



# Release Notes

FortiClient (Windows) 7.4.3



**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](mailto:techdoc@fortinet.com)



March 02, 2026

FortiClient (Windows) 7.4.3 Release Notes

04-743-1109381-20260302

# TABLE OF CONTENTS

<b>Change log</b> .....	<b>5</b>
<b>Introduction</b> .....	<b>6</b>
Licensing .....	6
<b>Special notices</b> .....	<b>7</b>
FortiClient (Windows) 7.4.3 GA hotfix 1 .....	7
FortiClient (Windows) 7.4.3 free VPN-only agent GA update 1 .....	7
Nested VPN tunnels .....	8
SAML IdP configuration for Save Password .....	8
FortiClient support for newer Realtek drivers in Windows 11 .....	8
FortiGuard Web Filtering category v10 update .....	9
<b>What's new in FortiClient (Windows) 7.4.3</b> .....	<b>10</b>
<b>Installation information</b> .....	<b>11</b>
Firmware images and tools .....	11
Upgrading from previous FortiClient versions .....	12
Downgrading to previous versions .....	13
Firmware image checksums .....	13
<b>Product integration and support</b> .....	<b>14</b>
Language support .....	15
Conflict with third-party endpoint protection software .....	16
Intune product codes .....	16
<b>Resolved issues</b> .....	<b>18</b>
Configuration .....	18
Deployment and installers .....	18
Endpoint control .....	18
Install and upgrade .....	18
Onboarding .....	19
PAM .....	19
Remote Access .....	19
Remote Access - IPsec VPN .....	20
Remote Access - SSL VPN .....	20
Security posture tags .....	21
Vulnerability Scan .....	21
Web Filter and plugin .....	22
ZTNA connection rules .....	22
Common Vulnerabilities and Exposures .....	22
<b>Known issues</b> .....	<b>23</b>
New known issues .....	23
Application Firewall .....	23
Endpoint control .....	23
Malware Protection and Sandbox .....	23
Remote Access - IPsec VPN .....	24

---

Remote Access - SSL VPN .....	24
Security posture tags .....	24
Vulnerability Scan .....	24
Web Filter and plugin .....	24
ZTNA .....	25
ZTNA connection rules .....	25
Other .....	25
Existing known issues .....	25
Application Firewall .....	25
Deployment and installers .....	26
GUI .....	26
Install and upgrade .....	26
Malware Protection and Sandbox .....	26
Multitenancy .....	26
Quarantine management .....	27
Performance .....	27
Remote Access .....	27
Remote Access - SSL VPN .....	27
Web Filter and plugin .....	28

# Change log

Date	Change description
2025-03-20	Initial release of 7.4.3.
2025-03-24	Updated <a href="#">Product integration and support</a> on page 14.
2025-03-26	Updated <a href="#">Product integration and support</a> on page 14.
2025-05-28	Updated <a href="#">Product integration and support</a> on page 14.
2025-08-18	Added 1133715 to <a href="#">New known issues</a> on page 23.
2025-11-25	Updated <a href="#">Product integration and support</a> on page 14.
2025-11-26	Updated <a href="#">Product integration and support</a> on page 14.
2025-12-11	Added <a href="#">FortiClient (Windows) 7.4.3 GA hotfix 1</a> on page 7 and <a href="#">FortiClient (Windows) 7.4.3 free VPN-only agent GA update 1</a> on page 7.
2026-03-02	Updated <a href="#">New known issues</a> on page 23,

# Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 7.4.3 build 1790.

- [Special notices on page 7](#)
- [What's new in FortiClient \(Windows\) 7.4.3 on page 10](#)
- [Installation information on page 11](#)
- [Product integration and support on page 14](#)
- [Resolved issues on page 18](#)
- [Known issues on page 23](#)

Review all sections prior to installing FortiClient.

FortiClient (Windows) 7.4.3 components that interact with Microsoft Security Center are signed with an Azure Code Signing certificate, which fulfills Microsoft requirements.

Fortinet uses the following version number format:

<Major version number>.<minor version number>.<patch number>.<build number>

Example: 7.4.3.1790

Release Notes correspond to a certain version and build number of the product.

## Licensing

See [Windows, macOS, and Linux endpoint licenses](#).

