Administration Guide

FortiProxy 7.2.8

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

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

January 19, 2024
FortiProxy 7.2.8 Administration Guide
45-728-980930-202401119

TABLE OF CONTENTS

Change log

<table>
<tr><th>Date</th><th>Change Description</th></tr>
<tr><td>2023-12-08</td><td>Initial release.</td></tr>
<tr><td>2023-12-15</td><td>Updated Create or edit a traffic-shaping policy on page 164.</td></tr>
<tr><td>2024-01-03</td><td>Added HA virtual cluster setup on page 473.
Updated HA on page 469.</td></tr>
<tr><td>2024-01-04</td><td>Updated HA virtual cluster setup on page 473.</td></tr>
<tr><td>2024-01-05</td><td>Moved the license sharing topic to the License Sharing Deployment Guide.</td></tr>
<tr><td>2024-01-10</td><td>Added the following topics:
Transparent mode management on page 467
HA cluster out-of-band management on page 476</td></tr>
<tr><td>2024-01-11</td><td>Updated the following topics:
Transparent and NAT/route modes on page 14
HA on page 469</td></tr>
<tr><td>2024-01-12</td><td>Added Using FortiNDR inline scanning with antivirus on page 273.
Updated Create or edit an antivirus profile on page 265.</td></tr>
<tr><td>2024-01-18</td><td>Added Restricted SaaS access on page 66.
Updated the following topics:
HA cluster out-of-band management on page 476
Transparent mode management on page 467</td></tr>
<tr><td>2024-01-19</td><td>Updated Using FortiNDR inline scanning with antivirus on page 273.</td></tr>
</table>

Introduction

FortiProxy provides a secure web gateway that protects against web attacks using URL filtering, visibility and control of encrypted web traffic through SSL and SSH inspection, and the application of granular web application policies. Flexible deployment modes cover inline, explicit, and transparent deployments.

- Application Control allows you to identify and control applications on networks and endpoints regardless of the port, protocol, and IP address used. It gives you unmatched visibility and control over application traffic, even traffic from unknown applications and sources.
- SSL and SSH inspection allows you to determine which inspection method will be applied to SSH and SSL traffic; identify how to treat invalid, unsupported or untrusted SSL certificates; and configure which web sites or web site categories are exempt from SSL inspection.
- Web filtering provides web URL filtering to block access to harmful, inappropriate, and dangerous web sites that can contain phishing/pharming attacks, malware such as spyware, or objectionable content that can expose your organization to legal liability. Based on automatic research tools and targeted research analysis, real-time updates enable you to apply highly-granular policies that filter web access based on 78 web content categories, over 45 million rated web sites, and more than two billion web pages—all continuously updated.
- The FortiProxy data leak prevention (DLP) system allows you to prevent sensitive data from leaving your network. When you define sensitive data patterns, data matching these patterns will be blocked or logged and allowed when passing through the FortiProxy unit. You configure the DLP system by creating individual filters based on file type, file size, a regular expression, an advanced rule, or a compound rule, in a DLP sensor and assign the sensor to a security policy. Although the primary use of the DLP feature is to stop sensitive data from leaving your network, it can also be used to prevent unwanted data from entering your network and to archive some or all of the content passing through the FortiProxy unit.

The FortiProxy unit also provides WAN optimization, web caching, and WCCP. FortiProxy WAN optimization and web caching improve performance and security of traffic passing between locations on your wide area network (WAN) or from the Internet to your web servers. You can use the FortiProxy unit as an explicit FTP and web proxy server. In addition, you can add web caching to any HTTP sessions including WAN optimization, explicit web proxy, and other HTTP sessions.

Supported protocols

Application layer security

- SSH
- FTP/FTPS/FTPoHTTP/FTPoHTTPConnect
- SMTP/SMTPS
- IMAP/IMAPS
- POP3/POP3S
- CIFS/SMB
- MAPI/MAPIoRPC/MAPIoHTTPS
- DNS

- ICAP/WCCP
- SCP/SFTP

VPN

- IPsec/SSL VPNs

About this document

This document contains the following sections:

Appendices:

Deployments

This section describes the following:

- Transparent and NAT/route modes on page 14
- Web proxy on page 15
- WAN optimization on page 20
- Web caching on page 24
- WCCP on page 27

Transparent and NAT/route modes

A FortiProxy unit can operate in either NAT/route mode or transparent mode.

In NAT/route mode, a FortiProxy unit is installed as a gateway or router between multiple networks, such as a private network and the internet. One function of NAT/route mode is to allow the FortiProxy to hide the IP addresses on the private network using NAT.

The FortiProxy operates in layer 2 to forward traffic between network devices such as routers, firewalls, and switches. For example. it can be installed inline between a router and a switch to perform security scanning without changing the network topology or modifying the IP addresses.

Transparent mode is used primarily when there is a need to increase network protection but changing the configuration of the network itself is impractical. When you add a FortiProxy that is in transparent mode to a network, it only needs to be provided with a management IP address in order to access the device. It is recommended to configure a dedicated management interface when out-of-band management is required in transparent mode. See Transparent mode management on page 467.

Changing the operation mode removes most configurations, including any policies and address objects. To keep your configuration, back it up before changing the mode.

To back up your configuration in the GUI:

1. Click on the user name and select *Configuration* > *Backup*.
2. Select where to store the backup file, *Local PC* or *USB Disk* (if available).
3. Optionally, enable *Encryption* and enter a password.
4. Click *OK*.

To back up your configuration in the CLI:

```
# execute backup {config | full-config} {flash | ftp | management-
     station | sftp | tftp | usb | usb-mode} ...
```

To change from NAT/route mode to transparent mode:

```
config system settings
    set opmode transparent
    set manageip <IP_address>
    set gateway <gateway_address>
end
```

The gateway setting is optional, but after the operation mode has been changed, the gateway configuration is in the static router settings:

```
config router static
    edit <seq-num>
        set gateway <IP_address>
    next
end
```

To change from transparent mode to NAT/route mode:

```
config system settings
    set opmode nat
    set ip <IP_address>
    set device <interface>
    set gateway <gateway_address>
end
```

The IP and device settings are mandatory, and the gateway setting is optional. After the operation mode is changed, the IP address configuration is in the interface settings and the gateway and device configurations are in the static router settings:

```
config system interface
    edit <interface>
        set ip <IP_address>
    next
end
```

```
config router static
    edit <seq-num>
        set gateway <IP_address>
        device <interface>
    next
end
```

Web proxy

Web proxy covers both transparent proxy and explicit proxy.

This section covers the following topics:

- Web proxy concepts
- Explicit web proxy concepts
- Transparent web proxy concepts
- Explicit web proxy topologies

Web proxy concepts

This section covers the following concepts that apply to both transparent proxy and explicit proxy:

- Proxy policy
- Proxy authentication
- Proxy addresses
- Web proxy firewall services and service groups
- Learn client IP

Proxy policy

Any time a security profile that uses a proxy is enabled, you need to configure the proxy options. Certain inspections defined in security profiles require that the traffic be held in proxy while the inspection is carried out, and the proxy options define how the traffic will be processed and to what level the traffic will be processed. In the same way that there can be multiple security profiles of a single type, there can also be a number of unique proxy option profiles so that, as the requirements for a policy differ from one policy to the next, you can also configure a different proxy option profile for each individual policy or you can use one profile repeatedly.

The proxy options support the following protocols:

- HTTP
- FTP
- CIFS
- SSH

The configuration for each of these protocols is handled separately.

Proxy authentication

Authentication is separated from authorization for user-based policies. You can add authentication to proxy policies to control access to the policy and to identify users and apply different UTM features to different users. The described authentication methodology works with explicit web proxy and transparent proxy.

Authentication of web proxy sessions uses HTTP basic and digest authentication as described in RFC 2617 (HTTP Authentication: Basic and Digest Access Authentication) and prompts the user for credentials from the browser allowing individual users to be identified by their web browser instead of IP address. HTTP authentication allows the FortiProxy unit to distinguish between multiple users accessing services from a shared IP address.

The authentication rule table defines how to identify user-ID. It uses the match factors:

- Protocol
- Source address

For one address and protocol, there is only one authentication rule. It is possible to configure multiple authentication methods for one address. The client browser will chose one authentication method from the authentication methods list, but you cannot control which authentication method will be chosen by the browser.

Proxy addresses

Proxy addresses are used for both transparent web proxy and explicit web proxy.

In some respects, they can be like FQDN addresses in that they refer to an alphanumeric string that is assigned to an IP address, but then they go an additional level of granularity by using additional information and criteria to further specify locations or types of traffic within the web site itself.

Proxy address group

In the same way that IPv4 and IPv6 addresses can only be grouped together, proxy addresses can only be grouped with other proxy addresses. Unlike other address groups, the proxy address groups are further divided into source address groups and destination address groups.

Web proxy firewall services and service groups

Web proxy services are similar to standard firewall services. You can configure web proxy services to define one or more protocols and port numbers that are associated with each web proxy service. Web proxy services can also be grouped into web proxy service groups.

One way in which web proxy services differ from firewall services is the protocol type you can select. The following protocol types are available:

- ALL
- CONNECT
- FTP
- HTTP
- SOCKS-TCP
- SOCKS-UDP

Learn client IP

If there is another NATing device between the FortiProxy unit and the client (browser), this feature can be used to identify the real client in spite of the address translation. Knowing the actual client is imperative in cases where authorization is taking place.

Explicit web proxy concepts

The following is information that is specific to explicit proxy. Any information that is common to web proxy in general is covered in Web proxy concepts on page 16.

You can use the FortiProxy explicit web proxy to enable explicit proxying of IPv4 and IPv6 HTTP and HTTPS traffic on one or more FortiProxy interfaces. The explicit web proxy also supports proxying FTP sessions from a web browser and proxy auto-config (PAC) to provide automatic proxy configurations for explicit web proxy users. From the CLI you can also configure the explicit web proxy to support SOCKS sessions from a web browser. The explicit web and FTP proxies can be operating at the same time on the same or on different FortiProxy interfaces.

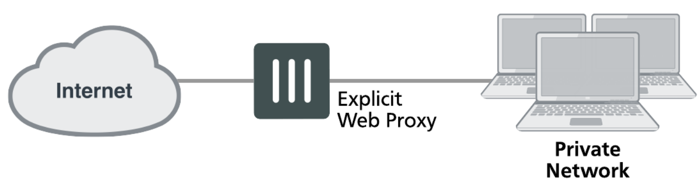
In most cases, you would configure the explicit web proxy for users on a network by enabling the explicit web proxy on the FortiProxy interface connected to that network. Users on the network would configure their web browsers to use a proxy server for HTTP and HTTPS, FTP, or SOCKS and set the proxy server IP address to the IP address of the FortiProxy interface connected to their network. Users could also enter the PAC URL into their web browser PAC configuration to automate their web proxy configuration using a PAC file stored on the FortiProxy unit.

Enabling the explicit web proxy on an interface connected to the Internet is a security risk because anyone on the Internet who finds the proxy could use it to hide their source address.

If the FortiProxy unit is operating in transparent mode, users would configure their browsers to use a proxy server with the FortiProxy management IP address.

The web proxy receives web browser sessions to be proxied at FortiProxy interfaces with the explicit web proxy enabled. The web proxy uses FortiProxy routing to route sessions through the FortiProxy unit to a destination interface. Before a session leaves the exiting interface, the explicit web proxy changes the source addresses of the session packets to the IP address of the exiting interface. When the FortiProxy unit is operating in transparent mode, the explicit web proxy changes the source addresses to the management IP address. You can configure the explicit web proxy to keep the original client IP address.

Example explicit web proxy topology



To allow all explicit web proxy traffic to pass through the FortiProxy unit you can set the explicit web proxy default firewall policy action to *ACCEPT*. However, in most cases you would want to use security policies to control explicit web proxy traffic and apply security features such as access control/authentication, virus scanning, web filtering, application control, and traffic logging. You can do this by keeping the default explicit web proxy security policy action to *DENY* and then adding web-proxy security policies.

You can also change the explicit web proxy default security policy action to accept and add explicit web proxy security policies. If you do this, sessions that match web-proxy security policies are processed according to the security policy settings. Connections to the explicit web proxy that do not match a web-proxy security policy are allowed with no restrictions or additional security processing. **NOTE:** This configuration is not recommended and is not a best practice.

The explicit web-proxy can accept VIP addresses for destination addresses. If an external IP matches a VIP policy, the IP is changed to the mapped-IP of the VIP.

Web-proxy policies can selectively accept or deny traffic, apply authentication, enable traffic logging, and use security profiles to apply virus scanning, web filtering, IPS, application control, DLP, and SSL/SSH inspection to explicit web proxy traffic.

You cannot configure IPsec, SSL VPN, or traffic shaping for explicit web proxy traffic. Web proxy policies can only include firewall addresses not assigned to a FortiProxy unit interface or with interface set to *any*. (On the web-based manager, you must set the interface to *any*. In the CLI you must unset the associated interface.)

Authentication of explicit web proxy sessions uses HTTP authentication and can be based on the user’s source IP address or on cookies from the user’s web browser.

To use the explicit web proxy, you must add the IP address of a FortiProxy interface on which the explicit web proxy is enabled and the explicit web proxy port number (default 8080) to the proxy configuration settings of their web browsers.

You can also enable web caching for explicit web proxy sessions.

Transparent web proxy concepts

In addition to the explicit web proxy, the FortiProxy unit supports a transparent web proxy. While it does not have as many features as explicit web proxy, the transparent proxy has the advantage that nothing needs to be done on the user’s system to forward supported web traffic over to the proxy. There is no need to reconfigure the browser or publish a PAC file. Everything is transparent to the end user, hence the name. This makes it easier to incorporate new users into a proxy deployment.

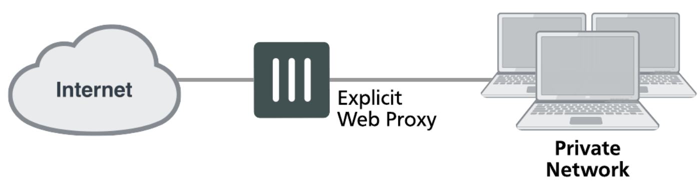
You can use the transparent proxy to apply web authentication to HTTP traffic accepted by a firewall policy.

Normal FortiProxy authentication is IP-address based. Users are authenticated according to their IP address and access is allowed or denied based on this IP address. On networks where authentication based on IP address will not work, you can use the transparent web proxy to apply web authentication that is based on the user's browser and not on their IP address. This authentication method allows you to identify individual users even if multiple users on your network are connecting to the FortiProxy unit from the same IP address.

Explicit web proxy topologies

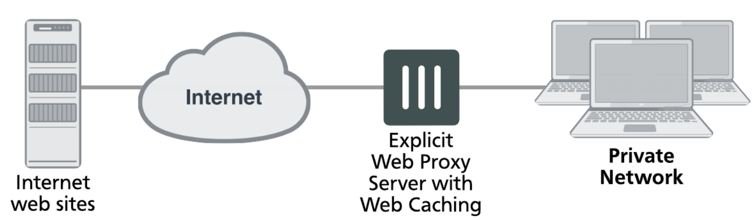
You can configure a FortiProxy unit to be an explicit web proxy server for Internet web browsing of IPv4 and IPv6 web traffic. To use the explicit web proxy, users must add the IP address of the FortiProxy interface configured for the explicit web proxy to their web browser proxy configuration.

Explicit web proxy topology



If the FortiProxy unit supports web caching, you can also add web caching to the security policy that accepts explicit web proxy sessions. The FortiProxy unit then caches Internet web pages on a hard disk to improve web browsing performance.

Explicit web proxy with web caching topology



WAN optimization

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, web 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. Web caching stores web pages o FortiProxy units to reduce latency and delays between the WAN and web servers. SSL offloading offloads SSL decryption and encryption from web servers onto FortiProxy SSL acceleration hardware. Secure tunneling secures traffic as it crosses the WAN.

You can apply different combinations of these WAN optimization techniques to a single traffic stream depending on the traffic type. For example, you can apply byte caching and secure tunneling to any TCP traffic. For HTTP and HTTPS traffic, you can also apply protocol optimization and web caching.

You can configure a FortiProxy unit to be an explicit web proxy server for both IPv4 and IPv6 traffic and an explicit FTP proxy server. Users on your internal network can browse the Internet through the explicit web proxy server or connect to FTP servers through the explicit FTP proxy server. You can also configure these proxies to protect access to web or FTP servers behind the FortiProxy unit using a reverse proxy configuration.

Web caching can be applied to any HTTP or HTTPS traffic, this includes normal traffic accepted by a security policy, explicit web proxy traffic, and WAN optimization traffic.

You can also configure a FortiProxy unit to operate as a Web Cache Communication Protocol (WCCP) client or server. WCCP provides the ability to offload web caching to one or more redundant web caching servers.

FortiProxy units can also apply security profiles to traffic as part of a WAN optimization, explicit web proxy, explicit FTP proxy, web cache and WCCP configuration. Security policies that include any of these options can also include settings to apply all forms of security profiles supported by your FortiProxy unit.

To check how much memory has been allocated for the WAN-optimization daemon (WAD), use the `diagnose wad memory track [<mem-id>]` command.

WAN optimization supports TLS 1.3.

WAN optimization transparent mode

WAN optimization is transparent to users. This means that with WAN optimization in place, clients connect to servers in the same way as they would without WAN optimization. However, servers receiving packets after WAN optimization “see” different source addresses depending on whether or not transparent mode is selected for WAN optimization. If transparent mode is selected, WAN optimization keeps the original source address of the packets, so servers appear to receive traffic directly from clients. Routing on the server network should be configured to route traffic with client source IP addresses from the server-side FortiProxy unit to the server and back to the server-side FortiProxy unit.

Some protocols, for example CIFS, may not function as expected if transparent mode is not selected. In most cases, for CIFS WAN optimization you should select transparent mode and make sure the server network can route traffic as described to support transparent mode.

If transparent mode is not selected, the source address of the packets received by servers is changed to the address of the server-side FortiProxy unit interface that sends the packets to the servers. So servers appear to receive packets from the server-side FortiProxy unit. Routing on the server network is simpler in this case because client addresses are not involved. All traffic appears to come from the server-side FortiProxy unit and not from individual clients.

Do not confuse WAN optimization transparent mode with FortiProxy transparent mode. WAN optimization transparent mode is similar to source NAT. FortiProxy transparent mode is a system setting that controls how the FortiProxy unit processes traffic. See Transparent and NAT/route modes on page 14.

WAN optimization topologies

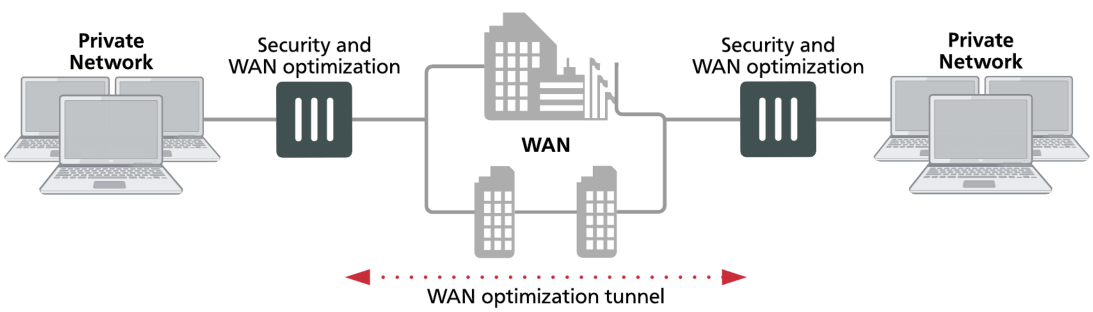
The WAN optimization topologies are described in the following sections:

- Basic WAN optimization topology
- Out-of-path WAN optimization topology
- Topology for multiple networks
- WAN optimization with web caching

Basic WAN optimization topology

The basic FortiProxy WAN optimization topology consists of two FortiProxy units operating as WAN optimization peers intercepting and optimizing traffic crossing the WAN between the private networks.

Security device and WAN optimization topology



FortiProxy units can be deployed as security devices that protect private networks connected to the WAN and also perform WAN optimization. In this configuration, the FortiProxy units are configured as typical security devices for the private networks and are also configured for WAN optimization. The WAN optimization configuration intercepts traffic to be optimized as it passes through the FortiProxy unit and uses a WAN optimization tunnel with another FortiProxy unit to optimize the traffic that crosses the WAN.

You can also deploy WAN optimization on single-purpose FortiProxy units that only perform WAN optimization. In the out of path WAN optimization topology shown below, FortiProxy units are located on the WAN outside of the private networks. You can also install the WAN optimization FortiProxy units behind the security devices on the private networks.

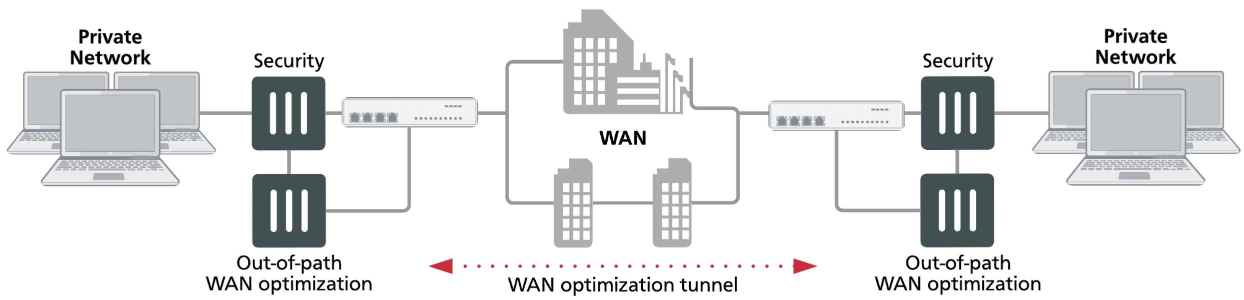
The WAN optimization configuration is the same for FortiProxy units deployed as security devices and for single-purpose WAN optimization FortiProxy units. The only differences would result from the different network topologies.

Out-of-path WAN optimization topology

In an out-of-path topology, one or both of the FortiProxy units configured for WAN optimization are not directly in the main data path. Instead, the out-of-path FortiProxy unit is connected to a device on the data path, and the device is configured to redirect sessions to be optimized to the out-of-path FortiProxy unit.

The following out-of-path FortiProxy units are configured for WAN optimization and connected directly to FortiProxy units in the data path. The FortiProxy units in the data path use a method such as policy routing to redirect traffic to be optimized to the out-of-path FortiProxy units. The out-of-path FortiProxy units establish a WAN optimization tunnel between each other and optimize the redirected traffic.

Out-of-path WAN optimization



One of the benefits of out-of-path WAN optimization is that out-of-path FortiProxy units only perform WAN optimization and do not have to process other traffic. An in-path FortiProxy unit configured for WAN optimization also has to process other non-optimized traffic on the data path.

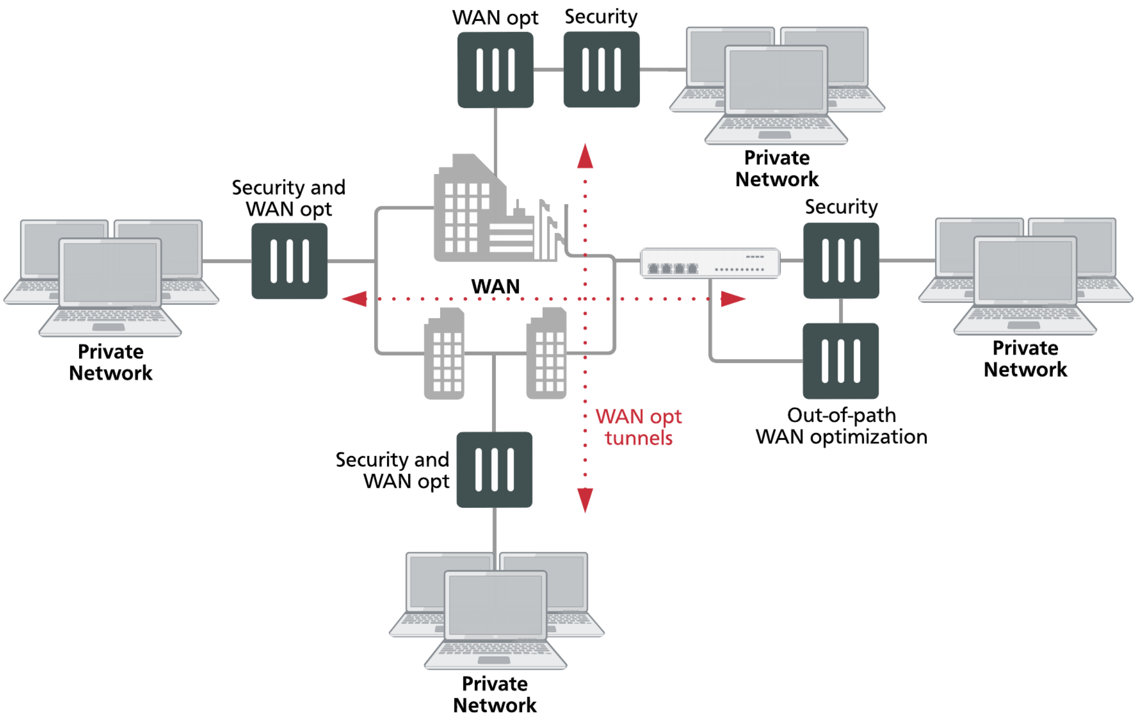
The out-of-path FortiProxy units can operate in NAT/Route or transparent mode.

Other out-of-path topologies are also possible. For example, you can install the out-of-path FortiProxy units on the private networks instead of on the WAN. Also, the out-of-path FortiProxy units can have one connection to the network instead of two. In a one-arm configuration such as this, security policies and routing have to be configured to send the WAN optimization tunnel out the same interface as the one that received the traffic.

Topology for multiple networks

As shown in the following figure, you can create multiple WAN optimization configurations between many private networks. Whenever WAN optimization occurs, it is always between two FortiProxy units, but you can configure any FortiProxy unit to perform WAN optimization with any of the other FortiProxy units that are part of your WAN.

WAN optimization among multiple networks

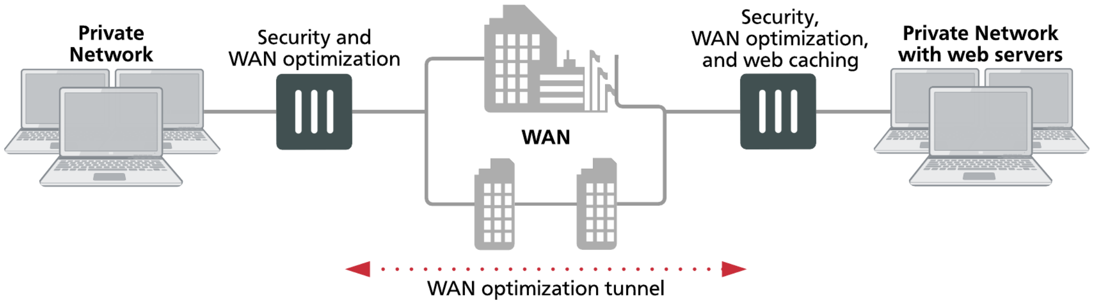


You can also configure WAN optimization between FortiProxy units with different roles on the WAN. FortiProxy units configured as security devices and for WAN optimization can perform WAN optimization as if they are single-purpose FortiProxy units just configured for WAN optimization.

WAN optimization with web caching

You can add web caching to a WAN optimization topology when users on a private network communicate with web servers located across the WAN on another private network.

WAN optimization with web-caching topology



The topology above is the same as that shown in Basic WAN optimization topology on page 21 with the addition of web caching to the FortiProxy unit in front of the private network that includes the web servers. You can also add web caching to the FortiProxy unit that is protecting the private network. In a similar way, you can add web caching to any WAN optimization topology.

Web caching

Web caching is a form of object caching that accelerates web applications and web servers by reducing bandwidth usage, server load, and perceived latency.

Web caching involves storing HTML pages, images, videos, servlet responses, and other web-based objects for later retrieval. These objects are stored in the web cache storage location defined by the `config system storage` command. You can also go to *System > Advanced* to view the storage locations on the FortiProxy unit hard disks in the *System Storage Setting* section.

There are three significant advantages to using web caching to improve HTTP performance:

- Reduced bandwidth consumption because fewer requests and responses go over the WAN or Internet
- Reduced web server load because there are fewer requests for web servers to handle
- Reduced latency because responses for cached requests are available from a local FortiProxy unit instead of from across the WAN or Internet

When enabled in a web-caching policy, the FortiProxy unit caches HTTP traffic processed by that policy. A web-caching policy specifies the source and destination addresses and destination ports of the traffic to be cached.

Web caching caches compressed and uncompressed versions of the same file separately. If the HTTP considers the compressed and uncompressed versions of a file as the same object, only the compressed or uncompressed file will be cached.

You can deploy a mix of hardware and virtual appliances, operating together and managed from a common centralized management platform. FortiProxy high-performance web-caching virtual appliances address bandwidth saturation, high latency, and poor performance caused by caching popular internet content locally for carriers, service providers, enterprises and educational networks.

The FortiProxy unit supports the following:

- KVM hypervisor
- VMware hypervisor
- Xen hypervisor
- Hyper-V hypervisor

Collaboration web caching

Collaboration web caching allows multiple FortiProxy units within one organization to share all cached objects.

Cache-sharing requests are broadcasted from one FortiProxy unit to one or more destination FortiProxy units to prevent loops. The first FortiProxy unit to respond to a cache-sharing request is accepted, and the rest of the responses are ignored. Cache data from a remote (destination) FortiProxy unit participating in collaboration web caching is not saved to the local (source) FortiProxy disk; instead the data is saved to the local memory cache.

NOTE: Sending and receiving cache-sharing requests can impact the performance of FortiProxy units that participate in collaboration web caching. The performance impact depends on how many cache-sharing requests are being handled.

Use the following commands to connect a source FortiProxy unit to a destination FortiProxy unit for collaboration web caching:

```
config wanopt cache-service
   set collaboration enable
   set device-id “fch-1”
   config dst-peer
      edit “peer-id”
         set ip xxx.xxx.xxx.xxx
      next
   end
end
```

Use the following commands to identify all FortiProxy units participating in collaboration web caching:

```
config wanopt cache-service
   set collaboration enable
   set device-id “peer-id”
   set acceptable-peers any
end
```

Use the following commands to allow a FortiProxy unit to accept cache-sharing requests:

```
config wanopt cache-service
   set collaboration enable
   set acceptable-peers any
end
```

For example, use the following commands to allow a destination FortiProxy unit to accept cache-sharing requests from a single source FortiProxy unit:

```
config wanopt cache-service
   set collaboration enable
   set acceptable-peers src-peer
   set device-id “peer-id”
   config src-peer
```

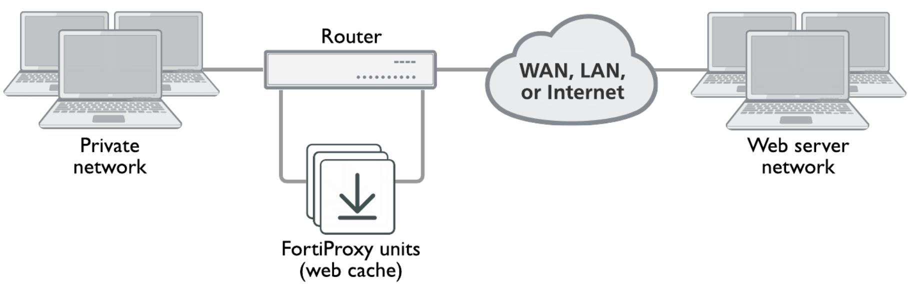
```
        edit "fch-1"
            set ip xxx.xxx.xxx.xxx
        next
    end
```

Web-caching topologies

FortiProxy web caching involves one or more FortiProxy units installed between users and web servers. The FortiProxy unit can operate in both Network Address Translator (NAT) and transparent modes. The FortiProxy unit intercepts HTTP requests for web objects accepted by web cache policies, requests the web objects from the web servers, caches the web objects, and returns the web objects to the users. When the FortiProxy unit intercepts subsequent requests for cached web pages, the FortiProxy unit contacts the destination web server just to check for changes.

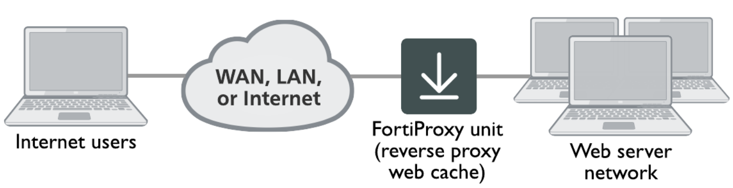
Most commonly the topology uses a router to route HTTP and HTTPS traffic to be cached to one or more FortiProxy units. Traffic that should not be cached bypasses the FortiProxy units. This is a scalable topology that allows you to add more FortiProxy units if usage increases.

Web-caching topology with web traffic routed to FortiProxy units



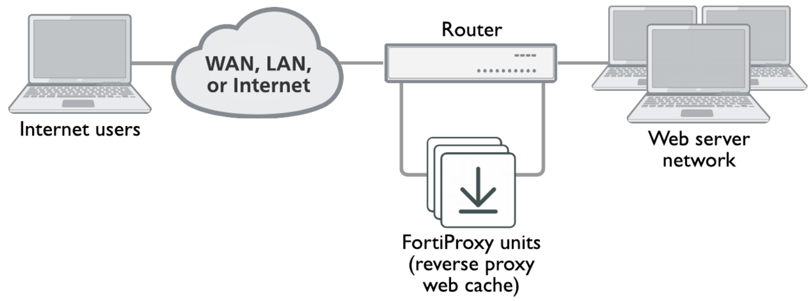
You can also configure reverse proxy web caching. In this configuration, users on the Internet browse to a web server installed behind a FortiProxy unit. The FortiProxy unit intercepts the web traffic (HTTP and HTTPS) and caches pages from the web server. Reverse proxy web caching on the FortiProxy unit reduces the number of requests that the web server must handle, leaving it free to process new requests that it has not serviced before. Because all traffic is to be cached, the FortiProxy unit can be installed in transparent mode directly between the web server and the Internet.

Reverse proxy web-caching topology



The reverse proxy configuration can also include a router to route web traffic to a group of FortiProxy units operating in transparent mode. This solution for reverse proxy web caching is also scalable.

Reverse proxy web-caching topology with web traffic routed to FortiProxy unit



When web objects and video are cached on the FortiProxy hard disk, the FortiProxy unit returns traffic back to client using the cached object from cache storage. The clients do not connect directly to the server.

When web objects and video are not available in the FortiProxy hard disk, the FortiProxy unit forwards the request to original server. If the HTTP response indicates it is a object that can be cached, the object is forwarded to cache storage, and the HTTP request is served from cache storage. Any other HTTP request for the same object will be served from cache storage as well.

The FortiProxy unit forwards HTTP responses that cannot be cached from the server back to the client that originated the HTTP request.

All non-HTTP traffic and HTTP traffic that is not cached by FortiProxy will pass through the unit. HTTP traffic is not cached by the FortiProxy unit if a web cache policy has not been added for it.

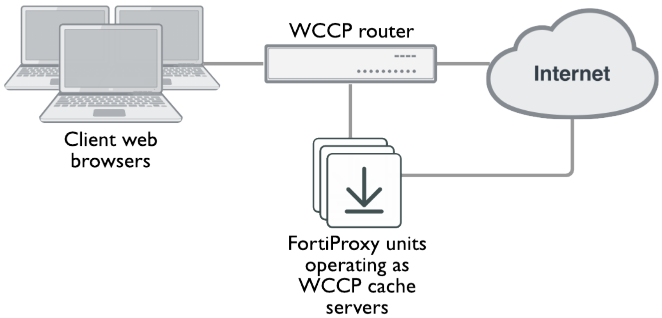
WCCP

You can also configure a FortiProxy unit to operate as a Web Cache Communication Protocol (WCCP) client. WCCP provides the ability to offload web caching to one or more redundant web-caching servers.

WCCP topology

You can operate a FortiProxy unit as a WCCP cache engine. As a cache engine, the FortiProxy unit returns the required cached content to the client web browser. If the cache server does not have the required content, it accesses the content, caches it, and returns the content to the client web browser.

WCCP topology



WCCP is transparent to client web browsers. The web browsers do not have to be configured to use a web proxy.

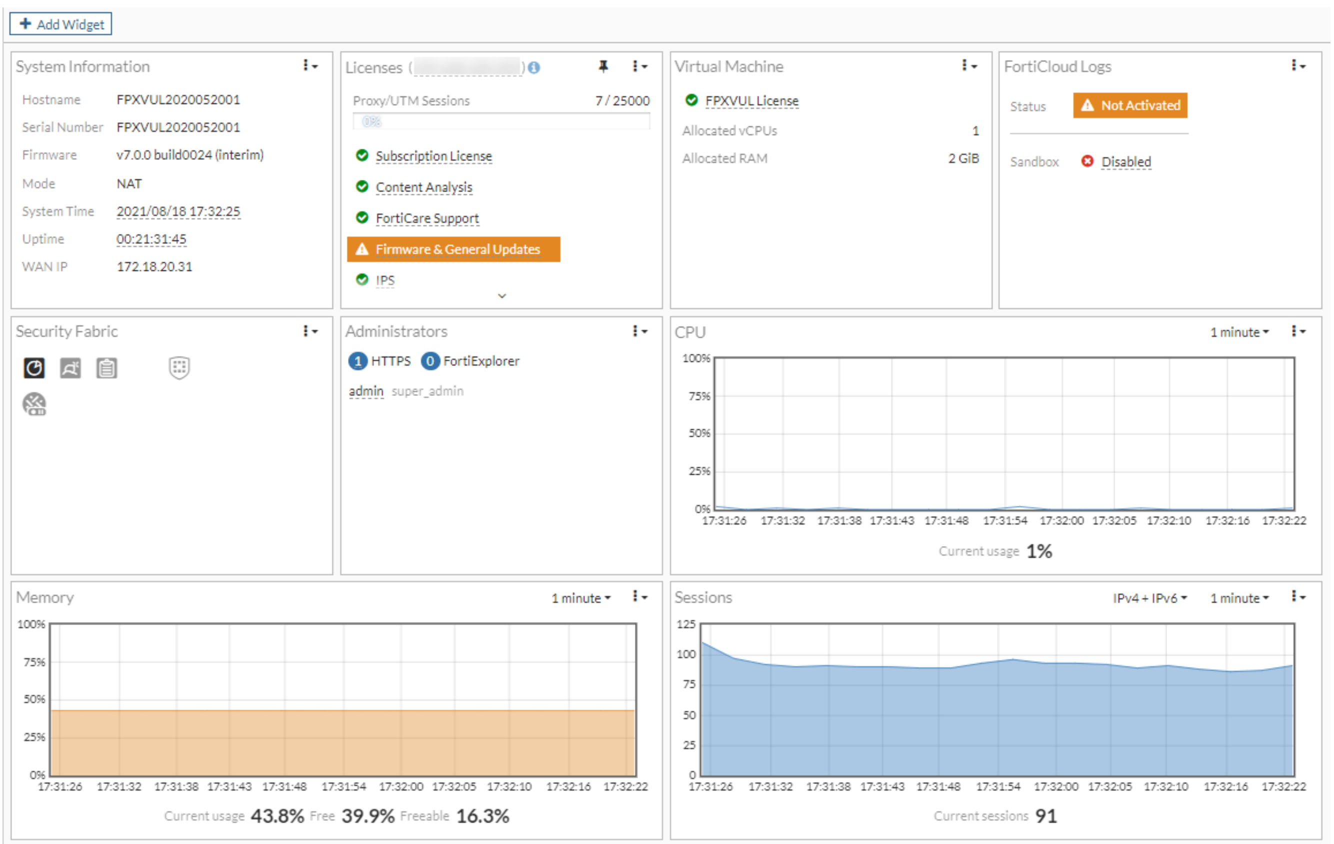
Dashboard

The dashboard provides a location to view real-time system information. By default, the dashboard displays the key statistics of the FortiProxy unit itself, providing the memory and CPU status, licenses, and current number of sessions.

The dashboard provides a Network Operations Center (NOC) view with a focus on alerts. Widgets are interactive; by clicking or hovering over most widgets, you can get additional information or follow links to other pages.

To access the main dashboard, go to *Dashboard > Status*.

Your browser must support JavaScript to view the dashboard.



