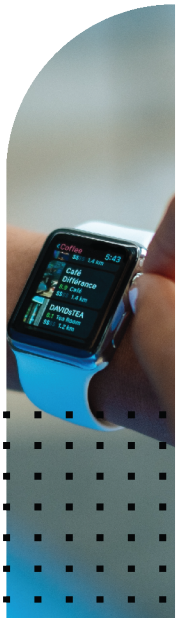
Release Notes

FortiProxy 7.0.0



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

March 22, 2022
FortiProxy 7.0.0 Release Notes
45-700-717317-20220322

TABLE OF CONTENTS

Change log **5**
Introduction **6**
Security modules 6
Caching and WAN optimization 7
Supported models 7
What's new **8**
General usability enhancements 8
GUI-based global search 8
SSL-VPN and IPsec monitor improvements 8
API Preview 9
Network 10
Option added to select source interface and address for Telnet and SSH 10
File filter rules available in sniffer policy 10
Explicit mode with DoT and DoH 11
DNS inspection with DoT and DoH 11
Zones 11
Selectively forward web requests to a transparent web proxy 11
FortiProxy unit as an IPv6 DDNS client for generic DDNS 14
Allow backup and restore commands to use IPv6 addresses 14
Policy and objects 15
Virtual IPs 15
Zero Trust Network Access 15
Security profiles 18
Stream-based antivirus scan in proxy mode for FTP, SFTP, and SCP 18
TCP windows 18
Configure threat feed and outbreak prevention without AV engine scan 19
Content disarm and reconstruction for antivirus 21
External malware block list for antivirus 22
FortiGuard Outbreak Prevention for antivirus 22
FortiGuard web filter categories to block child sexual abuse and terrorism 23
Video filtering 24
Web filter antiphishing profile enhanced 24
Highlight of on-hold IPS signatures 28
HTTP/2 support in SSL inspection 28
Multiple certificates can be defined in an SSL profile in replace mode 28
Handling SSL offloaded traffic from an external decryption device 29
New filters for application control groups 30
Support for secure ICAP remote servers 31
Add TCP connection pool for connections to ICAP server 31
WAN optimization 31
Improved WAD traffic dispatcher 31
VPN 32
Dual-stack IPv4 and IPv6 support for SSL VPN 32
Disable the clipboard in SSL-VPN web-mode RDP connections 32

System ... 32
Allow administrators to define password policy with minimum character change ... 32
ACME certificate support ... 33
New option to automatically update schedule frequency ... 36
Security Fabric ... 36
Simplify EMS pairing with Security Fabric so one approval is needed for all devices ... 36
External threat feeds integrations ... 37
External block list file hashes ... 38
External block list (threat feed) for policy ... 38
Log and report ... 39
Add logs for the execution of CLI commands ... 39
Other new features and enhancements ... 39
Product integration and support ... 40
Web browser support ... 40
Fortinet product support ... 40
Fortinet Single Sign-On (FSSO) support ... 40
Virtualization environment support ... 41
New deployment of the FortiProxy VM ... 41
Upgrading the FortiProxy VM ... 41
Downgrading the FortiProxy VM ... 42
Software upgrade path for physical appliances ... 42
Resolved issues ... 43
Known issues ... 45

Change log

Date	Change Description
August 23, 2021	Initial release for FortiProxy 7.0.0
August 24, 2021	Updated the “Virtual IPs” and “FortiGuard Outbreak Prevention for antivirus” sections.
August 25, 2021	Updated the “Fortinet product support” section.
September 1, 2021	Updated to the latest template.
September 13, 2021	Made the “What’s new” section a separate section.
September 14, 2021	Added the “New filters for application control groups” section. Removed the “FortiAI integration” section.
October 6, 2021	Updated the “What’s new” section.
February 14, 2022	Updated the “Product integration and support” section.
March 22, 2022	Added bug 764817.

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 7.0.0, build 0029:

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

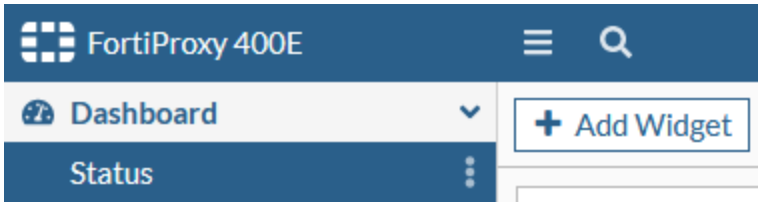
The following sections describe the new features and enhancements:

- General usability enhancements on page 8
- Network on page 10
- Policy and objects on page 15
- Security profiles on page 18
- WAN optimization on page 31
- VPN on page 32
- System on page 32
- Security Fabric on page 36
- Log and report on page 39
- Other new features and enhancements on page 39

General usability enhancements

GUI-based global search

The global search option in the GUI allows users to search for keywords appearing in objects and navigation menus to quickly access the object and configuration page. Click the magnifying glass icon in the top-left corner of the banner to access the global search.



The global search includes the following features:

- Keep a history of frequent and recent searches
- Sort results alphabetically by increasing or decreasing order, and relevance by search weight
- Search by category
- Search in Security Fabric members (accessed by the Security Fabric members dropdown menu in the banner)

SSL-VPN and IPsec monitor improvements

The *SSL-VPN* monitor now includes *Duration* and *Connection Summary* charts. The *IPsec* monitor displays information about Phase 1 and Phase 2 tunnels. Both monitors also identify users who have not enabled two-factor authentication.

SSL-VPN monitor

To view the SSL-VPN monitor:

1. Go to *Dashboard* and click *Add Widget*.
2. Under *Network*, click *SSL-VPN*.
3. Click *Default* or specify the FortiProxy unit.
4. Click *Add Widget*.
5. Click *Close*.
6. The *SSL-VPN* overview widget is displayed.
   A warning appears when at least one VPN user has not enabled two-factor authentication.
7. Hover over the widget and click *Expand to full screen*. The *Duration* and *Connection Summary* charts are displayed at the top of the monitor.
   A warning appears in the *Username* column when a user has not enabled two-factor authentication.
8. Right-click a user to *End Session*, *Locate on VPN Map*, *Show Matching Logs*, and *Show in FortiView*.

IPSec monitor

To view the IPSec Monitor:

1. Go to *Dashboard* and click *Add Widget*.
2. Under *Network*, click *IPsec*.
3. Click *Default* or specify the FortiProxy unit.
4. Click *Add Widget*.
5. Click *Close*.
6. The *IPsec* overview widget is displayed.
7. Hover over the widget and click *Expand to full screen*. A warning appears when an unauthenticated user is detected.

API Preview

The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

To use the API Preview:

1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Network

Option added to select source interface and address for Telnet and SSH

The new commands `execute telnet-options` and `execute ssh-options` allow administrators to set the source interface and address for their connection:

```
# execute telnet-options {interface <outgoing interface> | reset | source <source interface IP> | view-settings}
```

```
# execute ssh-options {interface <outgoing interface> | reset | source <source interface IP> | view-settings}
```

To edit the Telnet options:

```
# execute telnet-options interface port1
```

```
# execute telnet-options source 1.1.1.1
```

To confirm that the Telnet packets are using the configured port and address:

```
# diagnose sniffer packet any "port 23" 4
4.070426 port1 out 1.1.1.1.13938 -> 15.15.15.2.23: syn 400156130
4.070706 port1 in 15.15.15.2.23 -> 1.1.1.1.13938: syn 2889776642 ack 400156131
```

To edit the SSH options:

```
# execute ssh-options interface port1
```

```
# execute ssh-options source 1.1.1.1
```

To confirm that the SSH packets are using the configured port and address:

```
# diagnose sniffer packet any "port 22" 4
6.898985 port1 out 1.1.1.1.20625 -> 15.15.15.2.22: syn 1704095779
6.899286 port1 in 15.15.15.2.22 -> 1.1.1.1.20625: syn 753358246 ack 1704095780
```

File filter rules available in sniffer policy

File filter rules can be used in one-arm sniffer policies in the CLI.

The following example shows how to configure a file filter profile that blocks PDF and RAR files used in a one-arm sniffer policy:

```
config file-filter profile
    edit "sniffer-profile"
        set comment "File type inspection."
        config rules
            edit "1"
                set protocol http ftp smtp imap pop3 cifs
                set action block
                set file-type "pdf" "rar"
            next
```

```
        end
    next
end
```

Explicit mode with DoT and DoH

DNS over TLS (DoT) and DNS over HTTPS (DoH) are supported in explicit mode where the FortiProxy unit acts as an explicit DNS server that listens for DoT and DoH requests. Local-out DNS traffic over TLS and HTTPS is also supported.

