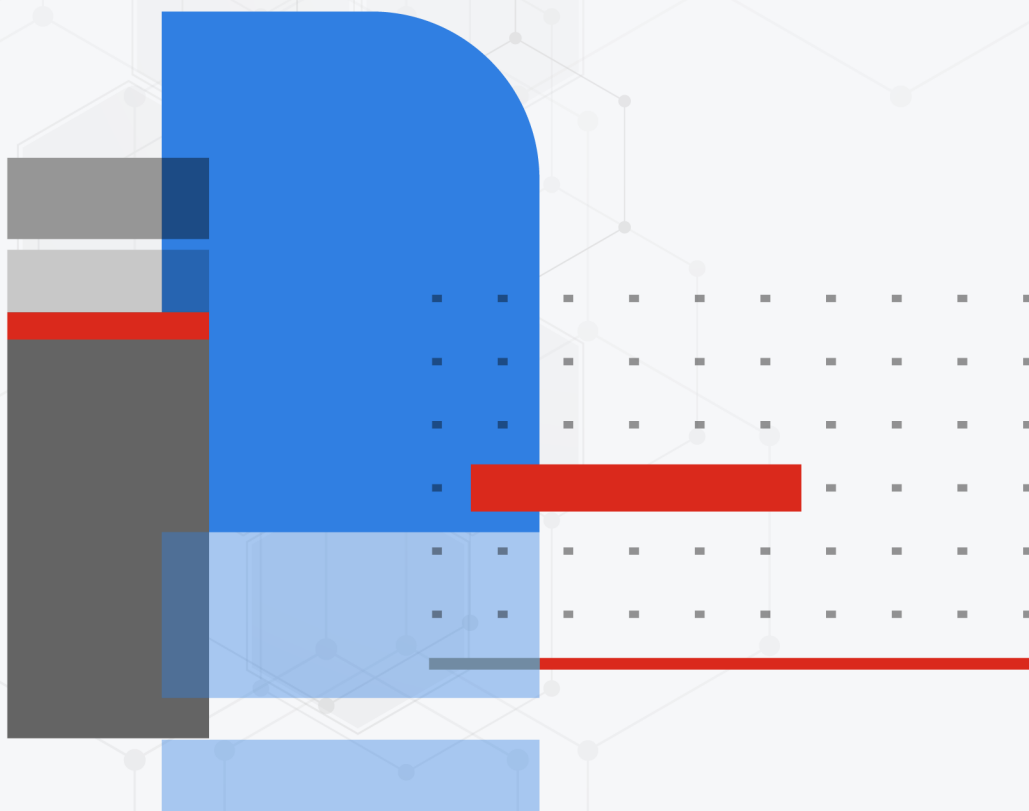




# Release Notes

**FortiClient (Windows) 7.4.1**



**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)



November 01, 2024

FortiClient (Windows) 7.4.1 Release Notes

04-741-1079630-20241101

# 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>
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
<b>What's new in FortiClient (Windows) 7.4.1</b>	<b>9</b>
<b>Installation information</b>	<b>10</b>
Firmware images and tools	10
Upgrading from previous FortiClient versions	11
Downgrading to previous versions	11
Firmware image checksums	11
<b>Product integration and support</b>	<b>12</b>
Language support	13
Conflicts with third party AV products	14
Intune product codes	14
<b>Resolved issues</b>	<b>15</b>
Avatar and social login information	15
Deployment and installers	15
Endpoint control	15
Endpoint management	15
Install and upgrade	16
Logs	16
Malware Protection and Sandbox	16
Onboarding	16
Privilege Access Management	17
Real-time Protection	17
Remote Access	17
Remote Access - IPsec VPN	17
Remote Access - SSL VPN	18
Vulnerability Scan	19
Web Filter and plugin	20
ZTNA connection rules	20
Zero Trust tags	20
Zero Trust telemetry	21
Other	21
<b>Known issues</b>	<b>22</b>
New known issues	22

---

Endpoint control .....	22
Multitenancy .....	22
Quarantine management .....	22
Remote Access - SSL VPN .....	22
Web Filter and plugin .....	23
Other .....	23
Existing known issues .....	23
Application Firewall .....	24
Configuration .....	24
Deployment and installers .....	24
Endpoint control .....	24
Endpoint policy and profile .....	24
Logs .....	24
Malware Protection and Sandbox .....	25
Performance .....	25
Remote Access .....	25
Remote Access - IPsec VPN .....	25
Remote Access - SSL VPN .....	25
Vulnerability Scan .....	26
Web Filter and plugin .....	26
ZTNA connection rules .....	26
Other .....	27
<b>Numbering conventions .....</b>	<b>28</b>

# Change log

Date	Change description
2024-11-01	Initial release of 7.4.1.

# Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 7.4.1 build 1736.

- [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 22](#)

Review all sections prior to installing FortiClient.

FortiClient (Windows) 7.4.1 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 7.4.1 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](https://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) 7.4.1

For information about what's new in FortiClient (Windows) 7.4.1, 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_7.4.1.1736.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_7.4.1.1736_x64.zip	Fortinet single sign on (FSSO)-only installer (64-bit).
FortiClientVPNSetup_7.4.1.1736_x64.exe	Free VPN-only installer (64-bit).

EMS 7.4.1 includes the FortiClient (Windows) 7.4.1 standard installer and zip package containing FortiClient.msi and language transforms.

The following tools and files are available in the FortiClientTools\_7.4.1.1736.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_7.4.1.1736_x64.zip	Standard installer package for Windows (64-bit).
FortiClientVPNSetup_7.4.1.xxxx_x64.exe	Free VPN-only installer (64-bit).



Review the following sections prior to installing FortiClient version 7.4.1: [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 7.4.1, do one of the following:

- Deploy FortiClient 7.4.1 as an upgrade from EMS. See [Recommended upgrade path](#).
- Manually uninstall existing FortiClient version from the device, then install FortiClient (Windows) 7.4.1.

FortiClient (Windows) 7.4.1 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) 7.4.1 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 7.4.1 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 7.4.1 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) 7.4.1.</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>	<ul style="list-style-type: none"><li>• 7.00026</li></ul>
<b>VCM engine</b>	<ul style="list-style-type: none"><li>• 2.0043</li></ul>
<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></ul>
<b>FortiClient EMS</b>	<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>

**FortiOS**

The following FortiOS versions support ZTNA with FortiClient (Windows) 7.4.1. This includes both ZTNA access proxy and ZTNA tags:

- 7.4.0 and later
- 7.2.0 and later
- 7.0.6 and later

The following FortiOS versions support IPsec and SSL VPN with FortiClient (Windows) 7.4.1:

- 7.4.0 and later
- 7.2.0 and later
- 7.0.0 and later
- 6.4.0 and later

**FortiSandbox**

- 4.4.0 and later
- 4.2.0 and later
- 4.0.0 and later
- 3.2.0 and later

**FortiEDR for Windows**

- 5.2.5.0037

## 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.

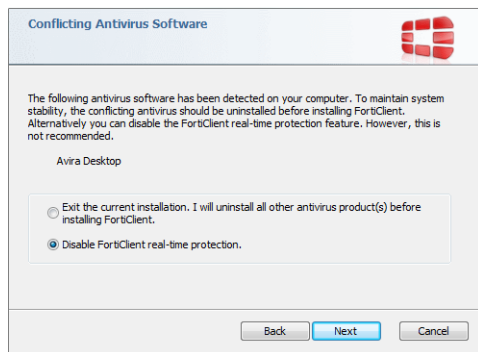


If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

## 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 7.4.1 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 7.4.1. For inquiries about a particular bug, contact [Customer Service & Support](#).

### Avatar and social login information

Bug ID	Description
1075028	Avatar image not displayed in FortiClient console.

### Deployment and installers

Bug ID	Description
1039041	Unable to open FortiClient after getting a scheduled deployment task.
1057992	FortiClient online installer is returning digital a signature invalid error when trying to install.
1076809	Updating from version 7.2.4 to 7.2.5 disables the FortiESNAC on the Microsoft register key.
1083623	FortiClient shows a reboot prompt in a loop after upgrade.

### Endpoint control

Bug ID	Description
975704	FortiClient is not reporting <i>Most Recent Completed Scan</i> time stamp due to incorrect last scan time on the EMS dashboard.
1045373	FortiClient installer created on FortiClient EMS will not auto register if user profile has non-English alphabet in it.

### Endpoint management

Bug ID	Description
1034892	Can't download diagnostic logs for FortiClient from FortiClient EMS.

## Install and upgrade

Bug ID	Description
1035052	FortiClient stops FortiMonitor Agent Service for Windows.
1057335	FortiAuthenticator Windows Agent broke after the FortiClient upgrade.

## Logs

Bug ID	Description
1027844	FortiClient UTM and system event logs do not appear in FortiAnalyzer.
1041193	FortiClient logging to FortiAnalyzer is not working using translated port.

