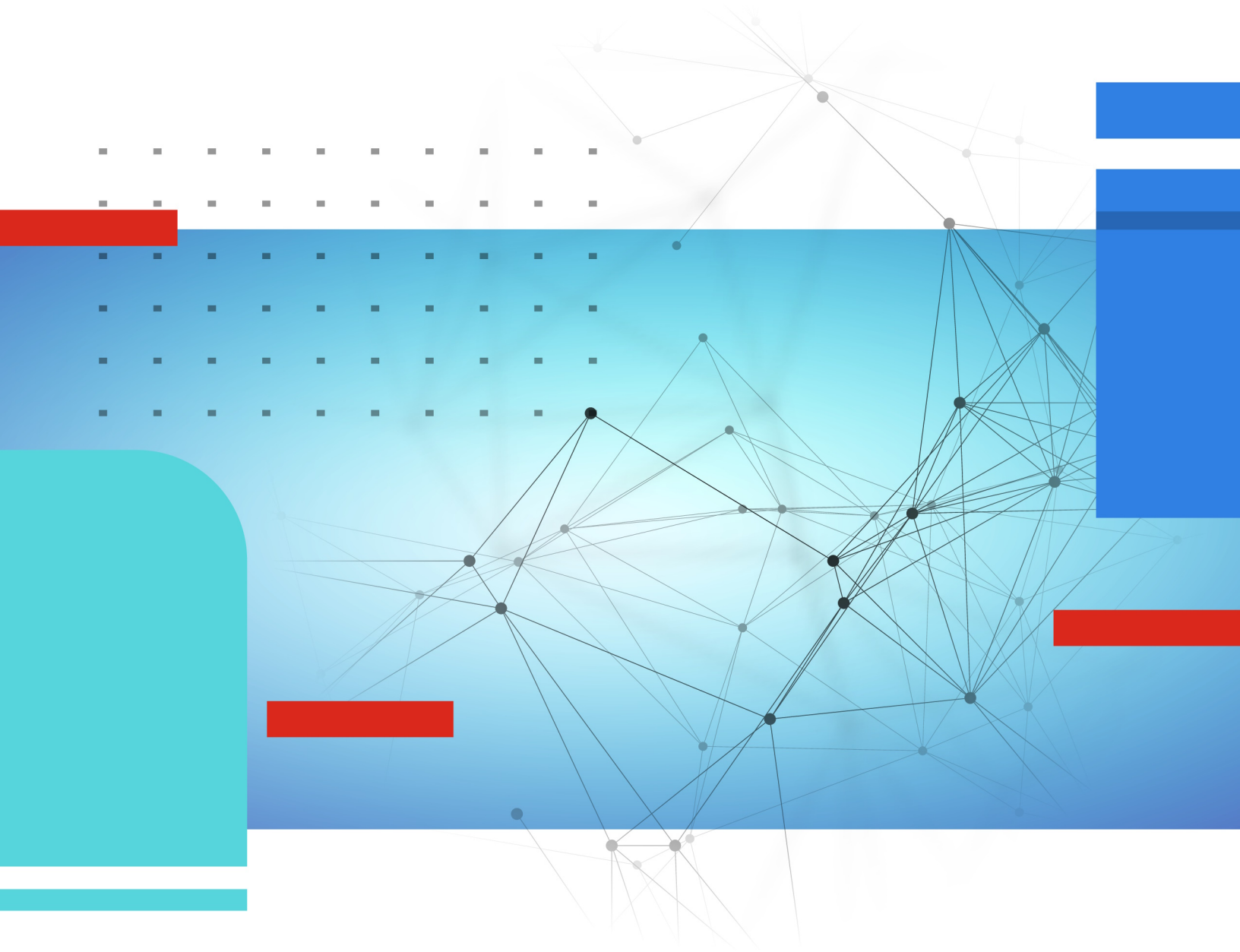
Release Notes

FortiProxy 7.6.2



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 7.6.2 Release Notes
45-762-1116324-20251015

TABLE OF CONTENTS

Change log

Date	Change Description
2025-01-24	Initial release.
2025-03-07	Updated What's new on page 7.
2025-05-13	Added CVE-2025-22252 to Resolved issues on page 17.
2025-06-10	Added CVE-2025-22254 to Resolved issues on page 17.
2025-07-09	Added CVE-2024-55599 and CVE-2024-52965 to Resolved issues on page 17.
2025-10-15	Added CVE-2025-25253, CVE-2025-22258, and CVE-2025-47890 to Resolved issues on page 17.

