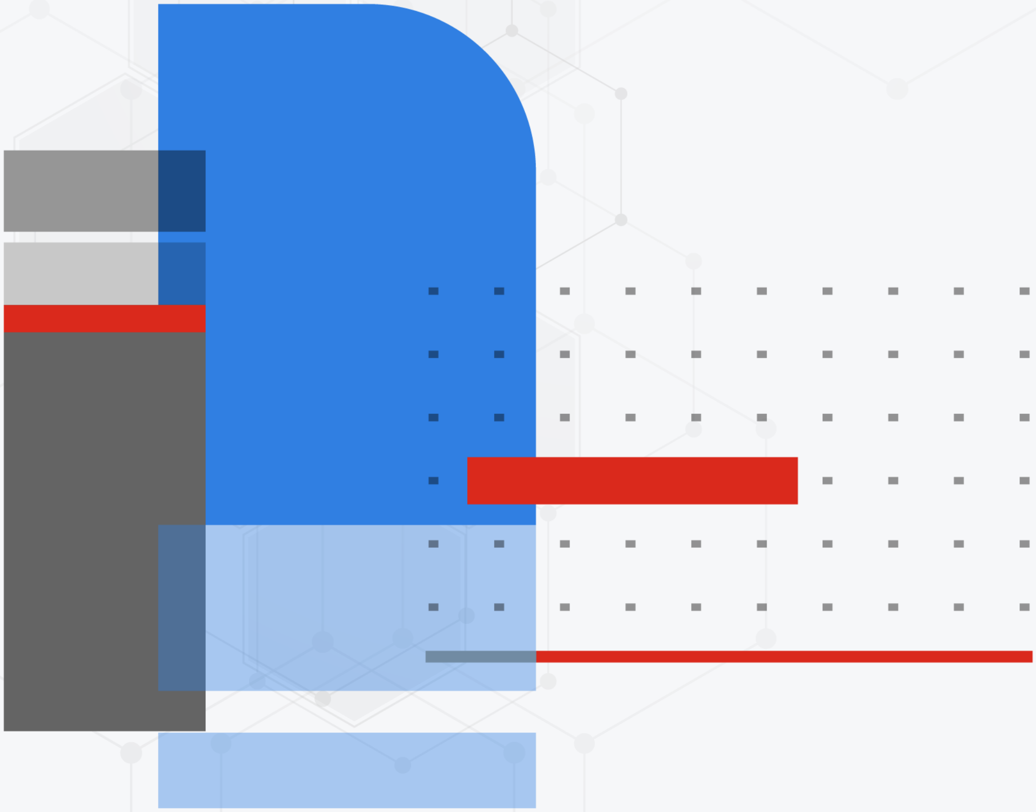
Release Notes

FortiProxy 7.4.12



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

January 06, 2026
FortiProxy 7.4.12 Release Notes
45-7412-1222622-20260106

TABLE OF CONTENTS

Change log

Date	Change Description
2025-11-17	Initial release.
2026-01-06	Added CVE-2025-25255 to Resolved issues on page 15.

Introduction

FortiProxy delivers a class-leading Secure Web Gateway, security features, unmatched performance, and the best user experience for web sites and cloud-based applications.

FortiProxy 7.4.12 supports upgrade from 7.4.x only. Refer to Deployment information on page 11 for detailed upgrade instructions.

All FortiProxy models include the following features out of the box:

Security modules

The unique FortiProxy architecture offers granular control over security, understanding user needs and enforcing Internet policy compliance with the following security modules:

Web filtering	The web-filtering solution is designed to restrict or control the content a reader is authorized to access, delivered over the Internet using the web browser. The web rating override allows users to change the rating for a web site and control access to the site without affecting the rest of the sites in the original category.
DNS filtering	Similar to the FortiGuard web filtering. DNS filtering allows, blocks, or monitors access to web content according to FortiGuard categories.
Email filtering	The FortiGuard Antispam Service uses both a sender IP reputation database and a spam signature database, along with sophisticated spam filtering tools on Fortinet appliances and agents, to detect and block a wide range of spam messages. Updates to the IP reputation and spam signature databases are provided continuously by the FDN.
CIFS filtering	CIFS UTM scanning, which includes antivirus file scanning and DLP file filtering.
Application control	Application control technologies detect and take action against network traffic based on the application that generated the traffic.
Inline CASB	The inline CASB security profile enables the FortiProxy to perform granular control over SaaS applications directly on policies.
Data Loss Prevention (DLP)	The FortiProxy DLP system allows you to prevent sensitive data from leaving your network.

