

Release Notes

FortiProxy 7.2.3



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



December 12, 2023

FortiProxy 7.2.3 Release Notes

45-723-887206-20231212

TABLE OF CONTENTS

Change log	4
Introduction	5
Security modules	5
Caching and WAN optimization	6
What's new	7
Health check on ICAP remote servers	7
Forward server status monitoring	8
New commands to diagnose conntrack	10
New command to diagnose IP set lists	10
New command to configure trust hosts	10
Hold primary config-sync unit for some time before upgrading or rebooting	11
Match FQDNs from domain-list against SNI header for HTTPS requests	11
Add local URL list as data source for firewall	11
Process file access monitoring	12
Using existing HTTP header content for ICAP	12
Reverse proxy server support	13
Detect configuration changes in Windows Active Directory server	15
Diagnose memory of all wad processes	15
Changes to set domain-fronting configuration	15
Remove config fabric-device configuration	15
New event logs to indicate source port usage	16
Product integration and support	17
Deployment information	19
Downloading the firmware file	19
Deploying a new FortiProxy appliance	19
Deploying a new FortiProxy VM	19
Upgrading the FortiProxy	19
Downgrading the FortiProxy	20
Resolved issues	22
Common vulnerabilities and exposures	27

Change log

Date	Change Description
2023-03-01	Initial release.
2023-03-07	Added CVE-2022-41329 to Resolved issues on page 22 .
2023-03-08	Added CVE-2023-25610 to Resolved issues on page 22 .
2023-04-11	Deleted ticket 866011 and CVE-2022-41328 from Resolved issues on page 22 .
2023-04-21	Updated Introduction on page 5 .
2023-06-23	Updated Deployment information on page 19 .
2023-06-27	Updated Deployment information on page 19 .
2023-06-28	Added a few links in What's new on page 7 .
2023-08-02	Added the following CVEs to Resolved issues on page 22 : <ul style="list-style-type: none">• CVE-2023-33307• CVE-2023-33308
2023-10-26	Updated Product integration and support on page 17 .
2023-12-12	Added CVE-2023-41675 to Resolved issues on page 22 .

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:

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.
Data Leak 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.

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:

- [Health check on ICAP remote servers on page 7](#)
- [Forward server status monitoring on page 8](#)
- [New commands to diagnose conntrack on page 10](#)
- [New command to diagnose IP set lists on page 10](#)
- [New command to configure trust hosts on page 10](#)
- [Hold primary config-sync unit for some time before upgrading or rebooting on page 11](#)
- [Match FQDNs from domain-list against SNI header for HTTPS requests on page 11](#)
- [Add local URL list as data source for firewall on page 11](#)
- [Process file access monitoring on page 12](#)
- [Using existing HTTP header content for ICAP on page 12](#)
- [Reverse proxy server support on page 13](#)
- [Detect configuration changes in Windows Active Directory server on page 15](#)
- [Diagnose memory of all wad processes on page 15](#)
- [Changes to set domain-fronting configuration on page 15](#)
- [Remove config fabric-device configuration on page 15](#)
- [New event logs to indicate source port usage on page 16](#)

Health check on ICAP remote servers

Under *Content Analyses > ICAP Remote Servers*, you can now configure whether to enable health check of the ICAP remote server using the *Health Check* button. When enabled, FortiProxy attempts to connect to the ICAP remote server to verify that the server is operating normally and generates an event log each time the ICAP remote server health check fails or goes back online. You must also specify the ICAP service name to use for health check in the *Health Check Service* field.

In the ICAP remote server table, the *Health Check* column shows if health check is enabled for the ICAP remote server. The *Status* column shows the status of ICAP remote server, including *Online*, *Offline*, and *Unknown*.

Name	Address	Port	Health Check	Status	Ref.
server_1	10.1.1.100	1344	Enabled	Unknown	0