FortiClient 7.4.3 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

## FortiClient (Windows) 7.4.3 GA hotfix 1

FortiClient (Windows) 7.4.3 GA hotfix 1 (7.4.3.1790.1.8758) was released on December 11, 2025 to address the following vulnerabilities:

Bug ID	Description
1129740	CVE-2025-46373
1147064	CVE-2025-47761
1188354	CVE-2025-66535

To install the hotfix from EMS, collect the EMS serial numbers and contact [Fortinet Support](#).

### To install the hotfix locally:

1. Download the `FortiClientTools_7.4.3.8758.zip` file from the [Fortinet Support](#) website.
2. Unzip the file and copy the `FortiClientTools_7.4.3.8758\SupportUtils\hotfix.exe` file to the Downloads folder.
3. Shutdown FortiClient and run the following installation command in PowerShell:

```
C:\Users\ftntt\Downloads>cmd /k hotfix.exe
```

4. When the *Hotfix 7.4.3.8758 is now installed* message is displayed, verify the following:
  - The `C:\windows\system32\driver\fortips_74.sys` file has been updated (check modification date)
  - The `C:\Program Files\Fortinet\FortiClient\resources\app.asar` file has been updated (check modification date)
  - The FortiClient version is *7.4.3 hotfix 1.8758* in the *About* page of the FortiClient GUI.

## FortiClient (Windows) 7.4.3 free VPN-only agent GA update 1

FortiClient (Windows) 7.4.3 free VPN-only agent GA update 1 (7.4.3.1790.1.8758) was released on December 11, 2025 to address the following vulnerabilities:

Bug ID	Description
1129740	<a href="#">CVE-2025-46373</a>
1147064	<a href="#">CVE-2025-47761</a>
1188354	<a href="#">CVE-2025-66535</a>

To install the update, download the latest FortiClient VPN-only agent installation file for Windows from [FortiClient.com](#) and double-click it to complete the installation. To verify the installation is successful, make sure the FortiClient version is *7.4.3 hotfix 1.8758* in the *About* page of the FortiClient GUI.

## Nested VPN tunnels

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

## 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.

See the following CSB for more information to caveats on the usage in FortiManager and FortiOS:  
<https://support.fortinet.com/Information/Bulletin.aspx>

# What's new in FortiClient (Windows) 7.4.3

For information about what's new in FortiClient (Windows) 7.4.3, 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
forticlient-7.4.3-windows-release-notes.pdf	Release Notes file.
FortiClientPAMSetup_7.4.3.1790_x64.exe	Privilege access management agent installer (64-bit).
FortiClientSetup_7.4.3.1790_ARM64.zip	ARM installer (64-bit).
FortiClientSetUp_7.4.3.1790_x64.zip	Installer (64-bit).
FortiClientSSOSetup_7.4.3.1790_ARM64.zip	ARM FSSO-only installer (64-bit).
FortiClientSSOSetup_7.4.3.1790_x64.zip	Fortinet single sign on (FSSO)-only installer (64-bit).
FortiClientTools_7.4.3.1790.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientVPNSetup_7.4.3.1790_x64.exe	Free VPN-only installer (64-bit).
FortiClientVPNSetup_7.4.31790_ARM64.exe	ARM free VPN-only installer (64-bit). An EMS license must be present on the logged-in FortiCloud account to download this file.

EMS 7.4.3 includes the FortiClient (Windows) 7.4.3 standard installer and zip package containing FortiClient.msi and language transforms.

The following tools and files are available in the FortiClientTools\_7.4.3.1790.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.

File	Description
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://FortiClient.com):

File	Description
FortiClientSetup_7.4.3.1790_x64.zip	Standard installer package for Windows (64-bit).
FortiClientVPNSetup_7.4.3.xxxx_x64.exe	Free VPN-only installer (64-bit).



Review the following sections prior to installing FortiClient version 7.4.3: [Introduction on page 6](#), [Special notices on page 7](#), and [Product integration and support on page 14](#).

## Upgrading from previous FortiClient versions

Upgrading from FortiClient (Windows) 7.4.0 or 7.4.1 to 7.4.3 using .msi files with a Windows Active Directory (AD) deployment mechanism may cause FortiClient (Windows) services to fail to start after upgrade. Fortinet recommends using one of the following methods to solve this issue after upgrading to FortiClient (Windows) 7.4.3:

- Reboot the device.
- Use a script that Windows AD deployed that starts the FortiClient Windows scheduler. You must run the script as an administrator:

```
C:\Windows\system32>sc start fa_scheduler
```

Instead of using AD, you can use Microsoft System Center Configuration Manager deployment to upgrade FortiClient (Windows) from 7.4.0 or 7.4.1 to 7.4.3 by using the following command:

```
msiexec /I "FortiClient.msi" REINSTALL=ALL REINSTALLMODE=vomus /forcerestart /q
```

If you upgrade FortiClient (Windows) using .exe files, the aforementioned methods are irrelevant.

