



Release Notes

FortiClient (Windows) 7.4.0



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



October 09, 2024

FortiClient (Windows) 7.4.0 Release Notes

04-740-1012261-20241009

TABLE OF CONTENTS

Change log	5
Introduction	6
Licensing	6
Special notices	7
SAML IdP configuration for Save Password	7
FortiClient support for newer Realtek drivers in Windows 11	7
FortiGuard Web Filtering Category v10 Update	7
Nested VPN tunnels	8
What's new in FortiClient (Windows) 7.4.0	9
Installation information	10
Firmware images and tools	10
Upgrading from previous FortiClient versions	11
Downgrading to previous versions	11
Firmware image checksums	11
Product integration and support	12
Language support	13
Conflicts with third party AV products	14
Intune product codes	14
Resolved issues	15
Avatar and social login information	15
Deployment and installers	15
Endpoint control	15
FSSOMA	16
GUI	16
Install and upgrade	16
Logs	16
Malware Protection and Sandbox	17
PAM	17
Performance	17
Quarantine management	17
Remote Access	17
Remote Access - IPsec VPN	18
Remote Access - SSL VPN	18
Security posture tags	19
Vulnerability Scan	19
Web Filter and plugin	20
ZTNA connection rules	20
Other	20
Known issues	21
New known issues	21

Application Firewall	21
Chromebook	21
Configuration	21
Endpoint control	22
Endpoint management	22
FSSOMA	22
GUI	22
Logs	22
Malware Protection and Sandbox	23
Onboarding	23
Real-time protection	23
Security posture tags	23
Quarantine management	24
Performance	24
Remote Access	24
Remote Access - IPsec VPN	24
Remote Access - SSL VPN	24
Web Filter and plugin	25
ZTNA connection rules	25
PAM	25
Other	26
Existing known issues	26
Remote Access - IPsec VPN	26
Remote Access - SSL VPN	26
Logs	26
Web Filter and plugin	27
ZTNA connection rules	27
Other	27
Numbering conventions	28

Change log

Date	Change description
2024-06-03	Initial release of 7.4.0.
2024-06-25	Added Nested VPN tunnels on page 8.
2024-07-03	Updated Product integration and support on page 12.
2024-10-01	Added Web Filter and plugin on page 27.
2024-10-09	Added Numbering conventions on page 28.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 7.4.0 build 1658.

- [Special notices on page 7](#)
- [Installation information on page 10](#)
- [Product integration and support on page 12](#)
- [Resolved issues on page 15](#)
- [Known issues on page 21](#)

Review all sections prior to installing FortiClient.

FortiClient (Windows) 7.4.0 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 7.4.0 offers a free VPN-only version that you can use for VPN-only connectivity to FortiGate devices running FortiOS 6.4 and later versions. You can download the VPN-only application from FortiClient.com.

FortiClient offers a free standalone installer for the single sign on mobility agent. This agent does not include technical support.

Special notices

SAML IdP configuration for Save Password

FortiClient provides an option to the end user to save their VPN login password with or without SAML configured. When using SAML, this feature relies on persistent sessions being configured in the identity provider (IdP), discussed as follows:

- [Microsoft Entra ID](#)
- [Okta](#)

If the IdP does not support persistent sessions, FortiClient cannot save the SAML password. The end user must provide the password to the IdP for each VPN connection attempt.

The FortiClient save password feature is commonly used along with autoconnect and always-up features.

FortiClient support for newer Realtek drivers in Windows 11

Issues regarding FortiClient support for newer Realtek drivers in Windows 11 have been resolved. The issue is that Realtek and Qualcomm used the NetAdapterCx structure in their drivers, and Microsoft's API had an error in translating the flags, which may result in IPsec VPN connection failure.

FortiGuard Web Filtering Category v10 Update

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

- FortiManager - Fixed in 6.0.12, 6.2.9, 6.4.7, 7.0.2, 7.2.0, 7.4.0.
- FortiOS - Fixed in 7.2.8 and 7.4.1.
- FortiClient - Fixed in Windows 7.2.3, macOS 7.2.3, Linux 7.2.3.
- FortiClient EMS - Fixed in 7.2.1.
- FortiMail - Fixed in 7.0.7, 7.2.5, 7.4.1.
- FortiProxy - Fixed in 7.4.1.