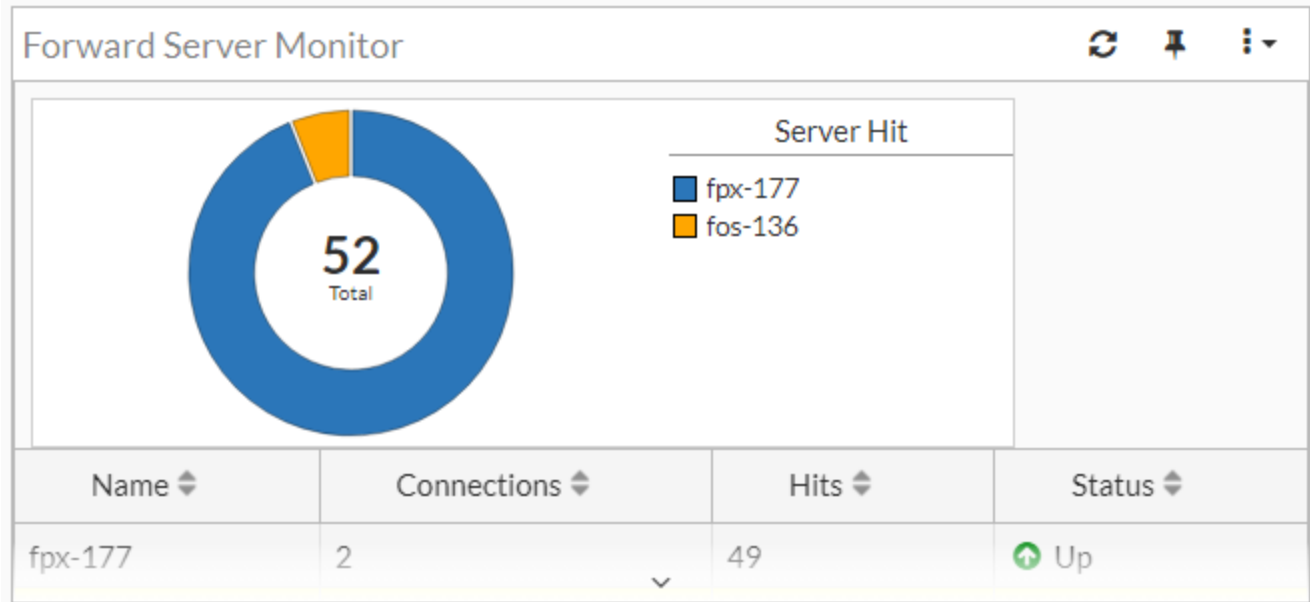
Refer to [Create or edit an ICAP remote server](#) in the Admin Guide for more details about creating or editing an ICAP remote server.

Alternatively, you can configure the health status check via CLI:

```
config icap remote-server
  edit <name>
    set healthcheck [disable|enable]
    set healthcheck-service {string}
  next
end
```

Forward server status monitoring

Use the new *Forward Server Monitor* widget to monitor the forward server status. See [Dashboard](#) in the Admin Guide for more information about this widget or other widgets available.



Alternatively, you can use the following new commands to monitor the forward server status:

- `diag wad webproxy forward-server`—For monitoring forward servers.
- `diag wad webproxy forward-server-group`—For monitoring forward server groups.

Sample output for monitoring forward servers:

```

VDOM=root group_name=1
lb-alg=weight n_servers=2 affinity=enable
hits=1 weight_total=10 weight_gen=2 weight_cur=9
VDOM=root group_name=1 server_name=fpx-177
hits=1 status=up weight=10 weight_gen=2 weight_cur=9
VDOM=root group_name=1 server_name=fos-136
hits=0 status=down weight=10 weight_gen=0 weight_cur=0
=====
VDOM=root group_name=my_srv_grp
lb-alg=weight n_servers=1 affinity=enable
hits=0 weight_total=10 weight_gen=1 weight_cur=0
VDOM=root group_name=my_srv_grp server_name=fpx-177
hits=0 status=up weight=10 weight_gen=0 weight_cur=0
    
```

Sample output for monitoring forward server groups:

```

VDOM=root group_name=g1
lb-alg=active-passive n_servers=2 affinity=disable
    
```

```
hits=107 weight_total=0 weight_gen=1 weight_cur=0
VDOM=root group_name=g1 server_name=227
hits=107 status=up weight=10 weight_gen=0 weight_cur=0
VDOM=root group_name=g1 server_name=229
hits=0 status=up weight=10 weight_gen=0 weight_cur=0
```

New commands to diagnose conntrack

Use the following commands to diagnose conntrack:

- `diag sys session conntrack count`
- `diag sys session conntrack list`
- `diag sys session conntrack clear`
- `diagnose sys session conntrack stats`
- `diagnose sys session conntrack list-dying`
- `diagnose sys session conntrack list-unconfirmed`

New command to diagnose IP set lists

Use the new `diagnose ipset list` command to diagnose IP set lists in case of policy matching issues on the kernel, which means the IP table is correct while the IP set list might be problematic.

