FORTINET

# Release Notes

## FortiClient (Windows) 7.2.4

**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

June 25, 2024
FortiClient (Windows) 7.2.4 Release Notes
04-724-998650-20240625

# TABLE OF CONTENTS

# Change log

| Date | Change description |
|---|---|
| 2024-03-04 | Initial release of 7.2.4. |
| 2024-03-06 | Updated Firmware images and tools on page 9. |
| 2024-03-13 | Added 1009737 to Known issues on page 18. |
| 2024-03-20 | Added 1008116 to Known issues on page 18. |
| 2024-04-04 | Updated:<br>• SSL VPN with SAML issue on page 8<br>• Known issues on page 18<br>• Other on page 30 |
| 2024-04-08 | Updated FortiGuard Web Filtering Category v10 Update on page 7. |
| 2024-04-25 | Updated:<br>• Resolved issues on page 14<br>• Known issues on page 18 |
| 2024-06-25 | Added Nested VPN tunnels on page 8. |

# Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 7.2.4 build 0972.



Review all sections prior to installing FortiClient.

FortiClient (Windows) 7.2.4 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 7.2.4 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.

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.

Please read the following CSB for more information to caveats on the usage in FortiManager and FortiOS:
https://support.fortinet.com/Information/Bulletin.aspx

# SSL VPN with SAML issue

SSL VPN with SAML may fail to bring up the VPN when the CA certificate is saved to *Personal Certificates*. When this occurs, you may observe the VPN stuck at 0% with an error message in the *Notifications* tab reading: *The server you want to connect to requests identification, please choose a certificate and try again. (-6005)*

You can use one of the following workarounds for this issue. The workarounds support Windows 10 and 11 with external and internal browsers:

1. Move the CA certificate to the corresponding folder instead of the personal store. For example, you may move the certificate to *Certificates (Current User)\Trusted Root Certification Authorities* or *Intermediate Certification Authorities*.
2. Remove the CA certificate from *Certificates (Current User)\Personal\Certificates* if unneeded.
3. If the SSL VPN tunnel does not require certificate authentication, set a certificate filter to NOT match any certificate. The following shows an example XML configuration:

```
<certificate>
   <common_name>
      <match_type>wildcard</match_type>
      <pattern>*</pattern>
   </common_name>
   <issuer>
      <match_type>simple</match_type>
      <pattern>NOTHING</pattern>
   </issuer>
</certificate>
```

4. Set `<certs_require_keyspec>` to `1`.
   - If you set this element to `0`, FortiClient includes all certificates that have a NULL key specification when prompting the user to select a certificate.
   - If you set this element to `1`, FortiClient only lists certificates that include AT_KEYEXCHANGE/AT_SIGNATURE/CERT_NCRYPT_KEY_SPEC when prompting the user to select a certificate. The state of the key spec is only accessible by querying the certificate for its private key. If the certificate is on a smartcard or if the private key is password-protected, Windows requests a PIN/password. This can result in unwanted PIN/password prompts when the FortiClient GUI is opened. For example, it can result in PIN/password prompts when just viewing the *Remote Access* tab in the FortiClient GUI, with potentially one prompt for each certificate on the smartcard.

   The following shows an example XML configuration:

```
<vpn>
   <options>
      <certs_require_keyspec>1</certs_require_keyspec>
   </options>
</vpn>
```

# 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 |
|---|---|
| FortiClientTools_7.2.4.0972.zip | Zip package containing miscellaneous tools, including VPN automation files. |
| FortiClientSSOSetup_ 7.2.4.0972_x64.zip | Fortinet single sign on (FSSO)-only installer (64-bit). |
| FortiClientVPNSetup_ 7.2.4.0972_x64.exe | Free VPN-only installer (64-bit). |

EMS 7.2.4 includes the FortiClient (Windows) 7.2.4 standard installer and zip package containing FortiClient.msi and language transforms.

The following tools and files are available in the FortiClientTools_7.2.4.0972.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_7.2.4.0972_x64.zip | Standard installer package for Windows (64-bit). |
| FortiClientVPNSetup_7.2.4.0972_x64.exe | Free VPN-only installer (64-bit). |

Review the following sections prior to installing FortiClient version 7.2.4: Introduction on page 6 and Product integration and support on page 11.

