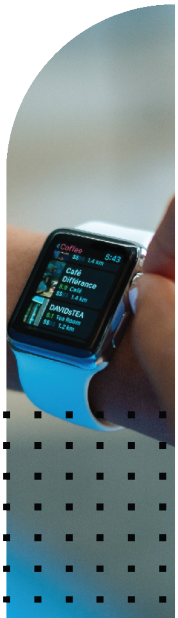
Release Notes

FortiProxy 7.0.1



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

February 28, 2023
FortiProxy 7.0.1 Release Notes
45-701-745519-20230228

TABLE OF CONTENTS

Change log

Date	Change Description
October 28, 2021	Initial release for FortiProxy 7.0.1
February 14, 2021	Updated the Product integration and support on page 22 section.
March 22, 2022	Added bug 764817.
February 1, 2023	Added the *Export policy list to CSV and JSON formats* feature to What's new on page 8.
February 28, 2023	Added the *Disable weak ciphers in the HTTPS protocol* feature to What's new on page 8.

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 7.0.1, build 0047:

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 the new features and enhancements:

Proxy settings

This section includes new features related to proxy settings:

LDAP user cache

You can now use the following CLI commands to control the LDAP user cache for explicit proxy and transparent proxy users:

```
config web-proxy global
   set ldap-user-cache {enable | disable}
end
```

New masquerade command for the isolator server

You can now use the CLI to control whether the web proxy uses the device address to connect to the proxy server for the isolator server. By default, this feature is enabled.

```
config web-proxy isolator-server
   edit <server_name>
      set masquerade {enable | disable}
   next
```

```
end
```

Web proxy header expanded

The `set content` command (under the `config web-proxy profile` command) was previously limited to 256 characters. The header content can now be as long as 512 characters.

Increased size of the cache object

Use the following CLI commands to set the maximum size of the cacheable object:

```
config webcache settings
   set max-object-size <1-2147483>
end
```

Disabling IP-based URL rating

You can now disable IP-based URL rating for SSL-exemption and proxy-address objects. By default, IP-based URL rating is enabled. Use the following CLI commands:

```
config firewall ssl-ssh-profile
   edit <name>
      set ssl-exemption-ip-rating {enable | disable}
   next
end

config web-proxy global
   set address-ip-rating {enable | disable}
end
```

HTTP domain fronting blocking

You can now block HTTP domain fronting with the following commands:

```
config firewall profile-protocol-options
   edit <name>
      config http
         set domain-fronting disable
      end
   next
end
```

Use the body of the HTTP POST method to control web access

You can now control access to web services based on login information. Use the new `set post-arg` command:

```
config firewall proxy-address
   edit <name>
      set post-arg {enable | disable}
   next
```

```
end
```

For example:

```
config firewall proxy-address
   edit "xaddr-url-user"
      set host "all"
      set path "/t"
      set query "username=.*&"
      set post-arg enable
   next
end
```

Policy and objects

This section includes new features related to policies and objects:

- New pass-through policy on page 10
- Export policy list to CSV and JSON formats on page 10

New pass-through policy

There is a new option to define a policy as a pass-through policy. When traffic matches a pass-through policy, the firewall continues to the next policy. After FortiProxy tries to match all policies, it will set the last matched pass-through policy as the matched policy. By default, the pass-through option is disabled.

To enable a pass-through policy in the GUI:

1. Go to *Policy & Objects* > *Policy*.
2. Create a new policy or edit an existing policy.
3. Enable *Enable Policy Matching Pass Through*.
4. Configure the remaining settings as needed.
5. Click *OK*.

To control a pass-through policy in the CLI:

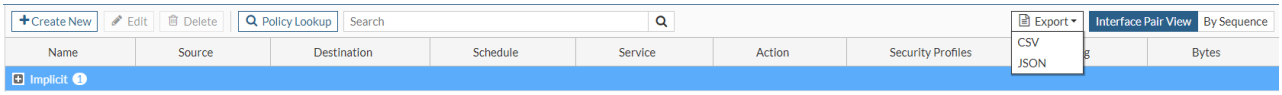
```
config firewall policy
   edit <policy_ID>
      set pass-through {enable | disable}
   next
end
```

Export policy list to CSV and JSON formats

In the *Policy* list page, users can export the current view to CSV and JSON formats.

To export the policy list to a CSV or JSON file:

1. Go to *Policy & Objects* > *Policy*.
2. In the toolbar above the list, click *Export*.
3. Select *CSV* or *JSON*.



The file is automatically downloaded.