New command to configure trust hosts

Under `config system admin`, use the new `config trusthosts` command to configure a list of trust hosts without the limitation of only 10 trust hosts using the existing `set trusthostX` command:

```
config trusthosts
  Description: Table of trusthosts.
  edit <id>
    set type [ipv4|ipv6]
    set ipv4 {ipv4-classnet}
    set ipv6 {ipv6-prefix}
  next
end
```

Hold primary config-sync unit for some time before upgrading or rebooting

Under `config system ha`, use the new `primary-hold-before-reboot {time}` command to hold primary config-sync unit for some time before upgrading or rebooting. Valid time values are integers within 0 and 600.

Match FQDNs from domain-list against SNI header for HTTPS requests

Under `config firewall policy`, when setting data source (`set dstaddr`), you can now reference the "domain" type that you set in `config system.external-resource` to avoid connection leakage.

To reference the "domain" type data via CLI:

```
config firewall policy
  edit <policyid>
    set dstaddr <external-resource domain list name>
  next
end
```

Add local URL list as data source for firewall

To add local URL list as data source for firewall via CLI:

1. Define the local URL list in web filter:

```
config webfilter url-list
  edit <name>
    set uuid {uuid}
    set status [enable|disable]
    set comment {var-string}
    config entries
      edit <url>
        next
      end
    next
  end
```

2. Configure the firewall proxy to use the local URL list:

```
config firewall proxy-address
  edit <name>
    set type url-list
    set url-list <External or webfilter URL list>
  next
end
```

- Reference the local URL list as data source of firewall using the `firewall.policy.dstaddr` command.

Process file access monitoring

Use the new `diag sys iotop` command to monitor process file access, which is useful for tracing what causes frequent disk access. By default, the command prints results at an interval of 5 seconds. You can also customize the interval to suit your needs. To print results immediately, press `Enter`.

For each file access, the following information is displayed: PID, process name, accessed file path, and the number of open, read, write, or close events during the interval. Delete and move information is not included. You can also use blacklists to hide sensitive or irrelevant files.

Sample output:

```
# diag sys iotop
PID #O #R #W #C PROCESS FILE
1078 1 0 2 0 miglogd /var/log/log/root/alog.65504
1078 1 0 2 0 miglogd /var/log/log/root/dlog.65504
1078 1 0 2 0 miglogd /var/log/log/root/hlog.65504
```

Using existing HTTP header content for ICAP

Under `config icap profile`, use the `config icap-headers` command to extract the HTTP header content for use in ICAP:

```
config icap-headers
  Description: Configure ICAP forwarded request headers.
  edit <id>
    set name {string}
    set source [content|http-header|...]
    set content {string}
    set http-header {string}
    set session-info-type [client-ip|user|...]
    set base64-encoding [disable|enable]
  next
end
```

Parameter	Description	Type	Size	Default
name	HTTP forwarded header name.	string	Maximum length: 79	
source	HTTP append header source.	option	-	content
	Option	Description		
	<i>content</i>	Create ICAP header from content.		