Antivirus	Antivirus uses a suite of integrated security technologies to protect against a variety of threats, including both known and unknown malicious codes (malware), plus Advanced Targeted Attacks (ATAs), also known as Advanced Persistent Threats (APTs).
SSL/SSH inspection (MITM)	SSL/SSH inspection helps to unlock encrypted sessions, see into encrypted packets, find threats, and block them.
Intrusion Prevention System (IPS)	IPS technology protects your network from cybercriminal attacks by actively seeking and blocking external threats before they can reach potentially vulnerable network devices.
Zero Trust Network Access (ZTNA)	ZTNA is an access control method that uses client device identification, authentication, and Zero Trust tags to provide role-based application access. It gives administrators the flexibility to manage network access for users. Access to applications is granted only after device verification, authenticating the user's identity, authorizing the user, and then performing context based posture checks using Zero Trust tags.
Content Analysis	Content Analysis allow you to detect adult content images in real time. This service is a real-time analysis of the content passing through the FortiProxy unit.
Client-based native browser isolation (NBI)	Client-based native browser isolation (NBI) uses a Windows Subsystem for Linux (WSL) distribution (distro) to isolate the browser from the rest of the computer in a container, which helps decrease the attack surface.

Caching and WAN optimization

All traffic between a client network and one or more web servers is intercepted by a web cache policy. This policy causes the FortiProxy unit to cache pages from the web servers on the FortiProxy unit and makes the cached pages available to users on the client network. Web caching can be configured for standard and reverse web caching.

FortiProxy supports WAN optimization to improve traffic performance and efficiency as it crosses the WAN. FortiProxy WAN optimization consists of a number of techniques that you can apply to improve the efficiency of communication across your WAN. These techniques include protocol optimization, byte caching, SSL offloading, and secure tunneling.

Protocol optimization can improve the efficiency of traffic that uses the CIFS, FTP, HTTP, or MAPI protocol, as well as general TCP traffic. Byte caching caches files and other data on FortiProxy units to reduce the amount of data transmitted across the WAN.

FortiProxy is intelligent enough to understand the differing caching formats of the major video services in order to maximize cache rates for one of the biggest contributors to bandwidth usage. FortiProxy will:

- Detect the same video ID when content comes from different CDN hosts.
- Support seek forward/backward in video.
- Detect and cache separately; advertisements automatically played before the actual videos.

What's new

The following sections describe new features, enhancements, and changes in FortiProxy 7.4.12:

- Multi-condition support for proxy addresses and address groups on page 7
- Logging for license sharing events on page 7
- CLI changes on page 8

Multi-condition support for proxy addresses and address groups

When configuring proxy addresses and address groups, you can now specify multiple addresses or address groups and configure the AND/OR relationship among them, The addresses or address groups can then be used in firewall policies.

For example, you can now specify multiple addresses: A, B, C, D and configure them as "**A** AND **B**) OR (**C** AND **D**" using the following:

```
config firewall proxy-addrgrp
   edit "A_and_B"
      set logic-type and
      set member "A" "B"
   next
   edit "C_and_D"
      set logic-type and
      set member "C" "D"
   next
end
config firewall policy
   ed 1
      set dstaddr A_and_B C_and_D
      ...
   next
end
```

Logging for license sharing events

FortiProxy 7.4.12 adds logging for the following license sharing events:

- When a member becomes stale and recovers from stale status, the event is recorded on the root node.
- When a member node is promoted as root or reverts back as a member, the event is recorded on the member node.

- When the effective root node changes, the event is recorded on each member node.

See the License Sharing Deployment Guide for more details.

CLI changes

FortiProxy 7.4.12 includes the following CLI changes:

- `config web-proxy global`—Use the new `set policy-partial-match` subcommand to enable/disable policy partial match. The default is enable.
- `config firewall profile-protocol-options`—The `set domain-fronting` sub-command includes the new `strict` option to block and log domain fronting, including potential matching IP and domain. This option is different from the block option which blocks and logs domain fronting but not potential matching IP and domain.

