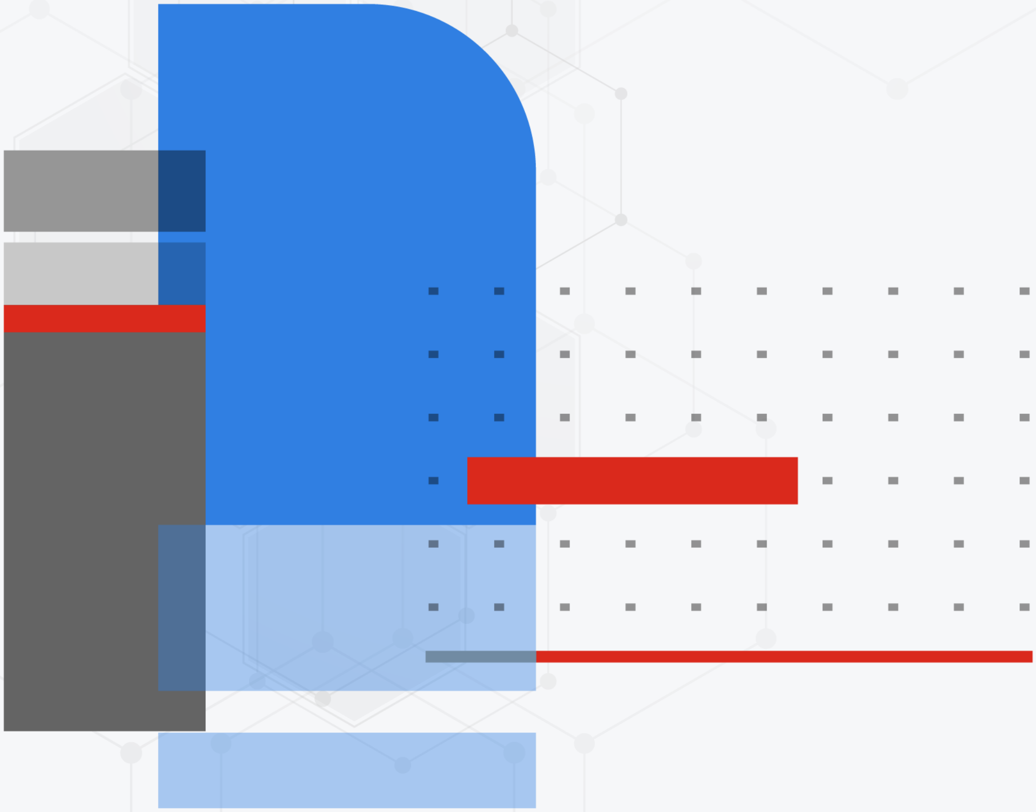
FORTINET

Release Notes

FortiClient (Windows) 7.4.6



March 24, 2026
FortiClient (Windows) 7.4.6 Release Notes
04-746-1252781-20260324

TABLE OF CONTENTS

Change log

Date	Change description
2026-03-17	Initial release of 7.4.6.
2026-03-18	Updated Special notices on page 7.
2026-03-24	Updated Existing known issues on page 21.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 7.4.6 build 2001.M.

- Special notices on page 7
- What’s new in FortiClient (Windows) 7.4.6 on page 9
- Installation information on page 10
- Product integration and support on page 13
- Resolved issues on page 17
- Known issues on page 21

Review all sections prior to installing FortiClient.

FortiClient (Windows) 7.4.6 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: 7.4.6.2001.M

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

Upgrade recommended

FortiClient (Windows) 7.4.6 has been updated to recognize newly issued April 16, 2026 Digicert CA used by FortiGuard Anycast servers (see Resolved issues on page 17). We recommend upgrading your existing 7.4 deployments to 7.4.6 to take advantage of this change. See CSB-260303-1 for more information.

IPv6 support for IPsec VPN

FortiClient (Windows) 7.4.6 adds back IPv6 support for IPsec VPN.

No more support for `#username#` and `#password#` placeholders in on_connect and on-disconnect scripts for VPN

FortiClient (Windows) 7.4.5 or later do not support the `#username#` and `#password#` placeholders in on_connect and on-disconnect scripts which are executed when the VPN tunnel is connected or disconnected.