Parameter	Description	Type	Size	Default																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>http-header</i></td> <td>Create ICAP header from HTTP header.</td> </tr> <tr> <td><i>session</i></td> <td>Create ICAP header from session info.</td> </tr> </tbody> </table>	Option	Description	<i>http-header</i>	Create ICAP header from HTTP header.	<i>session</i>	Create ICAP header from session info.																	
Option	Description																							
<i>http-header</i>	Create ICAP header from HTTP header.																							
<i>session</i>	Create ICAP header from session info.																							
content	HTTP header content.	string	Maximum length: 255																					
http-header	HTTP header-field name.	string	Maximum length: 79																					
session-info-type	Session info type.	option	-	client-ip																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>client-ip</i></td> <td>Client ip address.</td> </tr> <tr> <td><i>user</i></td> <td>Authentication user name.</td> </tr> <tr> <td><i>upn</i></td> <td>Authentication user principal name.</td> </tr> <tr> <td><i>domain</i></td> <td>User domain name.</td> </tr> <tr> <td><i>local-grp</i></td> <td>Firewall group name.</td> </tr> <tr> <td><i>remote-grp</i></td> <td>Group name from authentication server.</td> </tr> <tr> <td><i>proxy-name</i></td> <td>Proxy realm name.</td> </tr> <tr> <td><i>auth-user-uri</i></td> <td>Authenticated user uri.</td> </tr> <tr> <td><i>auth-group-uri</i></td> <td>Authenticated group uri.</td> </tr> </tbody> </table>	Option	Description	<i>client-ip</i>	Client ip address.	<i>user</i>	Authentication user name.	<i>upn</i>	Authentication user principal name.	<i>domain</i>	User domain name.	<i>local-grp</i>	Firewall group name.	<i>remote-grp</i>	Group name from authentication server.	<i>proxy-name</i>	Proxy realm name.	<i>auth-user-uri</i>	Authenticated user uri.	<i>auth-group-uri</i>	Authenticated group uri.			
Option	Description																							
<i>client-ip</i>	Client ip address.																							
<i>user</i>	Authentication user name.																							
<i>upn</i>	Authentication user principal name.																							
<i>domain</i>	User domain name.																							
<i>local-grp</i>	Firewall group name.																							
<i>remote-grp</i>	Group name from authentication server.																							
<i>proxy-name</i>	Proxy realm name.																							
<i>auth-user-uri</i>	Authenticated user uri.																							
<i>auth-group-uri</i>	Authenticated group uri.																							
base64-encoding	Enable/disable use of base64 encoding of HTTP content.	option	-	disable																				
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>disable</i></td> <td>Disable use of base64 encoding of HTTP content.</td> </tr> <tr> <td><i>enable</i></td> <td>Enable use of base64 encoding of HTTP content.</td> </tr> </tbody> </table>	Option	Description	<i>disable</i>	Disable use of base64 encoding of HTTP content.	<i>enable</i>	Enable use of base64 encoding of HTTP content.																	
Option	Description																							
<i>disable</i>	Disable use of base64 encoding of HTTP content.																							
<i>enable</i>	Enable use of base64 encoding of HTTP content.																							

Reverse proxy server support

Under `config firewall vip`, you can now configure the type to be `server-load-balance` and specify the load balancing method. You can also define the health check protocol using the `set health-check-proto` command under `config realservers` under `config firewall access-proxy`.

```
config firewall vip
  Description: Configure virtual IP for IPv4.
  edit <name>
    set type [static-nat|server-load-balance|...]
```

```
set ldb-method [static|round-robin|...]
```

```
config realservers
```

Description: Select the real servers that this server load balancing VIP will distribute traffic to.

```
edit <id>
```

```
set type [ip|address]
```

```
set healthcheck [disable|enable]
```

```
set health-check-proto [ping|http]
```

```
next
```

```
end
```

Parameter	Description	Type	Size	Default												
type	Configure between a static NAT and access proxy VIP.	option	-	static-nat												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>static-nat</i></td> <td>Static NAT.</td> </tr> <tr> <td><i>server-load-balance</i></td> <td>Server load balance.</td> </tr> <tr> <td><i>access-proxy</i></td> <td>Access proxy.</td> </tr> </tbody> </table>	Option	Description	<i>static-nat</i>	Static NAT.	<i>server-load-balance</i>	Server load balance.	<i>access-proxy</i>	Access proxy.							
Option	Description															
<i>static-nat</i>	Static NAT.															
<i>server-load-balance</i>	Server load balance.															
<i>access-proxy</i>	Access proxy.															
ldb-method	Method used to distribute sessions to real servers.															
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>static</i></td> <td>Distribute to server based on source IP.</td> </tr> <tr> <td><i>round-robin</i></td> <td>Distribute to server based round robin order.</td> </tr> <tr> <td><i>weighted</i></td> <td>Distribute to server based on weight.</td> </tr> <tr> <td><i>first-alive</i></td> <td>Distribute to the first server that is alive.</td> </tr> <tr> <td><i>http-host</i></td> <td>Distribute to server based on host field in HTTP header.</td> </tr> </tbody> </table>	Option	Description	<i>static</i>	Distribute to server based on source IP.	<i>round-robin</i>	Distribute to server based round robin order.	<i>weighted</i>	Distribute to server based on weight.	<i>first-alive</i>	Distribute to the first server that is alive.	<i>http-host</i>	Distribute to server based on host field in HTTP header.			
Option	Description															
<i>static</i>	Distribute to server based on source IP.															
<i>round-robin</i>	Distribute to server based round robin order.															
<i>weighted</i>	Distribute to server based on weight.															
<i>first-alive</i>	Distribute to the first server that is alive.															
<i>http-host</i>	Distribute to server based on host field in HTTP header.															
healthcheck	Enable to check the responsiveness of the real server before forwarding traffic.	option	-													
health-check- proto	Protocol of the health check monitor to use when polling to determine server's connectivity status.	option	-	ping												
	<table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><i>ping</i></td> <td>Use PING to test the link with the server.</td> </tr> <tr> <td><i>http</i></td> <td>Use HTTP-GET to test the link with the server.</td> </tr> </tbody> </table>	Option	Description	<i>ping</i>	Use PING to test the link with the server.	<i>http</i>	Use HTTP-GET to test the link with the server.									
Option	Description															
<i>ping</i>	Use PING to test the link with the server.															
<i>http</i>	Use HTTP-GET to test the link with the server.															

