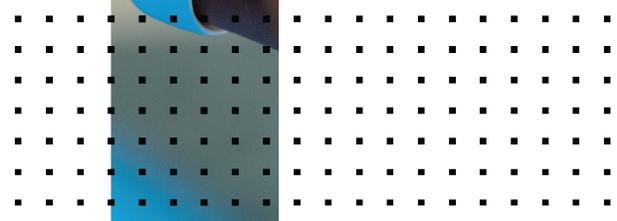


# Release Notes

## FortiProxy 7.0.21



**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](mailto:techdoc@fortinet.com)



July 9, 2025

FortiProxy 7.0.21 Release Notes

45-7021-1167690-20250709

# TABLE OF CONTENTS

<b>Change log</b> .....	<b>4</b>
<b>Introduction</b> .....	<b>5</b>
Security modules .....	5
Caching and WAN optimization .....	6
<b>What's new</b> .....	<b>7</b>
New FortiGuard web filter categories for AI and Cryptocurrency .....	7
CLI changes .....	7
<b>Product integration and support</b> .....	<b>8</b>
<b>Deployment information</b> .....	<b>10</b>
Downloading the firmware file .....	10
Deploying a new FortiProxy appliance .....	10
Deploying a new FortiProxy VM .....	10
Upgrading the FortiProxy .....	11
Downgrading the FortiProxy .....	12
<b>Resolved issues</b> .....	<b>14</b>
Common vulnerabilities and exposures .....	14
<b>Known issues</b> .....	<b>15</b>

# Change log

Date	Change Description
2025-06-11	Initial release.
2025-07-09	Added <a href="#">CVE-2024-52965</a> to Resolved issues on page 14.

# 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:

<b>Web filtering</b>	<p>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.</p> <p>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.</p>
<b>DNS filtering</b>	<p>Similar to the FortiGuard web filtering. DNS filtering allows, blocks, or monitors access to web content according to FortiGuard categories.</p>
<b>Email filtering</b>	<p>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.</p>
<b>CIFS filtering</b>	<p>CIFS UTM scanning, which includes antivirus file scanning and DLP file filtering.</p>
<b>Application control</b>	<p>Application control technologies detect and take action against network traffic based on the application that generated the traffic.</p>
<b>Data Loss Prevention (DLP)</b>	<p>The FortiProxy DLP system allows you to prevent sensitive data from leaving your network.</p>
<b>Antivirus</b>	<p>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).</p>
<b>SSL/SSH inspection (MITM)</b>	<p>SSL/SSH inspection helps to unlock encrypted sessions, see into encrypted packets, find threats, and block them.</p>

<b>Intrusion Prevention System (IPS)</b>	IPS technology protects your network from cybercriminal attacks by actively seeking and blocking external threats before they can reach potentially vulnerable network devices.
<b>Content Analysis</b>	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

The following sections describe new features, enhancements, and changes in FortiProxy 7.0.21:

- [New FortiGuard web filter categories for AI and Cryptocurrency on page 7](#)
- [CLI changes on page 7](#)

## New FortiGuard web filter categories for AI and Cryptocurrency

FortiProxy 7.0.21 adds the following new FortiGuard [web filter](#) categories:

- **Artificial intelligence technology** (category 100): sites that offer solutions, insights, and resources related to artificial intelligence (AI).
- **Cryptocurrency** (category 101): sites that specialize in digital or virtual currencies that are secured by cryptography and operate on decentralized networks.

**To configure a web filter profile to block the AI and cryptocurrency categories in the GUI:**

1. Go to *Security Profiles > Web Filter* and click *Create New*.
2. Enter a name for the web filter profile.
3. In the category table, locate the *General Interest - Business* section. Select the *Artificial Intelligence Technology* and *Cryptocurrency* categories, and set the *Action* to *Block*.
4. Configure the remaining settings as needed.
5. Click *OK*.

## CLI changes

FortiProxy 7.0.21 includes the following new commands:

FortiProxy 7.0.21 does not include any new features, enhancements, or changes.

- `diagnose sys filesystem tree`—Use this new command to list the top files/folders tree.
- `diagnose sys filesystem hash`—Use this new command to generate hash for files within the filesystem. See [Computing file hashes](#) in the Administration Guide for more details.
- `diagnose system filesystem last-modified-files`—Use this new command to list the last modified files.
- `diagnose sys session list-verbose`—Use this new command to list sessions in verbose detail.
- `diagnose sys mpstat`—Use this new command to diagnose mpstat.

