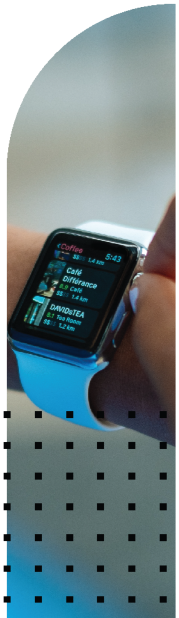
Release Notes

FortiClient (Windows) 7.0.1



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

FORTINET VIDEO GUIDE
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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

September 21, 2021
FortiClient (Windows) 7.0.1 Release Notes
04-701-729344-20210921

TABLE OF CONTENTS

Change log

Date	Change Description
2021-08-10	Initial release of 7.0.1.
2021-09-2021	Updated link in What’s new in FortiClient (Windows) 7.0.1 on page 6.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 7.0.1 build 0083.

- What’s new in FortiClient (Windows) 7.0.1 on page 6
- Installation information on page 7
- Product integration and support on page 9
- Resolved issues on page 12
- Known issues on page 14

Review all sections prior to installing FortiClient.

Licensing

See Windows, macOS, and Linux endpoint licenses.

FortiClient 7.0.1 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. You cannot use the VPN-only client with the FortiClient Single Sign On Mobility Agent (SSOMA). To use VPN and SSOMA together, you must purchase an EMS license.

What’s new in FortiClient (Windows) 7.0.1

For information about what's new in FortiClient (Windows) 7.0.1, see the *FortiClient & FortiClient EMS 7.0 New Features Guide*.

Installation information

Firmware images and tools

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

File	Description
FortiClientTools_7.0.1.xxxx.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_ 7.0.1.xxxx.zip	FSSO-only installer (32-bit).
FortiClientSSOSetup_ 7.0.1.xxxx_x64.zip	FSSO-only installer (64-bit).
FortiClientVPNSetup_ 7.0.1.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_ 7.0.1.xxxx_x64.exe	Free VPN-only installer (64-bit).

EMS 7.0.1 includes the FortiClient (Windows) 7.0.1 standard installer and zip package containing FortiClient.msi and language transforms.

The following tools and files are available in the FortiClientTools_7.0.xx.xxxx.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.
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).

The following files are available on FortiClient.com:

File	Description
FortiClientSetup_7.0.1.xxxx.zip	Standard installer package for Windows (32-bit).
FortiClientSetup_7.0.1.xxxx_ x64.zip	Standard installer package for Windows (64-bit).

File	Description
FortiClientVPNSetup_ 7.0.1.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_ 7.0.1.xxxx_x64.exe	Free VPN-only installer (64-bit).

Review the following sections prior to installing FortiClient version 7.0.1: Introduction on page 5 and Product integration and support on page 9.

Upgrading from previous FortiClient versions

To upgrade a previous FortiClient version to FortiClient 7.0.1, do one of the following:

- Deploy FortiClient 7.0.1 as an upgrade from EMS
- Manually uninstall existing FortiClient version from the device, then install FortiClient (Windows) 7.0.1

FortiClient (Windows) 7.0.1 features are only enabled when connected to EMS 7.0.

See the *FortiClient and FortiClient EMS Upgrade Paths* for information on upgrade paths.

Downgrading to previous versions

FortiClient (Windows) 7.0.1 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 Checksums*, enter the image file name, including the extension, and select *Get Checksum Code*.

Product integration and support

The following table lists version 7.0.1 product integration and support information:

Desktop operating systems	• Microsoft Windows 10 (32-bit and 64-bit) • Microsoft Windows 8.1 (32-bit and 64-bit) • Microsoft Windows 7 (32-bit and 64-bit) FortiClient 7.0.1 does not support Microsoft Windows XP and Microsoft Windows Vista.
Server operating systems	• Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 FortiClient 7.0.1 does not support Windows Server Core. For Microsoft Windows Server, FortiClient (Windows) supports the Vulnerability Scan, SSL VPN, Web Filter, and 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.
Embedded system operating systems	Microsoft Windows 10 IoT Enterprise LTSC 2019
Minimum system requirements	• 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	• 6.00258
FortiAnalyzer	• 7.0.0 and later
FortiAuthenticator	• 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	• 7.0.0 and later
FortiManager	• 7.0.0 and later