DNS inspection with DoT and DoH

DNS over TLS (DoT) and DNS over HTTPS (DoH) are supported in DNS inspection. Before FortiProxy 7.0.0, DoT and DoH traffic silently passes through the DNS proxy. In FortiProxy 7.0.0, the WAD is able to handle DoT and DoH and redirect DNS queries to the DNS proxy for further inspection.

Zones

Zones are a group of one or more physical or virtual FortiProxy interfaces that you can apply security policies to control inbound and outbound traffic. Grouping interfaces into zones simplifies the creation of security policies where a number of network segments can use the same policy settings and protection profiles. Interfaces that are included in a zone must not be assigned to another zone or have firewall policies defined.

Verification

When a client visits a HTTP website, the client will be redirected to the captive portal for authentication by HTTPS. For example, the client could be redirected to a URL by a HTTP 303 message similar to the following:

HTTP/1.1 303 See Other

Connection: close

Content-Type: text/html

Cache-Control: no-cache

Location: https://fpx.fortinetqa.local:7831/XX/YY/ZZ/cpauth?scheme=http&4Tmthd=0&host=172.16.200.46&port=80&rule=75&uri=Lw==&

Content-Length: 0

The captive portal URL used for authentication is *https://fpx.fortinetqa.local:7831/...*. After the authentication is complete with all user credentials protected by HTTPS, the client is redirected to the original HTTP website it intended to visit.

Selectively forward web requests to a transparent web proxy

Web traffic over HTTP/HTTPS can be forwarded selectively by the FortiProxy unit's transparent web proxy to an upstream web proxy to avoid overwhelming the proxy server. Traffic can be selected by specifying the proxy address (`set webproxy-forward-server`), which can be based on a FortiGuard URL category.

The FortiGuard web filter service must be enabled on the downstream FortiProxy unit.

Forwarding behavior

The forward server will be ignored if the proxy policy matching for a particular session needs the FortiProxy unit to see authentication information inside the HTTP (plain text) message. For example, assume that user authentication is required and a forward server is configured in the transparent web proxy, and the authentication method is an active method (such as basic). When the user or client sends the HTTP request over SSL with authentication information to the FortiProxy unit, the request cannot be forwarded to the upstream proxy. Instead, it will be forwarded directly to the original web server (assuming deep inspection and `http-policy-redirect` are enabled in the firewall policy).

The FortiProxy unit will close the session before the client request can be forwarded if all of the following conditions are met:

- The certificate inspection is configured in the firewall policy that has the `http-policy-redirect` option enabled.
- A previously authenticated IP-based user record cannot be found by the FortiProxy unit's memory during the SSL handshake.
- Proxy policy matching needs the FortiProxy unit to see the HTTP request authentication information.

Use the following best practices to enable user authentication and use `webproxy-forward-server` in the transparent web proxy policy at the same time:

- In the firewall policy that has the `http-policy-redirect` option enabled, set `ssl-ssh-profile` to use the `deep-inspection` profile.
- Use IP-based authentication rules; otherwise, the `webproxy-forward-server` setting in the transparent web proxy policy will be ignored.
- Use a passive authentication method such as FSSO. With FSSO, once the user is authenticated as a domain user by a successful login, the web traffic from the user's client will always be forwarded to the upstream proxy as long as the authenticated user remains unexpired. If the authentication method is an active authentication method (such as basic, digest, NTLM, negotiate, form, and so on), the first session containing authentication information will bypass the forward server, but the following sessions will be connected through the upstream proxy.

Sample configuration

On the downstream FortiProxy proxy, there are two category proxy addresses used in two separate transparent web proxy policies as the destination address:

- In the policy with `upstream_proxy_1` as the forward server, the proxy address `category_infotech` is used to match URLs in the information technology category.
- In the policy with `upstream_proxy_2` as the forward server, the proxy address `category_social` is used to match URLs in the social media category.

To configure forwarding requests to transparent web proxies:

1. Configure the proxy forward servers:

```
config web-proxy forward-server
    edit "upStream_proxy_1"
        set ip 172.16.200.20
    next
    edit "upStream_proxy_2"
        set ip 172.16.200.46
```

```
    next
end
```

2. Configure the web proxy addresses:

```
config firewall proxy-address
    edit "category_infotech"
        set type category
        set host "all"
        set category 52
    next
    edit "category_social"
        set type category
        set host "all"
        set category 37
    next
end
```

3. Configure the firewall policy:

```
config firewall policy
    edit 1
        set srcintf "port10"
        set dstintf "port9"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "deep-inspection"
        set av-profile "av"
    next
end
```

4. Configure the proxy policies:

```
config firewall policy
    edit 1
        set type transparent
        set srcintf "port10"
        set dstintf "port9"
        set srcaddr "all"
        set dstaddr "category_infotech"
        set action accept
        set schedule "always"
        set logtraffic all
        set webproxy-forward-server "upStream_proxy_1"
        set utm-status enable
        set ssl-ssh-profile "deep-inspection"
        set av-profile "av"
    next
    edit 2
        set type transparent
        set srcintf "port10"
        set dstintf "port9"
        set srcaddr "all"
        set dstaddr "category_social"
```

```
            set action accept
            set schedule "always"
            set logtraffic all
            set webproxy-forward-server "upStream_proxy_2"
            set utm-status enable
            set ssl-ssh-profile "deep-inspection"
            set av-profile "av"
        next
    end
```

FortiProxy unit as an IPv6 DDNS client for generic DDNS

When configuring the generic DDNS service provider as a DDNS server, the server type and address type can be set to IPv6. This allows the FortiProxy unit to connect to an IPv6 DDNS server and provide the FortiProxy unit's IPv6 interface address for updates.

```
config system ddns
    edit <ID>
        set ddns-server genericDDNS
        set server-type {ipv4 | ipv6}
        set ddns-server-addr <address>
        set addr-type {ipv4 | ipv6}
        set monitor-interface <port>
    next
end
```

To configure an IPv6 DDNS client with generic DDNS:

```
config system ddns
    edit 1
        set ddns-server genericDDNS
        set server-type ipv6
        set ddns-server-addr "2004:16:16:16::2" "16.16.16.2" "ddns.genericddns.com"
        set ddns-domain "test.com"
        set addr-type ipv6
        set monitor-interface "port3"
    next
end
```

Allow backup and restore commands to use IPv6 addresses

IPv6 addresses are now supported in the `execute backup` and `execute restore` commands to TFTP and FTP servers.

To back up a configuration file to an IPv6 TFTP server:

```
# execute backup config tftp fpx.conf 2000:172:16:200::55
```

To restore a configuration file from an IPv6 TFTP server:

```
# execute restore config tftp fpx.conf 2000:172:16:200::55
```

To back up a configuration file to an IPv6 FTP server:

```
# execute backup config ftp fpx.conf 2000:172:16:200::55 root xxxxxxxxxx
```

To restore a configuration file from an IPv6 FTP server:

```
# execute restore config ftp fpx.conf 2000:172:16:200::55 root xxxxxxxxxx
```

Policy and objects

Virtual IPs

Static Virtual IPs (VIP) are used to map external IP addresses to internal IP addresses. This is also called destination NAT, where a packet's destination is being NAT'd, or mapped, to a different address.

Static VIPs are commonly used to map public IP addresses to resources behind the FortiProxy unit that use private IP addresses. A static on-to-one VIP is when the entire port range is mapped. A port forwarding VIP is when the mapping is configured on a specific port or port range.

To create a virtual IP in the GUI:

1. In *Policy & Objects* > *Virtual IPs* and click *Create New* > *Virtual IP*.
2. Select a *VIP Type* based on the IP versions used.
3. Enter a unique name for the virtual IP.
4. Enter values for the external IP address/range and map to IPv4/IPv6 address/range fields.
5. Click *OK*.

To create a virtual IP in the CLI:

```
config firewall vip
   edit "Internal_WebServer"
      set extip 10.1.100.199
      set extintf "any"
      set mappedip "172.16.200.55"
   next
end
```

Zero Trust Network Access

Zero Trust Network Access (ZTNA) is an access control method that uses client device identification, authentication, and Zero Trust tags to provide role-based application access. It gives administrators the flexibility to manage network access for on-net local users and off-net remote users. Access to applications is granted only after device verification, authenticating the user's identity, authorizing the user, and then performing context based posture checks using Zero Trust tags.