# Upgrading from previous FortiClient versions

To upgrade a previous FortiClient version to FortiClient 7.2.4, do one of the following:

- Deploy FortiClient 7.2.4 as an upgrade from EMS. See Recommended upgrade path.
- Manually uninstall existing FortiClient version from the device, then install FortiClient (Windows) 7.2.4.

FortiClient (Windows) 7.2.4 features are only enabled when connected to EMS 7.2.

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

You must be running EMS 7.2 before upgrading FortiClient.

# Downgrading to previous versions

FortiClient (Windows) 7.2.4 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 7.2.4 product integration and support information:

| | |
|---|---|
| **Desktop operating systems** | • Microsoft Windows 11 (64-bit)<br>• Microsoft Windows 10 (64-bit) |
| **Server operating systems** | • Microsoft Windows Server 2022<br>• Microsoft Windows Server 2019<br>FortiClient 7.2.4 does not support Windows Server Core.<br>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.<br>Microsoft Windows Server 2019 supports zero trust network access (ZTNA) with FortiClient (Windows) 7.2.4.<br>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.<br>• Compatible operating system and minimum 2 GB RAM<br>• 1 GB free hard disk space<br>• Native Microsoft TCP/IP communication protocol<br>• Native Microsoft PPP dialer for dialup connections<br>• Ethernet network interface controller (NIC) for network connections<br>• Wireless adapter for wireless network connections<br>• Adobe Acrobat Reader for viewing FortiClient documentation<br>• Windows Installer MSI installer 3.0 or later |
| **AV engine** | • 6.00287 |
| **VCM engine** | • 2.0040 |
| **FortiAnalyzer** | • 7.4.0 and later<br>• 7.2.0 and later<br>• 7.0.0 and later |
| **FortiAuthenticator** | • 6.5.0 and later<br>• 6.4.0 and later<br>• 6.3.0 and later<br>• 6.2.0 and later<br>• 6.1.0 and later<br>• 6.0.0 and later |
| **FortiClient EMS** | • 7.2.0 and later |

| | |
|---|---|
| **FortiManager** | • 7.4.0 and later<br>• 7.2.0 and later<br>• 7.0.0 and later |
| **FortiOS** | The following FortiOS versions support ZTNA with FortiClient (Windows) 7.2.4. This includes both ZTNA access proxy and ZTNA tags:<br>• 7.4.0 and later<br>• 7.2.0 and later<br>• 7.0.6 and later<br>The following FortiOS versions support IPsec and SSL VPN with FortiClient (Windows) 7.2.4:<br>• 7.4.0 and later<br>• 7.2.0 and later<br>• 7.0.0 and later<br>• 6.4.0 and later<br>• 6.2.0 and later<br>• 6.0.0 and later |
| **FortiSandbox** | • 4.4.0 and later<br>• 4.2.0 and later<br>• 4.0.0 and later<br>• 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.

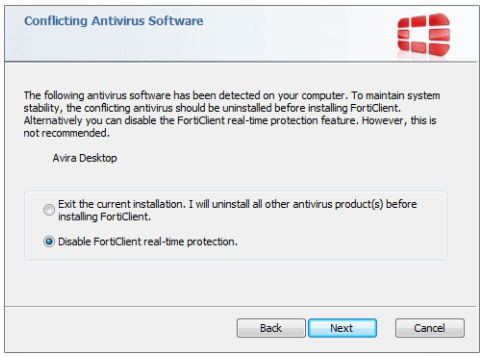
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

## Conflicts with third party AV products

The FortiClient antivirus (AV) feature 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 7.2.4 are as follows:

| Version | Product code |
|---|---|
| Enterprise | 611804A7-F14E-45A2-9F55-345D33EDD28E |
| VPN-only agent | D6A52B20-063A-4BF6-8228-CDADBF8ACBCF |
| Private access management-only agent | E28AF72E-B96C-405E-8281-7F1329ADB947 |
| Single sign on-only agent | 165D1BE3-2F3D-4E74-8108-74B755371E69 |

See Configuring the FortiClient application in Intune.

# Resolved issues

The following issues have been fixed in version 7.2.4. For inquiries about a particular bug, contact Customer Service & Support.

