ZTNA) with FortiClient (Windows) 7.0.12. 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 and later • 7.2.0 and later • 7.0.0 and later
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	• 7.2.0 and later • 7.0.0 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) 7.0.12. This includes both ZTNA access proxy and ZTNA tags: • 7.2.0 and later • 7.0.6 and later The following FortiOS versions support IPsec and SSL VPN with FortiClient (Windows) 7.0.12: • 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
FortiSandbox	• 4.2.0 and later • 4.0.0 and later • 3.2.0 and later • 3.1.0 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.

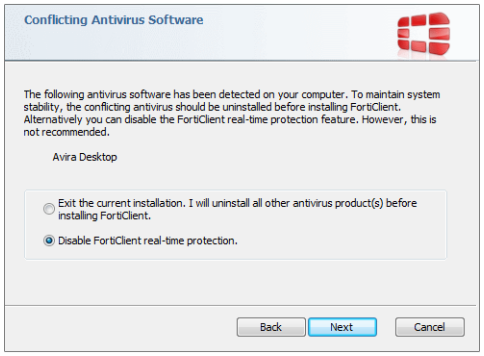
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

Conflicts with third party AV products

The 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.



Intune product codes

Deploying FortiClient with Intune requires a product code. The product codes for FortiClient 7.0.12 are as follows:

Version	Product code
Full	BEC9D8A8-8D04-4A6C-BBD8-A6DF80569B0C
VPN-only agent	7B645F4A-532C-4A11-AD69-7240A1892E3A
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 7.0.12. For inquiries about a particular bug, contact Customer Service & Support.

GUI

Bug ID	Description
990496	FortiClient flickers and opens.

Deployment and installers

Bug ID	Description
953124	FortiClient Orchestrator notification does not appear when upgrade is scheduled.

Remote Access

Bug ID	Description
961079	New Microsoft Teams application does not work if using application-based split tunnel.
962995	FortiSASE secure Internet access VPN frequently disconnects and requires user to log in again.
970005	DNS over TCP does not work when connected to FortiSASE and split DNS is configured.
1003780	IPsec VPN IKEv1 with certificate authentication has connection issues when off-net.

FSSOMA

Bug ID	Description
935090	FortiClient single sign-on mobility agent (FSSOMA) stops sending SSO session information to FortiAuthenticator while service is running on host.

ZTNA rules

Bug ID	Description
977234	Zero trust network access (ZTNA) SAML authentication reprompts user after successful authentication with different identity providers such as FortiAuthenticator or Okta.

Avatar and social login information

Bug ID	Description
950503	FortiClient (Windows) does not use the image that the user uploaded as their avatar.

Other

Bug ID	Description
1015880	User can manually stop FortiClient scheduler service installed with FortiClient under Windows Services.

Known issues

The following issues have been identified in FortiClient (Windows) 7.0.12. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Application Firewall

Bug ID	Description
717628	Application Firewall causes issues with Motorola RMS high availability client.
814391	FortiClient Cloud application signatures block allowlisted applications.
823292	FortiClient cannot connect to JVC wireless display.
827788	Threat ID is 0 on Firewall Events.
842534	After upgrading FortiClient (Windows), Application Firewall blocks internal webpage.
844997	FortiClient sees several packet losses on different internal resources after connecting telemetry.
853808	FortiClient (Windows) blocks Veeam with messages related to Remote.CMD.Shell and VeeamAgent.exe.
860062	Application Firewall slows down opening Microsoft Active Directory (AD) Users and Computers application.
884911	FortiClient detects IntelliJ IDEA Community Edition 2021.2.2 as Java.Debug.Wire.Protocol.Insecure.Configuration.
902866	Application Firewall does not block Google Drive.
958651	Application Firewall violation list always shows violated programs as the same as applications, which is less accurate than Windows.
980803	Image gets corrupted/damaged with a green patch when user tries to view it from a shared location.

Deployment and installers

Bug ID	Description
783690	FortiClient (Windows) does not display reboot prompt after login.
955066	FortiClient 7.0.8 to 7.0.9 upgrade requires multiple restarts.
992045	FortiClient is not installed on AD domain endpoint after deployment from EMS for that domain.