Traditionally, a user and a device have different sets of rules for on-net access and off-net VPN access to company resources. With a distributed workforce and access that spans company networks, data centers, and cloud, managing

the rules can become complex. User experience is also affected when multiple VPNs are needed to get to various resources.

Access proxy

The FortiProxy access proxy can proxy HTTP and TCP traffic over secure HTTPS connections with the client. This enables seamless access from the client to the protected servers, without needing to form IPsec or SSL VPN tunnels.

HTTPS access proxy

The FortiProxy HTTPS access proxy works as a reverse proxy for the HTTP server. When a client connects to a webpage hosted by the protected server, the address resolves to the FortiProxy unit's access proxy VIP. The FortiProxy unit proxies the connection and takes steps to authenticate the user. It prompts the user for their certificate on the browser, and verifies this against the ZTNA endpoint record that is synchronized from the EMS. If an authentication scheme, such as SAML authentication, is configured, the client is redirected to a captive portal for sign-on. If this passes, traffic is allowed based on the ZTNA rules, and the FortiProxy unit returns the webpage to the client.

TCP forwarding access proxy (TFAP)

TCP forwarding access proxy works as a special type of HTTPS reverse proxy. Instead of proxying traffic to a web server, TCP traffic is tunneled between the client and the access proxy over HTTPS, and forwarded to the protected resource. The FortiClient endpoint configures the ZTNA connection by pointing to the proxy gateway, and then specifying the destination host that it wants to reach. An HTTPS connection is made to the FortiProxy unit's access proxy VIP, where the client certificate is verified and access is granted based on the ZTNA rules. TCP traffic is forwarded from the FortiProxy unit to the protected resource, and an end to end connection is established.

Basic requirements for ZTNA configuration

The following are the basic requirements for configuring full ZTNA on the FortiProxy unit:

- FortiClient EMS fabric connector and ZTNA tags
- FortiClient EMS running version 7.0.0 or later
- FortiClient running 7.0.0 or later
- ZTNA server
- ZTNA rule
- Firewall policy

Basic ZTNA configuration

To deploy full ZTNA, configure the following components on the FortiProxy unit:

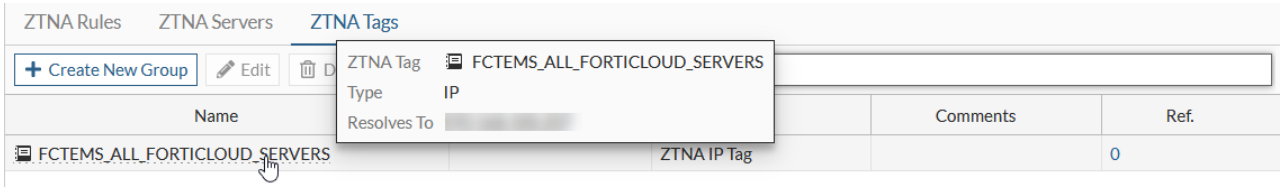
1. Configure a FortiClient EMS fabric connector and ZTNA tags.
2. Configure a ZTNA server.
3. Configure a ZTNA rule.
4. Configure a firewall policy for full ZTNA.
5. Optionally configure authentication.

ZTNA tags

After the FortiProxy unit connects to the FortiClient EMS, it automatically synchronizes ZTNA tags.

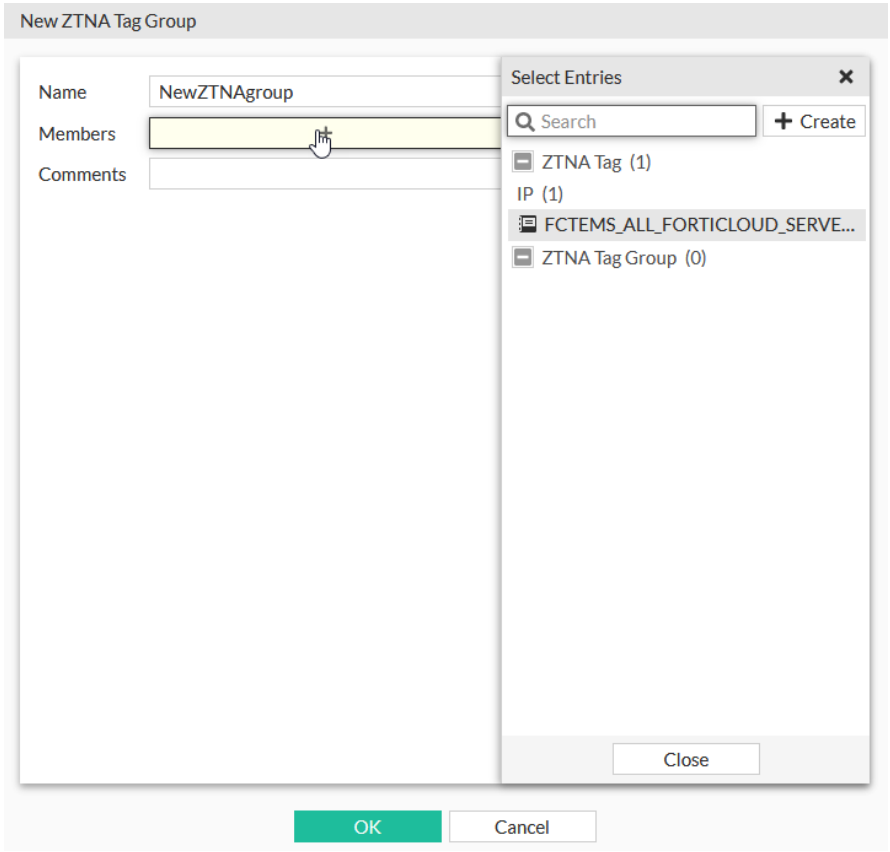
To view the synchronized ZTNA tags in the GUI:

1. Go to *Policy & Objects* > *ZTNA* and select the *ZTNA Tags* tab.
2. Hover the cursor over a tag name to view more information about the tag, such as its resolved addresses.



To create a ZTNA tag group in the GUI:

1. Go to *Policy & Objects* > *ZTNA* and select the *ZTNA Tags* tab.
2. Click *Create New Group*.
3. Enter a name for the group and select the group members.



4. Click *OK*.

To create a ZTNA tag group in the CLI:

```
config firewall addrgrp
    edit <group name>
        set category ztna-ems-tag
        set member <members>
    next
end
```

Security profiles

Stream-based antivirus scan in proxy mode for FTP, SFTP, and SCP

Stream-based antivirus scanning in proxy mode is supported for FTP, SFTP, and SCP protocols.

- Stream-based antivirus scanning optimizes memory usage for large archive files by decompressing the files on the fly and scanning the files as they are extracted.
- File types can be determined after scanning a few KB, without buffering the entire file.
- Viruses can be detected even if they are hiding in the middle or end of a large archive.
- When scanning smaller files, traffic throughput is improved by scanning the files directly on the proxy based WAD daemon, without invoking scanunit.

Stream-based scanning is the default scan mode when an antivirus is in proxy mode. To disable steam-based scanning, the scan mode can be set to legacy mode, and the archive will only be scanned after the entire file has been received.

To configure stream-based scan:

```
config antivirus profile
    edit <string>
        ...
        set scan-mode {default* | legacy}
        ...
    next
end
```

TCP windows

Some file transfer applications can negotiate large TCP windows. For example, WinSCP can negotiate an initial TCP window size of about 2 GB.

The TCP window options can be used to prevent overly large initial TCP window sizes, helping avoid channel flow control issues. It allows stream-based scan's flow control to limit peers from sending data that exceeds a policy's configured oversize limit.