## ZTNA connection rules

| Bug ID | Description |
|---|---|
| 885014 | Zero trust network access (ZTNA) fails to resolve FQDN destination hosts with certain domains. |
| 976003 | Web access with ZTNA proxy using FQDN fails to work. |

## Web Filter and plugin

| Bug ID | Description |
|---|---|
| 812794 | Downloads are canceled in Firefox when Web Filter extension is enabled. |
| 984427 | Web Filter traffic logs show that 0 bytes were sent and received. |

## GUI

| Bug ID | Description |
|---|---|
| 975622 | GUI does not launch when user clicks EMS invitation link when FortiClient (Windows) is closed. |

## Endpoint control

| Bug ID | Description |
|---|---|
| 976602 | Use the previous resolved IP address when DNS server fails to respond endpoint DNS query. |
| 979593 | One-way message GUI is not translated. |
| 979756 | FortiClient disconnects from Windows primary EMS after first sync. |

## FSSOMA

| Bug ID | Description |
|---|---|
| 935090 | Single sign-on mobility agent (SSOMA) stops sending SSO session information to FortiAuthenticator while service runs on host. |

## Install and upgrade

| Bug ID | Description |
|---|---|
| 953124 | Orchestrator notification does not appear when upgrade is scheduled. |

## Logs

| Bug ID | Description |
|---|---|
| 811746 | FortiClient (Windows) sends duplicated and old logs to FortiAnalyzer. |
| 962704 | FortiClient floods FortiAnalyzer with SYN packets. |
| 966018 | FortiClient uploads logs more frequently than its configured upload interval. |
| 974960 | Log daemon makes connections to FortiAnalyzer when updating or starting VPN. |
| 1001042 | FortiClient cannot send SIEM logs to FortiAnalyzer. |

## Zero Trust tags

| Bug ID | Description |
|---|---|
| 976374 | CURRENT_USER registry tag does not work. |
| 988269 | Using spaces in common name when creating certificate-based ZTNA rules with regular expressions do not pass tags. |

## Vulnerability Scan

| Bug ID | Description |
|---|---|
| 956805 | FortiClient EMS shows *Scheduled* as patch status for critical FortiClient EMS Microsoft Office Memory Corruption Vulnerability, but it is not fixed with next telemetry communication. |
| 987137 | vcm.exe 2.0.39.39 crashes. |

## Remote Access

| Bug ID | Description |
|---|---|
| 949945 | Network lockdown blocks FortiClient Cloud Telemetry. |
| 966713 | User certificate-only tunnels do not autoconnect if user does not connect the tunnel once before logging out of Windows. |
| 976050 | FortiClient does not provide Entrust eGRID information so user can put in their 2F grid information. |
| 979166 | Black screen appears on VPN before logon. |

## Remote Access - IPsec VPN

| Bug ID | Description |
|---|---|
| 909573 | With multifactor authentication enabled and autoconnect, user account password becomes empty after Windows login. |
| 912980 | IPsec VPN fails to connect if `vpn-ems-sn-check` is enabled and FortiClient is registered to custom site. |
| 953319 | IPsec VPN IKEv2 with IPv6 gateway does not assign IPv6 address to the virtual adapter. |

## Remote Access - SSL VPN

| Bug ID | Description |
|---|---|
| 882408 | When using VPN before logon, if user password expires, user cannot change password on Windows login page. |
| 890000 | FortiClient 7.2.0 configured with `on-os-start-connect` is slow compared to FortiClient 7.0.7. |
| 907248 | FortiClient cannot connect to FortiSASE SAML VPN using OneLogin as identity provider (IdP) with |

| Bug ID | Description |
|---|---|
| | built-in browser when IdP requires client certificate. |
| 930740 | FortiClient (Windows) cannot set up SSL VPN if the password contains Polish characters ł, ą, and ń. |
| 936354 | FortiClient (Windows) cannot establish SSL VPN connection with Azure SAML when Micorsoft Entra ID auto login is enabled. |
| 951269 | SSL VPN logs out immediately after login when application split tunnel is enabled. |
| 954004 | FortiClient (Windows) cannot establish DTLS tunnel when handshake packet has a large MTU. |
| 962287 | SSL VPN reaches an infinite loop that keeps trying to connect to SSL VPN but fails. |
| 963039 | SslvpnAgent: Pipe is broken for writing. |
| 970620 | SAML SSL VPN still connects to SAML without asking for credentials when save password is disabled. |
| 974129 | Script error occurs while initiating SAML VPN. |
| 998146 | SSL VPN disconnects every 20-30 minutes. |