Upgrading FortiClient (Windows) endpoints using EMS is recommended.

To upgrade a previous FortiClient version to FortiClient 7.4.3, do one of the following:

- Deploy FortiClient 7.4.3 as an upgrade from EMS. See [Recommended upgrade path](#).
- Manually uninstall existing FortiClient version from the device, then install FortiClient (Windows) 7.4.3.

FortiClient (Windows) 7.4.3 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) 7.4.3 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 7.4.3 product integration and support information:

<b>Desktop operating systems</b>	<ul style="list-style-type: none"><li>• Microsoft Windows 11 (64-bit)</li><li>• Microsoft Windows 10 (64-bit)</li><li>• Windows 10 IoT Enterprise</li><li>• Windows 11 IoT Enterprise</li></ul>
<b>Server operating systems</b>	<ul style="list-style-type: none"><li>• Microsoft Windows Server 2022</li><li>• Microsoft Windows Server 2019</li></ul> <p>FortiClient (Windows) 7.4.3 does not support Guiless (Core) OS. Microsoft Windows Server does not support Application Firewall.</p>
<b>Minimum system requirements</b>	<ul style="list-style-type: none"><li>• Microsoft Windows-compatible computer with Intel processor or equivalent. ARM-based processor support is in beta. As such, for ARM-based processors, FortiClient (Windows) supports a limited feature set as follows:<ul style="list-style-type: none"><li>• Fortinet Security Fabric agent (connection to EMS and Telemetry)</li><li>• Remote Access (VPN)</li><li>• Web Filter</li><li>• Vulnerability Scan</li></ul></li><li>• ARM images are only available for download from the <a href="#">Fortinet Support portal</a>.</li><li>• Compatible operating system and minimum 2 GB RAM</li><li>• 1 GB free hard disk space</li><li>• Native Microsoft TCP/IP communication protocol</li><li>• Native Microsoft PPP dialer for dialup connections</li><li>• Ethernet network interface controller for network connections</li><li>• Wireless adapter for wireless network connections</li><li>• Adobe Acrobat Reader for viewing FortiClient documentation</li><li>• Windows Installer MSI installer 3.0 or later</li></ul>
<b>FortiClient EMS</b>	7.4.0 and later
<b>FortiOS</b>	<ul style="list-style-type: none"><li>• 7.6.0 and later. FortiOS 7.6.3 and later versions do not support SSL VPN tunnel mode. See <a href="#">Migrating from SSL VPN tunnel mode to IPsec VPN</a>.</li><li>• 7.4.0 and later</li><li>• 7.2.0 and later</li><li>• 7.0.0 and later</li><li>• 6.4.0 and later</li></ul>
<b>AV engine</b>	7.0.38

<b>VCM engine</b>	2.0043
<b>IPS Engine</b>	7.6.1040
<b>FortiAnalyzer</b>	<ul style="list-style-type: none"> <li>• 7.6.0 and later</li> <li>• 7.4.0 and later</li> <li>• 7.2.0 and later</li> <li>• 7.0.0 and later</li> </ul>
<b>FortiEDR for Windows</b>	<ul style="list-style-type: none"> <li>• 5.2.5.0052</li> </ul>
<b>FortiAuthenticator</b>	<ul style="list-style-type: none"> <li>• 6.5.0 and later</li> <li>• 6.4.0 and later</li> <li>• 6.3.0 and later</li> </ul>
<b>FortiManager</b>	<ul style="list-style-type: none"> <li>• 7.6.0 and later</li> <li>• 7.4.0 and later</li> <li>• 7.2.0 and later</li> <li>• 7.0.0 and later</li> </ul>
<b>FortiSandbox</b>	<ul style="list-style-type: none"> <li>• 4.4.0 and later</li> <li>• 4.2.0 and later</li> <li>• 4.0.0 and later</li> </ul>

## Language support

The following table lists FortiClient language support information:

Language	GUI	XML configuration	Documentation	
English	Yes	Yes	Yes	
Chinese (simplified)		No	No	No
Chinese (traditional)				
French (France)				
German				
Japanese				
Korean				
Portuguese (Brazil)				
Russian				
Spanish (Spain)				