To configure TCP window size options:

```
config firewall profile-protocol-options
    edit <string>
        config {ftp | ssh}
```

```
            ...
            set stream-based-uncompressed-limit <integer>
            set tcp-window-type {system | static | dynamic}
            set tcp-window-size <integer>
            set tcp-window-minimum <integer>
            set tcp-window-maximum <integer>
            ...
        end
    next
end
```

`{ftp | ssh}`	• `ftp`: Configure FTP protocol options. • `ssh`: Configure SFTP and SCP protocol options.
`stream-based-uncompressed-limit <integer>`	The maximum stream-based uncompressed data size that will be scanned, in MB (default = 0 (unlimited)). Stream-based uncompression used only under certain conditions.).
`tcp-window-type {system | static | dynamic}`	The TCP window type to use for this protocol. • `system`: Use the system default TCP window size for this protocol (default). • `static`: Manually specify the TCP window size. • `dynamic`: Vary the TCP window size based on available memory within the limits configured in `tcp-window-minimum` and `tcp-window-maximum`.
`tcp-window-size <integer>`	The TCP static window size (65536 - 33554432, default = 262144). This option is only available when `tcp-window-type` is `static`.
`tcp-window-minimum <integer>`	The minimum TCP dynamic window size (65536 - 1048576, default = 131072). This option is only available when `tcp-window-type` is `dynamic`.
`tcp-window-maximum <integer>`	The maximum TCP dynamic window size (1048576 - 33554432, default = 8388608). This option is only available when `tcp-window-type` is `dynamic`.

Configure threat feed and outbreak prevention without AV engine scan

In the CLI, users can enable malware threat feeds and outbreak prevention without performing an antivirus scan. In the GUI and CLI, users can choose to use all malware thread feeds, or specify the ones that they want to use. Replacement messages have been updated for external block lists.

```
config antivirus profile
    edit <name>
        config http
            set av-scan {disable | block | monitor}
            set outbreak-prevention {disable | block | monitor}
            set external-blocklist {disable | block | monitor}
            set quarantine {enable | disable}
        end
        ...
        set outbreak-prevention-archive-scan {enable | disable}
        set external-blocklist-enable-all {enable | disable}
        set external-blocklist <source>
    next
end
```

To configure malware threat feeds and outbreak prevention without performing an AV scan in the CLI:

```
config antivirus profile
    edit "Demo"
        set mobile-malware-db enable
        config http
            set av-scan disable
            set outbreak-prevention block
            set external-blocklist block
            set quarantine enable
            set emulator enable
            set content-disarm disable
        end
        config ftp
            set av-scan disable
            set outbreak-prevention block
            set external-blocklist block
            set quarantine enable
            set emulator enable
        end
        config imap
            set av-scan monitor
            set outbreak-prevention block
            set external-blocklist block
            set quarantine enable
            set emulator enable
            set executables default
            set content-disarm disable
        end
        config pop3
            set av-scan monitor
            set outbreak-prevention block
            set external-blocklist block
            set quarantine enable
            set emulator enable
            set executables default
            set content-disarm disable
        end
        config smtp
            set av-scan monitor
            set outbreak-prevention block
            set external-blocklist block
            set quarantine enable
            set emulator enable
            set executables default
            set content-disarm disable
        end
        config mapi
            set av-scan monitor
            set outbreak-prevention block
            set external-blocklist block
            set quarantine enable
            set emulator enable
            set executables default
        end
        config nntp
```

```
            set av-scan disable
            set outbreak-prevention disable
            set external-blocklist disable
            set quarantine disable
            set emulator enable
        end
        config cifs
            set av-scan monitor
            set outbreak-prevention block
            set external-blocklist block
            set quarantine enable
            set emulator enable
        end
        config ssh
            set av-scan disable
            set outbreak-prevention disable
            set external-blocklist disable
            set quarantine disable
            set emulator enable
        end
        set outbreak-prevention-archive-scan enable
        set external-blocklist-enable-all disable
        set external-blocklist "malhash1"
        set av-virus-log enable
        set av-block-log enable
        set extended-log disable
        set scan-mode default
    next
end
```

In this example, configuring the quarantine setting is done in each protocol (`set quarantine`). The malware threat feed is also specified (`set external-blocklist-enable-all disable`) to the threat connector, malhash1 (`set external-blocklist "malhash1"`).

Content disarm and reconstruction for antivirus

Content Disarm and Reconstruction (CDR) allows the FortiProxy unit to sanitize Microsoft documents and PDF files (disarm) by removing active content such as hyperlinks, embedded media, JavaScript, macros, and so on from the office document files without affecting the integrity of its textual content (reconstruction).

This feature allows network admins to protect their users from malicious office document files.

Files processed by CDR can have the original copy quarantined on the FortiProxy unit, allowing admins to observe them. These original copies can also be obtained in the event of a false positive.

Support and limitations

- CDR can only be performed on Microsoft Office documents and PDF files.
- Local Disk CDR quarantine is only possible on FortiProxy models that contain a hard disk.
- CDR is only supported on HTTP, SMTP, POP3, IMAP.
  - SMTP splice and client-comfort mode is not supported.
- CDR can only work on files in .ZIP type archives.

Configuring the feature

To configure antivirus to work with CDR, you must enable CDR on your antivirus profile, set the quarantine location, and then fine tune the CDR detection parameters.

External malware block list for antivirus

External malware block list is a new feature that falls under the umbrella of Outbreak Prevention.

This feature provides another means of supporting the AV Database by allowing users to add their own malware signatures in the form of MD5, SHA1, and SHA256 hashes.

This feature provides a mechanism for Antivirus to retrieve an external malware hash list from a remote server and polls the hash list every *n* minutes for updates.

Support and limitations

Malware detection using the external malware block list in proxy-based policy inspections.

Just like FortiGuard Outbreak Prevention, the external dynamic block list is not supported in AV quick scan mode.

Using different types of hash simultaneously may slow down the performance of malware scanning. For this reason, Fortinet recommends using one type of hash (either MD5, SHA1, or SHA256), not all three simultaneously.

FortiGuard Outbreak Prevention for antivirus

FortiGuard Outbreak Prevention allows the FortiProxy antivirus database to be subsidized with third-party malware hash signatures curated by the FortiGuard. The hash signatures are obtained from external sources such as VirusTotal, Symantec, Kaspersky, and other third-party websites and services.

This feature provides the mechanism for antivirus to query the FortiGuard with the hash of a scanned file. If the FortiGuard returns a match from its many curated signature sources, the scanned file is deemed to be malicious.

The concept of FortiGuard Outbreak Prevention is to detect zero-day malware in a collaborative approach.

Support and limitations

- FortiGuard Outbreak Prevention policy inspections across all supported protocols.
- FortiGuard Outbreak Prevention does not support AV in quick scan mode.

Configuring the feature

For antivirus to work with an external block list, you must register the FortiProxy unit with a FortiGuard Outbreak Prevention license and enable FortiGuard Outbreak Prevention in the antivirus profile.

Important Note

The FortiGuard Outbreak Prevention service will be available as part of a future SWG Protection bundle. Customers that want to enable this feature need to renew the contract or purchase a new SWG Protection bundle.

FortiGuard web filter categories to block child sexual abuse and terrorism

Web filter categories 83 (Child Sexual Abuse, formerly Child Abuse) and 96 (Terrorism) can be used to enforce blocking and logging the Internet Watch Foundation (IWF) and Counter-Terrorism Internet Referral Unit (CTIRU) lists, respectively.

To create a web filter profile to block the Child Sexual Abuse and Terrorism categories in the GUI:

1. Go to *Security Profiles* > *Web Filter* and click *Create New*.
2. Enter a name for the new filter.
3. Enable *FortiGuard Category Based Filter*.
4. In the category table, in the *Potentially Liable* section, set the *Action* for the *Child Sexual Abuse* and *Terrorism* categories to *Block*.
5. Configure the remaining settings as required.
6. Click *OK*.

To create a web filter profile to block category 83 (Child Sexual Abuse) in the CLI:

```
config webfilter profile
    edit newfilter
        config ftgd-wf
            unset options
            config filters
                ...
                edit 83
                    set category 83
                    set action block
                next
                ...
            end
        end
    next
end
```

To test the web filter:

1. Use the web filter profile in a policy.
2. On a device that is connected through the FortiProxy unit and that uses the policy, visit the test URLs for each category:
   ```
   http://wfurltest.fortiguard.com/wftest/83.html
   http://wfurltest.fortiguard.com/wftest/96.html
   ```
3. Log in to the FortiProxy unit and go to *Log & Report* > *Web filter* to view the logs for the blocked websites.

Video filtering

With the video filter profile, you can filter YouTube videos by channel ID for a more granular override of a single channel, user, or video. The video filter profile is currently supported in proxy-based policies and requires SSL deep inspection.