Product integration and support

The following table lists product integration and support information for FortiProxy 7.4.12 build 721:

Type	Product and version
FortiProxy appliance	• FPX-400E • FPX-2000E • FPX-4000E • FPX-400G • FPX-2000G • FPX-4000G
FortiProxy VM	• FPX-AZURE • FPX-HY • FPX-KVM • FPX-KVM-ALI • FPX-KVM-AWS • FPX-KVM-GCP • FPX-KVM-OPC • FPX-VMWARE • FPX-XEN
Fortinet products	• FortiOS 6.x and 7.0 to support the WCCP content server • FortiOS 6.0 and 7.0 to support the web cache collaboration storage cluster • FortiManager - See the FortiManager Release Notes. • FortiAnalyzer - See the FortiAnalyzer Release Notes. • FortiSandbox and FortiCloud FortiSandbox- See the FortiSandbox Release Notes and FortiSandbox Cloud Release Notes. • FortiIsolator 2.2 and later - See the FortiIsolator Release Notes.
Fortinet Single Sign-On (FSSO)	5.0 build 0301 and later (needed for FSSO agent support OU in group filters) • Windows Server 2019 Standard • Windows Server 2019 Datacenter • Windows Server 2019 Core • Windows Server 2016 Datacenter • Windows Server 2016 Standard • Windows Server 2016 Core • Windows Server 2012 Standard • Windows Server 2012 R2 Standard • Windows Server 2012 Core

<table>
<tr><th>Type</th><th>Product and version</th></tr>
<tr><td></td><td><ul><li>Windows Server 2008 64-bit (requires Microsoft SHA2 support package)</li><li>Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package)</li><li>Windows Server 2008 Core (requires Microsoft SHA2 support package)</li><li>Novell eDirectory 8.8</li></ul></td></tr>
<tr><td><b>Web browsers</b></td><td><ul><li>Microsoft Edge</li><li>Mozilla Firefox version 87</li><li>Google Chrome version 89</li></ul>Other web browsers may work correctly, but Fortinet does not support them.</td></tr>
<tr><td><b>Virtualization environments</b></td><td>Fortinet recommends running the FortiProxy VM with at least 4 GB of memory because the AI-based Image Analyzer uses more memory compared to the previous version.
<table>
<tr><td><b>Hyper-V</b></td><td><ul><li>Hyper-V Server 2008 R2, 2012, 2012R2, 2016, 2019, and 2022</li></ul></td></tr>
<tr><td><b>Linux KVM</b></td><td><ul><li>RHEL 7.1/Ubuntu 12.04 and later</li><li>CentOS 6.4 (qemu 0.12.1) and later</li></ul></td></tr>
<tr><td><b>Xen hypervisor</b></td><td><ul><li>OpenXen 4.13 hypervisor and later</li><li>Citrix Hypervisor 7 and later</li></ul></td></tr>
<tr><td><b>VMware</b></td><td><ul><li>ESXi versions 6.5, 6.7, 7.0, and 8.0</li></ul></td></tr>
<tr><td><b>Openstack</b></td><td><ul><li>Ussuri</li></ul></td></tr>
<tr><td><b>Nutanix</b></td><td><ul><li>AHV</li></ul></td></tr>
</table></td></tr>
<tr><td><b>Cloud platforms</b></td><td><ul><li>AWS (Amazon Web Services)</li><li>Microsoft Azure</li><li>GCP (Google Cloud Platform)</li><li>OCI (Oracle Cloud Infrastructure)</li><li>Alibaba Cloud</li></ul></td></tr>
</table>

Deployment information

You can deploy the FortiProxy on a FortiProxy unit or VM. You can also upgrade or downgrade an existing FortiProxy deployment. Refer to Product integration and support on page 9 for a list of supported FortiProxy units and VM platforms.

Downloading the firmware file

1. Go to https://support.fortinet.com.
2. Click *Login* and log in to the Fortinet Support website.
3. From the *Support > Downloads* menu, select *Firmware Download*.
4. In the *Select Product* dropdown menu, select *FortiProxy*.
5. On the *Download* tab, navigate to the FortiProxy firmware file for your FortiProxy model or VM platform in the *Image Folders/Files* section. `.out` files are for upgrade or downgrade. `.zip` and `.gz` files are for new deployments.
6. Click *HTTPS* to download the firmware that meets your needs.