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.

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

FortiProxy 7.6.2 supports upgrade from 7.4.x or 7.6.x only. Refer to Deployment information on page 13 for detailed upgrade instructions.

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 7.6.2:

ZTNA agentless web-based application access

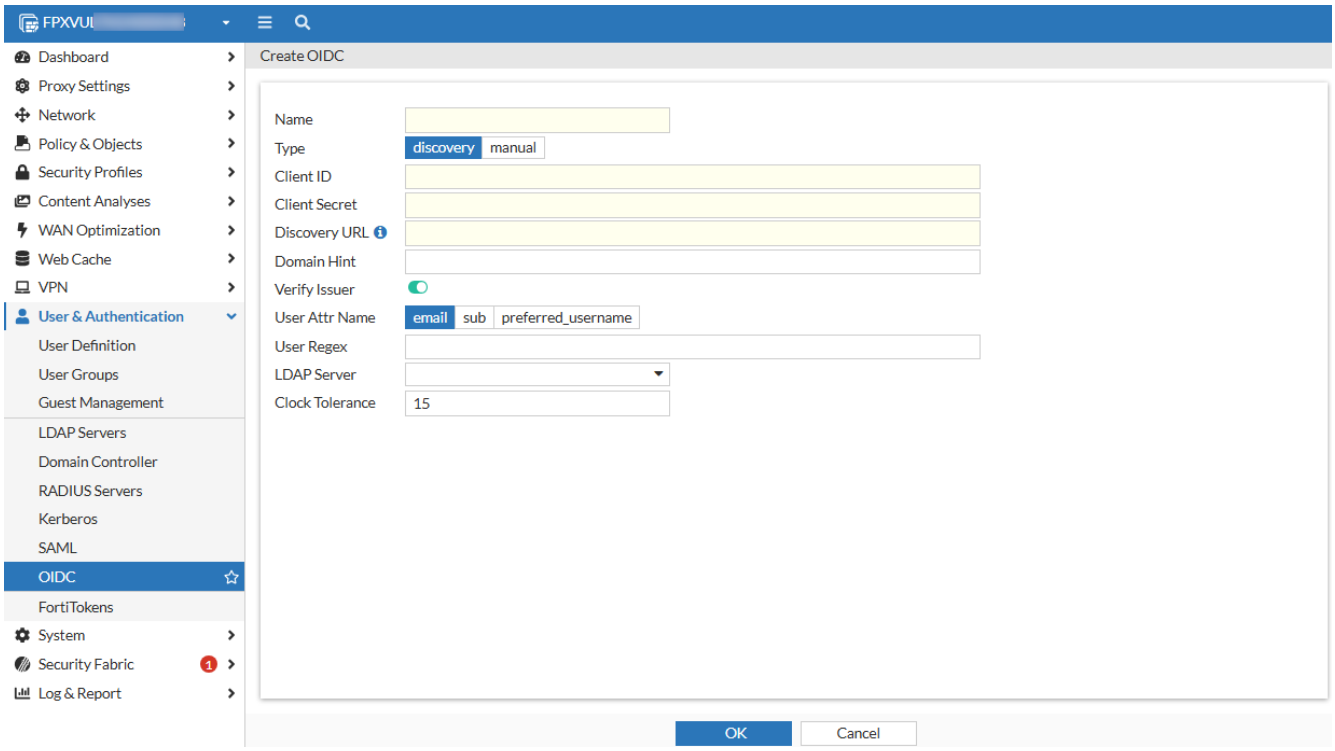
A ZTNA web portal is now available to provide end-user access to applications without FortiClient or client certificate checks. The ZTNA portal handles authentication and authorization of traffic destined for the protected resources. It is implemented entirely in WAD. When end-users connect to the ZTNA web portal, they are directed to a login page. Once logged in, end-users can access bookmarks defined by the administrator. Administrators can define dynamic bookmarks to generate personalized application shortcuts using an LDAP or SAML attribute within the user's LDAP or SAML account so that bookmarks are auto-populated with the values defined in that attribute instead of static pre-defined IP or hostnames.

