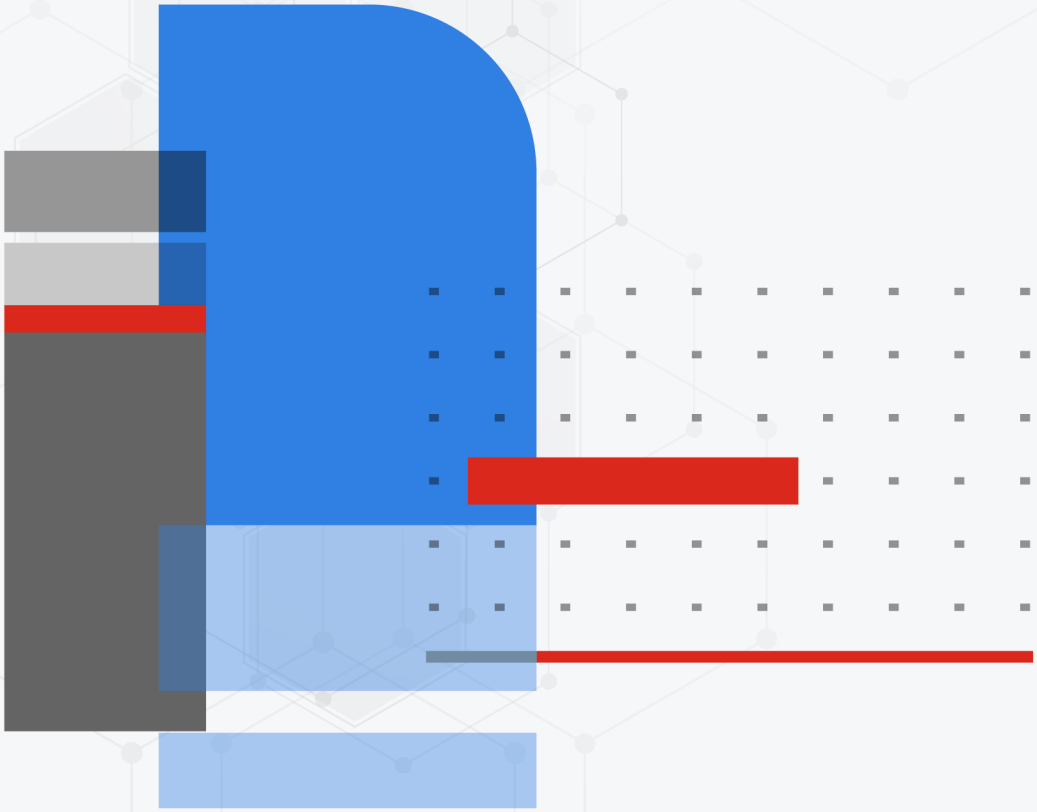
Release Notes

FortiProxy 7.4.8



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

October 15, 2025
FortiProxy 7.4.8 Release Notes
45-748-1115345-20251015

TABLE OF CONTENTS

Change log **4**
Introduction **5**
Security modules 5
Caching and WAN optimization 6
What's new **7**
Support switching to an alternate FortiSandbox if the main FortiSandbox is unavailable 7
Change to HTTP header content maximum length 8
UEFI support for GCP 8
CLI changes 8
Product integration and support **9**
Deployment information **11**
Downloading the firmware file 11
Deploying a new FortiProxy appliance 11
Deploying a new FortiProxy VM 11
Upgrading the FortiProxy 12
Downgrading the FortiProxy 13
Resolved issues **15**
Common vulnerabilities and exposures 16
Known issues **17**

Change log

Date	Change Description
2025-01-15	Initial release.
2025-06-10	Added CVE-2025-22254 to Resolved issues on page 15.
2025-10-15	Added CVE-2023-46718 and CVE-2025-22258 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 7.4.8 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.