Deploying a new FortiProxy appliance

Refer to the FortiProxy QuickStart Guide for detailed instructions of deploying a FortiProxy appliance. Refer to Product integration and support on page 9 for a list of supported FortiProxy units.

Deploying a new FortiProxy VM

Refer to the FortiProxy Public Cloud or FortiProxy Private Cloud deployment guides for more information about how to deploy the FortiProxy VM on different public and private cloud platforms. Refer to Product integration and support on page 9 for a list of supported VM platforms.

Upgrading the FortiProxy

FortiProxy 7.4.12 supports upgrade from 7.4.x only.

If Security Fabric is enabled, all FortiProxy units must be upgraded to the same version. For example, if Security Fabric is enabled in FortiProxy 7.4.12, all FortiProxy devices in the Security Fabric must run FortiProxy 7.4.12. Otherwise, some devices may get stale or disconnected from the root, resulting in issues with fabric logging and address synchronization.

To upgrade FortiProxy units or VMs from 7.4.x to 7.4.12:

If you are using a RADIUS server that does not support the message-authenticator attribute, upgrading to 7.4.12 is not recommended.

1. Reboot the FortiProxy.

   You must reboot the FortiProxy before the upgrade process. Otherwise, the device may be damaged due to upgrade failure during critical processing.

2. In the GUI, go to *System > Fabric Management*.
3. Select the device you want to upgrade in the table and click *Upgrade*.
4. Click *Browse* in the *File Upload* tab.
5. Select the file on your PC and click *Open*.
6. Click *Confirm and Backup Config*.
7. Click *Continue*.

   The configuration file is automatically saved and the system will reboot.
8. Click *Reset All Dashboards* in the GUI to avoid any issues with FortiView.

If you are currently using FortiProxy 2.0.x, 7.0.x, or 7.2.x, Fortinet recommends that you perform the upgrade procedure for each major version in between from low to high before attempting to upgrade to 7.4.12. For example, to upgrade from 2.0.12 to 7.4.12, upgrade to 7.0.11 or later first, and then 7.2.5 or later (reboot before upgrading to 7.2.x), and then 7.4.0, and then 7.4.12.

Upgrading a FortiProxy 2.0.5 VM to 7.0.x requires a different upgrade process with additional backup and configuration as FortiProxy 2.0.6 introduced a new FortiProxy VM license file that cannot be used by earlier versions of the FortiProxy VM.

To upgrade a FortiProxy 2.0.5 VM to 7.0.x:

1. Back up the configuration from the GUI or CLI. Make sure the VM license file is stored on the PC or FTP or TFTP server.
2. Shut down the original VM.
3. Deploy the new VM. Make sure that there is at least 4 GB of memory to allocate to the VM.
4. From the VM console, configure the interface, routing, and DNS for GUI or CLI access to the new VM and its access to FortiGuard.
5. Upload the VM license file using the GUI or CLI.
6. Restore the configuration using the CLI or GUI.
7. Click *Reset All Dashboards* in the GUI to avoid any issues with FortiView.

Downgrading the FortiProxy

Downgrading FortiProxy 7.4.12 to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user account
- session helpers
- system access profiles

If Security Fabric is enabled, all FortiProxy units must be downgraded to the same version. For example, if Security Fabric is enabled in FortiProxy 7.4.12, all FortiProxy devices in the Security Fabric must run FortiProxy 7.4.12. Otherwise, some devices may get stale or disconnected from the root, resulting in issues with fabric logging and address synchronization.

You can downgrade FortiProxy units or VMs from 7.4.12 to 7.2.x by following the steps below:

1. In the GUI, go to *System > Fabric Management*.
2. Select the device you want to upgrade in the table and click *Upgrade*.
3. Click *Browse* in the *File Upload* tab.
4. Select the file on your PC and click *Open*.
5. Click *Confirm and Backup Config*.
6. Click *Continue*.

The configuration file is automatically saved and the system will reboot.

7. Click *Reset All Dashboards* in the GUI to avoid any issues with FortiView.

To downgrade from FortiProxy 7.4.12 to 7.0.x or 2.0.x, Fortinet recommends that you perform the downgrade procedure for each major version in between from high to low before attempting to downgrade to the target version. For example, to downgrade from 7.4.12 to 2.0.12, downgrade to 7.2.5 or later first, and then 7.0.11 or later, and then 2.0.12.