To configure a video filter in the GUI:

1. Go to *Security Profiles* > *Video Filter* and click *Create New*.
2. In the *Channel override list* section, click *Create New*. The *New Channel Override Entry* pane opens.
3. Enter a *Channel ID*.
4. In the *Comments* field, enter a description of the entry.
5. Select *Allow*, *Monitor*, or *Block* for the action.
6. Click *OK*.

To configure a video filter in the GUI:

```
config videofilter youtube-channel-filter
   edit <identifier>
      set name <string>
      config entries
         edit <identifier>
            set action{allow | monitor | block}
            set channel-id <string>
         next
      end
   next
end
```

For example:

```
config videofilter youtube-channel-filter
   edit 1
      set name "channel_filter"
      config entries
         edit 1
            set action block
            set channel-id "UCJHo4AuVomwMRzgkA5DQEOA"
         next
      end
   next
end
```

Web filter antiphishing profile enhanced

The following enhancements have been made to the antiphishing profile:

- Allow username and password field patterns to be fetched from FortiGuard.
- Add DNS support for domain controller IP fetching.
- Add support to specify a source IP or port for the fetching domain controller.
- Add LDAP server as a credential source (only the OpenLDAP server is supported).
- Block or log valid usernames regardless of password match.

- Add literal custom patterns type for username and password.
- Add support for Active Directory Lightweight Directory Services (AD LDS).

In previous versions of the FortiProxy CLI, the domain controller for antiphishing is configured under `config credential-store domain-controller`. Starting in 7.0.0, it is configured under `config user domain-controller`.

To update the antiphish pattern database:

1. Go to *System* > *FortiGuard* and in the right-side pane, click *Update Licenses & Definitions Now*.
2. Enter the following in the CLI:

```
# diagnose autoupdate versions
...
AntiPhish Pattern DB
---------
Version: 0.00000
Contract Expiry Date: n/a
Last Updated using manual update on Tue Nov 30 00:00:00 1999
Last Update Attempt: Wed Sep 29 14:00:11 2021
Result: No Updates
```

To enable DNS service lookup:

```
config user domain-controller
    edit "win2016"
        set ad-mode ds
        set dns-srv-lookup enable
        set hostname "win2016"
        set username "replicate"
        set password **********
        set domain-name "SMB2016.LAB"
    next
end
```

To specify the source IP and port for the fetching domain controller:

```
config user domain-controller
    edit "win2016"
        set ad-mode ds
        set hostname "win2016"
        set username "replicate"
        set password **********
        set ip-address 172.18.52.188
        set source-ip-address 172.16.100.1
        set source-port 2000
        set domain-name "SMB2016.LAB"
    next
end
```

To use an LDAP server as a credential store:

1. Configure the LDAP server:

```
config user ldap
    edit "openldap"
        set server "172.18.60.214"
        set cnid "cn"
        set dn "dc=qafsso,dc=com"
        set type regular
        set username "cn=Manager,dc=qafsso,dc=com"
        set password **********
        set antiphish enable
        set password-attr "userPassword"
    next
end
```

2. Configure the web filter profile:

```
config webfilter profile
    edit "webfilter"
        config ftgd-wf
            unset options
            config filters
                edit 1
                    set action block
                next
            end
        end
        config antiphish
            set status enable
            config inspection-entries
                edit "cat34"
                    set fortiguard-category 34
                    set action block
                next
            end
            set authentication ldap
            set ldap "openldap"
        end
        set log-all-url enable
    next
end
```

To configure user-name-only credential matching:

```
config webfilter profile
    edit "webfilter"
        config ftgd-wf
            unset options
            ...
        end
        config antiphish
            set status enable
            set check-username-only enable
            config inspection-entries
                edit "cat34"
```

```
                    set fortiguard-category 34
                    set action block
                next
            end
            set domain-controller "win2016"
        end
        set log-all-url enable
    next
end
```

To configure different custom pattern types for user names and passwords:

```
config webfilter profile
    edit "webfilter"
        config ftgd-wf
            unset options
            ...
        end
        config antiphish
            set status enable
            config inspection-entries
                edit "cat34"
                    set fortiguard-category 34
                    set action block
                next
            end
            config custom-patterns
                edit "qwer"
                    set type literal
                next
                edit "[0-6]Dat*"
                next
                edit "dauw9"
                    set category password
                    set type literal
                next
                edit "[0-5]foo[1-4]"
                    set category password
                next
            end
            set domain-controller "win2016"
        end
        set log-all-url enable
    next
end
```

In this example, the `qwer` and `dauw9` entries use the literal type, while `[0-6]Dat*` and `[0-5]foo[1-4]` use the default regex type.

To configure Active Directory in LDS mode:

```
config user domain-controller
    edit "win2016adlds"
        set ad-mode lds
        set hostname "win2016adlds"
        set username "foo"
```

```
        set password **********
        set ip-address 192.168.10.9
        set domain-name "adlds.local"
        set adlds-dn "CN=adlds1part1,DC=ADLDS,DC=COM"
        set adlds-ip-address 192.168.10.9
        set adlds-port 3890
    next
end
```

Highlight of on-hold IPS signatures

IPS signatures that are on hold (administrator-added delay for activation time) are highlighted in the GUI as follows:

- On-hold signatures are grayed out with an hourglass icon beside the signature name.
- The signature tooltip displays the on hold expiry time.
- Users can still use on-hold signatures in an IPS sensor profile; however, the profile will not block matching traffic. It will monitor it instead (logging in effect) until the on hold time expires.

After a hold time is configured in the CLI, go to *Security Profiles* > *IPS Signatures*. Hover over the grayed-out entry to view the tooltip, which includes the action and hold time expiry.

The same tooltip is available on the *Edit IPS Sensor* (*Security Profiles* > *Intrusion Prevention*) page when creating or editing the IPS signatures. In the *Add Signatures* pane when the *Type* is *Signature*, on-hold signatures are only displayed as on hold if `override-signature-hold-by-id` is enabled.

HTTP/2 support in SSL inspection

Security profiles can perform SSL inspection on HTTP/2 traffic that is secured by TLS 1.2 or 1.3 using the Application-Layer Protocol Negotiation (ALPN) extension.

To set the ALPN support:

```
config firewall ssl-ssh-profile
   edit <profile>
      set supported-alpn {all | http1-1 | http2 | none}
   next
end
```

Multiple certificates can be defined in an SSL profile in replace mode

Multiple certificates can be defined in an SSL inspection profile in replace mode (*Protecting SSL Server*). This allows multiple sites to be deployed on the same protected server IP address, and inspection based on matching the SNI in the certificate.

When the FortiProxy unit receives the client and server hello messages, it will compare the SNI and CN with the certificate list in the SSL profile, and use the matched certificate as a replacement. If there is no matched server certificate in the list, the first server certificate in the list is used as a replacement.

To configure an SSL profile in replace mode with multiple certificates:

```
config firewall ssl-ssh-profile
    edit "multi-cert"
        set server-cert-mode replace
        set server-cert "bbb" "aaa"
    next
end
```

To configure a policy that uses the SSL profile:

```
config firewall policy
    edit 1
        set name "multi-cert"
        set srcintf "port6"
        set dstintf "port11"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "multi-cert"
        set av-profile "default"
        set webfilter-profile "default"
        set logtraffic all
    next
end
```

Results

If the Server Name Identification (SNI) matches the Common Name (CN) in the certificate list in the SSL profile, then the FortiProxy unit uses the matched server certificate.

If the Server Name Identification (SNI) does not match the Common Name (CN) in the certificate list in the SSL profile, then the FortiProxy unit uses the first server certificate in the list.

Handling SSL offloaded traffic from an external decryption device

In scenarios where the FortiProxy unit is sandwiched between load-balancers and SSL processing is offloaded on the external load-balancers, the FortiProxy unit can perform scanning on the unencrypted traffic by specifying the `ssl-offloaded` option in `firewall profile-protocol-options`.

To configure SSL offloading:

```
config firewall profile-protocol-options
   edit <name>
     config http
        set ports <1-65535>
        set ssl-offloaded {no | yes}
     end
     config ftp
        set ports <1-65535>
```

```
      set ssl-offloaded {no | yes}
    end
    config imap
      set ports <1-65535>
      set ssl-offloaded {no | yes}
    end
    config pop3
      set ports <1-65535>
      set ssl-offloaded {no | yes}
    end
    config smtp
      set ports <1-65535>
      set ssl-offloaded {no | yes}
    end
    config ssh
      set ports <1-65535>
      set ssl-offloaded {no | yes}
    end
  next
end
```

New filters for application control groups

When creating an application group, you can now define the application group by protocols, risk, vendor, technology, behavior, popularity, and category.

