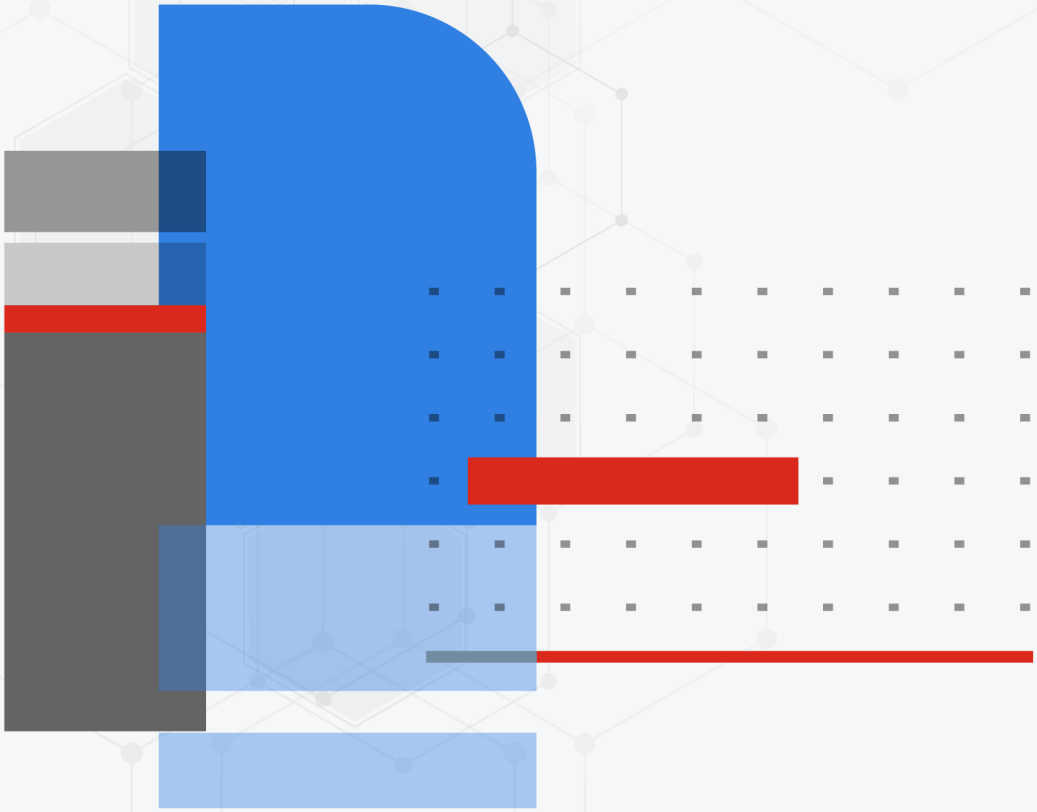
Release Notes

FortiProxy 7.4.11



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 7.4.11 Release Notes
45-7411-1187494-20260106

TABLE OF CONTENTS

Change log

Date	Change Description
2025-08-25	Initial release.
2025-08-26	Added ticket 1188294 to Known issues on page 22.
2026-01-06	Added CVE-2025-59718 and CVE-2025-59719 to Resolved issues on page 19.

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 7.4.11 supports upgrade from 7.4.x only. Refer to Deployment information on page 15 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:

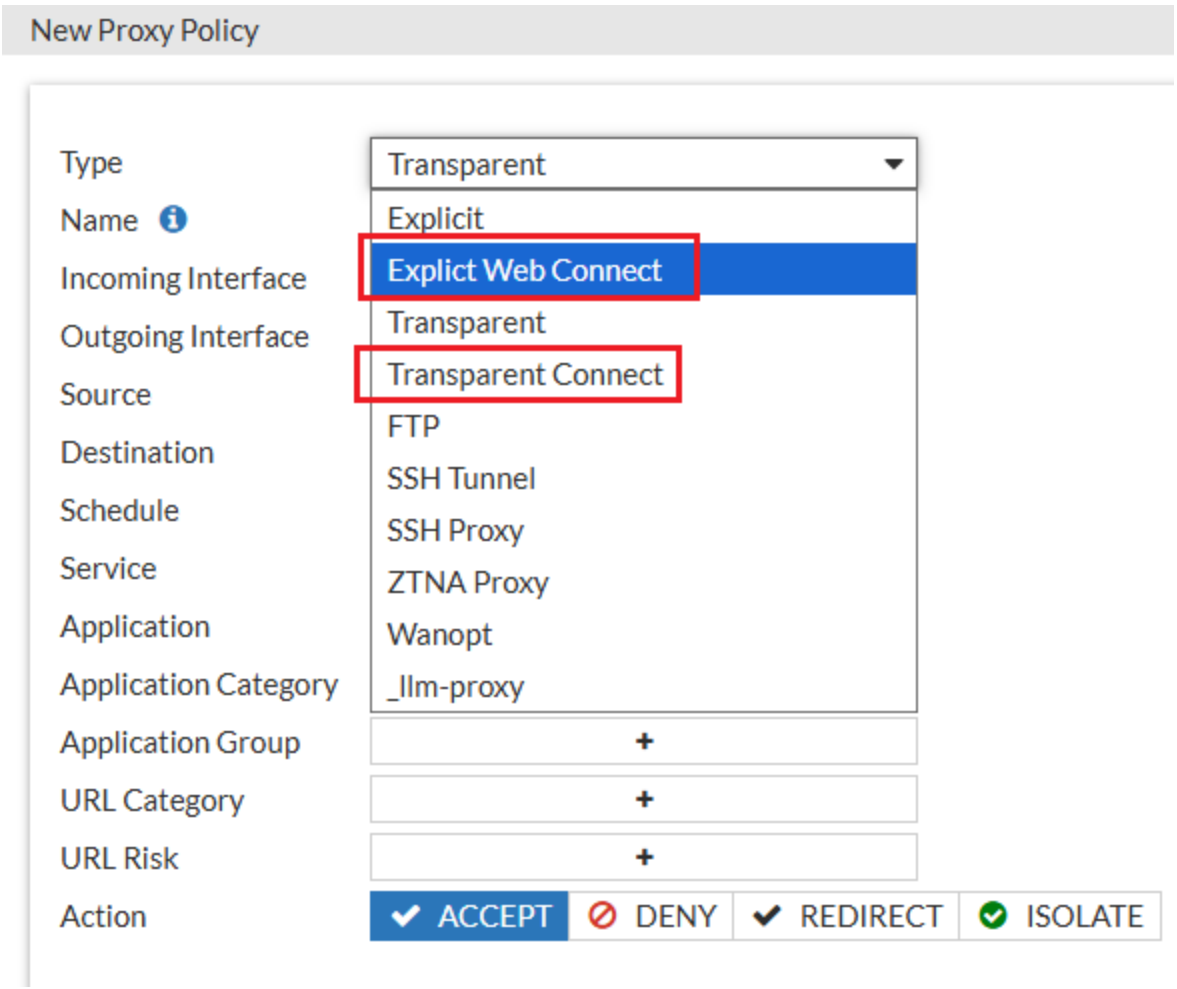
- Detect the same video ID when content comes from different CDN hosts.
- Support seek forward/backward in video.
- Detect and cache separately; advertisements automatically played before the actual videos.

What's new

The following sections describe new features, enhancements, and changes in FortiProxy 7.4.11:

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

FortiProxy7.4.11 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
```

Enhancements to traffic shaping based on HTTP response

FortiProxy 7.4.11 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:

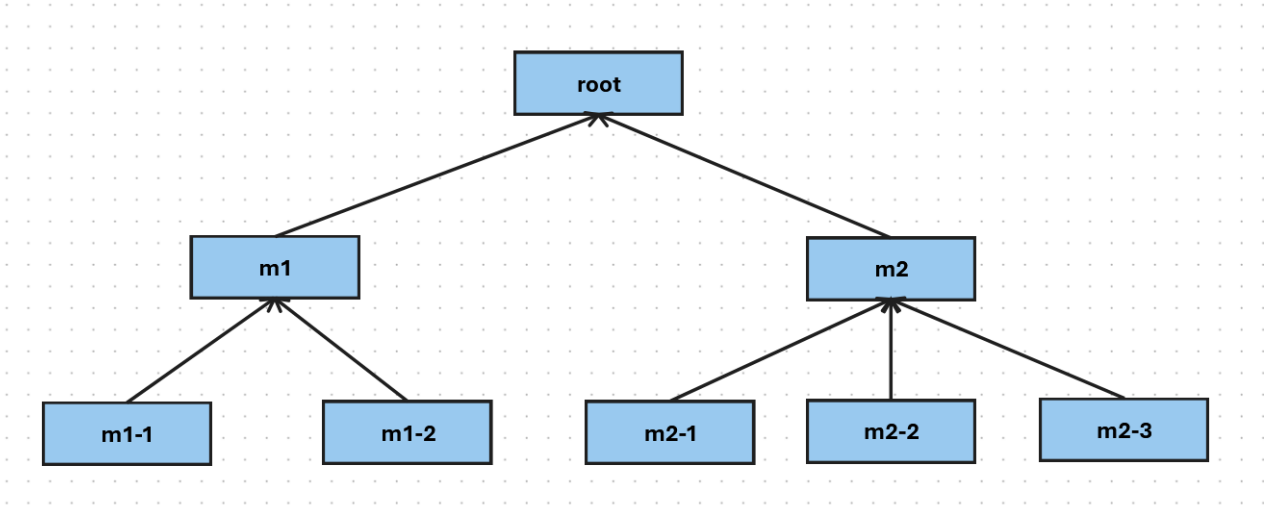
Use the following new fields in the `config firewall response-shaping-policy` command:

```
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 7.4.11 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.