Downgrading a FortiProxy 7.0.x VM to 2.0.5 or earlier requires a different downgrade process with additional backup and configuration as FortiProxy 2.0.6 introduced a new FortiProxy VM license file that cannot be used by earlier versions of the FortiProxy VM.

To downgrade a FortiProxy 7.0.x VM to FortiProxy 2.0.5 or earlier:

1. Back up the configuration from the GUI or CLI. Make sure the VM license file is stored on the PC or FTP or TFTP server.
2. Shut down the original VM.
3. Deploy the new VM. Make sure that there is at least 2 GB of memory to allocate to the VM.
4. From the VM console, configure the interface, routing, and DNS for GUI or CLI access to the new VM and its access to FortiGuard.
5. Upload the VM license file using the GUI or CLI
6. Restore the configuration using the CLI or GUI.
7. Click *Reset All Dashboards* in the GUI to avoid any issues with FortiView.

Resolved issues

The following issues have been fixed in FortiProxy 7.4.12. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
1192922	iptables cannot match DNS server hosted on loop interface.
1188294	Transparent-connect policy with service set to *ALL* incorrectly accepts all non-HTTPS traffic without redirect.
1177408, 1177663, 1181700, 1181736, 1181744, 1181930, 1181958, 1185020, 1187659, 1192982, 1193199, 1194087	Replacement message issues.
1193761, 1194130	Inline IPS crash.
1028368, 1177336, 1194732	Improve ICAP connection pool counting to count overall connections from multiple workers.
1179919	Fix \`ftgd-wf\` configuration in "sniff-profile" to match other default profiles.
1185240	Fix source address added to unknown http header on virtual server
1190655	Webfilter service is not enabled when deny policy configured with url-category.
1188619	HTTPS over SOCKS traffic fails when \`inspect-all deep-inspection\` is configured.
1188912	Incorrect and misleading logs for files detected as malware by FortiSandbox.
1180336	Authentication is not triggered for deny and redirect policy.
1189849, 1187323, 1200523, 1200528, 1202754	GUI issues.
1166666	Upper case domain name triggered domain-fronting block on http1.1
1178104	External resource HTTP password cannot be blank when username is set.
1185498, 1189006	Count file not generated for threat feed external resource.
1168867	Inconsistent behaviour with authenticated users when the XFF is in the HTTP header and IP-based authentication is enabled in authentication rule.
1203616	Remove wcs socket console message.
1189440, 1199676, 1200447	Memory allocation requests exceeding the limit (2 GB) are rejected with no record in the system, making it difficult to diagnose and analyze related issues.
1200594	After uploading image to a HA cluster, the active unit responds passive unit's MAC

Bug ID	Description
	address to the ARP request, which leads to client wrongly connect to the passive unit when trying to access the cluster with the cluster IP.
1200971	Non-HTTP traffic fails to match address group with "and" logic.
1174407	external-resource download does not support IPv6 for FQDN.
1200523, 1200528	FQDN with wildcard is not supported for source address matching.
1199969	ICAP: WAD keeps crashing with stress traffic.
1200290	Crash for YouTube player request when the request is blocked.
1160437	DNS lookup does not work for IPv6.
1198497	ICAP debug log issues.
1198548	ICAP response ISTag header content should be quoted-string.
1199135	The username to be authenticated is not converted to lowercase when username-case-sensitivity is disabled.
1186176	File download hangs with medium severity IPS sensor.
1197206	WAD url-lookup fails to find webproxy if the first web-proxy explicit-proxy is invalid.
1018161	Improve DLP EDM optional field when optional columns are configured in CLI.
1194819	Crash when printing more than 25 forward servers
1170853	No PSU monitoring for FPX-400E.
776013	Authentication refactor to support multiple authentication request so as to prevent race condition.
776013, 1180097	Authentication refactor to support multiple authentication request so as to prevent race condition.
1194046	When a web-filter blocks a QUIC initial packet, the QUIC CONNECTION_CLOSE frame is returned with an incorrect error code.
1143184	Policy test does not working on service set on app-service-type app-id
1178204	FortiProxy lacks visibility of the performance of a shared traffic shaper.
1202928	When a video filter profile is configured to block all videos except some YouTube channels, errors may occur with a "no internet" page when loading a video from the allowed channel.
1203968	Proxy HTTPS traffic bypasses authentication when SSL profile is cert-inspection.
1200107	Active mode data channel fails to walk through FortiProxy when WAD is kicked in.
915834	Standby FortiProxy tries reaching out to FortiGuard services through HA port hitting implicit deny rule and spams the forward traffic logs.
1212053	Entry errors when upgrading FortiProxy on FPX-400E/G/F models due to wrong limits for FPX-400E/G/F models.