# Product integration and support

The following table lists product integration and support information for FortiProxy 7.0.21 build 0217:

Type	Product and version
<b>FortiProxy appliance</b>	<ul style="list-style-type: none"><li>• FPX-400E</li><li>• FPX-2000E</li><li>• FPX-4000E</li><li>• FPX-400G</li><li>• FPX-2000G</li><li>• FPX-4000G</li></ul>
<b>FortiProxy VM</b>	<ul style="list-style-type: none"><li>• FPX-AZURE</li><li>• FPX-HY</li><li>• FPX-KVM</li><li>• FPX-KVM-ALI</li><li>• FPX-KVM-AWS</li><li>• FPX-KVM-GCP</li><li>• FPX-KVM-OPC</li><li>• FPX-VMWARE</li><li>• FPX-XEN</li></ul>
<b>Fortinet products</b>	<ul style="list-style-type: none"><li>• FortiOS 6.x and 7.0 to support the WCCP content server</li><li>• FortiOS 6.0 and 7.0 to support the web cache collaboration storage cluster</li><li>• FortiManager - See the <a href="#">FortiManager Release Notes</a>.</li><li>• FortiAnalyzer - See the <a href="#">FortiAnalyzer Release Notes</a>.</li><li>• FortiSandbox and FortiCloud FortiSandbox- See the <a href="#">FortiSandbox Release Notes</a> and <a href="#">FortiSandbox Cloud Release Notes</a>.</li><li>• Fortisolator 2.2 and later - See the <a href="#">Fortisolator Release Notes</a>.</li></ul>
<b>Fortinet Single Sign-On (FSSO)</b>	5.0 build 0301 and later (needed for FSSO agent support OU in group filters) <ul style="list-style-type: none"><li>• Windows Server 2019 Standard</li><li>• Windows Server 2019 Datacenter</li><li>• Windows Server 2019 Core</li><li>• Windows Server 2016 Datacenter</li><li>• Windows Server 2016 Standard</li><li>• Windows Server 2016 Core</li><li>• Windows Server 2012 Standard</li><li>• Windows Server 2012 R2 Standard</li><li>• Windows Server 2012 Core</li><li>• Windows Server 2008 64-bit (requires Microsoft SHA2 support)</li></ul>