## Malware Protection and Sandbox

Bug ID	Description
946756	USB events are logged when there is an allow rule configured.
948985	AV engine failed to verify the signature after <code>update_task</code> downloaded an AV signature.
996431	Remote NDIS Device cannot be blocked when the net class device is set to block in Removable Media Access function.
1005341	FortiClient stops reporting AV signatures to EMS when <i>Malware Protection</i> tab is hidden.
1034857	FortiClient does not send the file to FortiSandbox for analysis if the hashes are the same.
1060437	FortiClient Cloud Sandbox is not scanning downloaded files from Outlook.

## Onboarding

Bug ID	Description
1018839	FortiClient console fails to open automatically upon clicking the SAML notification.



## Privilege Access Management

Bug ID	Description
797048	The recorded video uploaded shows only a part of the application window.
1045815	FortiPAM browser agent causes customer's PAC file configuration to not work.
1071343	FortiPAM extension doesn't fill credentials on wordpress sites correctly.

## Real-time Protection

Bug ID	Description
1036535	C:\PublishedSites\ files are detected as threats by FortiClient and quarantined.

## Remote Access

Bug ID	Description
933603	SSL VPN connection is being dropped intermittently because of error 0x2747.
970982	FortiClient GUI is getting stuck in the disconnecting screen when connected from the tray.
1010271	When VPN connection name on FortiClient has more than 10 Japanese characters, VPN connection fail.
1052284	Per-machine pre-logon tunnel is not work by per-user auto connect configuration.
1059326	VPN before log on fails with <i>Use Windows Credentials</i> .
1060034	VPN before logon displays the incorrect tunnel list order.
1062785	FortiClient truncates <i>domain\user</i> input during VPN authentication.

## Remote Access - IPsec VPN

Bug ID	Description
969995	Autoconnect is not working reliably with IPsec VPN using credentials, OTP, and client certificate.
973544	IPsec and SAML login doesn't support for <i>Use external browser as user agent</i> for authentication.
974157	IPsec SAML with redundant gateways fails to start.

Bug ID	Description
993280	The FortiGate does not answer on the right port during P2 initiation of Dial-up VPN with NAT-T.
995183	VPN IPsec IKEv2 with RSA authentication asks for FortiToken even if multi-factor authentication is disabled on the FortiGate.
1005025	FortiClient notification <i>VPN blocked, please contact IT administrator</i> prompts again after clicking OK.
1037063	IKEv2 SAML login failed to work if choosing electron as SAML authentication framework and FortiClient failed to validate server certificate.
1058958	Save-Password is not working when we enable <i>Disable Connect/Disconnect</i> from EMS thus failing autoconnect and always up.
1079599	FortiClient IPsec with save username makes a double slash after disconnection.

## Remote Access - SSL VPN

Bug ID	Description
920383	FortiClient always enables <i>Turn off smart multi-homed name resolution</i> on the Windows after successful connection.
922941	Connect to SSL VPN with FQDN resolved to both IPv4 and IPv6 as remote gateway but it stopped at 98 percent.
942668	Split-DNS on SSL VPN is only resolving the 1st DNS server.
964036	Gateway selection based on Ping speed or TCP round trip doesn't work.
986416	FortiClient (Windows) always-up is not working when endpoint wakes up from sleep.
997010	FortiClient fails to establish the SSL VPN tunnel to alternative server when primary server is down using <i>Server</i> method.
1000589	VPN stuck on connecting and error 6005 if SAML takes longer than 60 seconds.
1002456	After upgrading FortiClient to 7.2.3, customize host check fail warning doesn't appear when a tag is on the device.
1006295	FortiClient fails to consistently connect (40%) with DNS round robin of FortiGates.
1007613	<code>sslvpn-ems-sn-check</code> error is not descriptive on SAML VPNSSL connections.
1011690	<code>SamlGetResponseUsingWebBrowser</code> could not start SamlAuthWB.exe.
1012434	SAML VPN username is not saved when the user closes internal SAML authentication window deliberately.
1016971	FortiClient 7.2.4 GA for Windows fails to auto-connect and gets stuck in <i>Connecting</i> state until reboot.
1023437	The VPN connection can not be established automatically after sleep status.