To create an application group in the CLI:

```
config application group
  edit <name>
    set type filter
    set protocols <0-47 | all>
    set risk <1-5>
    set vendor <0-25 | all>
    set technology <all | 0-4>
    set behavior <all | 2 | 5 | 6 | 9>
    set popularity <1-6>
    set category <2 | 3 | 5-8 | 12 | 15 | 17 | 21-23 | 25 | 26 | 28-32>
  next
end
```

To create an application group in the GUI:

1. Go to *Security Profiles* > *Application Signatures*.
2. Select *Create New* > *Application Group*.
3. Enter a group name.
4. Select *Filter*.
5. Click + to add members to the group.
6. Enter an optional description of the group.
7. Click *OK*.

Support for secure ICAP remote servers

A secure SSL connection from the FortiProxy unit to the remote ICAP server can be configured as follows:

```
config icap remote-sever
   edit <server_name>
      set secure enable
      set ssl-cert <certificate>
   next
end
```

Add TCP connection pool for connections to ICAP server

A TCP connection pool can maintain local-out TCP connections to the external ICAP server due to a backend update in the FortiProxy unit. TCP connections will not be terminated once data has been exchanged with the ICAP server, but instead are reused in the next ICAP session to maximize efficiency.

Use case

In this scenario, an ICAP profile is used as a UTM profile in an explicit web proxy policy, and a client visits web servers through this proxy policy.

After the WAD is initialized, when a HTTP request is sent from the client to the server through the FortiProxy unit with an ICAP profile applied to the matched proxy policy, a TCP connection is established between the FortiProxy unit and the ICAP server to exchange data.

When an ICAP session is finished, the TCP connection is kept in the WAD connection pool. When another ICAP session needs to be established, the WAD will check if there are any idle connections available in the connection pool. If an idle connection is available, it will be reused; otherwise, a new TCP connection is established for the ICAP session. This process can be checked in the WAD debug log.

WAN optimization

Improved WAD traffic dispatcher

The WAD traffic dispatcher now allows incoming traffic to be directly distributed to the workers. This enhancement also allows source addresses to be exempt from proxy affinity, which allows traffic from the same source and different server to be distributed to workers in a round-robin configuration. A maximum of 255 workers is now supported.

VPN

Dual-stack IPv4 and IPv6 support for SSL VPN

Dual-stack IPv4 and IPv6 support for SSL-VPN servers and clients enables a client to establish a dual-stack tunnel to allow both IPv4 and IPv6 traffic to pass through. FortiProxy SSL-VPN clients also support dual stack, which allows it to establish dual stack tunnels with other FortiProxy units.

Users connecting in web mode can connect to the web portal over IPv4 or IPv6. They can access bookmarks in either IPv4 or IPv6, depending on the preferred DNS setting of the web portal.

To enable dual stack in the CLI:

```
config vpn ssl settings
    set dual-stack-mode enable
end
```

Disable the clipboard in SSL-VPN web-mode RDP connections

In web portal profiles, the clipboard can be disabled for SSL VPN web-mode RDP/VNC connections. Users will not be able to copy and paste content to or from the internal server.

To disable the RDP/VNC clipboard in the GUI:

1. Go to *VPN* > *SSL-VPN Portals*.
2. Select a portal and click *Edit*.
3. Disable *RDP/VNC clipboard*.
4. Click *OK*.

To disable the RDP/VNC clipboard in the CLI:

```
config vpn ssl web portal
    edit <portal_name>
        set clipboard disable
    next
end
```

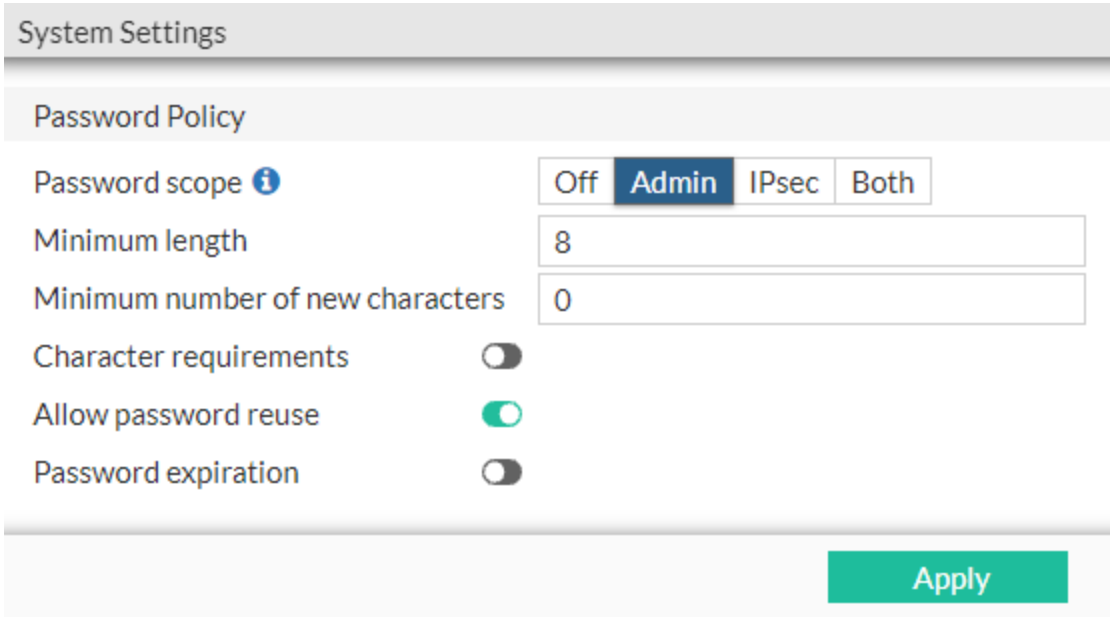
System

Allow administrators to define password policy with minimum character change

In previous FortiProxy versions, password policies were restricted to only enable or disable a minimum of four new characters in new password. Administrators can now set a minimum number of unique characters in the new password that do not exist in the old password. This setting overrides the password reuse option if both are enabled.

To configure the password policy in the GUI:

1. Go to *System* > *Settings* and navigate to the *Password Policy* section.
2. For *Password scope*, select *Admin*.
3. Enter a value for *Minimum number of new characters*.



4. Click *Apply*.

To configure the password policy in the CLI:

```
config system password-policy
    set status enable
    set min-change-characters <0-128>
end
```