No new version of VPN-only agent

FortiClient (Windows) 7.4.4 to 7.4.6 do 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 7.4.6. Users can continue to use the FortiClient (Windows) 7.4.3 free VPN-only agent.

No IKEv1 support for IPsec VPN

Starting from 7.4.4, FortiClient (Windows) does not support IKEv1 for IPsec VPN. Please migrate to using IKEv2 instead.

No support for concurrent third-party tunneling or proxy clients

Using third-party tunneling or proxy clients (including VPN, DNS, HTTP(s), SOCKS, ZTNA or PAC files) in parallel or nested combination with FortiClient's VPN, ZTNA or Web Filter is not recommended nor supported.

No support for ZTNA TCP forwarding on Windows WSL2

FortiClient (Windows) does not support ZTNA TCP forwarding on Windows WSL2. As a workaround, use WSL1 or install FortiClient Linux directly within the Ubuntu environment in WSL.

What’s new in FortiClient (Windows) 7.4.6

For information about what's new in FortiClient (Windows) 7.4.6, 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-7.4.6-windows-release-notes.pdf	Release Notes file.
FortiClientPAMSetup_7.4.6.2001.M_x64.exe	Privilege access management agent installer (64-bit).
FortiClientSetup_7.4.6.2001.M_ARM64.zip	ARM installer (64-bit).
FortiClientSetUp_7.4.6.2001.M_x64.zip	Installer (64-bit).
FortiClientSSOSetup_7.4.6.2001.M_ARM64.zip	ARM FSSO-only installer (64-bit).
FortiClientSSOSetup_7.4.6.2001.M_x64.zip	Fortinet single sign on (FSSO)-only installer (64-bit).
FortiClientTools_7.4.6.2001.M.zip	Zip package containing miscellaneous tools, including VPN automation files.

EMS 7.4.6 includes the FortiClient (Windows) 7.4.6 standard installer and zip package containing FortiClient.msi and language transforms.

The following tools and files are available in the FortiClientTools_7.4.6.2001.M.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.
ReinstallNIC.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_7.4.6.2001.M_x64.zip	Standard installer package for Windows (64-bit).

Review the following sections prior to installing FortiClient version 7.4.6: Introduction on page 6, Special notices on page 7, and Product integration and support on page 13.

Upgrading from previous FortiClient versions

Upgrading from FortiClient (Windows) 7.4.0 or 7.4.1 to 7.4.6 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) 7.4.6:

- 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 7.4.6 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 7.4.6, do one of the following:

- Deploy FortiClient 7.4.6 as an upgrade from EMS. See Recommended upgrade path.
- Manually uninstall existing FortiClient version from the device, then install FortiClient (Windows) 7.4.6.

FortiClient (Windows) 7.4.6 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) 7.4.6 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 7.4.6 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 2025 • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 FortiClient (Windows) 7.4.6 does not support Guiless (Core) OS. Microsoft Windows Server does not support Application Firewall.
Minimum system requirements	• Microsoft Windows-compatible computer with Intel or ARM-based processors or equivalent. 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 • 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	• 7.4.6 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
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
FortiEDR for Windows	5.2.8.0044
FortiAuthenticator	8.0.0 and later 6.6.0 and later 6.5.0 and later
FortiManager	7.6.0 and later 7.4.0 and later 7.2.0 and later
FortiSandbox	5.0.0 and later 4.4.0 and later 4.2.0 and later

Language support

The following table lists FortiClient language support information:

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

No support for multi-user sessions

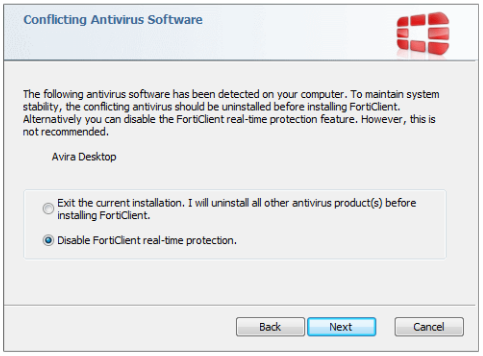
FortiClient (Windows) does not support multi-user sessions using terminal servers, multi-session OSes, or via user switch.

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.



