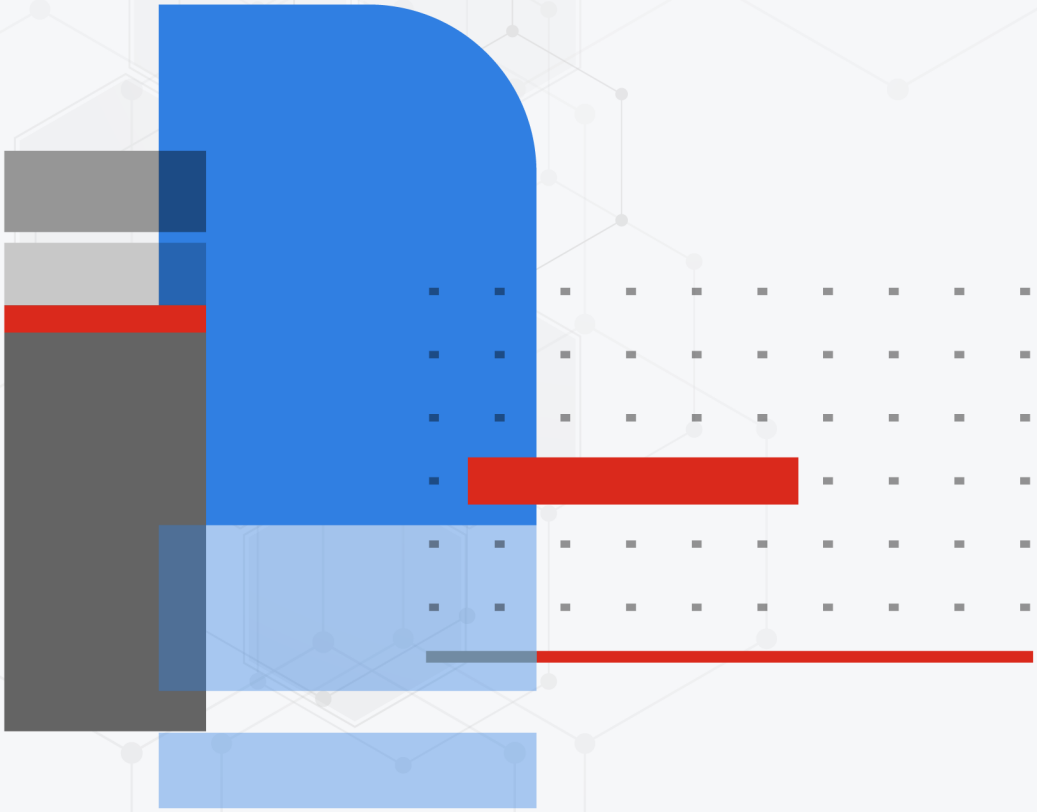
Release Notes

FortiClient (Windows) 7.4.4



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

September 25, 2025
FortiClient (Windows) 7.4.4 Release Notes
04-744-1147559-20250925

TABLE OF CONTENTS

Change log

Date	Change description
2025-09-09	Initial release of 7.4.4.
2025-09-10	Updated Special notices on page 7.
2025-09-11	Updated Special notices on page 7 and Existing known issues on page 24.
2025-09-16	Updated New known issues on page 23.
2025-09-18	Updated New known issues on page 23 and Existing known issues on page 24.
2025-09-22	Added FortiClient (Windows) 7.4.4 GA hotfix 1 on page 7.
2025-09-23	Updated Resolved issues on page 18.
2025-09-25	• Added FortiClient (Windows) 7.4.4 GA hotfix 2 on page 7. • Updated New known issues on page 23.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 7.4.4 build 1887.F.

Review all sections prior to installing FortiClient.

FortiClient (Windows) 7.4.4 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: 7.4.4.1887.F

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

Licensing

See Windows, macOS, and Linux endpoint licenses.

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

Special notices

FortiClient (Windows) 7.4.4 GA hotfix 2

FortiClient (Windows) 7.4.4 GA hotfix 2 (7.4.4.1887.2.8348) was released on September 25, 2025 to address the following issue:

Bug ID	Description
1199087	A crash may occur in the antivirus RTP service. The anti-ransomware service may fail to observe the scan inclusion list.

FortiClient (Windows) hotfixes are accumulated, which means hotfix 2 includes all fixes from hotfix 1.

FortiClient (Windows) 7.4.4 GA hotfix 1

FortiClient (Windows) 7.4.4 GA hotfix 1 (7.4.4.1887.1.8297) was released on September 22, 2025 to address the following issue:

Bug ID	Description
1196704	During a FortiClient EMS switch, the ZTNA certificate from the old EMS is not removed after switching to the new FortiClient EMS server.

