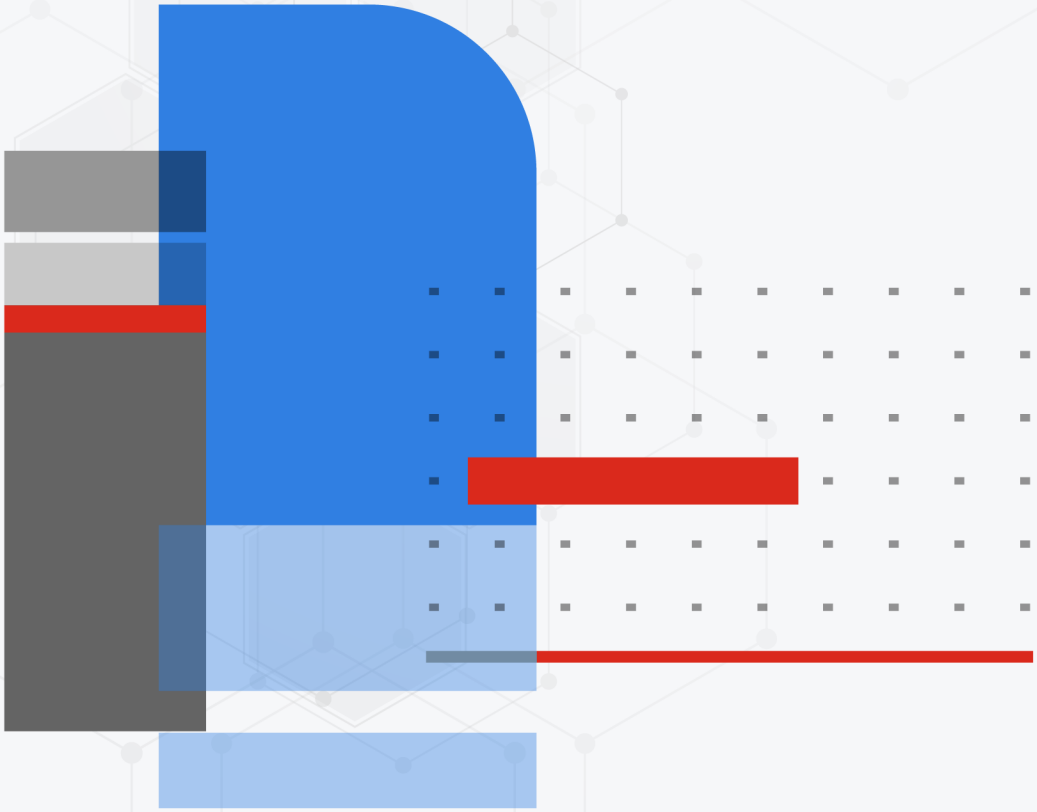
Release Notes

FortiClient (Windows) 7.4.2



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 18, 2025
FortiClient (Windows) 7.4.2 Release Notes
04-742-1105661-20250318

TABLE OF CONTENTS

Change log **5**
Introduction **6**
Licensing 6
Special notices **7**
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
What's new in FortiClient (Windows) 7.4.2 ..... **9**
Installation information **10**
Firmware images and tools 10
Upgrading from previous FortiClient versions 11
Downgrading to previous versions 11
Firmware image checksums 12
Product integration and support **13**
Language support 14
Conflict with third-party endpoint protection software 15
Intune product codes 15
Resolved issues **17**
PAM 17
Remote Access 17
Vulnerability Scan 17
Common Vulnerabilities and Exposures 17
Known issues **19**
New known issues 19
Install and upgrade 19
Remote Access - IPsec VPN 19
Remote Access - SSL VPN 19
Other 20
Existing known issues 20
Application Firewall 20
Avatar and social network login 20
Configuration 20
Deployment and installers 21
Endpoint control 21
GUI 21
Endpoint policy and profile 21
Install and upgrade 21
Logs 22
Malware Protection and Sandbox 22
Multitenancy 22

Onboarding 22
Security posture tags 22
Quarantine management 23
Performance 23
Remote Access 23
Remote Access - IPsec VPN 23
Remote Access - SSL VPN 24
Vulnerability Scan 24
Web Filter and plugin 24
ZTNA connection rules 25
Other 25

Change log

Date	Change description
2024-12-11	Initial release of 7.4.2.
2025-01-14	Added Other on page 20.
2025-02-19	Updated Product integration and support on page 13.
2025-03-18	Added Remote Access - IPsec VPN on page 19.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 7.4.2 build 1737.