Conflicting Antivirus Software

The following antivirus software has been detected on your computer. To maintain system stability, the conflicting antivirus should be uninstalled before installing FortiClient. Alternatively you can disable the FortiClient real-time protection feature. However, this is not recommended.

Avira Desktop

○ Exit the current installation. I will uninstall all other antivirus product(s) before installing FortiClient.

● Disable FortiClient real-time protection.

Intune product codes

Deploying FortiClient with Intune requires a product code. The product codes for FortiClient 7.4.6 are as follows:

Version	Product code
Enterprise	2A74516F-E643-4C78-93EE-786F06F78340

Version	Product code
Private access management-only agent	68D75EA7-9778-489B-9E2D-247C9F71A019
Single sign on-only agent	EC217288-43B9-4E63-AE08-5FD1E0E9F7A8

See Configuring the FortiClient application in Intune.

Resolved issues

The following issues have been fixed in version 7.4.6. For inquiries about a particular bug, contact Customer Service & Support.

Deployment and Installers

Bug ID	Description
1178692	EMS deployment to update FortiClient feature sets for the same FortiClient version fails unless the initial deployment was done using the EMS-generated FortiClient EXE installer or the MSI file (rather than the MST file).
1232032	FortiClient upgrade from PAM-only 7.4.4.1887 to SSO+PAM 7.4.5.1947 fails with “Setup Wizard ended prematurely". **Workaround:** Upgrade to 7.4.5 without using the TRANSFORMS file generated by the config util.
1247941	EMS deployment for the same FortiClient version but different FortiClient feature sets fails because cached mst file is reused.

GUI

Bug ID	Description
1216497	FortiClient incorrectly display French message during authentication.

Installation and Upgrade

Bug ID	Description
1226762	Cannot install or launch FortiClient on AMR64 Windows. **Workaround**: Manually install the latest release of Microsoft Visual C++ Redistributable (version 14.50+).

Malware Protection

Bug ID	Description
1228642	FortiClient RTP cannot block files copied to endpoint using Shared Folder.

Privilege Access Management

Bug ID	Description
1245812	FortiClient fails to send video uploading chunks to PAM for WinSCP launcher.

Remote Access

Bug ID	Description
1228751	VPN pop-ups still appear when "Suppress VPN notifications" is enabled in remote access profile and "Show bubble notifications" is disabled in System Settings profile.
1252602	VPN tunnels with "VPN before logon" enabled shows the SAML authentication prompt window twice.

Remote Access - IPsec VPN

Bug ID	Description
1232949	Support "no_dns_registration" in dual VPN IPsec implementation.
1190628	SMB traffic is leaked to SASE IPsec VPN full tunnel despite the configuration of subnet in *Steering bypass destination*.
1116375	IPsec IKEv2 VPN with session resumption is unable to switch between different wifi SSID.
1119728	Before VPN is established, if "TCP/IP Settings > register this connection's address in DNS server" is unselected for both local and FortiClient virtual Adapter on the device after VPN is up, the option will remain unselected regardless of the value of no_dns_registration.

Bug ID	Description
1189237	IPsec does not have IPv6 support in 7.4.4 because of dual VPN changes.
1192355	"SIA-IPSec is down (NetworkOtherError)" when disable_internet_check=1 and the endpoint is not connected to the Internet.
1197941	Session resumption does not work. FortiClient disconnect IKEv2 VPN with DPD timeout even with physical NIC disconnected.
1206610	SIA IPsec VPN cannot connect with endpoint using dual-stack and ISP performing DNS64.
1207277	IPsec VPN does not connect after upgrade (VpnParameterConfigError).
1209318	Failover SSL VPN connection is terminated when the initial popup from IPsec VPN failure is closed.
1211272	IPSec VPN should support client resume when the IP changes.
1214677	FortiClient fails to establish IPsec tunnel if certificate's common name uses German umlauts.
1236111	No downstream traffic after tunnel is up when IPsec VPN gateway is behind NAT device with VIP mapping.
1236397	On-connect script for Windows stopped working after FortiClient upgrade.
1236854	MS Teams exception for Steering bypass does not work.
1237189	"Failed to install VPN configuration" error after "dns_priority" is changed from EMS when tunnel is up.
1237853	When Auto-Connect is enabled and WebView2 + Web Browser for SAML authentication is used, if the user closes the SAML authentication window at system startup, FortiClient does not retry the authentication process and the endpoint does not reconnect until the next reboot.
1239093	IPsec VPN tunnels with EAP enabled fail to connect with local or LDAP user authentication before logon if *Save Username* is enabled.
1241832	IPsec crash because of too many subnets configured.
1242911	FortiClient does not autoconnect for IPsec tunnels on Windows Server 2019.
1246553	FortiClient does not show MAC address of Fortinet VPN-V Network Adapter.
1248046	IPSec VPN connection issue when "Validate IKE Phase1 cert hostname" is enabled and multiple gateways configured.
1251773	Subnet Exclusion does not work properly in dial-up IPsec.
1253023	"VPN before logon" does not work as expected for VPN tunnels with EAP Azure SAML and Certificate configured.