See ZTNA agentless web-based application access in the Administration Guide for more details.

Authentication with OpenID Connect (OIDC)

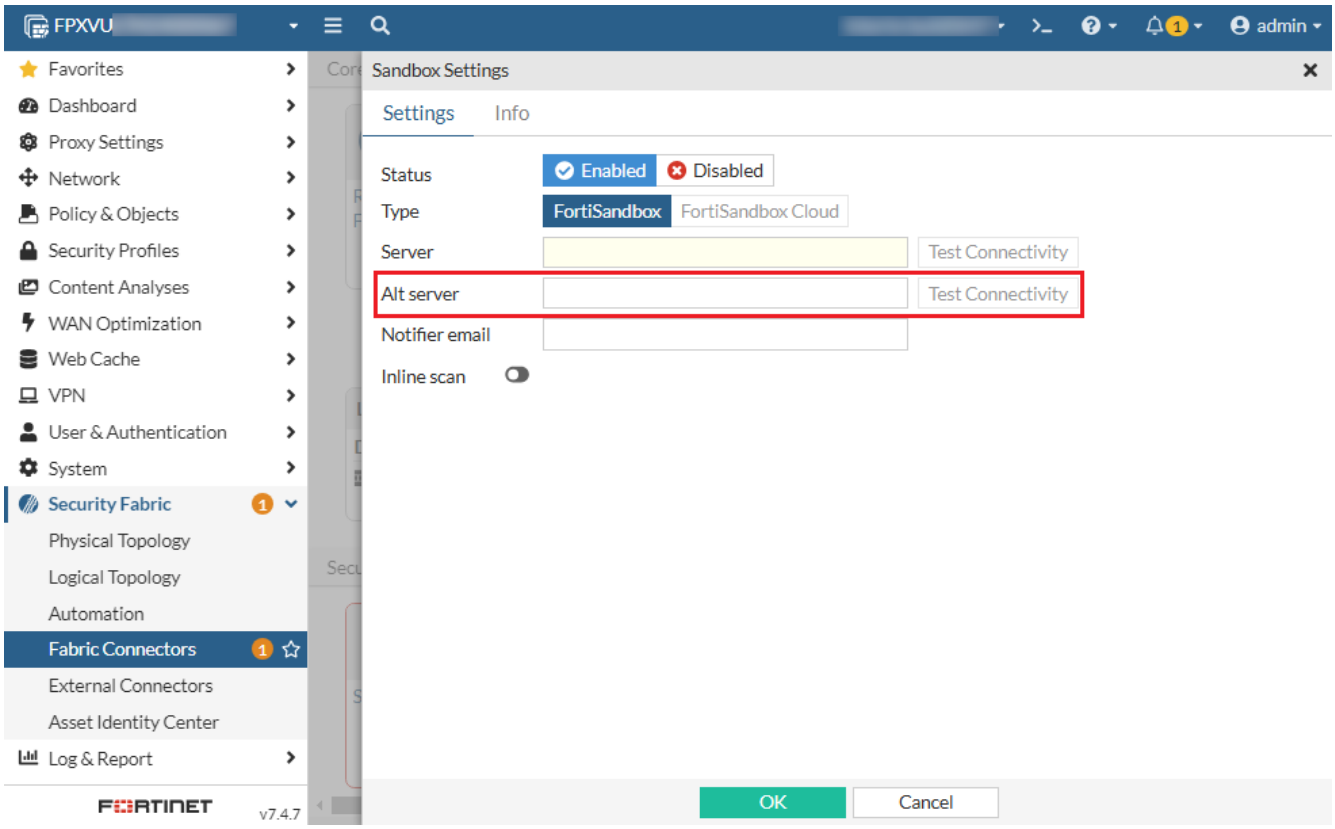
FortiProxy 7.6.2 adds support for authentication with OpenID Connect (OIDC), a widely adopted JSON-based identity layer built on top of the OAuth 2.0 protocol. If you have an Identity Provider (IdP) like Azure AD, Google Identity, or any other service that supports OIDC, you can use it to authenticate users seamlessly across your FortiProxy instance and other integrated systems.

