FORTINET

Release Notes

FortiClient (Windows) 7.4.5

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

February 25, 2026
FortiClient (Windows) 7.4.5 Release Notes
04-745-1208451-20260225

TABLE OF CONTENTS

Change log

Date	Change description
2025-12-11	Initial release of 7.4.5.
2025-12-15	Updated New known issues on page 23.
2025-12-17	Updated Resolved issues on page 18 and Existing known issues on page 24.
2025-12-22	Updated New known issues on page 23.
2026-01-20	Updated Product integration and support on page 14 and Existing known issues on page 24.
2026-01-23	Updated Existing known issues on page 24.
2026-01-27	Updated New known issues on page 23.
2026-01-28	Updated Existing known issues on page 24.
2026-02-10	Added CVE-2025-62676 to Resolved issues on page 18.
2026-02-19	Added FortiClient (Windows) 7.4.5 GA hotfix 1 on page 7 to Special notices on page 7.
2026-02-25	Updated Existing known issues on page 24.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 7.4.5 build 1949.M.

- Special notices on page 7
- What's new in FortiClient (Windows) 7.4.5 on page 10
- Installation information on page 11
- Product integration and support on page 14
- Resolved issues on page 18
- Known issues on page 23

Review all sections prior to installing FortiClient.

FortiClient (Windows) 7.4.5 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: 7.4.5.1949.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

FortiClient (Windows) 7.4.5 GA hotfix 1

The following issues have been fixed in FortiClient (Windows) 7.4.5 GA hotfix 1 (7.4.5.1949.1.4589).

Bug ID	Description
1255625	Update FortiClient Windows and FortiClient EMS to recognize newly issued April 16, 2026 Digicert CA used by FortiGuard Anycast servers.
1237189	VPN configuration installations may fail if the DNS priority setting is changed from FortiClient EMS.

If you need this hotfix, please collect the EMS serial numbers and contact Fortinet Support.

See the EMS Administration Guide for detailed instructions about deploying FortiClient hotfix installers from EMS.

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

FortiClient (Windows) 7.4.5 no longer supports 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) 7.4.4-7.4.5 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 7.4.5. 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 IPv6 support for IPsec VPN

FortiClient (Windows) 7.4.4-7.4.5 do not support IPv6 for IPsec VPN. Support may be added in future releases.

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.

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

What’s new in FortiClient (Windows) 7.4.5

For information about what's new in FortiClient (Windows) 7.4.5, 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-7.4.5-windows-release-notes.pdf	Release Notes file.
FortiClientPAMSetup_7.4.5.1949.M_x64.exe	Privilege access management agent installer (64-bit).
FortiClientSetup_7.4.5.1949.M_ARM64.zip	ARM installer (64-bit).
FortiClientSetUp_7.4.5.1949.M_x64.zip	Installer (64-bit).
FortiClientSSOSetup_7.4.5.1949.M_ARM64.zip	ARM FSSO-only installer (64-bit).
FortiClientSSOSetup_7.4.5.1949.M_x64.zip	Fortinet single sign on (FSSO)-only installer (64-bit).
FortiClientTools_7.4.5.1949.M.zip	Zip package containing miscellaneous tools, including VPN automation files.

EMS 7.4.5 includes the FortiClient (Windows) 7.4.5 standard installer and zip package containing FortiClient.msi and language transforms.

The following tools and files are available in the FortiClientTools_7.4.5.1949.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.
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_7.4.5.1949.M_x64.zip	Standard installer package for Windows (64-bit).

Review the following sections prior to installing FortiClient version 7.4.5: Introduction on page 6, Special notices on page 7, and Product integration and support on page 14.

Upgrading from previous FortiClient versions

Upgrading from FortiClient (Windows) 7.4.0 or 7.4.1 to 7.4.5 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) 7.4.5:

- 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 7.4.5 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 7.4.5, do one of the following:

- Deploy FortiClient 7.4.5 as an upgrade from EMS. See Recommended upgrade path.
- Manually uninstall existing FortiClient version from the device, then install FortiClient (Windows) 7.4.5.

FortiClient (Windows) 7.4.5 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) 7.4.5 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 7.4.5 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) 7.4.5 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	• 7.4.5 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
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

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
FortiSandbox	• 5.0.0 and later • 4.4.0 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

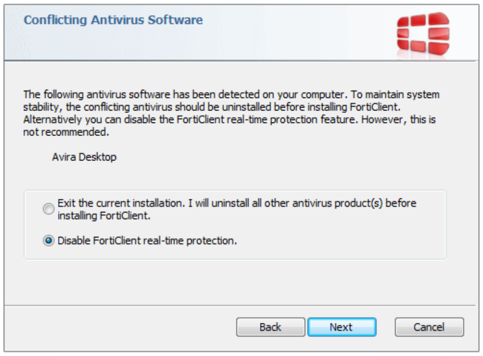
FortiClient (Windows) does not support multi-user sessions using terminal servers, multi-session OSes, or via user switch.