- Special notices on page 7
- Installation information on page 10
- Product integration and support on page 13
- Resolved issues on page 17
- Known issues on page 19

Review all sections prior to installing FortiClient.

FortiClient (Windows) 7.4.2 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: 7.4.2.1737

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

Licensing

See Windows, macOS, and Linux endpoint licenses.

FortiClient 7.4.2 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.

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.

See 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 does not support parallel independent VPN connections to different sites. However, FortiClient may still establish VPN connection over existing third-party (for example, AT&T Client) VPN connection (nested tunnels).

What’s new in FortiClient (Windows) 7.4.2

For information about what's new in FortiClient (Windows) 7.4.2, 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_7.4.2.1737.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_ 7.4.2.1737_x64.zip	Fortinet single sign on (FSSO)-only installer (64-bit).
FortiClientVPNSetup_ 7.4.2.1737_x64.exe	Free VPN-only installer (64-bit).

EMS 7.4.2 includes the FortiClient (Windows) 7.4.2 standard installer and zip package containing FortiClient.msi and language transforms.

The following tools and files are available in the FortiClientTools_7.4.2.1737.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.
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_7.4.2.1737_x64.zip	Standard installer package for Windows (64-bit).
FortiClientVPNSetup_7.4.2.xxxx_x64.exe	Free VPN-only installer (64-bit).

Review the following sections prior to installing FortiClient version 7.4.2: 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 7.4.2 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) 7.4.2:

- 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 7.4.2 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 7.4.2, do one of the following:

- Deploy FortiClient 7.4.2 as an upgrade from EMS. See Recommended upgrade path.
- Manually uninstall existing FortiClient version from the device, then install FortiClient (Windows) 7.4.2.

FortiClient (Windows) 7.4.2 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) 7.4.2 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 7.4.2 product integration and support information:

Desktop operating systems	• Microsoft Windows 11 (64-bit) • Microsoft Windows 10 (64-bit)
Server operating systems	• Microsoft Windows Server 2022 • Microsoft Windows Server 2019 FortiClient 7.4.2 does not support Windows Server Core. For Microsoft Windows Server, FortiClient (Windows) supports the Vulnerability Scan, SSL VPN, Web Filter, and antivirus (AV), 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. Microsoft Windows Server 2019 supports zero trust network access (ZTNA) with FortiClient (Windows) 7.4.2. 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.
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 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 (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	• 7.00026
VCM engine	• 2.0043
FortiAnalyzer	• 7.4.0 and later • 7.2.0 and later • 7.0.0 and later
FortiAuthenticator	• 6.5.0 and later • 6.4.0 and later • 6.3.0 and later • 6.2.0 and later
FortiClient EMS	• 7.4.0 and later
FortiEDR for Windows	• 5.2.5.0037

FortiManager	• 7.4.0 and later • 7.2.0 and later • 7.0.0 and later
FortiOS	The following FortiOS versions support ZTNA with FortiClient (Windows) 7.4.2. This includes both ZTNA access proxy and security posture 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) 7.4.2: • 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

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.