Security profiles

This section includes new features related to security profiles:

- Client authentication with client certificate for Original Content Server on page 11

Client authentication with client certificate for Original Content Server

Clients can now use a client certificate for authentication on behalf of the Original Content Server. Use the following CLI commands:

```
config firewall ssl-ssh-profile
   edit <profile_name>
      config ssl-client-certificate
         set status <*do-not-offer | keyring-list | ca-sign>
         set keyring-list <keyring_list_used_to_find_client_certificate>
         set caname <CA_certficate_used_to_sign_client_certificate>
      end
   next
end

config firewall ssl keyring-list
   edit <keyring_list_used_to_find_client_certificate>
      set uuid <UUID>
   next
end
```

Content analyses

This section includes new features related to content analyses:

- X-Scan-Progress-Interval header supported in the FortiProxy ICAP client on page 12
- Timeout configuration available for the FortiProxy ICAP client on page 12
- ICAP load balancing available in the GUI on page 12
- ICAP scanning supported for FTP on page 12

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 in the FortiProxy ICAP client and specify the scan progress 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 (default is 10)>
   next
end
```

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 (default is 30)>
   next
end
```

ICAP load balancing available in the GUI

You can now configure ICAP load balancing in the GUI:

1. Go to *Content Analyses* > *ICAP Load Balancing*.
2. Click *Create New*.
3. Enter a name for the ICAP load-balancing configuration.
4. Select the load-balancing method:
   - *Weighted*—Balance the traffic load to ICAP servers based on the assigned weights.
   - *Least Session*—Send new sessions to the ICAP server with the lowest session count.
   - *Active Passive*—Send new sessions to the active ICAP server with the highest weight.
5. To create a server list for load balancing, click *Create New*.
6. Select or create a remote server.
7. Enter a weight for the remote server.
8. Click *OK* to save the remote server entry.
9. Click *OK* save your ICAP load-balancing configuration.

ICAP scanning supported for FTP

NOTE: The ICAP profile must be configured in the CLI before it is used in the GUI.

To forward transferred files with FTP to the ICAP server for further processing using the GUI:

1. Configure the ICAP remote server:
   a. Go to *Content Analyses* > *ICAP Remote Server*.
   b. Create a new configuration for an ICAP server or edit an existing configuration.
   c. Click *OK*.
2. Create an ICAP profile that references the ICAP remote server:
   a. Go to *Content Analyses* > *ICAP Profile*.
   b. Click *Create New*.
   c. In the *FTP* section, click *FTP*.
   d. From the *Server* dropdown, select the ICAP server to use for the file transfer.
   e. Click *Error* or *Bypass* for the action to take if the ICAP server cannot be contacted when processing a file transfer.
   f. In the *Path* field, enter the path of the file transfer processing service.
   g. Configure the remaining settings as needed.
   h. Click *OK* to save the ICAP profile.
3. Create an explicit FTP proxy policy that uses the ICAP policy:
   a. Go to *Policy & Objects* > *Policy*.
   b. Click *Create New*.
   c. Select *FTP* in the *Type* dropdown.
   d. Enable *ICAP* and select the ICAP profile that references the ICAP remote server.
   e. Enable *Enable this policy*.
   f. Configure the remaining settings as needed.
   g. Click *OK*.

To forward transferred files with FTP to the ICAP server for further processing using the CLI:

1. Configure the ICAP remote server:

```
config icap server
   edit <name_of_ICAP_server>
      set ip-version {4 | 6}
      set ip-address <IPv4_address_of_ICAP_server>
      set ip6-address <IPv6_address_of_ICAP_server>
      set port <ICAP_server_port>
      set max-connections <1-65535>
      set secure {enable | disable}
   next
end
```

   For example:

```
config icap remote-server
   edit "icap1"
      set ip-address 172.18.20.43
   next
end
```