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



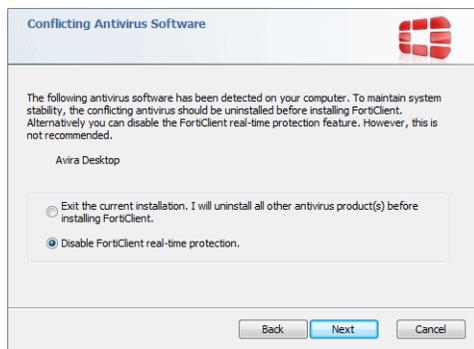
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

## Conflict with third-party endpoint protection software

As a Fortinet Fabric Agent that provides protection, compliance, and secure access, FortiClient may conflict with antimalware products on the market that provide similar AV, web filtering, application firewall, and ransomware protection features as FortiClient. If you encounter a conflict, there are a few steps you can take to address it:

- Do not use other AV products when FortiClient AV is enabled.
- If FortiClient AV is disabled, configure the third party AV product to exclude the FortiClient installation folder from being scanned.

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 7.4.3 are as follows:

Version	Product code
Enterprise	7267071F-D578-4E11-AB6A-478C0C0B85EC
VPN-only agent	15C7B361-A0B2-4E79-93E0-868B5000BA3F

Version	Product code
Private access management-only agent	99C4E612-E8CE-4712-8817-BE2507A00FE7
Single sign on-only agent	2FBE9D1B-BBBB-4BBD-9146-0FD4AA26BBCC

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

# Resolved issues

The following issues have been fixed in version 7.4.3. For inquiries about a particular bug, contact [Customer Service & Support](#).

## Configuration

Bug ID	Description
1087936	EMS disconnect password with special characters does not work.

## Deployment and installers

Bug ID	Description
1113057	Install does not follow unsupervised scheduled deployment time.

## Endpoint control

Bug ID	Description
1100661	FortiClient (Windows) does not send SNI connecting to on-premise EMS.
1110524	After reboot, FortiClient enters configuration loop when switching from SSL VPN-only profile to zero trust network access (ZTNA)-only profile.

## Install and upgrade

Bug ID	Description
1080006	FortiClient (Windows) .exe installer does not properly handle v and msic1 command line parameters.

Bug ID	Description
1111464	FortiClient daemon crashes with Visual C++ runtime version lower than 14.40.33810.0.

## Onboarding

Bug ID	Description
1081547	Authentication dialog is blank when using invitation code with local or LDAP authentication to connect to EMS.

## PAM

Bug ID	Description
1099622	FortiPAM fails to automatically fill password for proxy mode enabled secret when FortiClient (Windows) fails to add FortiPAM zero trust network access rules in time.
1101380	<i>This site can't be reached</i> error occurs on first attempt through web launcher in FortiPAM.

## Remote Access

Bug ID	Description
706804	Disabling local LAN access does not restrict remote access.
1027199	FortiClient (Windows) sometimes does not log in to system when using SAML VPN before logon.
1059326	VPN before logon fails with <i>Use Windows Credentials</i> .
1065837	FortiTray network lockdown is not translated and language should be more consistent with macOS.
1066263	Free VPN-only agent does not minimize after establishing a tunnel with <code>&lt;minimize_window_on_connect&gt;</code> enabled.
1086017	Failed to prompt Host Check Fail warning even though secure remote access is on and endpoint is non-compliant.
1089023	VPN SAML external browser (e.g Chrome) authentication does not work after

Bug ID	Description
	successful authentication.
1090354	Using Windows credentials for VPN is always selected for VPN before logon when <code>&lt;use_windows_credentials&gt;</code> is disabled.
1109326	<code>&lt;keep_fqdn_resolution_consistency&gt;1&lt;/keep_fqdn_resolution_consistency&gt;</code> appends entry to same line in hosts file.