ACME certificate support

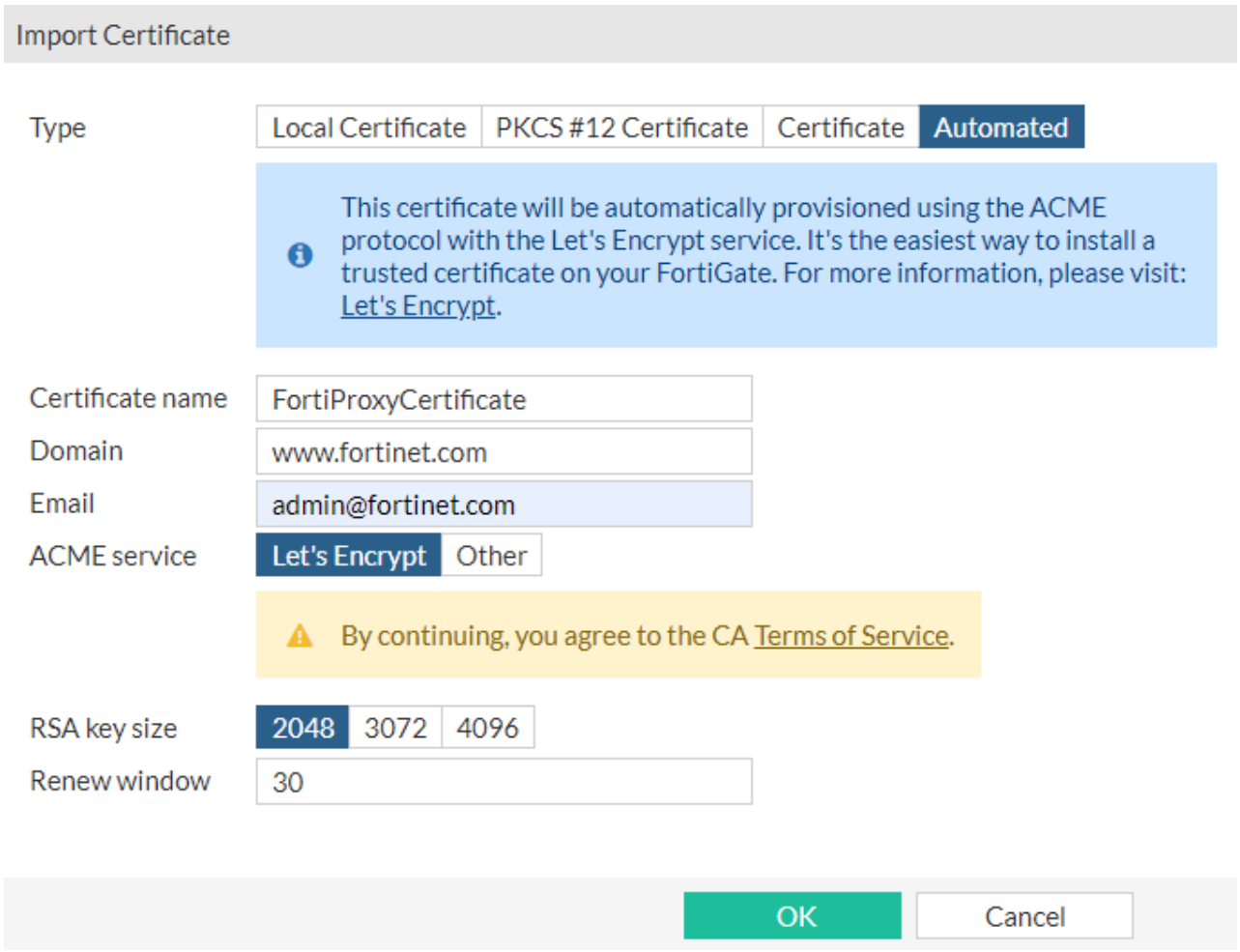
The Automated Certificate Management Environment (ACME), as defined in RFC 8555, is used by the public Let's Encrypt certificate authority (https://letsencrypt.org) to provide free SSL server certificates. The FortiProxy unit can be configured to use certificates that are manged by Let's Encrypt, and other certificate management services, that use the ACME protocol. The server certificates can be used for secure administrator log in to the FortiProxy unit.

- The FortiProxy unit must have a public IP address and a hostname in DNS (FQDN) that resolves to the public IP address.
- The configured ACME interface must be public facing so that the FortiProxy unit can listen for ACME update requests. It must not have any VIPs, or port forwarding on port 80 (HTTP) or 443 (HTTPS).
- The Subject Alternative Name (SAN) field is automatically filled with the FortiProxy DNS hostname. It cannot be edited, wildcards cannot be used, and multiple SANs cannot be added.

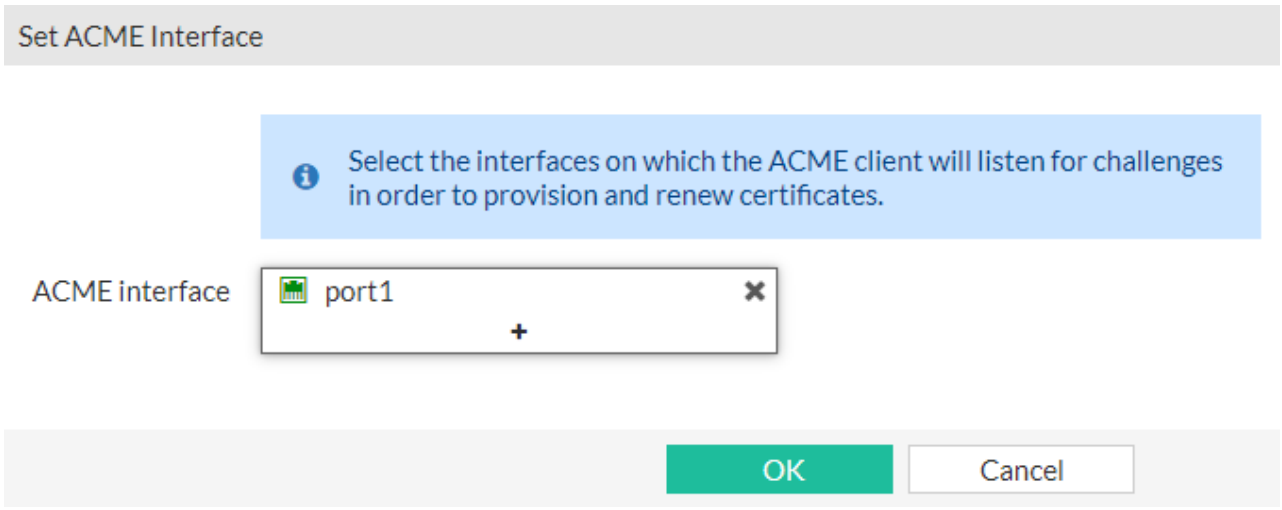
NOTE: To configure certificates in the GUI, go to *System* > *Feature Visibility* and enable *Certificates*.

To import an ACME certificate in the GUI:

1. Go to *System* > *Certificates* and click *Import* > *Local Certificate*.
2. Set *Type* to *Automated*.
3. Set *Certificate name* to an appropriate name for the certificate.
4. Set *Domain* to the public FQDN of the FortiProxy unit.
5. Set *Email* to a valid email address. The email is not used during the enrollment process.
6. Ensure that *ACME service* is set to *Let's Encrypt.*



7. Configure the remaining settings as required and then click *OK*.
8. If this is the first time enrolling a server certificate with Let's Encrypt on this FortiProxy unit, the *Set ACME Interface* pane opens. Select the interface that the FortiProxy unit communicates with Let's Encrypt on and then click *OK*.



The ACME interface can later be changed in *System* > *Settings*.

9. Select the new server certificate in the *Local Certificate* list and then click *View Details* to verify that the FortiProxy unit's FQDN is in the certificate's Subject: Common Name (CN).

   The *Remote CA Certificate* list includes the issuing Let's Encrypt intermediate CA, issued by the public CA DST Root CA X3 from Digital Signature Trust Company.

To exchange the default FortiProxy administration server certificate for the new public Let's Encrypt server certificate in the GUI:

1. Go to *System* > *Settings*.
2. Set the HTTPS server certificate to the new certificate.
3. Click *Apply*.
4. Log in to the FortiProxy unit using an administrator account from any Internet browser. There should be no warnings related to nontrusted certificates, and the certificate path should be valid.

To import an ACME certificate in the CLI:

1. Set the interface that the FortiProxy unit communicates with Let's Encrypt on:

```
config system acme
   set interface port1
end
```

2. Make sure that the FortiProxy unit can contact the Let's Encrypt enrollment server:

```
FortiProxy-400E # execute ping acme-v02.api.letsencrypt.org
PING ca80a1adb12a4fbdac5ffcbc944e9a61.pacloudflare.com (172.65.32.248): 56 data bytes
64 bytes from 172.65.32.248: icmp_seq=0 ttl=56 time=4.8 ms
64 bytes from 172.65.32.248: icmp_seq=1 ttl=56 time=4.5 ms
64 bytes from 172.65.32.248: icmp_seq=2 ttl=56 time=4.5 ms
64 bytes from 172.65.32.248: icmp_seq=3 ttl=56 time=4.5 ms
64 bytes from 172.65.32.248: icmp_seq=4 ttl=56 time=4.5 ms

--- ca80a1adb12a4fbdac5ffcbc944e9a61.pacloudflare.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 4.5/4.5/4.8 ms
```

3. Configure the local certificate request:

```
config vpn certificate local
```

```
    edit "acme-test"
       set enroll-protocol acme2
       set acme-domain "test.ftntlab.de"
       set acme-email "techdoc@fortinet.com"
       next
       By enabling this feature you declare that you agree to the Terms of Service at
       https://acme-v02.api.letsencrypt.org/directory
       Do you want to continue? (y/n)y
end
```

4. Verify that the enrollment was successful:
   ```
   # get vpn certificate local details acme-test
   ```

To exchange the default FortiProxy administration server certificate for the new public Let's Encrypt server certificate in the CLI:

```
config system global
   set admin-server-cert "acme-test"
end
```

When you log in to the FortiProxy unit using an administrator account, there should be no warnings related to nontrusted certificates, and the certificate path should be valid.