Please read the following CSB for more information to caveats on the usage in FortiManager and FortiOS:

<https://support.fortinet.com/Information/Bulletin.aspx>

Nested VPN tunnels

FortiClient (Windows) does not support parallel independent VPN connections to different sites. However, FortiClient (Windows) may still establish VPN connection over existing third-party (for example, AT&T Client) VPN connection (nested tunnels).

What's new in FortiClient (Windows) 7.4.0

For information about what's new in FortiClient (Windows) 7.4.0, see the [FortiClient & FortiClient EMS 7.4 New Features Guide](#).

Installation information

Firmware images and tools

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

File	Description
FortiClientTools_7.4.0.1658.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_7.4.0.1658_x64.zip	Fortinet single sign on (FSSO)-only installer (64-bit).
FortiClientVPNSetup_7.4.0.1658_x64.exe	Free VPN-only installer (64-bit).

EMS 7.4.0 includes the FortiClient (Windows) 7.4.0 standard installer and zip package containing FortiClient.msi and language transforms.

The following tools and files are available in the FortiClientTools_7.4.0.1658.zip file:

File	Description
OnlineInstaller	Installer files that install the latest FortiClient (Windows) version available.
SSLVPNcmdline	Command line SSL VPN client.
SupportUtils	Includes diagnostic, uninstallation, and reinstallation tools.
VPNAutomation	VPN automation tool.
VC_redist.x64.exe	Microsoft Visual C++ 2015 Redistributable Update (64-bit).
vc_redist.x86.exe	Microsoft Visual C++ 2015 Redistributable Update (86-bit).
CertificateTestx64.exe	Test certificate (64-bit).
CertificateTestx86.exe	Test certificate (86-bit).
FCRemove.exe	Remove FortiClient if unable to uninstall FortiClient (Windows) via Control Panel properly.
FCUnregister.exe	Deregister FortiClient (Windows).
FortiClient_Diagnostic_tool.exe	Collect FortiClient diagnostic result.
ReinstallNIC.exe	Remove FortiClient SSLVPN and IPsec network adapter, if not uninstall it via control panel.
RemoveFCTID.exe	Remove FortiClient UUID.

The following files are available on [FortiClient.com](https://www.fortinet.com):

File	Description
FortiClientSetup_7.4.0.1658_x64.zip	Standard installer package for Windows (64-bit).
FortiClientVPNSetup_7.4.0.xxxx_x64.exe	Free VPN-only installer (64-bit).



Review the following sections prior to installing FortiClient version 7.4.0: [Introduction on page 6](#), [Special notices on page 7](#), and [Product integration and support on page 12](#).

Upgrading from previous FortiClient versions

To upgrade a previous FortiClient version to FortiClient 7.4.0, do one of the following:

- Deploy FortiClient 7.4.0 as an upgrade from EMS. See [Recommended upgrade path](#).
- Manually uninstall existing FortiClient version from the device, then install FortiClient (Windows) 7.4.0.

FortiClient (Windows) 7.4.0 features are only enabled when connected to EMS 7.2 or later.

See the [FortiClient and FortiClient EMS Upgrade Paths](#) for information on upgrade paths.

Downgrading to previous versions

FortiClient (Windows) 7.4.0 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 7.4.0 product integration and support information:

Desktop operating systems	<ul style="list-style-type: none">• Microsoft Windows 11 (64-bit)• Microsoft Windows 10 (64-bit)
Server operating systems	<ul style="list-style-type: none">• Microsoft Windows Server 2022• Microsoft Windows Server 2019 <p>FortiClient 7.4.0 does not support Windows Server Core.</p> <p>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.</p> <p>Microsoft Windows Server 2019 supports zero trust network access (ZTNA) with FortiClient (Windows) 7.4.0.</p> <p>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.</p>
Minimum system requirements	<ul style="list-style-type: none">• Microsoft Windows-compatible computer with Intel processor or equivalent. FortiClient (Windows) does not support ARM-based processors.• Compatible operating system and minimum 2 GB RAM• 1 GB free hard disk space• Native Microsoft TCP/IP communication protocol• Native Microsoft PPP dialer for dialup connections• Ethernet network interface controller (NIC) for network connections• Wireless adapter for wireless network connections• Adobe Acrobat Reader for viewing FortiClient documentation• Windows Installer MSI installer 3.0 or later
AV engine	<ul style="list-style-type: none">• 7.00026
VCM engine	<ul style="list-style-type: none">• 2.0043
FortiAnalyzer	<ul style="list-style-type: none">• 7.4.0 and later• 7.2.0 and later• 7.0.0 and later
FortiAuthenticator	<ul style="list-style-type: none">• 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
FortiClient EMS	<ul style="list-style-type: none">• 7.2.0 and later
FortiManager	<ul style="list-style-type: none">• 7.4.0 and later