## PAM

| Bug ID | Description |
|---|---|
| 982033 | Native launchers fail after upgrading standalone FortiClient from previous version. |
| 990358 | Browser privilege access management (PAM) extension does not autofill credentials correctly for EMS and password field remains blank. |

## Other

| Bug ID | Description |
|---|---|
| 964456 | FortiClient does not allow Windows DNS only secure dynamic updates. |
| 971090 | FortiClient daemon (fcaptmon) has memory leak. |
| 982997 | FortiShield.sys causes blue screen of death on Windows 10. |

# Known issues

The following issues have been identified in FortiClient (Windows) 7.2.4. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

## Administration

| Bug ID | Description |
|---|---|
| 867818 | fortishield.sys and fortimon3.sys are incompatible with HVCI. |

## Application Firewall

| Bug ID | Description |
|---|---|
| 814391 | FortiClient Cloud application signatures block allowlisted applications. |
| 827788 | Threat ID is 0 on Firewall Events. |
| 834500 | FortiClient (Windows) fails to block Application Firewall categories when Web Client category is set as *Monitor*. |
| 842534 | After upgrade, Application Firewall blocks internal webpage. |
| 844997 | FortiClient loses several packets on different internal resources after connecting telemetry. |
| 860062 | Application Firewall slows down opening of Microsoft Entra ID Users and Computers application. |
| 869671 | FortiClient (Windows) bypasses Application Firewall block after matching detection rule. |
| 879985 | Application Firewall fails to block Web.Client category HTTPS traffic. |
| 884911 | FortiClient detects IntelliJ IDEA Community Edition 2021.2.2 as Java.Debug.Wire.Protocol.Insecure.Configuration. |
| 902866 | Application Firewall does not block Google Drive. |
| 958651 | Application Firewall violation list always shows violated programs as the same as applications, which is not as accurate as Windows. |
| 980803 | Image becomes corrupted or damaged with a green patch when trying to view it from a shared location. |

## Avatar and social network login

| Bug ID | Description |
|---|---|
| 878050 | FortiClient avatar does not update on FortiOS dashboards and FortiOS cannot show updated information. |
| 950503 | FortiClient does not use image that user uploaded as their avatar. |
| 1010145 | FortiClient (Windows) grays out avatar page when using Salesforce login. |

## Chromebook

| Bug ID | Description |
|---|---|
| 997927 | On Chromebook, fallback action is to override exclusion list, which is unlike FortiClient (Windows). |

## Configuration

| Bug ID | Description |
|---|---|
| 730415 | FortiClient backs up configuration that is missing locally configured zero trust network access (ZTNA) connection rules. |

## Deployment and installers

| Bug ID | Description |
|---|---|
| 783690 | Reboot prompt does not display after user login. |
| 870370 | Upgrading FortiClient from FortiClient Cloud uses expired invitation code to register. |
| 1012187 | Upgraded FortiClient installs features that are disabled in the EMS deployment package. |

## Endpoint control

| Bug ID | Description |
|---|---|
| 804552 | FortiClient shows all feature tabs without registering to EMS after upgrade. |
| 815037 | After administrator selects *Mark All Endpoints As Uninstalled*, FortiClient (Windows) connected with verified user changes to unverified user. |
| 833717 | EMS shows endpoints as offline, while they show their own status as online. |
| 841764 | EMS does not show third-party features in endpoint information. |
| 855851 | EMS remembered list shows FQDN duplicates. |
| 868230 | "Connection expiring due to FortiClient Connect license exceeded" error occurs. |
| 996844 | FortiClient loses VPN configuration settings and no VPN tunnels are available. |
| 996850 | FortiClient sends different username to EMS when user logs on to computer with SmartCard. |
| 1002476 | Disconnecting from EMS using password does not work. |
| 1003435 | FortiClient (Windows) shows Sandbox, Web Filter, and Vulnerability Scan profiles when unregistered from EMS due to expired license. |
| 1016378 | FortiClient (Windows) does not prompt for user verification when other Azure user is logged in. |

## Endpoint management

| Bug ID | Description |
|---|---|
| 916566 | FortiClient reports USB as blocked but user can access the storage files. |

## GUI

| Bug ID | Description |
|---|---|
| 888185 | FortiClient does not minimize after successful VPN connection. |
| 902595 | SAML prompt flashes on autoconnect. |
| 981993 | Remote Access GUI shows an incorrect message when FortiClient (Windows) is unregistered from EMS. |
| 990496 | FortiClient flickers and opens. |
| 1011345 | GUI has mistranslation in Slovak for Cloud Sandbox. |