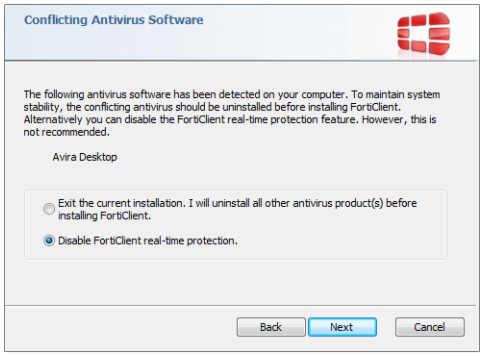
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

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's AV feature 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 7.4.2 are as follows:

Version	Product code
Enterprise	D47820AB-F024-4323-A7E1-04CEB6D24345
VPN-only agent	B94F6ED2-7970-4E4D-9445-DE275493ABA0

Version	Product code
Private access management-only agent	8D14953C-7F26-4DC7-B95C-D227544A5310
Single sign on-only agent	01D594DE-B846-4E18-9FCC-3437A9E2D7E7

See Configuring the FortiClient application in Intune.

Resolved issues

The following issues have been fixed in version 7.4.2. For inquiries about a particular bug, contact Customer Service & Support.

PAM

Bug ID	Description
1099622	FortiPAM fails to automatically fill password for proxy mode enabled secret when FortiClient (Windows) fails to add FortiPAM zero trust network access rules in time.
1101380	*This site can't be reached* error occurs on first attempt through web launcher in FortiPAM.

Remote Access

Bug ID	Description
1066263	Free VPN-only agent does not minimize after establishing a tunnel with `<minimize_window_on_connect>` enabled.

Vulnerability Scan

Bug ID	Description
1054778	FortiClient (Windows) displays incorrect detected version on Vulnerability Scan report GUI.

Common Vulnerabilities and Exposures

Bug ID	Description
945320	FortiClient (Windows) 7.4.2 is no longer vulnerable to the following CVE Reference:

Bug ID	Description
	• CVE-2024-50570 Visit https://fortiguard.com/psirt for more information.

Known issues

Known issues are organized into the following categories:

- New known issues on page 19
- Existing known issues on page 20

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 7.4.2.

Install and upgrade

Bug ID	Description
1106731	When upgraded from 7.4.1 GA to 7.4.2 using .msi files, VM does not restart and FortiClient (Windows) services do not start automatically. **Workaround**: See Upgrading from previous FortiClient versions on page 11.

Remote Access - IPsec VPN

Bug ID	Description
1121087	Subnet exclusion does not work properly in dialup IPsec VPN.

Remote Access - SSL VPN

Bug ID	Description
1113234	FortiClient cannot dial SSl VPN to FortiGate with SAML login when using internal browser as user agent for SAML user authentication.

Other

Bug ID	Description
1105661	FortiClient (Windows) daemons crash with Microsoft Visual C++ (VC) runtime version lower than 14.40.33810.0. **Workaround**: do one of the following: • Update the VC runtime library. See Microsoft Visual C++ Redistributable latest supported downloads. • Download the latest VC redistributable version and run it. Download the x64 installer.

Existing known issues

The following issues have been identified in a previous version of FortiClient (Windows) and remain in FortiClient (Windows) 7.4.2.

Application Firewall

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

Avatar and social network login

Bug ID	Description
1106444	User identity information popup does not allow user to enter username, email address, and phone number.

Configuration

Bug ID	Description
1087936	EMS disconnect password with some special characters does not work.

Deployment and installers

Bug ID	Description
1104334	Deployment message is in English for PC with local language not set to English.
1113057	Installation does not follow unsupervised scheduled deployment time.

Endpoint control

Bug ID	Description
1012497	FortiClient should send empty `USER/USER_SID` to EMS when the user logs out for Domain/Azure users.
1086370	Unverified FortiClient doesn't prompt for verification after upgrade with user verification invite being part of the installer.

GUI

Bug ID	Description
1100909	FortiClient (Windows) language change affects Windows logon screen language.

Endpoint policy and profile

Bug ID	Description
1087262	Policy is not correctly assigned to all Active Directory group members.

Install and upgrade

Bug ID	Description
1080006	FortiClient (Windows) .exe installer does not properly handle `v` and `msicl` command line parameters.

Logs

Bug ID	Description
1103313	FortiAnalyzer is missing some Web Filter log entries.

Malware Protection and Sandbox

Bug ID	Description
1039172	FortiClient non-manual files send for scanning to on-prem Sandbox don't show *ATP Scan* dialog.
1098883	Sandbox does not restore file when antivirus is not installed.
1103310	German message on reboot prompt does not show completely.