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 7.4.5 are as follows:

Version	Product code
Enterprise	6B74BAA3-9F20-4F6E-84D2-1230945E503B

Version	Product code
Private access management-only agent	3A976D64-2CA7-4B4F-8C47-5D5D84F3F396
Single sign on-only agent	BA732507-8F6F-4866-BADD-A635BFB439EF

See Configuring the FortiClient application in Intune.

Resolved issues

The following issues have been fixed in version 7.4.5. For inquiries about a particular bug, contact Customer Service & Support.

Deployment and installers

Bug ID	Description
1212810	FortiClient does not upgrade after installer has been pushed to the endpoint.

Malware Protection

Bug ID	Description
1199087	A crash may occur in the antivirus RTP service. The antiransomware service may fail to observe the scan inclusion list.

Onboarding

Bug ID	Description
1196704	During a FortiClient EMS switch, the ZTNA certificate from the old EMS is not removed after switching to the new FortiClient EMS server.

Privilege Access Management

Bug ID	Description
1127812	Warning or error messages appear behind a shadow and do not allow continuing.

Bug ID	Description
1192930	Cannot connect to VPN when FortiClientPAMSetup_7.4.3.1790_x64 is installed side by side with Ivanti.
1195403	Video freezes when being recorded and played on FortiPAM or from backup file.

Remote Access

Bug ID	Description
1194067	VPN connection status is not updated after tunnel for OS_Start_To_Connect is up.

Remote Access - IPsec VPN

Bug ID	Description
1237189	VPN configuration installations may fail if the DNS priority setting is changed from FortiClient EMS.
1168356	Communication issues after upgrade.
1191792	*Last Disconnect Reason* shows *Crash* for a DPD error.
1195916	"Crashed" error when FortiClient tries to establish an IKEv2 IPsec tunnel using transport mode AUTO.
1091700	High volume of LDAP traffic when endpoint connects to tunnel.
1180286	ECDSA certificate-based IKEv2 tunnel fails to establish.
1186077	Certificate error when connecting to IPsec IKEv2 tunnel if "set peertype peer" is set on FortiGate.
1186588	Network lockdown captive portal detection is failing when using an invalid certificate.
1187353	Cannot auto-connect to the IPsec VPN using Entra ID logon session information.
1190617	Extending two-factor-email-expiry, remote-auth-timeout and negotiate-timeout do not work for IKEv2 local user。
1194172	FortiClient does not disconnect IPsec tunnel gracefully before machine reboot.
1195748	Network lockdown is enforced when the VPN is connected.
1199155	Save username option from EMS does not work properly when trying to connect to IKEv2 tunnel.

Bug ID	Description
1199352	Missing DH-Group 28 for IPSEC phase 1 and phase 2 settings.
1205084	IPsec VPN tunnel that requires client certificate fails to connect after upgrade to 7.4.4.
1210330	Intermittent connection issue to IPSec VPN with error: *Last Disconnect Reason: VpnParameterConfigError*.
1212116	No traffic passes over VPN tunnel when using SHA512.
1213765	IPsec VPN tunnel with SHA-512 (IKEv2) is established successfully but no data transmission from FortiClient to FortiGate through the tunnel.
1215480	FortiVNAError when establishing IPsec VPN tunnel after fresh installation of FortiClient.
1215952	The DPD configuration does not work as expected.
1217208	Unclear IPsec error messages.

Remote Access - SSL VPN

Bug ID	Description
1184072	SSL VPN host check fails when both GUID and version (e.g., 4.18.23110.3) are specified.
1192332	SSL VPN tunnels are not listed in FortiTray if the IPsec section is disabled in the EMS remote access profile containing only SSL VPN tunnels.
1194015	Security alert for untrusted server certificate when the SSL VPN tunnel tries to autoconnect.
1198658	SAML-based SSL VPN tunnel does not work when multiple gateways are configured for VPN resilience.
1199635	*Enforce Acceptance of Disclaimer Message* does not work for SSL VPN tunnels.
1199759	Unable to establish SSL VPN.
1208884	SSL VPN does not work with LoginTC (Radius Server) and 2FA.