2. Create an ICAP profile that references the ICAP remote server:

```
config icap profile
   edit {<ICAP_profile_name>new | default}
      set replacemsg-group <replacement_message_group>
      set request {disable | enable}
      set response {disable | enable}
      set file-transfer ftp
      set file-transfer-server <remote_server_name>
      set file-transfer-failure {error | bypass}
      set file-transfer-path <string>
      set streaming-content-bypass {disable | enable}
      set allow-204-response {disable | enable}
      set preview {disable | enable}
      set methods {delete | get | head | options | post | put | trace | other}
      set icap-block-log {disable | enable}
      set chunk-encap {disable | enable}
      set extension-feature scan-progress
      set timeout {30-3600}
      set preview-data-length <0-4096>
      set request-server <ICAP_server>
      set response-server <ICAP_server>]
      set request-failure {error | bypass}
      set response-failure {error | bypass}
      set request-path <string>
      set response-path <string>
      set response-req-hdr {disable | enable}
      set respmod-default-action {forward | bypass}
   next
end
```

For example:

```
config icap profile
   edit "new1"
      set request enable
      set response enable
      set file-transfer ftp
      set request-server "icap1"
      set response-server "icap1"
      set file-transfer-server "icap1"
      set request-path "test"
      set response-path "test"
      set file-transfer-path "test"
   next
end
```

3. Create an explicit FTP proxy policy that uses the ICAP policy:

```
config firewall policy
   edit <policy_ID>
      set type explicit-ftp
      set status enable
      set name <policy_name>
      set uuid <UUID>
      set dstintf <interface_name>
```

```
      set srcaddr <address_name>
      set dstaddr <address_name>
      set srcaddr6 <address_name>
      set dstaddr6 <address_name>
      set action {accept | deny}
      set schedule {<schedule_name} | always | none}
      set ztna-ems-tag <address_name>
      set ztna-tags-match-logic {or | and}
      set internet-service {enable | disable}
      set pass-through {enable | disable}
      set internet-service-name <Internet_service_name>
      set logtraffic {all | utm | disable}
      set logtraffic-start {enable | disable}
      set groups <group_name>
      set users <user_name>
      set comments <string>
      set replacemsg-override-group <string>
      set srcaddr-negate {enable | disable}
      set dstaddr-negate {enable | disable}
      set max-session-per-user <0-4294967295>
      set profile-group <profile_group_name>
      set profile-protocol-options <profile_name>
      set ssl-ssh-profile <profile_name>
   next
end
```

For example:

```
config firewall policy
   edit 3
      set type explicit-ftp
      set uuid 9b932658-3214-51ec-f906-09ea9dd7e6dd
      set dstintf "port1"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set utm-status enable
      set logtraffic all
      set ssl-ssh-profile "certificate-inspection"
      set av-profile "fai"
      set icap-profile "new1"
   next
end
```

WAN optimization

This section includes new features related to WAN optimization:

- TLS 1.3 supported for WAN optimization on page 16
- Tracking WAD memory on page 16

TLS 1.3 supported for WAN optimization

WAN optimization now supports TLS 1.3.

Tracking WAD memory

Use the following command to check how much memory has been allocated for the WAN-optimization daemon (WAD):

```
diagnose wad memory track [<mem-id>]
```

User and authentication

This section includes new features related to users and authentication:

- SAML features improved on page 16

SAML features improved

The following SAML features have been improved:

- You can now use external browser SAML authentication.
- Clock-skew tolerance is now supported.
- Error messages have been improved.

System

This section includes new features related to system:

- Disable weak ciphers in the HTTPS protocol on page 16

Disable weak ciphers in the HTTPS protocol

Administrators can select what ciphers to use for TLS 1.3 in administrative HTTPS connections and what ciphers to ban for TLS 1.2 and below.

To select the ciphers to use for TLS 1.3 and ban for TLS 1.2 and lower:

```
config system global
    set admin-https-ssl-ciphersuites {TLS-AES-128-GCM-SHA256 TLS-AES-256-GCM-SHA384 TLS-
CHACHA20-POLY1305-SHA256 TLS-AES-128-CCM-SHA256 TLS-AES-128-CCM-8-SHA256}
    set admin-https-ssl-banned-ciphers {RSA DHE ECDHE DSS ECDSA AES AESGCM CAMELLIA 3DES
SHA1 SHA256 SHA384 STATIC CHACHA20 ARIA AESCCM}
end
```

`admin-https-ssl-ciphersuites {TLS-AES-128-GCM-SHA256 TLS-AES-256-GCM-SHA384 TLS-CHACHA20-POLY1305-SHA256 TLS-AES-128-CCM-SHA256 TLS-AES-128-CCM-8-SHA256}`	Select one or more TLS 1.3 cipher suites to enable. Ciphers in TLS 1.2 and below are not affected. At least one must be enabled. To disable all, remove TLS1.3 from `admin-https-ssl-versions`. TLS-AES-128-CCM-SHA256 and TLS-AES-128-CCM-8-SHA256 are only available when strong-crypto is disabled.
`admin-https-ssl-banned-ciphers {RSA DHE ECDHE DSS ECDSA AES AESGCM CAMELLIA 3DES SHA1 SHA256 SHA384 STATIC CHACHA20 ARIA AESCCM}`	Select one or more cipher technologies that cannot be used in GUI HTTPS negotiations. Only applies to TLS 1.2 and below.