The following widgets are displayed:

- System Information
- Licenses
- Virtual Machine
- FortiGate Cloud
- Security Fabric

- Administrators
- CPU
- Memory
- Proxy Sessions
- Advanced Threat Protection Statistics

You can add the following FortiView widgets to the dashboard:

- FortiView Applications
- FortiView Cloud Applications
- FortiView Countries/Regions
- FortiView Destination Firewall Objects
- FortiView Destination Interfaces
- FortiView Destination Owners
- FortiView Destinations
- FortiView Interface Pairs
- FortiView Policies
- FortiView Search Phrases
- FortiView Servers
- FortiView Sessions
- FortiView Source Firewall Objects
- FortiView Source Interfaces
- FortiView Sources
- FortiView Sources - WAN
- FortiView Traffic Shaping
- FortiView VPN
- FortiView Web Categories
- FortiView Web Sites

This section describes the following:

- Managing widgets
- System Information widget
- Licenses widget
- Virtual Machine widget
- FortiProxy Cloud widget
- Security Fabric widget
- Administrators widget
- CPU widget
- Memory widget
- Sessions widget
- SSL-VPN widget
- IPSec widget
- Forward Server Monitor widget
- License Sharing Information widget
- License Usage History widget

- Sensor Information widget
- User dropdown menu
- GUI-based global search

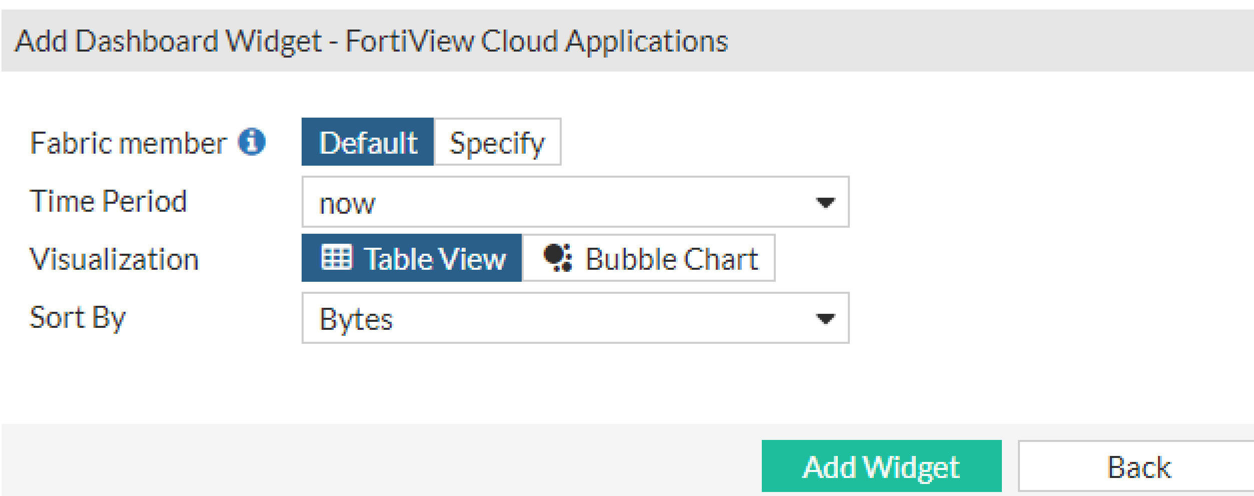
Managing widgets

To rearrange widgets on the dashboard, drag the widgets by their title bars.

All widgets have the following two title bar options:

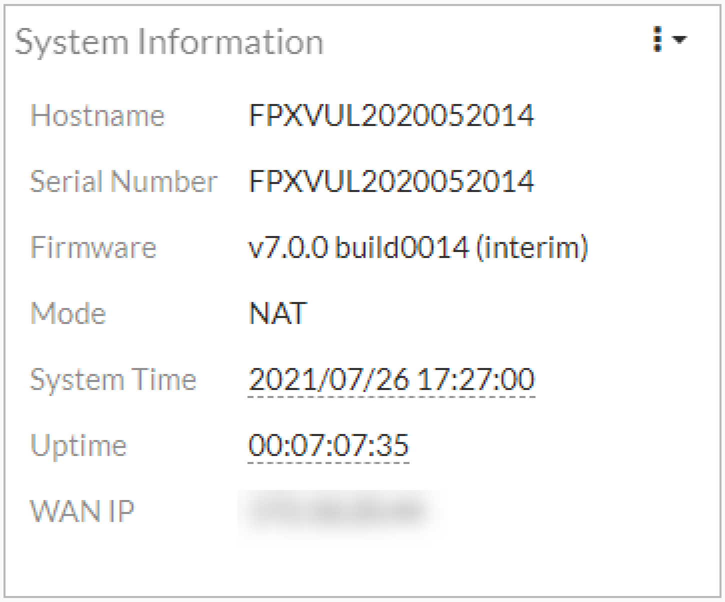
Resize	Select the size of the widget.
Remove	Remove the widget from the dashboard.

To add a FortiView widget to a dashboard:

1. Go to *Dashboard* > *Status*.
2. At the top the dashboard, click *Add Widget*.
3. Click + for the FortiView widget that you want to add.
   The *Add Dashboard Widget*window opens.
   

4. Click *Specify* if you want the widget to monitor all FortiProxy units instead of a single FortiProxy unit.
5. Select the time period to display.
6. Select *Table View* or *Bubble Chart*.
7. Select the *Sort By* value.
8. Click *Add Widget*.
   The new widget is displayed in the main dashboard.
9. Click *Close*.

System Information widget

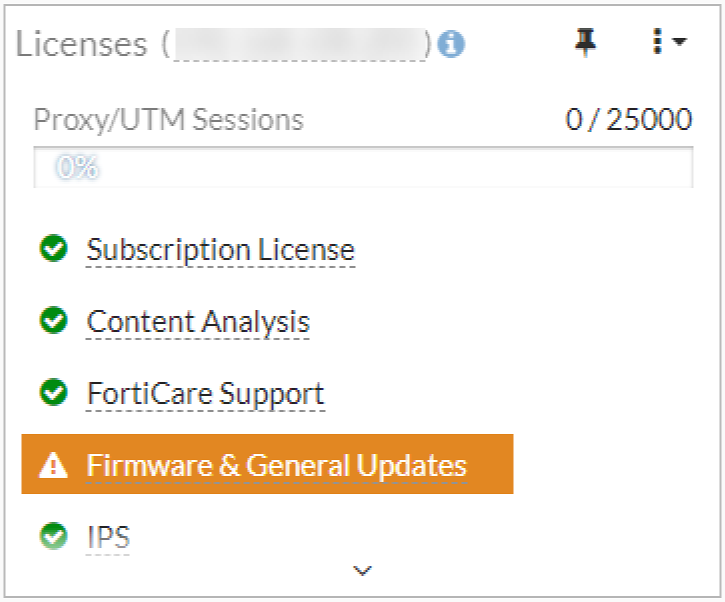


The *System Information* widget displays general system information, such as the FortiProxy unit serial number, firmware version, host name, and system time. Clicking on the widget provides you links to two other pages:

- To configure settings, go to *System* > *Settings*.
- To update the firmware version, go to *System* > *Firmware*.

Hostname	The host name of the current FortiProxy unit.
Serial Number	The serial number of the FortiProxy unit. The serial number is specific to that unit and does not change with firmware upgrades.
Firmware	The version of the firmware currently installed on the FortiProxy unit. To update the firmware version, go to *System* > *Firmware*. By installing an older firmware image, some system settings might be lost. You should always back up your configuration before changing the firmware image. To back up your configuration, go to *<user_name>* > *Configuration* > *Backup*. You must register your unit with Fortinet Customer Support to access firmware updates for your model. For more information, go to https://support.fortinet.com or contact Fortinet Customer Service & Support.
Mode	The current operating mode of the FortiProxy unit. A unit can operate in NAT mode or transparent mode.
System Time	The current date and time according to the FortiProxy unit's internal clock.
Uptime	The time in days, hours, and minutes since the FortiProxy unit was started.
WAN IP	The WAN IP address and location. Additionally, if the WAN IP is blocked in the FortiGuard server, there is a notification in the notification area, located in the upper right-hand corner of the Dashboard. Clicking on the notification opens a window with the relevant blocklist information.

Licenses widget

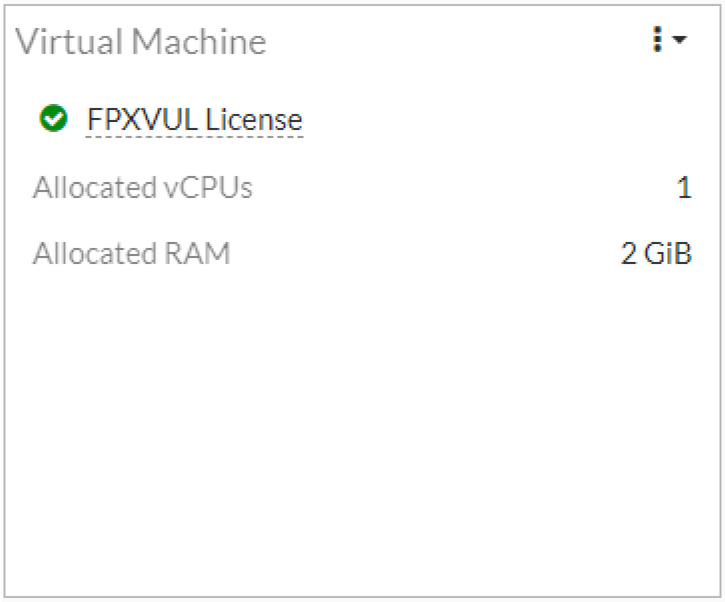


The *Licenses* widget displays the statuses of your licenses and FortiGuard subscriptions. It also allows you to update your device’s registration status and FortiGuard definitions.

Hovering over the Licenses widget displays status information for Subscription License, Content Analysis, FortiCare Support, IPS, AntiVirus, and Web Filtering. Clicking on each license provides links to renew, register, subscribe, or add your FortiCare contract number.

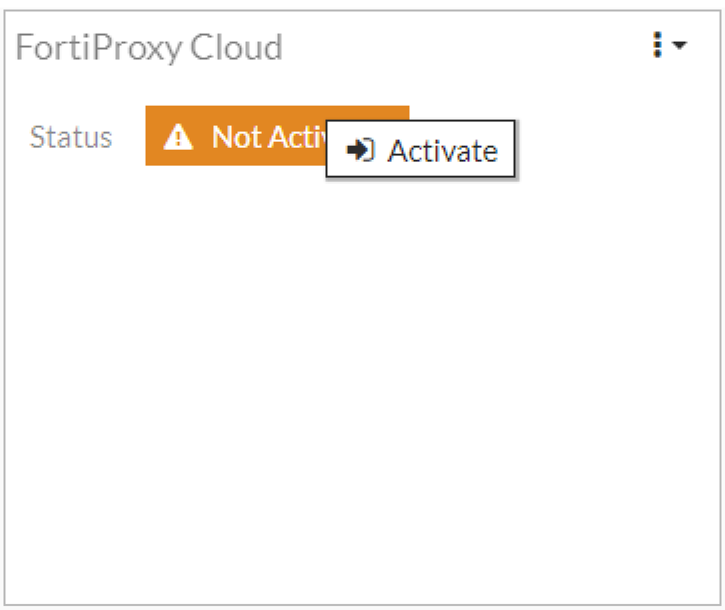
Go to *System > FortiGuard* to register for FortiCare Support, upgrade databases, and view details. See FortiGuard on page 502.

Virtual Machine widget



This widget displays license information, number of allocated vCPUs, and how much RAM has been allocated.

FortiProxy Cloud widget



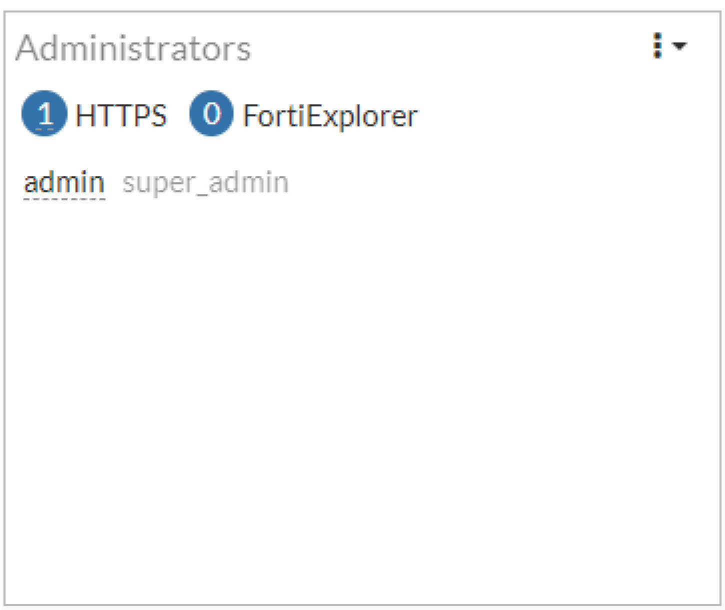
This widget displays the FortiProxy Cloud status and provides a link to activate FortiProxy Cloud.

Security Fabric widget

You can hover over the icons along the top of the Security Fabric widget to get a quick view of the status of various components of in the Security Fabric. Hover over the host name to display system information.

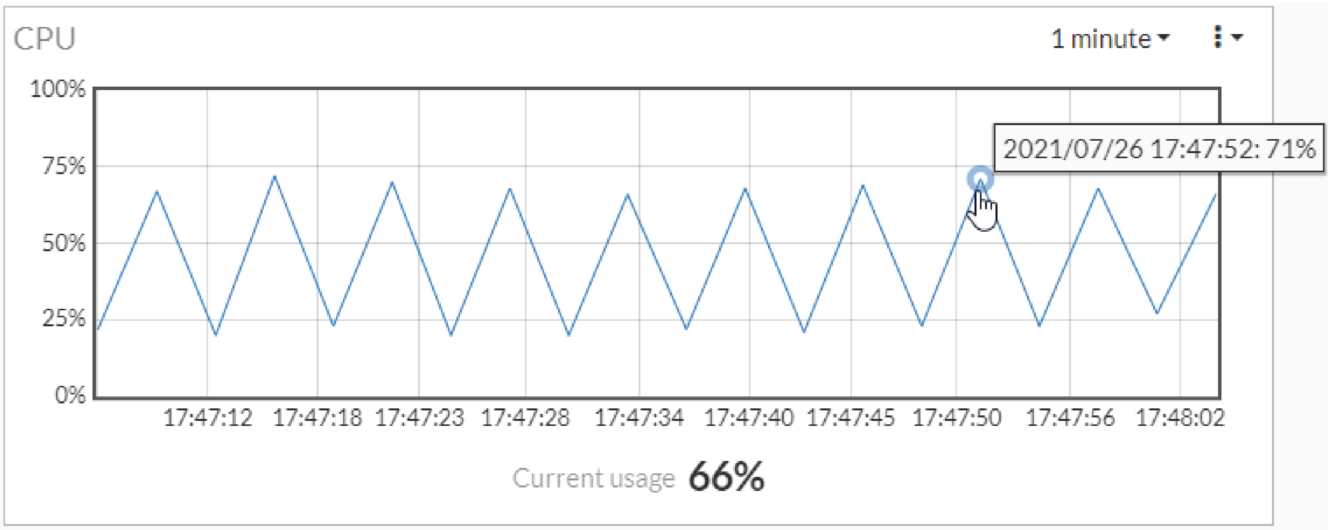
Click on an icon for a link to configure the settings for that component.

Administrators widget



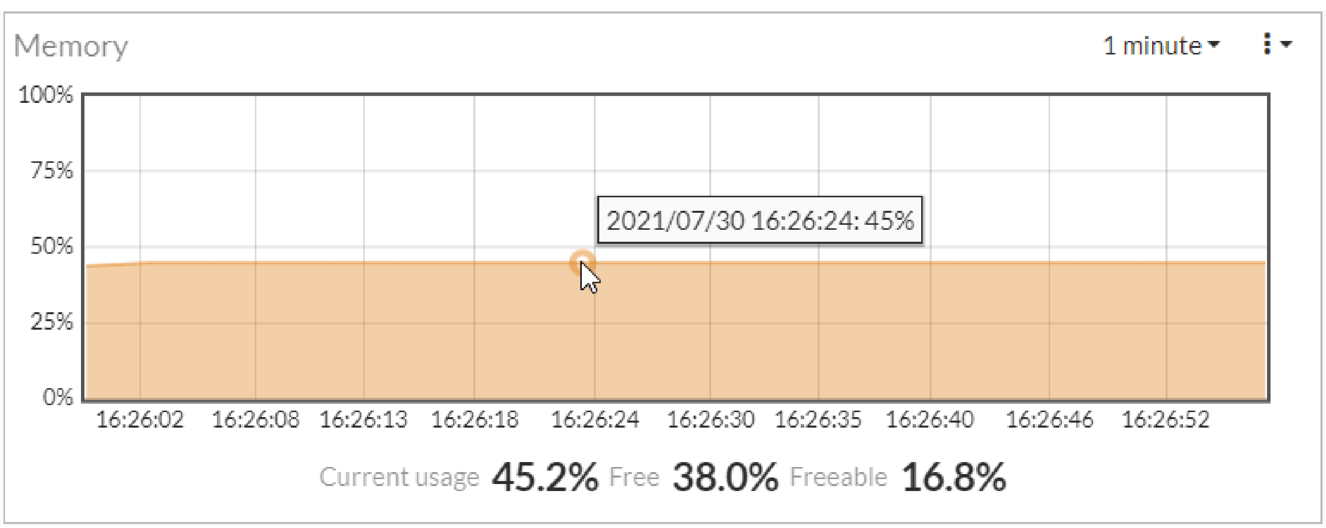
This widget allows you to view which administrators are logged in and how many sessions are active. Clicking on the widget provides you a link to a page displaying active administrator sessions.

CPU widget



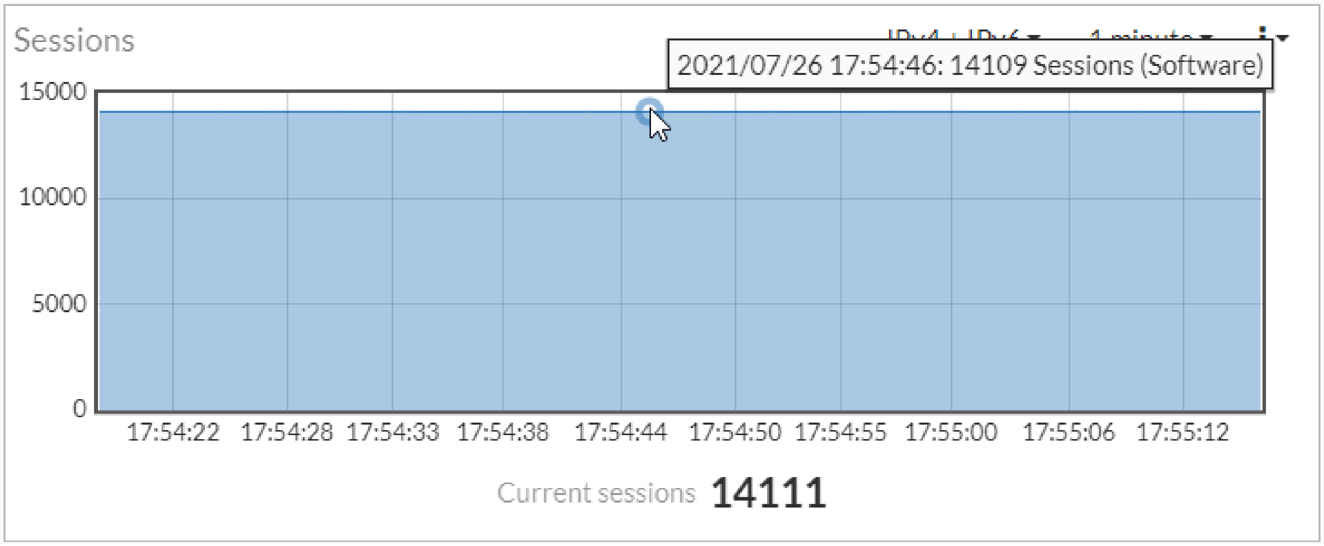
The real-time CPU usage is displayed for different time frames. Select the time frame from the drop-down list at the top of the widget. Hovering over any point on the graph displays the average CPU usage along with a time stamp.

Memory widget



Real-time memory usage is displayed for different time frames. Select the time frame from the drop-down list at the top of the widget. Hovering over any point on the graph displays the percentage of memory used along with a time stamp.

Sessions widget



This widget allows you to view how many proxy sessions are active. Select the time frame from the drop-down list at the top of the widget. Select whether to display *IPv4*, *IPv6*, or *IPv4 + IPv6* sessions. Hovering over any point on the graph displays the number of proxy sessions with a time stamp.

SSL-VPN widget

The *SSL-VPN* widget now includes *Duration* and *Connection Summary* charts. The widget also identifies users who have not enabled two-factor authentication.

To view the SSL-VPN widget:

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*.

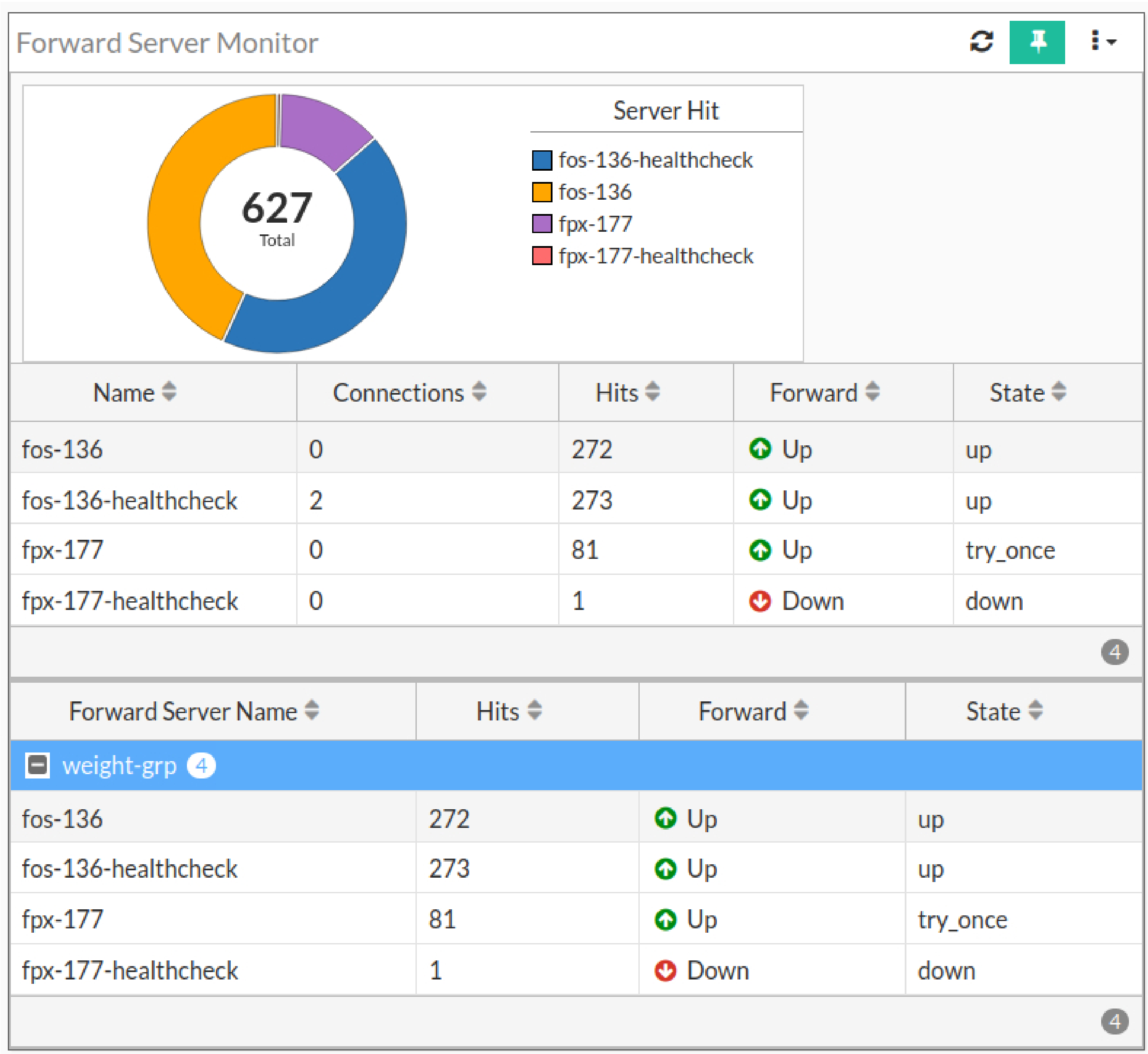
IPSec widget

The *IPsec* widget displays information about Phase 1 and Phase 2 tunnels. The widget also identifies users who have not enabled two-factor authentication.

To view the IPSec widget:

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.

Forward Server Monitor widget



This widget allows you to monitor the forward server status, connections, and hits. Hover over the graph or server name in the widget to get a quick view of the server status. Forward servers with *Health Check* disabled will always be *Up* in the *Forward* column. When such a forward server is part of a server group, it serves as a backup option when no other server is up and running.

The *State* column is added in 7.2.4 to provide more specific state information about the forward server. The following states are available:

- *pending*—Initial state of all forward servers. A pending forward server can mean one of the following:
  - The state of the forward server is unknown, which means no connection has been established yet or the state has not been updated yet.

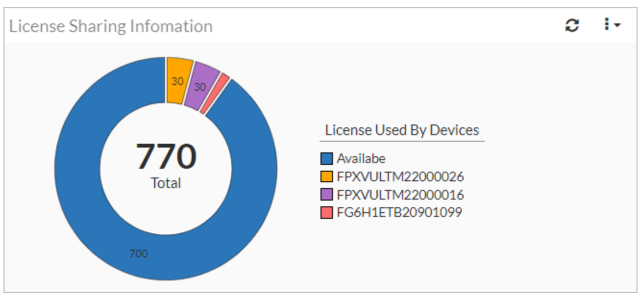
  - The forward server is running but pending FQDN resolve. FQDN resolve failure triggers a state change to *down*.
- *try_once*—For forward servers in *down* state with *Health Monitor* disabled, FortiProxy periodically switches its state from *down* to *try_once* to verify the latest status of the server to avoid situations where a server in down state is ignored in all subsequent health state checks.
- *busy*—The forward server is running but unstable.
- *down*—The forward server is not running and connections are blocked.

See Create or edit a forwarding server on page 74 for more information about how to enable and configure health monitoring for the forward server.

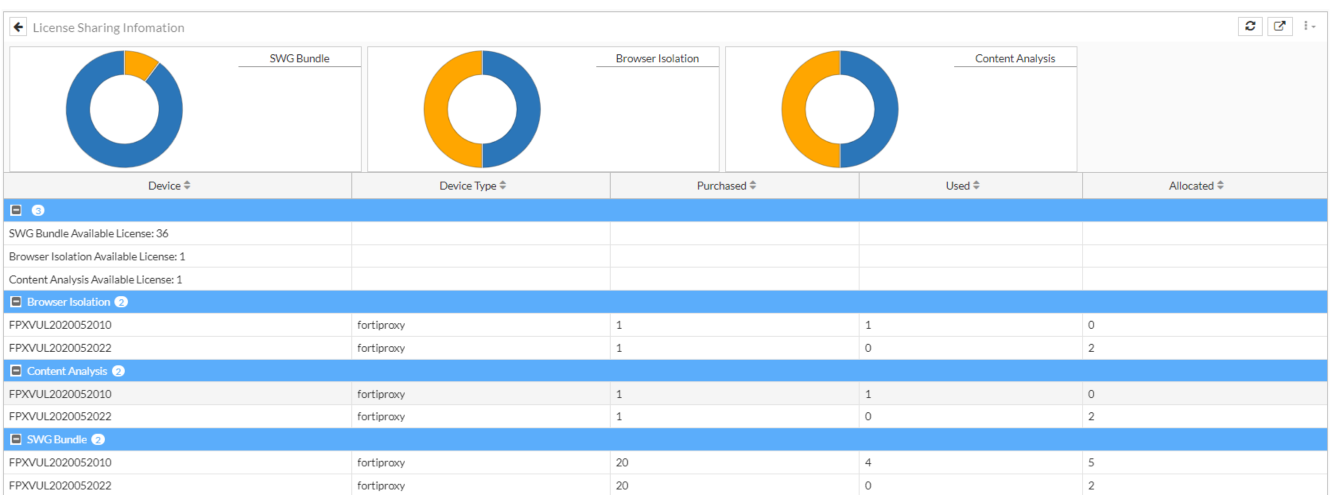
License Sharing Information widget

FortiProxy shares available seats among devices in HA on page 469 active-passive mode or in a Security Fabric on page 521 group with license sharing enabled. The *License Sharing Information* widget displays the total number of available licenses, and the numbers used by the devices in the license pool. Click on a specific section in the chart for more details about the license usage.

In FortiProxy 7.2.4 and earlier, the widget displays license sharing information of the SWG Bundle license type only. See example below.

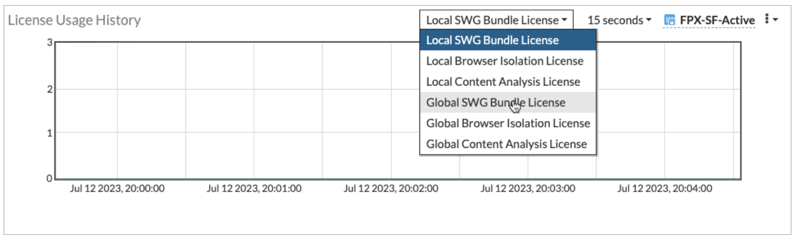


FortiProxy 7.2.5 adds support for displaying Browser Isolation (FNBI) and Content Analyses on page 342 (FCAS) license sharing information in the widget. See example below.



Refer to the FortiProxy datasheet for more information about different license types. See the License Sharing Deployment Guide for more information about how license sharing works and how to configure license sharing to meet your needs.

License Usage History widget



The *License Usage History* widget displays the global or local license usage history of the following license types at a certain interval:

- SWG Bundle License
- Browser Isolation License
- Content Analysis License

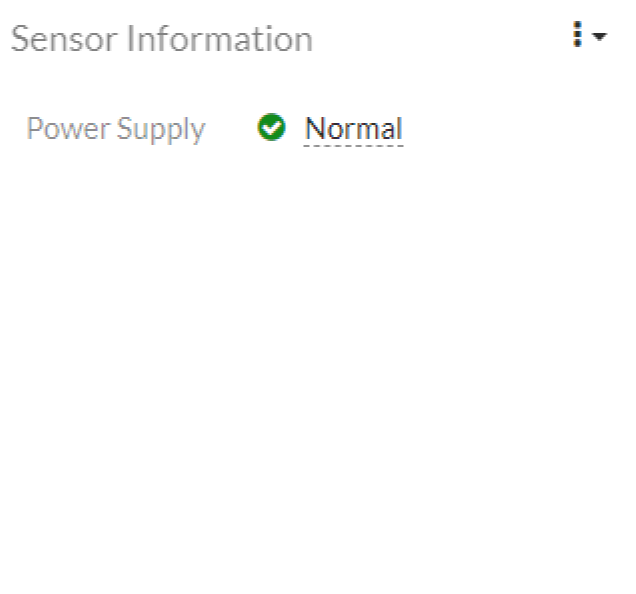
Use the filter at the top to display license usage data for a specific license type. Configure the interval at the top-right corner with the following options: 15 seconds, 5 minutes, 1 hour, 1 day, 1 week, 1 month, or 1 year.

For each timestamp, the widget displays the following values:

- **Min Usage**—Minimum number of license seats used during the past interval.
- **Max Usage**—Maximum number of license seats used during the past interval.
- **Average Usage**—Average number of license seats used during the past interval.

Refer to the FortiProxy datasheet for more information about different license types. See the License Sharing Deployment Guide for more information about how license sharing works and how to configure license sharing to meet your needs.

Sensor Information widget



This widget allows you to view the status of power supply sensor in the hardware system. You can click on the status icon in the widget for more detailed information about the status, such as the real-time and expected power supply voltage values.

Sensor List - Power Supply

Name	Description	Status	Value
PSU1	Main 12V power supply #1	Normal	12.13 V
PSU2	Main 12V power supply #2	Normal	12.13 V
5VCC	Main 5V power supply	Normal	4.97 V
3.3VCC	Main 3.3V power supply	Normal	3.32 V
VBAT	Battery power supply	Normal	3.13 V
Vcpu1	CPU #1 voltage	Normal	1.8 V
Vcpu2	CPU #2 voltage	Normal	1.8 V
VDIMMAB	Memory channel 1 voltage	Normal	1.19 V
VDIMMCD	Memory channel 2 voltage	Normal	1.18 V
VDIMMEF	Memory channel 3 voltage	Normal	1.19 V
VDIMMGH	Memory channel 4 voltage	Normal	1.19 V
5VSB	5V standby	Normal	5.05 V
3.3VSB	3.3V standby	Normal	3.4 V
1.5V PCH	1.5V platform controller voltage	Normal	1.52 V
1.2V BMC	1.2V baseboard controller voltage	Normal	1.21 V
1.05V PCH	1.05V platform controller voltage	Normal	1.04 V

This widget is available only for FPX-2000E/4000E/2000G/4000G units.

User dropdown menu

In the right corner of the FortiProxy title bar, the user dropdown menu provides the following actions:

- Reboot the system.
- Shut down the system.
- Upload anew version of the FortiProxy firmware or restore an older firmware version.
- Back up your FortiProxy configuration.
- Restore a saved FortiProxy configuration.
- Check the available versions of your saved FortiProxy configurations.
- Upload or run a script.
- Change your password.
- Log out.

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)

FortiView

FortiView is a comprehensive monitoring system for your network that integrates real-time and historical data into a single view on your FortiProxy unit. It can log and monitor threats to networks, filter data on multiple levels, keep track of administrative activity, and more.

FortiView allows you to use multiple filters within the consoles, enabling you to narrow your view to a specific time (up to 24 hours in the past), by user ID or local IP address, by application, and in many more ways.

FortiView can be used to investigate traffic activity, such as user uploads/downloads or videos watched on YouTube, on a network-wide, user group, and individual-user level, with information relayed in both text and visual format. FortiView makes it easy to get an actionable picture of your network's Internet activity.

This section covers the following topics:

- FortiView dependencies on page 44
- FortiView interface on page 46
- FortiView consoles on page 47

FortiView dependencies

By default, FortiView is enabled on FortiProxy units. You will find the FortiView consoles in the main menu.

Most FortiView consoles require the user to enable several features to produce data. The following table summarizes the dependencies:

FortiView Console	Dependencies
FortiView Applications	• Application control profile added to a policy • Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy
FortiView Cloud Applications	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy • Full SSL inspection enabled for all protocols in an SSL/SSH Inspection profile • Application Control profile and Full SSL Inspection profile added to the same policy
FortiView Countries/Regions	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy
FortiView Destination Firewall Objects	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy

FortiView Console	Dependencies
FortiView Destination Interfaces	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy
FortiView Destination Owners	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy
FortiView Destinations	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy
FortiView Interface Pairs	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy
FortiView Policies	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy
FortiView Search Phrases	• FortiGuard categories enabled in a Web Filter profile • Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy • Log all search keywords enabled in a Web Filter profile • Profile-based NGFW mode
FortiView Servers	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy
FortiView Sessions	• Disk logging enabled • Traffic logging enabled in a policy
FortiView Source Firewall Objects	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy
FortiView Source Interfaces	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy
FortiView Sources	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy
FortiView Sources - WAN	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy
FortiView Traffic Shaping	• Enable traffic-shaping feature

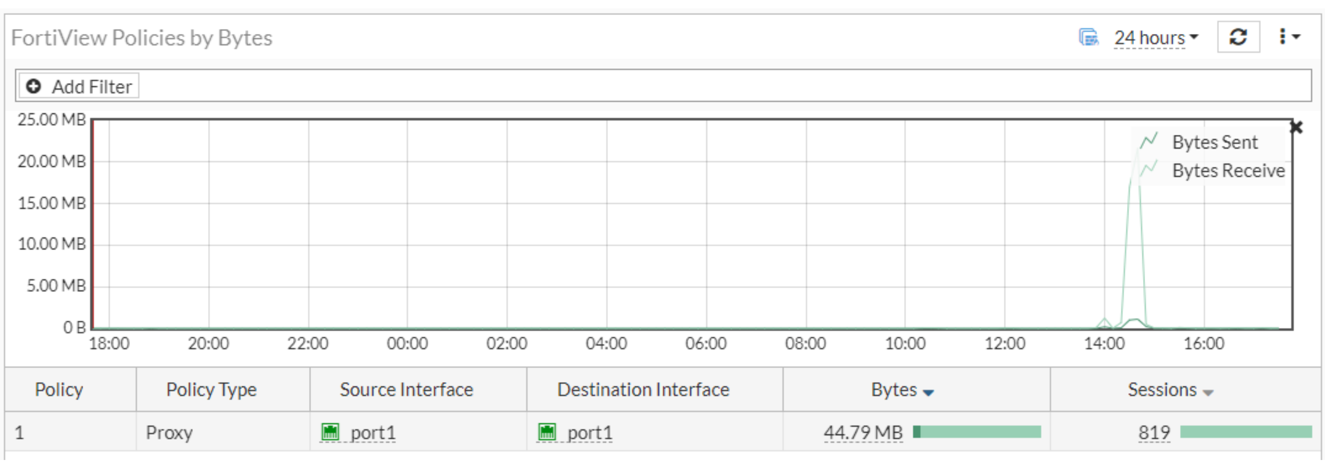
FortiView Console	Dependencies
	• Disk logging enabled • Historical FortiView enabled
FortiView Web Categories	• FortiGuard categories enabled in a Web Filter profile • Web Filter profile added to a policy • Traffic logging enabled in a policy • Logging device set up and enabled • Historical FortiView enabled
FortiView Web Sites	• FortiGuard categories enabled in a Web Filter profile • Web Filter profile added to a policy • Traffic logging enabled in a policy • Logging device set up and enabled • Historical FortiView enabled
FortiView VPN	• Logging device set up and enabled • Historical FortiView enabled • Traffic logging enabled in a policy

To enable disk logging and historical FortiView:

1. Go to *Log & Report > Log Settings*.
2. Under *Local Log*, enable *Disk* and *Enable Historical FortiView*.
3. Click *Apply*.

FortiView interface

FortiView lets you access information about the traffic activity on your FortiProxy unit, visually and textually. FortiView is broken up into several consoles, each of which features a top menu bar and a graph window, as seen in the following image:



Depending on the FortiView console, the top menu bar contains various controls:

- *Refresh* button, which updates the data displayed
- *Add Filter* button, for filtering the data by category
- Filter buttons to select what data to view
- View drop-down menu to select *Table View* or *Bubble Chart*
- Time Display drop-down menu (options: *5 minutes*, *1 hour*, or *24 hours*; if you are using FortiAnalyzer, you can select longer time periods)
- Dashboard widget drop-down menu
- *Settings* button
- Information icon

FortiView consoles

This section briefly describes the consoles available in FortiView:

- FortiView Applications console on page 48 displays applications used on the network that have been recognized by Application Control and allows you to view what sort of applications individual employees are using.
- FortiView Cloud Applications console on page 48 displays Web/Cloud Applications used on the network and allows you to access detailed data on cloud application usage, for example, YouTube.
- FortiView Countries/Regions console on page 48 provides a geographical display of threats, in real time, from international sources as they arrive at your FortiProxy unit.
- FortiView Destination Firewall Objects console on page 49 displays the top traffic sessions aggregated by destination object.
- FortiView Destination Interfaces console on page 49 displays the number of destination interfaces connected to your network, how many sessions there are in each interface, and what sort of traffic is occurring.
- FortiView Destination Owners console on page 49 displays the top traffic sessions aggregated by owner.
- FortiView Destinations console on page 49 displays the top traffic sessions aggregated by destination.
- FortiView Interface Pairs console on page 49 displays the top traffic sessions aggregated by interface pair.
- FortiView Policies console on page 49 displays what policies are in affect on your network, what their source and destination interfaces are, how many sessions are in each policy, and what sort of traffic is occurring.
- FortiView Search Phrases console on page 50 displays the top traffic sessions aggregated by website search phrase.
- FortiView Servers console on page 50 displays the top servers aggregated by server address.
- FortiView Sessions console on page 50 displays complete information on all FortiProxy sessions, with the ability to filter sessions by port number and application type.
- FortiView Source Firewall Objects console on page 51 displays the top traffic sessions aggregated by source object.
- FortiView Source Interfaces console on page 51 displays the number of source interfaces connected to your network, how many sessions there are in each interface, and what sort of traffic is occurring.
- FortiView Sources console on page 51 displays detailed information on the sources of traffic passing through the FortiProxy unit so that you can investigate an unusual spike in traffic to determine which user is responsible.
- FortiView Sources - WAN console on page 51 displays the top traffic sessions for interfaces with a role of WAN, aggregated by source.
- FortiView Traffic Shaping console on page 52 displays the top traffic sessions aggregated by traffic shaper.
- FortiView VPN console on page 52 displays the top traffic sessions aggregated by VPN user.
- FortiView Web Categories console on page 52 displays the top traffic sessions aggregated by website category.