This hotfix is available only to customers considering a switch between FortiClient EMS servers. If you need this hotfix, please collect the EMS serial numbers and contact Fortinet Support.

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 the Microsoft 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

No new version of VPN-only agent

FortiClient (Windows) 7.4.4 does not include a new version of the free VPN-only agent as no feature updates were made to the free VPN-only agent between 7.4.3 and 7.4.4. Users can continue to use the FortiClient (Windows) 7.4.3 free VPN-only agent.

No IKEv1 support for IPsec VPN

FortiClient (Windows) 7.4.4 no longer supports IKEv1 for IPsec VPN. Please migrate to using IKEv2 instead.

No IPv6 support for IPsec VPN

FortiClient (Windows) 7.4.4 does not support IPv6 for IPsec VPN due to dual VPN changes. Support may be added in future releases.

What’s new in FortiClient (Windows) 7.4.4

For information about what's new in FortiClient (Windows) 7.4.4, 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-7.4.4-windows-release-notes.pdf	Release Notes file.
FortiClientPAMSetup_7.4.4.1887.F_x64.exe	Privilege access management agent installer (64-bit).
FortiClientSetup_7.4.4.1887.F_ARM64.zip	ARM installer (64-bit).
FortiClientSetUp_7.4.4.1887.F_x64.zip	Installer (64-bit).
FortiClientSSOSetup_7.4.4.1887.F_ARM64.zip	ARM FSSO-only installer (64-bit).
FortiClientSSOSetup_7.4.4.1887.F_x64.zip	Fortinet single sign on (FSSO)-only installer (64-bit).
FortiClientTools_7.4.4.1887.F.zip	Zip package containing miscellaneous tools, including VPN automation files.

EMS 7.4.4 includes the FortiClient (Windows) 7.4.4 standard installer and zip package containing FortiClient.msi and language transforms.

The following tools and files are available in the FortiClientTools_7.4.4.1887.F.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).

File	Description
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.
ReinstallINIC.exe	Remove FortiClient SSLVPN and IPsec network adpater, if not uninstall it via control pannel.
RemoveFCTID.exe	Remove FortiClient UUID.

The following files are available on FortiClient.com:

File	Description
FortiClientSetup_ 7.4.4.1887.F_x64.zip	Standard installer package for Windows (64-bit).

Review the following sections prior to installing FortiClient version 7.4.4: 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 7.4.4 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) 7.4.4:

- 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 7.4.4 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 7.4.4, do one of the following:

- Deploy FortiClient 7.4.4 as an upgrade from EMS. See Recommended upgrade path.
- Manually uninstall existing FortiClient version from the device, then install FortiClient (Windows) 7.4.4.

FortiClient (Windows) 7.4.4 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) 7.4.4 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 7.4.4 product integration and support information:

Desktop operating systems	• Microsoft Windows 11 (64-bit) • Microsoft Windows 10 (64-bit) • Windows 10 IoT Enterprise • Windows 11 IoT Enterprise
Server operating systems	• Microsoft Windows Server 2022 • Microsoft Windows Server 2019 Microsoft Windows Server does not support Application Firewall.

Minimum system requirements	• 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:
	  • Fortinet Security Fabric agent (connection to EMS and Telemetry)
	  • Remote Access (VPN)
	  • Web Filter
	  • Vulnerability Scan
	ARM images are only available for download from the Fortinet Support portal.
	• 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 for network connections
	• Wireless adapter for wireless network connections
	• Adobe Acrobat Reader for viewing FortiClient documentation
	• Windows Installer MSI installer 3.0 or later

FortiClient EMS	7.4.0 and later
FortiOS	• 7.6.0 and later. FortiOS 7.6.3 and later versions do not support SSL VPN tunnel mode. See Migrating from SSL VPN tunnel mode to IPsec VPN. • 7.4.0 and later • 7.2.0 and later • 7.0.0 and later • 6.4.0 and later
AV engine	7.0.38
VCM engine	2.0043

IPS engine	7.6.1040
FortiAnalyzer	• 7.6.0 and later • 7.4.0 and later • 7.2.0 and later • 7.0.0 and later
FortiEDR for Windows	• 5.2.5.0052
FortiAuthenticator	• 6.5.0 and later • 6.4.0 and later • 6.3.0 and later
FortiManager	• 7.6.0 and later • 7.4.0 and later • 7.2.0 and later • 7.0.0 and later
FortiSandbox	• 4.4.0 and later • 4.2.0 and later • 4.0.0 and later

Language support

The following table lists FortiClient language support information:

Language	GUI	XML configuration	Documentation
English	Yes	Yes	Yes
Chinese (simplified)		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.

