

Release Notes

FortiClient (Windows) 7.0.14



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



March 03, 2025

FortiClient (Windows) 7.0.14 Release Notes

04-7014-1012260-20250303

TABLE OF CONTENTS

Change log	4
Introduction	5
Licensing	5
Special notices	6
FortiGuard Anycast Certificate Expiration	6
Nested VPN tunnels	6
Installation information	7
Firmware images and tools	7
Upgrading from previous FortiClient versions	9
Downgrading to previous versions	9
Firmware image checksums	9
Product integration and support	10
Language support	11
Conflicts with third party AV products	12
Intune product codes	12
Resolved issues	13
Install and upgrade	13
Remote Access	13
Remote Access - SSL VPN	13
Common Vulnerabilities and Exposures	14
Known issues	15
New known issues	15
Existing known issues	15
Configuration	15
Remote Access	15
Remote Access - IPsec VPN	16
Remote Access - SSL VPN	16
Web Filter and plugin	16
ZTNA connection rules	17

Change log

Date	Change description
2024-12-04	Initial release of 7.0.14.
2025-02-11	Updated Common Vulnerabilities and Exposures on page 14.
2026-03-03	Updated Special notices on page 6 and Existing known issues on page 15.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 7.0.14 build 0585.

- [Special notices on page 6](#)
- [Installation information on page 7](#)
- [Product integration and support on page 10](#)
- [Resolved issues on page 13](#)
- [Existing known issues on page 15](#)

Review all sections prior to installing FortiClient.

FortiClient (Windows) 7.0.14 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 7.0.14 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](#).

Special notices

FortiGuard Anycast Certificate Expiration

FortiClient (Windows) 7.0.14 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.

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
Chrome_Extension_Debug.7.0.14.0585.zip	Web Filter extension build for Google Chrome, unminified and minified.
Chrome_Extension_Release.7.0.14.0585.zip	
Edge_Extension_Debug.7.0.14.0585.zip	Web Filter extension build for Microsoft Edge, unminified and minified.
Edge_Extension_Release.7.0.14.0585.zip	
fct_log_def_7.0.14.0585.xml	Log definition file.
Firefox_Extension_Debug.7.0.14.0585.zip	Web Filter extension build for Mozilla Firefox, unminified and minified.
Firefox_Extension_Release.7.0.14.0585.zip	
FortiClientOnlineInstaller_7.0.14.0585.exe	Minimal installer for 32- and 64-bit Windows.
FortiClientSetup_7.0.14.0585.zip	Zip package containing FortiClient.msi and language transforms for 32-bit Windows.
FortiClientSetup_7.0.14.0585_x64.zip	Zip package containing FortiClient.msi and language transforms for 64-bit Windows.
FortiClientSSOConfigurationTool_7.0.14.0585.zip	Zip package containing FortiClient single sign on (FSSO) configurator tool.
FortiClientSSOSetup_7.0.14.0585.zip	FSSO-only installer (32-bit).
FortiClientSSOSetup_7.0.14.0585_x64.zip	FSSO-only installer (64-bit).
FortiClientTools_7.0.14.0585.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientV5SHA256_build0585.sum	SHA256 hashes for files in the image file folder.
FortiClientVPNOnlineInstaller_7.0.14.0585.exe	Minimal FortiClientVPN installer for 32-bit and 64-bit Windows.
FortiClientVPNSetup_7.0.14.0585.exe	Free VPN-only installer (32-bit)
FortiClientVPNSetup_7.0.14.0585.zip	

File	Description
FortiClientVPNSetup_7.0.14.0585_x64.exe	Free VPN-only installer (64-bit)
FortiClientVPNSetup_7.0.14.0585_x64.zip	
md5sum.txt	MD5 hashes for files in the image file folder.
Readme_1st.txt	Read me file that explains files available in the image file folder.
sha512sum.txt	SHA5 hashes for files in the image file folder.

EMS 7.0.14 includes the FortiClient (Windows) 7.0.14 standard installer and zip package containing FortiClient.msi and language transforms.

The following tools and files are available in the FortiClientTools_7.0.14.0585.zip file:

File	Description
FortiClientVirusCleaner	Virus cleaner.
OnlineInstaller	Installer files that install the latest FortiClient (Windows) version available.
SSLVPNcmdline	Command line SSL VPN client.
SupportUtils	Includes diagnostic, uninstallation, and reinstallation tools.
VC_redist.x64.exe	Microsoft Visual C++ 2015 Redistributable Update (64-bit).
vc_redist.x86.exe	Microsoft Visual C++ 2015 Redistributable Update (86-bit).
VPNAutomation	VPN automation tool.