- FortiView Web Sites console on page 52 displays web sites visited as part of network traffic that have been recognized by Web Filtering so that you can investigate instances of proxy avoidance, which is the act of circumventing blocks using proxies.

FortiView Applications console

The *FortiView Applications* console provides information about the applications being used on your network.

This console can be sorted by sessions or bytes. The data can be filtered by 5 minutes, 1 hour, or 24 hours. You can select which applications are displayed.

For information to appear in the *FortiView Applications* console, Application Control must be enabled in a policy.

FortiView Cloud Applications console

The *FortiView Cloud Applications* console provides information about the cloud applications being used on your network. This includes information such as:

- The names of videos viewed on YouTube (visible by hovering the cursor over the session entry)
- Filed uploaded and downloaded from cloud hosting services such as Dropbox
- Account names used for cloud services

Two different views are available for the Cloud Applications: *Applications* and *Users* (located in the top menu bar next to the time periods). *Applications* shows a list of the programs being used. *Users* shows information on the individual users of the cloud applications, including the username, if the FortiProxy unit was able to view the login event.

You can sort the data by bytes, sessions, or files (up or down). The data can be filtered by 5 minutes, 1 hour, or 24 hours. You can select which cloud applications are displayed.

For information to appear in the Cloud Applications console, an application control profile (that has Deep Inspection of Cloud Applications enabled) must be enabled in a policy, and SSL Inspection must use deep-inspection.

FortiView Countries/Regions console

The *FortiView Countries/Regions* console displays network activity by geographic region. Threats from various international destinations will be shown, but only those arriving at your destination, as depicted by the FortiProxy unit. You can place your cursor over the FortiProxy's location to display the device name, IP address, and the city name/location.

The color gradient of the darts on the map indicate the traffic risk, where red indicates the more critical risk.

This console can be sorted by bytes, sessions, or threat scores. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

FortiView Destination Firewall Objects console

The *FortiView Destination Firewall Objects* console displays the top destination firewall objects. You can drill down by destination object.

This console leverages UUIDs to resolve firewall object address names for improved usability, which requires address objects' UUIDs to be logged.

To enable address object UUID logging in the CLI:

```
config system global
   set log-uuid-address enable
end
```

This console can be sorted by sessions or bytes. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

FortiView Destination Interfaces console

The *FortiView Destination Interfaces* console lists the total number of destination interfaces connected to your network, how many sessions there are in each interface, and the number of bytes sent.

This console can be sorted by bytes or sessions. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

FortiView Destination Owners console

The *FortiView Destination Owners* console displays the top destination owners. This console can be sorted by bytes or sessions. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

FortiView Destinations console

The *FortiView Destinations* console provides information about the destination IP addresses of traffic on your FortiProxy unit, as well as the application used. You can select the country/region, destination device, or destination IP address to display.

This console can be sorted by bytes or sessions. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

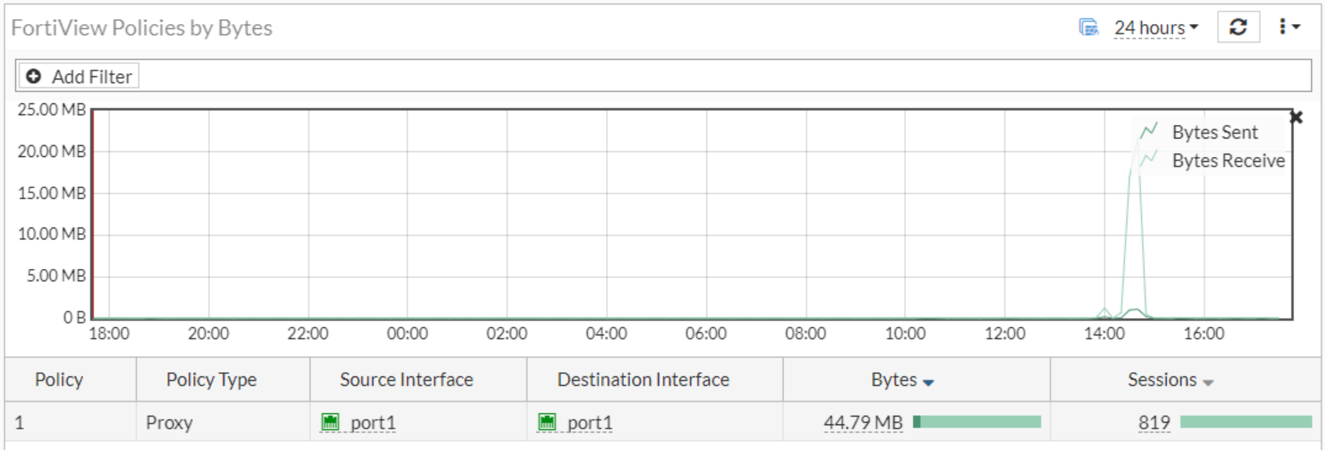
FortiView Interface Pairs console

The *FortiView Interface Pairs* console displays the top traffic sessions aggregated by the interface pair. You can select the destination interface or the source interface to display.

This console can be sorted by bytes or sessions. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

FortiView Policies console

The *FortiView Policies* console shows what policies are in affect on your network, what their source and destination interfaces are, how many sessions are in each policy, and what sort of traffic is occurring, represented in bytes sent and received. You can select which policies to display.



This console can be sorted by bytes or sessions. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

FortiView Search Phrases console

The *FortiView Search Phrases* console displays the top search phrases, sorted by count. You can drill down by search phrase.

The data can be filtered by 5 minutes, 1 hour, or 24 hours.

FortiView Servers console

The *FortiView Servers* console displays the top servers. You can drill down by the server address. You can select the country/region, destination device, or destination IP address to display.

This console can be sorted by bytes or sessions. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

FortiView Sessions console

The *FortiView Sessions* console displays the top sessions by traffic source and can be used to end sessions.

This console has the greatest number of column options to choose from. To choose which columns you want to view, select the column settings cog at the far right of the columns and select your desired columns. They can then be clicked and dragged in the order that you wish them to appear.

Some of the columns available in FortiView are only available in All Sessions. For example, the Action column displays the type of response taken to a security event. This function can be used to review what sort of threats were detected, whether the connection was reset due to the detection of a possible threat, and so on. This would be useful to display alongside other columns such as the Source, Destination, and Bytes (Sent/Received) columns, as patterns or inconsistencies can be analyzed.

Similarly, there are a number of filters that are only available in All Sessions, one of which is Protocol. This allows you to display the protocol type associated with the selected session, for example, TCP, FTP, HTTP, HTTPS, and so on.

The *FortiView Sessions* console is useful when verifying open connections. For example, if you have a web browser open to browse the Fortinet website, you would expect a session entry from your computer on port 80 to the IP address for the Fortinet website. You can also use a session table to investigate why there are too many sessions for the FortiProxy unit to process.

You can also view the session data in the CLI.

To view session data using the CLI:

```
# diagnose sys session list
```

The session table output in the CLI is very large. You can use the supported filters in the CLI to show only the data you need.

To view session data with filters using the CLI:

```
# diagnose sys session filter {sintf | dintf | src | nsrc | dst | proto | sport | nport |
dport | policy | clear}
```

FortiView Source Firewall Objects console

The *FortiView Source Firewall Objects* console displays the top source firewall objects. You can drill down by source object.

This console leverages UUIDs to resolve firewall object address names for improved usability, which requires address objects' UUIDs to be logged.

To enable address object UUID logging in the CLI:

```
config system global
   set log-uuid-address enable
end
```

This console can be sorted by sessions or bytes. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

FortiView Source Interfaces console

The *FortiView Source Interfaces* console lists the total number of source interfaces connected to your network, how many sessions there are in each interface, and the number of bytes sent.

This console can be sorted by bytes or sessions. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

FortiView Sources console

The *FortiView Sources* console provides information about the sources of traffic on your FortiProxy unit.

You can select which source devices and source IP addresses are displayed. This console can be sorted by bytes, sessions, or threat scores. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

FortiView Sources - WAN console

The *FortiView Sources - WAN* console displays the top traffic sessions for interfaces with a role of WAN, aggregated by source.

You can select which source devices and source IP addresses are displayed. This console can be sorted by bytes, sessions, or threat scores. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

FortiView Traffic Shaping console

The *FortiView Traffic Shaping* console displays the top traffic sessions aggregated by traffic shaper.

You can select which source devices and source IP addresses are displayed. This console can be sorted by dropped bytes, bytes, sessions, bandwidth, or packets.

For information to appear in the *Traffic Shaping* console, at least one traffic shaper and at least one traffic-shaping policy must be configured.

FortiView VPN console

The *FortiView VPN* console displays the top traffic sessions aggregated by VPN user.

You can select which user names and VPN types are displayed. This console can be sorted by connections or bytes. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

FortiView Web Categories console

The *FortiView Web Categories* console displays the top web categories. You can drill down by category.

You can select which domains and web categories are displayed. This console can be sorted by browsing time, threat score, bytes, or sessions. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

For information to appear in the *FortiView Web Categories* console, web filtering must be enabled in a policy, with FortiGuard categories enabled.

FortiView Web Sites console

The *FortiView Web Sites* console lists the top allowed and top blocked web sites. You can view information by domain or by FortiGuard categories by using the options in the top right corner. Each FortiGuard category can be selected to see a description of the category and several example sites, with content loaded from FortiGuard on demand.

You can select which domains and web categories are displayed. This console can be sorted by browsing time, threat score, bytes, or sessions. The data can be filtered by 5 minutes, 1 hour, or 24 hours.

For information to appear in the *FortiView Web Sites* console, web filtering must be enabled in a policy, with FortiGuard categories enabled.

Using the process monitor

The *Process Monitor* displays running processes with their CPU and memory usage levels. Administrators can sort, filter, and terminate processes within the *Process Monitor* pane.

To access the process monitor:

1. Go to *Dashboard* > *Status*:
   - Left-click in the *CPU* or *Memory* widget and select *Process Monitor*.
   - Click the user name in the upper right-hand corner of the screen, then go to *System* > *Process Monitor*.

   The *Process Monitor* appears, which includes a line graph, donut chart, and process list.
2. Click the + beside the search bar to view which columns can be filtered.

To kill a process within the process monitor:

1. Select a process.
2. Click the *Kill Process* dropdown.
3. Select one of the following options:
   - *Kill*: the standard kill option that produces one line in the crash log (`diagnose debug crashlog read`).
   - *Force Kill*: the equivalent to `diagnose sys kill 9 <pid>`. This can be viewed in the crash log.
   - *Kill & Trace*: the equivalent to `diagnose sys kill 11 <pid>`. This generates a longer crash log and backtrace. A crash log is displayed afterwards.

Proxy Settings

For more information about web proxy and explicit web proxy, see Deployments on page 14.

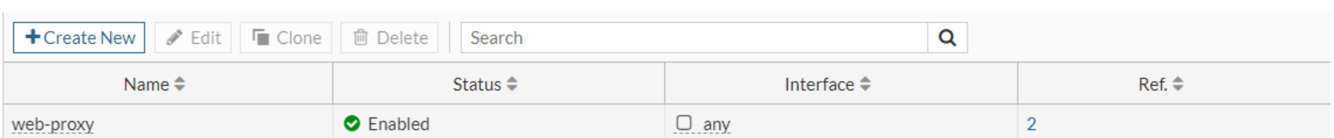
This section covers the following topics:

Explicit Proxy

Use the explicit web proxy configuration to enable the explicit HTTP proxy on one or more Fortinet interfaces. IPv6 is supported.

IP pools support the explicit web proxy, allowing such traffic to be sourced from a range of IP addresses.

To configure the explicit web proxy configuration, go to *Proxy Settings > Explicit Proxy*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

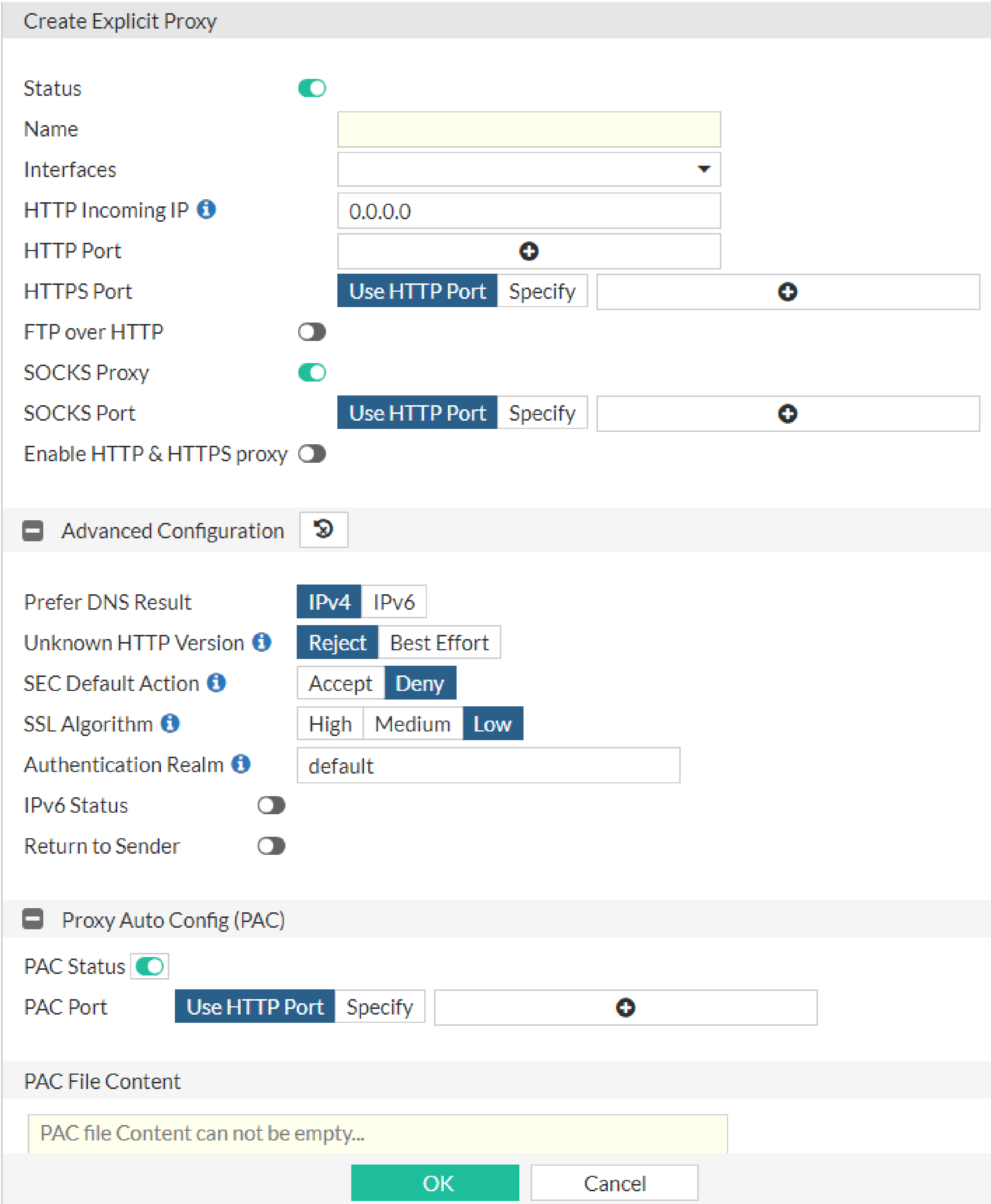
The following options are available:

Create New	Create an explicit web proxy configuration. See Create or edit an explicit web proxy on page 55.
Edit	Modify settings to an explicit web proxy configuration. See Create or edit an explicit web proxy on page 55.
Clone	Copies an existing explicit web proxy configuration.

Delete	Remove a proxy from the list.
Search	Enter a search term to find in the list.
Name	The name of the explicit web proxy configuration.
Status	The status of the explicit web proxy configuration.
Interface	The interface to which the proxy applies.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit an explicit web proxy

Select *Create New* to open the *Create Explicit Proxy* window.



Select an explicit web proxy configuration and then click *Edit* to open the *Edit Explicit Proxy* window.

Configure the following settings in the *Explicit Proxy* window and then click *OK*:

Status	This explicit web proxy configuration is enabled by default. Toggle to disable this explicit web proxy configuration.
Name	Enter the name of the explicit web proxy configuration.
Interfaces	Select the interface or interfaces that are being monitored by the explicit web proxy from the drop-down list.
HTTP Incoming IP	This field restricts the explicit HTTP proxy to accept sessions only from the specified IP address.
HTTP Port	Enter the port number that HTTP traffic from client web browsers use to connect to the explicit proxy for the specific protocol. Explicit proxy users must configure their web browser's protocols proxy settings to use this port. The default port is 8080. You can enter a maximum of eight ports. Separate multiple ports with a comma. The range of values is 1-65535.
HTTPS Port	Select *Use HTTP Port* or select *Specify* and then enter the port number that HTTPS traffic from client web browsers use to connect to the explicit proxy for the specific protocol. Explicit proxy users must configure their web browser's protocols proxy settings to use this port. You can enter a maximum of eight ports. Separate multiple ports with a comma. The range of values is 1-65535.
FTP Over HTTP	Select this checkbox to enable FTP over HTTP for the explicit web proxy. Then select *Use HTTP Port* or select *Specify* and enter the port number. The FTP over HTTP proxy engine supports PORT mode, FTP over HTTP CONNECT, and uploads through PUT (UTM scanning).
SOCKS Proxy	Select this checkbox to enable the SOCKS proxy. Then select *Use HTTP Port* or select *Specify* and enter the port number.
Enable HTTP/HTTPS proxy - NEW	Select this option to enable HTTP/HTTPS proxy. The default is enabled.
Prefer DNS Result	Select whether the DNS result uses an *IPv4* or *IPv6* address.
Unknown HTTP Version	You can select the action to take when the proxy server must handle an unknown HTTP version request or message. Set the unknown HTTP version to *Best Effort*, *Reject*, or *Tunnel*. • *Best Effort* attempts to handle the HTTP traffic as best as it can. • *Reject* treats known HTTP traffic as malformed and drops it.
SEC Default Action	Accept or deny explicit web proxy sessions when no web proxy firewall policy exists.
SSL Algorithm	Select the strength of the encryption algorithms accepted in HTTPS deep scan.
Authentication Realm	Enter an authentication realm to identify the explicit web proxy.

	The realm can be any text string of up to 63 characters. If the realm includes spaces, you need to enclose it in quotes. When a user authenticates with the explicit web proxy, the HTTP authentication dialog box includes the realm so that you can use the realm to identify the explicitly web proxy for your users.
IPv6 Status	Toggle this setting if you want to use IPv6 addresses.
Return to Sender	Toggle this setting to allow the FortiProxy to remember the MAC address of the last hop and send responses to that MAC address instead of the default gateway.
PAC Status	Toggle this setting to use a proxy auto-config (PAC) file to define how web browsers can choose a proxy server for receiving HTTP content. PAC files include the FindProxyForURL(url, host) JavaScript function that returns a string with one or more access method specifications. These specifications cause the web browser to use a particular proxy server or to connect directly.
PAC Port	Select *Use HTTP Port* or select *Specify* and then enter the port number that traffic from client web browsers use to connect to the explicit proxy for the specific protocol. Explicit proxy users must configure their web browser's protocols proxy settings to use this port.
PAC File Content	Select *Edit* to make changes to a PAC file that was previously uploaded or select *Download* and then select *Save* to save a copy of the PAC file.
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.

Web Proxy Setting

Use the web proxy setting to change the global configuration of explicit web proxies.

Go to *Proxy Settings > Web Proxy Setting* to change the global explicit web proxy settings.

Configure the following settings and then click *Apply*:

Proxy FQDN	The FQDN for the global proxy server. This is the domain name to enter into browsers to access the proxy server.
Max HTTP request length	The maximum length of an HTTP request that can be cached, in KB. Larger requests are rejected. The default is 8 KB.

Max HTTP message length	The maximum length of an HTTP message that can be cached, in KB. Larger messages are rejected. The default is 32 KB.
Realm	You can enter an authentication realm to identify the explicit web proxy. The realm can be any text string of up to 63 characters. If the realm includes spaces, enclose it in quotes. When a user authenticates with the explicit web proxy, the HTTP authentication dialog box includes the realm, so you can use the realm to identify the explicitly web proxy for your users.
Explicit Outgoing IP	Enter the IP address to use as the source address for outgoing HTTP requests by explicit web proxy. Select + to enter another IP address.
Webproxy Profile	Enter the name of the web proxy profile that will be applied when explicit proxy traffic is allowed by default and traffic is accepted that does not match an explicit proxy policy.
Default CA Certificate	Select which certificate to use as a default. The default certificate is Fortinet_CA_SSL.
Forward Server Affinity Timeout	Enter the number of minute before the traffic from the source IP address is no longer assigned to the forwarding server. The default is 30 minutes. The range is 6-60 minutes.
Fast Policy Match	The fast policy match function improves the performance of IPv4 explicit and transparent web proxies on FortiProxy units. When enabled, after the proxy policies are configured, the FortiProxy unit builds a fast searching table based on the different proxy policy matching criteria. When fast policy matching is disabled, web proxy traffic is compared to the policies one at a time from the beginning of the policy list.
LDAP User Cache	Enable or disable the LDAP user cache.
Strict Web Check	Enable or disable (by default) the blocking of web sites that send incorrect headers that don't conform to HTTP 1.1 (see RFC 2616 for more information). Enabling this option may block some commonly used websites.
Forward Proxy Auth	Enable or disable (by default) the forwarding of proxy authentication headers. Note that this option is only practical when in explicit mode, because proxy authentication headers are always forwarded when in transparent mode. By default, in explicit mode, proxy authentication headers are blocked by the explicit web proxy. Therefore, enable this entry if you need to allow proxy authentication through the explicit web proxy.
Strict Guest	Enable or disable whether the explicit web proxy uses strict guest user checking.
HTTPS Replacement Message	Enable or disable whether a replacement message is displayed for HTTPS requests.
Message Upon Server Error	Enable or disable whether a replacement message is displayed when a server error is detected.
Trace Auth No Resp	Enable or disable whether timed-out authentication requests are logged.

Extended Log	Enable or disable the recording of extended log for implicit policies. The extended log includes the useragent, referralurl, httpmethod, and statuscode fields.
Log HTTP Transaction	Configure the logging of HTTP transactions: • *All*—Log all HTTP transactions. • *Security Profiles* (default)—Log HTTP transaction on UTM event. • *Disable*—Disable HTTP transaction log. When *All* or *Security Profiles* is selected, you can find the HTTP transaction logs under *Log & Report > HTTP Transaction*. See Types of logs on page 590.
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.

Logging client IP for forward traffic and HTTP transaction

The HTTP transaction and Forward session logs include the ClientIP column that records the client IP address based on the `learn-client-ip` configuration. By default, the `original-source-ip` is recorded.

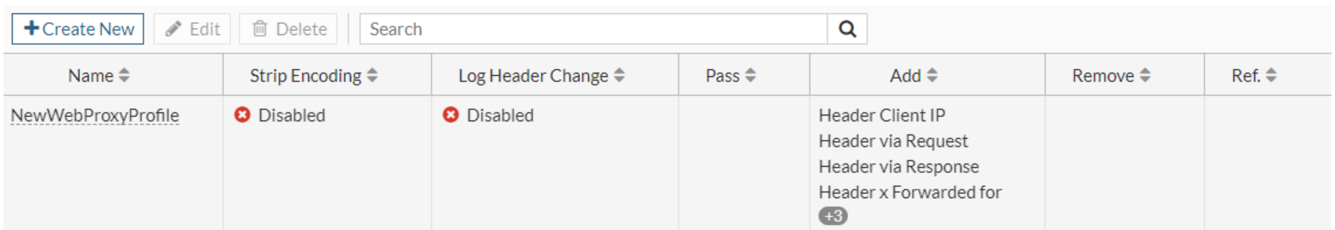
```
config web-proxy global
    set learn-client-ip {enable | disable}
    set learn-client-ip-from-header {true-client-ip x-real-ip x-forwarded-for}
    set learn-client-ip-srcaddr <address>
    set learn-client-ip-srcaddr6 <address>
end
```

`learn-client-ip {enable | disable}`	Enable/disable learning the client's IP address from headers (default = disable).
`learn-client-ip-from-header {true-client-ip | x-real-ip | x-forwarded-for}`	Learn client IP address from the specified headers: True-Client-IP, X-Real-IP, and X-Forwarded-For.
`learn-client-ip-srcaddr (6) <address>`	Source address name (srcaddr or srcaddr6 must be set).

Web Proxy Profile

You can create web proxy profiles that can add, remove, and change HTTP headers. The web proxy profile can be added to the web proxy global configuration.

Go to *Proxy Settings > Web Proxy Profile* to change the web proxy profiles.



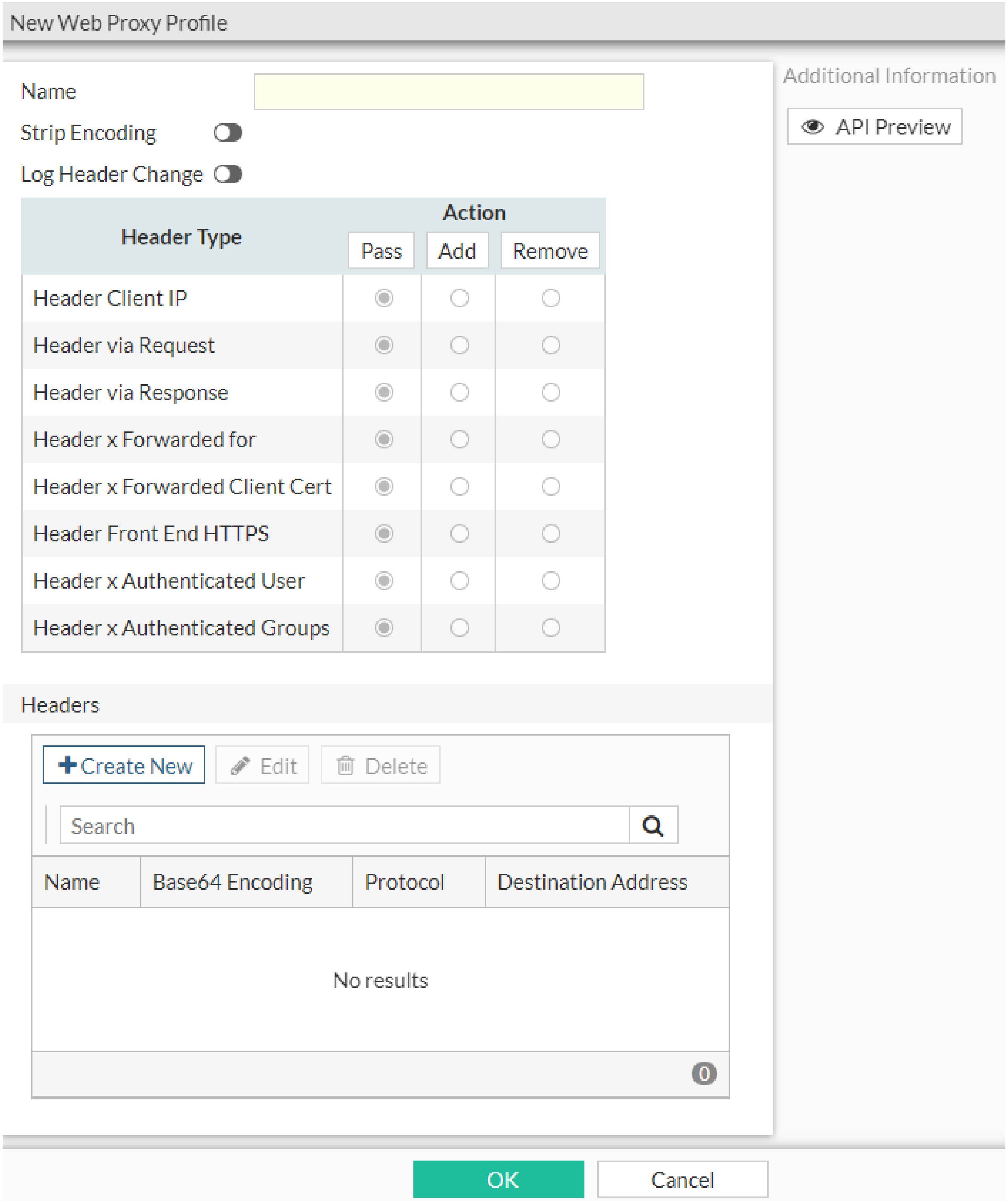
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a web proxy profile. See Create or edit a web proxy profile on page 61.
Edit	Edit the selected web proxy profile. See Create or edit a web proxy profile on page 61.
Delete	Remove the selected web proxy profile.
Search	Enter a search term to find in the list.
Name	The name of the web proxy profile.
Strip Encoding	Whether the profile strips out unsupported encoding from request headers and correctly block banned words.
Log Header Change	Whether the profile allows changes to the log header.
Pass	Which HTTP headers will be forwarded in forwarded requests.
Add	Which HTTP headers will be added in forwarded requests.
Remove	Which HTTP headers will be removed from forwarded requests.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in *Ref.*, and the *Object Usage* window appears displaying the various locations of the referenced object.

Create or edit a web proxy profile

Select *Create New* to open the *New Web Proxy Profile* window.



To open the *Edit Web Proxy Profile* window, select a web proxy profile and then click *Edit*.

Configure the following settings in the *New Web Proxy Profile* window or *Edit Web Proxy Profile* window and then click *OK*:

Name	Enter the name of the new web proxy profile.
Strip Encoding	Toggle whether to strip out unsupported encoding from request headers and correctly block banned words. This option can resolve issues when attempting to successfully block content using Google Chrome.
Log Header Change	Toggle whether to allow changes to the log header.
Header Client IP	Select whether to *Pass*, *Add*, or *Remove* this HTTP header.
Header via Request	Select whether to *Pass*, *Add*, or *Remove* this HTTP header.
Header via Response	Select whether to *Pass*, *Add*, or *Remove* this HTTP header.
Header x Forwarded for	Select whether to *Pass*, *Add*, or *Remove* this HTTP header.
Header x Forwarded Client Cert	Select whether to *Pass*, *Add*, or *Remove* this HTTP header.
Header Front End HTTPS	Select whether to *Pass*, *Add*, or *Remove* this HTTP header.
Header x Authenticated User	Select whether to *Pass*, *Add*, or *Remove* this HTTP header.
Header x Authenticated Groups	Select whether to *Pass*, *Add*, or *Remove* this HTTP header.
Create New	Select to add a new header. See Create or edit an HTTP header on page 64.
Edit	Select to change an existing header. See Create or edit an HTTP header on page 64.
Delete	Select to remove an existing header.
Search	Enter a search term to find in the list.
Name	The name for the HTTP forwarded header.
Base64 Encoding	Whether base64 encoding is enabled or disabled.
Protocol	Whether the new header uses HTTP, HTTPS, or both.
Destination Address	The destination addresses and destination address groups for the HTTP forwarded header.
Action	The action for the HTTP forwarded header: *add-to-request*, *add-to-response*, *remove-from-request*, or *remove-from-response*.
Add Option	How the new header is added: *append*, *new-on-not-found*, or *new*.
Header Content	The content of the HTTP header.
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 for the CMDB API that creates the explicit proxy configuration.
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.

Create or edit an HTTP header

You can change the following HTTP headers:

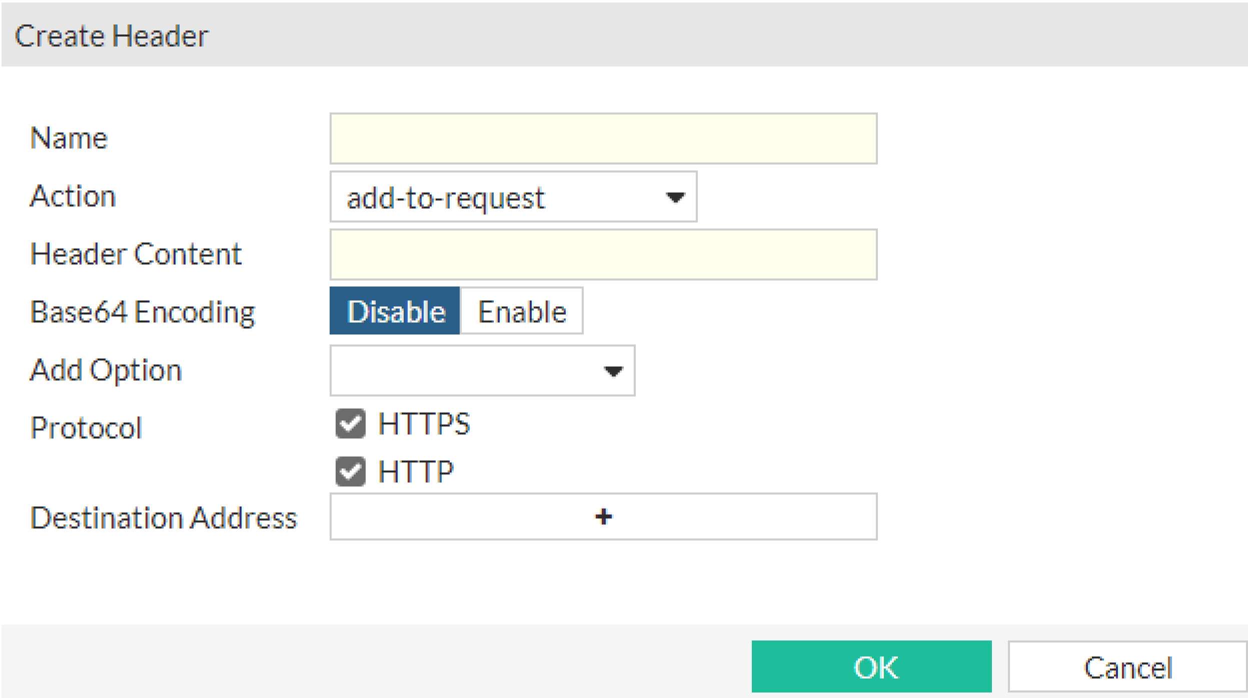
- Header Client IP
- Header via Request
- Header via Response
- Header x Forwarded For
- header-x-forwarded-client-cert
- Header Front End HTTPS
- Header x Authenticated User
- Header x Authenticated Groups

For each of these headers, you can set the action to the following:

- Forward (pass) the same HTTP header
- Add the HTTP header
- Remove the HTTP header

The web proxy can add or remove custom headers from requests or responses. If you are adding a header, you can specify the content to be included in the added header.

Select *Create New* to open the *Create Header* window.



To open the *Edit Header* window, select a header and then click *Edit*.

Configure the following settings in the *Create Header* window or *Edit Header* window and then click *OK*:

Name	Enter a name for the HTTP forwarded header.
Action	Select the action for the HTTP forwarded header: *add-to-request*, *add-to-response*, *remove-from-request*, or *remove-from-response*.
Header Content	Enter the content of the HTTP header.
Base64 Encoding	Enable or disable base64 encoding.
Add Option	Select how the new header is added: *append*, *new-on-not-found*, or *new*.
Protocol	Select whether the new header uses HTTP, HTTPS, or both.
Destination Address	Select + to add destination addresses and destination address groups.

To create a web proxy profile and header from the CLI:

```
config web-proxy profile
   edit <name>
      set header-client-ip {add | pass | remove}
      set header-via-request {add | pass | remove}
      set header-via-response {add | pass | remove}
      set header-x-forwarded-for {add | pass | remove}
      set header-front-end-https {add | pass | remove}
      set header-x-authenticated-user {add | pass | remove}
      set header-x-authenticated-groups {add | pass | remove}
      set strip-encoding {enable | disable}
      set log-header-change {enable | disable}
      config headers
         edit <id>
```

```
            set action {add-to-request | add-to-response | remove-from-request | remove-from-
                 response}
            set content <string>
            set name <name>
         end
      end
   next
end
```

Restricted SaaS access

Large organizations may want to restrict SaaS access to resources like Microsoft Office 365, Google Workspace, and Dropbox by tenant to block non-company login attempts and secure the users from accessing non-approved cloud resources. Many cloud vendors enable this by applying tenant restrictions for access control. For example, users accessing Microsoft 365 applications with tenant restrictions through the corporate proxy will only be allowed to log in as the company's tenant and access the organization's applications.

To implement this, access requests from the clients pass through the company's web proxy, which inserts headers to notify the SaaS service to apply tenant restrictions with the permitted tenant list. Users are redirected the SaaS service login page, and are only allowed to log in if they belong to the permitted tenant list.

For more information, refer to the vendor-specific documentation:

- Office 365: Restrict access to a tenant
- Google Workspace: Block access to consumer accounts
- Dropbox: Network control

Basic configuration

A web proxy profile can specify access permissions for Microsoft Office 365, Google Workspace, and Dropbox by inserting vendor-defined headers that restrict access to the specific accounts. Custom headers can also be inserted for any destination. The web proxy profile can then be applied to a policy to control the header's insertion.

To implement Office 365 tenant restriction, Google Workspace account access control, and Dropbox network access control:

1. Create or edit a web proxy profile on page 61 according to the vendors' specifications:
   a. Set the header name (defined by the service provider).
   b. Set the traffic destination (the service provider).
   c. Set the HTTP header content to be inserted into the traffic (defined by your settings).

```
config web-proxy profile
       edit <name>
        config headers
        edit <id>
               set name <string>
               set dstaddr <address>
               set action add-to-request
               set base64-encoding disable
               set add-option new
               set protocol https http
               set content <string>
```

```
            next
      end
      next
     end
```

2. Apply the web proxy profile to a policy. SSL deep inspection must be used in the firewall policy:

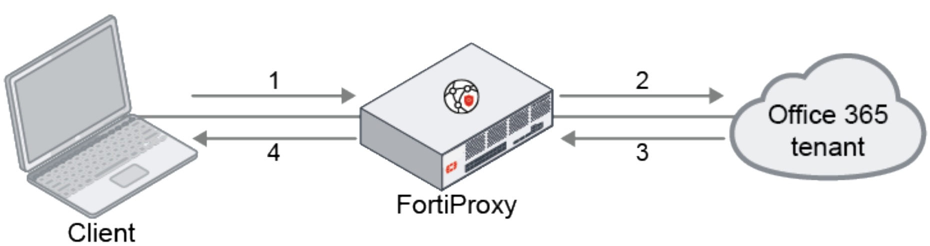
The following table lists the vendor-specific `config headers` settings that must be configured in the web proxy profile (`config web-proxy profile`):

Setting	Vendor specification		
	Microsoft Office 365	Google Workspace	Dropbox
name <string>	• Restrict-Access-To-Tenants • Restrict-Access-Context	• X-GoogApps-Allowed-Domains	• X-Dropbox-allowed-Team-Ids
dstaddr <address>	• Use the built-in Microsoft Office 365 address.	• Use the built-in G Suite address.	• Use the built-in wildcard.dropbox.com address.
content <string>	• Enter the domain for Restrict-Access-To-Tenants. • Enter the directory ID for Restrict-Access-Context.	• Enter the domain.	• Enter the Dropbox team ID.

Due to vendors' changing requirements, these settings may no longer comply with the vendors' official guidelines. See the vendor documentation for more details.

Microsoft Office 365 example

In this example, a web proxy profile is created to control permissions for Microsoft Office 365 to allow corporate domains and deny personal accounts, such as Hotmail and Outlook that are accessed through login.live.com.



1. When a user attempts to access login.microsoftonline.com, login.microsoft.com, or login.windows.net, the traffic will match a proxy inspection mode policy with the assigned web proxy profile.

2. The web proxy profile adds new headers to the customer tenant, indicating the allowed domain and restricted access for personal accounts. Next, the FortiProxy starts a new connection with the Microsoft Office 365 domain controller including the new headers.
3. The Microsoft Office 365 domain controller assesses this data and will allow or deny this access, then sends a reply to the FortiProxy.
4. The FortiProxy sends a reply to the client.

The FortiProxy will only indicate the correct domains to be allowed or denied through the headers to Microsoft. The custom sign-in portal in the browser is generated by Microsoft.

Configuration summary

The following must be configured in FortiOS:

- An FQDN address for login.live.com
- An SSL inspection profile that uses deep inspection with an exemption for login.live.com

Ensure that the firewall certificate is installed on the client machines. A company certificate signed by an internal CA is recommended.