Detect configuration changes in Windows Active Directory server

To configure FortiProxy to detect configuration changes in Windows Active Directory server via CLI:

```
config user domain-controller
    edit <name>
        set change-detection [enable|disable]
        set change-detection-period {integer}
    next
end
```

enable	Enable detection of configuration changes in the Active Directory server.
disable	Disable detection of configuration changes in the Active Directory server (default).
integer	Intervals (in minutes) to detect configuration changes in the Active Directory server. Valid value range is between 5 and 10080. The default is 60.

Diagnose memory of all wad processes

Use the new `diagnose wad memory workers` command to show all wad processes cmem stats, as opposed to only workers.

Use the `diagnose wad memory track` command to show all wad processes cmem stats, fmem stats, pool stats, block stats, mmap stats, mallinfo summed up, and then mmap stats, pool stats, block stats, mallinfo, top 6 cmem stats, top 5 fmem stats per process. mallinfo is written to process shm every 30 seconds.

Changes to set domain-fronting configuration

Under `config firewall profile-protocol-options`, the options for the `set domain-fronting` configuration change from

`[enable|disable]` to `[allow|block|monitor]`.

allow	Allow domain fronting.
block	Block and log domain fronting.
monitor	Allow and log domain fronting.

Remove config fabric-device configuration

Under `config system csf`, the `config fabric-device` configuration is removed.

New event logs to indicate source port usage

The following logs are added for reporting or warning about source port usage:

- **High source port usage**—This log is recorded when more than half of the available source ports on an IP is in use during the last few consecutive attempts of the FortiProxy to get a source port.
- **Source port exhaustion**—This log is recorded when no available source port can be found for a source IP.


Use the following two diagnose commands to dump the cache of recent events for the new event types:

- `dia test app forticron 50`
- `dia test app forticron 51`

Product integration and support

The following table lists product integration and support information for FortiProxy 7.2.3 build 0356:

Type	Product and version
FortiProxy appliance	<ul style="list-style-type: none">• FPX-2000E• FPX-4000E• FPX-400E
FortiProxy VM	<ul style="list-style-type: none">• FPX-AZURE• FPX-HY• FPX-KVM• FPX-KVM-ALI• FPX-KVM-AWS• FPX-KVM-GCP• FPX-KVM-OPC• FPX-VMWARE• FPX-XEN
Fortinet products	<ul style="list-style-type: none">• 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.• Fortisolator 2.2 and later - See the Fortisolator Release Notes.
Fortinet Single Sign-On (FSSO)	5.0 build 0301 and later (needed for FSSO agent support OU in group filters) <ul style="list-style-type: none">• 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• 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

