

Release Notes

FortiProxy 7.0.8



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 26, 2023

FortiProxy 7.0.8 Release Notes

45-708-864483-20231026

TABLE OF CONTENTS

Change Log	4
Introduction	5
Security modules	5
Caching and WAN optimization	6
Supported models	6
What's new	7
Toggle logging pending traffic	7
Passive FTP mode for explicit proxy	7
Use the first hard disk for logging only	8
Toggle TLS fingerprint	8
Support AliCloud platform	8
Product integration and support	9
Web browser support	9
Fortinet product support	9
Fortinet Single Sign-On (FSSO) support	9
Virtualization environment support	10
New deployment of the FortiProxy VM	10
Upgrading the FortiProxy VM	10
Downgrading the FortiProxy VM	11
Software upgrade path for physical appliances	11
Resolved issues	12
Common vulnerabilities and exposures	15

Change Log

Date	Change Description
2022-12-15	Initial release.
2023-03-07	Added "CVE-2022-45861" to Resolved issues on page 12 .
2023-04-11	Added the following CVEs to Resolved issues on page 12 : <ul style="list-style-type: none">• CVE-2022-41330• CVE-2022-43947
2023-06-13	Added the following CVEs to Resolved issues on page 12 : <ul style="list-style-type: none">• CVE-2022-42474• CVE-2022-41327
2023-10-26	Updated Product integration and support on page 9 .

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 data leak prevention (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 data leak prevention 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)**
 - Intrusion Prevention System 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.

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

Supported models

The following models are supported on FortiProxy 7.0.8, build 0122:

FortiProxy	<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

What's new

The following sections describe new features and enhancements:

- [Toggle logging pending traffic on page 7](#)
- [Passive FTP mode for explicit proxy on page 7](#)
- [Use the first hard disk for logging only on page 8](#)
- [Toggle TLS fingerprint on page 8](#)
- [Support AliCloud platform on page 8](#)

Toggle logging pending traffic

Logging pending traffic can be enabled/disabled. When enabled, all traffic, including pending traffic, is logged. When disabled, only traffic matched to a policy is logged. It is disabled by default.

To configure the logging sessions depending on policy matching:

```
config web-proxy global
    set log-policy-pending {enable | disable}
end
```

enable	Enable logging sessions that are pending on policy matching.
disable	Disable logging sessions that are pending on policy matching (default).

Passive FTP mode for explicit proxy

The FTP mode for explicit proxy can be changed to passive mode. When in passive mode, the FTP client mode is based on the FTP client's preference, while the FTP proxy to FTP server connection is always passive (if supported by the FTP server).

By default, the FTP mode is client, meaning that the FTP mode for both the client and server is based on the FTP client's preference.

To configure the FTP mode for explicit proxy:

```
config ftp-proxy explicit
    set status enable
    set server-data-mode {client | passive}
end
```

client	Use the same transmission mode for client and server data sessions (default).
passive	Use passive mode on server data session.

Use the first hard disk for logging only

On high end models, such as the FortiProxy 2000E and 4000E, the first hard disk can be configured to be used only for logging, as opposed to logging and WAN optimization.

To configure what the first hard disk is used for:

```
config system storage
    edit "HD1"
        set usage {mix | log}
    next
end
```

mix	Use the hard disk for both logging and WAN Optimization.
log	Use the hard disk for logging.

Toggle TLS fingerprint

The TLS fingerprint can be updated when deep-inspection is enabled. By default, this option is disabled.

```
config system global
    set update-tls-finger-print {enable | disable}
end
```

Support AliCloud platform

FortiProxy-VM supports Alibaba Cloud (AliCloud).

AliCloud Elastic Compute Service (ECS) provides fast memory and the latest Intel CPUs to help you power your cloud applications and achieve faster results with low latency.

Product integration and support

Web browser support

The following web browsers are supported by FortiProxy 7.0.8:

- Microsoft Edge
- Mozilla Firefox version 87
- Google Chrome version 89

Other web browsers might function correctly but are not supported by Fortinet.

Fortinet product support

- 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) support

- 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
 - 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

Virtualization environment support

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.

