



FortiProxy Release Notes

Version 1.2.7

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



September 9, 2020

FortiProxy 1.2.7 Release Notes

Revision 3

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 |
| Known issues | 12 |

Change log

| Date | Change Description |
|-------------------|---|
| September 4, 2020 | Initial release for FortiProxy 1.2.7 |
| September 8, 2020 | Updated the “What’s new” and “Virtualization environment support” sections. |
| September 9, 2020 | Updated the “Supported models” and “Virtualization environment support” sections. |

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 masquerade feature in the New Forwarding Server and Edit Forwarding Server forms.
- You can now specify more than one authentication method in the authentication scheme in the GUI.
- You can now create and view authentication rules and authentication schemes on the *Policy & Objects > Authentication Rules* page.

Supported models

The following models are supported on FortiProxy 1.2.7, build 0298:

| | |
|---------------|---|
| 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-AWS• FPX-KVM-GCP• FPX-KVM-OPC• FPX-VMWARE |

Product integration and support

Web browser support

The following web browsers are supported by FortiProxy 1.2.7:

- 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 | <ul style="list-style-type: none">• RHEL 7.1/Ubuntu 12.04 and later• CentOS 6.4 (qemu 0.12.1) and later |
| VMware | <ul style="list-style-type: none">• 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 | <ul style="list-style-type: none">• Hyper-V Server 2008 R2, 2012, 2012R2, and 2016 |

New deployment of the FortiProxy VM

The minimum memory size for the FortiProxy VM for 1.2.7 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 1.2.7 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 1.2.7 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 1.2.7. For inquiries about a particular bug, please contact [Customer Service & Support](#).

| Bug ID | Description |
|--------|---|
| 615202 | The WAD daemon crashes when the client tries to authenticate using the NTLM guest user. |
| 621787 | The WAN-optimization daemon (WAD) application crashed during SSL Proxy antivirus HTTPS throughput tests |
| 634890 | The FortiProxy GUI and CLI should not list options that are not supported. |
| 638922 | Traffic should correctly match the explicit proxy policy when it contains an ISDB object. |
| 639086 | After authentication was enabled for a few days, expired WAD users are still listed, instead of being automatically deleted. |
| 641428 | After upgrading from FortiProxy 1.2.4 to 1.2.5, the WAD crashes. |
| 643476 | After upgrading from FortiProxy 1.2.3 to 1.2.6, FortiProxy cluster members become unresponsive, and there are kernel crashes. |
| 646121 | Only the HA primary device can be reached using the FortiProxy dedicated management interface, and the secondary unit is sending traffic through the HA primary link instead of the dedicated management interface. |
| 647697 | When <i>Management Interface Reservation</i> is enabled on the <i>System > HA</i> page, the Interface field is missing. |
| 649138 | The FortiProxy VM freezes when using ESXi. |
| 651090 | The <code>diagnose iptables refresh</code> command fails. |
| 651613 | When FortiAnalyzer is the log source, logs do not appear in FortiView for the "Now" time period. |
| 651720 | After upgrading to FortiProxy 1.2.5, traffic is not matching the correct policy, and the WAD keeps crashing. |
| 652701 | After rebooting a FortiProxy cluster, the aggregate interface stops working. |
| 653083 | TLS websites cannot be accessed when deep inspection and authentication are enabled in FortiProxy 1.2.3. |
| 653380 | Traffic does not match the firewall policy when the destination address is an FQDN. |
| 654106 | When using the Edit LDAP Server form to make changes, the port is reset to 636. |

| Bug ID | Description |
|-------------------|---|
| 654166 | When trying to access the administrator Web UI, there is a NET::ERR_CERT_INVALID message. |
| 654279 | Selecting "now" for the time range for FortiView results in no activity details. |
| 654684, 661695 | The WAD process crashes continuously. |
| 655754 | There was high memory usage on a FortiProxy VM, and the crash log reports the dnspoxy daemon is being killed frequently. |
| 656239 | After traffic stops, the dashboard shows that the proxy/UTM sessions are at 100 percent. |
| 656259 | Deleting the aggregate interface in the CLI does not delete the aggregate interface in the kernel. |
| 656372 | When traffic matches a policy with the action set to deny, the logs show the action as accept. |
| 656436 | User names should not be case sensitive. |
| 656559 | The WAD process crashes. |
| 657027 | Two different user names with the same initial characters both match the same firewall policy, even though only one user name should match. |
| 660748 | The GUI and CLI should not refer to "master" or "slave." |
| 661242 | When deep inspection (SSL/SSH inspection) is enabled in the transparent policy, HTTPS traffic is not scanned. |
| 661447 | The WAD process crashes when the single sign-on (SSO) guest user is matched. |

Known issues

FortiProxy 1.2.7 includes the known issues listed in this section. For inquiries about a particular issue, please contact [Fortinet Customer Service & Support](#).

| Bug ID | Description |
|--------|--|
| 491027 | Filtering the YouTube channel does not work. |
| 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© 2020 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.