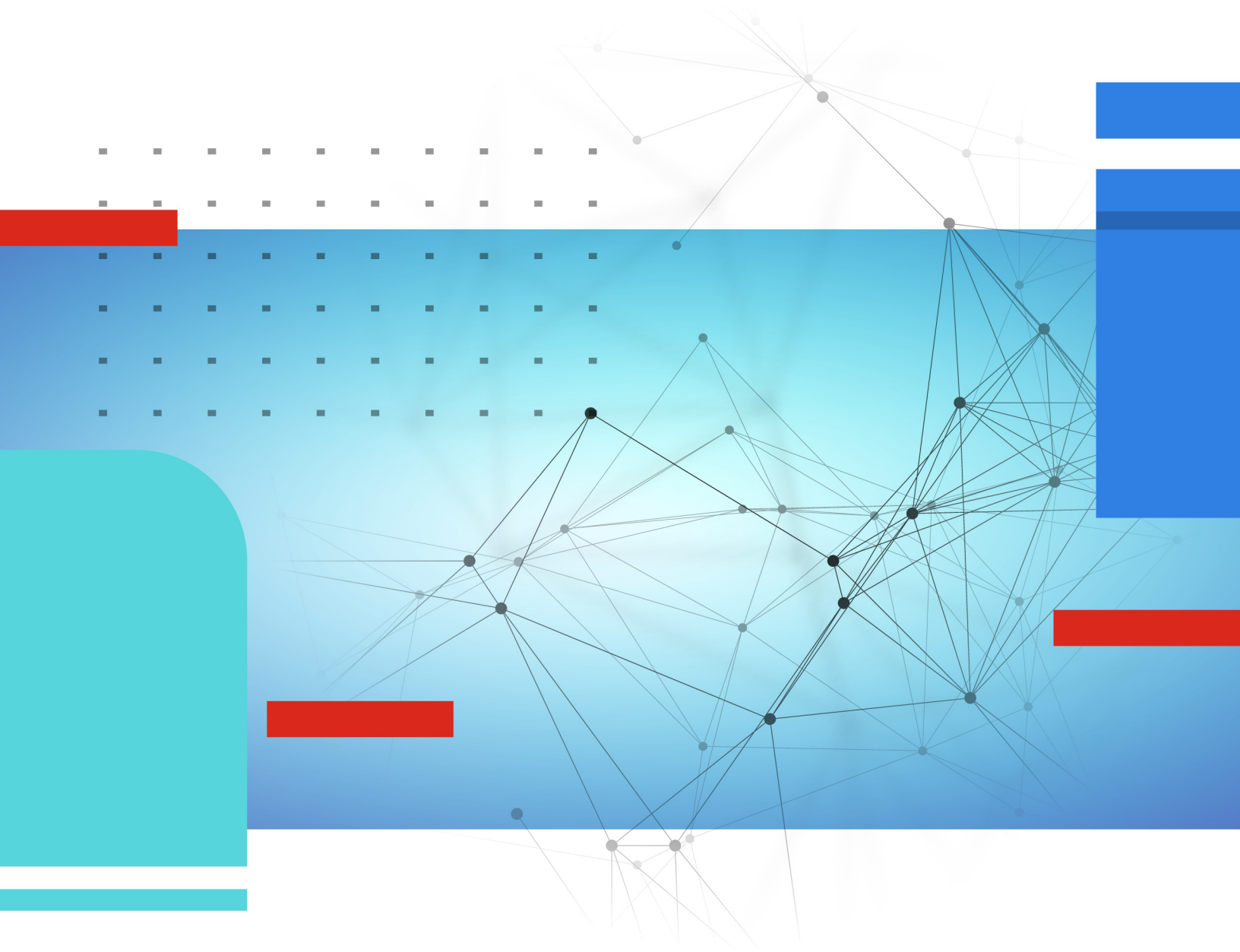
Release Notes

FortiProxy 7.6.4



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

January 06, 2026
FortiProxy 7.6.4 Release Notes
45-764-1182708-20260106

TABLE OF CONTENTS

Change log

Date	Change Description
2025-09-16	Initial release.
2025-10-15	Added CVE-2025-31366, CVE-2025-25255, and CVE-2025-31514 to Resolved issues on page 24.
2025-11-13	Updated Known issues on page 32 and Resolved issues on page 24.
2025-11-18	Added CVE-2025-54821 to Resolved issues on page 24.
2026-01-06	Added the following CVEs to Resolved issues on page 24 • CVE-2025-59718 and CVE-2025-59719 • CVE-2025-25255

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 7.6.4 supports upgrade from 7.4.x or 7.6.x only. Refer to Deployment information on page 20 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:

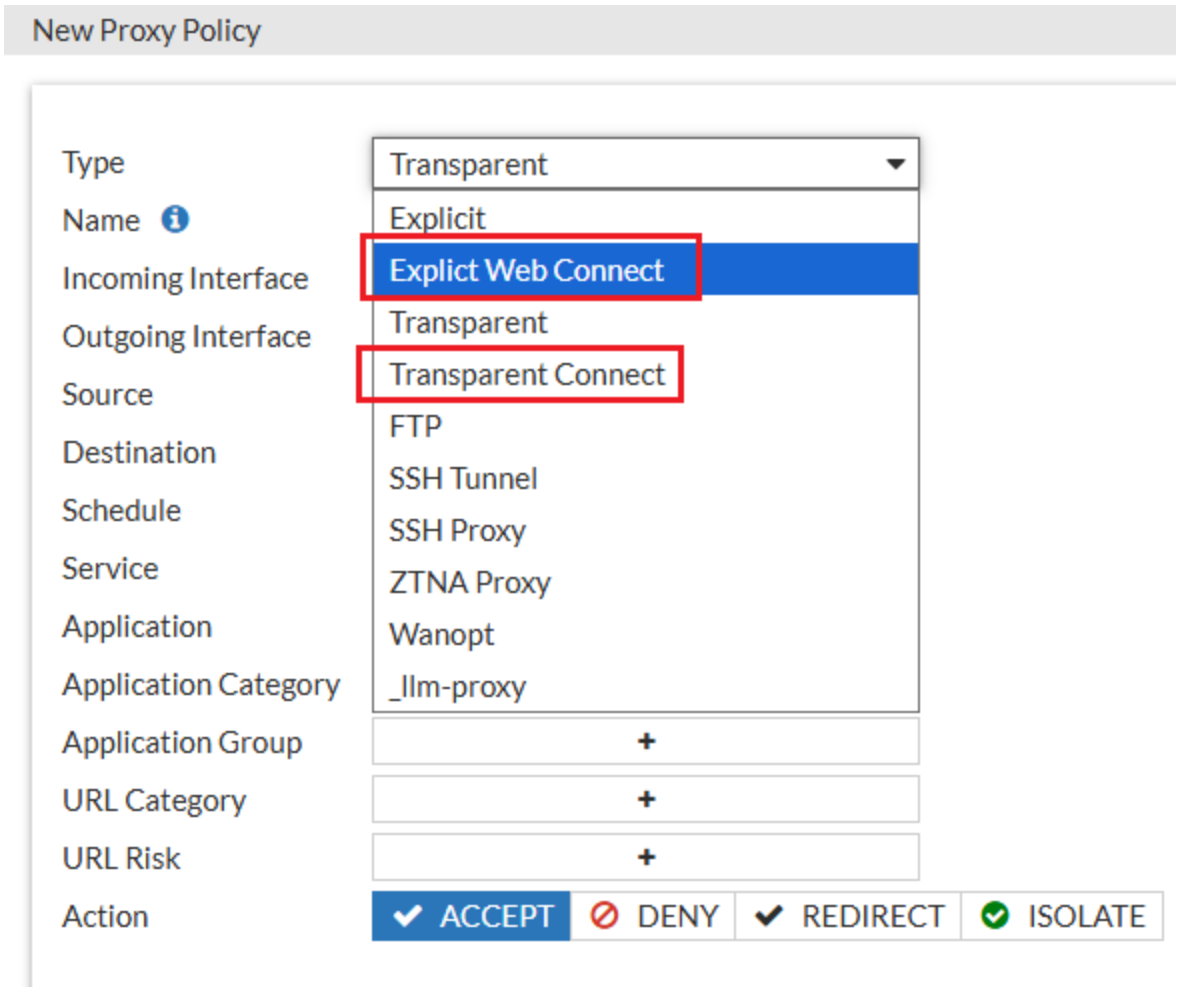
- Detect the same video ID when content comes from different CDN hosts.
- Support seek forward/backward in video.
- Detect and cache separately; advertisements automatically played before the actual videos.

What's new

The following sections describe new features, enhancements, and changes in FortiProxy 7.6.4:

New connection policy types *Explicit Web Connect* and *Transparent Connect* for HTTPS

FortiProxy 7.6.4 introduces the *Explicit Web Connect* and *Transparent Connect*policy types to handle forward server and SSL deep inspection in HTTPS CONNECT/SNI state. See Create or edit a policy.



The connection policies have higher priority than regular transparent and explicit policies. When a connection policy is configured, HTTPS requests will first match the connection policy before proceeding to the regular transparent and explicit policies. Content scan related UTM profiles are not available for connection policies.

Plain-text HTTP or decrypted HTTPS traffic will only match regular transparent and explicit policies.

The new policy types are also added to the `config firewall policy` command:

```
config firewall policy
   edit <id>
      set type <explicit-web-connect/transparent-connect>
   next
end
```

LLM security gateway on ZTNA web portal

The FortiProxy LLM gateway securely manages and controls organizational user interactions with Large Language Models (LLMs), such as ChatGPT. Users access LLM services through the FortiProxy ZTNA web portal that dynamically displays links to LLM tools authorized for each user based on their role, credentials, and security posture. Links redirect users to proxy-managed LLM interactions or directly to the LLM service. Gateway-to-LLM authentication is managed using API keys, simplifying implementation while ensuring robust security and compliance.