The following files are available on FortiClient.com:

File	Description
FortiClientSetup_7.0.14.0585.zip	Standard installer package for Windows (32-bit).
FortiClientSetup_7.0.14.0585_x64.zip	Standard installer package for Windows (64-bit).
FortiClientVPNSetup_7.0.14.0585.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_7.0.14.0585_x64.exe	Free VPN-only installer (64-bit).



Review the following sections prior to installing FortiClient version 7.0.14: [Introduction on page 5](#) and [Product integration and support on page 10](#).

Upgrading from previous FortiClient versions

To upgrade a previous FortiClient version to FortiClient 7.0.14, do one of the following:

- Deploy FortiClient 7.0.14 as an upgrade from EMS. With the endpoint security improvement feature, there are backward compatibility issues to consider while planning upgrades. See [Recommended upgrade path](#).
- Manually uninstall existing FortiClient version from the device, then install FortiClient (Windows) 7.0.14.

FortiClient (Windows) 7.0.14 features are only enabled when connected to EMS 7.0 or 7.2.

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

You must be running EMS 7.0.2 or later before upgrading FortiClient.

Downgrading to previous versions

FortiClient (Windows) 7.0.14 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 7.0.14 product integration and support information:

Desktop operating systems	<ul style="list-style-type: none">• Microsoft Windows 11 (64-bit)• Microsoft Windows 10 (32-bit and 64-bit)• Microsoft Windows 8.1 (32-bit and 64-bit)
Server operating systems	<ul style="list-style-type: none">• Microsoft Windows Server 2022• Microsoft Windows Server 2019 <p>FortiClient 7.0.14 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 and 2022 support zero trust network access (ZTNA) with FortiClient (Windows) 7.0.14.</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>
Minimum system requirements	<ul style="list-style-type: none">• Microsoft Windows-compatible computer with Intel processor or equivalent. FortiClient (Windows) does not support ARM-based processors.• Compatible operating system and minimum 512 MB RAM• 600 MB free hard disk space• Native Microsoft TCP/IP communication protocol• Native Microsoft PPP dialer for dialup connections• Ethernet network interface controller (NIC) for network connections• Wireless adapter for wireless network connections• Adobe Acrobat Reader for viewing FortiClient documentation• Windows Installer MSI installer 3.0 or later
AV engine	<ul style="list-style-type: none">• 6.00294
FortiAnalyzer	<ul style="list-style-type: none">• 7.4.0 and later• 7.2.0 and later• 7.0.0 and later
FortiAuthenticator	<ul style="list-style-type: none">• 6.4.0 and later• 6.3.0 and later• 6.2.0 and later• 6.1.0 and later• 6.0.0 and later
FortiClient EMS	<ul style="list-style-type: none">• 7.2.0 and later• 7.0.0 and later

FortiManager	<ul style="list-style-type: none"> • 7.4.0 and later • 7.2.0 and later • 7.0.0 and later
FortiOS	<p>The following FortiOS versions support ZTNA with FortiClient (Windows) 7.0.14. This includes both ZTNA access proxy and ZTNA tags:</p> <ul style="list-style-type: none"> • 7.2.0 and later • 7.0.6 and later <p>The following FortiOS versions support IPsec and SSL VPN with FortiClient (Windows) 7.0.14:</p> <ul style="list-style-type: none"> • 7.4.0 and later • 7.2.0 and later • 7.0.0 and later • 6.4.0 and later • 6.2.0 and later
FortiSandbox	<ul style="list-style-type: none"> • 4.2.0 and later • 4.0.0 and later • 3.2.0 and later • 3.1.0 and later

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.



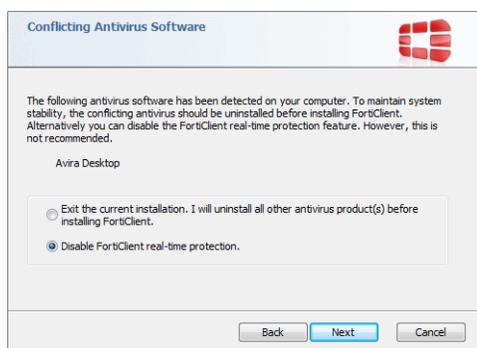
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

Conflicts with third party AV products

The AV feature in FortiClient is known to conflict with other similar products in the market.

