

# Release Notes

## FortiClient (Windows) 7.2.9



**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)



January 12, 2026

FortiClient (Windows) 7.2.9 Release Notes

04-729-1140137-20260112

# TABLE OF CONTENTS

|  |           |
|--|-----------|
| <b>Change log</b> .....                                      | <b>4</b>  |
| <b>Introduction</b> .....                                    | <b>5</b>  |
| Licensing .....  | 5         |
| <b>Special notices</b> .....                                 | <b>6</b>  |
| SAML IdP configuration for Save Password .....               | 6         |
| FortiGuard Web Filtering Category v10 Update .....           | 6         |
| Nested VPN tunnels .....                                     | 6         |
| <b>Installation information</b> .....                        | <b>7</b>  |
| Firmware images and tools .....                              | 7         |
| Upgrading from previous FortiClient versions .....           | 8         |
| Downgrading to previous versions .....                       | 8         |
| Firmware image checksums .....                               | 8         |
| <b>Product integration and support</b> .....                 | <b>9</b>  |
| Language support .....                                       | 10        |
| Conflict with third-party endpoint protection software ..... | 11        |
| Intune product codes .....                                   | 11        |
| <b>Resolved issues</b> .....                                 | <b>13</b> |
| Deployment and installers .....                              | 13        |
| Endpoint control .....                                       | 13        |
| Install and upgrade .....                                    | 13        |
| Remote Access .....  | 14        |
| Remote Access - IPsec VPN .....                              | 14        |
| Remote Access - SSL VPN .....                                | 15        |
| Zero trust network access connection rules .....             | 15        |
| Zero Trust tags .....  | 15        |
| Other .....  | 16        |
| Common Vulnerabilities and Exposures .....                   | 16        |
| <b>Known issues</b> .....                                    | <b>17</b> |
| New known issues .....                                       | 17        |
| Remote Access - IPsec VPN .....                              | 17        |
| Remote Access - SSL VPN .....                                | 17        |
| ZTNA connection rules .....                                  | 17        |
| Existing known issues .....                                  | 18        |
| Avatar and social network login .....                        | 18        |
| Malware Protection and Sandbox .....                         | 18        |
| Remote Access .....  | 18        |
| Remote Access - SSL VPN .....                                | 18        |
| Web Filter and plugin .....                                  | 19        |
| ZTNA connection rules .....                                  | 19        |

# Change log

| Date       | Change description   |
|------------|--|
| 2025-04-09 | Initial release of 7.2.9.  |
| 2025-04-21 | Added <a href="#">Zero trust network access connection rules</a> on page 15.<br>Updated <a href="#">Product integration and support</a> on page 9. |
| 2025-11-18 | Added <a href="#">Common Vulnerabilities and Exposures</a> .   |
| 2026-01-12 | Updated <a href="#">Resolved issues</a> on page 13.  |

# Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 7.2.9 build 1185.

- [Special notices on page 6](#)
- [Installation information on page 7](#)
- [Product integration and support on page 9](#)
- [Resolved issues on page 13](#)
- [Known issues on page 17](#)

Review all sections prior to installing FortiClient.

FortiClient (Windows) 7.2.9 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: 7.2.9.1185

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

## Licensing

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

FortiClient 7.2.9 offers a free VPN-only version that you can use for VPN-only connectivity to FortiGate devices running FortiOS 5.6 and later versions. You can download the VPN-only application from [FortiClient.com](#).

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

# 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.

## 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 following versions:

- 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).

# Installation information

## Firmware images and tools

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

| File                                   | Description   |
|--|---|
| FortiClientTools_7.2.9.1185.zip        | Zip package containing miscellaneous tools, including VPN automation files. |
| FortiClientSSOSetup_7.2.9.1185_x64.zip | Fortinet single sign on (FSSO)-only installer (64-bit).                     |
| FortiClientVPNSetup_7.2.9.1185_x64.exe | Free VPN-only installer (64-bit).   |

EMS 7.2.9 includes the FortiClient (Windows) 7.2.9 standard installer and zip package containing FortiClient.msi and language transforms.