## Endpoint policy and profile

| Bug ID | Description |
|---|---|
| 889517 | EMS fails to assign the correct endpoint policy and shows FortiClient as out-of-sync despite the client syncing. |
| 915678 | FortiClient does not send acknowledged event to EMS if it disconnects and reconnects to EMS immediately after the user acknowledges the one-way message. |
| 989640 | FortiClient does not follow EMS profile after EMS updates feature selecting setting. |

## Endpoint security

| Bug ID | Description |
|---|---|
| 975704 | FortiClient does not report most recent completed scan timestamp to EMS and causes last scan time to show incorrectly on EMS dashboard. |

## Install and upgrade

| Bug ID | Description |
|---|---|
| 955268 | User can uninstall FortiClient when it is registered to EMS. |
| 960301 | FortiClient fails to install due to orphaned registry key. |
| 982747 | FortiPAM password filter extension is not removing automatically from Firefox when FortiClient (Windows) is uninstalled. |
| 993353 | FortiClient is missing telemetry pages after upgrading from 7.2.2 to 7.2.3. |

## Malware Protection and Sandbox

| Bug ID | Description |
|---|---|
| 844988 | FortiClient (Windows) does not block USB drive with attempt to copy contents even if WPD/USB is set to block in profile. |
| 857041 | Windows 10 security center popup shows FortiClient and Windows Defender are off. |
| 863802 | FortiClient (Windows) cannot detect SentinelOne when they have product on OS level. |

| Bug ID | Description |
|---|---|
| 871078 | Antiexploit protection blocks Adobe plugin in Chrome. |
| 872970 | Bubble notifications do not appear when inserting USB drive in endpoint machine. |
| 874578 | Real-time protection (RTP) does not delete quarantined files after cullage time. |
| 901065 | Logitech driver breaks after installing FortiClient with Malware Protection feature enabled in installer. |
| 915300 | FortiClient (Windows) detects file configured as exception as malware. |
| 919007 | FortiClient (Windows) cannot scan mapped drives on-demand. |
| 919499 | Windows Security Center shows that FortiClient (Windows) is inactive when FortiClient (Windows) is running and up-to-date. |
| 946756 | EMS logs USB events logged when there is an allow rule configured. |
| 948985 | update_task downloads AV signature from FDS, but AV engine fails to verify the signature. FortiClient (Windows) does not keep copy of problem signature. |
| 956963 | FortiClient Spoolsv is blocked when Windows antimalware scan is enabled. |
| 966195 | Antimalware detects W64/AI.Pallas Suspicious and fails to quarantine. |
| 972036 | Sandbox agent uses high CPU/memory/I/O when connecting to external SSD. |
| 972671 | If Malware Protection is enabled, Valorant fails to work. |
| 984972 | RTP fails to detect ransomware Lockbit.K!tr.ransom. |
| 988110 | Sandbox fails to exclude trusted files from scanning if the file is in network folder. |
| 991539 | FortiClient (Windows) cannot open AV logs on the scan result page after performing on-demand or scheduled scan. |
| 996029 | fmon blocks shared directory that sumidero SNC SQL Tool uses due to suspicious virus that FortiClient (Windows) detects in bitacora.exe. |
| 996431 | FortiClient (Windows) cannot block remote NDIS device when the net class device is set to block in removable media access function. |
| 998905 | FortiClient cannot detect a malicious file, PowerISO6.exe. |
| 1004611 | FortiClient removable media access does not scan USB drive. |
| 1012083 | If Anti Exploit is enabled on EMS, FortiClient (Windows) blocks certificates on DocuSign. |

# Zero Trust tags

| Bug ID | Description |
|---|---|
| 1002079 | Security Zero Trust tagging rule to tag endpoints where automatic updates are enabled does not work as expected. |

| Bug ID | Description |
|---|---|
| 1013973 | Host check policy does not work as expected when using OR logic. |

## Software Inventory

| Bug ID | Description |
|---|---|
| 737970 | Software Inventory on EMS does not properly reflect software changes (adding/deleting) on Windows endpoints. |
| 844392 | Software Inventory shows last installation time in future. |

