



FortiProxy Release Notes

Version 1.2.10

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

FORTICAST

<http://forticast.fortinet.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FORTINET PRIVACY POLICY

<https://www.fortinet.com/corporate/about-us/privacy.html>

FEEDBACK

Email: techdocs@fortinet.com



January 29, 2021

FortiProxy 1.2.10 Release Notes

Revision 1

TABLE OF CONTENTS

Change log	4
Introduction	5
Security modules	5
Caching and WAN optimization	6
What's new	7
Supported models	7
Product integration and support	8
Web browser support	8
Fortinet product support	8
Software upgrade path	8
Virtualization environment support	8
New deployment of the FortiProxy VM	8
Upgrading the FortiProxy VM	9
Downgrading the FortiProxy VM	9
Resolved issues	10
Common vulnerabilities and exposures	11
Known issues	12

Change log

Date	Change Description
January 29, 2021	Initial release for FortiProxy 1.2.10

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

What's new

This release contains the following new features and enhancements:

- You can now enable or disable the proxy captive portal on an interface in the New Interface page and the Edit Interface page.
- There is a new CLI command to enable the FortiProxy ICAP client to support the HTTP CONNECT method:

```
config icap profile
  edit "<name | default>"
    set methods {delete get head options post put trace connect other}
  next
end
```

Supported models

The following models are supported on FortiProxy 1.2.10, build 0316:

FortiProxy	• FPX-2000E • FPX-4000E • FPX-400E
FortiProxy VM	• FPX-AZURE • FPX-HY • FPX-KVM • FPX-KVM-AWS • FPX-KVM-GCP • FPX-KVM-OPC • FPX-VMWARE

Product integration and support

Web browser support

The following web browsers are supported by FortiProxy 1.2.10:

- Microsoft Internet Explorer version 11
- Mozilla Firefox version 61
- Google Chrome version 67

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

Fortinet product support

- FortiOS 5.x and 6.0 to support the WCCP content server
- FortiOS 5.6.3 and 6.0 to support the web cache collaboration storage cluster
- FortiAnalyzer 5.6.5
- FortiSandbox and FortiCloud FortiSandbox, 2.5.1

Software upgrade path

FortiProxy supports upgrading directly from 1.0.x or 1.1.x to 1.2.x.

Virtualization environment support

NOTE: Fortinet recommends running the FortiProxy VM with 2G+ memory because the AI-based Image Analyzer uses more memory comparing to the previous version.

Linux KVM	• RHEL 7.1/Ubuntu 12.04 and later • CentOS 6.4 (qemu 0.12.1) and later
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, and 6.5
Microsoft	• Hyper-V Server 2008 R2, 2012, 2012R2, and 2016

New deployment of the FortiProxy VM

The minimum memory size for the FortiProxy VM for 1.2.10 or later is 2G. You must have at least 2G of memory to allocate to the FortiProxy VM from the VM host.

Upgrading the FortiProxy VM

If you are upgrading from FortiProxy 1.1.2 or earlier, including FortiProxy 1.0 to FortiProxy 1.2.10 or later, use the following procedure:

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 2G 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

If you are downgrading from FortiProxy 1.2.10 or later to FortiProxy 1.1.2 or earlier, use the following procedure:

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 2G 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.

Resolved issues

The following issue has been fixed in FortiProxy 1.2.10. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
590299	The WAN-optimization daemon (WAD) process crashed with a signal 11 (segmentation fault) when a user was using the ICAP CLI commands.
591954	The WAD process crashed with a signal 11 (segmentation fault) when a user configured an illegal server address.
635346	Enabling the return-to-sender feature causes the FortiProxy unit in HA mode to reboot, which causes disk corruption.
670917	After creating an IPsec tunnel or changing the configuration for the first time, the IPsec tunnel cannot be brought up.
671803	SSH does not match the policy when there is a policy with a proxy address or wildcard FQDN address in the policy list before it.
677158	The DLP file name pattern cannot be added in the GUI.
682754	The cmdbsvr crashes when a user configures high availability (HA) mode in the GUI.
682909	DNS resolution only works with the HA management interface but not with the default route.
684464	The captive portal port is not listening on the FQDN address.
684510	The SSL-VPN configuration cannot be saved in the GUI.
684541	After running for three days, the FortiProxy VM4 stops transmitting traffic.
685558	Using the <code>set pac-data enable</code> command (under <code>config user krb-keytab</code>) causes a "matched cached grp:NA" result.
685883	A programming tool discovered an invalid read.
686142	When the ICAP client on the F5 device uses FortiProxy 1.2 as the ICAP server, the HTTP request is not processed.
686514	The FPX 2000E CPU processing rises to 100% use during a load test.
687697	The WAD process crashed with a signal 11 when matching an authentication rule with a category proxy address as the destination address.
688578	The HTTPS request fails after the FortiProxy unit receives an ICAP 200 OK response from the ICAP server when the web proxy policy, forward server, and ICAP are configured on the FortiProxy unit.

Bug ID	Description
690191	The HTTPS daemon crashes when an authenticated user sends a malformed request.
691086	The web cache database daemon (wacs) crashes every 5 minutes.
691752	The FortiProxy unit does not answer the ICAP OPTIONS request.

Common vulnerabilities and exposures

FortiProxy 1.2.10 is no longer vulnerable to the following CVEs:

- CWE-79
- CWE-80
- CWE-121
- CWE-284
- CWE-312
- CWE-352
- CWE-534
- CWE-601
- CWE-922
- CVE-2018-13384
- CVE-2019-15706

Visit <https://fortiguard.com/psirt> for more information.

Known issues

FortiProxy 1.2.10 includes the known issues listed in this section. For inquiries about a particular issue, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
491027, 681567	Filtering the YouTube channel does not work. Workaround: The fix is scheduled for a future release.
490951	The <code>append explicit-outgoing-ip</code> command is not validated.
499787	The FortiGuard firmware versions are not listed on the <i>System > Firmware</i> page.



FORTINET®



Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.