The following tools and files are available in the FortiClientTools\_7.2.9.1185.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://FortiClient.com):

| File                                   | Description                                      |
|--|--|
| FortiClientSetup_7.2.9.1185_x64.zip    | Standard installer package for Windows (64-bit). |
| FortiClientVPNSetup_7.2.9.1185_x64.exe | Free VPN-only installer (64-bit).                |



Review the following sections prior to installing FortiClient version 7.2.9: [Introduction on page 5](#) and [Product integration and support on page 9](#).

---

## Upgrading from previous FortiClient versions

To upgrade a previous FortiClient version to FortiClient 7.2.9, do one of the following:

- Deploy FortiClient 7.2.9 as an upgrade from EMS. See [Recommended upgrade path](#).
- Manually uninstall existing FortiClient version from the device, then install FortiClient (Windows) 7.2.9.

FortiClient (Windows) 7.2.9 features are only enabled when connected to EMS 7.2.

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

You must be running EMS 7.2 before upgrading FortiClient.

## Downgrading to previous versions

FortiClient (Windows) 7.2.9 does not support downgrading to previous FortiClient (Windows) versions.

## Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the [Customer Service & Support portal](#). After logging in, click *Download > Firmware Image Checksum*, enter the image file name, including the extension, and select *Get Checksum Code*.

# Product integration and support

The following table lists version 7.2.9 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> </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 7.2.9 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) 7.2.9.</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> |
| <b>Minimum system requirements</b> | <ul style="list-style-type: none"> <li>• Microsoft Windows-compatible computer with Intel processor or equivalent. FortiClient (Windows) does not support ARM-based processors.</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 (NIC) 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>AV engine</b>                   | 6.00301   |
| <b>VCM engine</b>                  | 2.0040  |
| <b>FortiAnalyzer</b>               | <ul style="list-style-type: none"> <li>• 7.4.0 and later</li> <li>• 7.2.0 and later</li> <li>• 7.0.0 and later</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> <li>• 6.2.0 and later</li> <li>• 6.1.0 and later</li> <li>• 6.0.0 and later</li> </ul>  |
| <b>FortiClient EMS</b>             | <ul style="list-style-type: none"> <li>• 7.4.0 and later</li> </ul>   |

|                           |   |
|---------------------------|---|
|                           | <ul style="list-style-type: none"> <li>• 7.2.0 and later</li> </ul>   |
| <b>FortiManager</b>       | <ul style="list-style-type: none"> <li>• 7.4.0 and later</li> <li>• 7.2.0 and later</li> <li>• 7.0.0 and later</li> </ul>   |
| <b>FortiMonitor agent</b> | 24.3.3  |
| <b>FortiOS</b>            | <p>The following FortiOS versions support ZTNA with FortiClient (Windows) 7.2.9. This includes both ZTNA access proxy and ZTNA tags:</p> <ul style="list-style-type: none"> <li>• 7.4.0 and later</li> <li>• 7.2.0 and later</li> <li>• 7.0.6 and later</li> </ul> <p>The following FortiOS versions support IPsec and SSL VPN with FortiClient (Windows) 7.2.9:</p> <ul style="list-style-type: none"> <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>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> <li>• 3.2.0 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)  | 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.