Endpoint control

Bug ID	Description
804552	FortiClient shows all feature tabs without registering to EMS after upgrade.
815037	After EMS administrator selects *Mark All Endpoints As Uninstalled*, FortiClient (Windows) connected with verified user changes to unverified user.
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.
820483	EMS device control does not block camera.
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 many FQDN duplicates.
868230	*Connection expiring due to FortiClient Connect license exceeded* error occurs.

Endpoint management

Bug ID	Description
760816	Group assignment rules based on IP addresses do not work when using split tunnel.
904348	FortiClient (Windows) and EMS detect encryption status as not enabled when only one hard disk has encryption (Bitlocker) enabled.

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

FSSOMA

Bug ID	Description
841316	Some single sign on mobility agent (SSOMA) versions do not present client certificate to FortiAuthenticator.
909844	User FSSO sessions drop earlier than expected.

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.
827394	FortiClient does not report profile change update in *Notifications*.
934351	FortiSASE VPN gets stuck at wrong VPN connection status until FortiClient console restarts from sleep wakeup or network interruption. **Workaround**: Restart FortiClient console.

Install and upgrade

Bug ID	Description
769639	FortiDeviceGuard is not installed on Windows Server 2022.
820672	Zero trust network access (ZTNA) driver FortiTransCtrl.sys fails to start on Windows Server 2016.
867982	Blank certificate pops up when upgrading.

Logs

Bug ID	Description
820067	FortiClient forwards logs despite being completely disabled.
849043	SSL VPN add/close action does not show on FortiGate *Endpoint Event* section.

Bug ID	Description
876810	FortiClient does not indicate VPN user in logs when the connection succeeds.
903480	FortiClient fails to generate log message to FortiAnalyzer or EMS when ZTNA tag prohibits access to VPN.
948887	FortiClient does not send Windows log of Exchange Server logon failure(Event ID 4625).
984729	FortiClient traffic logs do not populate on FortiAnalyzer.
996345	After enabling then disabling logging from the EMS profile, it is still enabled.

Configuration

Bug ID	Description
730415	FortiClient backs up configuration that is missing locally configured ZTNA connection rules.
1016803	After installation, FortiClient (Windows) hides *Remote Access* tab even if a Remote Access profile is embedded in the installer.

User and authentication

Bug ID	Description
765184	RADIUS authentication failover between two servers for high availability does not work well.

Performance

Bug ID	Description
749348	Performance issues after upgrade.

Zero Trust Telemetry

Bug ID	Description
683542	FortiClient (Windows) fails to register to EMS if registration key contains a special character: " !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~".

Malware Protection and Sandbox

Bug ID	Description
760073	FortiDeviceGuard could not be installed on Windows Server through installer.
793926	FortiShield blocks spoolsv.exe on Citrix virtual machine servers.
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 if attempting to copy contents even if WPD/USB is set to be blocked in profile.
857041	Windows 10 security center popup shows both FortiClient and Windows Defender are turned off.
863802	EMS and FortiClient (Windows) cannot detect SentinelOne even if they have product on operating system level.
872970	Bubble notifications do not appear when inserting USB drive in endpoint machine.
876925	Antiexploit protection blocks Microsoft Signing application in Chrome.
882904	FortiClient (Windows) does not include XML option to decide if FortiClient (Windows) should be snoozed or allowed to run side by side with FortiEDR.
903371	FortiClient causes an unhandled exception on third party process when AV components are installed but disabled.
915300	FortiClient (Windows) detects file included in exception as malware.
919007	You cannot perform an on-demand Scan for mapped drives.
925850	RTP stops downloading file on Windows 11.
926155	If Malware Protection is enabled, O hangs up during export of .MOV file to Telestream switch.
926383	When RTP is enabled, logon takes around two to three minutes.
966195	Antimalware detects *W64/AI.Pallas Suspicious* and fails to quarantine the file.
984972	Realtime protection fails to detect ransomware-Lockbit.K!tr.ransom.
991539	FortiClient (Windows) cannot open AV logs on the scan result page after performing on-demand or scheduled scan.
996029	fmon blocks shared directory that sumidero SNC SQL Tool uses due to suspicious virus detected in bitacora.exe.
1015600	On-demand scan fails to quarantine Eicar files from C drive root folder.