Vulnerability Scan

Bug ID	Description
1140857	False positives in vulnerability scan results on Windows 11 23H2.

Web Filter and plugin

Bug ID	Description
1255625	Update FortiClient Windows and FortiClient EMS to recognize newly issued April 16, 2026 Digicert CA used by FortiGuard Anycast servers.
1193198	Website loading is slow with the Web Filter Browser Extension.
1198223	Incorrect destination port for URLs in FortiClient Web Filter logs.
1199364	FortiClient Web Filter Extension fails to block `copilot.microsoft.com` and `google.com` in Microsoft Edge and Google Chrome

ZTNA

Bug ID	Description
1008632	When visiting SaaS application web pages using ZTNA, web pages can stall or return an ERR_CERT_COMMON_NAME_INVALID error.

ZTNA TCP/UDP Forwarding

Bug ID	Description
1045428	ZTNA destination rules work only with full FQDN and not hostname.
1177255	Wildcard ZTNA destinations do not exclude the EMS FQDN and/or allow to specify exceptions from the wildcard domain.

Security Posture Tags

Bug ID	Description
1170327	FortiGate sometimes cannot resolve IP for client in security posture tag after the user disconnects and connects VPN immediately.
1175158	FortiClient cannot receive a tag from a combination rules randomly.
1205691	The `last Windows Update time` tag is lost after FortiClient is upgrade from 7.4.3 to 7.4.4.

Zero Trust Telemetry (On Boarding)

Bug ID	Description
1078953	SaaS and SaaS group ZTNA applications with UDP protocol fail to work.
1183973	After de-registeration from cloud EMS, FortiClient auto-registers back to cloud EMS on reboot.
1187361	Autoconnect is triggered even when the endpoint is on fabric.

Other

Bug ID	Description
1119669	FortiClient frequently loses user identity information.

Vulnerabilities and Exposures

FortiClient (Windows) 7.4.5 is no longer vulnerable to the following CVE references. Visit https://fortiguard.com/psirt for more information.

Bug ID	Description
1198148	CVE-2025-6965
1193312	CVE-2025-62676

Known issues

Known issues are organized into the following categories:

- New known issues on page 23
- Existing known issues on page 24

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 7.4.5.

Deployment and installers

Bug ID	Description
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.

Application Firewall

Bug ID	Description
1219088	Alert messages containng "Linux.Kernel.Netfilter.xt_TCPMSS.DoS" after upgrade to 7.4.4.

Privilege Access Management

Bug ID	Description
1203452	FortiPAM extension does not pass credentials to Elastic Web server.

Remote Access - IPsec VPN

Bug ID	Description
1168839	EMS IPsec VPN drops when uploading large files via SMB.
1239093	IPsec VPN tunnels with EAP enabled fail to connect with local or LDAP user authentication before logon if *Save Username* is enabled.

Other

Bug ID	Description
1189783	Forticlient FSSOMA does not send the AzureUserInfo to FortiAuthenticator intermittently.

Existing known issues

The following issues have been identified in a previous version of FortiClient (Windows) and remain in FortiClient (Windows) 7.4.5.

Application Firewall

Bug ID	Description
1219602	Application Firewall does not block AnyDesk.

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).

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+).

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.
1215862	On-fabric detection rules does not work as expected with default gateway MAC address: on-fabric devices are incorrectly shown as off-fabric.

Malware Protection

Bug ID	Description
1098883	Sandbox does not restore file when antivirus is not installed.
1211995	Malware protection causes issues with accessing SD card through Bosch Video Client.

#1236056 Driver (3M PRF UMDF USB driver) impacted if 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
999139	Laptop Wifi DNS setting is stuck in unknown DNS server after FortiClient connects and disconnects IPsec or SSL VPN.
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.

Remote Access - IPsec VPN

Bug ID	Description
1105003	Machine tunnel persists after hibernation, preventing user tunnel from establishing.
1116375	IPsec IKEv2 VPN with session resumption is unable to switch between different wifi SSID.
1114230	FortiClient cannot change radius user expired password on FortiClient IPsec VPN. Fields do not change.
1189237	IPsec does not have IPv6 support in 7.4.4 because of dual VPN changes.
1197941	Session resumption does not work. FortiClient disconnect IKEv2 VPN with DPD timeout even with physical NIC disconnected.

Remote Access - SSL VPN

Bug ID	Description
999139	Network adapter DNS setting gets stuck in unknown DNS server after SSL VPN connects and disconnects.
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.

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.
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.
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.

Release Notes

FortiClient (Windows) 7.4.5