Type	Product and version		
Web browsers	<ul style="list-style-type: none"> • Microsoft Edge • Mozilla Firefox version 87 • Google Chrome version 89 		
	 <p>Other web browsers may work correctly, but Fortinet does not support them.</p>		
Virtualization environments	<p>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.</p>		
	<table border="0"> <tr> <td>HyperV</td> <td> <ul style="list-style-type: none"> • Hyper-V Server 2008 R2, 2012, 2012R2, 2016, and 2019 </td> </tr> </table>	HyperV	<ul style="list-style-type: none"> • Hyper-V Server 2008 R2, 2012, 2012R2, 2016, and 2019
	HyperV	<ul style="list-style-type: none"> • Hyper-V Server 2008 R2, 2012, 2012R2, 2016, and 2019 	
	<table border="0"> <tr> <td>Linux KVM</td> <td> <ul style="list-style-type: none"> • RHEL 7.1/Ubuntu 12.04 and later • CentOS 6.4 (qemu 0.12.1) and later </td> </tr> </table>	Linux KVM	<ul style="list-style-type: none"> • RHEL 7.1/Ubuntu 12.04 and later • CentOS 6.4 (qemu 0.12.1) and later
	Linux KVM	<ul style="list-style-type: none"> • RHEL 7.1/Ubuntu 12.04 and later • CentOS 6.4 (qemu 0.12.1) and later 	
	<table border="0"> <tr> <td>Xen hypervisor</td> <td> <ul style="list-style-type: none"> • OpenXen 4.13 hypervisor and later • Citrix Hypervisor 7 and later </td> </tr> </table>	Xen hypervisor	<ul style="list-style-type: none"> • OpenXen 4.13 hypervisor and later • Citrix Hypervisor 7 and later
	Xen hypervisor	<ul style="list-style-type: none"> • OpenXen 4.13 hypervisor and later • Citrix Hypervisor 7 and later 	
<table border="0"> <tr> <td>VMware</td> <td> <ul style="list-style-type: none"> • ESXi versions 6.5, 6.7, and 7.0 </td> </tr> </table>	VMware	<ul style="list-style-type: none"> • ESXi versions 6.5, 6.7, and 7.0 	
VMware	<ul style="list-style-type: none"> • ESXi versions 6.5, 6.7, and 7.0 		
<table border="0"> <tr> <td>Openstack</td> <td> <ul style="list-style-type: none"> • Ussuri </td> </tr> </table>	Openstack	<ul style="list-style-type: none"> • Ussuri 	
Openstack	<ul style="list-style-type: none"> • Ussuri 		
<table border="0"> <tr> <td>Nutanix</td> <td> <ul style="list-style-type: none"> • AHV </td> </tr> </table>	Nutanix	<ul style="list-style-type: none"> • AHV 	
Nutanix	<ul style="list-style-type: none"> • AHV 		
Cloud platforms	<ul style="list-style-type: none"> • 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 17](#) 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 17](#) 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 17](#) for a list of supported VM platforms.

Upgrading the FortiProxy

You can upgrade FortiProxy appliances or VMs from 7.0.x or 7.2.x to 7.2.3 by following the steps below:

1. In the GUI, go to *System > Firmware*.
2. Click *Browse* in the *File Upload* tab.
3. Select the file on your PC and click *Open*.
4. Click *Confirm and Backup Config*.

5. Click *Continue*.

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

If you are currently using FortiProxy 2.0.x, Fortinet recommends that you upgrade to 7.0.x first by following the same steps above before attempting to upgrade to 7.2.3.

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.

After you upgrade from 2.0.x to 7.0.x, click *Reset All Dashboards* in the GUI to avoid any issues with FortiView.

Downgrading the FortiProxy

You can downgrade FortiProxy appliances or VMs from 7.2.3 to 7.2.x or 7.0.x by following the steps below:

1. In the GUI, go to *System > Firmware*.
2. Click *Browse* in the *File Upload* tab.
3. Select the file on your PC and click *Open*.
4. Click *Confirm and Backup Config*.
5. Click *Continue*.

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

To downgrade from FortiProxy 7.2.3 to 2.0.x, Fortinet recommends that you downgrade to 7.0.x first by following the same steps above before attempting to downgrade to 2.0.x.

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.

After you downgrade from 7.0.x to 2.0.x, click *Reset All Dashboards* in the GUI to avoid any issues with FortiView.

Resolved issues

The following issues have been fixed in FortiProxy 7.2.3. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
871559	The command "exec bypass-mode enable/disable" is not functional.
875832	doh server crash when connecting to 443 port for GUI.
746587	Wad process crashes several times during file download.
756345	In certain circumstances, such as after booting, vd->policy_conf_gen lags behind g_wad.policy_generation, causing a logic failure that leads to conflict with IANA protocol numbers.
776260	MAPI HTTP messages do not come through when ICAP profile is enabled.
779361	When AV profile has outbreak-prevention, FortiProxy reports an error while handling requests from FTP servers that require non-anonymous login.
796510	When all server in a forward server group goes down, traffic through the group is forwarded to the original destination directly even if down-option is set to `block`.
811975	Multiple widgets do not have a data source when VDOMs are enabled.
812888	When a client sends an HTTP/1.0 request, FortiProxy's forwarded response is always HTTP/1.1. Furthermore, if the server's response has chunked encoding, then FPX does not remove chunked encoding before forwarding the response to the client.
820383	IPv6 support for FNBI.
822829	FortiProxy does not have default policy for ftp. When a client tries to access an ftps server, ses_ctx->sec_profile is none in wad_ftp_on_auth_cmd(), which causes crash.
825977	Fix crash on avscan submission error due to double close.
828194	SSLVPN stops passing traffic after some time.
831069	Blank page displayed after login to back-end server in SSLVPN web mode.
835636	No indicator for egress TCP port exhaustion.
842517	Adding a local user to a group containing lot of users causes delay on GUI and CLI due to cmdbsvr (high CPU).
843318	WAD worker may crash with signal 11 if the request header contains "Cache-Control: only-if-cached".
844488	FNBI installation fails on Windows 10 VMs.
851581	Change FortiView shaper monitor to show real-time information.
853060	Wad crash on wad_hmsg_strm_buffering_put.

