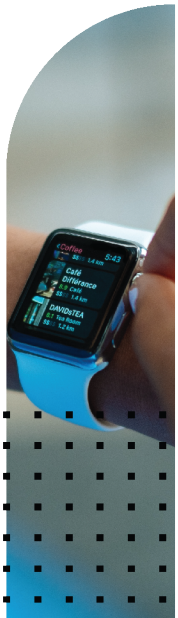
Release Notes

FortiProxy 7.0.7



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

October 06, 2022
FortiProxy 7.0.7 Release Notes
45-707-846239-20221006

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-10-06	Initial release.

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 7.0.7, build 0110:

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

What's new

The following sections describe new features and enhancements:

Certificate validation for external resources

Certification is verified before fetching data from the external connectors that have SSL enabled.

To configure certificate verification:

```
config system external-resource
    edit "test"
        set server-identity-check {none | basic | full}
    next
end
```

`none`	No certificate verification (default).
`basic`	Check server certificate only.
`full`	Check server certificate and domain match server certificate.

Detect HTTPS in HTTP request

In an explicit web proxy, you can enable detecting SSL in the HTTP request line. When enabled, HTTP get/post requests sent to the FortiProxy will be passed instead of blocked.

To enable detecting SSL in the HTTP request line:

```
config web-proxy explicit-proxy
    edit "web-proxy"
        set status enable
        set interface "any"
        set http-incoming-port 8080
        set detect-https-in-http-request enable
    next
end
```

Auto-script password encryption

When configuring an automatic script, the new `password` attribute can be set. It will replace the password in the script when the script uses the `%%PASSWD%%` tag. When the configuration is downloaded or viewed in the CLI, the password is encrypted.

To configure then view an automatic script with a password:

1. Configure the automatic script:

```
config system auto-script
    edit "autobackup"
        set interval 60
        set repeat 0
        set start auto
        set script "execute backup config sftp 10.0.0.1 admin <b>%%PASSWD%%</b>
/home/user/proxy.config"
        set password 1234567890
    next
end
```

2. View the script:

```
# show system auto-script
config system auto-script
    edit "autobackup"
        set interval 60
        set repeat 0
        set start auto
        set script "execute backup config sftp 10.0.0.1 admin <b>%%PASSWD%%</b>
/home/user/proxy.config"
        set password ENC
Dz6s2235D+GkaND0zptzOUQH2ptR2M4v5VEP3v3/NvB2So/yBat/tUGEavP71pUdn38HKFXUPeZ802C8+exOjDat
MSo5YVebkkDnL01J4EtGzcrJuQKl97+ekrHXMzkyxA/yxtkKURuVBlhKRqBFn03DleaR7vcbj4HnLLIY73WRI018
NDfPgOS3non02OqfFv9Oew==
    next
end
```

The password is encrypted.

Remove quotes from external resource

When a URL is entered for an external resource, the leading and tailing quote strings are automatically removed from the URL. This includes the following characters: `&quot;`, `&apos;`, `&39;`, `&34;`, and `&96;`.

For example: "`https://docs.fortinet.com`" will be changed to: `https://docs.fortinet.com`.

Learn the destination from the SNI

Learning the destination from the SNI in a client hello can be enabled in an explicit web proxy. This allows WAD to handle proxy traffic that sends a TLS client hello directly, without sending an HTTP connect.

```
config web-proxy explicit-proxy
    edit "web-proxy"
        set status enable
        set interface "any"
        set http-incoming-port 8080
        set https-incoming-port 8443
        set learn-dst-from-sni enable
    next
end
```

Product integration and support

Web browser support

The following web browsers are supported by FortiProxy 7.0.7:

- 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.

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.

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
Openstack	• Ussuri

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 7.0.7 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 7.0.7.

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 7.0.7. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
604172	Webfilter cannot communicate with FortiGuard through proxy.
669251	Removed the OPTIONS method from the HTTP 405 “Method Not Allowed” response.
734909	ICAP error messages use the correct replacement messages rather than the existing, hard-coded 502 response.
763951, 832173	Speed up policy learning by using a delta config.
780182	WAD crash at wad_http_fwd_msg_body.
805703	Select the next forward server by default for the least connection algorithm.
817056	The inactivity timer is 30 minutes, and renewed any time it is given out by the pool for ICAP traffic, or when any traffic flows through the connection in either direction.
821242	ICAP bypassing yields to web traffic corrupted upon ICAP_server failure to response.
822015	Add support for ACI dynamic address in WAD.
824259	Too many redirections error with session based authenthication and web-auth-cookie.
825349	WAD crashed at wad_http_req_finished with signal 11.
830907	WAD can crash when building a proxy policy if an address group has no member.
831428	Corrupted forward-server caused WAD crash.
833174, 835163, 835638, 836141, 836142, 837089, 840519, 840525	Fix GUI issues.
833372	WAD crash due to long line reponse from server and SSH filter vulnerability.
834684	Configuring SNMP wiped kernel SNAT settings.
835180	Fix traffic shaping on newly configured VLAN interface.
835623, 837608	Embed base64 string images instead of URLs for WAD blocking page.
835739	Website will not reply if `Connection` uses the wrong letter case
836286	ICAP infection headers could not show the correct file name.
836464	The mac address type removed from firewall addresses, as it is not supported.
836723	HTTP/HTTPS requests that match a policy with an L7 address are not forward to the isolate server.

Bug ID	Description
836915	DNS queries fail with dnsfilter applied.
837192	Fix virtual MAC setup in HA mode.
837598	cloudinitd crash when deploying FortiProxy on AWS.
837729	Bypass interface kernel driver reset after rebooting.
838354	FTP over TLS does not work through explicit proxy when ftp-over-http is enabled.
838888	Fix HA sequential upgrade.
838910	WAD crashes on attaching history traffic stats to NULL tcp_port from session.
840189	Rare case in HA configuration caused kernel panic.
840680	Fix SSLVPN connection issue.
841086	FortiProxy does not have any cache hits after memory usage passes 60%.
842338, 842826	Fix VPN widgets in the GUI.
842469	ZTNA access stuck when going through TCP-fwd towards HTTPS with a deep-inspection profile.
842835	Prefetch tasks added multiple times, leading to high resource usage .
842908	Fix synchronizing captive-portal IP/FQDN in config-sync mode .
842925	Image Analyzer (IA) profile not applied after being changed.
842926	Failure to perform SNAT when creating an FTP PASSIVE mode data channel.
844823, 846862	WAD can enter a dead loop when rebuilding explicit policy, and can timeout waiting for the DNS proxy daemon to reload a DNS profile.
845323	SNMP not responding when dedicated-to management is enable on an interface.
845849	XSS vulnerability on login check and SAML IdP route handler.
846114	DNS can cause a dead loop in the WAD main schedule loop.
847582	HLS vcache crash.
847944	Fix issues with the function of administrator trusted host settings.
848398	Access-Control-x headers not added to the owner tables and marked as invalid.
848493	User information daemon memory use increases steadily if the LDAP server is unreachable.
848534	Fix System Events is not accessible.
848592	Daemons can fail to start if the prefetch WGET processes consume a lot of resources.

Common vulnerabilities and exposures

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

Bug ID	CVE references
846234	FortiProxy 7.0.7 is no longer vulnerable to the following CVE Reference: • CVE-2022-40684
847070	FortiProxy7.0.7 is no longer vulnerable to the following CVE Reference: • CVE-2022-40684

www.fortinet.com