To test connecting from a PC using one of the cipher suites:

1. Disable strong-crypto and select all five cipher suites:

```
config system global
    set admin-https-redirect disable
    set admin-https-ssl-ciphersuites TLS-AES-128-GCM-SHA256 TLS-AES-256-GCM-SHA384 TLS-
CHACHA20-POLY1305-SHA256 TLS-AES-128-CCM-SHA256 TLS-AES-128-CCM-8-SHA256
    set strong-crypto disable
end
```

2. Connect from a PC using TLS_AES_128_CCM_SHA256:

```
~$ openssl s_client -connect 172.16.200.101:443 -tls1_3 -ciphersuites TLS_AES_128_CCM_
SHA256
CONNECTED(00000005)
Can't use SSL_get_servername
depth=0 O = Fortinet Ltd., CN = FortiGate
...
---
New, TLSv1.3, Cipher is TLS_AES_128_CCM_SHA256
Server public key is 2048 bit
....
```

3. Enable strong-crypto:

```
config system global
    set strong-crypto enable
end
TLS cipher suite 'TLS-AES-128-CCM-SHA256' can not be supported so removed.
TLS cipher suite 'TLS-AES-128-CCM-8-SHA256' can not be supported so removed.
```

4. Try to connect from the PC again using TLS_AES_128_CCM_SHA256:

```
~$ openssl s_client -connect 172.16.200.101:443 -tls1_3 -ciphersuites TLS_AES_128_CCM_
SHA256
CONNECTED(00000005)
139694547268800:error:14094410:SSL routines:ssl3_read_bytes:sslv3 alert handshake
failure:../ssl/record/rec_layer_s3.c:1528:SSL alert number 40
---
no peer certificate available
```

```
 ---
No client certificate CA names sent
---
SSL handshake has read 7 bytes and written 211 bytes
Verification: OK
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
....
```

The connection fails because TLS_AES_128_CCM_SHA256 is not supported when strong-ctrypo is enabled.

Security Fabric

This section includes new features related to the Security Fabric:

- FortiAI integration on page 18
- Support new external resource type for URL lists on page 19

FortiAI integration

FortiAI can now be added to the Security Fabric.

To add FortiAI to the Security Fabric in the GUI:

1. Go to *System* > *Settings*.
2. In the FortiAI section, enable *Status*.
3. Click *Apply*.
4. Go to *Security Fabric* > *Fabric Connectors*.
5. Double-click *Security Fabric Setup* to enable the Security Fabric and configure the interface to allow other Security Fabric devices to join.
6. Click *OK*.
7. In FortiAI, configure the device to join the Security Fabric:
   a. Go to *Security Fabric* > *Fabric Connectors* and double-click the connector card.
   b. Enable *Enable Security Fabric*.
   c. Enter the FortiProxy root IP address and the FortiAI IP address.
   d. Click *OK*.
8. Authorize FortiAI in FortiProxy:
   a. Go to *Security Fabric* > *Fabric Connectors*.
   b. In the topology tree in the rightmost pane, click the highlighted FortiAI serial number and click *Authorize*.
      The authorized device appears in the topology tree. Hover over the device name to view the tooltip.
      The *Security Fabric* widget on the dashboard also updates when the FortiAI is authorized.
   c. Click *OK*.

To add a Fabric Device widget for FortiAI:

1. Go to *Dashboard* > *Status* and click *Add Widget*.
2. In the *Security Fabric* section, click the + beside *Fabric Device*.
3. For *Device*, select the FortiAI device.
4. Select a *Widget name* and *Visualization type* from the dropdowns.
5. Click *Add Widget* and click *Close*.
   The *Fabric Device* widget is displayed in the dashboard.