Remote Access

Bug ID	Description
727695	FortiClient (Windows) on Windows 10 fails to block SSL VPN when FortiClient has a prohibit host tag.
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.
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.
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.
773920	Endpoint switches network connection after IPsec VPN connection and causes VPN to disconnect.
775633	Automatic failover to second remote gateway does not work when using priority-based IPsec VPN resiliency tunnel.
783412	Browser traffic goes directly to ZTNA site when SSL VPN is connected.
790021	Multifactor authentication using Okta with email notification does not work.
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.
800453	SSL VPN with certificate authentication fails to connect on OS start.
800934	DH group settings should be read-only for tunnel pushed by EMS.
801875	FortiClient cannot connect to VPN when there are two gateways listed using SAML.

Bug ID	Description
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.
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.
824298	SSL VPN with certificates cannot connect to VPN on Elitebook 850 G5/Elitebook 850 G3 laptops.
835042	After upgrading FortiClient (Windows), OpenVPN connection fails while FortiClient (Windows) VPN runs with application-based split tunnel enabled.
837391	FortiClient does not send public IP address for SAML, leading to 0.0.0.0 displaying on FortiOS and FortiSASE.
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.
851093	IPv6 DNS requests do not work.
851600	FortiClient fails to connect to SSL VPN with FQDN resolving to multiple IP addresses when it could not reach resolved IP address.
852507	When connecting to SSL VPN using FortiSSLVPNclient.exe, the VPN adapter IP address is incorrect.
858806	IKE/IPsec VPN sends the same token code multiple times within a second.
861231	VPN tunnel with `on_os_start` enabled does not start on Windows Server.
863138	TapiSrv does not run.
869362	FortiClient (Windows) has issues with multiple reconnections without reauthentication.
869477	When it fails a self test, 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 predfined VPN profiles for corporate or personal VPNs.
870087	Windows feature DeadGatewayDetection does bypass default route via VPN.
871346	When using SAML login with built-in browser, FortiAuthenticator, saved password and autoconnect selected, FortiClient (Windows) cannot remember username and password.
871374	SAML login does not display user warning when opening multiple connection with *Limit Users to One SSL-VPN Connection at a Time*.

Bug ID	Description
874208	FortiClient cannot dial up SSL VPN tunnel with ECDSA certificate.
874310	Using closest gateway based on ping speed and TCP round trip for SSL VPN resilience does not work if using different port.
877640	If FortiClient is registered to EMS, option to connect to IPsec VPN on OS start fails to work.
878070	FortiClient (Windows) intermittently grays out SAML button after device wakes from sleep.
882408	*Failed to renew password when user expires* message displays when logging in to Windows.
887631	Using closest gateway based on TCP round trip time for IPsec VPN resilience does not work if ping is disabled for first gateway.
888602	Autoconnect does not work when based on ping speed/TCP round trip to choose closest FortiGate if FortiClient cannot reach first gateway.
888974	SAML login first connection fails when using external browser for authentication with multifactor authentication.
890217	`<on_os_start_connect>` does not work when rebooting machine by clicking *Restart* in menu.
890227	FortiClient (Windows) stores VPN tunnels manually added by importing XML configuration under *Corporate VPN*.
890352	IPsec VPN for FIPS-enabled FortiClient fails to work when EMS-pushed IPsec/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.
891202	Autoconnect only when off-fabric does not work properly with user account and MFA with FortiToken for xAuth.
893237	FortiClient (Windows) gives no chance to reinput password during autoconnect after identity provider password change.
904871	IPsec VPN takes long time to connect and shows *Connect* button when connection is in progress.
905651	FortiSASE VPN always up has frequent issues when shifting endpoints from one public network to another.
909244	SSL VPN split DNS name resolution stops working.
914018	SSL VPN SAML login fails to work if using YubiKey for MFA.
916240	User from India cannot connect to SSL VPN using SAML authentication but can connect when located in the U.S.
916581	Static DNS entry is registered when on-fabric.
919754	SSL VPN with SAML authentication fails when using an invalid SSL certificate.
920302	Attempt to access local network resource via SMB fails after FortiClient (Windows) establishes IPsec VPN tunnel in some conditions.