	<ul style="list-style-type: none"> • 7.2.0 and later • 7.0.0 and later
FortiOS	<p>The following FortiOS versions support ZTNA with FortiClient (Windows) 7.4.0. This includes both ZTNA access proxy and ZTNA tags:</p> <ul style="list-style-type: none"> • 7.4.0 and later • 7.2.0 and later • 7.0.6 and later <p>The following FortiOS versions support IPsec and SSL VPN with FortiClient (Windows) 7.4.0:</p> <ul style="list-style-type: none"> • 7.4.0 and later • 7.2.0 and later • 7.0.0 and later • 6.4.0 and later
FortiSandbox	<ul style="list-style-type: none"> • 4.4.0 and later • 4.2.0 and later • 4.0.0 and later • 3.2.0 and later

Language support

The following table lists FortiClient language support information:

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

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

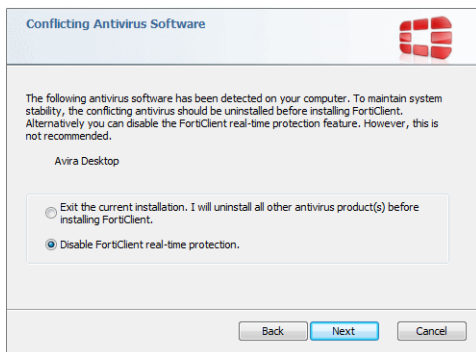


If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

Conflicts with third party AV products

Fortinet does not recommend running third party antivirus software while FortiClient's AV feature is running. If you are not using FortiClient's AV feature, exclude the FortiClient installation folder from scanning for the third party AV software.

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 7.4.0 are as follows:

Version	Product code
Enterprise	96A251BD-7532-4CF9-B87D-158FC685DBC4
VPN-only agent	0DC51760-4FB7-41F3-8967-D3DEC9D320EB
Private access management-only agent	1D444487-35DF-42E0-A9BD-E2D5C16921A6
Single sign on-only agent	AB704421-C207-4C1E-989D-4AF26FA9D002

See [Configuring the FortiClient application in Intune](#).

Resolved issues

The following issues have been fixed in version 7.4.0. For inquiries about a particular bug, contact [Customer Service & Support](#).

Avatar and social login information

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

Deployment and installers

Bug ID	Description
783690	FortiClient upgrade reboot prompt does not show after logging in to the endpoint to complete the installation.
953124	Orchestrator notification does not appear when upgrade is scheduled.
1012187	Upgraded FortiClient installs features that are disabled in the EMS deployment package.
1017674	FortiClient does not move to assigned group after installation when using EMS-created installer with installer ID.
1025278	Upgrade from 7.2.4 to 7.4.0 prompts multiple reboots even after completing deployment.

Endpoint control

Bug ID	Description
821024	FortiClient (Windows) fails to send username to EMS and EMS reports it as under different users.
979593	One-way message GUI is not translated.

FSSOMA

Bug ID	Description
909844	Single sign-on mobility agent (SSOMA) drops user FSSO sessions earlier.
935090	SSOMA stops sending SSO session information to FortiAuthenticator while service runs on host.
964769	FSSOMA for Microsoft Entra ID does not send tenant ID to FortiAuthenticator.

GUI

Bug ID	Description
981993	<i>Remote Access</i> GUI shows an incorrect message when FortiClient (Windows) is unregistered from the EMS.
990496	FortiClient icon flickers on the taskbar and opens console unexpectedly.

Install and upgrade

Bug ID	Description
1014145	JavaScript error occurs in FortiClient (Windows) console after installation.
1015715	Upgrade to 7.4.0 after reboot prompts user to reboot again due to <i>FortiDeviceGuard Device</i> .

Logs

Bug ID	Description
985044	FortiClient log level does not change from debug and user cannot delete log files from "%AppData%".
996767	FortiAnalyzer does not show endpoint logs after endpoint upgrade from FortiClient (Windows) 7.0.9 to 7.2.3.
1007868	Web Filter blocked URL log does not include blocked website information.
1016032	FCDBLog has high memory consumption.

Malware Protection and Sandbox

Bug ID	Description
820483	EMS device control does not block camera device.
988110	Sandbox fails to exclude trusted files from scanning if the file is in network folder.
1022991	GUI does not show timestamp for Sandbox quarantined file.
1032129	Sporadic network error occurs in Sandbox connection state.