The following LLMs are supported:

- ChatGPT (OpenAI)
- Bard (Google AI)
- Claude (Anthropic)
- Bing AI (Microsoft)
- Llama 2 (Meta)

To configure LLM secure gateway, use the following LLM proxy-related commands:

- `config llm profile`
- `config llm proxy`
- `config llm server`

You can then reference the LLM proxy in an LLM policy and configure forward server using the `config firewall policy` command. See example below:

```
config firewall policy
   edit 15
      set type llm-proxy
      set name "llmtest"
      set uuid ffa2f9e2-29f1-51f0-c076-82c1f20772ab
      set srcintf "any"
      set dstintf "any"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ALL"
      set utm-status enable
      set logtraffic all
      set webproxy-forward-server "fg2"
      set av-profile "g-default"
      set llm-profile "llm-profile-2"
   next
end
```

Support SAML users when configuring local users

FortiProxy 7.6.4 now supports SAML users when configuring local users, expanding its ability to define individual remote users for policy enforcement. Administrators can create local entries for SAML users, enabling precise, user-specific control in both policies and VPNs. This streamlines policy management and enhances flexibility for environments using SAML authentication.

A working SAML IdP connection must already be configured.

Chain proxy authentication using client certificates

With client certificate HTTP header (RFC 9440), FortiProxy now supports chain proxy authentication using client certificates. The upstream proxy verifies the client certificate with the HTTPS proxy and forwards the certificate in the HTTP headers if the verification is successful. The downstream proxy then further verifies the certificate (no verification of the key) and maps it to a user.

The downstream proxy should be configured to only accept the HTTP header certificate from the IP of the upstream proxy for security.

To enable authentication with user certificate in Client-Cert HTTP header:

```
config authentication scheme
   edit "client-cert-scheme"
      set method cert
      set user-cert enable
      set cert-http-header enable
   next
end
```

To configure the action to take on the HTTP Client-Cert/Client-Cert-Chain headers in forwarded responses:

```
config web-proxy profile
   edit "forward-client-cert"
      set header-client-cert [pass | add | remove]
   next
end
```

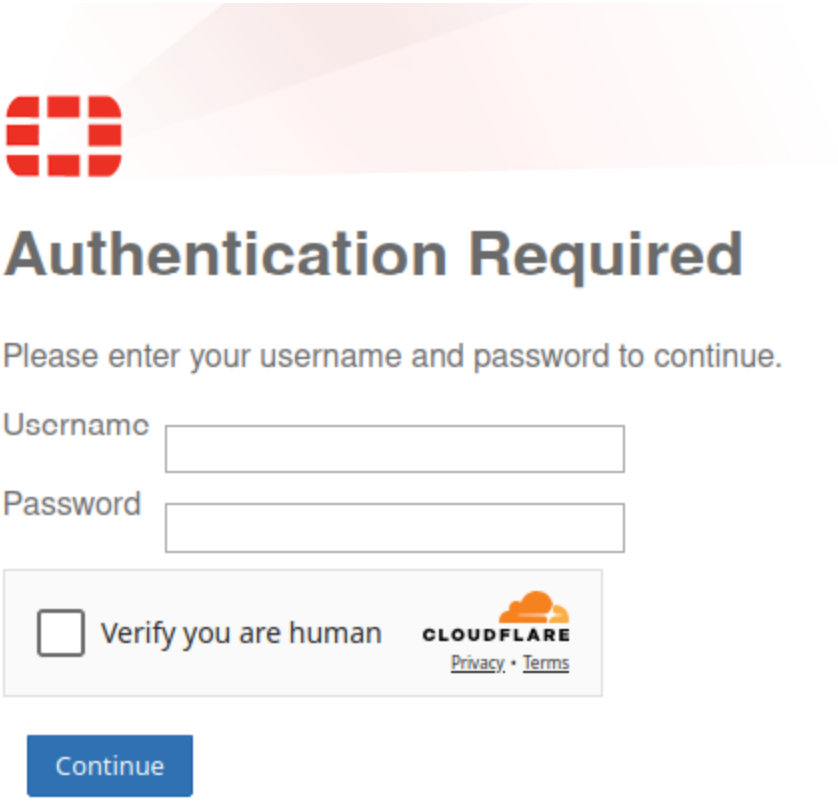
Support captcha in form-based authentication

You can now add captcha in form-based authentication to prevent robot login. The following captcha vendors are supported:

- Google reCAPTCHA

  To use Google reCAPTCHA, you must add a policy to allow `https://www.google.com/recaptcha/api.js` and `*.gstatic.com`.

- Cloudflare Turnstile



To enable and configure captcha in form-based authentication:

```
config authentication scheme
   edit "form-scheme"
      set method form
      set captcha enable
      set captcha-vendor google-recaptcha-v3
      set captcha-site-key "6LeS3DgrAAAAANTP04tXcclDFdIYRlktzq47WcxR"
      set captcha-secret-key "6LeS3DgrAAAAAMfs37y06eXe51e_cFitgm6__-3c"
      set user-database "local-user-db"
   next
end
```

Authentication behavior change for SSO_Guest_Users group

The *SSO_Guest_Users* group now only matches authenticated users and no longer allows unauthenticated users to pass through. See User Groups.