Supported hypervisor versions:

HyperV	<ul style="list-style-type: none"> Hyper-V Server 2008 R2, 2012, 2012R2, 2016, and 2019
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
Xen hypervisor	<ul style="list-style-type: none"> OpenXen 4.13 hypervisor and later Citrix Hypervisor 7 and later
VMware	<ul style="list-style-type: none"> ESXi versions 6.5, 6.7, and 7.0
Openstack	<ul style="list-style-type: none"> Ussuri
Nutanix	<ul style="list-style-type: none"> AHV

Supported cloud platforms:

- AWS (Amazon Web Services)
- Microsoft Azure
- GCP (Google Cloud Platform)
- OCI (Oracle Cloud Infrastructure)
- Alibaba Cloud

New deployment of the FortiProxy VM

The minimum memory size for the FortiProxy VM for 7.0.4 or later is 4 GB. You must have at least 4 GB of memory to allocate to the FortiProxy VM from the VM host.



A new FortiProxy VM license file was introduced in the FortiProxy 2.0.6 release. This license file cannot be used for FortiProxy 2.0.5 or earlier. Do not downgrade the FortiProxy 2.0.6 VM because the new VM license cannot be used by earlier versions of the FortiProxy VM.

Upgrading the FortiProxy VM



You can upgrade to FortiProxy 2.0.5 from earlier FortiProxy releases or you can upgrade from FortiProxy 2.0.6 to a higher version. You cannot upgrade from FortiProxy 2.0.5 because of the new FortiProxy VM license file that was introduced in the FortiProxy 2.0.6 release.

To upgrade FortiProxy VM to 2.0.5, or from 2.0.6 and later:

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.

Downgrading the FortiProxy VM

To downgrade from FortiProxy 7.0.8 or later 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.

Software upgrade path for physical appliances



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

You can upgrade FortiProxy appliances directly from 2.0.6 and later to 7.0.8.

To upgrade a FortiProxy appliance:

1. Back up the configuration from the GUI or CLI.
2. Go to *System > Firmware* and click *Browse*.
3. Select the file on your PC and click *Open*.
4. Click *Backup Config and Upgrade*.
The system will reboot.

Resolved issues

The following issues have been fixed in FortiProxy 7.0.8. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
550701	Fix signal 6 backtrace is not generated for forticron daemon.
553604	CMDB lock issues.
713286	WAD crash at signal 11 on video filter related process.
742483	Fix random system events log with the message "msg=UrlBwl-black gzopen fail".
764770	Fix external resource download DNS bottleneck.
784326	Flaws in auth_key_encrypt.
784785	Unsupported ZTNA logic prevents proper ZTNA matching. Fix default CA certificate changed to blank after refresh.
789153	A profile with higher privileges than the user's own profile can be set.
793651, 798873, 814265, 831805, 834375, 836260, 849803, 851521, 856031, 858061, 859390, 859420, 862510, 863235, 863428, 866115, 867418	Fix GUI issues.
809141	Client hung when FortiAI error encountered with fortiai-error-action as log-only in antivirus profile.
810989	GUI permission override should only apply to GET by default.
813957	Fix ZTNA Tag description message format problem.
815457	HTTPS request is blocked if the destination interfaces in proxy policy and outgoing interface to web-proxy forward-server are different.
817770	Change default source port range to 1024-65001.
818371	Fix WAD process crash at wad_http_req_add_option of wad_http_engine.
818869	FTP traffic does not get redirected to WAD.
819887	GCP does not process multipart MIME data.
823078, 855664, 855853	WAD user-info process randomly consumes 100% CPU of one core.

