FortiProxy Release Notes

Version 2.0.6

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 17, 2021

FortiProxy 2.0.6 Release Notes

Revision 1

TABLE OF CONTENTS

Change log

Date	Change Description
September 17, 2021	Initial release for FortiProxy 2.0.6

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.

X-Scan-Progress-Interval header supported in the FortiProxy ICAP client

You can now use the CLI to specify that the X-Scan-Progress-Interval header is used and specify the scan interval value:

```
config icap profile
   edit <profile_name>
      set response {enable | disable}
      set response-server <name_of_ICAP_server>
      set response-path <HTTP_response_processing_service>
      set extension-feature scan-progress
      set scan-progress-interval <5-30 seconds>
   next
end
```

FortiProxy VM license file includes certificates and keys

The FortiProxy VM uses a BIOS certificate to provide high trustworthiness.

Do not use the new VM license file for FortiProxy 2.0.5 or earlier.

Do not downgrade the FortiProxy 2.0.6 VM because the new VM license file cannot be used by earlier versions of FortiProxy.

Timeout configuration available for the FortiProxy ICAP client

You can now use the CLI to configure the number of seconds that the ICAP client waits for a response from the ICAP server:

```
config icap profile
   edit <profile_name>
      set timeout <30-3600 seconds>
   next
end
```

ICAP server logs include user and group information

The ICAP server logs now include the user and group information.

Specifying a list of URLs to forward to a forwarding server

You can now create a list of URLs to forward to a specific forwarding server.

To create the list of URLs:

```
config web-proxy url-list
   edit <name_of_URL_list>
      set comment <description_of_URL_list>
      config entries
         edit <list_ID>
```

```
            set status {enable | disable}
            set url <URL>
            set type {simple | wildcard}
         next
      end
   next
end
```

For example:

```
config web-proxy url-list
   edit "url-list-t"
      config entries
         edit 1
            set url "google.com"
         next
         edit 2
            set url "server11*.ftnt.net/*virus"
            set type wildcard
         next
         edit 3
            set url "url*.test"
            set type wildcard
         next
      end
   next
end
```

URLs can be a maximum of 512 characters. You can use * for wildcard-type URLs.

To forward the URLs in the URL list to the specified forwarding server:

```
config web-proxy url-match
   edit <name>
      set type list
      set url-list <URL_list_name>
      set forward-server <forward_server_name>
   next
end
```

For example:

```
config web-proxy url-match
   edit "test_list"
      set type list
      set url-list "url-list-t"
      set forward-server "fwd-127"
   next
   edit "tt"
      set url-pattern "/upload"
   next
   edit "*"
      set type wildcard
      set url-pattern "*"
      set forward-server "fwd-125"
   next
   edit "match-exempt-t"
      set type wildcard
      set url-pattern "*ftnt.net"
   next
end
```

Setting the maximum object size for caching

You can now configure the maximum size for objects to be cached with the `set max-cache-object-size` command. The default size is 0 KB; the maximum object size is 3.8 GB.

For example:

```
config web-proxy profile
   edit "1"
      set max-cache-object-size 1992192
      set header-client-ip pass
      set header-via-request pass
      set header-via-response pass
      set header-x-forwarded-for pass
      set header-front-end-https pass
      set header-x-authenticated-user pass
      set header-x-authenticated-groups pass
      set strip-encoding disable
      set log-header-change disable
   next
end
```

ICAP load balancing

You can now configure ICAP load balancing in the GUI.

Supported models

The following models are supported on FortiProxy 2.0.6, build 0060:

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 • FPX-XEN

Product integration and support

Web browser support

The following web browsers are supported by FortiProxy 2.0.6:

- 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, 1.1.x, or 1.2.x to 2.0.6.

Fortinet Single Sign-On (FSSO) support

- 5.0 build 0295 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

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

HyperV	• Hyper-V Server 2008 R2, 2012, 2012R2, 2016, and 2019
Linux KVM	• RHEL 7.1/Ubuntu 12.04 and later • CentOS 6.4 (qemu 0.12.1) and later
Xen hypervisor	• OpenXen 4.13 hypervisor and later • Citrix Hypervisor 7 and later
VMware	• ESXi versions 6.0, 6.5, 6.7, and 7.0

New deployment of the FortiProxy VM

The minimum memory size for the FortiProxy VM for 2.0.6 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 2.0.6 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

Do not downgrade the FortiProxy 2.0.6 VM because the new VM license file cannot be used by earlier versions of FortiProxy.