To configure OIDC, go to the *User & Authentication* > *OIDC* tab or use the `config user oidc` command.



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

FolrtiProxy 7.6.2 adds 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."
```

Policy-based service connector traffic forwarding

FortiProxy 7.6.2 adds support for policy-based service connector traffic forwarding. In previous versions, the service connector must be configured within the traffic forward proxy, accessible only through ZTNA proxy.

To configure policy-based service connector traffic forwarding:

```
config firewall policy
   edit 1
      set service-connector "fpx166"
   next
end
```

Change to HTTP header content maximum length

In FortiProxy 7.6.2, the HTTP header content maximum length is increased from 1023 to 4000.

New data type support for DLP and file filter

FortiProxy 7.6.2 adds support for `.com`, `.jar`, `.jnlp`, `.css`, and `.dll` files for DLP and file filter.

UEFI support for GCP

FortiProxy 7.6.2 adds UEFI support for GCP.

CLI changes

FortiProxy 7.6.2 includes the following CLI changes:

- `config firewall ssl-ssh-profile`—The `set client-certificate` subcommand adds the new `bypass-on-cert-req` option to configure FortiProxy to bypass on certificate requests.
- `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.
- `config firewall policy`—This command includes the following new options:
  - Use the new `set service-connector` option configure a policy-based service connector for traffic forwarding.
  - Use the new `set https-sub-category` option to enable or disable HTTPS sub-category policy matching. The default is disable.
- `config web-proxy global`—The `set policy-category-deep-inspect` option is removed.

Product integration and support

The following table lists product integration and support information for FortiProxy 7.6.2 build 1542:

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 11 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 11 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 11 for a list of supported VM platforms.

Upgrading the FortiProxy

FortiProxy 7.6.2 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 7.6.2, all FortiProxy devices in the Security Fabric must run FortiProxy 7.6.2. 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 7.6.2:

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 7.6.2. For example, to upgrade from 7.0.17 to 7.6.2, upgrade to 7.2.5 or later first (reboot before upgrading to 7.2.x), and then 7.4.x, and then 7.6.2.

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 7.6.2 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 7.6.2, all FortiProxy devices in the Security Fabric must run FortiProxy 7.6.2. 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 7.6.2 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 7.6.2 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 7.6.2 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 7.6.2. For inquiries about a particular bug, please contact Customer Service & Support.

Description	Bug ID
1100906	Source NAT shows 0.0.0.0 in the logs.
1105731	Add connection timeout and its handler in wad_p2s_http_sesmodule.
1105549	Wrong signature algorithm is specified in certificates re-signed by a CA with ECDSA public key.
1096728	Continuous WAD crashing on Azure which affects some VIP traffic.
1074493	Some HTTP Transaction logs do not contain category and category description when webfilter is enabled.
1103965	Fails to create local certificate file.
1102925	ZTNA: An http1 strm is unnecessary created and leak when p2s connection is http2.
1101083	WAD app-based policy crash.
1097877	The license sharing widget does not show the purchased license seats of temporarily disconnected members that are still within the 8-hour grace period.
1103035	No backward-compatibility for license sharing.
1107205	WAD worker memory leak.
1106916, 1107097	Potential buffer overrun in memcpy.
1107762	Web proxy does not respect the over-size limit value when system memory is large.