Bug ID	Description
826254	Fix disk formatting issue after changing usage.
830450	WAD crashes on wad_p2s_ciphers_filter.
832515, 834314	Crash due to connection aborting.
834378	Guest users able to access webpage past the provisioned time allotted for them.
834420, 834729	Extra, unnecessary X-authentication-User/Group field on ICAP header and default ICAP header change
835129	ICAP client header parser cannot handle piggy or sibling flag HTTP headers.
835745	WAD algorithm process crashes when the source interface of a firewall policy is set to virtual-wan-link.
838913	Fix malformed request false positive issue.
839201	ICAP client timeout issue .
840549	Fix WAD unable to recognize RSSO user.
841506	Fix WAD memory spike on ISO file when stream-scan enabled.
841571	Disable VXLAN configuration in transparent mode.
841828	Traffic is not authorized when AD username is provided without a domain.
842197	Fix CIFS under ZTNA does not respect the port setting, and should not start while no scan is needed.
844990	Enforce IP bans on existing traffic.
845570	Fix for re-compiling wad_ebpf_dispatcher.c.
845577	WAD crashes at fts_client_hello_cancel.
845818	Remove the 10 second count down for falling back URL when SSO IdP is not configured.
846630	ZTNA status removed from GUI.
846857	Fix TLS 1.1 certificate-inspection bypass failure.
846870	Allow management access to local interfaces with IPsec and SSLVPN.
847484	Read-only administrators able to sniff other administrators' cookies.
848190	Fix incorrect allocated RAM shown in the GUI.
849320	Improve performance when changing the configuration.
849549	In deep-inspection, FortiProxy cannot forward ALPN extension in clienthello to server.
849714	Keep the default value, <code>disable</code> , for the <code>pac-data</code> field in <code>config user krb-keytab</code> when upgrading.
850440	Fix WAD algorithm crash when loading ia-profile.
850558	Webcache is unable to retrieve large cached objects.

Bug ID	Description
850841	Arbitrary read/write vulnerability in custom language.
851188	Fix string comparing issue when the host name in the request is capitalized.
852192	Fix kernel memory corruption.
852416	Trusted host IP table rules are only generated for super administrators.
852416	Non-super administrators are skipped when checking for trusthost wildcards.
853406	Fix SSL certificate full check for external resources when the hostname is the IP address.
853406	Fix SSL certificate full check for external resources when the hostname is the IP address.
853473	WAD crash at sig 11 in wad_log_vs.c with ZTNA logging related tests .
854176	Patch for arbitrary file deletion in log reports.
854229	Path traversal vulnerability allowed VDOM escaping.
854432	Fix TCP port validate return false for proxy SSL redirect.
854833	Fix incorrect license information on secondary FortiProxy.
855009	Fix error when adding different URL lists to different URL match rules.
855603	Fix pipeline requests failure when enabling IPS/APPCTL.
855816	Clone DSCP marker to the other end of transparent proxies.
855838	High latency and CPU usage when deleting webcache entries matching a simple-string URL pattern.
856008	Fix netlink socket not closed when setting up IP pools.
856235	High memory usage by WAD worker in object ssl.fts.str.fstr_buffer_bytes.
857284	Remove NAF.
857338	Fix WAD traffic stats client add stats crash.
857507	WAD crash at wad_http_fwd_msg_body.
857691	Remove duplicate address-ip-rating in the profile-protocol-options.
858488	Fix wa_cs daemon crashes when the request data length is larger than the range data length.
858647	Fix race condition resulting in interfaces being stuck up or down with HA enabled .
860381	Fix webcache prefetch build crashes when an entry has an empty configuration.
860461	Fix wrong web proxy profile assignment issue.
860495	Decode DLP log URL field to utf-8 .
860520	Improve table build speed when policy uses a zone as the source and/or destination address.
860620	Potential memory leak on DoT traffic.
861151	SSL Mirror does not work.

Bug ID	Description
862001	Prevent password ciphertext exposure in logs.
862846	Configuration Backup and Restore in CLI is not working as expected. The <code>honor-df</code> , <code>send-pmtu-icmp</code> , and <code>ipv6-allow-anycast-probe</code> commands are removed from <code>config system global</code> .
863593, 864115	Both incoming and outgoing utm-filefilter logs are generated when email is passthrough with outgoing direction via MAPI.
864621	SSH public key changes after every reboot
865318	ICAP server with antivirus crash when sending HTTPS to eicar.com .
868043	WAD worker crashes when performing basic local authentication.

Common vulnerabilities and exposures

FortiProxy 7.0.8 is no longer vulnerable to the following CVE references. Visit <https://fortiguard.com/psirt> for more information.

Bug ID	CVE reference
854181	CVE-2022-42475
866003	CVE-2022-45861
845849	CVE-2022-41330
862003	CVE-2022-43947
854176	CVE-2022-42474
847484	CVE-2022-41327



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.