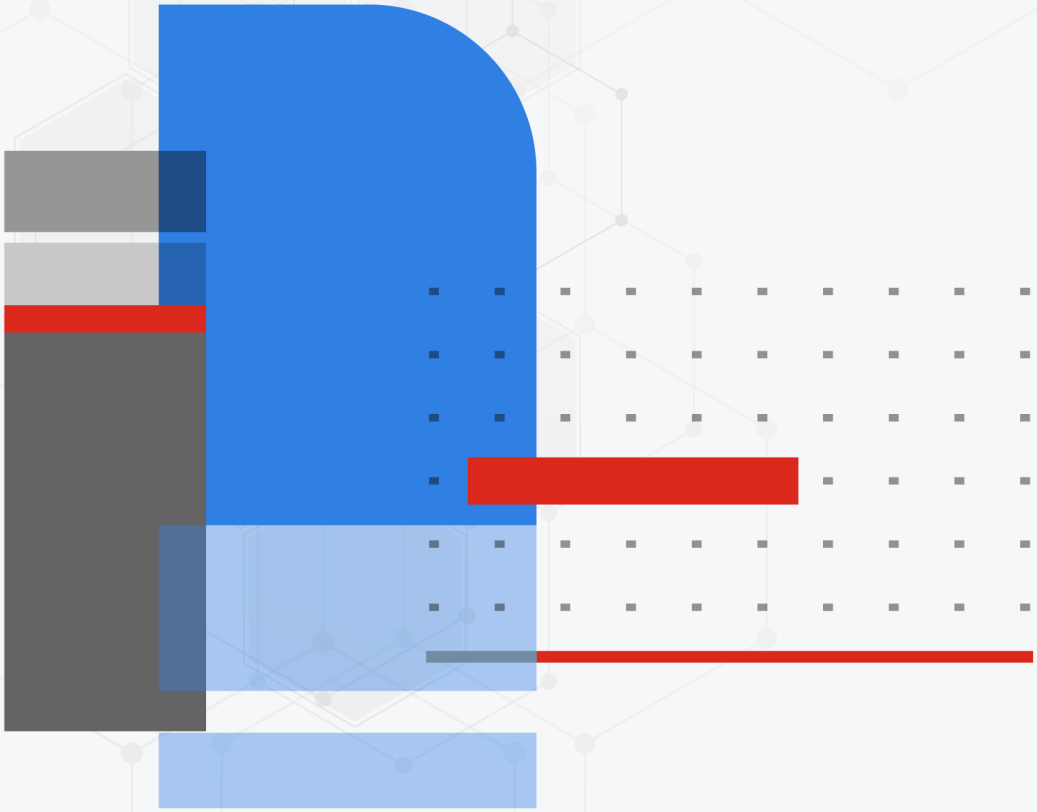
Release Notes

FortiClient (Windows) 7.4.7



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

May 19, 2026
FortiClient (Windows) 7.4.7 Release Notes
04-747-1284962-20260519

TABLE OF CONTENTS

Change log

Date	Change description
2026-04-27	Initial release of 7.4.7.
2026-05-07	Updated Existing known issues on page 16.
2026-05-19	Updated Existing known issues on page 16.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 7.4.7 build 2003.M.

Review all sections prior to installing FortiClient.

FortiClient (Windows) 7.4.7 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: 7.4.7.2003.M

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

Licensing

See Windows, macOS, and Linux endpoint licenses.

FortiClient (Windows) offers a separate free installer for the single sign on mobility agent. This agent does not include technical support.

Special notices

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 7.4.7 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 7.4.7. 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.

Installation information

Firmware images and tools

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

File	Description
forticlient-7.4.7-windows-release-notes.pdf	Release Notes file.
FortiClientPAMSetup_7.4.7.2003.M_x64.exe	Privilege access management agent installer (64-bit).
FortiClientSetup_7.4.7.2003.M_ARM64.zip	ARM installer (64-bit).
FortiClientSetUp_7.4.7.2003.M_x64.zip	Installer (64-bit).
FortiClientSSOSetup_7.4.7.2003.M_ARM64.zip	ARM FSSO-only installer (64-bit).
FortiClientSSOSetup_7.4.7.2003.M_x64.zip	Fortinet single sign on (FSSO)-only installer (64-bit).
FortiClientTools_7.4.7.2003.M.zip	Zip package containing miscellaneous tools, including VPN automation files.