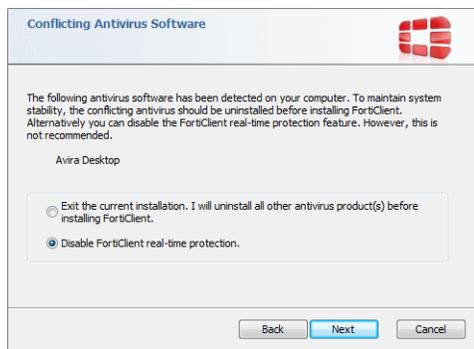
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

## Conflict with third-party endpoint protection software

As a Fortinet Fabric Agent that provides protection, compliance, and secure access, FortiClient may conflict with anti-malware 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's AV feature is enabled.
- If FortiClient's AV feature 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 7.2.9 are as follows:

| Version        | Product code                         |
|----------------|--------------------------------------|
| Enterprise     | B34BA2F5-7F43-481E-90A7-B343A70F2947 |
| VPN-only agent | CEAB81B8-1682-456F-A385-9FDA68C6361D |

| Version                              | Product code                         |
|--------------------------------------|--------------------------------------|
| Private access management-only agent | E6A3800D-EB2E-4CF1-938F-D25DB72B92FA |
| Single sign on-only agent            | BC5AE9F7-1BE3-4C2B-9BA9-D141F31C6DE2 |

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

# Resolved issues

The following issues have been fixed in version 7.2.9. For inquiries about a particular bug, contact [Customer Service & Support](#).

## Deployment and installers

| Bug ID  | Description  |
|---------|--|
| 1104334 | Deployment messages is in English for PC with the local language not set to English. |
| 1113057 | Install does not follow unsupervised scheduled deployment time.                      |

## Endpoint control

| Bug ID  | Description   |
|---------|---|
| 1023729 | When detecting Fortinet Security Fabric status via DHCP code, local subnet does not work as expected after connecting to VPN. |
| 1087936 | EMS disconnect password with special characters does not work.  |

## Install and upgrade

| Bug ID | Description   |
|--------|---|
| 995379 | Fortinet single sign on mobility agent does not properly install on CIS hardened Windows 10 and 11 image. |

## Remote Access

| Bug ID  | Description  |
|---------|--|
| 706804  | Disabling local LAN access does not restrict remote access.  |
| 1027199 | FortiClient (Windows) does not log in to system when using SAML VPN before logon.  |
| 1051036 | FortiClient (Windows) 7.2 does not support IPsec VPN SAML authentication using Electron and must support before logon and after logon scenarios. |
| 1109326 | <keep_fqdn_resolution_consistency>1</keep_fqdn_resolution_consistency> appends entry to same line in hosts file.                                 |
| 1111890 | VPN before logon fails to login to hybrid joined Windows as FortiClient (Windows) uses incorrect username format(username@azure_domain).         |

## Remote Access - IPsec VPN

| Bug ID  | Description  |
|---------|--|
| 1085855 | Saved password becomes empty after reboot when multifactor authentication (MFA), autoconnect, and client certificate are enabled on IPsec VPN.                       |
| 1091700 | High volume of LDAP traffic occurs when endpoint is connected to tunnel.   |
| 1099714 | When connecting to IPsec VPN with RADIUS authentication (Microsoft Entra ID), FortiClient (Windows) clears password field when asking for MFA.                       |
| 1099737 | Excessive FortiClient LDAP queries occur.  |
| 1101972 | Speed on dialup IPsec VPN with GCM cipher is lower compared to AES256.   |
| 1121089 | Listening IP address changes when connected to IPsec VPN.  |
| 1123378 | Abnormal FortiClient (Windows) dead peer detection behavior occurs after FortiClient phase 1 IKE SA is rekeyed (FortiClient (Windows) sending create-child request). |
| 1126275 | Performance issues (limited maximum throughput) occur on IPsec VPN dialup with phase 2 AES-GCM.  |