To add FortiAI to the Security Fabric in the CLI:

1. Configure the interface to allow other Security Fabric devices to join:

```
config system interface
       edit "port1"
               ...
               set allowaccess ping https ssh http fgfm fabric
               ...
       next
end
```

2. Configure the Security Fabric:

```
config system csf
       set status enable
       set group-name "FortiAI"
       set group-password ********
       config trusted-list
               edit "FAIVMSTM21000000"
                       set authorization-type certificate
                       set certificate "****************"
               next
       end
end
```

3. In FortiAI, configure the device to join the Security Fabric:

```
config system csf
       set status enable
       set upstream-ip 172.18.64.122
       set managment-ip 172.18.64.114
end
```

4. In FortiProxy, enable FortiAI:

```
config system fortiai
       set status enable
end
```

Support new external resource type for URL lists

You can now create and use lists of external URLs. The URL list is a plain text file with one URL on each line.

To specify external URL lists in the GUI:

1. Go to *Security Fabric* > *External Connectors*.
2. Click *Create New*.
3. Under *Threat Feeds*, click *URL List*.
4. In the *Name* field, enter a name for the URL list.
5. In the *URL of external resource* field, enter the Uniform Resource Identifier (URI) of the URL list.
6. If you enable *HTTP basic authentication*, enter the user name and password.
7. In the *Refresh Rate* field, enter the number of minutes before the URL list is refreshed.
8. In the *Comments* field, enter a description of the URL list.
9. Make certain that *Status* is enabled.
10. Click *OK*.

To specify external URL lists in the CLI:

1. Specify the URL list as an external resource:

```
config system external-resource
   edit <external_resource_name>
      set type url
      set resource <URI_of_URL_list>
      set username <user_name_for_HTTP_basic_authentication>
      set password <password_for_HTTP_basic_authentication>
      set refresh-rate <1-43200 minutes>
      set comments <string>
      set status enable
   next
end
```

For example:

```
config system external-resource
   edit "user-list1"
      set type url
      set resource "http://172.16.80.129/byte1.txt"
   next
end
```

2. Create a web proxy address that uses the URL list:

```
config firewall proxy-address
   edit "<address_name>
      set type url-list
      set host {all | none | <string>}
      set url-list <external_URL_list>
   next
end
```

For example:

```
config firewall proxy-address
   edit "xaddr-list"
      set type url-list
```

```
        set host all
        set url-list "user-list1"
    next
end
```

Log and report

This section includes new features related to logs and reports:

- ICAP group and user reported in logs on page 21
- Web filter log contains more information about HTTP traffic on page 21

ICAP group and user reported in logs

The ICAP server now reports the group name and user name in the data leak prevention (DLP), antivirus, web filter, and scan unit error logs when an ICAP request meets the blocking criteria.

Web filter log contains more information about HTTP traffic

The web filter log now contains the following information:

- How long it takes to scan the HTTP request
- Client request host header
- Client request host inside of the request line
- Server response code

Product integration and support

Web browser support

The following web browsers are supported by FortiProxy 7.0.1:

- Microsoft Edge 89
- 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
- FortiAnalyzer 7.0.2
- FortiSandbox and FortiCloud FortiSandbox, 3.2.1 and 4.0
- FortiAI-VM-KVM 1.5.2

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

NOTE: Fortinet recommends running the FortiProxy VM with at least 2 GB of 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 release 7.0.0 or later is 2 GB. You must have at least 2 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.

If you are upgrading your FortiProxy VM to 2.0.5 or from 2.0.6 and higher, 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 2 GB of memory allocated 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 your FortiProxy VM from 7.0.0 or later to 2.0.5 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 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

You can upgrade FortiProxy appliances directly from 2.0.x to 7.0.1.

If you are upgrading a FortiProxy appliance, use the following procedure:

1. Back up the configuration from the GUI or CLI.
2. Go to *System* > *Firmware* and select *Browse*.
3. Select the file on your PC and select *Open*.
4. Select *Backup Config and Upgrade*.
   Your system will reboot.