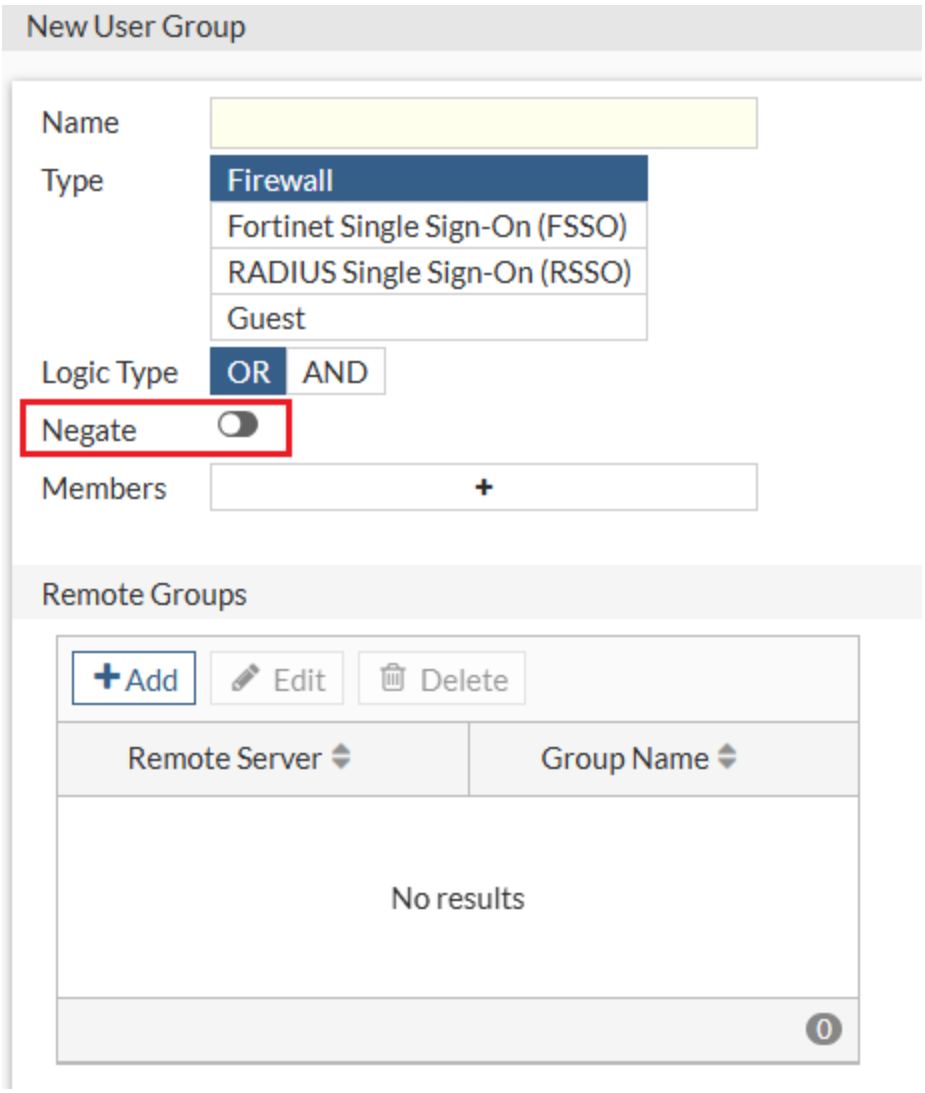
- **License sharing grace period for offline operation extended from 8 hours to 7 days**

  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 7.4.11, 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.

CLI changes

FortiProxy 7.4.11 includes the following CLI changes:

- `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 7.4.11 build 700:

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 13 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 13 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 13 for a list of supported VM platforms.

Upgrading the FortiProxy

FortiProxy 7.4.11 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 7.4.11, all FortiProxy devices in the Security Fabric must run FortiProxy 7.4.11. 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 7.4.11:

If you are using a RADIUS server that does not support the message-authenticator attribute, upgrading to 7.4.11 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 7.4.11. For example, to upgrade from 2.0.12 to 7.4.11, 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 7.4.11.