## Remote Access - IPsec VPN

Bug ID	Description
584953	Split tunnel does not work when choosing manual IP address.
1074153	FortiClient GUI has issues with IPsec VPN IKEv2 over TCP configuration.
1079047	FortiClient (Windows) on Windows 11 with Intel Wi-Fi 7 BE200 Wi-Fi network adapter cannot connect to IPsec VPN.
1085855	Saved password becomes empty after reboot when multifactor authentication (MFA), autoconnect, and client certificate are enabled.
1091700	LDAP traffic volume is high when endpoint is connected to tunnel.
1095388	FortiClient does not follow EMS setting for <code>&lt;xauth_timeout&gt;</code> .
1099714	When using IPsec VPN with RADIUS authentication (Microsoft Entra ID), FortiClient (Windows) clears password field when asking for MFA.
1099737	FortiClient (Windows) sends excessive LDAP queries.
1115380	IKEv2 IPsec VPN gets stuck on connected after resuming from CLIENT_RESUME if SA is expired on FortiGate.
1123378	Abnormal FortiClient (Windows) dead peer detection behavior occurs after FortiClient (Windows) phase1 IKE SA is rekeyed (FortiClient (Windows) sending create-child request).
1121087	Subnet exclusion does not work properly in dialup IPsec VPN.

## Remote Access - SSL VPN

Bug ID	Description
909244	Split-DNS name resolution fails after SSL VPN is up for a few minutes, until it runs <code>ipconfig /flushdns</code> .

Bug ID	Description
909755	SSL VPN split tunnel does not work for Microsoft Teams.
1052659	FortiClient (Windows) gets stuck at 98% and cannot reconnect when endpoint is left in standby or sleep for couple of hours until reboot.
1070783	SSL VPN cannot connect. After successful authentication, FortiClient (Windows) redirects to connection page multiple times.
1081068	SSL VPN does not connect on Windows Server 2019.
1085875	FortiClient does not apply regular expressions (regex) on some Remote Access profiles but applies regex on copy of the same profile.
1098696	FortiClient (Windows) cannot connect to VPN tunnel when the computer is connected to iPhone hotspot and connection attempt gets stuck at 98%.
1101287	SSL VPN certificate warning occurs for valid certificates if switching between valid certificates in FortiGate.
1103361	FortiClient (Windows) fails to autoconnect after deploying FortiClient (Windows) on machine that enabled passwordless automatic login.
1105603	There is a race condition between Windows autologin and autoconnect while connecting to SSL VPN tunnel.
1110569	FortiClient (Windows) connects to pre-login tunnel after user logs in and connects to telemetry.
1111305	Autoconnect is triggered when endpoint wakes from sleep or powers on in on-Fabric location.

## Security posture tags

Bug ID	Description
1027851	FortiClient (Windows) loses security posture tag based on combined rules and requires reinstalling FortiClient.
1103074	Endpoint has both individual security posture tags but is missing composite tag.

## Vulnerability Scan

Bug ID	Description
1054778	FortiClient (Windows) displays incorrect detected version on Vulnerability Scan report

Bug ID	Description
	GUI.
1092036	FortiClient logs for the detected vulnerability shows only UUID code as the detectedpath instead of the application's actual path.

## Web Filter and plugin

Bug ID	Description
753066	Web Filter extension requires migration to Manifest V3.
1061163	Web Filter plugin blocks some websites after file download.
1090048	Web Filter plugin blocks embedded Google Maps.
1119412	New FortiClient Web Filter extension 7.4.3.1761 causes slowness and websites opening with delay.

## ZTNA connection rules

Bug ID	Description
1094370	If a ZTNA application is configured to use redundant proxy gateways, FortiClient does not fail over to a secondary proxy gateway if the primary proxy gateway fails.

## Common Vulnerabilities and Exposures

FortiClient (Windows) 7.4.3 is no longer vulnerable to the following CVE References:

Bug ID	Description
945320	<a href="#">CVE-2024-50570</a>
1129740	<a href="#">CVE-2025-46373</a>
1147064	<a href="#">CVE-2025-47761</a>

# Known issues

Known issues are organized into the following categories:

- [New known issues on page 23](#)
- [Existing known issues on page 25](#)

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 7.4.3.

### Application Firewall

Bug ID	Description
1106844	Firewall does not block mozi.botnet.

### Endpoint control

Bug ID	Description
1023729	Fortinet Security Fabric status detection via DHCP code or local subnet does not work as expected after connecting to VPN.
1091988	Preconfigured option in the FortiClient installer does not function properly.
1117277	FortiClient fails to get Wi-Fi information from endpoint.

### Malware Protection and Sandbox

Bug ID	Description
1108242	On-demand scan fails to quarantine Eicar files from C drive root folders.
1111311	Removable media access does not work on Windows Server.
1112030	Antimalware detects W32/AI.Pallas.Suspicious. but does not quarantine it.