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
```

Enhancements to traffic shaping based on HTTP response

FortiProxy 7.6.4 includes the following enhancements to traffic shaping based on HTTP response:

- DSCP support
- Response policy matching based on matched shaping policy

To configure DSCP-related settings and matched shaping policies:

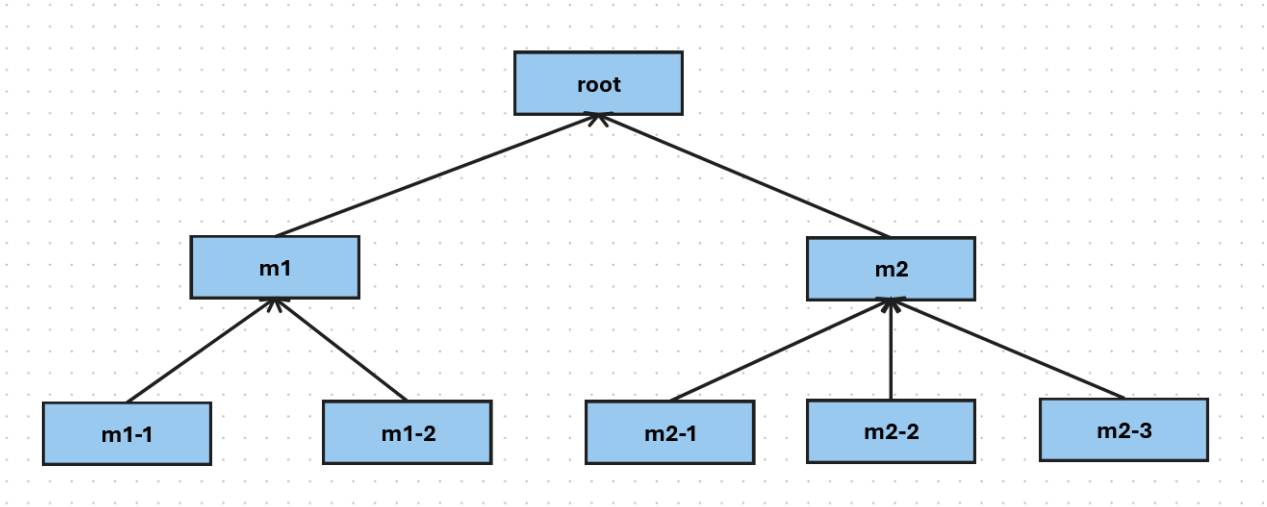
Use the following new fields in the `config firewall response-shaping-policy` command:

```
config firewall response-shaping-policy
   edit 1
      set uuid a0edf572-0378-51f0-f0f6-8f924dccfd53
      set dstaddr "resp-content-length"
      set class-id 10
      set diffserv-forward enable
      set diffservcode-forward 000000
      set diffserv-reverse enable
      set diffservcode-rev 000000
      set matched-shaping-policies 2 1 3
   set srcaddr "all"
```

License sharing enhancements

FortiProxy 7.6.4 improves license sharing stability in the following ways:

- **Additional layer of root nodes for better redundancy and recovery**
  You can now add a layer of child root nodes between the security fabric root node and downstream members. A security fabric root node can have multiple child root nodes, each with a different set of downstream nodes. In the following example, root is the security fabric root. m1 and m2 are the child root nodes with two and three downstream nodes respectively.



  - When the security fabric root is working as expected, the child root nodes act like regular downstream nodes, contributing and claiming licenses from the pool managed by the security fabric root node.
  - When the security fabric root node is down (e.g., due to a failure or network disconnection) for a specified period of time (10 minutes), the child root nodes take over license sharing responsibilities and coordinate seat allocation for downstream members to ensures the continuity of license sharing.

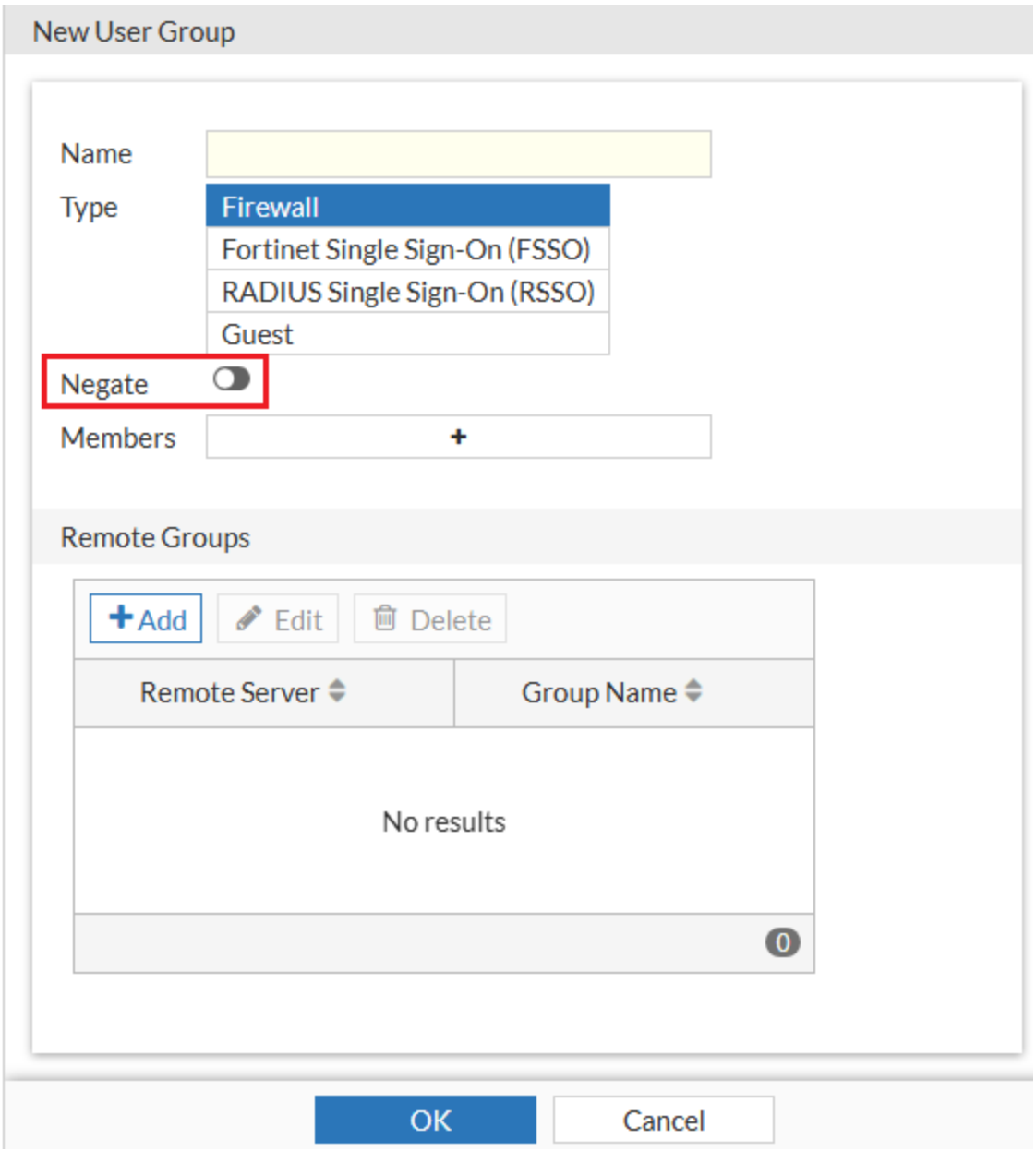
        - For the first 7 days of grace period, each child root node is entitled to the whole license pool that the security fabric root node used to manage. In the example above, if the purchased seats for each node is 100, both m1 and m2 will have a license pool of 800 during the first 7 days after root becomes available.
        - After 7 days, the license pool of each child root node is limited to licenses from itself and its downstream members. In the example above, if the purchased seats for each node is 100, m1 and m2 will have a license pool of 300 and 400 respectively after 7 days of root being unavailable.
    - When the security fabric root is restored, it re-claims license sharing responsibilities from the child root nodes and restores license sharing to the original state where all child root nodes and downstream members contribute and claim licenses from the security fabric root node.
- **License sharing grace period for offline operation extended from 8 hours to 7 days**

  In case of disconnection from the root, a security fabric member node can now retain its eligible seats (last allocated or locally purchased seats, whichever is greater) for 7 days before falling back to locally purchased seats . The seats are released back into the pool when the connection to the root recovers.

See the License Sharing Deployment Guide for more details.

Negate user group as source in policy match

When creating or editing a user group, you can now configure negate user group as source in policy match using the new `negate` option:



Alternatively use the new `negate` option in the `config user group` command:

```
config user group
   edit <name>
      set negate <enable/disable>
end
```

Authentication based on custom HTTP header

In FortiProxy 7.6.4, you can configure authentication based on custom HTTP headers in the authentication scheme if the method is x-auth-user using the new `auth-user-header` option in the `config authentication scheme` command:

```
config authentication scheme
   edit "1"
      set method x-auth-user
      set auth-user-header "custom-header1"
      set user-database "ldap1"
   next
end
```

If `auth-user-header` is not specified, the default value `x-authenticated-user` is used as the header name instead.

IKEv2 support for IPsec VPN

FortiProxy 7.6.4 adds IKEv2 support for IPsec VPN.

Increase proxy-address configuration limit

FortiProxy 7.6.4 includes the following changes to the proxy-address configuration limit for VM04 and VM08:

Proxy address object	New configuration limit for 7.6.4
Proxy Address Object	80K
Proxy Address Group	4096
Proxy Address Group Member	30K

CLI changes

FortiProxy 7.6.4 includes the following CLI changes:

- `config router static`—Use the new `set preferred-source` subcommand to configure the preferred source IP for the route.

- `config authentication rule`—Use the new `set session-logout` subcommand to enable/disable logging out users from the current session.
- `config web-proxy global`—Use the new `set policy-partial-match` subcommand to enable/disable policy partial match. The default is enable.
- `diagnose wad user explicit-proxy-users`—Use this new command to show the number of active users that have been processed by WAD.
- `diag wad user list`—This command now also displays dynamic bookmark related information in a the new *Dynamic Attributes* section.
- `diagnose sys filesystem tree`—Use this new command to list the top files/folders tree.
- `diagnose sys filesystem hash`—Use this new command to generate hash for files within the filesystem. See Computing file hashes in the Administration Guide for more details.
- `diagnose system filesystem last-modified-files`—Use this new command to list the last modified files.
- `diagnose sys session list-verbose`—Use this new command to list sessions in verbose detail.
- `diagnose sys mpstat`—Use this new command to diagnose mpstat.
- `diag wad user filter`—Use this new command to set a filter to query the user by the leading string (case insensitive). You can the use the `diag test` commands to check the data in ldap-cache and worker.
- `config firewall access-proxy`—The default value of `svr-pool-multiplex` is changed from enable to disable.

Product integration and support

The following table lists product integration and support information for FortiProxy 7.6.4 build 1593:

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

Type	Product and version
	• Windows Server 2008 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 Core (requires Microsoft SHA2 support package) • Novell eDirectory 8.8
Web browsers	• Microsoft Edge • Mozilla Firefox version 87 • Google Chrome version 89  Other web browsers may work correctly, but Fortinet does not support them.
Virtualization environments	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.
Hyper-V	• Hyper-V Server 2008 R2, 2012, 2012R2, 2016, 2019, and 2022
Linux KVM	• RHEL 7.1/Ubuntu 12.04 and later • CentOS 6.4 (qemu 0.12.1) and later
Xen hypervisor	• OpenXen 4.13 hypervisor and later • Citrix Hypervisor 7 and later
VMware	• ESXi versions 6.5, 6.7, 7.0, and 8.0
Openstack	• Ussuri
Nutanix	• AHV
Cloud platforms	• AWS (Amazon Web Services) • Microsoft Azure • GCP (Google Cloud Platform) • OCI (Oracle Cloud Infrastructure) • Alibaba Cloud

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 18 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 18 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 18 for a list of supported VM platforms.

Upgrading the FortiProxy

FortiProxy 7.6.4 supports upgrade from 7.4.x or 7.6.x.

If Security Fabric is enabled, all FortiProxy units must be upgraded to the same version. For example, if Security Fabric is enabled in FortiProxy 7.6.4, all FortiProxy devices in the Security Fabric must run FortiProxy 7.6.4. 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 7.6.4:

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 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 7.6.4. For example, to upgrade from 7.0.17 to 7.6.4, upgrade to 7.2.5 or later first (reboot before upgrading to 7.2.x), and then 7.4.x, and then 7.6.4.

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 7.6.4 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 7.6.4, all FortiProxy devices in the Security Fabric must run FortiProxy 7.6.4. 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 7.6.4 to 7.4.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 7.6.4 to 7.2.x or 7.0.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 7.6.4 to 7.0.17, downgrade to 7.4.x first, and then 7.2.5 or later, and then 7.0.

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 7.6.4. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
1130867	LDAP groups are not updated regularly in the WAD cache.
1142105	Inline-CASB shared memory has memory corruption when loading the signature with header match rules.
1140654	SAML authentication failure after configuration change.
1146216	Intermittent users traffic disconnection issues on FortiProxy VM after upgrading and applying a new user license.
1093881	Incorrect service name in inline IPS botnet log.
1130795	Wrong certificate for client certificate exchange in action deny explicit policy.
1103523, 1143534	Error when deploying fpx_arm64_aws due to short of flash space.
1139840	ZTNA web-portal authentication fails after configuration update.
1133901	When "https-replacement-message" is disabled and traffic is blocked, FortiProxy aborts HTTP CONNECT without returning any error code to the HTTP CONNECT request.
1040204, 1040494	Under FTP Active mode, AntiVirus NAC-quarantine will ban server side IP.
1149344	Client certificate is not offered without authenticated user when ssl-client-certificate is set to static.
1030015	BUFFER_SIZE found in UTM_Proxy.
1145481	Adding some regex entries to URL filter causes other urlfIter tables to stop working properly.
1144621	Unicast HA with transparent VDOM fails to sync.
1130882	Missing field details in http-transaction logs for deep-inspect https CONNECT traffic.
1147546	Kernel panic when clearing sessions.
1130928	ZTNA webportal's response contains body with HEAD method.
1149807	Policy lookup tool does not match source interface.
1149760	Inline-IPS does not match IPS sensor location.