Bug ID	Description
854115	ssh-policy-check results in TP policy being ignored.
855882	Memory leaking issue due to a typo in the calloc API.
857284	Unable to delete a VDOM from FortiProxy CLI.
857368	After upgrading to 7.0.8, WAD crash with signal 11 wad_hpack which is caused by a stack allocated buffer overflow.
857632	wad http2 hpack parsing error in an edge case.
859013	Debug daemon may get stuck and cause Web GUI to load slowly.
860190	A tp-policy without any ssh related UTM will fail to redirect to check ssh-policies.
863317	Fix GUI issue about FortiSandbox on the AntiVirus profile configuration page.
863855	Lack of certificate verification when establishing secure connections with fabric devices.
865301	AliCloud failure to rebind public eip to the new primary FortiProxy after HA failover.
867005	Sending traffic to icap client using icap secure results in "502 Bad Gateway".
867453	Enable IPv6 forwarding.
867900	Router is not learnt when the VDOM is newly created.
868250	No monitoring for disk access. Difficult to trace what causes frequent disk access.
868666	Improper use of snprintf to write into a buffer.
868782	Change the default value formula of config.system.global.contrack to be memory-size-based.
869105	A manual restart is needed to validate FNBI installer and iso image changes.
869120	Fix wad crashes when loading or updating policy configuration.
869267	config-sync cluster is not able to sync with NTP server using dedicated mgmt interfaces.
869359	Azure Auto-scale HA shows certificate error in secondary.
869453	Enable IPv6 forwarding.
869578	When solving eicar evasion problem, status code 1xx and 204/304 are handled together rather than separately.
869700	wad crash at wad_h2_proc_data when icap blocks the traffic.
869923	DNS filter not taking effect for DoT traffic.
870099	LDAP cache was not updated properly after the user group changed in Active Directory server.
870391	FortiProxy VDOM decrypted traffic mirror feature works only on root VDOM.
870764	In wad_ftp_tp_cancel, wad delete the session context lease after the session is closed
870900	Cannot add FortiProxy to FortiManager during the first setup or after factory reset.

Bug ID	Description
871449	WAD crashes on policy testing when test request destination is IP and port.
872358	The logout option does not work when "Keep-alive" authentication is enabled.
872366	"Insert empty policy" in GUI copies some fields from the parent policy instead of inserting a blank policy.
872368	Failed to save changes while adding a user as source in a policy using quick edit.
872617	SWG SSO shows "Firewall Authentication" failure on endpoint, which is caused by infinite redirects.
872685	When adding user objects to source field in a policy, the user objects are not highlighted.
872721	HA role is not updated on Web UI status bar.
872752	CSF config-sync management IP and port should not be synced.
872931	'diag sys session list' fails to list all sessions.
872950	wad_scan module is closed in wad_scan_handle_scan_results, which causes a crash.
873031	Web UI firmware upgrade option is not available.
873138	Cannot configure HA secondary heartbeat interface.
873369	HA fails to sync on KVM multicast HA when interface is virtio.
873458	Add forward server status update in passive mode for transparent traffic.
873475	Improvements to Security Fabric license sharing of user seats.
873652	FNBI does not work for web dialogue.
873656	Failed to validate the EMS certificate which is signed by third-party CA and installed into FortiProxy.
873851	When you create a new vdom, wad_ui_prefetch_vd_init and wad_ui_reverse_cache_server_vd_init are not called and the linked list is not initialized, which results in a crash while traversing the linked list.
874178	Eicar fetch traffic still gets blocked by AV after AV profile is removed from profile group.
874226	Fix policy session number overflow in GUI and diag command.
874563	Crash and compile error due to implementation or coding error.
874711	Explicit Proxy Traffic only has Policy ID recorded without the policy name on Web UI.
874989	Support multiple 'Server' headers to fix website login issues.
875100	Unable to remove external-resource in a certain VDOM when external resource has no reference in that VDOM.
875170	Cannot view more than 500 lines under <i>Log & Report > Forward Traffic</i> on FortiProxy-2000E.
875175	Requests from local non-domain LDAP users are denied by the explicit firewall policy.
875485	Log all socks traffic as https transaction and show domain name in "hostname" and "url" for