Bug ID	Description
1212765	HTTP-transaction logs show "deny" action while the traffic is allowed with the traffic log showing "allow" action.
1211406	"Agentforce" chat service on "help.salesforce.com" returns error messages when Appctrl is configured and inline IPS is enabled.
1184023	IP tables request fails to match policy with mix VIP and virtual server in destination address.
1207802	DNS resolve failure due to DNS query hash conflict with high traffic volume.
1197688	FortiSandbox setting in web filter prevents updates to URL list objects from taking effect.
1182981	SSH matching behaviors against isolate policy are inconsistent under different configurations. It fails to match the desired policy in some cases.
962298, 1195020	Add support for panic logging on FortiProxy G-series generation 2.
1214773	Memory leak for web UI LDAP query causing crash or process freezing.
1210950	Crash in crypto_soft_key_signature_schemes when memory malloc failed.
1188271	HTTPS is deep scanned silently when it matches a shaping policy with group configured.
1210657	ICAP client should compress multiple cookie headers when converting H2 to H1 for ICAP request.
1215809	Maximum seats change for VM04, FPX-2000G, and FPX-4000G.
1214773, 1215764	Unable to add remote LDAP user to FortiProxy while user group addition works normally.
1215438	HTTPS traffic does not trigger authentication challenge when passing through forward proxy Internet.
1216319	Web filter returns error-block when FortiGuard category resolution fails.
1192737	FPX-2000G and FPX-4000G generation 2 UID buttons are non-functional.
1216128	Failure in matching URL list with external resource URL feed.
1219846	Crash when ZTNA TCP forwarding destination is configured as FQDN.
1198336	Setting up SF-Root HA A/P cluster and the HA widget shows a negative value for uptime with state changed.
1219335	http3 does not jump to captive portal for cookie authentication.
1219314	HTTP/2 server stream statistics are not displayed in WAD stats output.
1220427	FortiProxy only removes the first header from the HTTP response when multiple HTTP-predefined headers are configured to be removed from response in the web-proxy.profile entry.

Bug ID	Description
1183724	Stream scan detects eicar as "FSA/RISK_MALICIOUS" while analytics-db is disabled.
1219985	FortiProxy fails to cache object with pnc no-cache indicated even with ignore-pnc set to enable.
1214555	Forticron process crashes when too many failed connections occur when fetching external resources.
1215282	FortiProxy transparent policy does not pass traffic when both schedule "none" and webfilter-profile exist in the policy.
1217944	Aggregate interface cannot be created in global scope.
1220551	Reports of nonsense sensor values.
1222790	The DLP signature database is not updated for HA Active-Passive clusters.
1225781	Improper bounds check leading to overflow if crashlog is longer than 128 lines.
1222972	tcp-random-srcport setting does not take effect after reboot.
1186225	Microsoft Outlook certificate errors after FortiProxy upgrade.
1226770, 1218198	WAD crash at wad_http_scan_unexpected().

Common vulnerabilities and exposures

FortiProxy 7.4.12 is no longer vulnerable to the following CVE references. Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE reference
1081024	CVE-2025-25255
1119207	CVE-2025-47890
1081024	CVE-2025-25255

Known issues

FortiProxy 7.4.12 includes the known issues listed in this section. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
1108489	Safe search does not work when configured in webfilter-profile and image-analyzer-profile in local ICAP server.
1091155	DNS resolution issues logged as "Request URL DNS resolve failure".
1096536	FortiProxy stop processing traffic after VIP modification.
996875	Traffic is failing because the replacement certificate created by FortiProxy during DPI does not contain CRL or OCSP.
1005060	Ingress traffic shaper hits a bandwidth throttle that cannot be more than 2.5 Gbps. **Workaround:** Use egress shaper for better scalability.

www.fortinet.com

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.