- A web filter profile in proxy mode with static URL filters for the SNI URLs
- A web proxy profile that adds new headers to the customer tenant
- A policy that applies the configured SSL SSL inspection, web filter, and web proxy profiles

The `Restrict-Access-To-Tenants` and `Restrict-Access-Context` headers are inserted for incoming requests to: login.microsoftonline.com, login.microsoft.com, and login.windows.net, which are part of the `Microsoft Office 365` address group.

To restrict access to personal accounts using the login.live.com domain, the `sec-Restrict-Tenant-Access-Policy` header is inserted and uses `restrict-msa` as the header content.

Before configuring the FortiProxy, collect the information related to the company domain in the Office 365 contract.

- `Restrict-Access-To-Tenants`: your <domain.com>
- `Restrict-Access-Context`: Directory ID

To find the Directory ID related to the domain, locate it in the Azure portal, or use the whatismytenantid.com open tool.

To configure the FortiProxy:

1. Add the FQDN address for login.live.com:

```
config firewall address
    edit "login.live.com"
        set type fqdn
        set fqdn "login.live.com"
    next
end
```

2. Configure the SSL inspection profile. In this example, the `deep-inspection` profile is cloned, and the `live.com` FQDN is removed from the exemption list.

a. Clone the `deep-inspection` profile:

```
config firewall ssl-ssh-profile
    clone "deep-inspection" to "Tenant"
end
```

b. Edit the `Tenant` profile and remove `live.com` from the `config ssl-exempt` list.

3. Configure the URL filter list:

```
config webfilter urlfilter
    edit 1
        set name "Auto-webfilter-urlfilter"
        config entries
            edit 1
                set url "login.microsoftonline.com"
                set action allow
            next
            edit 2
                set url "login.microsoft.com"
                set action allow
            next
            edit 3
                set url "login.windows.net"
                set action allow
            next
            edit 4
                set url "login.live.com"
                set action allow
            next
        end
    next
end
```

4. Configure the web filter profile:

```
config webfilter profile
    edit "Tenant"
        set comment "Office 365"
        config web
            set urlfilter-table 1
        end
    next
end
```

5. Configure the web proxy profile (enter the header names exactly as shown):

```
config web-proxy profile
    edit "SaaS-Tenant-Restriction"
        set header-client-ip pass
        set header-via-request pass
        set header-via-response pass
        set header-x-forwarded-for pass
        set header-x-forwarded-client-cert pass
        set header-front-end-https pass
        set header-x-authenticated-user pass
        set header-x-authenticated-groups pass
        set strip-encoding disable
        set log-header-change disable
        config headers
```

```
            edit 1
                set name "Restrict-Access-To-Tenants"
                set dstaddr "login.microsoft.com" "login.microsoftonline.com"
"login.windows.net"
                set action add-to-request
                set base64-encoding disable
                set add-option new
                set protocol https http
                set content <domain>
            next
            edit 2
                set name "Restrict-Access-Context"
                set dstaddr "login.microsoftonline.com" "login.microsoft.com"
"login.windows.net"
                set action add-to-request
                set base64-encoding disable
                set add-option new
                set protocol https http
                set content <directory_ID>
            next
            edit 3
                set name "sec-Restrict-Tenant-Access-Policy"
                set dstaddr "login.live.com"
                set action add-to-request
                set base64-encoding disable
                set add-option new
                set protocol https http
                set content "restrict-msa"
            next
        end
    next
end
```

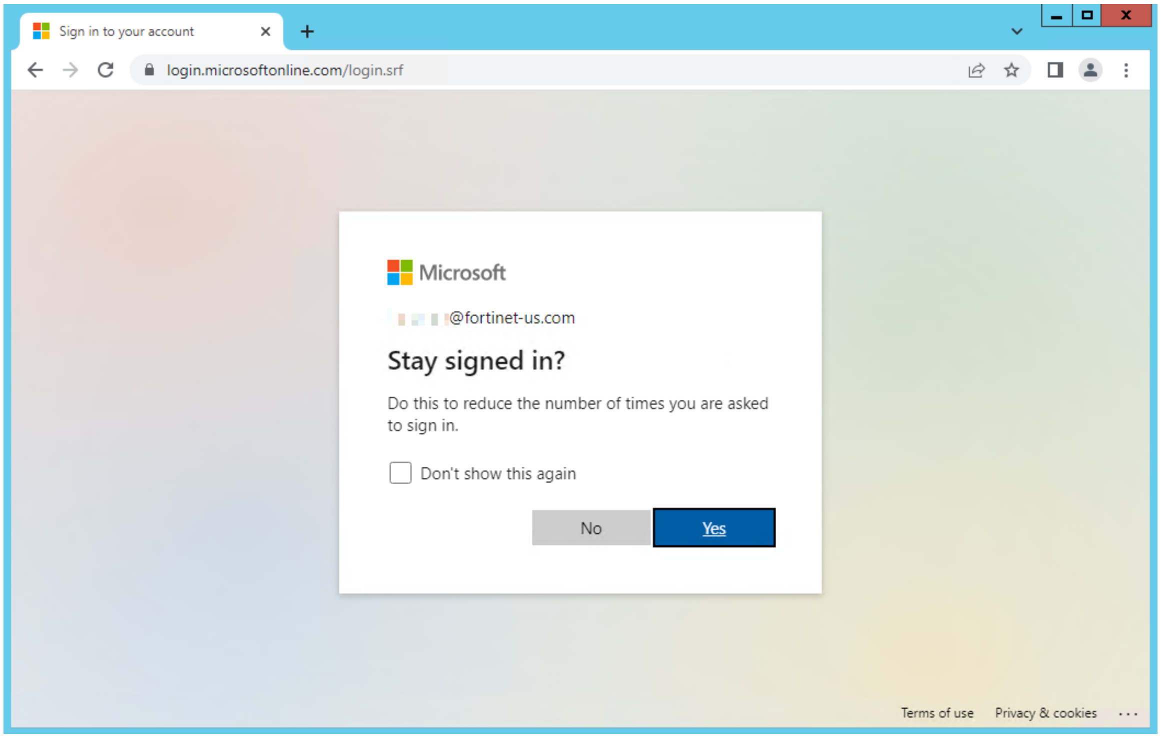
6. Configure the policy:

```
config firewall policy
    edit 10
        set name "Tenant"
        set srcintf "port2"
        set dstintf "port1"
        set action accept
        set srcaddr "users-lan"
        set dstaddr "login.microsoft.com" "login.microsoftonline.com"
"login.windows.net" "login.live.com"
        set schedule "always"
        set service "HTTP" "HTTPS"
        set utm-status enable
        set inspection-mode proxy
        set webproxy-profile "SaaS-Tenant-Restriction"
        set ssl-ssh-profile "Tenant"
        set webfilter-profile "Tenant"
        set logtraffic all
    next
end
```

Testing the access

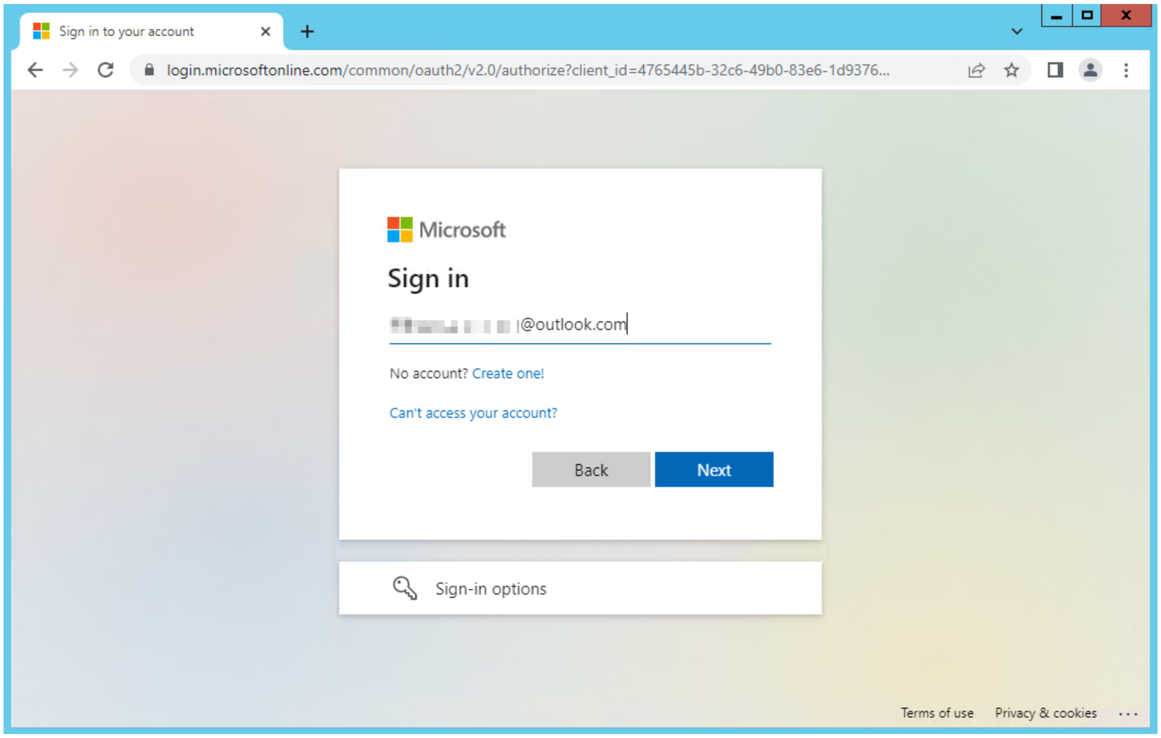
To test the access to corporate domains and personal accounts:

1. Get a client to log in with their corporate email using the login.microsoftonline.com domain.

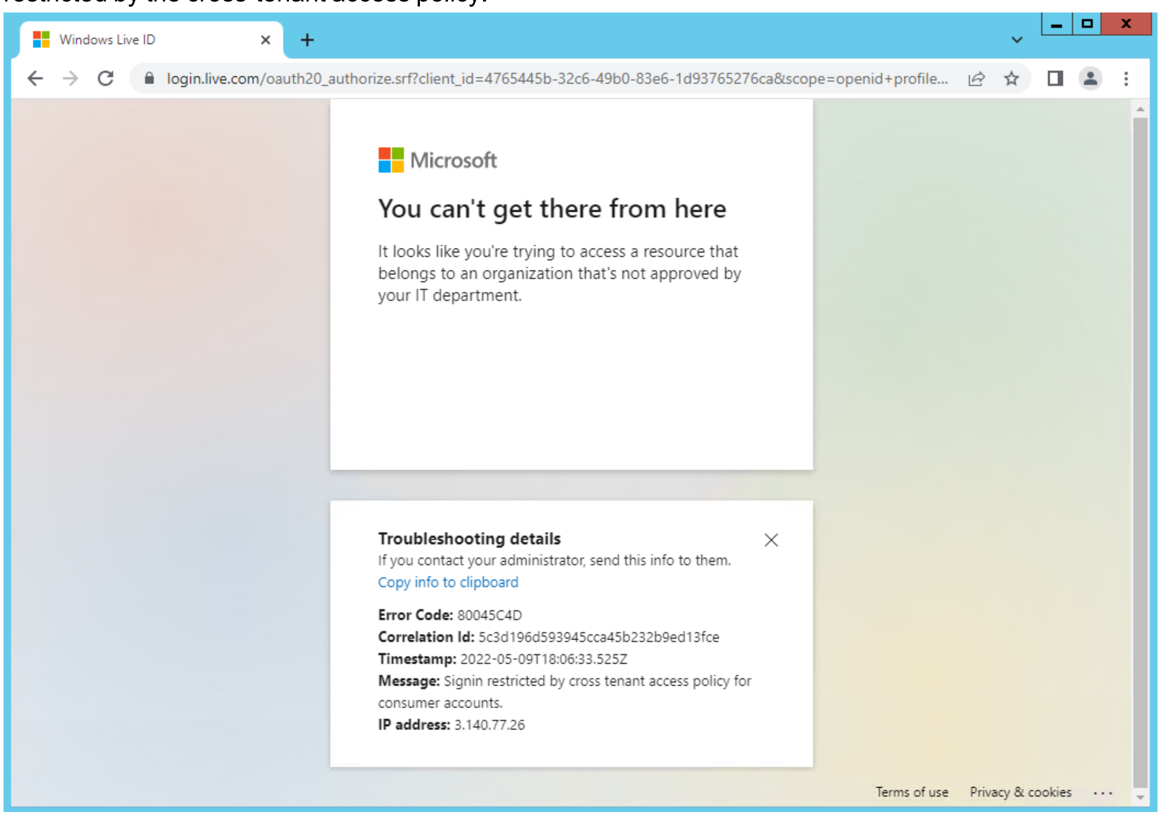


2. The client is able to enter their credentials and log in successfully.

3. Get a client to log in to their personal Outlook account.



4. After the client enters their credentials, a message appears that they cannot access this resource because it is restricted by the cross-tenant access policy.



Verifying the header insertion

To verify the header insertion for corporate domains and personal accounts:

1. On the FortiProxy, start running the WAD debugs:

```
# diagnose wad debug enable category http
# diagnose wad debug enable level info
# diagnose debug enable
```

2. After a client attempts to access corporate domains, verify that the header information is sent to the Microsoft Active Directory:

```
[I][p:234][s:2481][r:33] wad_dump_fwd_http_req            :2567  hreq=0x7fc75f0cd468
Forward request to server:
POST /common/GetCredentialType?mkt=en-US HTTP/1.1
Host: login.microsoftonline.com
Connection: keep-alive
Content-Length: 1961
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="101", "Google Chrome";v="101"
hpgrequestid: d7f706a8-1143-4cdd-ad52-1cc69dc7bb00
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/101.0.4951.54 Safari/537.36
client-request-id: 5c3d196d-5939-45cc-a45b-232b9ed13fce
...
Restrict-Access-To-Tenants: fortinet-us.com
Restrict-Access-Context: ********-****-452f-8535-************
```

3. After a client attempts to access a personal account, verify that the header information is sent to the Microsoft Active Directory:

```
[I][p:234][s:2519][r:34] wad_dump_fwd_http_req            :2567  hreq=0x7fc75f0ce6a8
Forward request to server:
GET /oauth20_authorize.srf?client_id=4765445b-32c6-49b0-83e6-
1d93765276ca&scope=openid+profile+https%3a%2f%2fwww.office.com%2fv2%2fOfficeHome.All&red
irect_uri=https%3a%2f%2fwww.office.com%2flandingv2&response_type=code+id_
token&state=7tAtndYhcA3132S--UOTyLVEtyIZs8FgndTpeYM9mJ1EeA-
X5nfqrSalnnPH41cHxfHGug6N5cbliK676v6xZgszgH_
JARVKrptZwBvjI2cbnZ4mttYNNdK1FTlbEtu5VBjgtBOX2u6v3F_
9g7UikCpGTnBRGhvO2pyTndT3EEIyAHvhg9LsKRtY3kxce8dQkfk1iDjLcc3q-01r4rpxSx2xZSbwg_
KkAN3kCRQ9uLfE0ziHAcpvunuKmzGBWKnBhC4sJJkXrMEfXwCg4nsOjg&response_mode=form_
post&nonce=637877163655610380.MjNjZmM4NzQtOTU5My00OGZlLTk0NTItZTE5NDU2YjVlODdjNjViOTQwYm
UtOTZlMS00M2Y5LTkyN2MtN2QyMjgwNjcxY2Uz&x-client-SKU=ID_NETSTANDARD2_0&x-client-
Ver=6.12.1.0&uaid=5c3d196d593945cca45b232b9ed13fce&msproxy=1&issuer=mso&tenant=common&u
i_locales=en-US&epct=AQABAAAAAAD--DLA3VO7QrddgJg7WevrfA6SLaDsJUcjb1Bg9OKonF3d_
lfNJsdDAIH5hlJdUSGejEBIqsko-A7JX67PzaGdEJgOIGa37VhJzGTYBZ-KgATe9FHssnNmLjM_
dojr0dAT83xDhiqQTN2-UcYdcP2s3vPainF7Nqes5ecXRaEoE9Vw9-
sN7jfASOkPRWW03aI6buz0niABvA860YOWDb98vdJWPGkWE-euDr6n8_
zI5iAA&jshs=0&username=****************%40outlook.com&login_
hint=**************%40outlook.com HTTP/1.1
Host: login.live.com
Connection: keep-alive
...
Referer: https://login.microsoftonline.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
sec-Restrict-Tenant-Access-Policy: restrict-msa
```

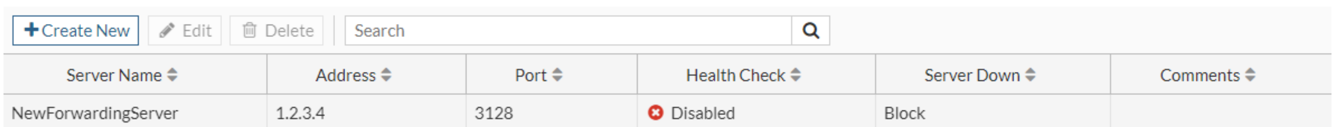
Forwarding Server

By default, the FortiProxy unit monitors a web proxy forwarding server by forwarding a connection to the remote server every 10 seconds. If the remote server does not respond, it is assumed to be down. Checking continues until, when the server does send a response, the server is assumed to be back up. If health checking is enabled, the FortiProxy unit attempts to get a response from a web server by connecting through the remote forwarding server every 10 seconds.

You can enable health checking for each remote forwarding server and specify a different web site to check for each one. Use the Forward Server Monitor widget in the dashboard to monitor the health status of the forwarding servers.

If the remote server is down, you can configure the FortiProxy unit to either block sessions until the server comes back up or allow sessions to connect to their destination using the original server. You cannot configure the FortiProxy unit to fail over to another remote forwarding server.

To configure the server-down action and enable health monitoring, go to *Proxy Settings > Forwarding Server*.



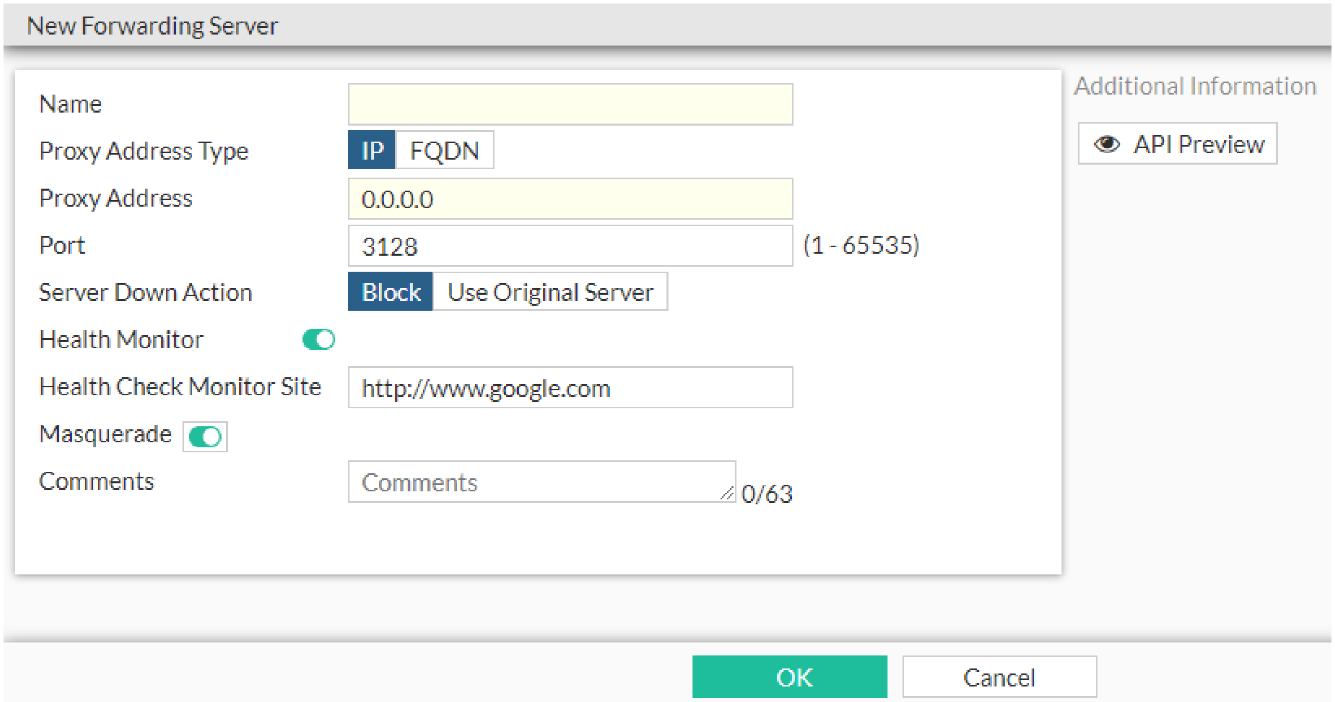
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a forwarding server. See Create or edit a forwarding server on page 74.
Edit	Edit a forwarding server. See Create or edit a forwarding server on page 74.
Delete	Remove a forwarding server from the list.
Search	Enter a search term to find in the list.
Server Name	The name of the forwarding server.
Address	The IP address of the forwarding server.
Port	The port number of the forwarding server.
Health Check	Indicates whether the health check is disabled or enabled for that forwarding server.
Server Down	The action that the FortiProxy unit takes when the server is down.
Comments	Optional description of the forwarding server.

Create or edit a forwarding server

Select *Create New* to open the *New Forwarding Server* window.



To open the *Edit Forwarding Server* window, select a forwarding server and then click *Edit*.

Configure the following settings in the *New Forwarding Server* window or *Edit Forwarding Server* window and then click *OK*:

<table>
<tr><td>Name</td><td>Enter the name of the forwarding server.</td></tr>
<tr><td>Proxy Address Type</td><td>Select the type of IP address of the forwarding server, either IP or FQDN.</td></tr>
<tr><td>Proxy Address</td><td>Enter the IP address or the fully qualified domain name of the forwarding server.</td></tr>
<tr><td>Port</td><td>Enter the port number of the forwarding server.</td></tr>
<tr><td>Server Down Action</td><td>Select what action the FortiProxy unit will take if the forwarding server is down, either Block or Use Original Server.</td></tr>
<tr><td>Health Monitor</td><td>Enable or disable health check monitoring.
This option behaves differently when the forward server is configured with different protocols:
<table>
<tr><th>Protocol</th><th>Behavior</th></tr>
<tr><td>FTP</td><td>When Health Monitor is enabled, health check is performed against the explicit FTP proxy server. You cannot configure Health Check Monitor Site.</td></tr>
<tr><td>HTTP or HTTP + HTTPS</td><td>When Health Monitor is enabled, health check is performed with HTTP only.</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td><table><tr><th>Protocol</th><th>Behavior</th></tr><tr><td>SOCKS only</td><td>The Health Monitor option is not available. No health check is performed.</td></tr></table>Use the Forward Server Monitor widget in the dashboard to monitor the health status of the forwarding server.</td></tr>
<tr><td>Health Check Monitor Site</td><td>If you enabled Health Monitor, enter the URL address of the health check monitoring site. This option is unavailable when the protocol of the forward server is FTP.</td></tr>
<tr><td>Masquerade</td><td>Enable or disable whether the web proxy uses the device address to connect to the proxy server.</td></tr>
<tr><td>Comments</td><td>Enter an optional description of the forwarding server.</td></tr>
<tr><td>API Preview</td><td>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.</td></tr>
</table>

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 for the CMDB API that creates the explicit proxy configuration.
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.

To create a forwarding server in the CLI:

```
config web-proxy forward-server
    edit <server_name>
        set addr-type {ip | fqdn}
        set ip <IPv4_address>
        set fqdn <FQDN>
        set port <1-65535>
        set healthcheck {disable | enable}
        server-down-option {block | pass}
        set comment <string>
        set authentication {disabled | immediately | upon-challenge}
        set masquerade {enable | disable}
    next
end
```

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"
```

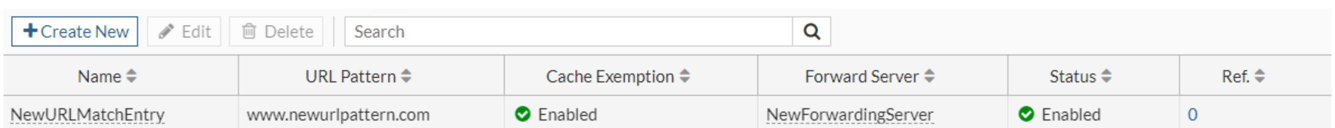
```
            set srcaddr "all"
            set dstaddr "category_social"
            set action accept
            set schedule "always"
            set logtraffic all
            set webproxy-forward-server "upStream_proxy_2"
            set utm-status enable
            set ssl-ssh-profile "deep-inspection"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

Server URL

The URL match list is used to exempt URLs from caching and to enable forwarding specific URLs to a web proxy server. URLs, URL patterns, and numeric IP addresses can be added to the match list.

For example, if your users access web sites that are not compatible with FortiProxy web caching, you can add the URLs of these web sites to the web caching exempt list, and all traffic accepted by a web cache policy for these websites will not be cached.

To see the available URL match entries, go to *Proxy Settings > Server URL*.



Hover over the leftmost edge of the column heading to display the Configure Table icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

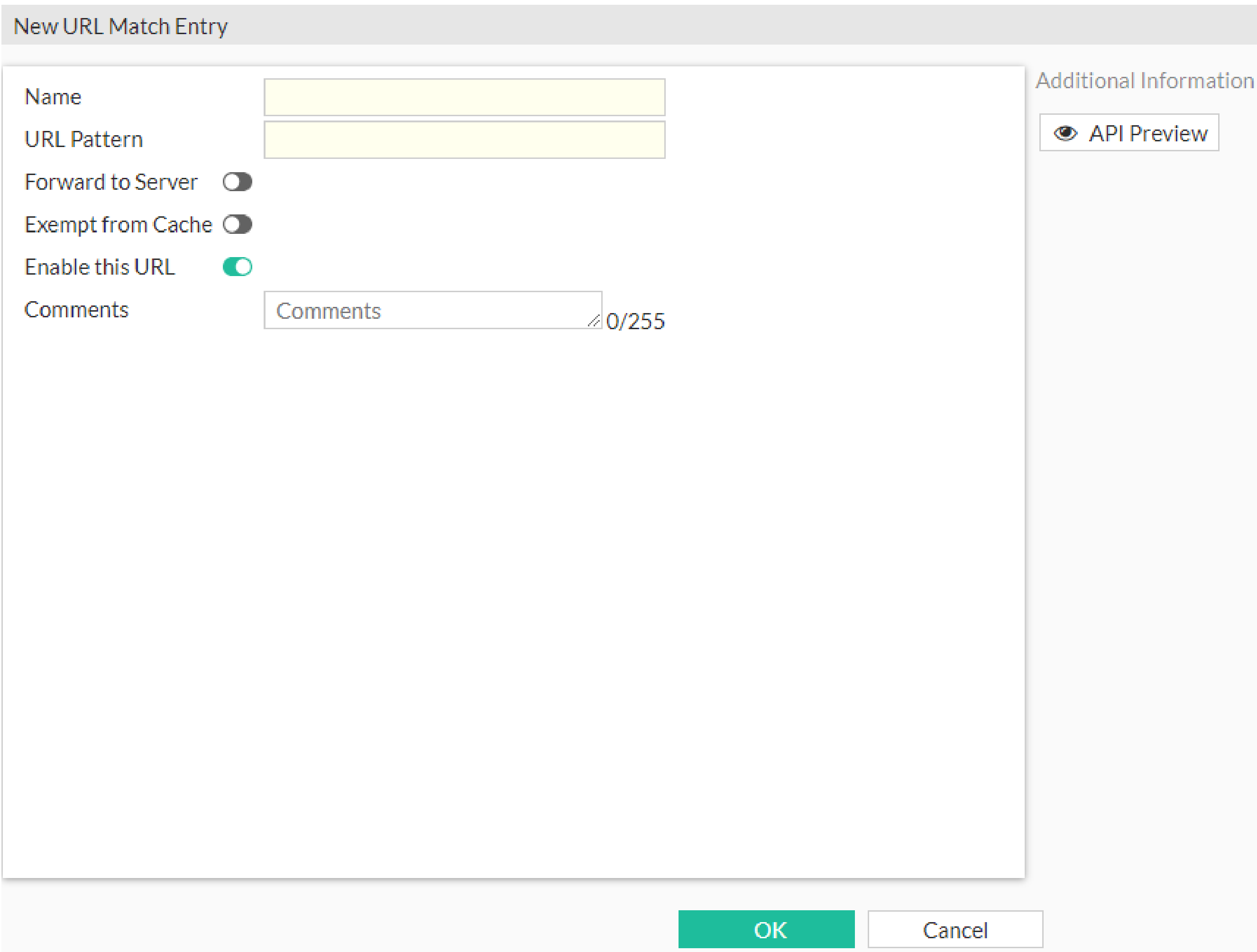
The following options are available:

Create New	Create a URL match entry. See Create or edit a URL match entry on page 80.
Edit	Edit a URL match entry. See Create or edit a URL match entry on page 80.
Delete	Remove a URL match entry from the list.
Search	Enter a search term to find in the list.
Name	The name for the URL match entry.
URL Pattern	The URL, URL pattern, or numeric IP address to match.
Cache Exemption	Whether the URL is exempt from caching.
Forward Server	Name of the forwarding server that the URL is forwarded to. To create a forwarding server, see Create or edit a forwarding server on page 74.
Status	The status is either *enable* or *disable*.
Ref.	Displays the number of times the object is referenced to other objects.

	To view the location of the referenced object, select the number in *Ref.*, and the *Object Usage* window appears displaying the various locations of the referenced object.
Comments	Optional description of the URL match entry.

Create or edit a URL match entry

Select *Create New* to open the *New URL Match Entry* window.



To open the *Edit URL Match Entry* window, select a URL match entry and then click *Edit*.

Configure the following settings in the *New URL Match Entry* window or *Edit URL Match Entry* window and then click *OK*.

Name	Enter a name for the URL match entry.
URL Pattern	Enter the URL, URL pattern, or numeric IP address to match.
Forward to Server	If you want to forward the URL to a web proxy server, enable *Forward to Server* and select the server from the drop-down list.

	To create a forwarding server, see Forwarding Server on page 74.
Exempt from Cache	Enable this option to exempt the URL from caching.
Enable this URL	Enable this option to make the URL match entry active.
Comments	Enter an optional description of the URL match entry.
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 create a URL match entry in the CLI:

```
config web-proxy url-match
   edit <name>
      set comment <optional_string>
      set url-pattern <value>
      set cache-exemption {enable | disable}
      set forward-server <forwarding_server_name>
      set status {enable | disable}
   next
end
```

To use the API Preview:

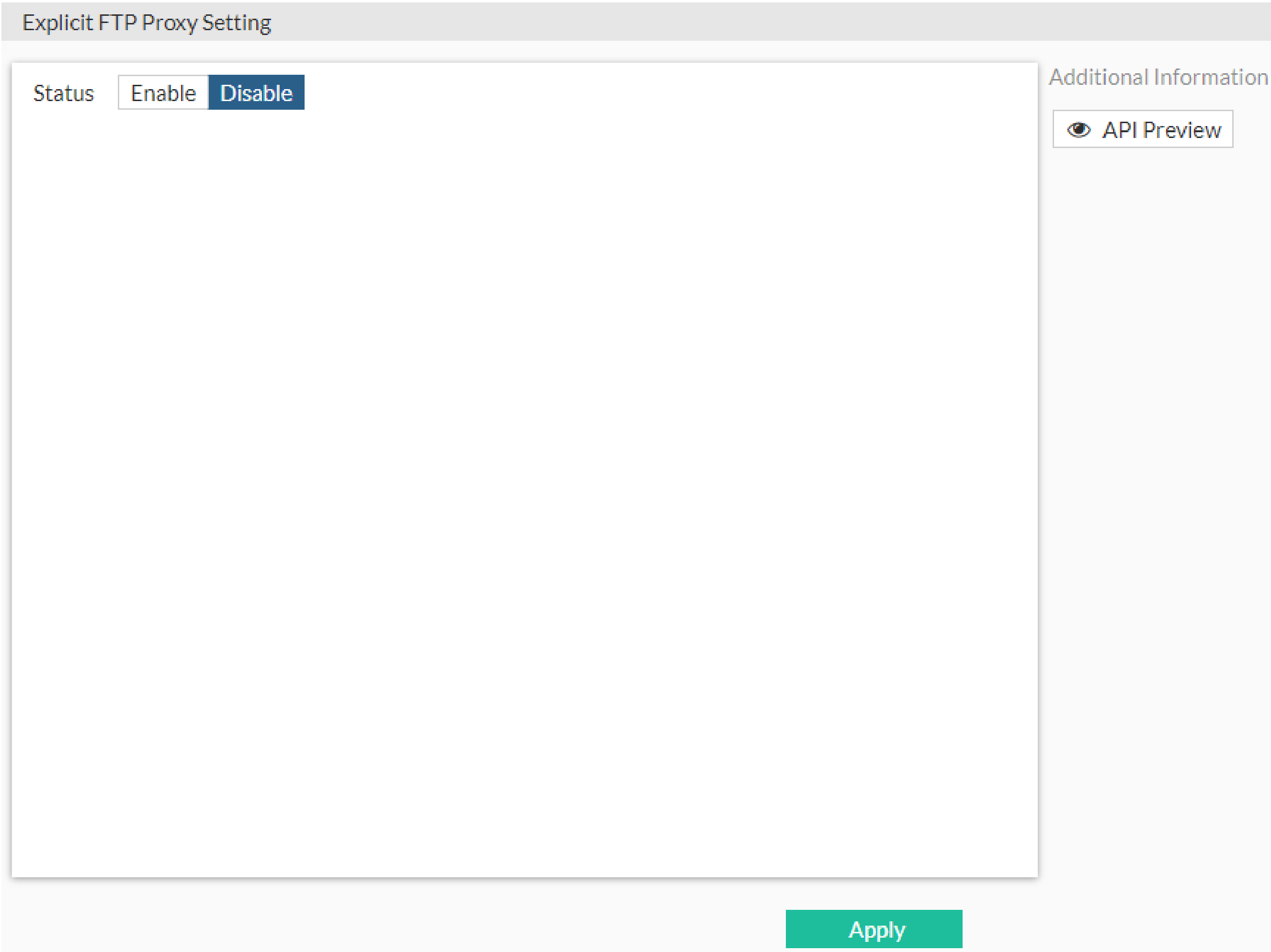
1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown for the CMDB API that creates the explicit proxy configuration.
2. Enable *Show modified changes only* to show the modified changes instead 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.

FTP Proxy

You can enable the explicit FTP proxy on one or more FortiProxy interfaces. The explicit web and FTP proxies can be operating at the same time on the same or on different FortiProxy interfaces.

Enabling the explicit FTP proxy on an interface connected to the Internet is a security risk because anyone on the Internet who finds the proxy could use it to hide their source address.

To configure the explicit FTP proxy, go to *Proxy Settings > FTP Proxy*.



Configure the following settings and then click *Apply*:

Status	Select *Enable* to make the explicit FTP proxy active.
Incoming IP	Enter the incoming IP address.
Outgoing IP	Enter the outgoing IP address.
Default Firewall Policy Action	If *Default Firewall Policy Action* is set to *Deny*, traffic sent to the explicit FTP proxy that is not accepted by an explicit FTP proxy policy is dropped. If *Default Firewall Policy Action* is set to *Allow*, all FTP proxy sessions that do not match a policy are allowed.
Incoming Port	Enter the range of incoming port numbers. Click + to add another range.
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 for the CMDB API that creates the explicit proxy configuration.
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.

FTPS handling

When `explicit-ftp-tls` is enabled in the FTP protocol options, FTP control sessions are proxied to enforce deep inspection so that the proxy can understand FTP control commands after STARTTLS and open a pinhole for FTP data sessions regardless of FTPS deep inspection and/or UTM status.

```
config firewall profile-protocol-options
    edit "test"
        config ftp
            set ports 21
            set status enable
            set explicit-ftp-tls {disable | enable}
        end
    next
end
```

When deep inspection is enabled, transparent policy FTP is always redirected.

Isolator Server

To see a list of isolator servers, go to *Proxy Settings > Isolator Server*.

Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

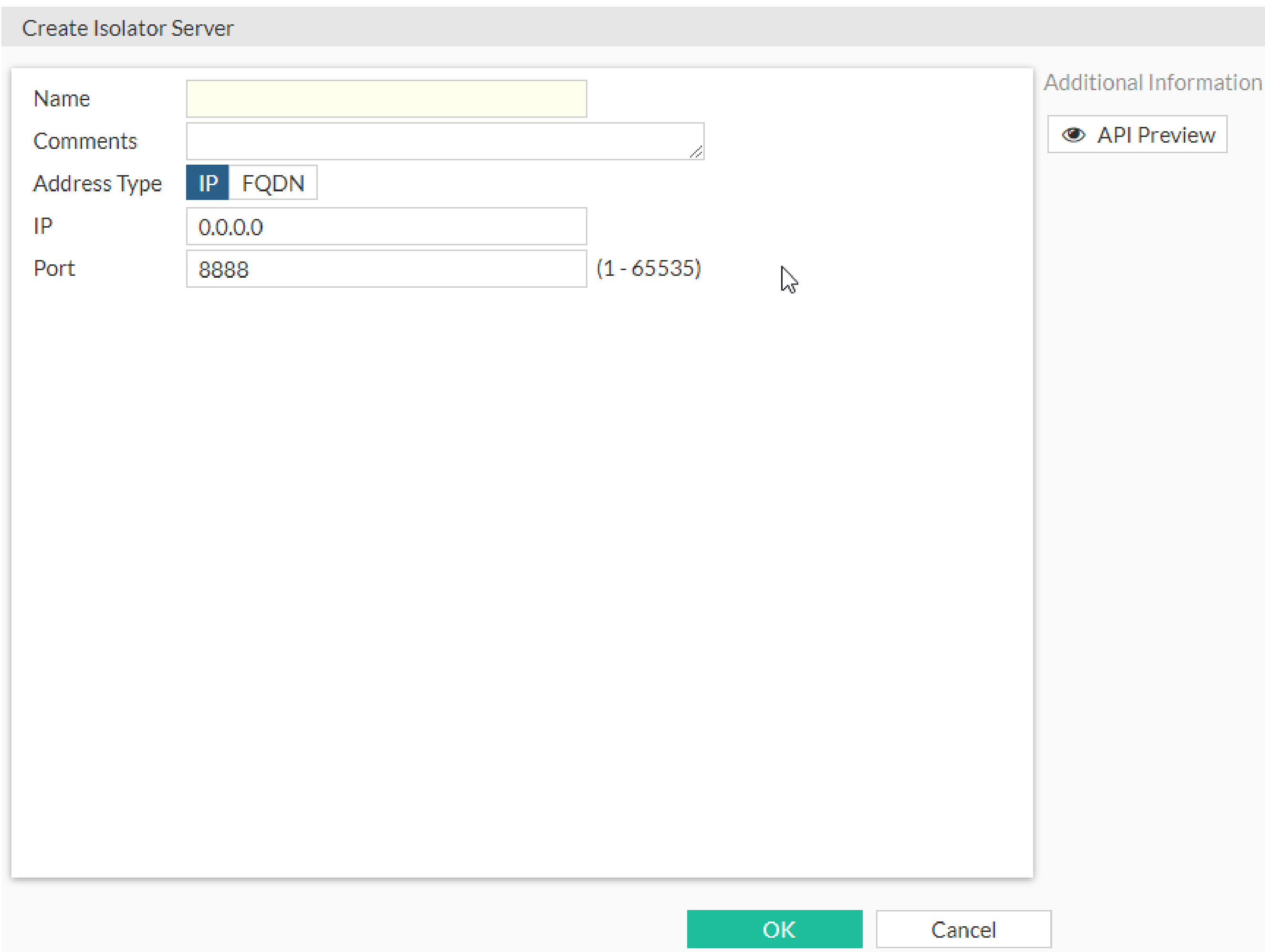
The following options are available:

Create New	Create an isolator server. See Create or edit an isolator server on page 84.
Edit	Edit an isolator server. See Create or edit an isolator server on page 84.
Clone	Copy an existing isolator server.
Delete	Remove an isolator server from the list.
Search	Enter a search term to find in the list of isolator servers.

Name	The name of the isolator server.
Address Type	The isolator server address is either an IP address or a fully qualified domain name (FQDN).
IP	The IP address of the isolator server.
FQDN	The FQDN of the isolator server.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref., and the Object Usage window appears displaying the various locations of the referenced object.
Comments	Optional description of the isolator server.