PAM

Bug ID	Description
993068	Firefox FortiPAM launch secret does not record screen for new opened tabs. Only first tab open from launch secret is recorded.
1023562	Web user account stays signed in even after the PAM session is closed.

Performance

Bug ID	Description
1012529	FortiClient (Windows) constantly and very frequently writes event files and cause CPU and overheating issues.

Quarantine management

Bug ID	Description
1006062	FortiClient (Windows) cannot restore files for network share.

Remote Access

Bug ID	Description
973808	When OS is non-English, such as Spanish, and endpoint is non-compliant, FortiClient (Windows)

Bug ID	Description
	fails to show warning prompt when trying to connect to VPN.
997718	When FortiClient (Windows) enables autoconnect, it behaves like always up is enabled.
997718	When autoconnect is enabled, FortiClient (Windows) behaves like it is always-up.
1000706	VPN before Windows logon requires second attempt due to CachedLogonsCount issue.

Remote Access - IPsec VPN

Bug ID	Description
740333	FortiClient modifies DNS settings of all network adapters.
758424	Same certificate works for IPsec VPN tunnel if put it in local compute but fails to work if certificate is in current user store.
974215	Resilient IPsec VPN tunnel fails to connect if first remote gateway is unreachable (e.g. down).
997277	FortiClient (Windows) autoconnects when autoconnect is not configured.
1002375	IPsec VPN <code>disclaimer_msg</code> option does not work.
1003780	IPsec VPN IKEv1 with certificate authentication has issues with connection when off-net.
1005618	IPsec VPN fails to connect if R3 Intermediate certificate is not imported and ISRG Root X1 issued FortiGate server certificate.
1006236	IKEv2 has fragmentation issue.
1021018	IPsec VPN before logon gets incorrect username or password error when using Windows credentials.
1033835	After IPsec VPN full tunnel is up for three to four hours, internet access starts to fail.

Remote Access - SSL VPN

Bug ID	Description
837391	FortiClient does not send public IP address for SAML, leading to FortiOS and FortiSASE displaying 0.0.0.0.
890000	FortiClient 7.2.0 configured with <code>on-os-start-connect</code> is slow compared to FortiClient (Windows) 7.0.7.
920953	SSL VPN intermittently fails to reconnect to tunnel without authentication after a network disruption.
954004	FortiClient (Windows) cannot establish DTLS tunnel when handshake packet has a large MTU.

Bug ID	Description
961079	New Microsoft Teams does not work if using application-based split tunnel.
970005	DNS over TCP does not work with FortiClient (Windows) connected to FortiSASE and split DNS configured.
983216	FortiClient attempts to connect back to VPN after <code>auth-timeout</code> expiry when <code>tunnel-connect-without-reauth</code> is enabled.
998146	SSL VPN disconnects every 20-30 minutes.
999205	Internal VPN browser is vulnerable for man-in-the-middle attack.
1000589	VPN gets stuck on connecting and error 6005 occurs if SAML takes longer than 60 seconds.
1008116	After FortiClient (Windows) upgrade, SAML VPN is stuck at 0% with error (-6005).
1008932	SASE secure internet access <code>reconnect_without_reauthentication</code> does not work.
1015381	FortiClient takes longer than usual to autoconnect.
1016971	FortiClient fails to autoconnect and gets stuck in <i>Connecting</i> state until reboot.
1017731	FortiClient (Windows) shows password mismatch after providing correct password in password confirmation field and pressing <code>Enter</code> .
1018126	WMIPRVSE.exe service CPU usage spikes when connected to Secure Internet Access VPN.
1019619	VPN always-up fails to come up with split DNS configured.

Security posture tags

Bug ID	Description
1002079	<i>Automatic Updates are enabled</i> Security Zero Trust tagging rule does not work as expected.

Vulnerability Scan

Bug ID	Description
989431	Vulnerability Scan recognizes Windows 10 as Windows 11 (KB 5033375).
1011358	Vulnerability Scan shows 0 results but third-party software reports multiple for same endpoints.

Web Filter and plugin

Bug ID	Description
851700	FortiClient displays <i>Microsoft Edge extension policy anomaly detected, please restart browser</i> popup.
1008112	Web Filter blocks downloading some files in web.whatsapp.com and always shows block page.
1013487	Web Filter blocks Webex because it considers it as unrated.