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 7.4.11 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 7.4.11, all FortiProxy devices in the Security Fabric must run FortiProxy 7.4.11. 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 7.4.11 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 7.4.11 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 7.4.11 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 7.4.11. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
1102694	"utmref" and "utmaction" fields are missing in forward traffic log and http-transaction traffic log for long-tcp sessions.
859182	WAD crashed at fts_crypto_kxp_pub_key_verify_done.
1143534	Error when deploying fpx_arm64_aws due to short of flash space.
1155295	Inline-CASB profile is not visible in the Profile Group in both CLI and GUI.
1001480	SSH policy display issues in both GUI and CLI.
1149600	In explicit proxy policy, if the outgoing interface type is pppoe, all traffic will be blocked when fast matching is enable.
1162685	Traffic blocked due to per-ip shaper when no shaping policies are configured.
1149915	PSK auth method does not work when setting up IPsec IKEv2.
1155022	Refine traffic log when forward server is down with server-down-option=block.
1156135	Crashes when configuring policy with mix VIP and L7 addresses on GUI.
1022507, 1039490	FortiProxy SSO users have no SSL enforcement.
1098400	Inline IPS custom app dependency issues.
1164508	Issue with machine account authentication in NTLM and Kerberos.
1148863	Interface speed statistics are not shown if the interface is moved to a non-root VDOM.
1071928	Duplicated utm log when log-http-transaction is enabled.
1167993	Improve WAD statistics through shared memory.
1169169	Cookie based form-authentication does not work with HTTPS.
1166774	Policy "max-session-per-user" config update does not take effect.
1169541	GUI should only be enabled when FortiCare is licensed.
1165461	Failure in generating CSR with safenet HSM.
1166902	Under the transparent policy configured with SAML authentication, user traffic fails to redirect to the authentication window.
1174803	Crash during krb fallback traffic.

Bug ID	Description
1174060	WAD crash on dia test app wad 110 for shm-stats.
1155100	Policy matching on WAD with VIP fails in transparent mode.
1048549	To allow SN prefix FPXVMR and FPXVMO for FortiFlex
1161593	Cannot configure ssl-ssh-profile for explicit-web policy with action redirect.
1128026	Video filter fails to effectively block YouTube videos.
1172637	"Bad Request" error after clicking LOGIN on captive portal.
1046939	CASB profile should only be configurable when utm-status is enabled.
1159424	Implicit deny does not include or block IPv6.
1177573	Issues related to error handling with wad_str objects and buffer operations.
1178166	The web browser displays the certificate selection dialog when you access the FortiProxy GUI.
1177714	Traffic log for proxy traffic does not include explicit-web-proxy name.
1178363	Occasional SSL error and WAD crash.
1168782	URL Catergory Deny not indicated in traffic logs.
1179713	Some fields are missing when policy type is set to transparent-connect.
1174812	Password-protected files sent from FortiProxy cannot be opened or scanned by FortiSandbox.
1178564	Unable to access any websites intermittently in explicit proxy.
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.
1173584	Bypass for oversize files does not work.
1156883, 1178985, 1183758, 1183978	GUI issues.
1174463, 1180682, 1182789	Inline IPS crash.
1172516	Request fails to match VIP on WAD.
1133068	Inconsistent blocking behaviors of banned IPs for different policy types and protocols.
1160110	Expired user seats are counted as valid in license sharing.
1160437	DNS lookup does not work for IPv6.
1178203	When inline IPS is enabled, WAD could crash in some HTTP traffic that use absolute or full URL in the requests.

Bug ID	Description
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.
1137133	Delay in loading a resolved address for Dynamic Address (FSSO) in the GUI.
1187305	Memory leak in inline IPS.
1189360	Inaccurate seat calculation for FNBI and FCAS license types during license sharing.
1138074	Log display issue when inline IPS is enabled.
1186795	Incorrect URL is displayed after form authentication.
1193771	When using cookie-based authentication, auth_method shows "NULL" instead of "Cookie".
1177720	Connection issues with FortiGate Cloud and FortiSandbox Cloud.
1193984	Crash when loading forward server monitor.
1189310	RadSec user authentication via local rule in the captive portal causes a crash.

Common vulnerabilities and exposures

FortiProxy 7.4.11 is no longer vulnerable to the following CVE reference. Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE reference
1187887, 1192040	CVE-2025-59718 and CVE-2025-59719

Known issues

FortiProxy 7.4.11 includes the known issues listed in this section. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
1188294	Transparent-connect policy with service set to *ALL* incorrectly accepts all non-HTTPS traffic without redirect. **Workaround:** Set service to *HTTPS* in the policy.
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