Create or edit an isolator server

Select *Create New* to open the *Create Isolator Server* window.



To open the *Edit Isolator Server* window, select an isolator server and then click *Edit*.

Configure the following settings in the *Create Isolator Server* window or *Edit Isolator Server* window and then click *OK*:

Name	Enter the name of the isolator server.
Comments	Enter an optional description of the isolator server.
Address Type	Select the type of isolator server address, either *IP* or *FQDN*.
IP	If you selected *IP* for the address type, enter the IP address of the isolator server.
FQDN	If you selected *FQDN* for the address type, enter the fully qualified domain name of the isolator server.
Port	Enter the port number of the isolator server.
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.

To control if the web proxy uses the device address to connect to the proxy server:

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

Proxy Options

Certain inspections defined in security profiles require that the traffic be held in proxy while the inspection is carried out. When a security profile requiring the use of a proxy is enabled in a policy, the *Proxy Options* field is displayed. The proxy options define the parameters of how the traffic will be processed and to what level the traffic will be processed. There can be multiple security profiles of a single type. There can also be a number of unique proxy option profiles. As the requirements for a policy differ from one policy to the next, a different proxy option profile for each individual policy can be configured or one profile can be repeatedly applied.

The proxy options refer to the handling of the following protocols:

- HTTP
- SMTP
- POP3
- IMAP
- FTP
- NNTP

- MAPI
- DNS
- CIFS

The configuration for each of these protocols is handled separately.

Just like other components of the FortiProxy unit, different proxy option profiles can be configured to allow for granular control of the FortiProxy unit. In the case of the proxy option profiles, you need to match the correct profile to a firewall policy that is using the appropriate protocols. If you are creating a proxy option profile that is designed for policies that control SMTP traffic into your network, you only want to configure the settings that apply to SMTP. You do not need or want to configure the HTTP components.

To view the available proxy option profiles, go to *Proxy Settings* > *Proxy Options*.

Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a proxy option profile. See Create or edit a proxy option profile on page 89 and Create a CIFS proxy option on page 92.
Edit	Modify the selected proxy option profile. See Create or edit a proxy option profile on page 89.
Clone	Make a copy of the selected proxy option profile.
Delete	Remove the selected proxy option profile.
Search	Enter a search term to find in the proxy option profile list.
Name	The name of the proxy option profile.
Read Only	The `default` proxy option profile is read only. It cannot be changed or deleted.
Comments	An optional description of the proxy option profile.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Video streaming splitting

The following are the most popular audio/video streaming protocols:

1. Real-time Transport Protocol (RTP)
2. Real Time Streaming Protocol (RTSP)
3. MPEG-Dynamic Adaptive Streaming over HTTP (DASH)
4. Apple HTTP Live Streaming (HLS)

5. Adobe HTTP Dynamic Streaming (HDS)
6. Microsoft Smooth Streaming (MSS)

To deliver streams smoothly and transmit as much information as possible, video stream splitting splits streams into fragments, and their size is negotiated dynamically between the client and server. Sometimes, the fragment is kept unchanged. The default fragment sizes are 64 bytes for audio data and 128 bytes for video data and most other data types. Fragments from different streams can then be interleaved and multiplexed over a single connection. Streams can carry, for example, video and one or more audio channels, next to a control channel to control the streams. This is like an FTP command versus data session.

FortiProxy supports Apple HLS and MPEG-DASH stream splitting, which can be transferred over HTTP(S) or TCP port 1935.

Configuring 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 {auto-tuning | 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 {auto-tuning	system	static	dynamic}`	The TCP window type to use for this protocol. • `auto-tuning`: Allow the system to automatically tune the TCP window size (default). When memory usage reaches the threshold of 80%, FortiProxy automatically changes the value to `system` to protect memory usage. • `system`: Use the system default TCP window size for this protocol. • `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`.

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
```

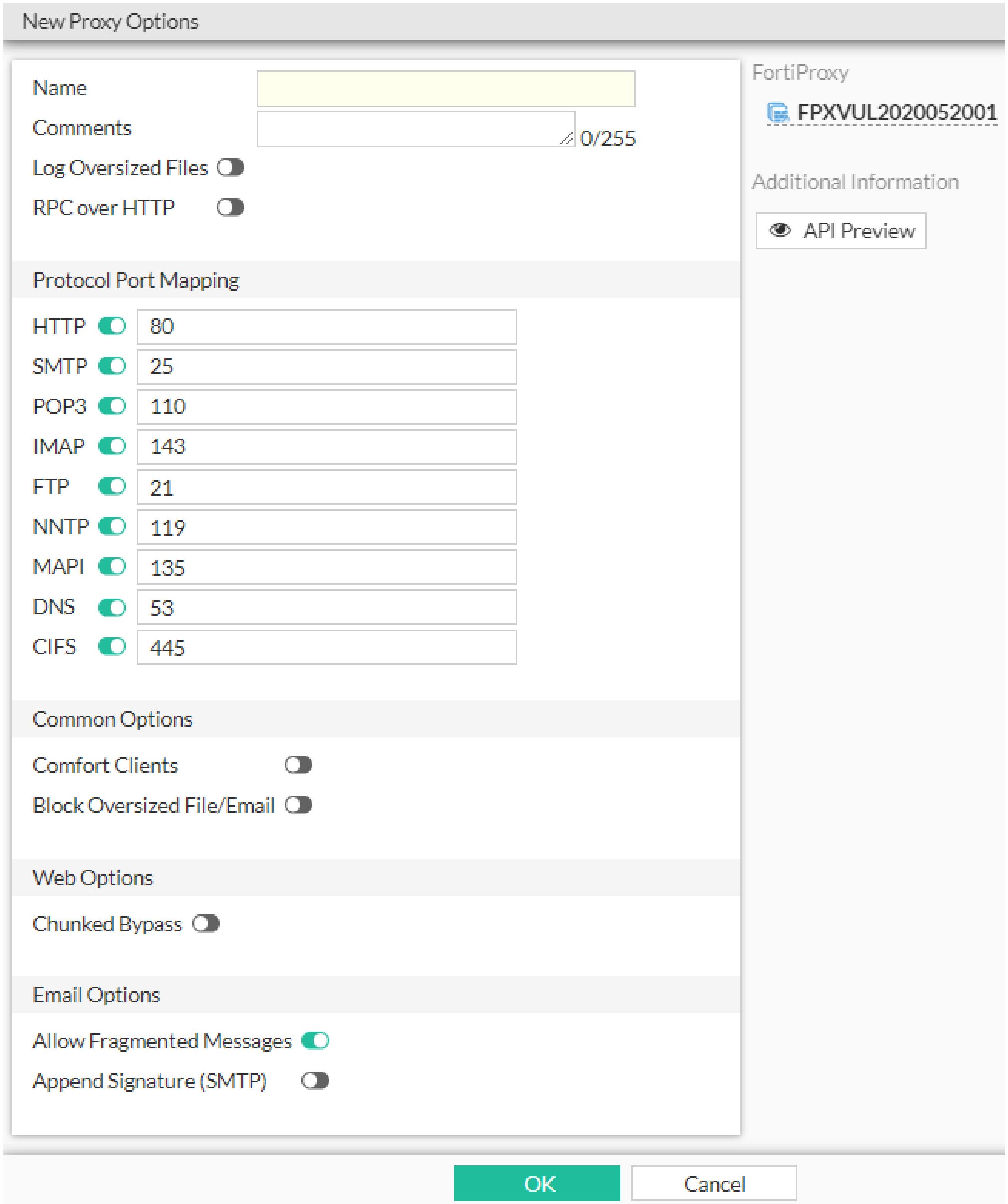
HTTP domain fronting blocking

To block HTTP domain fronting:

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

Create or edit a proxy option profile

To configure a new proxy option profile, go to *Proxy Settings > Proxy Options* and click *Create New*. The *New Proxy Options* page is displayed.



Configure the following settings and then click *OK* to save your changes:

Name	The name of the proxy option profile.

Comments	Optional description of the proxy option profile.
Log Oversized Files	Enable this setting to log when oversized files are processed. The setting does not change how the files are processed. It only enables the FortiProxy unit to log that they were either blocked or allowed through. A common practice is to allow larger files through without antivirus processing. This practice allows you to get an idea of how often this happens and decide on whether to alter the settings relating to the treatment of oversized files.
RPC over HTTP	Enable or disable the inspection of RPC over HTTP.
Protocol Port Mapping	To optimize the resources of the unit, enable or disable the mapping and inspection of protocols. When you enable a protocol, the default port numbers are automatically filled in, but you can change them.
Common Options	
Comfort Clients	When proxy-based antivirus scanning is enabled, the FortiProxy unit buffers files as they are downloaded. After the entire file is captured, the FortiProxy unit begins scanning the file. During the buffering and scanning procedure, the user must wait. After the scan is completed, if no infection is found, the file is sent to the next step in the process flow. If the file is a large one this part of the process can take some time. In some cases enough time that some users may get impatient and cancel the download. The *Comfort Clients* feature mitigates this potential issue by feeding a trickle of data while waiting for the scan to complete. The user then knows that processing is taking place and that there hasn't been a failure in the transmission. The slow transfer rate continues until the antivirus scan is complete. After the file has been successfully scanned and found to be clean of any viruses, the transfer will proceed at full speed. Enable and then configure the following: • *Interval (seconds)*—Enter the interval time in seconds. The default is 10. • *Amount (bytes*—Enter the amount in bytes. The default is 1.
Block Oversized File/Email	You can block files or emails that are larger than a specified size. Enable and then enter the threshold size in megabytes of the files and emails to block.
Web Options	
Chunked Bypass	The HTTP section allows the enabling of Chunked Bypass. This refers to the mechanism in version 1.1 of HTTP that allows a web server to start sending chunks of dynamically generated output in response to a request before actually knowing the actual size of the content. Where dynamically generated content is concerned, enabling this feature means that there is a faster initial response to HTTP requests. From a security stand point, enabling this feature means that the content is not held in the proxy as an entire file before proceeding. Enable or disable the chunked bypass setting.

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.

Create a CIFS proxy option

CIFS can be configure in the GUI by creating or editing a proxy option under *Proxy Settings* > *Proxy Options*, and in the CLI using the `config firewall profile-protocol-options` command. The `cifs-profile` command is no longer available from the `firewall policy` options.

The CIFS proxy option can then be used in a policy.

To create a CIFS proxy option:

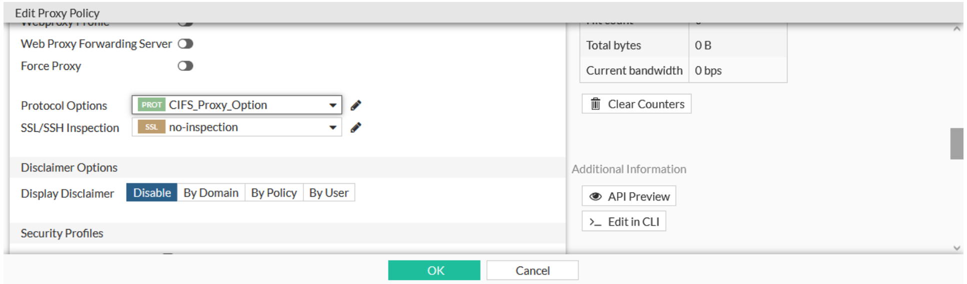
```
config firewall profile-protocol-options
    edit <option>
        config cifs
            set ports <port>
            set status {enable | disable}
            set options <string>
            set oversize-limit <integer>
            set uncompressed-oversize-limit <integer>
            set uncompressed-nest-limit <integer>
            set scan-bzip2 {enable | disable}
            set tcp-window-type {auto-tuning | system | static | dynamic}
            set server-credential-type {none | credential-replication | credential-keytab}
        end
    next
end
```

To use the CIFS proxy option in a policy:

- In the CLI, select the option using the set `profile-protocol-options <option>` command:

```
config firewall policy
    edit 1
        set profile-protocol-options <option>
    next
end
```

- In the GUI, select the option in the *Protocol Options* field when editing a policy.



SSL Keyring

The FortiProxy keyring file includes a list of SSL client certificates (maximum 240,000) or certificate chains in PEM format. The file is stored on the FortiProxy disk and is not encrypted. You can upload the file using the GUI or SCP.

The keyring list must start with `#keyring`, and uses the following format:

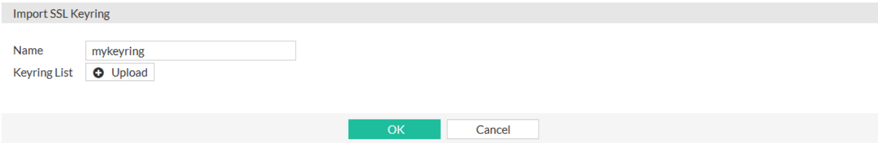
```
#keyring:1
<private_key_1>
<certificate_1>
<optional_certificate_chain_1>
#keyring:2
<private_key_2>
<certificate_2>
<optional_certificate_chain_2>
....
```

For example:

```
#keyring:1
-----BEGIN PRIVATE KEY-----
MC4CAQ...arfLXfXrEve+Yb8zQ
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MII...SDg==
-----END CERTIFICATE-----
#keyring:2
-----BEGIN EC PARAMETERS-----
Bg...Bw==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHc...onQ==
-----END EC PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MII...4Dh
-----END CERTIFICATE-----
```

To upload a keyring list in the GUI:

1. Go to *Proxy Settings* > *SSL Keyring* and click *Create New*.
2. Enter a name for the list.



3. Click *Upload* to upload the list from the management computer.
4. Click *OK*.

To upload a keyring list from the management computer using SCP:

```
scp <keyring-file-path> admin@<FPX address>:keyring-list:<optional profile name>
```

For example:

```
scp mykeyring admin@10.10.10.1:keyring-list:mykeyring
```

Network

The *Network* menu allows you to configure the unit to operate on the network. This menu provides features for configuring and viewing basic network settings, such as the unit's interfaces, Domain Name System (DNS) options, and routing table.

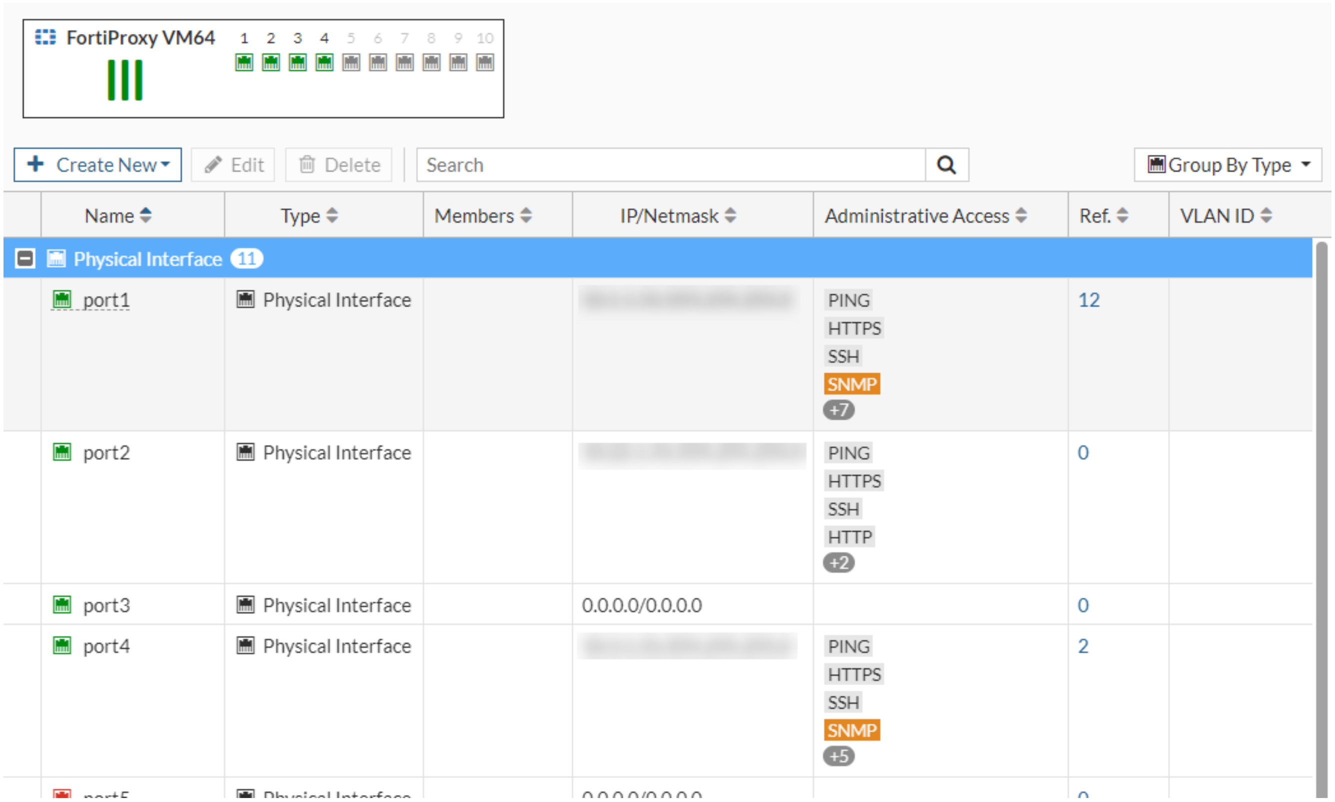
This section describes the following:

- Interfaces on page 95
- GRE Tunnel on page 109
- DNS Settings on page 112
- DNS Service on page 116
- Packet Capture on page 120
- Static routes on page 123
- Policy routes on page 126
- VXLAN on page 128

Interfaces

Unless stated otherwise, the term *interface* refers to a physical FortiProxy interface.

In *Network > Interfaces*, you can configure the interfaces that handle incoming and outgoing traffic.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

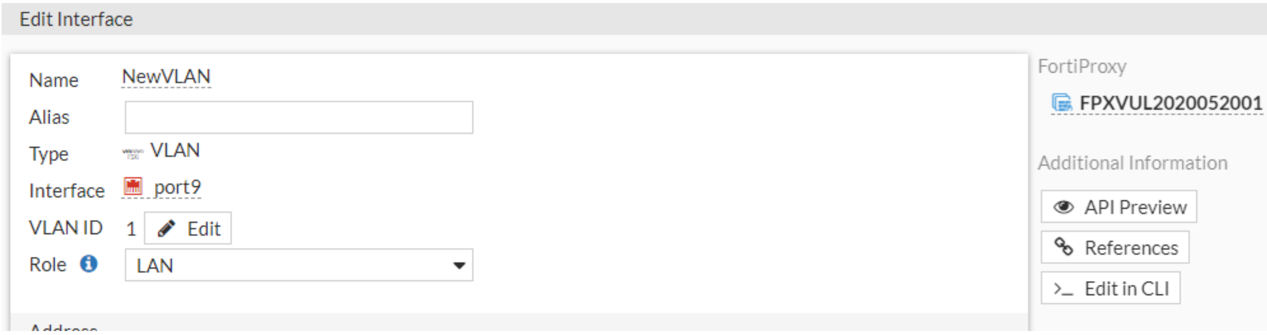
The following options are available:

Create New	Select to create an interface or a zone. See Create or edit an interface on page 101 and Create or edit a zone on page 107.
Edit	Modifies settings within the interface or zone. See Create or edit an interface on page 101 and Create or edit a zone on page 107.
Delete	Removes an interface from the list. To remove multiple interfaces, select multiple rows in the list by holding down the Ctrl or Shift keys and then select *Delete*.
Search	Enter a search term to find in the list.
Grouping	Select *Group By Type*, *Group By Role*, *Group By Status*, *Group By Zone*, or *No Grouping* to change how the rows are displayed on the interface list.
Status	The administrative status for the interface. If the administrative status is green, the interface is up and can accept network traffic. If the administrative status is red, the interface is administratively down and cannot accept traffic. To change the administrative status of an interface, right-click the icon and select the *Set Status* setting for the interface.

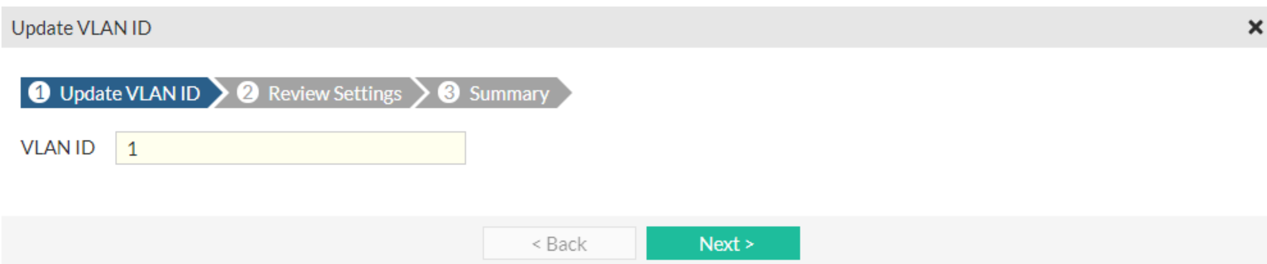
Name	The names of the physical interfaces on your FortiProxy unit. The names include any alias names that have been configured.
Type	The type of the interface, such as *Physical Interface*.
Members	Interfaces that belong to the virtual interface of the software switch.
IP/Netmask	The current IP address/netmask of the interface. When IPv6 Support is enabled on the GUI, IPv6 addresses are displayed in this column.
Administrative Access	The administrative access configuration for the interface.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in *Ref.*, and the *Object Usage* window appears displaying the various locations of the referenced object.
Bytes	The number of bytes being used.
Description	A description of the interface.
DHCP Clients	If the interface has been configured as a DHCP client.
DHCP Ranges	The range of IPv4 addresses.
Errors	Any errors detected.
IPv6 Access	The types of administrative access permitted for IPv6 connections to this interface.
IPv6 Address	The IPv6 address/subnet mask for the interface.
IPv6 DHCP Clients	If the interface has been configured as a DHCP client.
IPv6 DHCP Ranges	The range of IPv6 addresses.
Link Status	The status is *Up* when a valid cable is plugged in. The status is *Down* when an invalid cable is plugged in.
MAC Address	The MAC address of the interface.
Packets	The total number of packets that have been sent and received. Hover over the bar chart to see the separate packet numbers.
Role	The role can be *LAN*, *WAN*, *DMZ*, or *Undefined*.
Secondary IP(s)	The secondary IPv4 addresses added to the interface.
Secondary IPv6 Addresses	The secondary IPv6 addresses added to the interface.
Security Mode	The mode is either *None* or *Captive Portal*.
VLAN ID	The configured VLAN ID for VLAN subinterfaces.
VRRP	Whether the Virtual Router Redundancy Protocol is being used.
Zone	The name of the zone that the interface belongs to.

To change the VLAN ID:

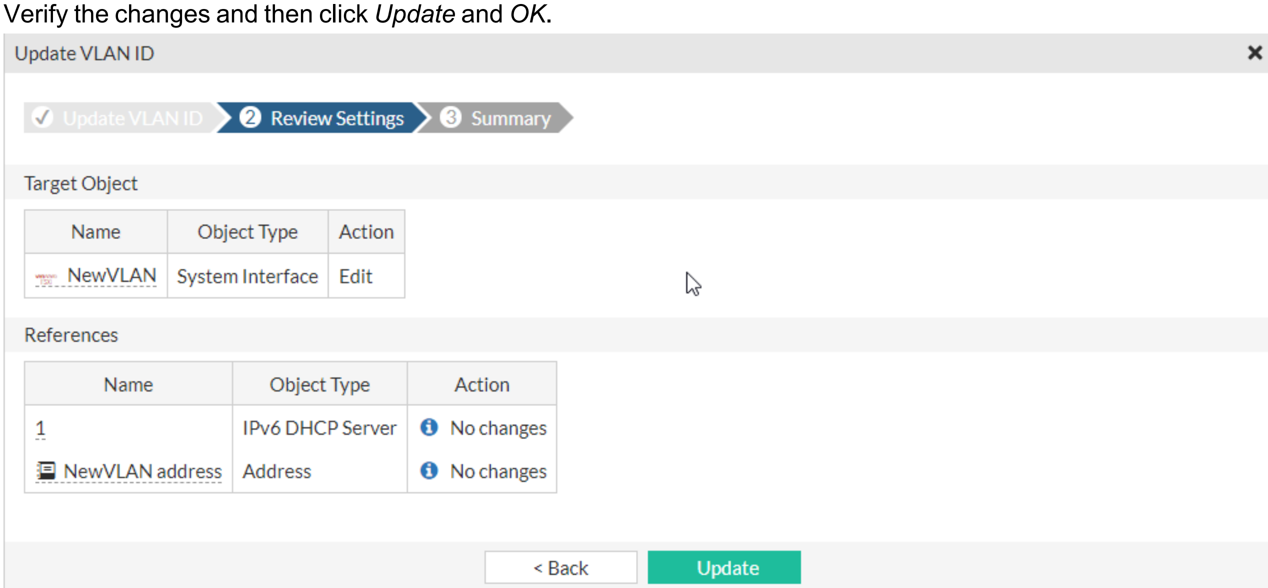
1. Go to *Network > Interfaces*, select a VLAN, and then click *Edit*.
2. Beside the *VLAN ID* field, click *Edit*. The *Update VLAN ID* window opens.



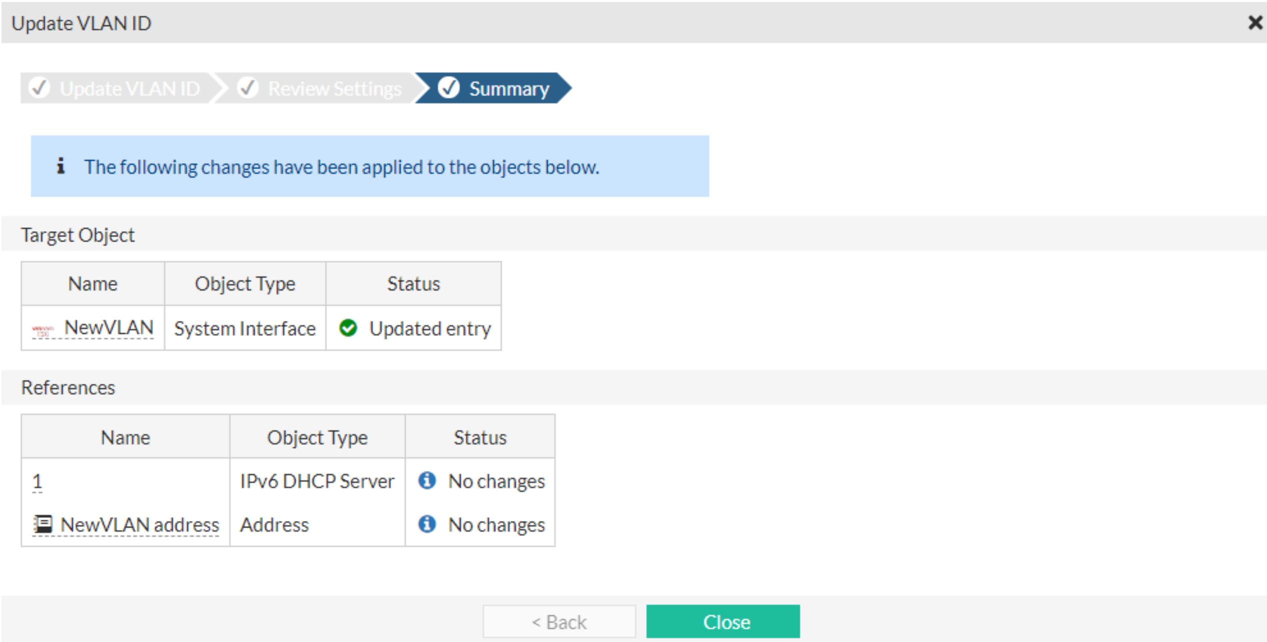
3. Enter the new ID and click *Next*.



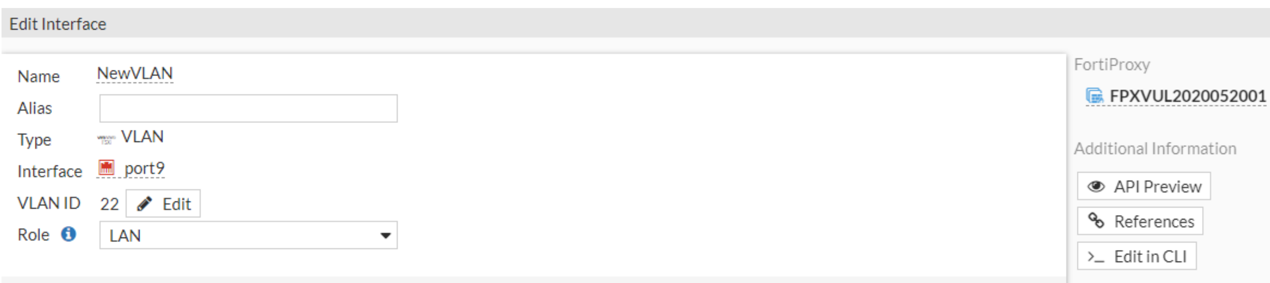
4. Verify the changes and then click *Update* and *OK*.



5. The target object status changes to *Updated entry*. Click *Close*.



In the interface settings, the new VLAN ID is displayed.



Link health monitor

A link health monitor confirms the connectivity of the device’s interface. You can detect possible routing loops with link health monitors. You can configure the FortiProxy unit to ping a gateway at regular intervals to ensure that it is online and working. When the gateway is not accessible, that interface is marked as down.

Set the `interval` (how often to send a ping) and `failtime` (how many lost pings are considered a failure). A smaller `interval` and smaller number of lost pings results in faster detection but creates more traffic on your network. You might also want to log CPU and memory usage, as a network outage causes your CPU activity to spike.

To configure a link health monitor using the CLI:

```
config system link-monitor
   edit <link_monitor_name>
      set srcintf <interface_name>
      set server <server_IP_address>
      set protocol {ping | tcp-echo | udp-echo | http | twamp}
      set gateway-ip <gateway_IPv4_address>
      set source-ip <IPv4_address>
      set interval <seconds>
      set timeout <seconds>
```

```
      set failtime <retry_attempts>
      set recoverytime <number_of_successful_responses>
      set ha-priority <priority>
      set update-cascade-interface {enable | disable}
      set update-static-route {enable | disable}
      set status {enable | disable}
   next
end
```

CLI option	Description
srcintf	The name of the interface to add the link health monitor to.
server	One or more IP addresses of the servers to be monitored. If the link health monitor cannot connect to all of the servers, remote IP monitoring considers the link to be down. You can add multiple IP addresses to a single link monitor to monitor more than one IP address from a single interface. If you add multiple IP addresses, the health checking will be with all of the addresses at the same time. The link monitor only fails when no responses are received from all of the addresses.
protocol	One or more protocols to be used to test the link. The default is `ping`.
gateway-ip	The IPv4 address of the remote gateway that the link monitor must communicate with to contact the server. Only required if there is no other route on for this communication.
source-ip	Optionally add a source IPv4 address for the monitoring packets. Normally the source address is the address of the source interface. You can add a different source address if required.
interval	The time between sending link health check packets. The default is 5 seconds. The range is 1 to 3600 seconds.
timeout	The time to wait before receiving a response from the server. The default is 1 second. The range is 1 to 255 seconds.
failtime	The number of times that a health check can fail before a failure is detected (the failover threshold). The default is 5. The range is 1 to 10.
recoverytime	The number of times that a health check must succeed after a failure is detected to verify that the server is back up. The default is 5. The range is 1 to 10.
ha-priority	The priority of this link health monitor when the ling health monitor is part of a remote link monitor configuration. The default is 1. The range is 1 to 50.
update-cascade-interface	Enable to bring down the source interface if the link health monitor fails. Disable to keep the interface up if the link health monitor fails. The default is `enable`.
update-static-route	Enable to remove static routes from the routing table that use this interface if the link monitor fails. The default is `enable`.
status	Enable or disable this link monitor. The default is `enable`.

Selecting the source interface and address for Telnet and SSH

The `execute telnet-options` and `execute ssh-options` commands 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
```

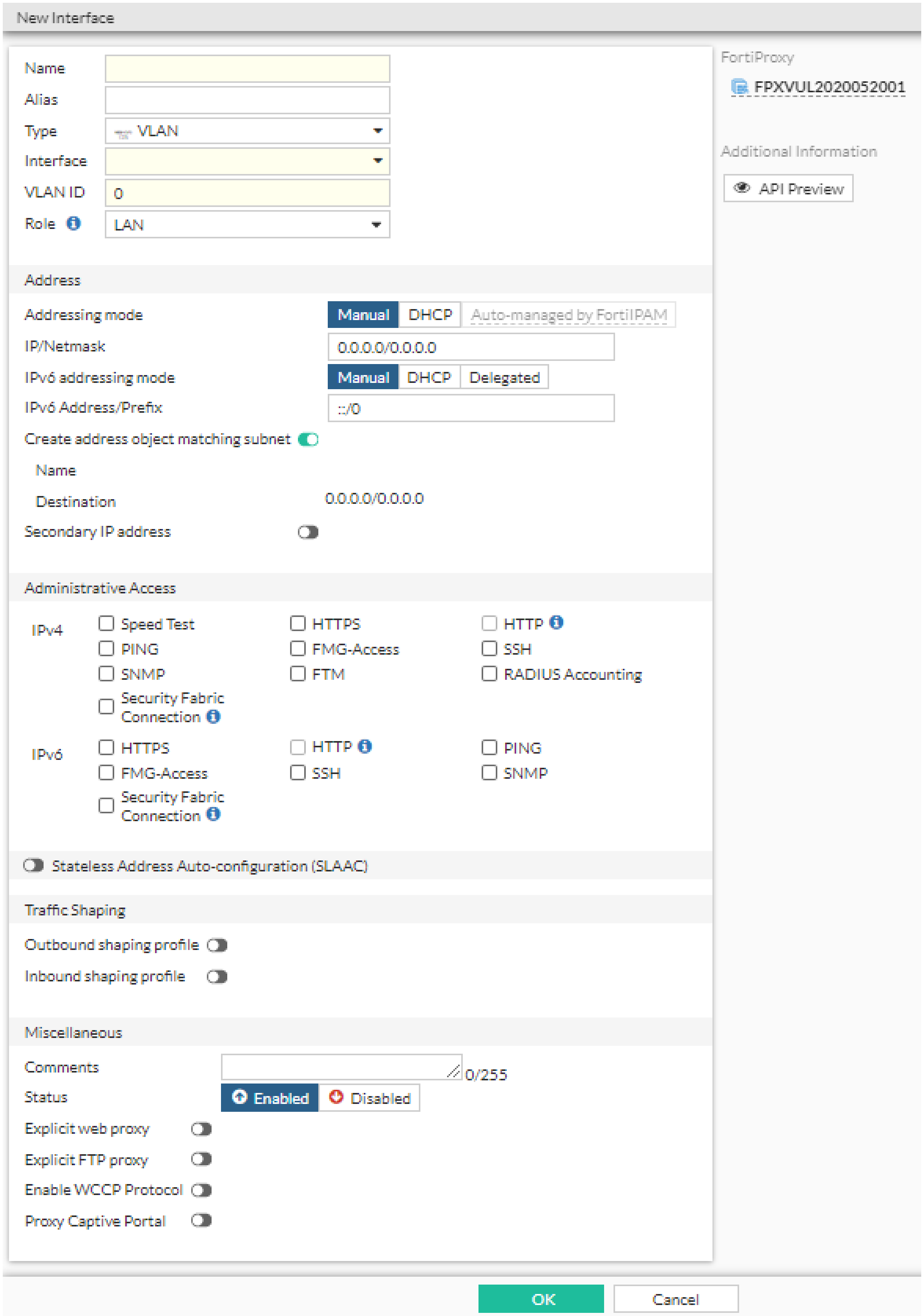
```
# execute ssh-options source 1.1.1.1
```