ZTNA connection rules

Bug ID	Description
919103	Clicking Settings > Clear Cookies causes FortiClient (Windows) to remove manually added local zero trust network access (ZTNA) rules.
931275	ZTNA destination rules stop working.
976028	ZTNA wildcard in destination with format name*.domain.com does not work.

Other

Bug ID	Description
964456	FortiClient does not allow Windows DNS only secure dynamic updates.
971090	FortiClient daemon (fcaptmon) has memory leak.
1003200	Silent and version-independent uninstall using CLI has issue.
1006130	FortiShield.sys causes blue screen of death.

Known issues

Known issues are organized into the following categories:

- [New known issues on page 21](#)
- [Existing known issues on page 26](#)

To inquire about a particular bug or to report a bug, contact [Customer Service & Support](#).

New known issues

The following issues have been identified in version 7.4.0.

Application Firewall

Bug ID	Description
979330	FortiClient (Windows) does not present Microsoft Loop in Application Firewall signatures list.
1020282	Application Firewall blocks some applications in the exclusion list.

Chromebook

Bug ID	Description
997927	On Chromebook, fallback action is to override exclusion list, which is unlike FortiClient (Windows).

Configuration

Bug ID	Description
1028865	If FortiClient (Windows) loses connectivity to EMS Telemetry, VPN profile sent to FortiClient PC does not show single sign on (SSO) settings.

Endpoint control

Bug ID	Description
996850	FortiClient sends different username to EMS when user logs on to computer with SmartCard.
1016378	FortiClient (Windows) does not prompt for user verification when other Entra ID user is logged in.
1016952	FortiClient telemetry gets stuck at syncing state after enabling zero trust network access.
1023356	FortiClient endpoint loses EMS connection when PC changes network connection.

Endpoint management

Bug ID	Description
1034892	EMS cannot download diagnostic logs for FortiClient (Windows) from EMS.

FSSOMA

Bug ID	Description
995379	FSSOMA does not properly install on CIS hardened Windows 10 and 11 image.
1033466	FSSOMA.exe stops running after upgrading SSO standalone agent from 7.2.4 to 7.4.0.

GUI

Bug ID	Description
1011345	GUI has mistranslation in Slovak for Cloud Sandbox.

Logs

Bug ID	Description
948887	FortiClient does not send Windows log for Exchange Server logon failure(Event ID 4625).
1016539	Vulnerability reports do not display username information in FortiAnalyzer.
1033630	FortiClient Sandbox events are not replicated on FortiAnalyzer.

Malware Protection and Sandbox

Bug ID	Description
965730	System drive as a USB-connected NVMe drive with Windows 10 fails to boot after installing FortiClient (Windows) with Malware Protection.
996431	FortiClient (Windows) cannot block remote NDIS device when the net class device is set to block in removable media access function.
1012083	If Antiexploit is enabled on EMS, it blocks certificates on DocuSign.
1012531	Antiexploit blocks applications defined in the <i>Excluded Applications</i> list.
1034857	FortiClient does not send the file to FortiSandbox for analysis if the hashes are the same.

Onboarding

Bug ID	Description
982079	FortiClient Cloud invitation with LDAP verification type to Entra ID fails with <i>Azure Token Required</i> error.
1018839	FortiClient console fails to open automatically upon clicking SAML notification.

Real-time protection

Bug ID	Description
1036535	FortiClient (Windows) detects <i>C:\PublishedSites\</i> files as threats and quarantines them.

Security posture tags

Bug ID	Description
988510	Windows OS tag with latest update within 30 days does not work reliably.
1013973	Host check policy does not work as expected using OR logic.
1027851	FortiClient (Windows) sometimes loses security posture tag based on combined rules and the only way to fix the issue is reinstalling FortiClient.
1030469	EMS does not match endpoint for <i>User in AD Group</i> security posture tag when the user is in the local AD but missing in the EMS database.
1034875	AD group security posture tag is not calculated correctly when multiple users are logged in.

Quarantine management

Bug ID	Description
1009212	EMS FCrestorequarant tool does not delete the restored file from quarantine folder.

Performance

Bug ID	Description
1015900	FortiESNAC has high RAM consumption on Windows Servers.
1022885	FortiClient (Windows) causes bootup delay on Windows 10 and 11.

Remote Access

Bug ID	Description
1010271	When VPN connection name has more than 10 Japanese characters, VPN connection fails

Remote Access - IPsec VPN

Bug ID	Description
973544	IPsec VPN IKEv2 with SAML login does not support using external browser as user agent for authentication.
1036306	IPsec VPN fails to autoconnect after installing EMS-repackaged FortiClient installer when <code>autoconnect_on_install</code> is enabled.
1037063	IKEv2 SAML login fails to work if Electron is used as the SAML authentication framework and FortiClient fails to validate server certificate.