Type	Product and version												
	package) <ul style="list-style-type: none"> <li>Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package)</li> <li>Windows Server 2008 Core (requires Microsoft SHA2 support package)</li> <li>Novell eDirectory 8.8</li> </ul>												
<b>Web browsers</b>	<ul style="list-style-type: none"> <li>Microsoft Edge</li> <li>Mozilla Firefox version 87</li> <li>Google Chrome version 89</li> </ul> <hr/> <div style="display: flex; align-items: center;">  <p>Other web browsers may work correctly, but Fortinet does not support them.</p> </div> <hr/>												
<b>Virtualization environments</b>	<p>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.</p> <table border="0" style="width: 100%;"> <tr> <td style="width: 30%;"><b>Hyper-V</b></td> <td> <ul style="list-style-type: none"> <li>Hyper-V Server 2008 R2, 2012, 2012R2, 2016, 2019, and 2022</li> </ul> </td> </tr> <tr> <td><b>Linux KVM</b></td> <td> <ul style="list-style-type: none"> <li>RHEL 7.1/Ubuntu 12.04 and later</li> <li>CentOS 6.4 (qemu 0.12.1) and later</li> </ul> </td> </tr> <tr> <td><b>Xen hypervisor</b></td> <td> <ul style="list-style-type: none"> <li>OpenXen 4.13 hypervisor and later</li> <li>Citrix Hypervisor 7 and later</li> </ul> </td> </tr> <tr> <td><b>VMware</b></td> <td> <ul style="list-style-type: none"> <li>ESXi versions 6.5, 6.7, and 7.0</li> </ul> </td> </tr> <tr> <td><b>Openstack</b></td> <td> <ul style="list-style-type: none"> <li>Ussuri</li> </ul> </td> </tr> <tr> <td><b>Nutanix</b></td> <td> <ul style="list-style-type: none"> <li>AHV</li> </ul> </td> </tr> </table>	<b>Hyper-V</b>	<ul style="list-style-type: none"> <li>Hyper-V Server 2008 R2, 2012, 2012R2, 2016, 2019, and 2022</li> </ul>	<b>Linux KVM</b>	<ul style="list-style-type: none"> <li>RHEL 7.1/Ubuntu 12.04 and later</li> <li>CentOS 6.4 (qemu 0.12.1) and later</li> </ul>	<b>Xen hypervisor</b>	<ul style="list-style-type: none"> <li>OpenXen 4.13 hypervisor and later</li> <li>Citrix Hypervisor 7 and later</li> </ul>	<b>VMware</b>	<ul style="list-style-type: none"> <li>ESXi versions 6.5, 6.7, and 7.0</li> </ul>	<b>Openstack</b>	<ul style="list-style-type: none"> <li>Ussuri</li> </ul>	<b>Nutanix</b>	<ul style="list-style-type: none"> <li>AHV</li> </ul>
<b>Hyper-V</b>	<ul style="list-style-type: none"> <li>Hyper-V Server 2008 R2, 2012, 2012R2, 2016, 2019, and 2022</li> </ul>												
<b>Linux KVM</b>	<ul style="list-style-type: none"> <li>RHEL 7.1/Ubuntu 12.04 and later</li> <li>CentOS 6.4 (qemu 0.12.1) and later</li> </ul>												
<b>Xen hypervisor</b>	<ul style="list-style-type: none"> <li>OpenXen 4.13 hypervisor and later</li> <li>Citrix Hypervisor 7 and later</li> </ul>												
<b>VMware</b>	<ul style="list-style-type: none"> <li>ESXi versions 6.5, 6.7, and 7.0</li> </ul>												
<b>Openstack</b>	<ul style="list-style-type: none"> <li>Ussuri</li> </ul>												
<b>Nutanix</b>	<ul style="list-style-type: none"> <li>AHV</li> </ul>												
<b>Cloud platforms</b>	<ul style="list-style-type: none"> <li>AWS (Amazon Web Services)</li> <li>Microsoft Azure</li> <li>GCP (Google Cloud Platform)</li> <li>OCI (Oracle Cloud Infrastructure)</li> <li>Alibaba Cloud</li> </ul>												

# Deployment information

You can deploy the FortiProxy on a FortiProxy unit or VM. You can also upgrade or downgrade an existing FortiProxy deployment. Refer to [Product integration and support on page 8](#) for a list of supported FortiProxy units and VM platforms.

## Downloading the firmware file

1. Go to <https://support.fortinet.com>.
2. Click *Login* and log in to the Fortinet Support website.
3. From the *Support > Downloads* menu, select *Firmware Download*.
4. In the *Select Product* dropdown menu, select *FortiProxy*.
5. On the *Download* tab, navigate to the FortiProxy firmware file for your FortiProxy model or VM platform in the *Image Folders/Files* section. .out files are for upgrade or downgrade. .zip and .gz files are for new deployments.
6. Click *HTTPS* to download the firmware that meets your needs.

## Deploying a new FortiProxy appliance

Refer to the [FortiProxy QuickStart Guide](#) for detailed instructions of deploying a FortiProxy appliance. Refer to [Product integration and support on page 8](#) for a list of supported FortiProxy units.

## Deploying a new FortiProxy VM

Refer to the [FortiProxy Public Cloud](#) or [FortiProxy Private Cloud](#) deployment guides for more information about how to deploy the FortiProxy VM on different public and private cloud platforms. Refer to [Product integration and support on page 8](#) for a list of supported VM platforms.



On ESXi 7.0 or later, you cannot deploy FortiProxy 7.0.21 directly. As a workaround, deploy FortiProxy 7.0.17 first and then upgrade to 7.0.21.