Bug ID	Description
	FQDN requests.
875708	Fix high CPU utilization when memory usage is high.
876394	Unable to run FortiNBI client on Windows 10 with error "FortiNBI Couldn't communicate with isolator".
876758	SSH key is added even if operation is aborted.
877128	ZTNA saml portal or auth portal cannot handle cors preflight because it does not take cors preflight request into consideration after matching (saml/auth) gateway.
877230	If an HB interface is disabled and enabled on a unit, the respective unit will never join the cluster unless it is restarted.
877774	psv_tm prints the wrong time in diagnose command.
878298	If the memory usage is out of control, the appending request is added to a 'hold-list' for a while to apply flow-control to the worker. The request might not be removed from the list properly for some corner cases.
878587	HA role in the list page is not consistent with the detail page.
878782	PAC configuration issue.
878863	Forward server group log only works when load-balance algorithm (ldb-method) is 'weighted'.
880092	icap server hangs when icap secure is enabled.
880205	Fix firewall policy schedule with year later than 2038.
880479	Fix debug daemon crash when session is not found, which usually happens when CLI or worker exits before the request is done.
881499	Icap client crashed on wad_conn_pool_conn error.
881693	Fix SSL/SSH Inspection inspection profile visible issue.
881697	After the cluster is formed and the slave is restarted, it comes back with "config file may contain errors".
881846	Every VDOM has ha-mgmt and ha-vsyst VRFs, which causes issues.
882475	Domain user suffix extract from krb ticket not matching what's shown in diag wad user list.
882728	SNAT occasionally fails on DNS requests.
883067	AV cache-infected-result causes false positives with incorrect dst addr.
883121	HTTP transaction log does not show status code for some cached traffics.
883170	Cached object is corrupted and client keeps resending request with token.
883589	Traffic is still blocked after FNBI license expires.
883618	New Alibaba region (SCCC) uses different region-id.
884280	FortiProxy does not respond to explicit proxy requests on VLAN interface.

Bug ID	Description
884339	Wad process keeps crashing with signal 11.
378251 860859	Fix nf_contrack_expect's reference for master contrack to avoid leaks.
802564 881341	Forticron crash when restoring VDOM configuration.
833306 884670	Intermittent error "Failed to retrieve FortiView data" on real-time FortiView sources and destination.
835903 842624	Change WAD's TCP port to delay close if datais pending on socket's write queue.
836705 836710	FNBI does not work for non-admin users on Windows 10.
843288 874159	No endpoint information is found when accessing ZTNA application FUSE.
850683 850688	Console keeps printing "bcm_nl.nr_request_drop 20753".
871749 874932	Wad crash about infection cache feature.
874049 860282	SSLVPN crashes when using webmode access.
877873 877875	When new hataalk is launched, ha_clear_state() is called to reset some shared memory information which could be accessed by hataalk.
880624 881471	Fix unpopulated ipset when FQDN dstaddr is specified.
880712 882878	Fix wad crash and memory leak on traffic mirror.
881208 882886	Fix masquerade 'disable' in transparent policy which causes traffic failure.
883762 823962	Unable to update AV/ISDB database.
845698 857358 866735	Google Cloud - When ha_filtered is called on slave's receiving, some packets are dropped as IP header is not correct.
861343 863428 870022	Fix policy hit counts not shown in GUI policy list and diag command.

Bug ID	Description
870846	FPX hardware models do not update CMOS time correctly.
871239	
871587	
881553	Fix some GUI issues.
882350	
882403	
869573	
885912	
886579	

Common vulnerabilities and exposures

FortiProxy 7.2.3 is no longer vulnerable to the following CVE references. Visit <https://fortiguard.com/psirt> for more information.

Bug ID	CVE reference
845848	CVE-2022-41329
874761	CVE-2023-25610
874049	CVE-2023-33307
857368	CVE-2023-33308
843318	CVE-2023-41675



www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.