## Remote Access - SSL VPN

| Bug ID  | Description  |
|---------|--|
| 786869  | FortiClient (Windows) does not support changing SSL VPN virtual adapter MTU dynamically via EMS configuration.                                 |
| 1070783 | VPN cannot connect. After successful authentication, it redirects to the connect page multiple times.  |
| 1085875 | FortiClient ignores partial certificate filters and requires both common name and issuer XML tags.   |
| 1101287 | SSL certificate warning displays for valid certificates if switching between valid certificates in FortiGate.                                  |
| 1103361 | FortiClient (Windows) fails to autoconnect after deploying FortiClient (Windows) on Windows machine that enabled passwordless automatic login. |
| 1105603 | VPN does not autoconnect when automatic login is enabled on Windows endpoint.  |
| 1110569 | FortiClient (Windows) connects to pre-login tunnel after user logs in and connects to telemetry.   |
| 1111300 | SSL VPN tunnel does not connect for almost 15 minutes when coming from sleep mode.   |
| 1111305 | Autoconnect triggers when endpoint wakes from sleep or powers on in on-Fabric location.  |
| 1113004 | SSL VPN gets stuck on 98% if hostname contains characters with umlauts, such as ä, ö, or ü.  |

## Zero trust network access connection rules

| Bug ID  | Description                                     |
|---------|---|
| 1130065 | fortitransctrl.sys causes blue screen of death. |

## Zero Trust tags

| Bug ID  | Description   |
|---------|---|
| 1103074 | If Zero Trust tag Tag_C is configured as applying to endpoints that are tagged with Tag_A and Tag_B, endpoint that is tagged with Tag_A and Tag_B is missing Tag_C. |

## Other

| Bug ID  | Description   |
|---------|---|
| 1131418 | Diagnostic file retrieved from the client via FortiClient Cloud is corrupted. |

## Common Vulnerabilities and Exposures

FortiClient (Windows) 7.2.9 is no longer vulnerable to the following CVE reference. Visit <https://fortiguard.com/psirt> for more information.

| Bug ID  | Description    |
|---------|----------------|
| 1129740 | CVE-2025-46373 |

# Known issues

Known issues are organized into the following categories:

- [New known issues on page 17](#)
- [Existing known issues on page 18](#)

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 7.2.9.

### Remote Access - IPsec VPN

| Bug ID | Description  |
|--------|--|
| 946059 | With VPN up, after signing out from the OS, tunnel disconnects whether <disconnect_on_log_off> is enabled or disabled. |

### Remote Access - SSL VPN

| Bug ID  | Description   |
|---------|---|
| 1132591 | SSL VPN drops when uploading files to SMB file share. |

### ZTNA connection rules

| Bug ID  | Description  |
|---------|--|
| 1114766 | Zero trust network access (ZTNA) bypasses all traffic from FortiClient FortiESNAC process. |

## Existing known issues

The following issues have been identified in a previous version of FortiClient (Windows) and remain in FortiClient (Windows) 7.2.9.

### Avatar and social network login

| Bug ID | Description   |
|--------|---|
| 777013 | Avatar image change or existing does not show on FortiAnalyzer. |

### Malware Protection and Sandbox

| Bug ID  | Description  |
|---------|--|
| 1103310 | Message in German on reboot prompt does not show completely. |

### Remote Access

| Bug ID | Description   |
|--------|---|
| 999139 | Laptop Wi-Fi DNS setting gets stuck in unknown DNS server after FortiClient (Windows) connects to and disconnects from VPN. |

### Remote Access - SSL VPN

| Bug ID  | Description   |
|---------|---|
| 994884  | SSL VPN connections get stuck on 40%.   |
| 997131  | FortiClient (Windows) continuously attempts connection and retains outdated saved password despite autoconnect failure for SSL VPN. |
| 1091993 | With <i>Disable Connect/Disconnect</i> on, FortiClient (Windows) loses saved VPN user credentials when waking from sleep.           |

## Web Filter and plugin

| Bug ID  | Description   |
|---------|---|
| 1106128 | FortiClient cannot block or warn unauthorized websites when Web Filter extension is disabled. |

## ZTNA connection rules

| Bug ID  | Description  |
|---------|--|
| 1090041 | If IPv6 is enabled on the Windows network adapter, access proxies are bypassed, including Inline CASB. |



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.