New option to automatically update schedule frequency

The default auto-update schedule for FortiGuard packages has been updated. Previously, the frequency was a reoccurring random interval within two hours. Starting in 7.0, the frequency is automatic, and the update interval is calculated based on the model and percentage of valid subscriptions. The update interval is within one hour.

```
config system autoupdate schedule
    set frequency {every | daily | weekly | automatic}
end
```

Security Fabric

Simplify EMS pairing with Security Fabric so one approval is needed for all devices

FortiClient EMS with Fabric authorization and silent approval capabilities will be able to approve the root FortiProxy unit in a Security Fabric once and then silently approve remaining downstream FortiProxy units in the Fabric. Similarly in an HA scenario, an approval only needs to be made once to the HA primary unit. The remaining cluster members are approved silently.

To use EMS silent approval:

1. Configure the EMS entry on the root FortiProxy unit or HA primary:

   ```
   config endpoint-control fctems
       edit "ems139"
           set fortinetone-cloud-authentication disable
           set server "172.16.200.139"
           set https-port 443
   ```

```
            set source-ip 0.0.0.0
            set pull-sysinfo enable
            set pull-vulnerabilities enable
            set pull-avatars enable
            set pull-tags enable
            set pull-malware-hash enable
            unset capabilities
            set call-timeout 30
            set websocket-override disable
        next
    end
```

When the entry is created, the capabilities are unset by default.

2. Authenticate the FortiProxy unit with EMS:

```
# execute fctems verify ems_139
...
```

The FortiProxy unit enables the Fabric authorization and silent approval based on the EMS supported capabilities.

```
config endpoint-control fctems
    edit "ems139"
        set server "172.18.62.12"
        set capabilities fabric-auth silent-approval websocket
    next
end
```

3. Configure a downstream device in the Security Fabric. The downstream device is silently approved.
4. Configure a secondary device in an HA system. The secondary device is silently approved.

External threat feeds integrations

You can define 511 thread feed entries using either the GUI or CLI.

To configure an external threat feed connector in the GUI:

1. Go to *Security Fabric* > *External Connectors* and click *Create New*.
2. In the *Threat Feeds* section, click one of the icons.
3. Configure the settings as needed.
4. Click *OK*.

To configure an external threat feed connector in the CLI:

```
config system external-resource
   edit "<external_resource_name"
      set status enable
      set uuid <universially_unique_identifier>
      set type {category | address | domain | malware}
      set category <192-221>
      set username <HTTP_basic_authentication_user_name>
      set password <HTTP_basic_authentication_password>
      set comments <descriptive_comments>
      set resource <URI_of_external_resource>
      set user-agent <HTTP_User-Agent_header>
      set refresh-rate <1-43200 minutes>
```

```
      set source-ip <source_IPv4_address_used_to_communicate_with_server>
      set interface-select-method {auto | sdwan | specify}
   next
end
```

External block list file hashes

The malware hash threat feed connector supports a list of file hashes that can be used as part of virus outbreak prevention.

To create a malware hash connector in the GUI:

1. Go to *Security Fabric* > *External Connectors* and click *Create New*.
2. In the *Threat Feeds* section, click *Malware Hash*.
3. Enter a name for the malware hash file.
4. Enter the URI for the malware hash file.
5. Click *OK*.

To create a malware hash connector in the CLI:

```
config system external-resource
   edit <external_resource_name>
      set type malware
      set resource<string>
   next
end
```

External block list (threat feed) for policy

You can use the external block list (threat feed) for web filtering and DNS. You can also use external block list (threat feed) in firewall policies.

To create an external IP list object:

Create a plain text file with one IP address, IP address range, or subnet per line. For example:

```
192.168.2.100
172.200.1.4/16
172.16.1.2/24
172.16.8.1-172.16.8.100
2001:0db8::eade:27ff:fe04:9a01/120
2001:0db8::eade:27ff:fe04:aa01-2001:0db8::eade:27ff:fe04:ab01
```

To use an external IP list object:

1. Go to *Security Fabric* > *External Connectors* and click *Create New*.
2. In the *Threat Feeds* section, click *IP Address*.
3. In the *URI of external resource* field, enter the link to the external IP list object.
4. Click *OK*.

Log and report

Add logs for the execution of CLI commands

The `cli-audit-log` option records the execution of CLI commands in system event logs (log ID 44548). In addition to `execute` and `config` commands, `show`, `get`, and `diagnose` commands are recorded in the system event logs.

The `cli-audit-log` data can be recorded on memory or disk and can be uploaded to FortiAnalyzer or a syslog server.

To enable the CLI audit log option:

```
config system global
    set cli-audit-log enable
end
```

To display the logs:

```
# execute log filter device disk
# execute log filter category event
# execute log filter field subtype system
# execute log filter field logid 0100044548
# execute log display
```

Other new features and enhancements

- Real-time logging to FortiAnalyzer
- TLS 1.3 is now supported.
- New FortiProxy VMware deployments now have two disks, one for logging and one for web caching.
- More FortiView widgets are available to add to the dashboard.
- The Content Analyses log is now available in the GUI.
- The TLS fingerprint library can now be uploaded or downloaded in the CLI and GUI.
- You can now use the Policy Lookup tool to find a specific policy.
- You can now use DNS translation.
- You can now use the x-auth-user from the HTTP header when configuring an authentication scheme.
- User authentication was improved for large deployments.
- The dedicated management interface is now available for NAT mode.
- The RAPTOR scheme can now be used in authentication scripts.
- You can now use the forwarding server without DNS lookup.
- New CLI commands let you display statistics for explicit web proxy and SSH proxy traffic.
- You can now manage the blocked-image cache in the GUI.

Product integration and support

Web browser support

The following web browsers are supported by FortiProxy 7.0.0:

- 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
- FortiManager 7.0.2

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 to allocate to the VM.
4. From the VM console, configure the interface, routing, and DNS for GUI or CLI access to the new VM and its access to FortiGuard.
5. Upload the VM license file using the GUI or CLI
6. Restore the configuration using the CLI or GUI.

Downgrading the FortiProxy VM

If you are downgrading from FortiProxy 7.0.0 or later to FortiProxy 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 7.0.0.

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

Bug ID	Description
682415	A web filter configured to block the adult category for HTTPS allows packets to leak through.
719681	WAD workers use too much memory.
721039	Microsoft Teams and Whereby video streaming is being disconnected briefly and randomly for proxy explicit users.
723104	Using SSL deep inspection prevents some internal applications from being accessed when running FortiProxy 6.2.6 in transparent mode with a virtual wire.
724129	Using a proxy-inspection firewall policy (with a proxy-based web filter and SSL deep inspection) with IPS and/or Application Control enabled causes the WebSocket connection to fail.
724149	SSL mirroring does not forward FTPS traffic to the mirroring port.
724670	There is a WAD crash when a user without group information configured logs off.
725628	The WAD process is using too much memory, causing the device to enter conserve mode.
726270	WAD uses either SNI or CNAME as the host name to check the web filter, instead of the actual host name.
726999	WAD crashes cause Internet access to fail.
728790	The ICAP client needs to be improved.
729538	The antivirus log shows the action as “passthrough” instead of “block.”
729544	When the web filter profile and the ICAP profile are used together, the web filter profile rule is ignored.
730042	The ICAP client crashes when traffic is sent from the ICAP client to the ICAP server.
731296	Blocking an oversize file in transparent proxy mode causes the session to be suspended without a replacement message or antivirus UTM log message.
732375	WAD encounters a signal-6 crash infrequently.
736218	In WAN optimization mode, expired certificates are not blocked.
736870	WAD crashes with a signal-6 error when an HTTP transparent policy is being used.
737737	When using explicit proxy, there are WAD signal 11 crashes.
739871	The default wildcard FQDN and default FQDN addresses need to be migrated correctly during an upgrade.

Bug ID	Description
739950	When proxy HTTPS deep-inspection is enabled, TLS 1.2 renegotiation fails.
740249	A memory corruption problem needs to be fixed.
740298	The `config ssl-exempt` settings are being ignored.
741660	When the LDAP server is slow to respond, the connection times out and disconnects.

Known issues

FortiProxy 7.0.0 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.

www.fortinet.com