Bug ID	Description
1024973	FortiClient SAML VPN stuck in connecting state when authentication timed out.
1029584	FortiClient doesn't apply FortiOS SSL VPN custom hostcheck-error message rather than using default one.
1034836	SSL VPN (without SAML) throws the credentials prompt repeatedly even if the correct credentials are shared.
1038155	SSL VPN always-up fails when both <i>tunnel-connect-without-reauth</i> and <i>vpn-ems-sn-check</i> are enabled.
1039560	FortiClient does not automatically reconnect to SSL VPN after FortiGate cluster failover.
1039896	Windows fails to auto-connect after switching network adapter with <code>keep running = 1</code> and <code>XAuth</code> is disabled.
1040725	VPN before logon is unable to connect after sleep until 2 or 3 attempts and the first attempt always fails.
1049241	FortiClient does not connect daily and laptop has to be rebooted to connect again.
1049437	FortiClient connects to SSL VPN despite SSL VPN server certificate being revoked.
1050911	SAML authentication login loop occurs with internal browser.
1052659	FortiClient gets stuck at 98% and unable to reconnect when endpoint is left in standby for a couple of hours until reboot.
1056908	SSL VPN connection using FortiClient with SAML opens a duplicate session.
1063310	SSL VPN use machine certificate fails to connect when launched from Fortitray.
1063513	Receive a host check error (-7006) after login if enabling either <i>Realtime Antivirus</i> or <i>both</i> for Hostcheck in SSL VPN portal.
1066122	Random VPN disconnects in some environment with Azure as SAML.
1071790	FortiClient VPN before logon failed with OS host check.
1078571	When auto-connect is enabled and VPN gateway is not reachable, it is stuck in a loop.
1083352	FortiClient does not wait for the On-fabric status check before auto-connect tunnel starts when waking up from sleep.

## Vulnerability Scan

Bug ID	Description
913032	EMS doesn't update the vulnerability events correctly after vulnerability scan is performed from FortiClient.

## Web Filter and plugin

Bug ID	Description
975694	FortiClient blocks Outlook and multiple destinations due unknown category error.
1036511	ChatGPT is identified as <i>Informationstechnologie</i> instead of AI.
1040592	Web Filter plugin requires web browser restart in order to work.
1043986	FortiClient Web Filter is blocking the URL <i>data:application/vnd</i> and exclusions don't work.
1057601	Web Filter browser extension ignores the <i>Bypass Private IP</i> setting during file downloads.
1069196	FortiClient Web Filter is not blocking access to unauthorized site with the Web Filter enabled.
1075358	FortiClient 7.2.5 Web Filter extension blocks some websites that have links to different categories.
1083774	Web Filter may block all sites for up to five minutes when rating error occurs.

## ZTNA connection rules

Bug ID	Description
831943	ZTNA client certificate is not getting removed from user certificate store after FortiClient is uninstalled.
990864	With SAML for ZTNA authentication, after closing the first session, the second session continues to request credentials.
1013466	FortiClient ZTNA destination for custom app with .NET8 Maui not working as expected.
1022199	FortiClient endpoint failed to handle DNS request for IPv6 and Tkey packets.
1031633	<i>ZTNA Destinations</i> is not working when using the SAP GUI.
1054366	VPN status is displayed incorrectly and ZTNA sometimes fails to pop up authentication.

## Zero Trust tags

Bug ID	Description
956947	Zero Trust tags disappearing from FortiClient avatar if a different user logs in to Windows machine.
988510	Windows OS tag with <i>latest update within 30 days</i> is not working reliably.

## Zero Trust telemetry

Bug ID	Description
1055456	Endpoint re-registers back with old EMS cloud instance when using the switch option.
1077673	FortiClient refusing to connect with EMS cloud due to authentication error.

## Other

Bug ID	Description
984763	<code>NETIO.SYS/FortiWF2.sys</code> causes BSODs on Windows 10 with FortiClient 7.0.10.

# Known issues

Known issues are organized into the following categories:

- [New known issues on page 22](#)
- [Existing known issues on page 23](#)

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 7.4.1.

### Endpoint control

Bug ID	Description
1071613	FortiClient received onnet.plain file in plain text.

### Multitenancy

Bug ID	Description
1089156	FortiClient automatically switches to the default site when multitenancy is enabled on the EMS.

### Quarantine management

Bug ID	Description
1072475	FortiClient is not blocking IPv6 traffic when the endpoint is quarantined.


### Remote Access - SSL VPN

Bug ID	Description
976800	FortiClient Azure autologin possible although Microsoft's Conditional Access Policy does not allow authentication.

Bug ID	Description
1010455	SAML authentication prompt timeout is set to default 300s and does not reflect the <code>remoteauthtimeout</code> configured on the FortiGate.
1024304	FortiClient SSL VPN is stuck on enter token page when clicking <i>Cancel</i> .
1070783	VPN is not able to connect. After successful authentication it redirects to the connect page multiple times.

## Web Filter and plugin

Bug ID	Description
1061163	FortiClient Web Filter plugin blocks some websites after a file download.
1092404	Web Filter would make the webpage fail to load when the Web Filter plugin was disabled.