Remote Access - SSL VPN

Bug ID	Description
909244	SSL VPN split DNS name resolution stops working.
950787	Domain filter cannot block access to specific server FQDN.
964036	Gateway selection (e.g. saml-login) based on ping speed or TCP round trip does not work.
997010	If first defined FortiGate is unreachable, FortiClient (Windows) does not try to establish connection with the secondary gateway.
1002456	After upgrade, customize host check fail warning does not appear when tag is on device.

Bug ID	Description
1006295	FortiClient fails to consistently connect (40%) with DNS round robin of FortiGates (SASE).
1012434	FortiClient (Windows) does not save SAML VPN username when user closes internal SAML authentication window deliberately with <code><use_gui_saml_auth></code> enabled.
1018817	User must click <i>Save Password</i> to save SAML username.
1019876	User gets stuck at 40% connectivity when connecting to any VPN.
1029584	FortiClient (Windows) does not apply FortiOS SSL VPN custom host check error message and always uses the default one.
1038155	SSL VPN always up fails when <code>tunnel-connect-without-reauth</code> and <code>vpn-ems-sn-check</code> are enabled.

Web Filter and plugin

Bug ID	Description
975694	FortiClient blocks Outlook and multiple destinations due unknown category error.
978252	Microsoft Edge guest browsing bypasses Web Filter blocked sites.
996420	Web Filter has issue with resolved IP addresses in multiple ISDB objects such as cloud applications.
1019249	Web Filter applies wrong categorization for artificial intelligence technology.
1022851	FortiClient (Windows) does not automatically disable Web Filtering after endpoint becomes on-fabric when configured for only off-fabric endpoints.

ZTNA connection rules

Bug ID	Description
1001116	FortiClient requests SAML credentials after network change in ZTNA connections.

PAM

Bug ID	Description
1015585	FortiClient completely closes MobaXterm application when a launched secret session reaches max duration.

Other

Bug ID	Description
984763	NETIO.SYS/FortiWF2.sys causes BSODs on Windows 10.
1013438	FortiClient blocks RADIUS authentication on Aruba HPE switch ports.
1013910	Installing FortiClient causes blue screen of death (BSOD).
1018650	FortiShield.sys causes BSOD with FortiClient.
1021271	BSOD issue occurs after connecting to VPN due to fortisniff2.sys and fortiwf2.sys.
1022847	FCDBLog.exe has memory leak.

Existing known issues

The following issues have been identified in a previous version of FortiClient (Windows) and remain in FortiClient (Windows) 7.4.0.

Remote Access - IPsec VPN

Bug ID	Description
971554	For IPsec VPN, FortiClient sends access request when password renewal was canceled.
1003308	FortiClient attempts to autoconnect to Azure autoconnect tunnels when the logged-in user is not an Azure user.

Remote Access - SSL VPN

Bug ID	Description
920383	FortiClient always enables <i>Turn off smart multi-homed name resolution</i> on Windows machine after successful connection.
930740	FortiClient (Windows) cannot set up SSL VPN if the password contains Polish characters: ł, ą, ń.
942668	Split DNS on SSL VPN only resolves the first DNS server.

Logs

Bug ID	Description
903480	FortiClient fails to generate log message to FortiAnalyzer or EMS when security posture tag

Bug ID	Description
	prohibits access to VPN.
979323	FortiClient does not send any logs to FortiAnalyzer unless <i>Log All URLs</i> is enabled.

Web Filter and plugin

Bug ID	Description
914636	Web Filter exclusion list does not support <i>Warn</i> action.

ZTNA connection rules

Bug ID	Description
831943	ZTNA client certificate does not get removed from user certificate store after FortiClient (Windows) is uninstalled.
955377	ZTNA is blocked because "device is offline".

Other

Bug ID	Description
994963	fwpkclnt.sys and fortisniff2 cause blue screen of death.

Numbering conventions

Fortinet uses the following version number format:

<First number>.<Second number>.<Third number>.<Fourth number>

Example: 7.4.0.15

- First number = major version
- Second number = minor version
- Third number = maintenance version
- Fourth number = build version

Release Notes pertain to a certain version of the product. Release Notes are revised as needed.



Release Notes

FortiClient (Windows) 7.4.0