Bug ID	Description
920383	FortiClient enables *Turn off smart multi-homed name resolution* on the Windows machine after successful connection.
920908	IPsec VPN password renew prompt differs from SSL VPN prompt.
921636	`SSL_accept` fails due to *1:bad signature* error.
922535	FortiClient crashes while using IPsec VPN IKEv1.
922941	Connecting to SSL VPN with FQDN resolved to both IPv4 and IPv6 as remote gateway gets stuck at 98%.
924736	IPsec VPN connection fails due to blank password with Duo multifactor authentication.
924823	SSL VPN connection has issues with SAML Azure.
929876	Attack surface reduction rule in Microsoft 365 Defender audits FortiSSLVPNdaemon.exe.
930172	With priority=0 and machine autoconnect, per-user autoconnect fails to connect after Windows login.
942668	Split DNS on SSL VPN only resolves the first DNS server.
945888	With VPN before logon, there is no one-time password (OTP) token request prompt if using FortiToken Mobile with FortiAuthenticator for OTP.
947381	With <prefer_sslvpn_dns>=0, when SSL VPN is up, FortiClient adds dns-suffix to all network interfaces.
950787	Domain filter cannot block access for specific server FQDN.
956472	FortiClient fails to resolve SRV records with split DNS.
967051	Initial IPsec VPN autoconnect on machine reboot fails.
975835	*About* page does not display ISDB signatures when only Remote Access profile is enabled.
987400	*Autoconnect* checkbox gray out behavior is inconsistent.
989187	If off-fabric profile is enabled, autoconnect only works when offnet sometimes does not work.
989250	Established VPN tunnel stays connected after EMS disables Remote Access profile.
989595	IPsec VPN IKEv2 tunnel shows SSL VPN username when using only PKI authentication with only certificate and EAP disabled.
991178	IPsec VPN routes traffic through VPN-FGT tunnel when local LAN is disabled on EMS.
992316	FortiClient fails to connect to SSL VPN tunnel with *ErrorCode=-25052*.
993876	FortiClient provides inaccurate error in German when SSL VPN password is incorrect.
994884	FortiShield blocks FortiSSLVPNsys.exe, causing SSL VPN connection failure.
995183	IPsec VPN V4-IKEv2 with RSA authentication asks for FortiToken when multifactor authentication is disabled in FortiGate.
995323	Java error occurs when connected through FortiClient over SSL VPN.

Bug ID	Description
995612	Negative split tunnel metric setting causes loop.
996877	Manage Engine ADSelfService-installed endpoint causes issue on other user screen when VPN before logon is enabled.
997151	IPsec VPN connection with RADIUS user (network policy server with MFA) fails to connect using previously saved password.
997277	FortiClient autoconnects without autoconnect configured.
997279	FortiClient (Windows) drops VPN connection after executing `taskkill` command.
997860	Reverse DNS queries in FortiSASE environment with secure private access causes problem as split DNS needs to support pointer records.
998144	You cannot use network lockdown and Entra ID in combination.
1000706	VPN before Windows logon requires second attempt due to CachedLogonsCount issue.
1003436	IPsec VPN disconnects or freezes sometimes.
1005618	IPsec VPN fails to connect if you did not import R3 intermediate certificate to Windows and ISRG Root X1 issued the FortiGate server certificate.
1006295	FortiClient fails to consistently connect (40%) with DNS round robin of FortiGates (FortiSASE).
1008691	SSL VPN with certificate authentication fails with certificate from PAV virtual card.
1010271	When SSL VPN connection name has more than ten consecutive Japanese characters, SSL VPN connection fails.
1011908	During IPsec VPN authentication, smart card popup displays behind FortiClient window.
1015381	FortiClient takes longer than usual to autoconnect.