1149110	With a wrong URL(but with huge body) in OIDC discovery field, the CPU usage will reach 100% when HTTP verbose log is enabled in console.

Bug ID	Description
1143212	The SSH fingerprint is changed when traffic passes through transparent mode FortiProxy.
1140953	HTTP2 large file download may get stuck and fail.
1144389	Device hangs with no GUI/SSH/serial console access. Traffic processing halts completely.
1143184	Policy test does not working on service set on app-service-type app-id
1080366	The FURL license seat does not control the inline CASB feature.
1154960	Failure in matching VIP in policy when multiple addresses are in the dstaddr list for transparent proxy.
1155578	When multiple VIPs are specified in dstaddr, crash may occur if the first VIP does not match and a subsequent VIP is checked for a match.
1102925	WAD ssl_cert leak in ZTNA.
1155170	Memory usage increases unexpectedly during high load when processing WAD-related tasks.
859182	WAD crashed at fts_crypto_kxp_pub_key_verify_done.
1155295	Inline-CASB profile is not visible in the Profile Group in both CLI and GUI.
1144818	Download failure occurs when accessing https://7-zip.de for domain objects.githubusercontent.com.
1149600	In explicit proxy policy, if the outgoing interface type is pppoe, all traffic will be blocked when fast matching is enable.
1152772	In non-transparent mode, enabling DNS protection for HTTP/HTTPS traffic causes the traffic to hang.
1146601	Inline IPS raw scan can leak memory.
1149337	IPsec tunnel does not forward traffic for certain interface port configurations.
1121980	Inline IPS blocks some LinkedIn pages that should be allowed.
1152286	WCCP crash after enabling WCCP under interface in FortiProxy VM.
1055898	Downstream server cannot get the payload from forwarded HTTP/2 messages because Content-Length or Transfer-Encoding information is not included in the forwarded messages, which can also cause HTTP smuggling attack.
1158174	Cannot use internet-service in single IPv4 and IPv6 policy.
1159963	Expired server certificates are issued during deep inspection.
1116834	Authentication pop-up does not appear when accessing HTTPS websites through FortiProxy with Explicit Proxy when authentication rules, webproxy-forward-server, and certificate-inspection are configured in policy.

Bug ID	Description
1095498	After override enabled under endpoint-control.settings, traffic still matches the policies which use EMS tags under global VDOM.
1102694	"utmref" and "utmaction" fields are missing in forward traffic log and http-transaction traffic log for long-tcp sessions.
1156135	Crashes when configuring policy with mix VIP and L7 addresses on GUI.
1154043	Fix incorrect locking and RCU usage in kernel.
1001480	SSH policy display issues in both GUI and CLI.
1164161	The first LDAP cache query always fails, even when both user node and group info are correct.
1141275	The FortiProxy is shut down unexpectedly when Active Directory is used.
1160001	Unexpected power off on FPX-400G.
1164508	Issue with machine account authentication in NTLM and Kerberos.
1160444	Global config wanopt content-delivery-network-rule is deleted after VDOM config restore.
1164865	detect-https-in-http-request no longer works.
1048549	To allow SN prefix FPXVMR and FPXVMO for FortiFlex
1162685	Traffic blocked due to per-ip shaper when no shaping policies are configured.
1155022	Refine traffic log when forward server is down with server-down-option=block.
1166774	Policy "max-session-per-user" config update does not take effect.
1098400	Inline IPS custom app dependency issues.
1148863	Interface speed statistics are not shown if the interface is moved to a non-root VDOM.
1096263	Intermittent 504 errors occur when an IPv6 HTTP request followed by an IPv4 request in the same pipeline goes through explicit proxy with outgoing-ip.
1169854	Tenant control is unavailable FortiProxy 7.4.9.
1166902	Under the transparent policy configured with SAML authentication, user traffic fails to redirect to the authentication window.
1168193	SOCKS policy match user/group info is not assigned to session context.
1167993	Improve WAD statistics through shared memory.
1168995	Login again from the same IP with a previous unfinished TFA form login causes crash.
1170853	No PSU monitoring for FPX-400E.

Bug ID	Description
1139201	Internal resources are inaccessible via IP or FQDN when using agentless ZTNA Access proxy-portal with apptype web on FortiProxy.
1174803	Crash during krb fallback traffic.
1174060	WAD crash on dia test app wad 110 for shm-stats.
1155100	Policy matching on WAD with VIP fails in transparent mode.
1161799	Incorrect MTU used for IPsec tunnel.
1167782	Unable to download archive with password.
1104165	GUI and CLI output for firewall and proxy authentication lists mismatch.
1168911	Creating a new address object from GUI on the secondary device fails when it's done under policy edit.
1156893	WAD keeps crashing with signal 6 after creating a server-load-balance with no real server.
1165461	Failure in generating CSR with safenet HSM.
1172637	"Bad Request" error after clicking LOGIN on captive portal.
1175018	FortiProxy reboots when removing groups from a policy.
1170884	FortiProxy repeatedly reboots.
1046939	CASB profile should only be configurable when utm-status is enabled.
1173302	Downstream nodes can not communicate with each other when root is unreachable in security fabric.
1128026	Video filter fails to effectively block YouTube videos.
1161593	Cannot configure ssl-ssh-profile for explicit-web policy with action redirect.
1177015	When deep-inspection is enabled in policy and https-replacement-message is disabled, web filter log is not generated and traffic log's utmaction shows "allow" for traffic blocked by web filter.
1174812	Password-protected files sent from FortiProxy cannot be opened or scanned by FortiSandbox.
1177714	Traffic log for proxy traffic does not include explicit-web-proxy name.
1178363	Occasional SSL error and WAD crash.
1177573	Issues related to error handling with wad_str objects and buffer operations.
1160437	DNS lookup does not work for IPv6.
1098827, 1133648, 1156883, 1163061, 1173794, 1174460, 1175314, 1178985,	GUI issues.

Bug ID	Description
1183154, 1183758, 1183978, 1189849, 1200399, 1200651	
1174463, 1180682, 1182789, 1193761, 1194130	Inline IPS crash.