Remote Access - SSL VPN

Bug ID	Description
1169395	FortiClient is unable to connect to SSL VPN from Hong Kong.
1186762	Forticlient fails to resolve DNS via TCP when the endpoint is EntraID joined.
1200862	SSL VPN tunnel cannot establish: the *Connect* button does not trigger VPN connection.
1229163	Unable to access any websites in the browser after switching from LAN to Wi-Fi.

Web Filter and plugin

Bug ID	Description
1255625	FortiClient (Windows) fails to recognize the newly issued April 16, 2026 Digicert CA used by FortiGuard Anycast servers, which results in failed communication for the following updates: • Web Filter rating • Video Filter rating • Split VPN using ISDB • Signature and engine updates See CSB-260303-1 for more information.
1216649	Poor performance when loading websites in browsers using the web filter extension.
1210804	The web filter extension remains in the browser's extension list after FortiClient is uninstalled.

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.

Known issues

Known issues are organized into the following categories:

- New known issues on page 21
- Existing known issues on page 21

To inquire about a particular bug or to report a bug, contact Customer Service & Support.

New known issues

No new issues have been identified in version 7.4.6.

Existing known issues

The following issues have been identified in a previous version of FortiClient (Windows) and remain in FortiClient (Windows) 7.4.6.

Endpoint control

Bug ID	Description
949324	Re-authentication error for verified registered FortiClient endpoints with the SAML or Entra ID user verification type when *User Verification Period* is enabled in EMS.
1222340	FortiClient EMS Cloud registration failures via Intune and Entra ID integration.
1222324	When deploying FortiClient using Windows Autopilot, EMS invitation is lost if the initial EMS user verification fails.
1213829	When "User verification period" is disable in EMS, the "auth_period" registry in FortiClient is not set to 0.

Malware Protection

Bug ID	Description
1098883	Sandbox does not restore file when antivirus is not installed.
1236056	Driver (3M PRF UMDF USB driver) is impacted when FortiClient is running on PC.

Quarantine Management

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

Remote Access - IPsec VPN

Bug ID	Description
1105003	Machine tunnel persists after hibernation, preventing user tunnel from establishing.
1114230	FortiClient cannot change radius user expired password on FortiClient IPsec VPN. Fields do not change.
1168839	EMS IPsec VPN drops when uploading large files via SMB.
1102421	IPsec IKEv2 SAML-based authentication is unreliable.
1151961	IPsec IKEv2 with an external DHCP server set via DHCP relay to FortiClient never receives the option 12 hostname value.

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.
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.

Bug ID	Description
1190598	Personal SSL VPN created with the "Save Login" option and a pre-entered username fails to establish.
1233683	Unable to connect with certificate in USB Smart Card (e.g.FTK310/300) because of failing to prompt box for PIN.

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.
1215190	The web filter extension does not support in-app request blocking due to MV3 limitation.

Security Posture Tags

Bug ID	Description
1104084	Tag for "OS system last update is within 60 days" is not working as expected.
1201729	The "AntiVirus Software" tag is not assigned as expected after adding a tagging rule for it.

ZTNA TCP/UDP Forwarding

Bug ID	Description
1214738	ZTNA driver fortitransctrl causes network error during file downloading.

Vulnerability Scan

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

Other

Bug ID	Description
1018097	Fortishield keeps preventing applications from writing to the log files.
1189783	Forticlient FSSOMA does not send the AzureUserInfo to FortiAuthenticator intermittently.

Release Notes

FortiClient (Windows) 7.4.6