## Remote Access - IPsec VPN

Bug ID	Description
1102421	IPsec VPN IKEv2 SAML-based authentication is unreliable.
1105003	Machine tunnel persists after hibernation, preventing user tunnel from establishing.
1116375	IPsec VPN IKEv2 with session resumption cannot switch between different Wi-Fi SSIDs.
1133715	Unreliable connection establishment with IKEv2 over TCP.

## Remote Access - SSL VPN

Bug ID	Description
1104520	When trying to connect to VPN, the connection status stuck at 98%.

## Security posture tags

Bug ID	Description
1104084	<i>OS system last update is within 60 days</i> tag does not work as expected.
1115703	Tag rules give illegal format error message with parse failed when != operator is used.

## Vulnerability Scan

Bug ID	Description
1099914	VCM scan runs slowly.
1134845	FortiClient fails to retrieve vulnerability signature updates from FortiManager 7.4.5.

## Web Filter and plugin

Bug ID	Description
1126310	Web Filter incorrectly blocks access to locally downloaded PDF files by treating file paths as unrated URLs.
1122215	When you enable <i>Bypass Private IP</i> , bypassed page displays slowly.

Bug ID	Description
1128043	Web Filter intermittently fails to block restricted websites for off-net users.
1137378	Chrome preloads a website that Web Filter blocks and FortiClient shows block message even if user does not click it.

## ZTNA

Bug ID	Description
1155875	In AVD multi-session with ZTNA and session-based SAML authentication, after the first user logs in, subsequent users are granted access to the RDP resource without being prompted for authentication.

## ZTNA connection rules

Bug ID	Description
1090041	FortiClient (Windows) bypasses access proxies including inline CASB if IPv6 is enabled on Windows network adapter.

## Other

Bug ID	Description
1018097	FortiShield prevents applications from writing to logs.

## Existing known issues

The following issues have been identified in a previous version of FortiClient (Windows) and remain in FortiClient (Windows) 7.4.3.

## Application Firewall

Bug ID	Description
1020282	Application Firewall blocks applications added to the exclusion list.
1069197	Application Firewall does not block peer-to-peer (torrent) traffic.

## Deployment and installers

Bug ID	Description
1104334	Deployment message is in English for PC with local language not set to English.

## GUI

Bug ID	Description
1100909	FortiClient (Windows) language change affects Windows logon screen language.

## Install and upgrade

Bug ID	Description
995379	FortiClient single sign on mobility agent does not properly install on CIS hardened Windows 10 and 11 image.
1106731	When upgraded from 7.4.0 or 7.4.1 to 7.4.3 using .msi files, VM does not restart and FortiClient (Windows) services do not start automatically. <b>Workaround:</b> see <a href="#">Upgrading from previous FortiClient versions on page 12</a> .

## Malware Protection and Sandbox

Bug ID	Description
1098883	Sandbox does not restore file when antivirus is not installed.
1103310	German message on reboot prompt does not show completely.

## Multitenancy

Bug ID	Description
1089156	FortiClient (Windows) automatically switches to default site when EMS enables multitenancy.

## Quarantine management

Bug ID	Description
1072475	FortiClient (Windows) does not block IPv6 traffic when EMS quarantines endpoint.

## Performance

Bug ID	Description
1099258	FortiClient (Windows) causes Windows Defender to have high CPU usage.

## Remote Access

Bug ID	Description
999139	Laptop Wifi DNS setting is stuck in unknown DNS server after FortiClient connects and disconnects IPsec or SSL VPN.

## Remote Access - SSL VPN

Bug ID	Description
930740	FortiClient (Windows) cannot set up SSL VPN if the password contains Polish characters ł, ą, or ń.
976800	Azure automatic login is possible when Microsoft conditional access policy does not allow authentication.
1018817	User must click <i>Save Password</i> to save SAML username.
1024304	FortiClient (Windows) is stuck on token entry page when user clicks <i>Cancel</i> for SSL VPN tunnel connection.
1091993	With <i>Disable Connect/Disconnect</i> on, FortiClient (Windows) loses saved SSL VPN user credentials when waking from sleep.
1111305	Autoconnect triggers when endpoint wakes from sleep or powers on in an on-Fabric location.

## Web Filter and plugin

Bug ID	Description
1084513	Windows 10 users cannot access websites due to Web Filter rating lookup errors.
1101902	Letsignit application cannot authenticate while connected to EMS telemetry.
1106128	FortiClient (Windows) cannot block or warn about unauthorized websites when Web Filter extension is disabled.



# Release Notes

FortiClient (Windows) 7.4.3