1172516	Request fails to match VIP on WAD.
1168867	Inconsistent behaviour with authenticated users when the XFF is in the HTTP header and IP-based authentication is enabled in authentication rule.
1179521	FortiProxy FortiView GUI does not work on HA secondary.
1179713	Some fields are missing when policy type is set to transparent-connect.
1180738	Crash when executing `get hardware nic <interface name>`.
1178564	Unable to access any websites intermittently in explicit proxy.
1177934	WAD workers are at 99% CPU for more than 10 minutes after a firewall policy is enabled or disabled, impacting traffic.
1175068	(SSL) HTTPS handshake fails when https-replacement-message is disable and authentication is required in policy.
1159424	Implicit deny does not include or block IPv6.
1178166	The web browser displays the certificate selection dialog when you access the FortiProxy GUI.
1168782	URL Catergory Deny not indicated in traffic logs.
1133068	Inconsistent blocking behaviors of banned IPs for different policy types and protocols.
1173584	Bypass for oversize files does not work.
1178203	FortiProxy becomes unresponsive (all interfaces down, no serial access) during traffic peak.
1185301	OIDC authentication timeout with session-based access in ZTNA.
1160110	Expired user seats are counted as valid in license sharing.
1026921	Application control cannot block QUIC when proxy-inline-ips is enabled in the policy.
1180491, 1188287	SOCKS request which matches any explicit-web-connect policy skips matching of explicit-web policies.
1187632	Duplicate log_id in WAD traffic logs when the forward server is down.
1185663	LDAP group queries do not work.
1189360	Inaccurate seat calculation for FNBI and FCAS license types during license sharing.

Bug ID	Description
1189482	License sharing crash issue.
1050336	When MFA method is used for administrator users and OTP length is set to 8 on FortiToken, FortiProxy will not log the user in with an error "Authentication failure" even if the OTP is correct.
1193771	When using cookie-based authentication, auth_method shows "NULL" instead of "Cookie".
1188912	Incorrect and misleading logs for files detected as malware by FortiSandbox.
1190655	Webfilter service is not enabled when deny policy configured with url-category.
1166666	Upper case domain name triggered domain-fronting block on http1.1
1178104	External resource HTTP password cannot be blank when username is set.
1187553	Increase external resource password length to 512 from 128.
1185498, 1189006	Count file not generated for threat feed external resource.
1186795	Incorrect URL is displayed after form authentication.
1180336	Authentication is not triggered for deny and redirect policy.
1138074	Log display issue when inline IPS is enabled.
1191149	CSF member does not update upstream path when HA AP switches from active to standby.
1028368, 1177336	Improve ICAP connection pool counting to count overall connections from multiple workers.
1138959	For parameterized signatures, inline IPS does not include parameter value in the msg field of utm app log.
1177408, 1177663, 1181700, 1181736, 1181744, 1181930, 1181958, 1185020, 1187659, 1192982, 1193199, 1194087	Replacement message issues.
1177720	Cannot connect to FortiGate Cloud.
1194732	ICAP server get policy deny for all ICAP req mode request
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
1188619	HTTPS over SOCKS traffic fails when `inspect-all deep-inspection` is configured.
1192922	iptables cannot match DNS server hosted on loop interface.
1170843	The ZTNA web-portal page show "{EXPAND}" instead of expected content.

Bug ID	Description
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.
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.
1198497	ICAP debug log issues.
1198548	ICAP response ISTag header content should be quoted-string.
1193984, 1194819, 1197596	Crash when printing more than 25 forward servers
1182981	SSH matching behaviors against isolate policy are inconsistent under different configurations. It fails to match the desired policy in some cases.
1201324	Missing default "web-proxy explicit-proxy" entry "web-proxy".
1200290	Crash for YouTube player request when the request is blocked.
1200844	Unable to change "Invalid SSL certificates" when "Inspect All" is enable on "SSL/SSH Inspection" page.
776013	Authentication refactor to support multiple authentication request so as to prevent race condition.
1184283	ZTNA web portal with dynamic ldap attribute bookmark does not work when the authentication method is form-based.
1200594	After uploading image to a HA cluster, the active unit responds passive unit's MAC 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.

Common vulnerabilities and exposures

FortiProxy 7.6.4 is no longer vulnerable to the following CVE references. Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE reference
1187887, 1192040	CVE-2025-59718 and CVE-2025-59719
1081024	CVE-2025-25255
1179551	CVE-2025-54821
1151885	CVE-2025-31366
1081024	CVE-2025-25255

Bug ID	CVE reference
1196322	CVE-2025-31514

Known issues

FortiProxy 7.6.4 includes the known issues listed in this section. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
1072072	Device identification detection is not yet supported in FortiProxy 7.6.
1197589	Explicit web HTTPS traffic fails to match policy if `set inspect-all deep-inspection` is configured under `ssl-ssh profile`.
1210368	FortiProxy in config-sync-only HA mode with the default certificate cannot establish stable connection to FortiManager. **Workaround**: 1. Add central management configuration in backup mode on both FortiProxy devices in the HA cluster. 2. Select both FortiProxy devices and authorize (instead of authorizing the devices one by one),

FortiNBI

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

Bug ID	Description
N/A	WSL2 X11 output corruption. This is a known bug on Microsoft's WSLg graphics. **Workaround:** • Try running "wsl –shutdown" and then restarting the isolator. • Use the FortiNBI WSLg graphics, which has lower performance than the Microsoft's WSLg graphics.
975570	Certificate warning when starting up the isolator. **Workaround**: Ignore the certificate warning.
881957	Error in Google Chrome or Microsoft Edge login page when FortiNBI is on. **Workaround**: Use Firefox.

www.fortinet.com