FortiOS	The following FortiOS versions support ZTNA with FortiClient (Windows) 7.0.1: • 7.0.0 and later The following FortiOS versions support IPsec and SSL VPN with FortiClient (Windows) 7.0.1: • 7.0.0 and later • 6.4.0 and later • 6.2.0 and later • 6.0.0 and later
FortiSandbox	• 4.0.0 and later • 3.2.0 and later • 3.1.0 and later • 3.0.0 and later • 2.5.0 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.

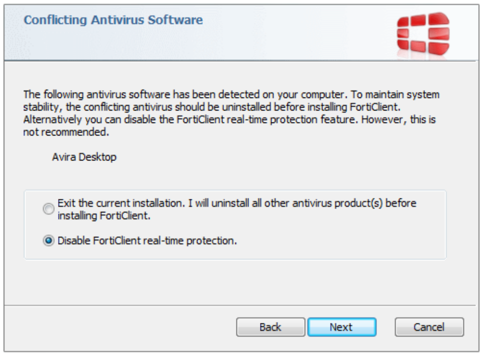
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

Conflicts with third party AV products

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

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

During a new installation of FortiClient, the installer searches for other registered third party software and, if any is found, warns users to uninstall them before proceeding with the installation. There is also an option to disable FortiClient Real Time Protection (RTP).



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.

Resolved issues

The following issues have been fixed in version 7.0.1. For inquiries about a particular bug, contact Customer Service & Support.

Zero Trust Telemetry

Bug ID	Description
697795	FortiClient fails to calculate on-Fabric result.
700915	FortiClient fails to disconnect from FortiClient Cloud when FortiClient Cloud server is unreachable.
715320	FortiClient (Windows) fails to update state when FortiClient Cloud is unreachable.
723465	EMS profiles do not sync IPsec VPN phase 2 configuration to FortiClient.

GUI

Bug ID	Description
683027	FortiClient (Windows) shows quarantine message even if Application Firewall is not installed and quarantine mode does not work.
685756	The SSL VPN *Click* button has no response to clicking action.

Malware Protection and Sandbox

Bug ID	Description
516704	Antivirus should recognize Windows-signed files.
590688	FortiClient says FortiSandbox scan does not support file type when extension is supported and enabled on FortiSandbox.
705761	FortiClient (Windows) does not block USB drives despite Removable Media Access being configured to block Windows portable devices.
717417	FortiClient cannot get FortiSandbox Cloud IP address list.
722597	Removable Media Access rule does not work.

Remote Access

Bug ID	Description
613868	Always up and autoconnect does not work for SAML SSL VPN connection.
643083	Dual SSL VPN certificates with the same name.
682249	SSL VPN DNS split tunnel issues.
692822	Six character limitation in token popup.
693687	FortiClient does not registers any interfaces' IP addresses to the DNS server when SSL VPN tunnel is up.
693913	Username and password become blank on console when connecting to second remote gateway via SSL VPN.
698407	VPN before logon does not work with IKEv2 and EAP.
702965	Host check interval does not work as expected after PC previously went into sleep mode.
703939	FortiClient (Windows) does not send UID to SSL VPN daemon.
709001	SSL VPN host check validation does not work for SAML user.
713909	If *Enable VPN before Windows logon* is enabled and there are multiple tunnels configured, there is a long delay before Windows login prompt.
716924	Azure multifactor authentication fails when redundant sort method is configured as ping or TCP round trip time.
717448	VPN before Windows logon fails to list certificate when `disable_internet_check` is `1`.
718343	Ransomware detection for DarkSide ransomware.
718737	FortiClient intermittently is missing SSL VPN user credentials after Windows logon.
719828	FortiClient (Windows) fails to allow SSL VPN even though FortiClient (Windows) does not have prohibit host tag.
721389	IPsec VPN fails to work.
721633	IPsec VPN fails to work on Windows 7 x64 and x86.
723379	SAML authentication error message is incomplete and has typos.
734146	IPv6 negative split tunnel support for SSL VPN may randomly fail to save to the registry.