- Do not use FortiClient's AV feature with other AV products.
- If not using FortiClient's AV feature, exclude the FortiClient installation folder from scanning for the third party AV product.

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 7.0.14 are as follows:

Version	Product code
Enterprise	707CAECE-5226-4BC8-AE2A-D9139C0C348C
VPN-only agent	C1CAB747-7463-4218-972B-56DA4032310F
Single sign on-only agent	991B7FFE-509E-4D25-96D5-07255805E6B7

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

Resolved issues

The following issues have been fixed in version 7.0.14. For inquiries about a particular bug, contact [Customer Service & Support](#).

Install and upgrade

Bug ID	Description
1057335	FortiAuthenticator Windows agent does not work after FortiClient upgrade.

Remote Access

Bug ID	Description
711402	FortiClient (Windows) fails to establish per-user autoconnect VPN tunnel and per-machine autoconnect tunnel remains connected after Windows logon.
930172	With priority=0 + machine autoconnect enabled, per-user autoconnect tunnel fails to connect after Windows logon.
1052284	Per-machine prelogon tunnel does not work by per-user autoconnect configuration.
1066263	Free VPN-only client console does not minimize after it establishes tunnel with <code><minimize_window_on_connect></code> enabled.
1092542	After upgrading FortiClient, FortiClient (Windows) quickly and automatically removes VPN credentials, making VPN connection difficult.

Remote Access - SSL VPN

Bug ID	Description
920383	FortiClient enables <i>Turn off smart multi-homed name resolution</i> on Windows machine after successful connection.
922941	Connecting to SSL VPN with FQDN resolved to both IPv4 and IPv6 as remote gateway gets stuck at 98%.

Bug ID	Description
1011690	SamIGetResponseUsingWebBrowser cannot start SamIAuthWB.exe.
1052659	FortiClient (Windows) gets stuck at 98% and cannot reconnect when endpoint is left in standby or sleep for a couple of hours until reboot.

Common Vulnerabilities and Exposures

Bug ID	Description
945320	FortiClient (Windows) 7.0.14 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2024-50570 Visit https://fortiguard.com/psirt for more information.
948253	FortiClient (Windows)7.0.14 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2024-40586 Visit https://fortiguard.com/psirt for more information.

Known issues

Known issues are organized into the following categories:

- [New known issues on page 15](#)
- [Existing known issues on page 15](#)

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 7.0.14.

No new issues have been identified in version 7.0.14.

Existing known issues

The following issues have been identified in a previous version of FortiClient (Windows) and remain in FortiClient (Windows)7.0.14.

Configuration

Bug ID	Description
1016803	After installation, the <i>Remote Access</i> tab is hidden even if a Remote Access profile is embedded in the installer.

Remote Access

Bug ID	Description
996877	Manage Engine ADSelfService-installed endpoint causes issue on other user screen when VPN before logon is enabled.

Remote Access - IPsec VPN

Bug ID	Description
758424	Certificate works for IPsec VPN tunnel if put it in current user store but fails to work if in local machine.

Remote Access - SSL VPN

Bug ID	Description
909244	Split DNS name resolution stops working after VPN is up for a few minutes in some environments until running <code>ipconfig /flushdns</code> .
914018	SSL VPN SAML login fails to work if using YubiKey for MFA.
916581	Static DNS entry is registered when on-fabric.
947381	With <code><prefer_sslvpn_dns></code> disabled, when SSL VPN is up, FortiClient (Windows) adds DNS suffix to all network interfaces.
950787	Domain filter cannot block access for specific server FQDN.
993876	FortiClient (Windows) provides inaccurate error in German when SSL VPN password is incorrect.
994884	SSL VPN connections get stuck on 40%.
1015381	FortiClient takes longer than usual to autoconnect.

Web Filter and plugin

Bug ID	Description
1255625	<p>FortiClient (Windows) 7.0.14 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:</p> <ul style="list-style-type: none"> • Web Filter rating • Video Filter rating • Split VPN using ISDB • Signature and engine updates <p>See CSB-260303-1 for more information.</p>

ZTNA connection rules

Bug ID	Description
839589	ZTNA TCP forwarding does not work for GoAnywhere application.
949507	ZTNA has multiple client certificates in certificate store.
1001116	FortiClient requests SAML credentials after network change in ZTNA connections.



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.