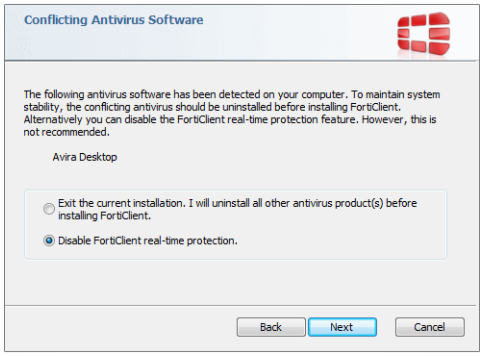
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

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 7.4.4 are as follows:

Version	Product code
Enterprise	C1534669-99D4-459E-8A05-7CD9FE9CD5BB

Version	Product code
Private access management-only agent	8CB9B7D6-22F4-40A2-834B-1B4246EA5EF1
Single sign on-only agent	CCFEAF24-6715-41E7-A915-847F1001D06A

See Configuring the FortiClient application in Intune.

Resolved issues

The following issues have been fixed in version 7.4.4. For inquiries about a particular bug, contact Customer Service & Support.

FortiClient (Windows) 7.4.4 GA hotfix 2

The following issue has been fixed in FortiClient (Windows) 7.4.4 GA hotfix 2 (7.4.4.1887.2.8348).

Bug ID	Description
1199087	A crash may occur in the antivirus RTP service. The anti-ransomware service may fail to observe the scan inclusion list.

FortiClient (Windows) hotfixes are accumulated, which means hotfix 2 includes all fixes from hotfix 1.

FortiClient (Windows) 7.4.4 GA hotfix 1

The following issue has been fixed in FortiClient (Windows) 7.4.4 GA hotfix 1 (7.4.4.1887.1.8297).

Bug ID	Description
1196704	During a FortiClient EMS switch, the ZTNA certificate from the old EMS is not removed after switching to the new FortiClient EMS server.

This hotfix is available only to customers considering a switch between FortiClient EMS servers. If you need this hotfix, please collect the EMS serial numbers and contact Fortinet Support.

FortiClient (Windows) 7.4.4 GA

The following issues have been fixed in FortiClient (Windows)7.4.4 GA build 1887.F.

Deployment and installers

Bug ID	Description
1104334	Deployment messages is in English for the PC with the local language set to non-English.
1189520	FortiClient shows "A JavaScript error occurred in the main process" after upgrade from 7.4.3.

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.
1117277	FortiClient fails to get Wi-Fi information from endpoint.
1157269	DHCP code for on-fabric detection rule fails.
1160546	FortiClient 7.2.9 cannot detect DHCP server for on-fabric rule when the server is reachable.

GUI

Bug ID	Description
1100909	FortiClient Language Change Affects Windows Logon Screen Language.
1118427	FortiTray does not translate the text in the dialog.
1158482	Incorrect characters on scheduled software upgrade popup on FortiClient.

Installation And Upgrade

Bug ID	Description
1144729	FortiClient is not installing on the ARM endpoint using the .exe installer from the InfoSite.

Bug ID	Description
1174966	FortiAuth.exe is missing if FortiClient is installed without the VPN feature.
995379	FSSO Mobility agent does not properly install on CIS hardened Windows 10 and 11 images.

Malware Protection and Sandbox

Bug ID	Description
1103310	German message on reboot prompt does not show completely.
1108242	On-demand scan fails to quarantine Eicar files from C drive root folders.
1125726	FortiClient 7.4.2 PowerShell crashing if Windows Antimalware Scan Interface feature enabled on old computers.
1126582	FortiClient 7.4.2 AV realtime protection blocks PowerShell.
1131405	Unable to detect custom ransomware.
1140744	FortiClient 7.2.8 Malware Custom Scan scans all files and folder on NAS share instead of selected folders.

Privilege Access Management

Bug ID	Description
1140797	Login error at Web "AWS console" using proxy.

Remote Access - IPsec VPN

Bug ID	Description
1068771	Failed to apply DNS suffix search list defined in FortiOS to machine network interface after VPN is up.
1133715	Unreliable connection establishment with IKEv2 over TCP.

Remote Access - SSL VPN

Bug ID	Description
997131	FortiClient keeps attempting and retaining outdated saved password despite auto-connect failure in SSL VPN.
1091993	With *Disable Connect/Disconnect* on, FortiClient (Windows) loses saved SSL VPN user credentials when waking from sleep.
1126919	FortiClient shows username/password instead of smartcard certificates in certain conditions.
1132591	SSL VPN drops when uploading files to SMB file share.
1146281	Authentication prompt on pre-logon machine tunnel VPN.

Vulnerability Scan

Bug ID	Description
1099914	VCM scan running slow in 7.2.5/7.4.0/7.4.1, but normal speed in 7.0.13.
1130643	FortiClient patches the application (Oracle VirtualBox) that is excluded from the vulnerability patch.