Web Filter and plugin

Bug ID	Description
720852	Web Filter fails to request to install plugin if browser is not installed in the default location.
720855	Web Filter still allows user to access website even though Edge plugin is not installed.

Known issues

The following issues have been identified in FortiClient (Windows) 7.0.1. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Install and deployment

Bug ID	Description
700396	The device driver cannot be loaded (code 38).
714268	Upgrade from 6.4.2 fails.
716597	Installation using `norestart` parameter requests reboot.

Application Firewall

Bug ID	Description
717628	Application Firewall causes issues with Motorola RMS high availability client.

GUI

Bug ID	Description
707440	Clicking *Unlock Settings* does not enable *Clear Logs* button in settings page.
725644	Google social network login does not work properly.
726971	Wrong password dialog is missing when connecting via SSL VPN.
729610	FortiClient (Windows) saves encrypted password incorrectly when user uses Spanish characters and FortiClient (Windows) is configured to save username and password.
730331	User cannot launch FortiClient (Windows) from SSL VPN web portal.
730756	For SSL VPN dual stack, GUI only shows IPv4 address.
731152	FortiClient reports corporate EMS as unreachable when SSL VPN is connected.
731450	Disable context menu in antivirus (AV) scan dialog when FortiClient is connected to EMS.

Bug ID	Description
731691	GUI does not refresh after disabling *Hide User Information* in EMS profile.
733485	SSL VPN password is blank with FortiToken.
735345	FortiClient does not translate *A FortiToken code is required for SSL VPN login authentication* prompt to Chinese.

ZTNA connection rules

Bug ID	Description
704234	Zero Trust tagging rule set syntax to check registry key value.
721958	Entire console should not launch during ZTNA TCP forward proxy authentication.
730415	Configuration backup misses locally configured ZTNA connection rules.
730459	FortiClient certificate serial number in endpoint is incorrect.
733871	FortiClient (Windows) should remove browser-based ZTNA settings.
735494	Windows 7 does not support ZTNA TCP forwarding feature.

FSSOMA

Bug ID	Description
725710	FSSOMA does not send user identities to FortiAuthenticator.

Zero Trust Telemetry

Bug ID	Description
648651	FortiClient (Windows) reaches *Unable to retrieve EMS Details* state after user cancels connection key popup.
687611	FortiClient does not calculate Active Directory group-based policy rule for tags.
693928	After FortiClient (Windows) migrates to new EMS successfully, it does not remove original EMS from EMS list.
702660	Switching AD users does not modify user details in EMS *Endpoints* table.

Bug ID	Description
705664	FortiGate waits about one minute to get ZTNA EMS tag update.
712603	CLI parameter to register FortiClient to EMS with Telemetry key.
714131	Migrating FortiClient to different server fails when connection key is enabled.
718995	FortiClient does not register to EMS after silent installation.
721651	When connected to a full VPN to FortiGate, FortiClient sends virtual IP and MAC addresses to EMS.
722082	EMS does not apply the tag for file type even though file exists on endpoint.
722199	FortiClient stays in registration progress to FortiClient Cloud and never returns connection result.
724038	Zero Trust tag rule does not work properly for AD-joined devices when endpoints connect to EMS via SSL VPN.
724988	FortiClient uses FortiSASE SIA egress IP address as the public IP address.
727570	FortiClient registry is missing key encryption when EMS-pushed rules enable encryption.
731525	FortiClient (Windows) does not detect AV is not up-to-date tagging rule result properly.
735189	FortiClient reports corporate EMS as unreachable when it is pingable.

Malware Protection and Sandbox

Bug ID	Description
672146	Antiransomware fails to detect some popular ransomware samples.
709729	`realtime_scan` log disappears after ten seconds.
712314	Ransomware protection rollback for Magniber.
713557	Exceptions do not work for AntiExploit.
721174	FortiClient (Windows) flags `bin_x64\FctRtMonitor.exe` as `Win32/AI.Pallas.Suspicious`.
724087	FortiClient (Windows) sends browser cache files to FortiSandbox and user cannot exclude them while browsing pages with FortiClient (Windows) installed.
724228	FortiClient quick scan cannot detect the `av_custom_malware.exe` file.
725936	Compatibility with USB key.
729475	User cannot look up file hash in antiransomware events.
731782	FortiClient cannot quarantine file with Ukrainian characters.