## Performance

| Bug ID | Description |
|---|---|
| 1012529 | FortiClient constantly and very frequently writes event files and cause CPU and overheating issues. |
| 1015900 | FortiESNAC has high RAM consumption on Windows servers. |

## Quarantine management

| Bug ID | Description |
|---|---|
| 1009212 | EMS FCrestorequarant tool does not delete the restored file from quarantine folder. |

## RTP

| Bug ID | Description |
|---|---|
| 1013796 | Real-time protection (RTP) scans compressed files above maximum file size defined in EMS. |

## Remote Access

| Bug ID | Description |
|---|---|
| 973808 | On a non-compliant endpoint using a non-English OS, such as Spanish, FortiClient (Windows) fails to show warning prompt when trying to connect to VPN. |
| 992814 | Disclaimer acceptance always pops up when VPN always on is configured. |
| 997718 | When FortiClient enables autoconnect, it behaves like always-up is enabled. |
| 1000706 | VPN before Windows logon requires second attempt -due to CachedLogonsCount issue. |
| 1021770 | Connecting to VPN in FortiTray does not open *Remote Access* tab when a remote gateway is not reachable. |

## Remote Access - IPsec

| Bug ID | Description |
|---|---|
| 758424 | Certificate works for IPsec VPN tunnel if put on local computer but fails to work if same certificate is in current user store. |
| 969995 | Autoconnect does not work reliably with IPsec VPN using username/password with one-time password and client certificate. |
| 971554 | FortiClient (Windows) sends access request for IPsec VPN when password renewal is canceled. |
| 986732 | After upgrading, IPsec VPN IKEv2 tunnel stops working. |
| 995970 | FortiClient (Windows) has GUI issues if connecting from FortiTray and the default tab is Remote Access. |
| 997277 | FortiClient autoconnects without autoconnect configured. |
| 1003780 | IPsec VPN IKEv1 with certificate authentication has connection issues when off-net. |
| 1005618 | IPsec VPN fails to connect if R3 Intermediate certificate is NOT imported and ISRG Root X1 issues FortiGate server certificate. |

## Remote Access - SSL VPN

| Bug ID | Description |
|---|---|
| 837391 | FortiClient does not send public IP address for SAML, leading to 0.0.0.0 displaying on FortiOS and FortiSASE. |
| 874759 | SSL VPN has DNS issues if AWS Route53 is configured for name resolution. |

| Bug ID | Description |
|---|---|
| 875999 | FortiClient does not show GUI prompt to enter PIN for SSL VPN certificate stored on USB PKI/SmartCard device. |
| 884926 | Okta SAML token window popup displays in low resolution. |
| 909244 | SSL VPN split DNS name resolution stops working. |
| 909755 | SSL VPN split tunnel does not work for Microsoft Teams. |
| 920383 | FortiClient (Windows) always enables *Turn off smart multi-homed name resolution* on the Windows machine after successful connection. |
| 922941 | Connecting to SSL VPN with FQDN that resolves to both IPv4 and IPv6 as remote gateway gets stuck at 98%. |
| 942668 | Split DNS on SSL VPN only resolves the first DNS server. |
| 950787 | Domain filter cannot block access specific server FQDN. |
| 961079 | New Microsoft Teams application does not work if application-based split tunnel is used. |
| 964036 | Gateway selection (e.g. saml-login) based on ping speed or TCP round trip does not work. |
| 979646 | FortiClient (Windows) cannot connect VPN with [-7200] or [-6006] error while using SAML with external browser. |
| 989864 | When network lockdown is enabled in Remote Access profile, signing in to Windows takes longer than usual. |
| 994884 | SSL VPN connections get stuck on 40%. |
| 999205 | Internal VPN browser is vulnerable for man in the middle attack. |
| 1000589 | VPN is stuck on connecting and error 6005 occurs if SAML takes longer than 60 seconds. |
| 1002294 | FortiClient does not reconnect to the VPN until restarted. |
| 1002456 | After upgrading FortiClient, customized host check fail warning does not appear when tag is on device. |
| 1006295 | FortiClient fails to consistently connect and gets stuck at 40% with DNS round robin of FortiGates (SASE). |
| 1008116 | After upgrade, SAML VPN is stuck at 0% with error (-6005) when CA is in user store. |
| 1015381 | FortiClient takes longer than usual to autoconnect. |
| 1016971 | FortiClient fails to autoconnect and gets stuck in *Connecting* state until reboot. |
| 1018126 | WMIPRVSE.exe service CPU% spikes when connected to SIA VPN. |