Multitenancy

Bug ID	Description
1089156	FortiClient (Windows) automatically switches to default site when EMS enables multitenancy.

Onboarding

Bug ID	Description
1081547	Authentication dialog is blank when using invitation code with local or LDAP authentication to connect to EMS.
1104465	FortiClient (Windows) cannot connect to telemetry through SAML authentication due to authorization failing to connect on EMS.

Security posture tags

Bug ID	Description
1027851	FortiClient (Windows) sometimes loses security posture tag based on combined rules and the only way to fix the issue is reinstalling FortiClient.
1101903	Windows automatic update check security posture tag does not work.
1103074	If security posture tag Tag_C is configured as applying to endpoints that are tagged with Tag_A and Tag_B, endpoint that is tagged with Tag_A and Tag_B is missing Tag_C.
1104084	Security posture tag for *OS system last update is within 60 days* does not work as expected.

Quarantine management

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

Performance

Bug ID	Description
1099258	FortiClient (Windows) causes Windows Defender to have high CPU usage.

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.
1027199	FortiClient (Windows) sometimes does not log in to system when using SAML VPN before logon.
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.
1036306	IPsec VPN fails to autoconnect after installing EMS-repackaged FortiClient installer when `autoconnect_on_install` is enabled.
1070788	IPsec is disconnected immediately after tunnel is up sometimes when working from home using WiFi.
1079047	FortiClient (Windows) on Windows 11 with Intel Wi-Fi 7 BE200 Wi-Fi network adapter cannot connect to IPsec VPN.
1091700	LDAP traffic volume is high when endpoint is connected to tunnel.

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 `ipconfig /flushdns`.
909755	SSL VPN split tunnel does not work for Microsoft Teams.
930740	Unable to setup SSL VPN if the password contains Polish characters "ł", "ą", or "ń".
950787	Domain filter cannot block access for *specific server FQDN*.
976800	Azure automatic login is possible when Microsoft conditional access policy does not allow authentication.
994884	SSL VPN connections get stuck on 40% in some cases.
1010455	SAML authentication prompt timeout is set to default value of 300 seconds and does not reflect the remote authentication timeout configured on FortiGate.
1018817	User must click *Save Password* to save SAML username.
1019876	User gets stuck at 40% connectivity when connecting to any VPN.
1024304	FortiClient (Windows) is stuck on token entry page when user clicks *Cancel* for SSL VPN tunnel connection.
1070783	SSL VPN cannot connect. After successful authentication, FortiClient (Windows)redirects to connection page multiple times.
1081068	SSL VPN does not connect on Windows Server 2019.
1091993	With *Disable Connect/Disconnect* on, FortiClient (Windows) loses saved SSL VPN user credentials when waking up from sleep.

Vulnerability Scan

Bug ID	Description
1092036	FortiClient logs for the detected vulnerability shows only UUID code as the `detectedpath` instead of the application's actual path.

Web Filter and plugin

Bug ID	Description
1061163	Web Filter plugin blocks some websites after file download.
1084513	Windows 10 users cannot access websites due to Web Filter rating lookup errors.

Bug ID	Description
1090048	Web Filter plugin blocks embedded Google Maps.
1092404	Webpage fails to load when Web Filter plugin is disabled.
1092975	Web Filter blocks Amazon Web Services S3 browser.
1097357	Web Filter cannot block https://chromewebstore.google.com in Edge and Chrome.
1101902	Letsignit application cannot authenticate while connected to EMS telemetry.
1103205	FortiClient blocks some websites due to Web Filter category being unknown.

ZTNA connection rules

Bug ID	Description
919832	Zero trust network access stops working after days with *No ZTNA client certificate was provided* error.
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.

Other

Bug ID	Description
1045956	NVR 3 CCTV software has issues when FortiClient is present.
1082299	FortiClient has duplicate UID entries when deployed on VMware and Citrix.

Release Notes

FortiClient (Windows) 7.4.2