Resolved issues

The following issues have been fixed in FortiProxy 7.0.1. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
561711	The TLS 1.3 performance needs to be improved.
677234	Web pages included in the external list (FortiGuard Category Threat Feed) should be blocked when users try to access them through https://translate.google.com.
706786	The WAN-optimization daemon (WAD) crashes at wad_cert_picker_get_X509_issuer.
725373	When the SSL Negotiation log is enabled, there should be an SSL UTM log available.
726691	LACP does not work between a FortiProxy unit and a Cisco Catalyst 9500.
728641	The abbreviated handshake fails when a fatal illegal parameter is received.
733104	The transparent proxy policy is not matching the proxy address object URL pattern.
733135	Validating the SSL certificate should not time out.
734840	The web filter blocks websites in proxy mode because validating the SSL certificate fails.
737285	There is a certificate error when using the proxy policy and the website being accessed has an incomplete certificate chain.
738331	When an address group is configured with an excluded address object on a proxy policy, the excluded members should be excluded in the address group.
739091	The WAD crashes multiple times at wad_tunnel_msg_ssl_handshake_send with signal 11 (Segmentation error).
739610	When the `ssh-policy-redirect` option is disabled, SSH-over-HTTP traffic still tries to match the SSH policy.
739923	The WAD causes memory usage to increase from 50% to 75% after one day.
740222	The `set filter-by file-type-and-size` command is missing from under the `config dlp sensor` command.
741866	An overrun problem occurred in WAN optimization when using explicit proxy.
741867	Negative returns occurred in WAN optimization when using explicit proxy.
741869	Memory is corrupted when a transparent proxy policy is used with web caching, IPS, web filter, and antivirus scanning.
742108	The WAD crashed with signal 11 (Segmentation error) when the video filter was being used.
742141	When external resources reply with HTTP 301, 302, 307, or 308, the response codes are not accepted.

Bug ID	Description
742178	After an interface is configured as the HA management interface, all input rules (such as Telnet, HTTP, SSH, and ping) are removed from the IP tables, and the interface cannot be accessed.
742241	When a security profile (such as antivirus, Application Control, or IPS) is active, traffic with the content encoding type of `amz-1.0` does not work through the proxy.
742437	When a ZTNA rule is created in the GUI, it does not include the destination address or source interface.
742620	The WAD crashes at fts_ssl_port_open_with_keys with signal 11 when there is HTTPS traffic with WAN optimization and SSL offload enabled.
743168	The WAD crashes continuously with signal 11 (segmentation fault).
743259	The GUI is not displaying the number of hits or active sessions.
743379	After upgrading to FortiProxy 7.0, the maximum number of proxy address objects is reduced from 24,576 to 8,192.
743602	An “empty reply from server” error results when there is HTTPS traffic with WAN optimization.
743656	If there is an authentication scheme configured but no authentication rules, the WAD user receives a 403 Forbidden error.
743750	There were many WAD scan unit crashes.
743894	When downloading 10 million samples with WAN optimization enabled, the download will stop halfway through.
743927	When UTM is enabled, ICAP server sessions are not included in the total number of licensed sessions.
743975	The URL column should be available to add to the HTTP Transaction logs.
743976	When two FortiProxy units and in a Config -Sync cluster, both FortiProxy units have the same hdisk, and one of the FortiProxy units keeps shutting down.
744312	The video filter prevents office.com to not load after the user logs in.
744430	The pencil button cannot used to edit fields in a policy.
744433	FortiProxy logs are not listing user names.
744563	The AND/OR logic is missing from the user group.
744569	The GUI should allow both the local user database and the remote user database to be selected at the same time.
744571	The GUI does not have the same matching criteria for authentication rules as the CLI.
744636	External files should be synchronized between blades.
744855	After upgrading to FortiProxy 7.0.0, some commands under `config firewall profile-group` are missing.
744857	After upgrading to FortiProxy 7.0.0, the link status for the aggregate interface is down in the GUI.
745115	The GUI does not display FSSO users on the User Monitor.