Two Workarounds are available for this mantis:

1. Enable the Web Filter plugin as reported by mantis 0549309.
2. Manually add XML in EMS Profile with following two settings, and set to 1.

```
<forticlient_configuration>
<webfilter>
<interception_mode>1</interception_mode>
<out_of_band_injection>1</out_of_band_injection>
```

## Other

Bug ID	Description
1038864	BSOD caused by FortiFilter.
1045956	NVR3 (CCTV) software having trouble with the presence of FortiClient.
1081675	<code>FortiAptFilter.sys</code> causing BSOD when FortiClient is upgraded to 7.2.5.

## Existing known issues

The following issues have been identified in a previous version of FortiClient (Windows) and remain in FortiClient (Windows) 7.4.1.

## Application Firewall

Bug ID	Description
1069197	FortiClient application firewall doesn't block P2P (Torrent) traffic.

## Configuration

Bug ID	Description
1087936	EMS disconnect password with some special characters doesn't work.
1089575	On Windows 11, 24H2 DNS for Ethernet Adapter is getting removed when FortiClient v7.2.5 is installed and connected to EMS.

## Deployment and installers

Bug ID	Description
1085559	FortiClient upgrade fails due to corrupted cabinet file <code>common.cab</code> .

## Endpoint control

Bug ID	Description
1012497	FortiClient should send empty <code>USER/USER_SID</code> to EMS when the user logs out for Domain/Azure users.
1084906	On-fabric Detection Rule (DHCP Server) does not work with IPsec tunnel on Windows 11.
1086370	Unverified FortiClient doesn't prompt for verification after upgrade with user verification invite being part of the installer.

## Endpoint policy and profile

Bug ID	Description
1082916	Invalid ZTNA destination in the form of <code>*.example.private</code> wildcard FQDN.

## Logs

Bug ID	Description
1082408	FortiClient tries to upload logs to FortiAnalyzer via both SSL enabled TCP 514 and syslog format UDP 514 at the same time.



## Malware Protection and Sandbox

Bug ID	Description
1039172	FortiClient non-manual files send for scanning to on-prem Sandbox don't show <i>ATP Scan</i> dialog.

## Performance

Bug ID	Description
1086957	FortiClient Network Access Control (FortiEsNac daemon) is causing high CPU on Windows server 2019.

## 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.
1084551	Endpoint auto-connects FortiSASE VPN when auto-connect VPN is disabled from FortiSASE.
1086017	Failed to prompt Host Check Fail warning even though secure remote access is on and endpoint is non-compliant.

## Remote Access - IPsec VPN

Bug ID	Description
971554	FortiClient sends Access-Request even though password renewal was canceled.
1003308	FortiClient attempts to autoconnect Azure Autoconnect tunnels when the logged-in user is not an Azure user.
1036306	IPsec VPN fails to autoconnect after installing EMS-repackaged FortiClient installer when <code>autoconnect_on_install</code> is enabled.
1070788	IPsec is disconnected immediately after tunnel is up sometimes when working from home using WiFi.

## 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
930740	Unable to setup SSL VPN if the password contains Polish characters "ł", "ą", or "ń".
950787	Domain filter cannot block access for <i>specific server FQDN</i> .
1018817	User must click <i>Save Password</i> to save SAML username.
1019876	User gets stuck at 40% connectivity when connecting to any VPN.

## Vulnerability Scan

Bug ID	Description
1077070	FortiClient is not reporting Windows OS vulnerabilities or security patches.
1092036	FortiClient logs for the detected vulnerability shows only UUID code as the <code>detectedpath</code> instead of the application's actual path.

## Web Filter and plugin

Bug ID	Description
951749	FortiClient displays notification message to enable <i>Allow in Incognito</i> even though it is already enabled.
1083327	FortiClient Web Filter extension anomaly in Chrome and Edge when downloading PDFs.
1084513	Windows 10 FortiClient users unable to access internal and external websites due to Web Filter rating look up errors.
1090048	FortiClient Web Filter plugin blocks embedded Google Maps.

## ZTNA connection rules

Bug ID	Description
919832	ZTNA stopped working after days with the error message <i>No ZTNA client certificate was provided</i> .
965630	Windows 11 with FortiClient 7.2.2 installed will fail to register DNS via secure DDNS.
977407	ZTNA TCP-forwarding with authentication is not working properly for SaaS and SaaS group applications.
1001116	FortiClient requests SAML credentials after network change in ZTNA connections.

## Other

Bug ID	Description
1086992	BSOD caused by <code>fortisniff2.sys</code> .

# Numbering conventions

Fortinet uses the following version number format:

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

Example: 7.4.1.15

- 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) 7.4.1**