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
```

Create or edit an interface

Selecting *Create New* > *Interface* opens the *New Interface* page, which provides settings for configuring a new interface.


New Interface
Name
Alias
Type
VLAN
Interface
VLAN ID
0
Role
LAN
FortiProxy
FPXVUL2020052001
Additional Information
API Preview
Address
Addressing mode
Manual
DHCP
Auto-managed by FortiIPAM
IP/Netmask
0.0.0.0/0.0.0.0
IPv6 addressing mode
Manual
DHCP
Delegated
IPv6 Address/Prefix
::/0
Create address object matching subnet
Name
Destination
0.0.0.0/0.0.0.0
Secondary IP address
Administrative Access
IPv4
Speed Test
HTTPS
HTTP
PING
FMG-Access
SSH
SNMP
FTM
RADIUS Accounting
Security Fabric Connection
IPv6
HTTPS
HTTP
PING
FMG-Access
SSH
SNMP
Security Fabric Connection
Stateless Address Auto-configuration (SLAAC)
Traffic Shaping
Outbound shaping profile
Inbound shaping profile
Miscellaneous
Comments
0/255
Status
Enabled
Disabled
Explicit web proxy
Explicit FTP proxy
Enable WCCP Protocol
Proxy Captive Portal
OK
Cancel

Selecting an interface and then selecting *Edit* opens the *Edit Interface* page.

Configure the following settings in the *New Interface* page or *Edit Interface* page and click *OK*:

Name	Enter a name for the interface. Physical interface names cannot be changed. If VLAN pooling is enabled, the maximum name length is 10 characters. You cannot edit the interface name after you create the interface.
Alias	Enter an alternate name for a physical interface on the FortiProxy unit. The alias can be a maximum of 25 characters. The alias name does not appear in logs. This field appears when editing an existing physical interface.
Type	Select the type of the interface: *VLAN*, *802.3ad Aggregate*, or *Redundant Interface*. Refer to Aggregation on page 106 for more information about the Aggregate interface type.
Interface Members	Select the ports to be included in the interface if the *Type* is *802.3ad Aggregate* or *Redundant Interface*.
Interface	This field is available when *Type* is set to *VLAN*. Select the name of the physical interface that you want to add a VLAN interface to. After it is created, the VLAN interface is listed below its physical interface in the Interface list. You cannot change the physical interface of a VLAN interface.
VLAN ID	This field is available when *Type* is set to *VLAN*. Enter the VLAN ID. You cannot change the VLAN ID except when you add a new VLAN interface. The VLAN ID must be a number between 1 and 4094. It must match the VLAN ID that the IEEE 802.1Q-compliant router or switch that is connected to the VLAN subinterface adds.
Role	Set the role setting for the interface. Different settings will be shown or hidden when editing an interface depending on the role. • *LAN*: Used to connected to a local network of endpoints • *WAN*: Used to connected to the internet. • *DMZ*: Used to connected to the DMZ. When selected, DHCP server and Security mode are not available. • *Undefined*: The interface has no specific role.
Estimated bandwidth	The estimated WAN bandwidth. Enter the upstream and downstream bandwidth. These values are used to estimate WAN usage.
Addressing mode	Select the addressing mode for the interface: • Select *Manual* and add an IPv4 address and network mask for the interface. If IPv6 configuration is enabled, you can add both an IPv4 and an IPv6 IP address. • Select *DHCP* to get the interface IP address and other network settings from a DHCP server. • Select *Auto-managed by FortiIPAM* if you have FortiIPAM Cloud. The FortiIPAM (IP Address Management) service automatically assigns subnets

	to the FortiProxy unit to prevent duplicate IP addresses from overlapping within the same Security Fabric. FortiIPAM is a paid service and must be registered to the FortiProxy unit in FortiCare.
IP/Netmask	Enter an IPv4 address and subnet mask for the interface. FortiProxy interfaces cannot have IP addresses on the same subnet. This option is available only if *Addressing mode* is set to *Manual*.
Retrieve default gateway from server	Enable this to retrieve a default gateway IP address from the DHCP server. The default gateway is added to the static routing table. This option is available only if *Addressing mode* is set to *DHCP*.
Distance	Enter the administrative distance for the default gateway retrieved from the DHCP server. The administrative distance is an integer from 1 to 255, and specifies the relative priority of a route when there are multiple routes to the same destination. A lower administrative distance indicates a more preferred route. This option is available only if *Addressing mode* is set to *DHCP* and *Retrieve default gateway from server* is enabled.
Override internal DNS	Enable this to use the DNS addresses retrieved from the DHCP server instead of the DNS server IP addresses on the DNS page. This option is available only if *Addressing mode* is set to *DHCP*.
IPv6 Addressing mode	Select the addressing mode for the interface: • Select *Manual* and add an IP address and network mask for the interface. • Select *DHCP* to get the interface IP address and other network settings from a DHCP server. • Select *Delegated* to select an *IPv6 upstream interface* that has DHCPv6 prefix delegation enabled and enter an *IPv6 subnet* if needed. The interface will get the IPv6 prefix from the upstream DHCPv6 server that is connected to the IPv6 upstream interface and form the IPv6 address with the subnet configured on the interface.
IPv6 Address/Prefix	If *Addressing Mode* is set to *Manual* and IPv6 support is enabled, enter an IPv6 address and subnet mask for the interface. A single interface can have an IPv4 address, IPv6 address, or both.
Create address object matching subnet	This option is available when *Role* is set to *LAN* or *DMZ*. Enable this option to automatically create an address object that matches the interface subnet.
Secondary IP address	Add additional IPv4 addresses to this interface.
IPv6 Address/Prefix	If IPv6 support is enabled on the GUI, enter an IPv6 address and subnet mask for the interface. A single interface can have both an IPv4 and IPv6 address or just one or the other. This option is available only if *IPv6 Addressing mode* is set to *Manual*.
IPv4 IPv6	Select the types of administrative access permitted for IPv4 and IPv6 connections to this interface.
Speed Test	Allows speed tests to be executed on the interface.

HTTPS	Allow secure HTTPS connections to the GUI through this interface.
HTTP	HTTP traffic is automatically redirected to HTTPS.
PING	Interface responds to pings. Use this setting to verify your installation and for testing.
FMG-Access	Allow FortiManager to access this interface.
SSH	Allow SSH connections to the CLI through this interface.
SNMP	Allow a remote SNMP manager to request SNMP information by connecting to this interface.
FTM	Allow FTM Push notifications, for when users are attempting to authenticate through a VPN and/or RADIUS (with FortiAuthenticator as the RADIUS server).
RADIUS Accounting	Allow RADIUS accounting records that the server forwards (originating from the RADIUS client). These records include the user's IP address and user group.
Security Fabric Connection	Allow Security Fabric access. This access enables CAPWAP and FortiTelemetry.
Stateless Address Auto-configuration	Enable to provide IPv6 addresses to connected devices using SLAAC.
IPv6 prefix list	Enable to provide a list of IPv6 prefixes.
IPv6 prefix	Enter the IPv6 prefix.
Outbound shaping profile	Enable or disable traffic shaping on the interface. This allows you to enforce bandwidth limits on individual interfaces.
Outbound bandwidth	Enable to specify the outbound bandwidth.
Inbound shaping profile	Enable or disable traffic shaping on the interface. This allows you to enforce bandwidth limits on individual interfaces.
Inbound bandwidth	Enable to specify the inbound bandwidth.
Comments	Enter a description of the interface of up to 255 characters.
Status	Enable or disable the interface.
Explicit web proxy	Select this to enable explicit web proxying on this interface.
Explicit FTP proxy	Enable or disable explicit FTP proxying on this interface.
Enable WCCP Protocol	The Web Cache Communication Protocol (WCCP) can be used to provide web caching with load balancing and fault tolerance. In a WCCP configuration, a WCCP server receives HTTP requests from a user's web browsers and redirects the requests to one or more WCCP clients. The clients either return cached content or request new content from the destination web servers before caching it and returning it to the server, which in turn returns the content to the original requester. If a WCCP configuration includes multiple WCCP clients, the WCCP server load balances traffic among the clients and can detect when a client fails and failover sessions to still operating clients. WCCP is described by the Web Cache Communication Protocol Internet draft.

Proxy Captive Portal	Enable or disable proxy captive portal on this interface.
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 add secondary IP addresses:

1. Go to *Network > Interfaces* and select *Create New > Interface*.
2. Enable *Secondary IP Address*.
3. Select *Create New*.
4. Enter the IPv4 address and network mask.
5. Select the types of administrative access to allow.
6. Click *OK*. The new IP address is added to the table.

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.

Aggregation

Link aggregation (IEEE 802.3ad) enables you to bind two or more physical interfaces together to form an aggregated (combined) link. This new link uses the total bandwidth of the functioning links in the group, up to eight. If a link in the group fails, traffic is transferred automatically to the remaining interfaces. The only noticeable effect is reduced bandwidth.

Only physical interfaces can be used in an aggregated (combined) link. You cannot aggregate VLAN interfaces, subinterfaces, or HA heartbeat interfaces. Each physical interface can belong to only one aggregated interface. If VDOM is enabled, all interfaces in the aggregated interface must be in the same VDOM.

Interfaced included in an aggregate interface are not listed under *Network > Interfaces* and cannot be configured individually with an IP address, DHCP, or PPPoE. They also cannot not be referenced in security policies, VIPs, IP pools, routing, or multicast policies. While you can see such interfaces in the CLI, configurations for those interfaces do not take effect.

Example configuration

This example creates an aggregate interface on a FortiProxy using ports 3-5 with an internal IP address of 10.1.1.123, as well as the administrative access to HTTPS and SSH.

To create an aggregate interface in the GUI:

1. Go to *Network > Interfaces* and select *Create New > Interface*.
2. Set *Name* to *aggregate*.

3. Set *Type* to *802.3ad Aggregate*.
4. Set *Interface members* to *port4*, *port5*, and *port6*.
5. Set *Addressing mode* to *Manual*.
6. Set *IP/Netmask* to *10.1.1.123/24*.
7. For *Administrative Access*, select *HTTPS* and *SSH*.
8. Click *OK*.

See Create or edit an interface on page 101 for more information.

To create an aggregate interface in the CLI:

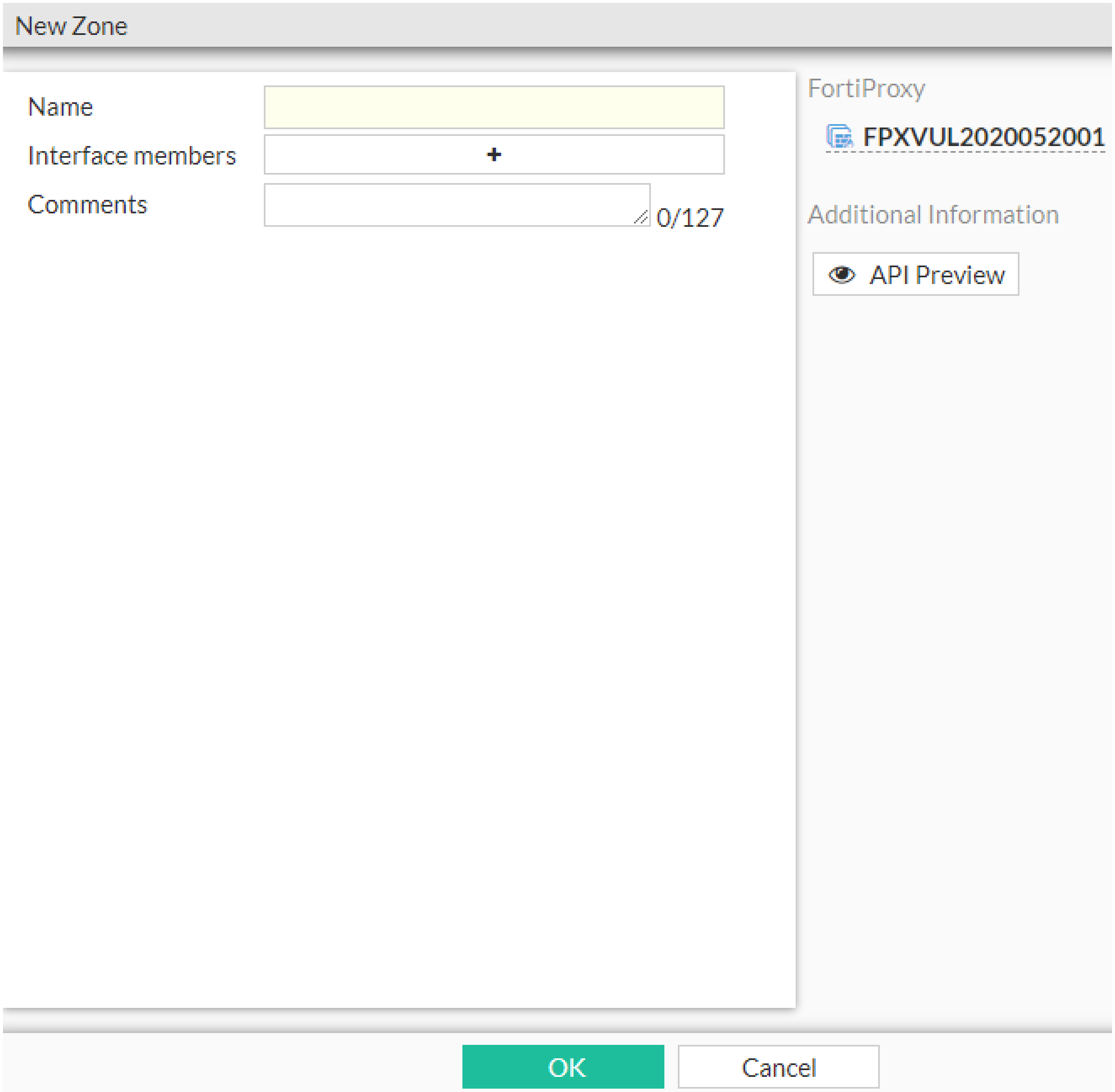
```
config system interface
    edit "aggregate"
        set vdom "root"
        set ip 10.1.1.123 255.255.255.0
        set allowaccess https ssh
        set type aggregate
        set member "port4" "port5" "port6"
        set snmp-index 45
    next
end
```

See `config system interface` for more information.

Create or edit a zone

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.

Selecting *Create New* > *Zone* opens the *New Zone* page, which provides settings for configuring a new zone.



Selecting a zone and then selecting *Edit* opens the Edit Zone page.

Configure the following settings in the New Zone page or Edit Zone page and click *OK*:

Name	Enter a name for the zone. You can change the name of the zone after creating it.
Interface Members	Select the ports to be included in the zone.
Comments	Enter a description up to 255 characters to describe the zone.
API Preview	Select the ports to be included in the zone.

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.

To create a zone:

```
config system zone
   edit <zone_name>
      set description <string>
      set interface <interface_names>
   next
end
```

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==&

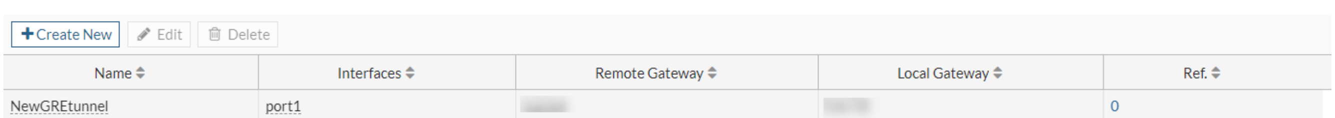
Content-Length: 0

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.

GRE Tunnel

The Generic Routing Encapsulation (GRE) tunnel allows direct communication between two nodes on a network.

Go to *Network > GRE Tunnel* to see which GRE tunnels have been configured.



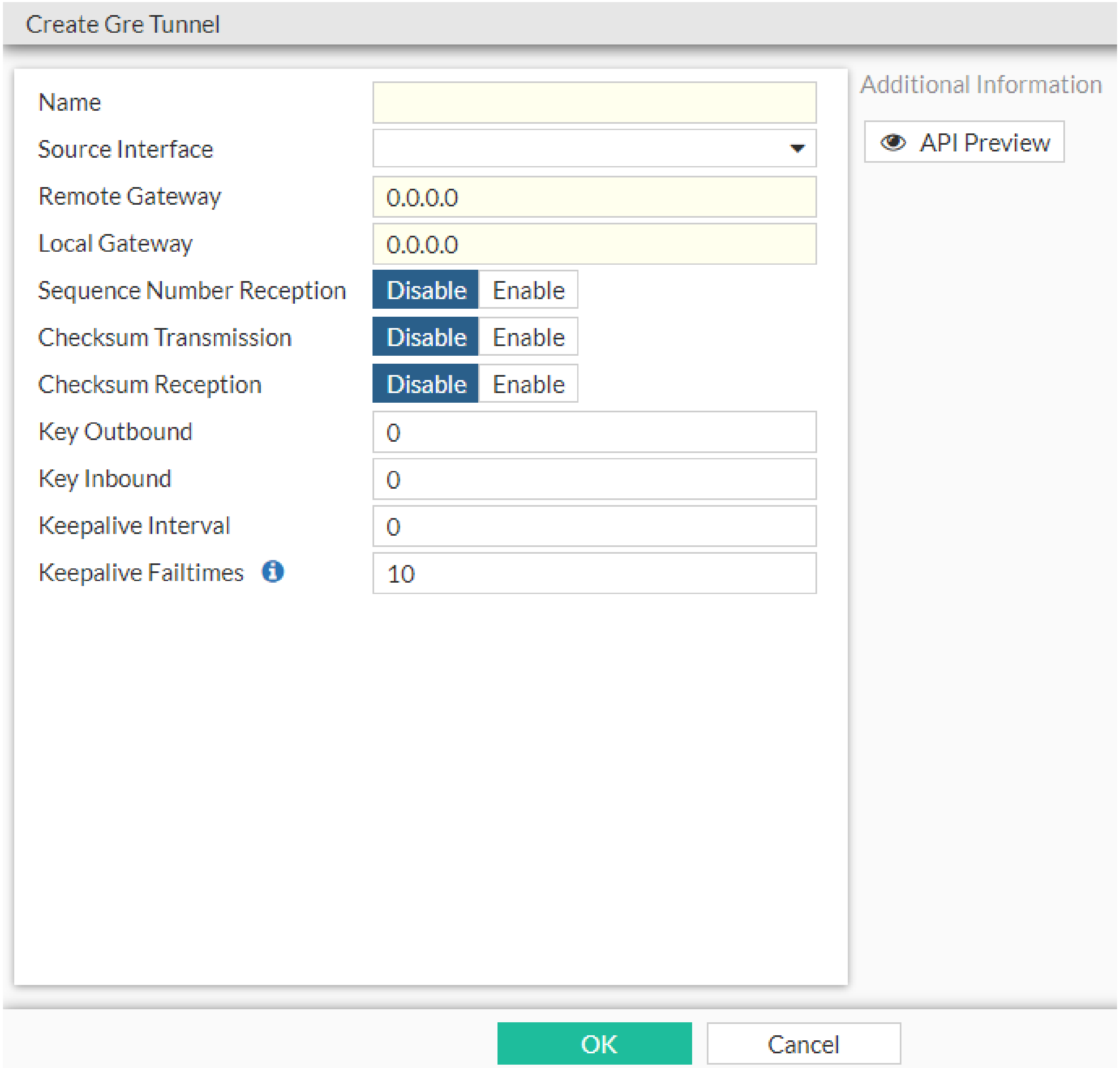
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Select to create a GRE tunnel. See Create or edit a GRE tunnel on page 110.
Edit	Modifies settings for the selected GRE tunnel. When you click *Edit*, the Edit GRE Tunnel page opens.
Delete	Removes the selected GRE tunnel.
Name	The name of the GRE tunnel.
Interfaces	Name of the source interface.
Remote Gateway	IP address of the remote gateway.
Local Gateway	IP address of the local gateway.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a GRE tunnel

Select *Create New* to open the *Create Gre Tunnel* page.



Select a GRE tunnel and then click *Edit* to open the *Edit Gre Tunnel* page.

Configure the following settings in the *Create Gre Tunnel* page or *Edit Gre Tunnel* page and then click *OK*:

Name	Enter the name to identify the GRE tunnel. You cannot edit the name after you create the GRE tunnel.
Source Interface	Name of the source interface. There is no default value.
Remote Gateway	IP address of the remote gateway. The default is 0.0.0.0.
Local Gateway	IP address of the local gateway. The default is 0.0.0.0.

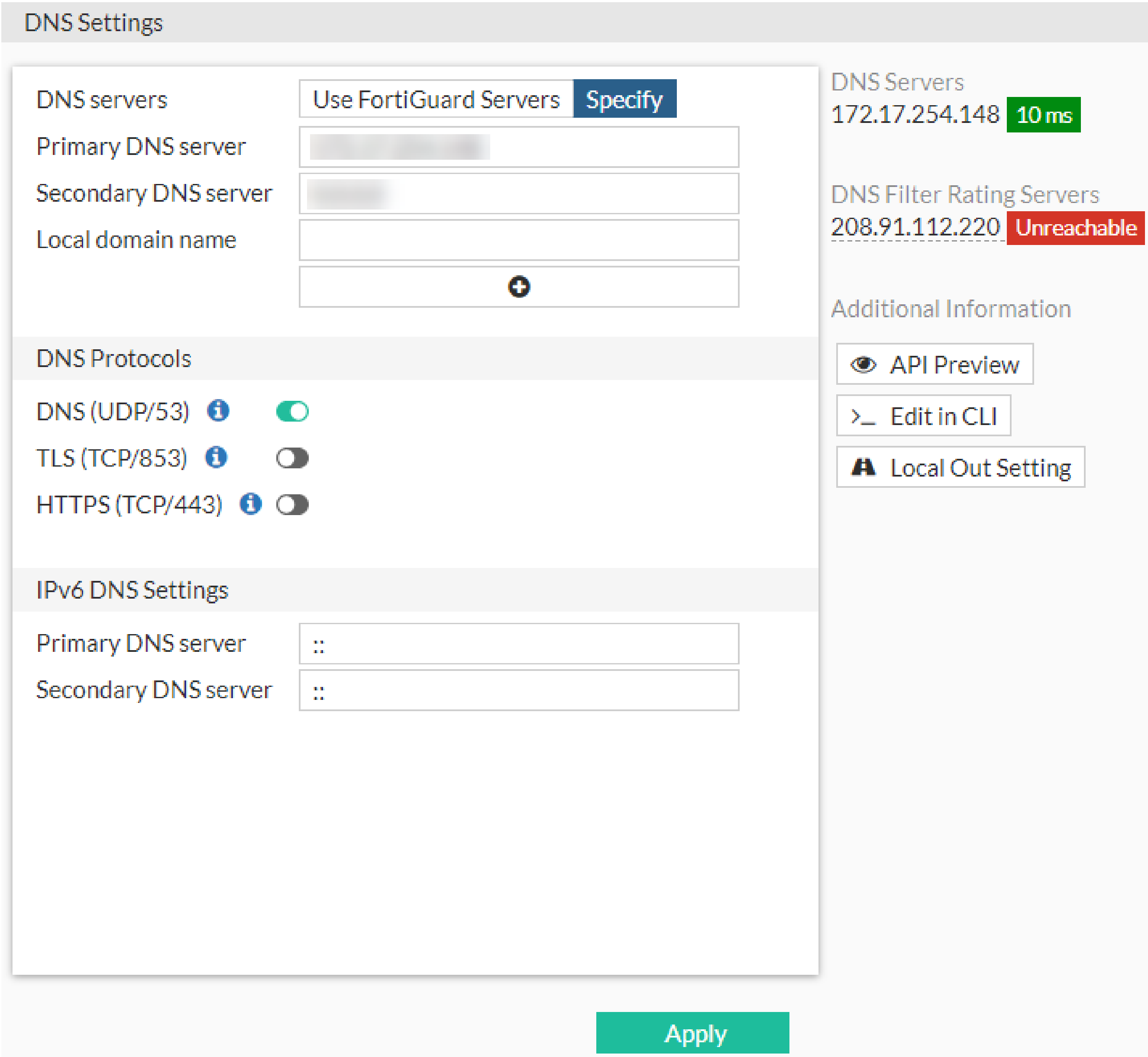
Sequence Number Reception	Enable or disable whether sequence numbers are validated in the received GRE packets. The default is disable.
Checksum Transmission	Enable or disable whether checksums are included in transmitted GRE packets. The default is disable.
Checksum Reception	Enable or disable whether checksums are validated in received GRE packets. The default is disable.
Key Outbound	Enter the key to be included in transmitted GRE packets. The range is 0 to 4,294,967,295. The default is 0.
Key Inbound	Enter the key that is required to be in received GRE packets. The range is 0 to 4,294,967,295. The default is 0.
Keepalive Interval	Specify how many minutes pass before a GRE keep-alive message is sent. The range is 0 to 32,767. Enter 0 to disable this feature. The default is 0.
Keepalive Failtimes	How many times the GRE keep-alive message fails before the GRE connection is considered down. The range is 1-255. The default is 10.
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.

DNS Settings

Several FortiProxy functions use DNS, including alert email. You can specify the IP addresses of the DNS servers that your unit connects to. DNS server IP addresses are usually supplied by your ISP. To configure DNS settings, go to *Network > DNS Settings*.



Configure the following settings and select *Apply*:

DNS Servers	Select *Use FortiGuard Severs* or *Specify*. If you select *Specify*, enter the IP addresses for the primary and secondary DNS servers. See also Use DNS over TLS for default FortiGuard DNS servers on page 114.
Primary DNS Server	Enter the IPv4 or IPv6 address for the primary DNS server.
Secondary DNS Server	Enter the IPv4 or IPv6 address for the secondary DNS server.
Local Domain Name	Enter the domain name to append to addresses with no domain portion when performing DNS lookups.
DNS (UDP/53)	Enable or disable the use of clear-text DNS over port 53.

TLS (TCP/853)	Enable or disable the use of DNS over TLS (DoT).
HTTPS (TCP/443)	Enable or disable the use of DNS over HTTPS (DoH).
SSL certificate	Select which SSL certificate or click *Create* to import a certificate.
Server hostname	Enter the host name of the DNS server.

To enable DoT and DoH DNS in the CLI:

```
config system dns
   set primary <IP_address>
   set secondary <IP_address>
   set protocol {cleartext | dot | doh}
end
```

Using the 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
```

Use DNS over TLS for default FortiGuard DNS servers

When using FortiGuard servers for DNS, the FortiProxy unit defaults to using DNS over TLS (DoT) to secure the DNS traffic. New FortiGuard DNS servers are added as primary and secondary servers.

Because DNS servers probably do not support low encryption DES, low encryption devices do not have the option to select DoT or DoH. The devices default to cleartext (UDP/53) instead.

The FortiGuard DNS server certificates are signed with the globalsdns.fortinet.net hostname by a public CA. The FortiProxy unit verifies the server hostname using the `server-hostname` setting.

To view the FortiGuard server DNS settings in the GUI:

1. Go to *Network > DNS Settings*.
2. For *DNS servers*, select *Use FortiGuard Servers*.
   The *Primary DNS server* is *96.45.45.45*, and the *Secondary DNS server* is *96.45.46.46*. *DNS Protocols* is set to *TLS* and cannot be modified.

To view the FortiGuard server DNS settings in the CLI:

```
# show system dns
config system dns
    set primary 96.45.45.45
    set secondary 96.45.46.46
    set protocol dot
    set server-hostname "globalsdns.fortinet.net"
end
```

The `protocol` and `server-hostname` settings should not be modified when using the default FortiGuard servers.

Alternate DNS servers

The alternate DNS servers are used only when DNS resolution of the primary or secondary DNS servers return a name error (NXDOMAIN). They are not used as failover DNS servers. If the query in the primary list times out, no alternate DNS server is contacted.

To configure the alternate DNS servers:

```
config system dns
    set alt-primary <ip_address>
    set alt-secondary <ip_address>
end
```

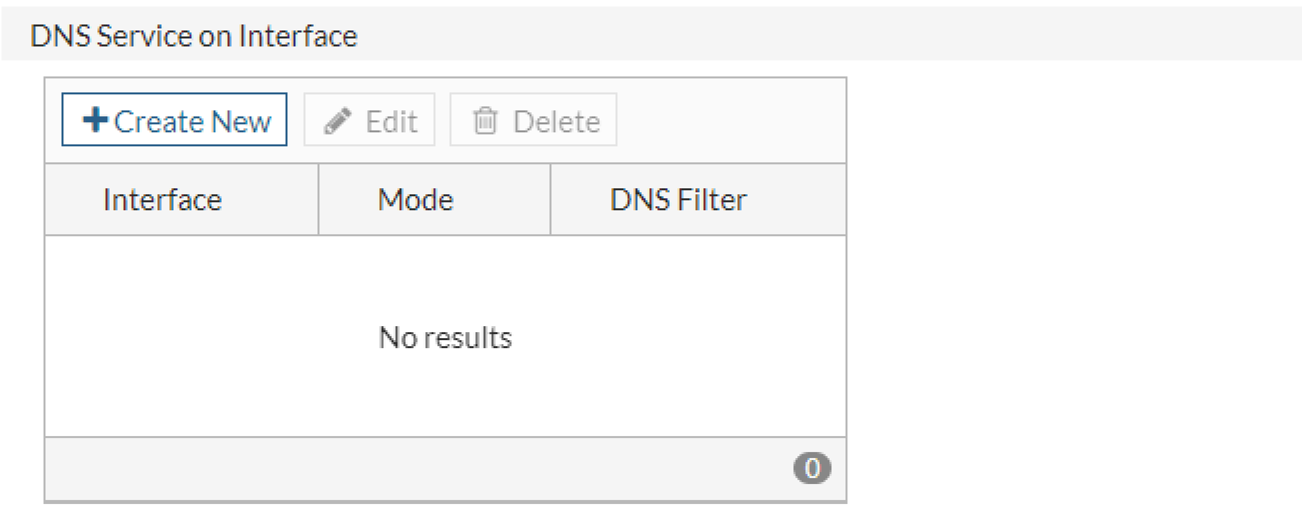
`alt-primary <ip_address>`	Alternate primary DNS server. This is not used as a failover DNS server.
`alt-secondary <ip_address>`	Alternate secondary DNS server. This is not used as a failover DNS server.

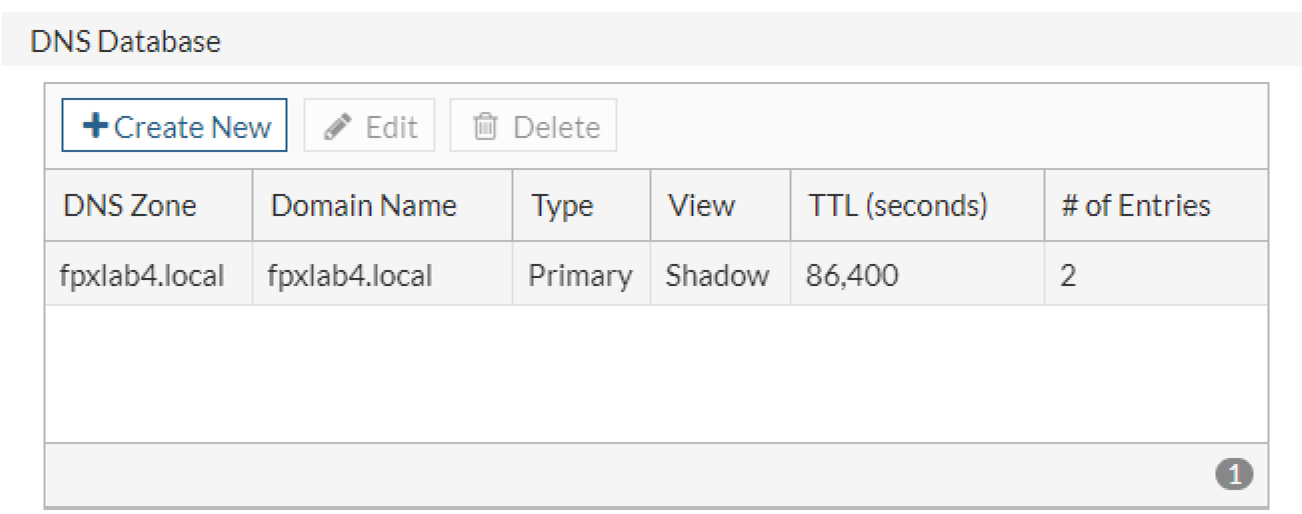
DNS Service

You can create local DNS servers for your network. Depending on your requirements, you can manually maintain your entries (primary DNS server) or use it as a jumping point, where the server refers to an outside source (secondary DNS server). A local primary DNS server works similarly to the DNS server addresses configured in *Network > DNS Settings*, but you must manually add all entries. This allows you to add a local DNS server to include specific URL and IP address combinations.

You can set an option to ensure this type of DNS server is not the authoritative server. When configured as a recursive DNS, the FortiProxy unit will check its internal DNS server (primary or secondary). If the request cannot be fulfilled, it will look to the external DNS servers. This is known as a split DNS configuration.

To configure DNS servers and zones, go to *Network > DNS Service*.





Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

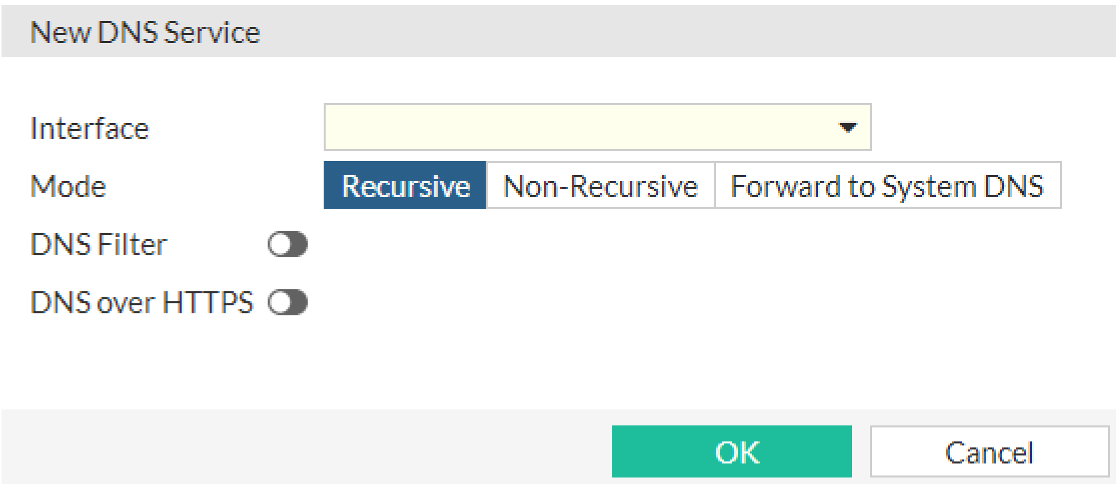
From the *DNS Service* page, you can do the following:

- Create or edit a DNS service on page 117
- Create or edit a DNS zone on page 118

Create or edit a DNS service

To add a DNS service on a specific interface:

1. Go to *Network > DNS Service* and, under *DNS Service on Interface*, select *Create New*.



2. Select an interface.
3. Select *Recursive*, *Non-Recursive*, or *Forward to System DNS*.
4. Enable *DNS Filter* if you want to use a DNS filter and select the DNS filter to use.
5. Enable *DNS over HTTPS* if you want to use DNS over HTTPS.
6. Click *OK*. The new DNS service is added to the table.

To edit a DNS service:

1. Go to *Network > DNS Service* and, under *DNS Service on Interface*, select a DNS service.
2. Select *Edit*.
3. Make your changes.
4. Click *OK*.

To enable DNS over HTTPS (DoH) on the DNS server in the CLI:

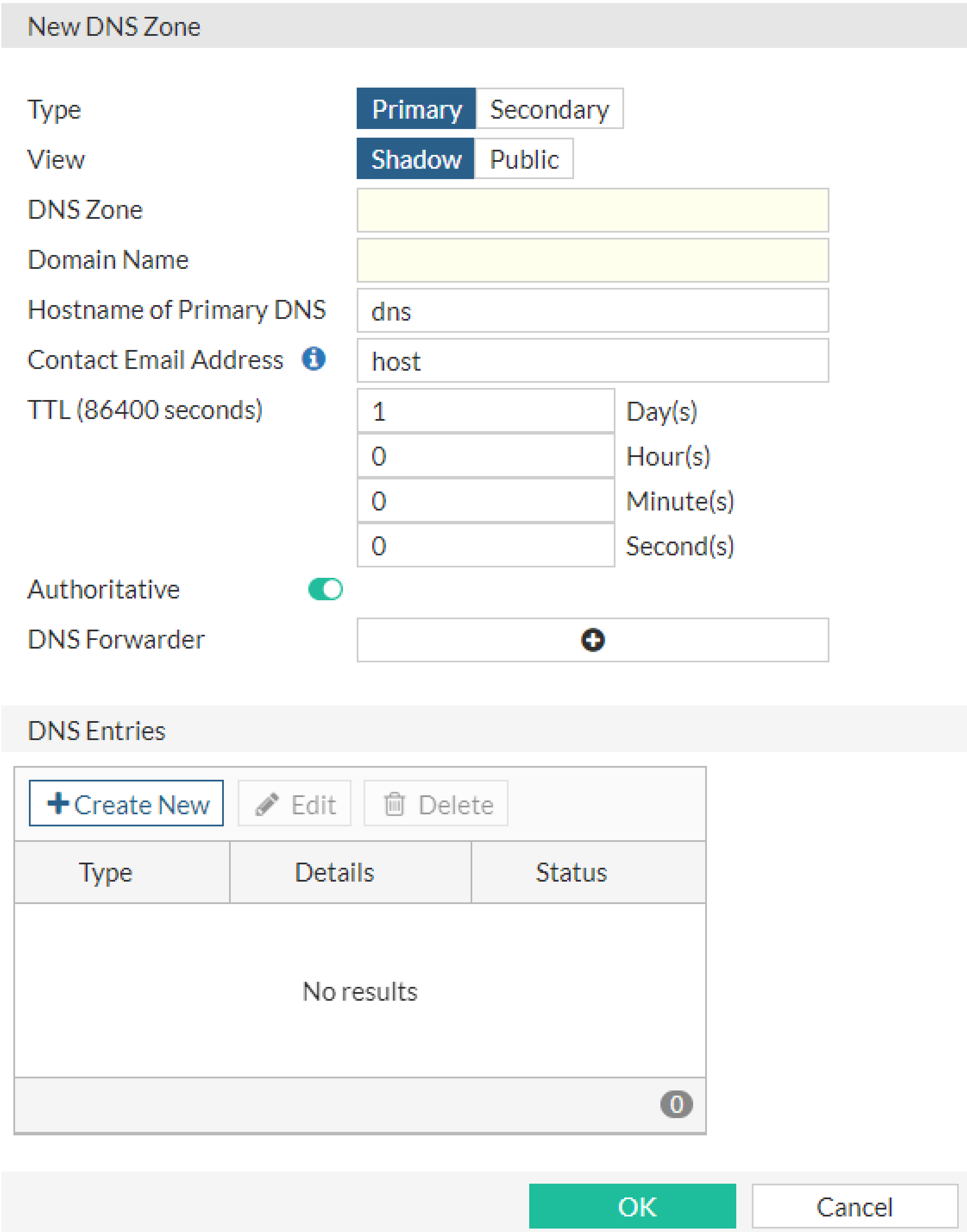
```
config system dns-server
   edit {<DNS_server_name> | <interface_name>}
      set dnsfilter-profile {<profile_name> | default}
      set doh enable
   next
end
```

Create or edit a DNS zone

You can create a primary or secondary DNS zone.

To create a primary DNS zone:

1. Go to *Network > DNS Service* and, under *DNS Database*, select *Create New*.



2. Select *Primary* for the type of DNS zone.
3. Select the accessibility of the DNS server. If you select *Public*, external users can use the DNS server. If you select *Shadow*, only internal users can use it.
4. Enter a name for the DNS zone.
5. Enter the domain name.
6. Enter the host name of the primary DNS server.
7. Enter the contact email address for the administrator, for example, `admin@example.com`.
8. Enter how long the DNS zone should exist in days, hours, minutes, and seconds. The maximum time to live (TTL) is 86,400 seconds.
9. Enable *Authoritative* if you want an authoritative zone.
10. Enter the IP address for the DNS zone forwarder.
11. Select or create a DNS entry. See Create or edit a DNS entry on page 119.
12. Click *OK* to save your new DNS zone. The new DNS zone is added to the table.

To create a secondary DNS zone:

1. Go to *Network > DNS Service* and, under *DNS Database*, select *Create New*.
2. Select *Secondary* for the type of DNS zone.
3. Select the accessibility of the DNS server. If you select *Public*, external users can use the DNS server. If you select *Shadow*, only internal users can use it.
4. Enter a name for the DNS zone.
5. Enter the domain name.
6. Enter the IP address of the primary DNS zone.
7. Enable *Authoritative* if you want an authoritative zone.
8. Enter the IP address for the DNS zone forwarder.
9. Click *OK* to save your new DNS zone. The new DNS zone is added to the table.

To edit a DNS zone:

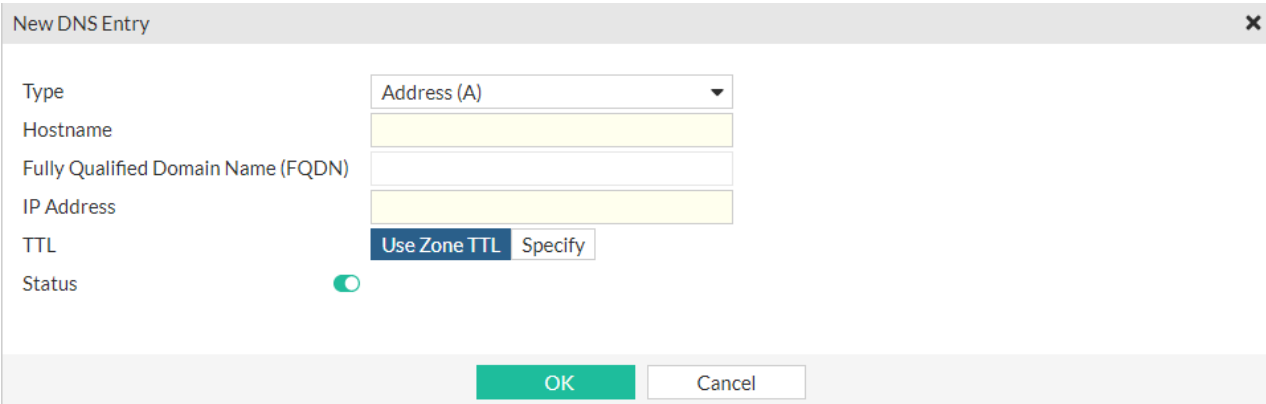
1. Go to *Network > DNS Service* and, under *DNS Database*, select a DNS zone.
2. Select *Edit*.
3. Make your changes.
4. Click *OK* to save your changes.

Create or edit a DNS entry

You can create or edit a DNS entry for the DNS service.

To create a DNS entry:

1. Go to *Network > DNS Service* and, under *DNS Database*, select a DNS zone and then click *Edit*.
2. In the *Edit DNS Zone* page, select *Create New*.



3. Select the type of DNS entry, one of *Address (A)*, *Name Server (NS)*, *Canonical Name (CNAME)*, *Mail Exchange (MX)*, *IPv6 Address (AAAA)*, *IPv4 Pointer (PTR)*, or *IPv6 Pointer (PTR)*.
4. Enter the host name for the DNS entry.
5. Enter the fully qualified domain name for the DNS entry.
6. Enter the IP address for the DNS entry.
7. For the time to live (TTL), select *Use Zone TTL* or *Specify*. If you select *Specify*, enter the number of days, hours, minutes, and seconds, up to a maximum of 86,400 seconds.
8. Enable or disable *Status* to make the DNS entry active or inactive.
9. Click *OK* to save your new DNS entry. The new DNS entry is added to the table.
10. Click *OK* to save your changes to the DNS zone.

To edit a DNS entry:

1. Go to *Network > DNS Service* and, under *DNS Database*, select a DNS zone and then click *Edit*.
2. Select a DNS entry and then click *Edit*.
3. In the *Edit DNS Entry* page, make your changes.
4. Click *OK* to save your changes to the DNS entry.
5. Click *OK* to save your changes to the DNS zone.

Packet Capture

You can create a filter on an interface to capture a specified number of packets to examine. Go to *Network > Packet Capture* to see existing packet capture filters.

Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

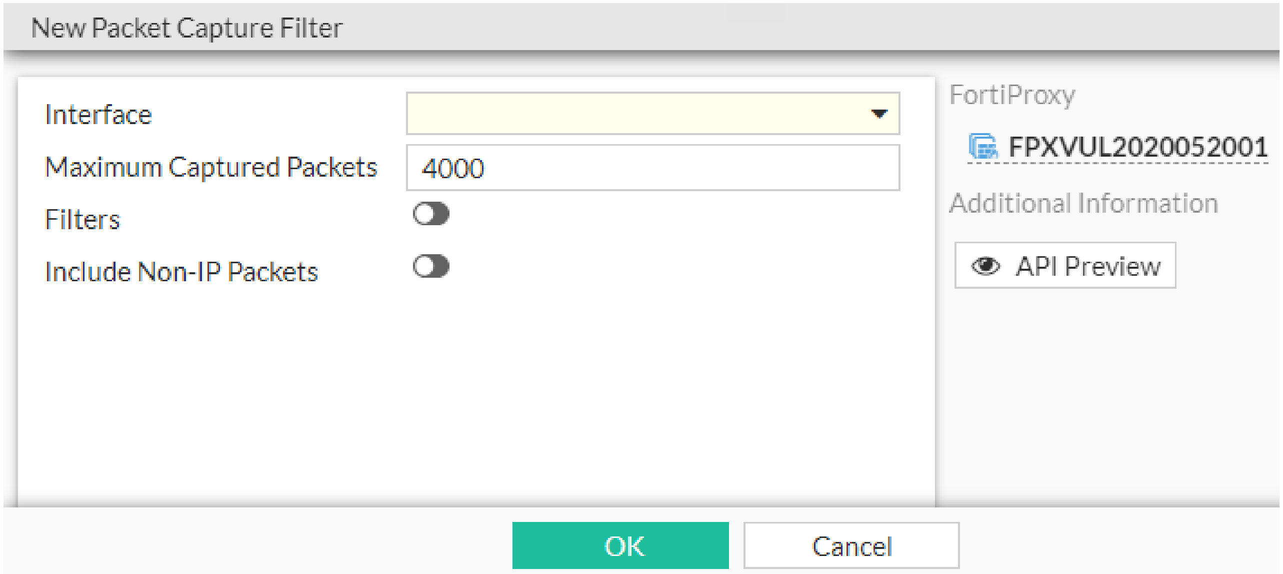
Create New	Creates a new packet capture filter. See Create or edit a packet capture filter on page 121.
Edit	Modifies settings within a packet capture filter.
Clone	Copies an existing packet capture filter.
Delete	Removes a packet capture filter from the list. To remove multiple filters, select multiple rows in the list by holding down the Ctrl or Shift keys and then select *Delete*.
Search	Enter a search term to search the filter list.
Interfaces	The interface or port number that the filter will examine.
Host Filter	The hosts being examined.
Port Filter	The ports being examined.
VLAN Filter	The VLANs being examined.
Protocol Filter	The protocols being examined.
Packets	The number of packets captured.
Max Packet Count	The maximum number of packets to collect.
Status	Whether the packet capture is running. To run the capture, select the play button in the progress column in the packet capture list. If the filter is not active, *Not Running* is displayed in the column cell. The progress bar indicates the status of the capture. You can stop and restart it at any time. When the capture is complete, select the *Download* icon to save the packet capture file to your hard disk for further analysis.
Capture IPv6	Whether the capture IPv6 packets has been enabled.
Capture Non-IP	Whether the capture of non-IP packets has been enabled.

Create or edit a packet capture filter

Go to *Network > Packet Capture* to create or edit a packet capture filter.

To create a packet capture filter:

1. Select *Create New*.



2. Configure the following settings and click *OK*:

Interface	Select an interface.
Maximum Captured Packets	Enter how many packets to collect.
Filters	Enable *Filters*, you can create filters for host names, ports, VLAN identifiers, and protocols. Use commas to separate items. Use a hyphen to specify a range.
Include Non-IP Packets	Select this option if you want to include packets from non-IP protocols.
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:

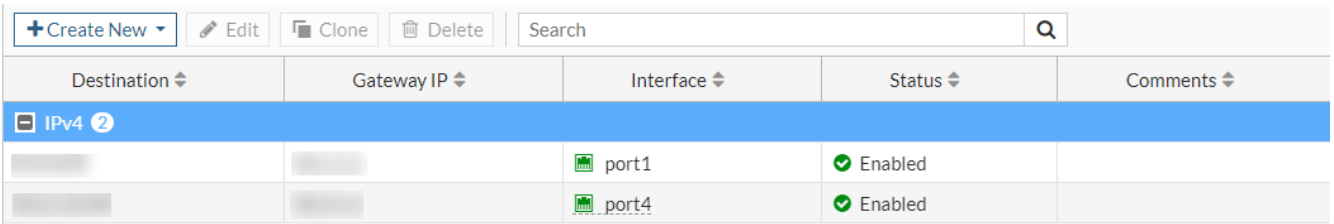
1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to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

To edit a packet capture filter:

1. Select a packet capture filter.
2. Select *Edit*.
3. Make your changes.
4. Click *OK* to save your changes.

Static routes

To see a list of static routes that control the flow of traffic through the unit, go to *Network > Static Routing*



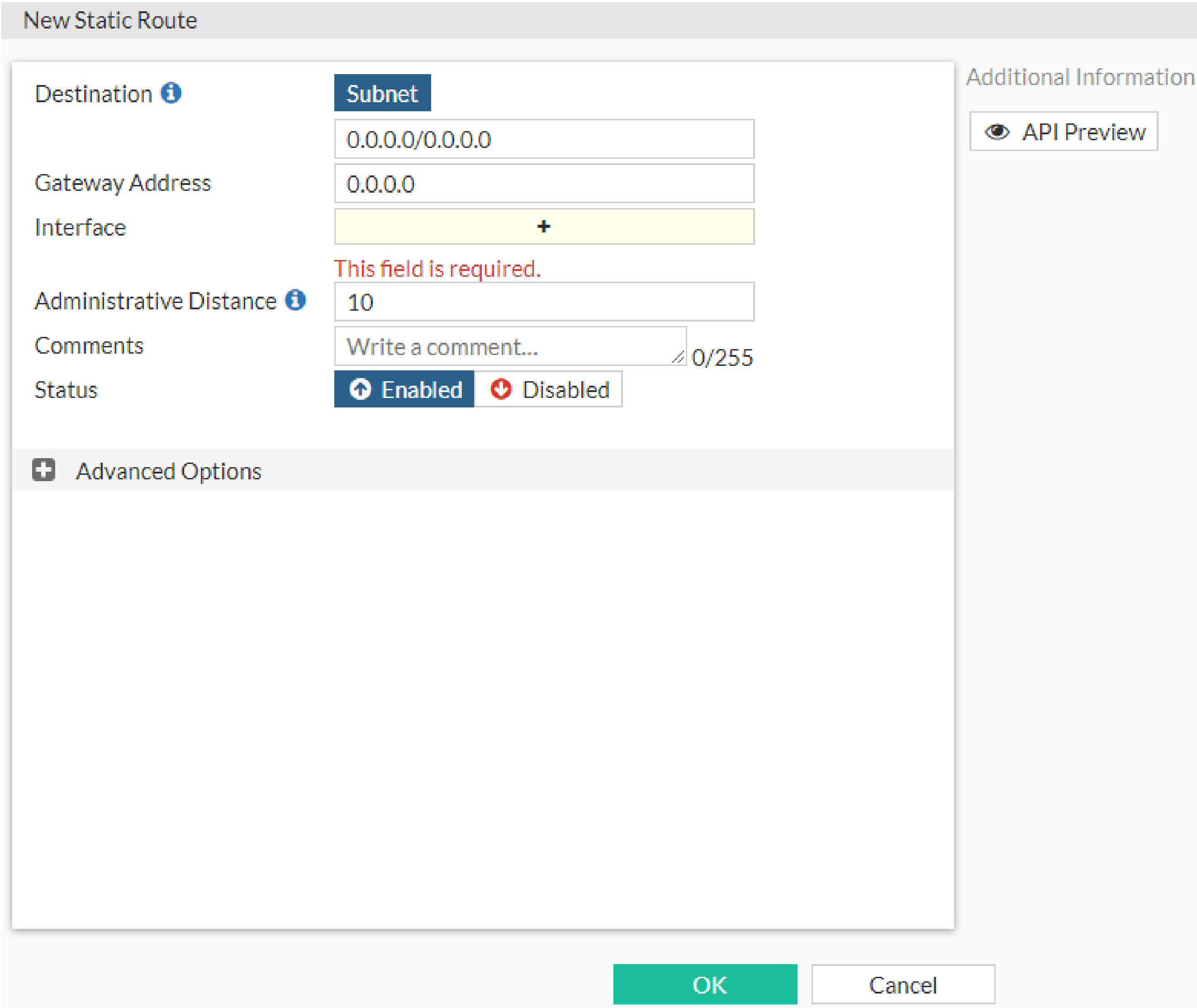
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

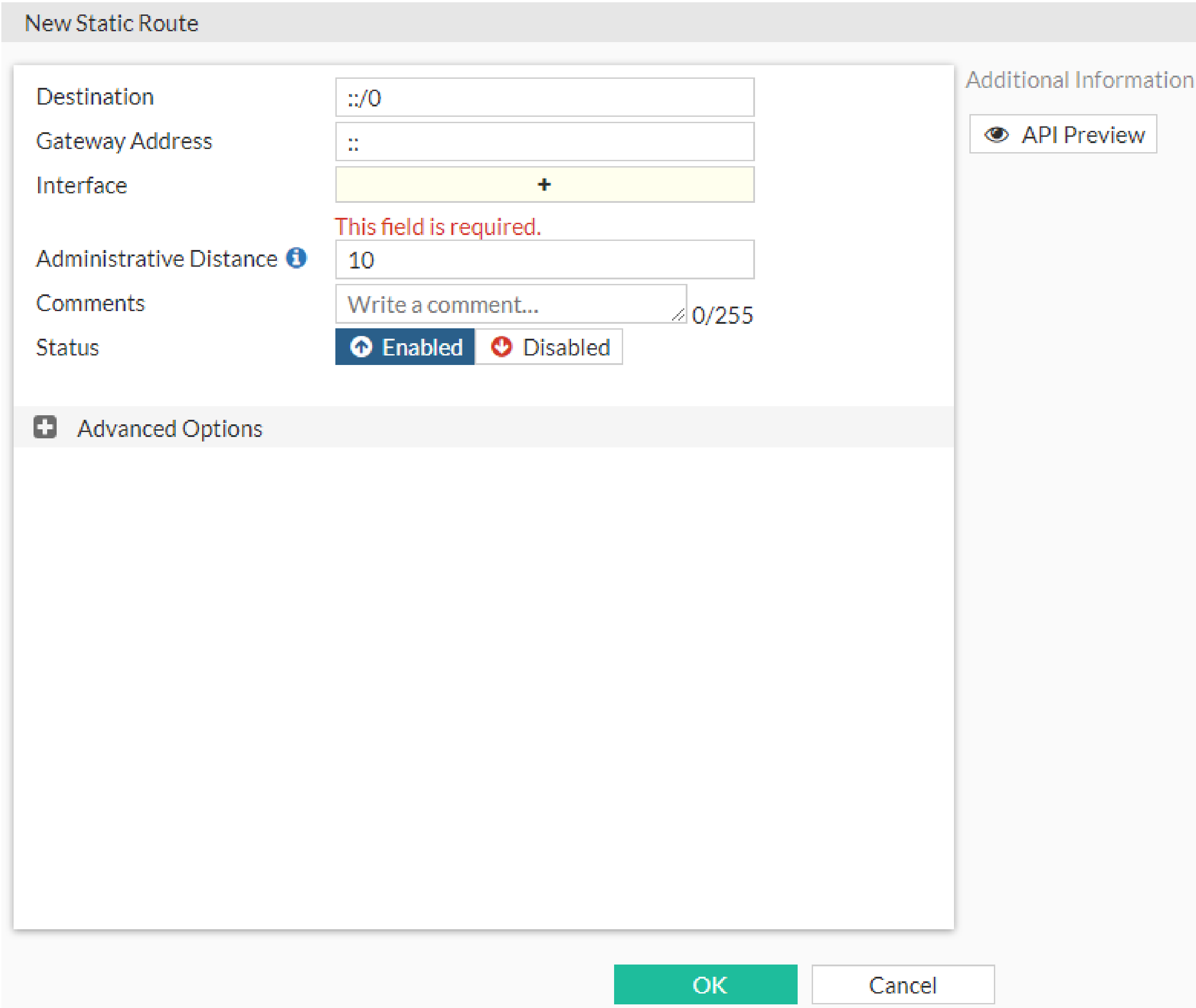
The following options are available:

Create New	Creates an IPv4 or IPv6 static route. See Create or edit a static route on page 123.
Edit	Modifies settings within the static route. See Create or edit a static route on page 123.
Clone	Copies an existing route.
Delete	Removes a static route from the list. To remove multiple static routes, select multiple rows in the list by holding down the Ctrl or Shift keys and then select *Delete*.
Search	Enter a search term to find in the list.
Destination	The destination IP addresses and network masks of packets that the FortiProxy unit intercepts.
Gateway IP	The IP addresses of the next-hop routers to which intercepted packets are forwarded.
Interface	The interface or port number the static route is configured to.
Status	The static route is either enabled or disabled.
Comments	A description of the route (optional).
Distance	The number of hops the static route has to the configured gateway. Routes with the same distance will be considered as equal-cost multi-path (ECMP)
Priority	A number for the priority of the static route. Routes with a larger number will have a lower priority. Routes with the same priority are considered as ECMP.

Create or edit a static route

Select *Create New > IPv4 Static Route* or *Create New > IPv6 Static Route* to open the New Static Route page and create a static route.


New Static Route
Destination
Subnet
0.0.0.0/0.0.0.0
Gateway Address
0.0.0.0
Interface
+
This field is required.
Administrative Distance
10
Comments
Write a comment...
0/255
Status
Enabled
Disabled
Advanced Options
Additional Information
API Preview
OK
Cancel



Select a static route and then click *Edit* to change a static route.

Configure the following settings in the *New Static Route* page or *Edit Static Route* page and click *OK*:

Destination	Enter the IPv4 or IPv6 address and netmask of the new static route.
Gateway Address	Enter the gateway IP address for those packets that you intend the unit to intercept.
Interface	Select the static route’s interface, port number, or *Blackhole.* A blackhole route is a route that drops all traffic sent to it. Blackhole routes are used to dispose of packets instead of responding to suspicious inquiries. This provides added security since the originator will not discover any information from the target network. Blackhole routes can also limit traffic on a subnet. If some subnet addresses are not in use, traffic to those addresses, which may be valid or malicious, can be directed to a blackhole for added security and to reduce traffic on the subnet.

Administrative Distance	The administrative distance is used to determine the cost of the route. Smaller distances are considered as a "better" route that should be used when multiple paths exist to the same destination. The routes with the same distance are considered as equal-cost multi-path routing (ECMP).
Comments	Enter a description up to 255 characters to describe the new static route.
Status	Select *Enabled* or *Disabled* to set the status of the new static route.
Advanced Options	Click + to show the *Priority* option.
Priority	Enter a number for the priority of the static route. Routes with a larger number have a lower priority. Routes with the same priority are considered as ECMP.
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.

Policy routes

Policy routing allows you to specify an interface to route traffic. This is useful when you need to route certain types of network traffic differently than you would if you were using the routing table. You can use the incoming traffic's protocol, source or destination address, source interface, or port number to determine where to send the traffic. Policy routes are sometimes referred to as Policy-based routes (PBR).

When a packet arrives, the FortiProxy starts at the top of the policy route list and attempts to match the packet with a policy. For a match to be found, the policy must contain enough information to route the packet. At a minimum, this requires the outgoing interface to forward the traffic, and the gateway to route the traffic to. If one or both of these are not specified in the policy route, then the FortiProxy searches the routing table to find the best active route that corresponds to the policy route. If no routes are found in the routing table, then the policy route does not match the packet. The FortiProxy continues down the policy route list until it reaches the end. If no matches are found, then the FortiProxy does a route lookup using the routing table.

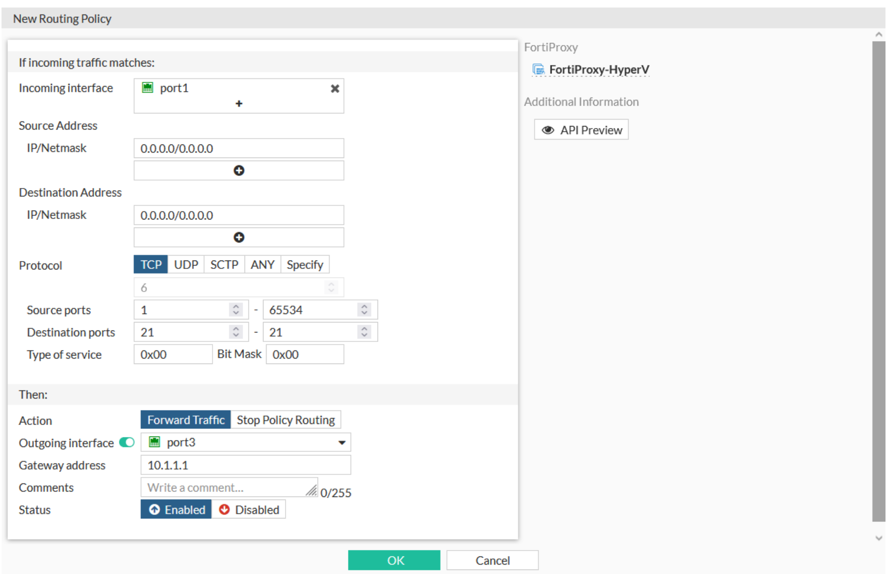
Configuring a policy route

In this example, a policy route is configured to send all FTP traffic received at port1 out through port3 and to a next hop router at 10.1.1.1. To route FTP traffic, the protocol is set to TCP (6) and the destination ports are set to 21 (the FTP port).

To configure a policy route in the GUI:

1. Go to *Network > Policy Routes* and click *Create New*.
2. Configure the following fields:

Incoming interface	port1
Source Address	0.0.0.0/0.0.0.0
Destination Address	0.0.0.0/0.0.0.0
Protocol	TCP
Destination ports	21 - 21
Type of service	0x00
Bit Mask	0x00
Outgoing interface	Enable and select port4
Gateway address	10.1.1.1



3. Click *OK*.

To configure a policy route in the CLI:

```
config router policy
    edit 1
        set input-device "port1"
        set src "0.0.0.0/0.0.0.0"
        set dst "0.0.0.0/0.0.0.0"
        set protocol 6
        set start-port 21
        set end-port 21
        set gateway 10.1.1.1
        set output-device "port3"
```

```
    next
end
```

VXLAN

Virtual Extensible LAN (VXLAN) is a network virtualization technology used in large cloud computing deployments. It encapsulates layer 2 Ethernet frames within layer 3 IP packets using the standard destination port 4789. VXLAN endpoints that terminate VXLAN tunnels can be virtual or physical switch ports, and are known as VXLAN tunnel endpoints (VTEPs). For more information about VXLAN, see RFC 7348.

To configure VXLAN:

```
config system vxlan
    edit <name>
        set interface <interface>
        set vni <vxlan_network_id>
        set ip-version {ipv4_unicast | ipv6_unicast}
        set remote-ip <ipv4_address>
        set remote-ip6 <ipv6_address>
        set dstport <port>
    next
end
```

`interface <interface>`	Outgoing interface for VXLAN encapsulated traffic.
`vni <vxlan_network_id>`	VXLAN network ID (default = 0).
`ip-version {ipv4_unicast | ipv6_unicast}`	The IP address version to use for the VXLAN interface, and for communication over the VXLAN (default = ipv4_unicast).
`remote-ip <ip_address>` `remote-ip6 <ipv6_address>`	The IPv4 or IPv6 address of the VXLAN interface on the device at the remote end of the VXLAN.
`dstport <port>`	The VXLAN destination port (1 - 65535, default = 4789).

To view the VXLAN forwarding database list for an interface:

```
diagnose sys vxlan fdb list <interface>
```

Policy & Objects

The *Policy & Objects* menu provides the following options:

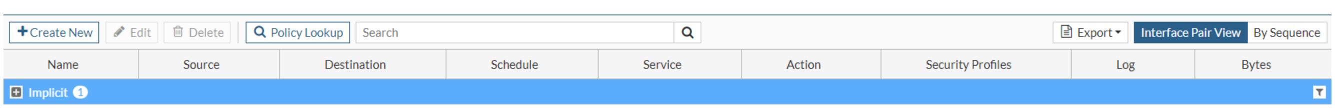
Policy

The policy list displays firewall policies in their order of matching precedence. Firewall policy order affects policy matching. For details about arranging policies in the policy list, see Change how the policy list is displayed.

You can add firewall policies that match HTTP traffic to be cached according to source and destination addresses and the destination port of the traffic.

Various right-click menus are available throughout the policy list. The columns displayed in the policy list can be customized, and filters can be added in a variety of ways to filter the information that is displayed. See Change how the policy list is displayed.

To view the policy list, go to *Policy & Objects > Policy*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Add a new policy. New policies are added to the bottom of the list. See Create or edit a policy on page 134.
Edit	Edit the selected policy. See Create or edit a policy on page 134.
Delete	Delete the selected policy.
Policy Lookup	Find a policy.
Search	Enter a search term to find in the policy list.
Export	Export the current view to CSV and JSON formats. Click *Export* and select *CSV* or *JSON* to download the file.
Interface Pair View/By Sequence	Select how to view the policy list: • *Interface Pair View*—Displays the policies in the order that they are checked for matching traffic, grouped by the pairs of Incoming and Outgoing interfaces. For instance, all of the policies referencing traffic from WAN1 to DMZ will be in one section. The policies referencing traffic from DMZ to WAN1 will be in another section. The sections are collapsible so that you only need to look at the sections with policies you are interested in. • *By Sequence*—Displays the policies in the order that they are checked for matching traffic without any grouping. The FortiProxy unit automatically changes the view on the policy list page to *By Sequence* whenever there is a policy containing the *any* interface. If the *Interface Pair View* is grayed out, one or more of the policies is using the *any* interface.
Type	The type of policy, such as Explicit Web, Transparent, or SSH Tunnel. See Policy types on page 135.
Name	The name of the policy.
Incoming Interface	The incoming interface or interfaces.
Outgoing Interface	The outgoing interface or interfaces.
Source	The source is the source address or source user of the initiating traffic.
Destination	The destination address or address range that the policy matches. For more information, see Web cache policy address formats on page 133.
Schedule	The time frame that is applied to the policy. See Schedules on page 225.
Service	The service or services chosen here represent the TCP/IP suite port numbers that will most commonly be used to transport the named protocols or group of protocols. See Services on page 216.
Action	The action to be taken by the policy, such as ACCEPT, DENY, REDIRECT, or ISOLATE.
Security Profiles	All the profiles used by the policy, such as AntiVirus, Web Filter, DLP Sensor, ICAP, SSL Inspection, and Content Analysis options. See Security Profiles on page 261.
Log	The logging level of the policy. Options vary depending on the policy type.

Bytes	The number of bytes.
Active Sessions	The number of active sessions.
Application Control	What action is taken when an application matches.
AV	The antivirus profile used by the policy. See AntiVirus on page 264.
Comments	Comments about the policy (up to 1023 characters).
Destination Address	The destination addresses that the policy matches. The destination address can be used as a traffic filter.
DNS Filter	The DNS filter profile used by the policy. See DNS Filter on page 292.
Email Filter	The email filter profile used by the policy. See .
Enforce ZTNA	Whether Zero Trust Network Access (ZTNA) is enabled or disabled. See ZTNA on page 237.
File Filter	The file filter profile used by the policy. See File Filter on page 306.
First Used	When the policy was first used.
Groups	Which groups the policy matches.
Hit Count	Number of results found.
ICAP	The ICAP profile used by the policy. See Create or edit an ICAP profile on page 346.
ID	The policy identifier. Policies are numbered in the order they are added to the configuration.
IPS	Which IPS signatures the policy uses.
Last Used	When the policy was last used.
Packets	The number of packets.
Protocol Options	The proxy options profile used by the policy. See Proxy Options on page 85.
Source Address	The addresses that a policy can receive traffic from. For more information, see Web cache policy address formats on page 133.
SSL Inspection	The SSL/SSH inspection options used by the policy. See SSL/SSH Inspection on page 308.
Status	Select to enable a policy or clear to disable a policy. A disabled policy is out of service.
Users	Which users the policy matches.
Video Filter	The video filter profile used by the policy. See Video Filter on page 289.
VPN Tunnel	The VPN tunnel used by the policy. See VPN on page 387.
Web Application Firewall	The web application firewall profile used by the policy. See .
Web Filter	The web filter profile used by the policy. See Web Filter on page 276.

ZTNA Tag	The ZTNA tags used in the ZTNA rule that is used by the policy. See ZTNA on page 237.

Change how the policy list is displayed

Policies can be added, edited, copied and pasted, moved, and deleted. To help organize your policies, you can also create sections to group policies together.

Policies can be inserted above or below existing policies and can also be disabled if needed.

The displayed policies can be filtered by either using the search field in the toolbar or by selecting the filter icon in a column heading. The available filter options vary depending on the type of data that the selected column contains.

How list order affects policy matching

The FortiProxy unit uses the first-matching technique to select which policy to apply to a communication session.

When policies have been added, each time the FortiProxy unit accepts a communication session, it then searches the policy list for a matching policy. Matching policies are determined by comparing the policy with the session source and destination addresses and the destination port. The search begins at the top of the policy list and progresses in order towards the bottom. Each policy in the policy list is compared with the communication session until a match is found. When the FortiProxy unit finds the first matching policy, it applies that policy and disregards subsequent policies.

If no policy matches, the session is accepted.

As a general rule, you should order the policy list from most specific to most general because of the order in which policies are evaluated for a match and because only the first matching policy is applied to a session. Subsequent possible matches are not considered or applied.

NOTE: Ordering policies from most specific to most general prevents policies that match a wide range of traffic from superseding and effectively masking policies that match exceptions.

Policy rules and authentication rules

Policy rules control what a user or user group can do. Authentication rules define how to authenticate a user. If a policy without a user group matches the type of traffic, authentication is not used because the user group was not specified in the policy.

For example, if a policy rule involving an explicit proxy has the Source field specifying an LDAP-based user group, any other policy rule referencing the explicit proxy is only matched if its Source field also specifies an LDAP-based group.

Move a policy

When more than one policy has been defined, the first matching policy is applied to the traffic session. You can arrange the policy list to influence the order in which policies are evaluated for matches with incoming traffic. See How list order affects policy matching on page 132 for more information.

NOTE: Moving a policy in the policy list does not change its ID, which only indicates the order in which the policies were created.

To move a policy, click and drag the name to a new location. You can also move a policy by cutting and pasting it into a new location.

Copy and paste a policy

Policies can be copied and pasted to create clones. Right-click on the policy name and then select *Copy* from the pop-up menu. Right-click in the policy name that the new clone policy will be placed next to and select *Paste Above* or *Paste Below* to insert the new policy before or after the selected policy.

Policy lookup

Firewall policy lookup is based on the `Source_interfaces/Protocol/Source_Address/Destination_Address` that matches the `source-port` and `dst-port` of the protocol. Use this tool to find out which policy matches specific traffic from a number of policies. After completing the lookup, the matching firewall policy is highlighted on the policy list page.

The Policy Lookup tool has the following requirements:

- Transparent mode does not support Policy lookup function.
- When executing the policy lookup, you need to confirm whether the relevant route required for the policy work already exists.

To use the policy lookup:

1. Go to *Policy & Objects* > *Policy*, click *Policy Lookup*.
2. Select the incoming interface.
3. Select *IPv4* or *IPv6* for the IP version.
4. Enter the protocol number.
5. Enter the source IP address.
6. Enter the destination IP address or fully qualified domain name.
7. Click *Search* to display the policy lookup results.

Web cache policy address formats

A source or destination address can contain one or more network addresses. Network addresses can be represented by an IP address with a netmask or an IP address range.

When representing hosts by an IP address with a netmask, the IP address can represent one or more hosts. For example, a source or destination address can be any of the following:

- a single computer, for example, `192.45.46.45`
- a subnetwork, for example, `192.168.1.*` for a class C subnet
- `0.0.0.0` matches any IP address

The netmask corresponds to the subnet class of the address being added and can be represented in either dotted decimal or CIDR format. The FortiProxy unit automatically converts CIDR-formatted netmasks to dotted decimal format. Example formats:

- netmask for a single computer: `255.255.255.255` or `/32`
- netmask for a class A subnet: `255.0.0.0` or `/8`
- netmask for a class B subnet: `255.255.0.0` or `/16`
- netmask for a class C subnet: `255.255.255.0` or `/24`
- netmask including all IP addresses: `0.0.0.0`

Valid IP address and netmask formats include:

- x.x.x.x/x.x.x.x, such as `192.168.1.0/255.255.255.0`
- x.x.x.x/x, such as `192.168.1.0/24`

An IP address `0.0.0.0` with the netmask `255.255.255.255` is not a valid source or destination address.

When representing hosts by an IP address range, the range indicates hosts with continuous IP addresses in a subnet, such as `192.168.1.[2-10]`, or `192.168.1.*`, to indicate the complete range of hosts on that subnet. You can also indicate the complete range of hosts on a subnet by entering `192.168.1.[0-255]` or `192.168.1.0-192.168.1.255`. Valid IP range formats include:

- x.x.x.x-x.x.x.x, for example, `192.168.110.100-192.168.110.120`
- x.x.x.[x-x], for example, `192.168.110.[100-120]`
- x.x.x.*, for a complete subnet, for example: `192.168.110.*`
- x.x.x.[0-255] for a complete subnet, such as `192.168.110.[0-255]`
- x.x.x.0 -x.x.x.255 for a complete subnet, such as `192.168.110.0 - 192.168.110.255`

You cannot use square brackets [ ] or asterisks * when adding addresses to the CLI. Instead you must enter the start and end addresses of the subnet range separated by a dash -. For example, `192.168.20.0-192.168.20.255` for a complete subnet and `192.168.10.10-192.168.10.100` for a range of addresses.

Create or edit a policy

New policies can be created by selecting *Create New* in the toolbar. By default, the new policy appears at the bottom of the policy list. New policies can also be created above or below an existing policy by right-clicking a policy name and selecting *Insert Empty Policy Above* or *Insert Empty Policy Below* or by copying or cutting an existing policy and then selecting *Paste Above* or *Paste Below* from the right-click menu.

Editing a policy

Policy information can be edited as required in four ways:

- By double-clicking on the sequence number of a policy or the policy name in the policy list
- By selecting a policy and then selecting *Edit* from the toolbar
- By hovering over the policy name and then selecting *Edit* (the pencil icon)
- By right-clicking on the sequence number of the policy or the policy name and selecting *Edit* from the right-click menu

The editing window for regular policies contains the same information as when creating new policies.

Policy types

There are six types of policies:

- *Explicit*—for an explicit web proxy policy.

  Use an explicit web proxy policy if you want to use the explicit web proxy.

  You can use the FortiProxy explicit web proxy to enable explicit proxying of IPv4 and IPv6 HTTP, and HTTPS traffic on one or more FortiProxy interfaces. The explicit web proxy also supports proxying FTP sessions from a web browser and proxy auto-config (PAC) to provide automatic proxy configurations for explicit web proxy users. From the CLI, you can also configure the explicit web proxy to support SOCKS sessions from a web browser.

  The explicit web and FTP proxies can be operating at the same time on the same or on different FortiProxy interfaces.

  The explicit web proxy receives web browser sessions to be proxied at FortiProxy interfaces with the explicit web proxy enabled. The explicit web proxy uses FortiProxy routing to route sessions through the FortiProxy unit to a destination interface. Before a session leaves the exiting interface, the explicit web proxy changes the source addresses of the session packets to the IP address of the exiting interface. You can configure the explicit web proxy to keep the original client IP address.
- *Transparent*—for a transparent firewall policy.

  Use a transparent firewall policy if you want to use the transparent web proxy.

  In addition to the explicit web proxy, the FortiProxy unit supports a transparent web proxy. While it does not have as many features as explicit web proxy, the transparent proxy has the advantage that nothing needs to be done on the user's system to forward supported web traffic over to the proxy. There is no need to reconfigure the browser or publish a PAC file. Everything is transparent to the end user, hence the name. This makes it easier to incorporate new users into a proxy deployment.

  You can use the transparent proxy to apply web authentication to HTTP traffic accepted by a firewall policy.

  On networks where authentication based on IP address will not work, you can use the transparent web proxy to apply web authentication that is based on the user's browser and not on their IP address. This authentication method allows you to identify individual users even if multiple users on your network are connecting to the FortiProxy unit from the same IP address.
- *FTP*—for an explicit FTP proxy policy.

  Use an explicit FTP proxy policy if you want to use the explicit FTP proxy.

  You can use the FortiProxy explicit FTP proxy to enable explicit FTP proxying on one or more FortiProxy interfaces. The explicit web and FTP proxies can be operating at the same time on the same or on different FortiProxy interfaces.

  The FTP proxy receives FTP sessions to be proxied at FortiProxy interfaces with the explicit FTP proxy enabled. The FTP proxy uses FortiProxy routing to route sessions through the FortiProxy unit to a destination interface. Before a session leaves the exiting interface, the explicit FTP proxy changes the source addresses of the session packets to the IP address of the exiting interface.
- *SSH Tunnel*—to perform access control for TCP/IP port forwarding traffic that is tunneled through the SSH proxy.
- *SSH Proxy*—to apply a proxy firewall policy with user authentication on SSH sessions.
- *Wanopt*—for a WAN optimization tunnel.

  All optimized traffic passes between the FortiProxy units or between a FortiClient peer and a FortiProxy unit over a WAN optimization tunnel. Traffic in the tunnel can be sent in plain text or encrypted using AES-128bit-CBC SSL.

  Both plain text and the encrypted tunnels use TCP destination port 7810.

  Before a tunnel can be started, the peers must be configured to authenticate with each other. Then, the clientside peer attempts to start a WAN optimization tunnel with the server-side peer. Once the peers authenticate with each other, they bring up the tunnel and WAN optimization communication over the tunnel starts. After a tunnel has been established, multiple WAN optimization sessions can start and stop between peers without restarting the tunnel.

Configuring a policy

To configure an explicit policy:

Type	Select *Explicit*. See Policy types.
Name	Enter a unique name for the new policy. Names can be changed later.
Explicit Web Proxy	If you selected *Explicit* for the policy type, select *web-proxy* or search for a policy. To create an explicit proxy policy, see Create or edit an explicit web proxy on page 55.
Outgoing Interface	Click +. A window slides out from the right where you can select from the available interfaces. You can select one or more specific interfaces, or you can select *any*. Selecting *any* removes the other interfaces.
Source	Click +. A window slides out from the right where you can select from the available sources. You can select source proxy addresses, source IPv4 addresses, source IPv6 addresses, source users, or source user groups. **NOTE:** You can mix IPv4 and IPv6 addresses. When the field is selected, a window slides out from the right. Address, IPv6 Address, and User tabs categorize the options. Click *Create* to create a source.
Destination	Click +. A window slides out from the right where you can select from the available destinations. You can select destination proxy addresses, destination IPv4 addresses, destination IPv6 addresses, and destination Internet services. **NOTE:** You can mix IPv4 and IPv6 addresses.
Negate Destination	Enable to use all destinations except the ones specified in the *Destination* field.
Schedule	Select a schedule from the drop-down list. Select *Create* to create a schedule. For more information, see Schedules on page 225.
Service	Select a service or service group that packets must match to trigger this policy. Select *Create* to create a service list. See Services on page 216. You can add multiple services or service groups.
Action	Select how you want the policy to respond when a packet matches the conditions of the policy. The options available will change depending on this selection. • *ACCEPT*—Accept traffic matched by the policy. • *DENY*—Reject traffic matched by the policy. • *REDIRECT*—Redirect traffic matched by the policy to the URL specified in the Redirect URL field. • *ISOLATE*—Isolate traffic matched by the policy to the isolator server selected in the Isolator Server drop-down list.

Web Cache	Enable or disable web caching.
Reverse Cache	Enable to use reverse proxy web caching. This option is available only if the *Action* is *Accept* and *Web Cache* is enabled.
Web Cache For HTTPS Traffic	Enable or disable web caching for HTTPS traffic.
Transparent	Enable or disable transparent proxy.
Poolname	If you configured an IP pool, enable this option and then select the IP pool from the drop-down list.
Webproxy Profile	If you configured a web proxy profile, enable this option and then select the web proxy profile from the drop-down list. See Web Proxy Profile on page 61.
Web Proxy Forwarding Server	If you configured a web proxy forwarding server, enable this option and then select a server from the drop-down list. See Create or edit a forwarding server on page 74.
Protocol Options	Select the proxy options profilefor the policy to use. See Proxy Options on page 85.
SSL/SSH Inspection	The SSL/SSH inspection options used by the policy. See SSL/SSH Inspection on page 308.
Display Disclaimer	If you want to display a disclaimer about Internet content that is not controlled by the network access provider, select *By Domain*, *By Policy*, or *By User*. This option is available only if *Action* is set to *ACCEPT*.
Customize Messages	Enable and then edit the existing message or create a message. This option is available only if *Display Disclaimer* is set to *By Domain*, *By Policy*, or *By User*.
Security Profiles	Select the security profiles to apply to the policy. These options are available only if *Action* is set to *ACCEPT*.
AntiVirus	Enable the antivirus profile and select or create a profile from the drop-down list. See AntiVirus on page 264.
Web Filter	Enable the web filter profile and select or create a profile from the drop-down list. See Web Filter on page 276.
Application Control	Enable the application sensor and select or create a sensor from the drop-down list. See Create or edit an application sensor on page 298.
IPS	Enable the IPS sensor and select or create a sensor from the drop-down list. See Create or edit an IPS sensor on page 303.
DLP Sensor	Enable DLP sensors and select or create a sensor from the drop-down list. See Data Leak Prevention on page 329.
Content Analysis	Enable the Content Analysis profile and select or create a profile from the drop-down list. See Create or edit an Image Analysis profile on page 343.
ICAP	Enable the ICAP profile and select or create a profile from the drop-down list. See Create or edit an ICAP profile on page 346.

Log Allowed Traffic	Enable and then select *Security Events* or *All Sessions*. This option is available only if *Action* is set to *ACCEPT*, *REDIRECT*, or *ISOLATE*.
Generate Logs when Session Starts	Enable or disable logging when the session starts.
Log HTTP Transaction	Configure the logging of HTTP transactions: • *All*—Log all HTTP transactions. • *Security Profiles* (default)—Log HTTP transaction on UTM event. • *Disable*—Disable HTTP transaction log. When *All* or *Security Profiles* is selected, you can find the HTTP transaction logs under *Log & Report* > *HTTP Transaction*. See Types of logs on page 590.
Comments	Enter a description up to 1,023 characters to describe the policy.
Enable this policy	Enable to use this policy.
Enable Policy Matching Pass Through	Enable to make the policy a pass-through policy. Disabled by default. 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.
Enable SSH policy check	Enable or disable whether to redirect SSH traffic to the matching proxy policy. See SSH policy matching on page 147.
Extended Log	Enable or disable the recording of extended log for implicit policies. The extended log includes the useragent, referralurl, httpmethod, and statuscode fields.

To configure a transparent policy:

Type	Select *Transparent*. See Policy types.
Name	Enter a unique name for the new policy. Names can be changed later.
ZTNA	Enable or disable Zero Trust Network Access (ZTNA). If you enable ZTNA, select whether to use *Full ZTNA* or *IP/MAC filtering*. • *Full ZTNA* allows users to securely access resources through a SSL encrypted access proxy. This simplifies remote access by eliminating the use of VPNs. • *IP/MAC filtering* uses ZTNA tags to provide an additional factor for identification and security posture check to implement role-based zero trust access.
ZTNA Server	Select one or more ZTNA servers to use.
ZTNA Tag	Select one or more ZTNA tags to use.
Incoming Interface	Click +. A window slides out from the right where you can select from the available interfaces. You can select one or more specific interfaces, or you can select *any*. Selecting *any* removes the other interfaces.
Outgoing Interface	Click +. A window slides out from the right where you can select from the available interfaces. You can select one or more specific interfaces, or you can select *any*. Selecting *any* removes the other interfaces.

Source	Click +. A window slides out from the right where you can select from the available sources. You can select source proxy addresses, source IPv4 addresses, source IPv6 addresses, source users, or source user groups. **NOTE:** You can mix IPv4 and IPv6 addresses. When the field is selected, a window slides out from the right. Address, IPv6 Address, and User tabs categorize the options. Click *Create* to create a source.
Destination	Click +. A window slides out from the right where you can select from the available destinations. You can select destination proxy addresses, destination IPv4 addresses, destination IPv6 addresses, and destination Internet services. **NOTE:** You can mix IPv4 and IPv6 addresses.
Negate Destination	Enable to use all destinations except the ones specified in the *Destination* field.
Schedule	Select a schedule from the drop-down list. Click *Create* to create a schedule. For more information, see Schedules on page 225.
Service	Select a service or service group that packets must match to trigger this policy. Click *Create* to create a service list. See Services on page 216. You can add multiple services or service groups.
Action	Select how you want the policy to respond when a packet matches the conditions of the policy. The options available will change depending on this selection. • *ACCEPT*—Accept traffic matched by the policy. • *DENY*—Reject traffic matched by the policy. • *REDIRECT*—Redirect traffic matched by the policy to the URL specified in the Redirect URL field. • *ISOLATE*—Isolate traffic matched by the policy to the isolator server selected in the Isolator Server drop-down list.
Web Cache	Enable or disable web caching.
Reverse Cache	Enable to use reverse proxy web caching. This option is available only if the *Action* is *Accept* and *Web Cache* is enabled.
Web Cache For HTTPS Traffic	Enable or disable web caching for HTTPS traffic.
Status	Enable or disable WAN optimization for traffic accepted by the policy. If *Status* is enabled, select *Active*, *Passive*, or *Manual*.
Profiles	If you enabled *Status* and selected *Active* or *Manual* WAN optimization, select a profile to use for WAN optimization. SeeCreate or edit a WAN optimization profile on page 360.
Passive Option	If you enabled *Status* and selected *Passive* WAN optimization, select *Default*, *Non-transparent*, or *Transparent*.
Peers	If you enabled *Status* and selected *Manual* WAN optimization, select a WAN peer. See Create or edit a WAN optimization peer on page 364.