EMS 7.4.7 includes the FortiClient (Windows) 7.4.7 standard installer and zip package containing FortiClient.msi and language transforms.

The following tools and files are available in the FortiClientTools_7.4.7.2003.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 (32-bit).
CertificateTestx64.exe	Test certificate (64-bit).

File	Description
CertificateTestx86.exe	Test certificate (32-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_7.4.7.2003.M_x64.zip	Standard installer package for Windows (64-bit).

Review the following sections prior to installing FortiClient version 7.4.7: Introduction on page 5, Special notices on page 6, and Product integration and support on page 11.

Upgrading from previous FortiClient versions

Upgrading from FortiClient (Windows) 7.4.0 or 7.4.1 to 7.4.7 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) 7.4.7:

- 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 7.4.7 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 7.4.7, do one of the following:

- Deploy FortiClient 7.4.7 as an upgrade from EMS. See Recommended upgrade path.
- Manually uninstall existing FortiClient version from the device, then install FortiClient (Windows) 7.4.7.

FortiClient (Windows) 7.4.7 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) 7.4.7 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 7.4.7 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) 7.4.7 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	• 7.4.7 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

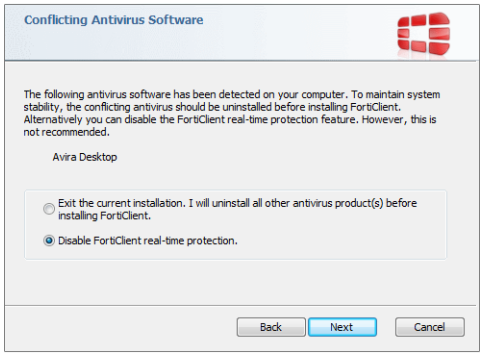
FortiClient (Windows) does not support multi-user sessions using terminal servers, multi-session OSes, or via user switch.

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.



Intune product codes

Deploying FortiClient with Intune requires a product code. The product codes for FortiClient 7.4.7 are as follows:

Version	Product code
Enterprise	5D667F30-8903-457D-99E7-DB56AE15A566

Version	Product code
Private access management-only agent	CFF9A47A-B477-4CAF-90CD-30E48C074AFF
Single sign on-only agent	10DEB330-9FEF-46E8-929C-A213BFB5572E

See Configuring the FortiClient application in Intune.

Resolved issues

The following issues have been fixed in version 7.4.7. For inquiries about a particular bug, contact Customer Service & Support.

Endpoint control

Bug ID	Description
1282506, 1283448	Connectivity issues and high disk usage after the upgrade to 7.4.6.

Malware Protection

Bug ID	Description
1272585	Lots of crashes for `fortiusbmon.exe`.

Remote Access - IPsec VPN

Bug ID	Description
1265871	"VpnConfigureParameterError" when trying to connect to IPsec VPN.
1270466	Unable to connect to IPv6 tunnel successfully when a temporary IPv6 address exists.

Other

Bug ID	Description
1188442	Security best practice: remove weak cipher support.

Known issues

Known issues are organized into the following categories:

- New known issues on page 16
- Existing known issues on page 16

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 7.4.7.

Existing known issues

The following issues have been identified in a previous version of FortiClient (Windows) and remain in FortiClient (Windows) 7.4.7.

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.
1244876	EMS registration with Azure passthrough using invitation code fails for some endpoints.
1249298	On-fabric rule fails to capture DHCP code.

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

Bug ID	Description
1256465	Connection failure using certificates with the common name format "Surname, First Name".
1257682	The VPN *Connect* button does not respond.

Remote Access - IPsec VPN

Bug ID	Description
1238988	FortiClient GUI does not show the VPN as connected while it is connected in the background.
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.
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.
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.
1262856	FortiClient keeps host file entry despite failed VPN connection.

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.

www.fortinet.com