Bug ID	Description
745212	The WAD crashes a with signal 11 when the video filter is being used.
745566	When CP9 is enabled on a FortiProxy 400E, HTTPS traffic fails.
745572	The WAD crashes at conn_pool_connection_error with signal 11 when the ICAP server cannot be reached.
746005	The GUI needs to allow the HTTP incoming port to be configured.
746007	Policies do not show the configured IP pool name in the GUI.
746009	When the IP pool is configured, the setting is not applied on outbound traffic.
746435	Configuring the ICAP server should not cause a crash.
746506	Stream-based antivirus scanning is not working for large files when using an ICAP local server.
746569	The options for the SSL/SSH inspection profile are not displayed correctly in the GUI.
746977	The forward server uses an invalid IP address with an explicit web proxy policy.
747250	The URL and IP external threat feeds are truncated.
747434	The ICAP server crashes when traffic is sent to the ICAP client.
748573	The `set transparent` command (under `config firewall policy`) is not working .
748764	The GUI does not let users configure an external malware block list.
748788	*Security Profiles* > *Web Application Firewall* is available in the GUI, but it is not used.
749432	After an FPX-4000E was rebooted, it started to automatically format the disk.
749625	The `datadrv2` file is missing from `FPX_VMWARE-v700-build0029-FORTINET.out.ovf.zip`.
750600	During the antivirus scanning of an HTTP request, a segmentation fault occurs.
750641	When an SSH request is sent to an ICAP client with IPv6, a crash occurs.
750650	The WAD crashes when the HTTPS request tries to match the URL address and `fast-policy-match` is disabled.
750893	The WAD crashes multiple times at wad_http_clt_read_hdr with HTTP transparent proxy traffic.
751188	The remote server group field is missing from the ICAP profile in the GUI.
751303	The WAD crashes every few seconds.
751693	The WAD crashes with signal 6 when using web filtering with WISP enabled.
751811	The WAD informer is not learning the global system correctly.
751972	When using the proxy policy and the SDN connector dynamic address, traffic is blocked.
752125	The FPX-2000E, FPX-4000E, and FPX-400E models should support the unicast gateway for an HA Config-Sync cluster.
752354	The ICAP client crashes when sending FTP-over-HTTP traffic.

Bug ID	Description
752410	The HTTP request does not match the policy when the proxy address is used with a specific (non-ALL) service.
752416	When the server setting is mismatched, the WAD sessions are cleared after a while.
753138	The SSH policy does not find matches when the address is set to a specific value.
753208	When IPS and application control are configured on a transparent proxy or SSH tunnel policy
753335	There are some issues with the ZTNA menu and pages in the GUI.
753422	When configuring a WAN-optimization policy, users should be able to set the values for the `set ssl-ssh-profile` and `set webcache-https` commands.
754499	Using the GUI or the `diagnose wad user clear` command to unauthenticate a user does not clear the user node in the kernel.
754572	When web caching is enabled, the image analyzer does not replace the blocked image.
754762	When an antivirus profile is enabled in a WAN-optimization proxy policy, the EICAR test file should be blocked when it is sent with HTTPS.
754969	The explicit FTP proxy policy selects a random destination port when the FTP client initiates the FTP session without using the default port.
755365	Firefox does not show the authentication pop-up message when explicit proxy is used.
755401	The WAD crashes multiple times at wad_http_body_move with signal 6.
755698	When the policy is not matched, user notes should not be cleared by the HTTPS request.
755706	The user monitor in the GUI is not displaying correct information.
755751	The kernel user should be refreshed.
755753	The WAD crashes at wad_diag_session_close.
755861	When upgrading FortiProxy, the units for the `proxy-auth-timeout` value need to be converted.
755878	The display is incorrect when configuring authentication rules in the GUI.
756364	The *Policy & Objects* > *Policy* table is not displaying users or user groups in the *Source Address* column.
756370	Using *Insert Empty Policy* > *Above* or *Insert Empty Policy* > *Below* creates a transparent policy instead of an explicit policy.
756402	The WAD crashes when there are multiple session-based user notes in WAD and IP-based authentication is triggered.
756421	In the GUI, the SSL Certificate SSL profile will not save without the server certificate.
756716	The WAD crashes at wad_hauth_start_usernum_report_task; afterward, the policy list in the worker is empty

Common vulnerabilities and exposures

FortiProxy 7.0.1 is no longer vulnerable to the following CVEs:

- CWE-190
- CWE-788
- CVE-2021-41024

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

Known issues

FortiProxy 7.0.1 includes the known issues listed in this section. For inquires about a particular issue, please contact Fortinet Customer Service & Support.

Bug ID	Description
490951	The `append explicit-outgoing-ip` command is not validated.
499787	The FortiGuard firmware versions are not listed on the *System* > *Firmware* page.
764817	You cannot import the Kerberos keytab file unless it has been encoded with base64. **Workaround:** Encode the Kerberos keytab file with base64 before importing it into FortiProxy.

Change log

Date	Change Description
October 28, 2021	Initial release for FortiProxy 7.0.1
February 14, 2021	Updated the Product integration and support on page 22 section.
March 22, 2022	Added bug 764817.
February 1, 2023	Added the *Export policy list to CSV and JSON formats* feature to What's new on page 8.
February 28, 2023	Added the *Disable weak ciphers in the HTTPS protocol* feature to What's new on page 8.

www.fortinet.com