Web Filter and plugin

Bug ID	Description
1114688	FortiClient video filter fails to block videos intermittently.
1122215	When *Bypass Private IP* is turned on, bypassed page is displayed with slowness.
1126310	FortiClient Web Filtering incorrectly blocks access to locally downloaded PDF files by treating file paths as unrated URLs.
1137378	Chrome preloads a website which is blocked in WF and FortiClient shows block message even if the user did not click on it.
1156146	Web filter is not working when accessed through a private browser tab.
1160681	FortiClient tries to resolve globalvideoquery.fortinet.net when Video filter is disabled.
1161902	Web filter does not block 2 specific google services (play & myaccount).
1170961	Force_Enable_in_Private mode resets to 1 on reboot.

Zero Trust Network Access (ZTNA) Connection Rules

Bug ID	Description
1114766	FortiClient ZTNA would bypass all TCP traffic from FortiClient FortiESNAC process.
1122544	The ZTNA daemon uses port 8888 to provide web services and should be changed to a random port.
1155036	Forticlient ZTNA TCP fwd SAML session should not start redirect with TCP fwf path.

Security Posture Tags

Bug ID	Description
1115703	Tag rules give illegal format error message with parse failed when not equal != operator is used.
1148246	FortiClient "Sandbox Detection: No malware detected in 7 days" tag does not work as expected.

Known issues

Known issues are organized into the following categories:

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 7.4.4.

Remote Access - IPsec VPN

Bug ID	Description
1114230	FortiClient cannot change radius user expired password on FortiClient IPsec VPN. Fields do not change.
1132631	Failed to validate misconfiguration(e.g EAP disabled) before trying to connect for IKEv2 and SAML authentication.
1151961	IPSEC IKEv2 with an external DHCP server set via DHCP relay to FortiClient never receive the option 12 hostname value.
1167846	FortiClient adds default route in the Windows routing table instead of splitting tunnel routes for IKEv2.
1172487	Subnet exclusion fails in IKEv2 split tunnel.
1180286	ECDSA certificate-based IKEv2 tunnel fails to establish.
1186588	Network lockdown captive portal detection is failing when using an invalid certificate.
1189237	IPsec does not have IPv6 support in 7.4.4 because of dual VPN changes.
1205084	IPsec VPN tunnel that requires client certificate fails to connect after upgrade to 7.4.4. **Workaround:** Re-import the client certificate with the private key.

Remote Access - SSL VPN

Bug ID	Description
1153078	FortiClient does not show any error messages when the VPN credentials are wrong. Bubble notice only shows SSL VPN connection is down.
1179056	Unable to establish SSL VPN while the Zscaler proxy is enabled.
1191512	Unable to establish VPN connection due to 2FA issue.
1198658	SAML-based SSL VPN tunnel does not work when multiple gateways are configured for VPN resilience.

Security Posture Tags

Bug ID	Description
1170327	FortiGate sometimes cannot resolve IP for client in security posture tag after the user disconnects and connects VPN immediately.

Vulnerability Scan

Bug ID	Description
1198602	FortiClient Vulnerability Scan fails to launch on first registration.

Existing known issues

The following issues have been identified in a previous version of FortiClient (Windows) and remain in FortiClient (Windows) 7.4.4.

Malware Protection And Sandbox

Bug ID	Description
1098883	Sandbox does not restore file when antivirus is not installed.

Other

Bug ID	Description
1018097	Fortishield keeps preventing applications from writing to the log files.

Quarantine Management

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

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 - IPsec VPN

Bug ID	Description
1070788	IPsec is disconnected immediately after tunnel is up sometimes when working from home using wifi.
1102421	IPsec IKEv2 SAML based authentication is unreliable.
1105003	Machine tunnel persists after hibernation, preventing user tunnel from establishing.
1116375	IPsec IKEv2 VPN with session resumption is unable to switch between different wifi SSID.

Remote Access - SSL VPN

Bug ID	Description
1018817	User must click *Save Password* to save SAML username.
1024304	FortiClient (Windows) is stuck on token entry page when user clicks *Cancel* for SSL VPN tunnel connection.
976800	Azure automatic login is possible when Microsoft conditional access policy does not allow authentication.

Web Filter And Plugin

Bug ID	Description
1084513	Windows 10 users cannot access websites due to Web Filter rating lookup errors.
1097357	FortiClient web filter cannot block https://chromewebstore.google.com in Edge and Chrome browsers.
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.

Security Posture Tags

Bug ID	Description
1104084	Tag for "OS system last update is within 60 days" is not working as expected.

ZTNA

Bug ID	Description
1008632	When visiting SaaS application web pages using ZTNA, web pages can stall or return an ERR_CERT_COMMON_NAME_INVALID error.

Release Notes

FortiClient (Windows) 7.4.4