---

# Upgrading the FortiProxy

---



- For FortiProxy appliances, you can upgrade from 7.0.x or 2.0.x to 7.0.21 directly.
  - For FortiProxy VMs, you can upgrade from 7.0.x or 2.0.6 or later to 7.0.21 directly. However, to upgrade from 2.0.5 or earlier to 7.0.21, additional backup and configuration is required as FortiProxy 2.0.6 introduced a new FortiProxy VM license file that cannot be used by earlier versions of the FortiProxy VM.
  - If Security Fabric is enabled, all FortiProxy units must be upgraded to the same version. For example, if Security Fabric is enabled in FortiProxy 7.0.21, all FortiProxy devices in the Security Fabric must run FortiProxy 7.0.21. Otherwise, some devices may get stale or disconnected from the root, resulting in issues with fabric logging and address synchronization.
- 

## **To upgrade FortiProxy appliances from 7.0.x or 2.0.x to 7.0.21, or to upgrade FortiProxy VMs from 7.0.x or 2.0.6 or later to 7.0.21:**

1. In the GUI, go to *System > Firmware*.
2. Click *Browse* in the *File Upload* tab.
3. Select the file on your PC and click *Open*.
4. Click *Confirm and Backup Config*.
5. Click *Continue*.  
The configuration file is automatically saved and the system will reboot.
6. Click *Reset All Dashboards* in the GUI to avoid any issues with FortiView.

## **To upgrade a FortiProxy 2.0.5 VM to 7.0.21:**

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.
7. Click *Reset All Dashboards* in the GUI to avoid any issues with FortiView.

# Downgrading the FortiProxy

---



- For FortiProxy appliances, you can downgrade from 7.0.21 to 7.0.x or 2.0.x directly.
  - For FortiProxy VMs, you can downgrade from 7.0.21 to 7.0.x or 2.0.6 or later directly. However, to downgrade from 7.0.21 to 2.0.5 or earlier, additional backup and configuration is required as FortiProxy 2.0.6 introduced a new FortiProxy VM license file that cannot be used by earlier versions of the FortiProxy VM.
  - If Security Fabric is enabled, all FortiProxy units must be downgraded to the same version. For example, if Security Fabric is enabled in FortiProxy 7.0.21, all FortiProxy devices in the Security Fabric must run FortiProxy 7.0.21. Otherwise, some devices may get stale or disconnected from the root, resulting in issues with fabric logging and address synchronization.
- 

## **To downgrade FortiProxy appliances from 7.0.21 to 7.0.x or 2.0.x, or to downgrade FortiProxy VMs from 7.0.21 to 2.0.6 or later:**

1. In the GUI, go to *System > Firmware*.
2. Click *Browse* in the *File Upload* tab.
3. Select the file on your PC and click *Open*.
4. Click *Confirm and Backup Config*.
5. Click *Continue*.  
The configuration file is automatically saved and the system will reboot.
6. Click *Reset All Dashboards* in the GUI to avoid any issues with FortiView.

## **To downgrade a FortiProxy 7.0.21 VM 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.
7. Click *Reset All Dashboards* in the GUI to avoid any issues with FortiView.



---

Downgrading FortiProxy7.0.21 to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
  - interface IP/management IP
  - static route table
  - DNS settings
  - admin user account
  - session helpers
  - system access profiles
-

# Resolved issues

The following issues have been fixed in FortiProxy 7.0.21. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
1074460	Crash due to buffer overflow issues related to corrupted traffic log files.
1117526	list_entry should be typesafe.
1117013	wad_hash_cache timeout issue.
1112600	The wad_ftp_session_task_start does not initiate while establishing the data connection.
924740	Improve WAD trace log precision of process-id-by-src filter.
1103476	License leak.
1126862	Traffic is passed by transparent deny policy when log-http-transaction is enabled.
1126749	Duplicate session ID in traffic logs across different connections.
1126862	Traffic is passed by transparent deny policy when log-http-transaction is enabled.
1018780, 1023127	WAD crash on wad_http_avscan_comfort.
1144421	ICAP crash.
1092529, 1095093, 1102694	"utmref" and "utmaction" fields are missing in forward traffic log and long-tcp sessions are missing in http-transaction traffic log.
1102796	Passive proxy member send LDAP requests to the LDAP servers.

## Common vulnerabilities and exposures

FortiProxy 7.0.21 is no longer vulnerable to the following CVE reference. Visit <https://fortiguard.com/psirt> for more information.

Bug ID	CVE reference
1121042	CVE-2024-52965

# Known issues

FortiProxy 7.0.21 includes the known issues listed in this section. For inquiries about a particular issue, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
996825	scanunit application inside FortiProxy firmware crash.
979076	WAD worker health status is not alive after moving users to FortiProxy.
1017952	FPX-2000E automatically powers off.



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2025 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 Chief Legal Officer, 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.