If you are downgrading from FortiProxy 2.0.5 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 issues have been fixed in FortiProxy 2.0.6. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
506798	When WCCP is configured in a Config-Sync cluster, all members are synchronized with the same WCCP configuration.
520176	The WAN-optimization daemon (WAD) crashed multiple times and reported in the log that “signal 6 (Aborted) received.”
667721	WAD crashes when an address has been corrupted.
669018	Links that currently go to http://www.fortiguard.com should go to https://www.fortiguard.com instead.
676403	The default replacement message is displayed in Google Chrome instead of the configured replacement message images.
717484	Using the a traffic shaper and a shaping policy works for transparent proxy but not for explicit proxy.
717527	When FortiProxy is configured to use FortiAI, the proxy process crashes.
721039	Microsoft Teams and Whereby video streaming is being disconnected briefly and randomly for proxy explicit users.
723089	The application control profile cannot be edited when it is used in an explicit-proxy policy with the proxy category blocked.
725628	The WAD process is using too much memory, causing the device to enter conserve mode.
725731	WAD crashes if ssl-ssh-profile and profile-protocol-options are not configured in a policy running in FortiProxy 2.0.
726691	LACP should be supported between a FortiProxy unit and a Cisco Catalyst 9500.
728866	The PAC File Data field should not be empty in the CLI or GUI.
729194	UTM-related attributes need to be hidden in the GUI for the isolate policy.
729608	FortiProxy 2.0.5 has continuous but random WAD crashes with signal 11 received.
729614	The ICAP 204 response code is not supported.
730760	When UTM is not enabled in a policy, the FortiProxy unit should not count UTM session.
731540	The FortiProxy unit is not blocking websites with invalid certificates.

Bug ID	Description
733104	The transparent policy does not match the proxy address URL pattern.
735694	The loading of web pages is slow when the ICAP profile, web-forwarding profile, and SSL deep inspection are enabled in a policy.
737127	After generating a certificate signing request (CSR) in the FortiProxy GUI, the CSR certificate cannot be downloaded from the GUI.
738651	When FortiProxy policies are being edited sequentially, the memory usage of one of the HA cluster members increases and will not decrease until the FortiProxy unit is restarted.
739463	The output of the `diagnose test app wad 803` command is incomplete.
739798	Explicit firewall policies are lost when upgrading from build 0049 to build 0054.
741660	When the LDAP server is slow to respond, the connection times out and disconnects.
741900	The CPU usage increases until traffic stops when using transparent proxy, deep inspection, and application control.
742156	When a second `web-proxy explicit` configuration is added to an HA cluster, the cluster members become unsynchronized.
742197	The user cannot block the team viewer from remote access.
742474	When application control is configured, an incorrect warning is displayed and the link for the policy number does not work.
742662	In the GUI, links for application control categories and application control signatures do not work.
742839	Kerberos authentication fails when using a transparent policy.
743927	When UTM is enabled, ICAP server sessions are not included in the total number of licensed sessions.
745401	The FortiProxy unit does not add the configured field to the HTTP response header.
745509	UTM features are not working when there is SSH-over-HTTP traffic for the explicit web policy or SSH policy.
745782	The description of the `set addr-type fqdn` command is not correct in the FortiProxy CLI.
745855	ICAP load balancing causes a crash when using an explicit policy or transparent policy with an ICP profile and ICAP remote server group.
746977	The forward server uses an invalid IP address with an explicit web proxy policy.
747362	The *System* > *Certificate* page is not loading.

Common vulnerabilities and exposures

FortiProxy 2.0.6 is no longer vulnerable to the following CVEs:

- CWE-284

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

Known issues

FortiProxy 2.0.6 includes the known issues listed in this section. For inquires about a particular issue, please contact Fortinet Customer Service & Support.

Bug ID	Description
491027, 681567	Filtering the YouTube channel does not work. **Workaround:**Upgrade to FortiProxy 7.0.0.
490951	The `append explicit-outgoing-ip` command is not validated.
499787	The FortiGuard firmware versions are not listed on the *System* > *Firmware* page.