Bug ID	Description
731873	FortiClient (Windows) blocks Veeam backups.
734012	FortiClient does not respect exclusions if it detects malicious file as riskware.
734993	Rule to block removable media (USB drives) stops working.

Remote Access

Bug ID	Description
637303	Certificate-only SSL VPN tunnel displays *Empty username is not allowed* error.
649426	IPsec/SSL VPN per-app VPN split tunnel does not work properly.
684913	SAML authentication on SSL VPN with realms does not work.
685951	FortiClient does not use fallback server IP address when *Show VPN before Logon* option is set.
698713	User can update SSL VPN user password without entering the same password to confirm the new password.
707882	IPsec VPN fails to autoconnect with *Failed to launch IPsec service* error.
710877	SSL VPN with SAML (Azure AD) and two gateways does not work.
711227	Per-user autoconnect starts to autoconnect before Windows logon.
711402	Per-user autoconnect does not get established, and per-machine autoconnect still remains connected after Windows logon.
714564	SAML connection stays in connecting state and never returns with error when FortiGate gateway is inaccessible.
717100	MTU issues when DTLS is enabled and client network tunnels IPv4 over IPv6.
717512	VPN disclaimer message present in EMS profile is not present on endpoints and endpoints show no disclaimer.
717913	FortiSASE SIA VPN failed to reestablish after FortiSASE SIA-related components were upgraded.
725941	After powering on/rebooting Windows, FortiClient (Windows) cannot establish SSL VPN tunnel for approx two minutes due to host check failure.
726249	Per-application split tunnel does not work for FortiSASE SIA SSL VPN. FortiClient cannot exempt the Trusted FQDNs effectively from FortiSASE SIA VPN.
726680	VPN client takes 20 seconds to disconnect.
727098	FortiClient appears disconnected when trying to connect to SSL VPN.
728110	FortiClient must dynamically update Windows hostnames in DNS AD-integrated database.
728240	SSL VPN negate split tunnel IPv6 address does not work on FortiClient (Windows).

Bug ID	Description
728244	Negate split tunnel IPv4 address does not work for dual stack mode using IPv6 access.
729233	FortiSASE SIA trusted traffic feature (split tunnel) requires restarting FortiClient (Windows) SSL VPN connection to take effect.
730095	Without EAP enabled, certificate-based IKEv2 does not work.
731011	FortiClient is stuck at 98% connecting to SSL VPN tunnel when integrated with SAML (Azure AD) authentication.
731127	SSL VPN SAML login displays *Empty username is not allowed.* error.
732594	SSL VPN `redundant_sort_method` does not work with realms.
734866	When per-machine autoconnect before OS start is enabled, FortiClient (Windows) keeps trying to connect after failing to connect to VPN.
735105	For per-machine autoconnect, certificate dropdown lists certificates in current user store before Windows logon.
735756	IPsec VPN sends unexpected xAuth authentication attempt.
735969	SSL VPN autoconnects after logging out of Windows and logging in as administrator.

Web Filter

Bug ID	Description
647955	Web Filter conflicts with third-party VPN client.
657715	FortiProxy fails to start.
712974	Web Filter blocks some WebEx communication due to unrated IP address.
729127	Web Filter affects Manufacturing Execution System software.
731982	Web rating overrides behavior between FortiClient Web Filter and FortiGate Web Filter differs.
734400	Proxy service fails to process HTTPS connections.

Logs

Bug ID	Description
652647	FortiClient fails to upload large diagnostic tool result file to EMS.
720388	FortiClient fails to provide log for secure Remote Access compliance enforcement.

Other

Bug ID	Description
720569	Update task returns error while doing full signature update.
729499	Endpoints fail to update AV signatures after EMS sends AV out-of-date email notifications.

FORTINET®

www.fortinet.com