1085418,1108118	Content analysis filename shows "Image Cache Was Cleared".
1107787	DLP license status is not correct on GUI.
983997,1099574	Failed to validate two different CAs with the same subject and issuer.
1103266	Remove default static client certificate for SSL/SSH inspection.
1106384	TFTP functions are not working.
1109812	Certificate authentication scheme Issue with IP-based policy and "user-cert" option.
1106496	Azure deployment failed with image-definition and HyperV Gen2.
1107077,1107230	No buffer size checking before memory copy and move operations.
1083120	Inline-IPS does not support FortiProxy reporting to FortiGuard for its triggered

Description	Bug ID
	signatures.
1109045	FPX-VM license does not change to invalid after FortiGuard server returns failure.
1110056	The service-connector configuration is global rather than per VDOM.
1097304	HA goes out-of-sync repeatedly despite no configuration changes.
1108723	Certificate authentication causes redirect loop between destination URL and authentication service port 7832.
1113147,1113148	BUFFER_SIZE found in daemon-dnsproxy.
1083357,1112229	Inline IPS does not block SharePoint upload.
1093606	Buffer overflow.
1112306	Fix heap buffer overflow in HTTP request line for the CSF proxy.
874516,1100819	Support AES-256 and AES-GMAC for SMB traffic in WAD and make krb5 vdom aware in 6.x kernel.
1108891	Permission escalation through websocket module in Node.js granting super admin access to the CLI.
1105419	SSL inspection is being applied even though traffic matches a policy that has no inspection.
1088866	Uploading of password-protected archive files is blocked.
1114890	ICAP UTM log does not have poluuid.
1115155	Bytes counter under *Policy & Objects* > *Policy* is always 0 although there are traffic hitting the policy.
1114569	L7 VIP does not work.
1115246	Release build fails with failover change.
1103696	When the ICAP client sends a preview 0 request, the request ends with only one CRLF.
1095678	OVERRUN found in daemon-wad.
1116523	FortiProxy video filter embedded block replacement message for Youtube shows FortiGate instead of FortiProxy.
1115137	Increase the maximum value of proxy-auth-timeout from 600 to 4320 minutes.
1112600	The wad_ftp_session_task_start does not initiate while establishing the data connection.
1109949	proxy-address http-method match failure.
1089162	In transparent mode, IP address changes on management interface is not learned until reboot.

Description	Bug ID
1115027	ICAP does not support sending SNI when FQDN is configured.
1117346	HTTPS Resource Record requests are bypassed by FortiProxy DNS filter.
1108350	Different category rating between FortiGuard web page and FortiProxy query.
1117073, 1117054, 1112756, 1115155, 1116117, 1115287, 1115283, 1107974, 1108244, 1117855, 1117604	GUI issues.
1107013	wad_hash_cache timeout issue.
1106446	No indication if a connection is websocket-based in HTTP transaction log.
1107113	ssl exempt logs "destination" and "destination-interface" fields not correct
1107847	Explicit proxy feature is not enabled by default.
1115799	VIP does not follow policy.
1117116	Failure in certificate authentication.
1117526	list_entry should be typesafe.
1115595	Traffic log says utmaction="allowed" when the security profile is not configured so.

Common vulnerabilities and exposures

FortiProxy 7.6.2 is no longer vulnerable to the following CVE references. Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE reference
1108969	CVE-2025-22252
1147743	CVE-2025-22254
1117346	CVE-2024-55599
1121042	CVE-2024-52965
1109747	CVE-2025-25253
1112306	CVE-2025-22258
1119207	CVE-2025-47890

Known issues

FortiProxy 7.6.2 includes the known issues listed in this section. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
1103523	The ARM64 image for AWS cannot be deployed correctly.
1072072	Device identification detection is not yet supported in FortiProxy 7.6.

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