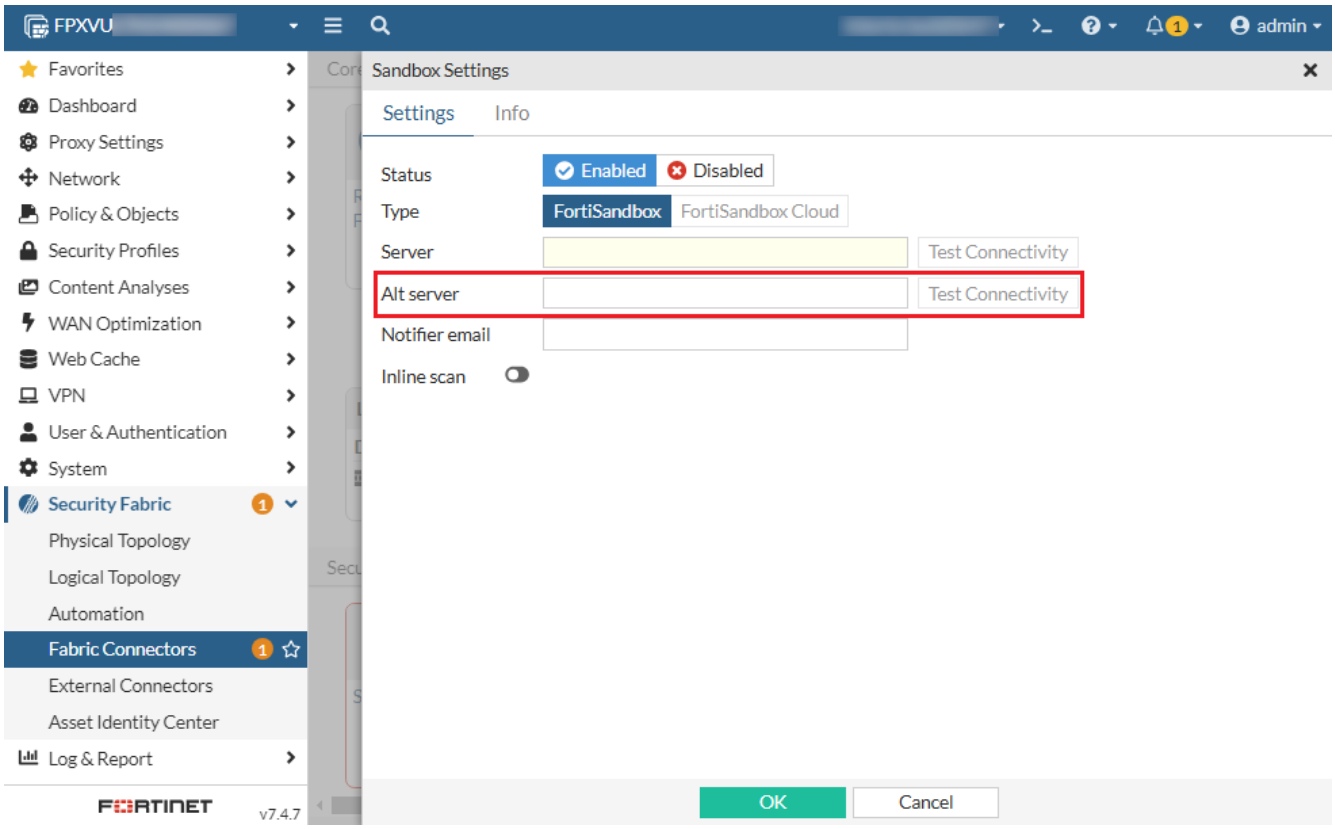
What's new

The following sections describe new features, enhancements, and changes in FortiProxy 7.4.8:

- Support switching to an alternate FortiSandbox if the main FortiSandbox is unavailable on page 7
- Change to HTTP header content maximum length on page 8
- UEFI support for GCP on page 8
- CLI changes on page 8

Support switching to an alternate FortiSandbox if the main FortiSandbox is unavailable

FolrtiProxy 7.4.8adds support for switching to an alternate FortiSandbox when the main FortiSandbox is unavailable. Once the connectivity is restored, it will automatically fall back to the primary FortiSandbox. You can configure an alternate FortiSandbox using the new *Alt server* option when configuring a FortiSandbox connector:



Alternatively, use the new `alt-server` option under `config system fortisandbox`. Use the new `health-check-interval` option to configure the interval of health check for the failover.