## Vulnerability Scan

| Bug ID | Description |
|---|---|
| 795393 | Vulnerability events are not removed from EMS after successful patch. |
| 849485 | FortiClient wrongly detects AnyDesk vulnerabilities CVE-2021-44426 and CVE-2021-44425. |
| 869253 | FortiClient (Windows) detects vulnerability when the required KB is installed. |
| 989431 | Vulnerability Scan recognizes Windows 10 as Windows 11. |
| 1010776 | FortiClient detects incorrect vulnerability for Rocket.chat and Rocket.chat.electron. |
| 1011358 | Vulnerability Scan shows no results, but Qualys reports multiple for same endpoints. |

## Logs

| Bug ID | Description |
|---|---|
| 849043 | SSL VPN add/close action does not show on FortiGate *Endpoint Event* section. |
| 903480 | FortiClient (Windows) fails to generate log message to FortiAnalyzer or EMS when ZTNA tag prohibits VPN access. |
| 948887 | FortiClient does not send Windows log of Exchange Server logon failure (Event ID 4625). |
| 965729 | FortiClient (Windows) does not send Web Filter monitor and block categories logs to FortiAnalyzer. |
| 979323 | FortiClient does not send any logs to FortiAnalyzer unless *Log All URLs* is enabled. |
| 984729 | Traffic logs do not populate on FortiAnalyzer. |
| 985044 | FortiClient log level does not change from debug and user cannot delete log files from "%AppData%". |
| 988706 | Web Filter log in FortiAnalyzer does not have URL information. |
| 993163 | FortiClient (Windows) does not generate fcdblog log file in the trace logs folder. |
| 996345 | Disabling logging from EMS profile still results in it being enabled. |
| 996767 | FortiAnalyzer does not show endpoint logs after endpoint upgrade from 7.0.9 to 7.2.3. |
| 1016539 | Vulnerability reports do not display username information in FortiAnalyzer. |

# Web Filter and plugin

| Bug ID | Description |
|---|---|
| 519066 | User cannot print to WSD network printer when FortiProxy is enabled. |
| 836906 | After FortiClient install, extended uptime results in audio cracking. |
| 851700 | Users get popup message from FortiClient: *Microsoft Edge extension policy anomaly detected, please restart browser.* |
| 871325 | Web Filter breaks DW Spectrum. |
| 875298 | Exclusion list does not work properly with regular expressions. |
| 883568 | Web Filter causes Docker pull command to fail and connectivity issues afterward. |
| 890433 | Firefox extension is stuck on older version. |
| 903426 | User cannot access internal application with Web Filter enabled.<br>**Workaround**: Add a simple rule to allow HTTP/HTTPS server IP addresses. |
| 904840 | When a user is performing a device recovery in iTunes, error 3500 occurs. |
| 909060 | User cannot update information on internal portal with Web Filter active. |
| 911410 | Safe Search restriction level does not apply properly if it is enabled for both Web and Video Filters. |
| 939986 | Web Filter blocks LUXTRUST middleware. |
| 948500 | Video Filter does not block YouTube channel if channel ID case changes in the URL. |
| 962502 | Web Filter does not respect exclusion list when imported from FortiGate with web category overrides. |
| 978252 | Microsoft Edge guest browsing bypasses Web Filter blocked sites. |
| 996420 | Web Filter has issue with resolved IP addresses in multiple ISDB objects such as cloud applications. |
| 997118 | Web Filter extension does not apply DNS restrictions when Safe Search is enabled on Web Filter profile. |
| 998747 | FortiClient does not block Gmail when using Gmail link in Chrome browser. |
| 999256 | FortiClient (Windows) blocks some HTTP exclusions that it should allow. |
| 1002532 | FortiClient does not take exceptions set on Web Filter profile and blocks download of RDP plugin, blocking access to server. |
| 1008112 | Web Filter blocks downloading some files in web.whatsapp.com and always shows block page. |
| 1013487 | Web Filter blocks WebEx as unrated. |