Vulnerability Scan

Bug ID	Description
741241	FortiClient (Windows) finds vulnerabilities for uninstalled software.
795393	EMS does not remove vulnerability events after successful patch.
849485	FortiClient wrongly detects AnyDesk vulnerabilities CVE-2021-44426 and CVE-2021-44425.
869253	FortiClient detects vulnerability when the required KB is installed.
908266	FortiClient fails to detect vulnerabilities possibly due to FCM skipping certain VIDs when scanning.
989431	Vulnerability Scan recognizes Windows 10 as Windows 11 (KB 5033375).
1011358	Vulnerability Scan shows no results, but third-party software reports multiple results for same endpoints.

Web Filter and plugin

Bug ID	Description
776089	FortiClient (Windows) does not block malicious sites when Web Filter is disabled.
789017	Web Filter is enabled on FortiSASE profile on EMS.
812207	Blocked web client shows dropped connection message instead of URL blocked message.
836906	After FortiClient install, extended uptime results in audio cracking.
871325	Web Filter breaks DW Spectrum.
904840	When a user is doing device recovery in iTunes, error 3500 displays.
909060	User cannot update information on internal portal with Web Filter active.
939986	Web Filter blocks LuxTrust middleware.
998747	FortiClient does not block Gmail when using Gmail link in Chrome.
1002532	FortiClient (Windows) does not take Web Filter profile exceptions and blocks downloading RDP plugin, blocking access to the server.

Avatar and social network login

Bug ID	Description
878050	Avatar does not update on FortiGate dashboards and FortiGate cannot show updated information.

Multitenancy

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

Onboarding

Bug ID	Description
811976	FortiClient (Windows) may prioritize using user information from authentication user registered to EMS.

Bug ID	Description
819989	FortiClient (Windows) does not show login prompt when installed with installer using LDAP/local verification.
992408	FortiClient (Windows) does not ask for authentication when upgrading from 6.4 to 7.0.11 with FortiClient Cloud.

ZTNA connection rules

Bug ID	Description
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 FortiClient (Windows) install.
831943	ZTNA client certificate is not removed from user certificate store after FortiClient uninstall.
836246	Going from off- to on-Fabric does not stop the ZTNA service and keeps endpoint from connecting.
839589	ZTNA TCP forwarding does not work for GoAnywhere application.
949507	ZTNA has multiple client certificates in certificate store.
990864	With SAML for ZTNA authentication, after closing the first session, the second session continues to request credentials
992649	User cannot create FortiGate tunnel if FortiGate works as both VPN and ZTNA proxy server.
995677	ZTNA TCP forwarding fails to prompt for SAML authentication with external browser after closing and reattempting the connection.
1001116	FortiClient requests SAML credentials after network change in ZTNA connections.
1013466	ZTNA destination for custom app with .NET 8 MAUI does not work as expected.

Quarantine management

Bug ID	Description
956891	FortiClient does not download EMS allowlist file and prevents file restore from *Quarantine Management*.
988911	FortiClient (Windows) cannot reach FortiGate or EMS after quarantine.
1009212	EMS FCrestorequarant tool does not delete the restored file from quarantine folder.

Zero Trust tags

Bug ID	Description
782394	ZTNA user identity tags do not work.
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.

Other

Bug ID	Description
780651	FortiClient (Windows) does not update signatures on expected schedule.
834389	FortiClient (Windows) has incompatibility with Fuji Nexim software.
919017	FortiClient (Windows) changes installer checksum/hash for Baramundi management agent.
984763	NETIO.SYS/FortiWF2.sys causes BSOD on Windows 10.
994963	fwpkclnt.sys and fortisniff2 cause BSOD.
998183	FortiESNAC.exe crashes and FortiClient (Windows) fails to update signatures.
1015385	Redstor Backup Pro causes BSOD when FortiClient (Windows) scans it.

www.fortinet.com