Log sample:

```
1: date=2025-01-09 time=07:15:56 eventtime=1736363756320902685 logid="0100022948"
type="event" subtype="system" level="warning" vd="root" logdesc="FSA failover status warning"
      name="sandbox" interface="undefined" probeproto="ping" msg="FortiSandbox changed
state from alive to dead, Peer:Primary status Primary:DOWN Alternate:DOWN protocol: ping."
```

Change to HTTP header content maximum length

In FortiProxy 7.4.8, the HTTP header content maximum length is increased from 1023 to 4000.

UEFI support for GCP

FortiProxy 7.4.8 adds UEFI support for GCP.

CLI changes

FortiProxy 7.4.8 includes the following CLI change:

- `config system fortisandbox`—Use the new `alt-server` option to configure an alternate FortiSandbox to be used when the main FortiSandbox is unavailable. Use the new `health-check-interval` option to configure the interval of health check for the failover.

Product integration and support

The following table lists product integration and support information for FortiProxy 7.4.8 build 649:

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 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 7.4.8 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 7.4.8, all FortiProxy devices in the Security Fabric must run FortiProxy 7.4.8. 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 7.4.8:

If you are using a RADIUS server that does not support the message-authenticator attribute, upgrading to 7.4.8 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 7.4.8. For example, to upgrade from 2.0.12 to 7.4.8, 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 7.4.8.

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 7.4.8 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 7.4.8, all FortiProxy devices in the Security Fabric must run FortiProxy 7.4.8. 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 7.4.8 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 7.4.8 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 7.4.8 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 7.4.8. For inquiries about a particular bug, please contact Customer Service & Support.

Description	Bug ID
1106496	Azure deployment failed with image-definition and HyperV Gen2.
1083120, 1051968	Inline-IPS does not support FortiProxy reporting to FortiGuard for its triggered signatures.
1097304	HA goes out-of-sync repeatedly despite no configuration changes.
1109045	FPX-VM license does not change to invalid after FortiGuard server returns failure.
1108723	Certificate authentication causes redirect loop between destination URL and authentication service port 7832.
1107762	Web proxy does not respect the over-size limit value when system memory is large.
1083357, 1112229	Inline IPS does not block SharePoint upload.
1093606	Buffer overflow.
1112733	Disable warning message from nf_ct_ext_add().
1112306	Fix heap buffer overflow in HTTP request line for the CSF proxy.
1108891	Permission escalation through websocket module in Node.js granting super admin access to the CLI.
1109812	Certificate authentication scheme Issue with IP-based policy and "user-cert" option.
1045789	Dynamic address not working in transparent policy.
1113147	BUFFER_SIZE found in daemon-dnsproxy.
1111621	"Unrated" URL category object is not visible in URL category group in GUI.
1108186	"config web-proxy profile" CLI mismatch between FortiProxy and FortiManager.
1114569	L7 VIP does not work.
1103696	When the ICAP client sends a preview 0 request, the request ends with only one CRLF.

Common vulnerabilities and exposures

FortiProxy 7.4.8 is no longer vulnerable to the following CVE references. Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE reference
1147743	CVE-2025-22254
1007270	CVE-2023-46718
1112306	CVE-2025-22258

Known issues

FortiProxy 7.4.8 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".
1106807	ERR_CONNECTION_CLOSED and ERR_HTTP2_PROTOCOL_ERROR occur randomly on Chrome and Edge.
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