# ZTNA connection rules

| Bug ID | Description |
|---|---|
| 814953 | Using an external browser for SSH ZTNA requires restarting FortiClient on Windows 11. |
| 836246 | Going from off-Fabric to on-Fabric does not stop the ZTNA service and keeps endpoint from connecting. |
| 839589 | ZTNA TCP forwarding not working for GoAnywhere application. |
| 857909 | FortiClient (Windows) does not support enabling encryption for ZTNA TCP forwarding rules acquired from ZTNA service portal. |
| 857999 | FortiClient does not support use of external browser for SAML authentication for ZTNA rules acquired through service portal. |
| 872153 | Old certificate is not deleted when FortiClient is uninstalled or upgraded. |
| 918045 | FortiClient (Windows) requests ZTNA certificate when switching between user accounts. |
| 919832 | ZTNA stops working after days with the error message *No ZTNA client certificate was provided*. |
| 921406 | ZTNA destination rule using hostname does not work. |
| 931275 | ZTNA destination rules stop working. |
| 942413 | Issue occurs when trying to reach a ZTNA destination added to FortiClient manually from public IP address as it does not resolve. |
| 949999 | SAML authentication does not work with Azure AD certificate-based authentication. |
| 952888 | IPv6 DNS servers bypass inline CASB IPv4 access proxies. |
| 954946 | ZTNA TCP forwarding does not show the untrusted certificate prompt warning with SAML authentication. |
| 955377 | FortiClient (Windows) blocks ZTNA because *device is offline*. |
| 955437 | With multiple browsers installed and external browser used for SAML authentication, choosing browser option does not show up if user does not choose any. |
| 965476 | User cannot access website with certificate warning and Forticlient DNS Root certificate signs the certificate. |
| 967199 | *No ZTNA client certificate was provided* error occurs when trying to access HTTPS page. |
| 975845 | FortiClient must notify end user that certificate is not trusted for ZTNA connection when `disallow_invalid_server_certificate` is enabled. |
| 976028 | ZTNA feature driver fortitransctrl fails to start and causes ZTNA TCP forwarding to not work as expected. |
| 977407 | ZTNA TCP forwarding with authentication does not work properly for SaaS and SaaS group applications. |
| 990864 | With SAML for ZTNA authentication, after closing the first session, the second session continues to request credentials. |

| Bug ID | Description |
|---|---|
| 992649 | User cannot create FortiGate tunnel if FortiGate works as both VPN and ZTNA proxy server. |
| 995677 | ZTNA TCP forwarding fails to prompt for SAML authentication with external browser after closing and reattempting the connection. |
| 1001116 | FortiClient requests SAML credentials after network change in ZTNA connections. |

## FSSOMA

| Bug ID | Description |
|---|---|
| 900953 | SSOMA does not send SSO sessions information to FortiAuthenticator. |
| 909844 | FSSO sessions drop earlier than expected. |
| 964769 | FSSOMA for Entra ID does not send tenant ID to FortiAuthenticator. |
| 995379 | FSSOMA does not properly install on CIS hardened Windows 10 and 11 image. |

## Onboarding

| Bug ID | Description |
|---|---|
| 982079 | FortiClient Cloud invitation with LDAP verification type to Entra ID fails with *Azure Token Required* error. |
| 1014158 | Telemetry page shows *Connecting to EMS* continuously when user authentication fails. |

## PAM

| Bug ID | Description |
|---|---|
| 993068 | Firefox FortiPAM launch secret does not record screen for newly opened tabs. It only records the first tab opened from launch secret. |
| 993164 | manifest.json needs update in Firefox PAM extension to include autoupdate link. |
| 1001231 | FortiPAM extension does not support Firefox. |
| 1015585 | FortiClient (Windows) closes entire MobeXterm application when a launched secret reaches the max session duration. |

## Other

| Bug ID | Description |
|---|---|
| 834389 | FortiClient has incompatibility with Fuji Nexim software. |
| 919017 | FortiClient changes the checksum hash of the installer for Baramundi Management Agent. |
| 984763 | NETIO.SYS/FortiWF2.sys causes blue screen of death (BSOD) on Windows 10. |
| 998183 | FortiESNAC.exe crashes and fails to update signatures. |
| 999139 | Laptop Wi-Fi DNS setting gets stuck in unknown DNS server after FortiClient connects to and disconnects from IPsec or SSL VPN. |
| 1006130 | FortiShield.sys causes BSOD with FortiClient. |
| 1013438 | FortiClient blocks RADIUS authentication on Arube HPE switch ports. |
| 1015385 | Redstor Backup Pro causes BSOD when FortiClient (Windows) scans it. |

www.fortinet.com