Scan Outgoing Connections to Botnet Sites	Select *Disable* or *Block* to protect from botnet and command-and-control traffic.
Webproxy Profile	If you configured a web proxy profile, enable this option and then select the web proxy profile from the drop-down list. See Web Proxy Profile on page 61.
Web Proxy Forwarding Server	If you configured a web proxy forwarding server, enable this option and then select a server from the drop-down list. See Create or edit a forwarding server on page 74.
Force Proxy	Enable or disable whether proxying will be forced.
Protocol Options	Select the proxy options profilefor the policy to use. See Proxy Options on page 85.
SSL/SSH Inspection	The SSL/SSH inspection options used by the policy. See SSL/SSH Inspection on page 308.
Display Disclaimer	If you want to display a disclaimer about Internet content that is not controlled by the network access provider, select *By Domain*, *By Policy*, or *By User*. This option is available only if *Action* is set to *ACCEPT*.
Customize Messages	Enable and then edit the existing message or create a message. This option is available only if *Display Disclaimer* is set to *By Domain*, *By Policy*, or *By User*.
Security Profiles	Select the security profiles to apply to the policy. These options are available only if *Action* is set to *ACCEPT*.
AntiVirus	Enable the antivirus profile and select or create a profile from the drop-down list. See AntiVirus on page 264.
Web Filter	Enable the web filter profile and select or create a profile from the drop-down list. See Web Filter on page 276.
DNS Filter	Enable the DNS filter profile and select or create a profile from the drop-down list. See DNS Filter on page 292.
Application Control	Enable the application sensor and select or create a sensor from the drop-down list. See Create or edit an application sensor on page 298.
IPS	Enable the IPS sensor and select or create a sensor from the drop-down list. See Create or edit an IPS sensor on page 303.
DLP Sensor	Enable DLP sensors and select or create a sensor from the drop-down list. See Data Leak Prevention on page 329.
Content Analysis	Enable the Content Analysis profile and select or create a profile from the drop-down list. See Create or edit an Image Analysis profile on page 343.
ICAP	Enable the ICAP profile and select or create a profile from the drop-down list. See Create or edit an ICAP profile on page 346.
Log Allowed Traffic	Enable and then select *Security Events* or *All Sessions*. This option is available only if *Action* is set to *ACCEPT*, *REDIRECT*, or *ISOLATE*.

Generate Logs when Session Starts	Enable or disable logging when the session starts.
Log HTTP Transaction	Configure the logging of HTTP transactions: • *All*—Log all HTTP transactions. • *Security Profiles* (default)—Log HTTP transaction on UTM event. • *Disable*—Disable HTTP transaction log. When *All* or *Security Profiles* is selected, you can find the HTTP transaction logs under *Log & Report > HTTP Transaction*. See Types of logs on page 590.
Comments	Enter a description up to 1,023 characters to describe the policy.
Enable this policy	Enable to use this policy.
Enable Policy Matching Pass Through	Enable to make the policy a pass-through policy. Disabled by default. 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.
Enable SSH policy check	Enable or disable whether to redirect SSH traffic to the matching proxy policy. See SSH policy matching on page 147.
Extended Log	Enable or disable the recording of extended log for implicit policies. The extended log includes the useragent, referralurl, httpmethod, and statuscode fields.

To configure an FTP policy:

Type	Select *FTP*. See Policy types.
Name	Enter a unique name for the new policy. Names can be changed later.
Outgoing Interface	Click +. A window slides out from the right where you can select from the available interfaces. You can select one or more specific interfaces, or you can select *any*. Selecting *any* removes the other interfaces.
Source	Click +. A window slides out from the right where you can select from the available sources. You can select source proxy addresses, source IPv4 addresses, source IPv6 addresses, source users, or source user groups. **NOTE:** You can mix IPv4 and IPv6 addresses. When the field is selected, a window slides out from the right. Address, IPv6 Address, and User tabs categorize the options. Click *Create* to create a source.
Destination	Click +. A window slides out from the right where you can select from the available destinations. You can select destination proxy addresses, destination IPv4 addresses, destination IPv6 addresses, and destination Internet services. **NOTE:** You can mix IPv4 and IPv6 addresses.
Negate Destination	Enable to use all destinations except the ones specified in the *Destination* field.

Schedule	Select a schedule from the drop-down list. Select *Create* to create a schedule. For more information, see Schedules on page 225.
Action	Select how you want the policy to respond when a packet matches the conditions of the policy. The options available will change depending on this selection. • *ACCEPT*—Accept traffic matched by the policy. • *DENY*—Reject traffic matched by the policy.
Security Profiles	Select the security profiles to apply to the policy. These options are available only if *Action* is set to *ACCEPT*.
AntiVirus	Enable the antivirus profile and select or create a profile from the drop-down list. See AntiVirus on page 264.
IPS	Enable the IPS sensor and select or create a sensor from the drop-down list. See Create or edit an IPS sensor on page 303.
DLP Sensor	Enable DLP sensors and select or create a sensor from the drop-down list. See Data Leak Prevention on page 329.
Log Allowed Traffic	Enable and then select *Security Events* or *All Sessions*. This option is available only if *Action* is set to *ACCEPT*.
Generate Logs when Session Starts	Enable or disable logging when the session starts.
Comments	Enter a description up to 1,023 characters to describe the policy.
Enable this policy	Enable to use this policy.
Enable Policy Matching Pass Through	Enable to make the policy a pass-through policy. Disabled by default. 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.

To configure an SSH tunnel policy:

Type	Select *SSH Tunnel*. See Policy types.
Name	Enter a unique name for the new policy. Names can be changed later.
Incoming Interface	Click +. A window slides out from the right where you can select from the available interfaces. You can select one or more specific interfaces, or you can select *any*. Selecting *any* removes the other interfaces.
Outgoing Interface	Click +. A window slides out from the right where you can select from the available interfaces. You can select one or more specific interfaces, or you can select *any*. Selecting *any* removes the other interfaces.
Source	Click +. A window slides out from the right where you can select from the available sources. You can select source proxy addresses, source IPv4 addresses, source IPv6 addresses, source users, or source user groups. **NOTE:** You can mix IPv4 and IPv6 addresses.

	When the field is selected, a window slides out from the right. Address, IPv6 Address, and User tabs categorize the options. Click *Create* to create a source.
Destination	Click +. A window slides out from the right where you can select from the available destinations. You can select destination proxy addresses, destination IPv4 addresses, destination IPv6 addresses, and destination Internet services. **NOTE:** You can mix IPv4 and IPv6 addresses.
Negate Destination	Enable to use all destinations except the ones specified in the *Destination* field.
Schedule	Select a schedule from the drop-down list. Click *Create* to create a schedule. For more information, see Schedules on page 225.
Service	Select a service or service group that packets must match to trigger this policy. Click *Create* to create a service list. See Services on page 216. You can add multiple services or service groups.
Action	Select how you want the policy to respond when a packet matches the conditions of the policy. The options available will change depending on this selection. • *ACCEPT*—Accept traffic matched by the policy. • *DENY*—Reject traffic matched by the policy.
Security Profiles	Select the security profiles to apply to the policy. These options are available only if *Action* is set to *ACCEPT*.
Application Control	Enable the application sensor and select or create a sensor from the drop-down list. See Create or edit an application sensor on page 298.
IPS	Enable the IPS sensor and select or create a sensor from the drop-down list. See Create or edit an IPS sensor on page 303.
Logging Options	This section is available only if *Action* is set to *ACCEPT*.
Log Allowed Traffic	Enable and then select *Security Events* or *All Sessions*. This option is available only if *Action* is set to *ACCEPT*.
Generate Logs when Session Starts	Enable or disable logging when the session starts.
Comments	Enter a description up to 1,023 characters to describe the policy.
Enable this policy	Enable to use this policy.
Enable Policy Matching Pass Through	Enable to make the policy a pass-through policy. Disabled by default. 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.

To configure an SSH proxy policy:

Type	Select *SSH Proxy*. See Policy types.
Name	Enter a unique name for the new policy. Names can be changed later.

Outgoing Interface	Click +. A window slides out from the right where you can select from the available interfaces. You can select one or more specific interfaces, or you can select *any*. Selecting *any* removes the other interfaces.
Source	Click +. A window slides out from the right where you can select from the available sources. You can select source proxy addresses, source IPv4 addresses, source IPv6 addresses, source users, or source user groups. **NOTE:** You can mix IPv4 and IPv6 addresses. When the field is selected, a window slides out from the right. Address, IPv6 Address, and User tabs categorize the options. Click *Create* to create a source.
Destination	Click +. A window slides out from the right where you can select from the available destinations. You can select destination proxy addresses, destination IPv4 addresses, destination IPv6 addresses, and destination Internet services. **NOTE:** You can mix IPv4 and IPv6 addresses.
Negate Destination	Enable to use all destinations except the ones specified in the *Destination* field.
Schedule	Select a schedule from the drop-down list. Click *Create* to create a schedule. For more information, see Schedules on page 225.
Action	Select how you want the policy to respond when a packet matches the conditions of the policy. The options available will change depending on this selection. • *ACCEPT*—Accept traffic matched by the policy. • *DENY*—Reject traffic matched by the policy.
Security Profiles	Select the security profiles to apply to the policy. These options are available only if *Action* is set to *ACCEPT*.
Application Control	Enable the application sensor and select or create a sensor from the drop-down list. See Create or edit an application sensor on page 298.
IPS	Enable the IPS sensor and select or create a sensor from the drop-down list. See Create or edit an IPS sensor on page 303.
Logging Options	This section is available only if *Action* is set to *ACCEPT*.
Log Allowed Traffic	Enable and then select *Security Events* or *All Sessions*. This option is available only if *Action* is set to *ACCEPT*.
Generate Logs when Session Starts	Enable or disable logging when the session starts.
Comments	Enter a description up to 1,023 characters to describe the policy.
Enable this policy	Enable to use this policy.
Enable Policy Matching Pass Through	Enable to make the policy a pass-through policy. Disabled by default. 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.

To configure a WAN-optimization tunnel policy:

Type	Select *Wanopt*. See Policy types.
Name	Enter a unique name for the new policy. Names can be changed later.
Outgoing Interface	Click +. A window slides out from the right where you can select from the available interfaces. You can select one or more specific interfaces, or you can select *any*. Selecting *any* removes the other interfaces.
Source	Click +. A window slides out from the right where you can select from the available sources. You can select source proxy addresses, source IPv4 addresses, source IPv6 addresses, source users, or source user groups. **NOTE:** You can mix IPv4 and IPv6 addresses. When the field is selected, a window slides out from the right. Address, IPv6 Address, and User tabs categorize the options. Click *Create* to create a source.
Destination	Click +. A window slides out from the right where you can select from the available destinations. You can select destination proxy addresses, destination IPv4 addresses, destination IPv6 addresses, and destination Internet services. **NOTE:** You can mix IPv4 and IPv6 addresses.
Negate Destination	Enable to use all destinations except the ones specified in the *Destination* field.
Schedule	Select a schedule from the drop-down list. Click *Create* to create a schedule. For more information, see Schedules on page 225.
Service	Select a service or service group that packets must match to trigger this policy. Click *Create* to create a service list. See Services on page 216. You can add multiple services or service groups.
Action	Select how you want the policy to respond when a packet matches the conditions of the policy. The options available will change depending on this selection. • *ACCEPT*—Accept traffic matched by the policy. • *DENY*—Reject traffic matched by the policy.
Web Cache	Enable or disable web caching.
Reverse Cache	Enable to use reverse proxy web caching. This option is available only if the *Action* is *Accept* and *Web Cache* is enabled.
Web Cache For HTTPS Traffic	Enable or disable web caching for HTTPS traffic.
Security Profiles	Select the security profiles to apply to the policy. These options are available only if *Action* is set to *ACCEPT*.
AntiVirus	Enable the antivirus profile and select or create a profile from the drop-down list. See AntiVirus on page 264.
Web Filter	Enable the web filter profile and select or create a profile from the drop-down list. See Web Filter on page 276.

Application Control	Enable the application sensor and select or create a sensor from the drop-down list. See Create or edit an application sensor on page 298.
IPS	Enable the IPS sensor and select or create a sensor from the drop-down list. See Create or edit an IPS sensor on page 303.
DLP Sensor	Enable DLP sensors and select or create a sensor from the drop-down list. See Data Leak Prevention on page 329.
Content Analysis	Enable the Content Analysis profile and select or create a profile from the drop-down list. See Create or edit an Image Analysis profile on page 343.
Log Allowed Traffic	Enable and then select *Security Events* or *All Sessions*. This option is available only if *Action* is set to *ACCEPT.*
Generate Logs when Session Starts	Enable or disable logging when the session starts.
Comments	Enter a description up to 1,023 characters to describe the policy.
Enable this policy	Enable to use this policy.
Enable Policy Matching Pass Through	Enable to make the policy a pass-through policy. Disabled by default. 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.

Web cache policy address formats

A source or destination address can contain one or more network addresses. Network addresses can be represented by an IP address with a netmask or an IP address range.

When representing hosts by an IP address with a netmask, the IP address can represent one or more hosts. For example, a source or destination address can be any of the following:

- a single computer, for example, `192.45.46.45`
- a subnetwork, for example, `192.168.1.*` for a class C subnet
- `0.0.0.0` matches any IP address

The netmask corresponds to the subnet class of the address being added and can be represented in either dotted decimal or CIDR format. The FortiProxy unit automatically converts CIDR-formatted netmasks to dotted decimal format. Example formats:

- netmask for a single computer: `255.255.255.255` or `/32`
- netmask for a class A subnet: `255.0.0.0` or `/8`
- netmask for a class B subnet: `255.255.0.0` or `/16`
- netmask for a class C subnet: `255.255.255.0` or `/24`
- netmask including all IP addresses: `0.0.0.0`

Valid IP address and netmask formats include:

- x.x.x.x/x.x.x.x, such as `192.168.1.0/255.255.255.0`
- x.x.x.x/x, such as `192.168.1.0/24`

An IP address `0.0.0.0` with the netmask `255.255.255.255` is not a valid source or destination address.

When representing hosts by an IP address range, the range indicates hosts with continuous IP addresses in a subnet, such as `192.168.1.[2-10]`, or `192.168.1.*`, to indicate the complete range of hosts on that subnet. You can also indicate the complete range of hosts on a subnet by entering `192.168.1.[0-255]` or `192.168.1.0-192.168.1.255`. Valid IP range formats include:

- x.x.x.x-x.x.x.x, for example, `192.168.110.100-192.168.110.120`
- x.x.x.[x-x], for example, `192.168.110.[100-120]`
- x.x.x.*, for a complete subnet, for example: `192.168.110.*`
- x.x.x.[0-255] for a complete subnet, such as `192.168.110.[0-255]`
- x.x.x.0 -x.x.x.255 for a complete subnet, such as `192.168.110.0 - 192.168.110.255`

You cannot use square brackets [ ] or asterisks * when adding addresses to the CLI. Instead you must enter the start and end addresses of the subnet range separated by a dash -. For example, `192.168.20.0-192.168.20.255` for a complete subnet and `192.168.10.10-192.168.10.100` for a range of addresses.

Device ownership

When device ownership is enabled, ownership enforcement is done at policy level. It is disabled by default.

To enable device ownership:

```
config firewall policy
    edit 2
        set ztna-status enable
        set ztna-ems-tag "FCTEMS_ALL_FORTICLOUD_SERVERS"
        set device-ownership enable
        ...
    next
end
```

SSH policy matching

SSH policy check is disabled by default, and can be enabled in transparent and explicit-web policies. When it is enabled, SSH policy matching will only match the SSH policy.

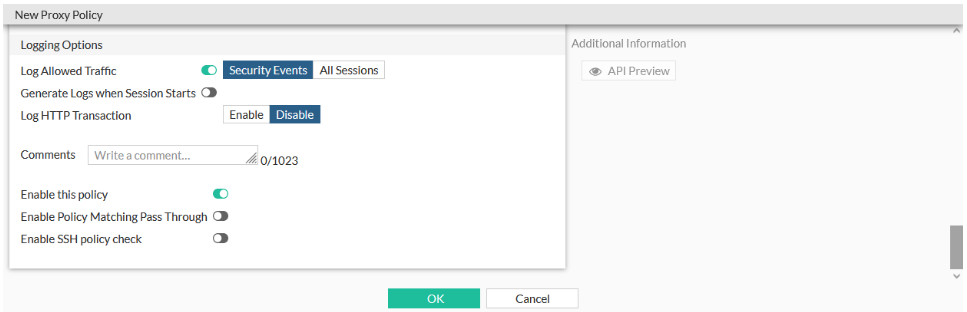
The *SSH Policy Redirect* (`ssh-policy-redirect`) command is no longer available.

To configure SSH policy check in the CLI:

```
config firewall policy
    edit <policy>
        set ssh-policy-check {disable | enable}
    next
end
```

To configure SSH policy check in the CLI:

1. Go to *Policy & Objects* > *Policy*.
2. Edit a transparent or explicit policy, or create a new policy and set *Type* to *Transparent* or *Explicit*.
3. Enable or disable *Enable SSH policy check*.



4. Click *OK*.

Authentication Rules

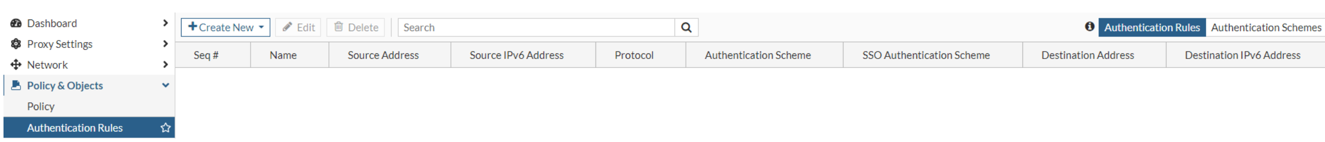
Authentication rules are used to receive user identity, based on the values set for the protocol and source address. If a rule fails to match based on the source address, there will be no other attempt to match the rule; however, the next policy will be attempted. This occurs only when:

- There is an authentication rule, but no authentication method has been set (under `config authentication scheme`), so the user identity cannot be found.
- The user is successfully matched in the rule but fails to match the current policy.

After a rule is positively matched through the protocol and/or source address, the authentication is checked (with `active-auth-method` and `sso-auth-method`). These methods point to schemes, as defined under `config authentication scheme`.

When you combine authentication rules and schemes, you have granular control over users and IP addresses, creating an efficient process for users to successfully match a criteria before matching the policy.

To manage authentication rules, go to *Policy & Objects* > *Authentication Rules*.



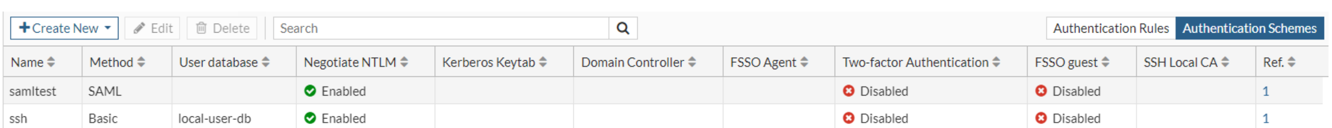
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create an authentication rule or authentication scheme. See Create or edit an authentication rule on page 151.
Edit	Modify an authentication rule or authentication scheme. See Create or edit an

	authentication rule on page 151.
Delete	Remove an authentication rule or rules.
Search	Enter a search term to find in the list.
Authentication Rules/Authentication Schemes	Select *Authentication Rules* to see a list of authentication rules. Select *Authentication Schemes* to see a list of authentication schemes.
Name	The name of the authentication rule.
Source Address	The source IPv4 addresses, address groups, *all*, or *none*.
Source IPv6 Address	The source IPv6 addresses, address groups, *all*, or *none*.
Protocol	The protocol that is matched for the rule.
Authentication Scheme	The authentication scheme that is being used. To create an authentication scheme, see Create or edit an authentication scheme on page 154.
SSO Authentication Scheme	The single sign-on authentication method.
Destination Address	The destination IPv4 addresses, address groups, *all*, or *none*.
Destination IPv6 Address	The destination IPv6 addresses, address groups, *all*, or *none*.
Comments	An optional description of the authentication rule.
IP-based Authentication	Whether IP-based authentication is enabled or disabled.
Status	Whether the rule is enabled or disabled.

To manage authentication schemes, go to *Policy & Objects > Authentication Rules* and then click *Authentication Schemes*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

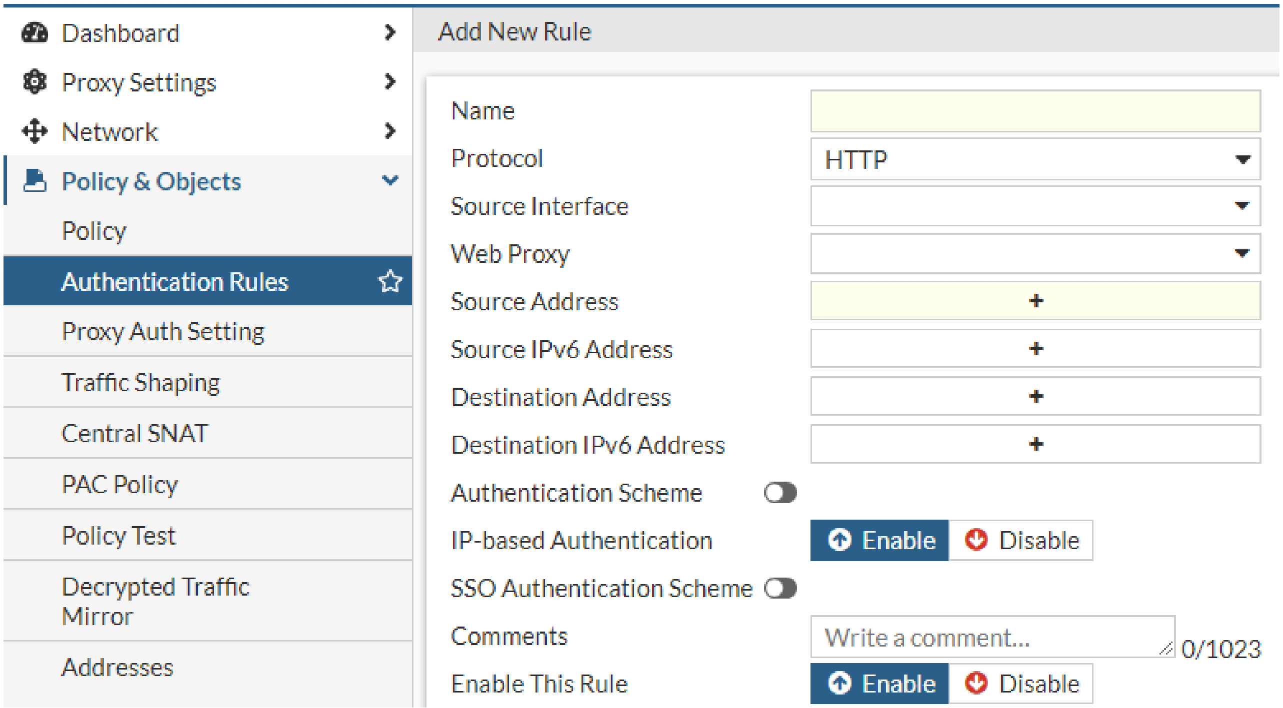
Create New	Create an authentication scheme. See Create or edit an authentication scheme on page 154.
Edit	Edit an authentication scheme. See Create or edit an authentication scheme on page 154
Delete	Delete an authentication scheme or schemes.
Search	Enter a search term to find in the list.
Authentication	Select *Authentication Rules* to see a list of authentication rules. Select

Rules/Authentication Schemes	*Authentication Schemes* to see a list of authentication schemes.
Name	The name of the authentication scheme.
Method	The authentication method: *NTLM*, *Basic*, *Digest*, *Form-based*, *Negotiate*, *SAML*, *SSH Public Key*, or *Fortinet Single Sign-On (FSSO)*.
User database	The name of the user database to use.
Negotiate NTLM	Whether NTLM negotiation is required.
Kerberos Keytab	The file containing the shared secret for Kerberos authentication.
Domain Controller	The domain controller.
FSSO Agent	The FSSO agent.
Two-factor Authentication	Whether two-factor authentication is required.
FSSO guest	Whether FSSO-guest authentication is required.
SSH Local CA	Which CA certificate is being used.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit an authentication rule

To create an authentication rule:

1. In the authentication rule list, select *Create New* > *Authentication Rules* from the toolbar.



2. Configure the following:

Name	The name of the authentication rule.
Protocol	Select which protocol is matched for the rule.
Source Interface	Select the source interface for the rule.
Web Proxy	Select the web proxy for the rule.
Source Address	Select the source IPv4 addresses, address groups, *all*, or *none*. Required for web-proxy authentication.
Source IPv6 Address	Select the source IPv6 address or address groups, *all*, or *none*. Required for web-proxy authentication.
Destination Address	The destination IPv4 addresses, address groups, *all*, or *none*.
Destination IPv6 Address	The destination IPv6 addresses, address groups, *all*, or *none*.
Authentication Scheme	Enable *Authentication Scheme* to use an authentication scheme and then select which authentication scheme to use. To create an authentication scheme, see Create or edit an authentication scheme on page 154.
IP-based Authentication	Select *Enable* if you want to use IP-based authentication.
SSO Authentication Scheme	If you selected *Enable* for IP-based authentication, enable *SSO Authentication Scheme* if you want to use single sign-on method and then select which single sign-on method to use.
Comments	Enter an optional description of the rule.
Enable This Rule	Select *Enable* or *Disable* to control whether the authentication rule is used or ignored.
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.

3. Click *OK* to create the new authentication rule.

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.

To edit an authentication rule:

1. Select the authentication rule you want to edit and then click *Edit* from the toolbar or double-click on the rule in the rule table.
2. Edit the rule information as required and click *OK* to apply your changes.

To set the authentication rule in the CLI:

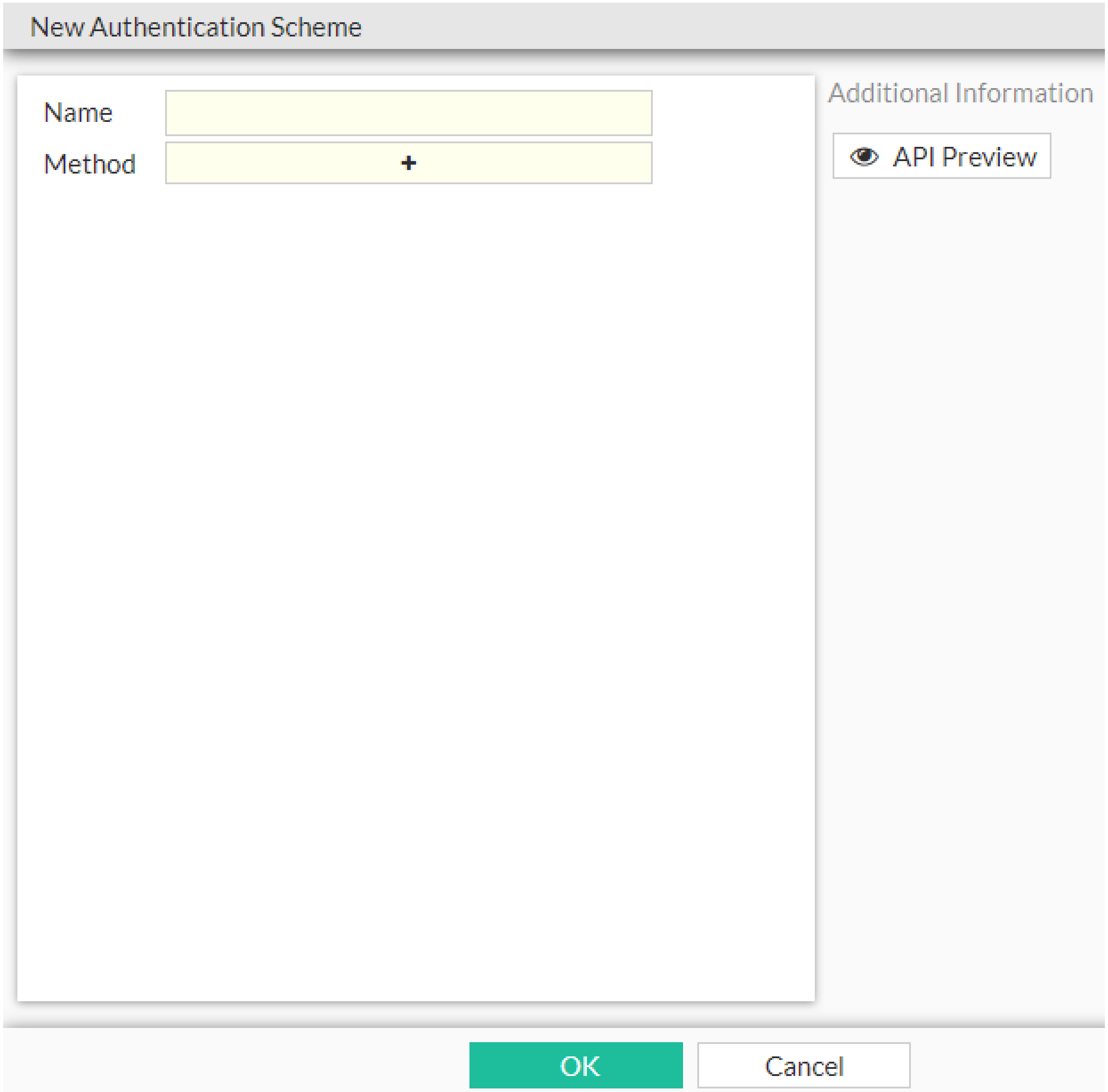
```
config authentication rule
   edit <name of rule>
      set status [enable|disable]
      set protocol [http|ftp|socks|ssh]
      set web-proxy <explicit_proxy_entity>
      set srcintf <name of incoming (ingress) interface>
      set srcaddr <name of IPv4 source address>
      set dstaddr <name of IPv4 destination address>
      set srcaddr6 <name of address object>
      set ip-based [enable|disable]
      set active-auth-method <string>
      set sso-auth-method <string>
      set web-auth-cookie [enable|disable]
      set transaction-based [enable|disable]
      set web-portal [enable|disable]
      set comments <string>
   next
end
```

Refer to config authentication rule in the CLI guide for more information.

Create or edit an authentication scheme

To create an authentication scheme:

1. In the authentication scheme list, select *Create New* > *Authentication Schemes* from the toolbar.



2. Configure the following:

Name	Enter the name of the authentication scheme.
Method	Select the authentication methods: • *Basic* • *Certificate* • *Digest* • *Form-based* • *Fortinet Single Sign-On (FSSO)* • *Negotiate* • *NTLM* • *RADIUS Single-Sign-On (RSSO)* • *SAML* • *SSH Public Key* Multi-methods supports *Basic*, *NTLM*, and *Negotiate*. For agentless NTML authentication, see Agentless NTLM support on page 156.
Negotiate NTLM	Enable/disable authentication negotiation for NTLM. When disabled, access is limited for non-domain users while using proxy authentication. This option is only available when the method includes *Negotiate*.
Kerberos keytab	Select the file containing the shared secret for Kerberos authentication.
Domain Controller	If you selected *NTLM*, select the domain controller.
User database	Select which user database to use.
Two-factor authentication	Move the slider to control whether two-factor authentication is required.
FSSO Agent	Move the slider to select the FSSO agent to use.
FSSO guest	Move the slider to control whether FSSO-guest authentication is required.
SSH local CA	Select which CA certificate to use.
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.

3. Click *OK* to create the new authentication scheme.

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.

To edit an authentication scheme:

1. Select the authentication scheme you want to edit and then click *Edit* from the toolbar or double-click on the scheme in the scheme table.
2. Edit the scheme information as required and click *OK* to apply your changes.

To create an authentication scheme in the CLI:

```
config authentication scheme
  edit <name>
    set method {ntlm | basic | digest | form | negotiate | fsso | rsso | ssh-publickey |
         cert | saml | saml-sp}
    set domain-controller <string>
    set fsso-agent-for-ntlm <string>
    set fsso-guest {enable | disable}
    set kerberos-keytab <string>
    set negotiate {enable | disable}
    set negotiate-ntlm {enable | disable}
    set require-tfa {enable | disable}
    set saml-ipd-portal <string>
    set ssh-ca <string>
    set user-database <auth_server>
  next
end
```

The following methods are available:

- `basic`—Basic HTTP authentication. This is the default method.
- `digest`—Digest HTTP authentication.
- `ntlm`—NTLM authentication. For agentless NTML authentication, see Agentless NTLM support on page 156. To configure the domain source when doing NTML authentication, see Domain name source when doing NTLM authentication on page 157.
- `form`—Form-based HTTP authentication.
- `negotiate`—Negotiate authentication.
- `fsso`—FSSO authentication.
- `rsso`—RADIUS Single Sign-On authentication.
- `saml`—SAML-IDP authentication (requires external FortiAuthenticator).
- `saml-sp`—SAML-IDP authentication with FortiProxy as the service provider.
- `publickey`—Public-key-based SSH authentication.
- `x-auth-user`—User from HTTP x-authenticated-user header.

Agentless NTLM support

Agentless NTLM authentication can be configured directly from the FortiProxy unit to the Domain Controller using the SMB protocol (no agent is required).

NOTE: This authentication method is only supported for proxy policies.

Syntax

NOTE: The `set domain-controller` command is only available when `method` is set to `ntlm` and/or `negotiate-ntlm` is set to `enable`.

```
config authentication scheme
   edit <name>
      set method ntlm
      set domain-controller <dc-setting>
   next
end

config user domain-controller
   edit <name>
      set ip-address <dc-ip>
      set port <port> // The default is 445.
      set domain-name <dns-name>
      set ldap-server <name>
   next
end
```

Domain name source when doing NTLM authentication

When doing NTLM authentication, the domain is extracted based on the following:

1. If the domain controller has a domain name configured, it is used.
2. Otherwise, if the NTLM type 3 message, from the user, is configured, it is used.
3. Otherwise, if the domain name from the NTLM type 2 message, from the DC, is configured, it is used.

To configure the domain name source, if it is not set:

```
config user domain-controller
    edit "adfs-dc"
        set ip-address 192.168.130.200
        unset domain-name
        set domain-name-src {server | client}
        set ldap-server "adfsldap"
    next
end
```

The domain name can be extracted from either the server's (DC) data, or from the client's data.

Proxy Auth Setting

This submenu provides settings for configuring authentication timeout, protocol support, authentication certificates, authentication schemes, and captive portals. When user authentication is enabled within a security policy, the authentication challenge is normally issued for any of the four protocols (depending on the connection protocol):

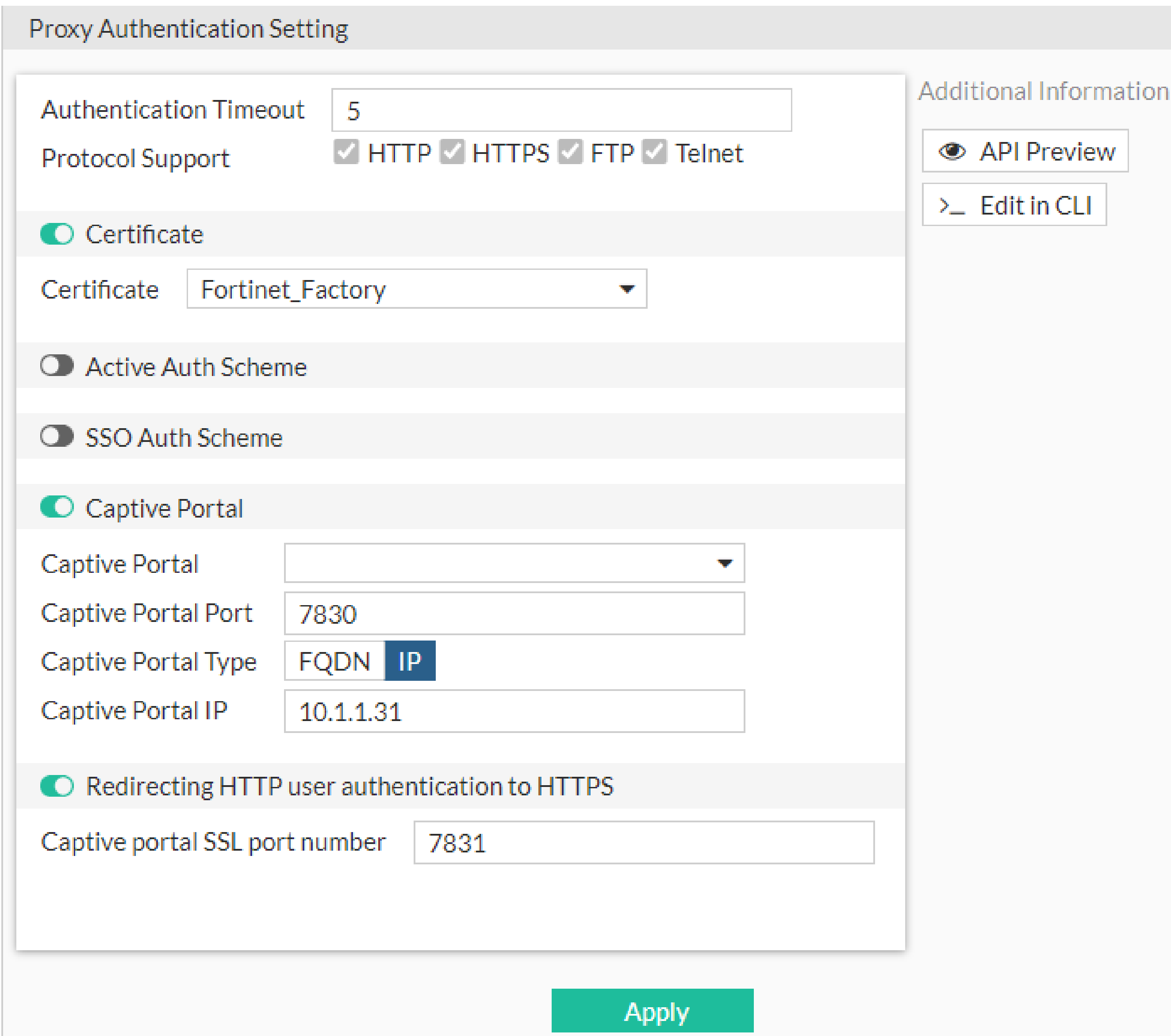
- HTTP (can also be set to redirect to HTTPS)
- HTTPS

- FTP
- Telnet

The selections control which protocols support the authentication challenge. Users must connect with a supported protocol first so that they can subsequently connect with other protocols. If HTTPS is selected as a method of protocol support, the user can authenticate with a customized local certificate.

When you enable user authentication within a security policy, the security policy user is challenged to authenticate. For user ID and password authentication, users must provide their user names and passwords. For certificate authentication (HTTPS or HTTP redirected to HTTPS only), you can install customized certificates on the unit, and the users can also have customized certificates installed on their browsers. Otherwise, users see a warning message and have to accept a default Fortinet certificate.

To configure proxy authentication settings, go to *Policy & Objects > Proxy Auth Settings*.



Configure the following settings and then select *Apply* to save your changes:

Authentication Timeout	Enter the amount of time, in minutes, that an authenticated firewall connection can be idle before the user must authenticate again. From 1 to 480 minutes. The default is 5.
Protocol Support	Select the protocols to challenge during firewall user authentication from the following: • *HTTP* • *HTTPS* • *FTP* • *Telnet*
Certificate	If you want to use a local certificate for authentication, enable *Certificate* and then select the certificate. The default is *Fortinet_Factory*.
Active Auth Scheme	If you want to use an active authentication scheme, enable *Active Auth Scheme* and then select which scheme to use. To create an authentication scheme, see Create or edit an authentication scheme on page 154.
SSO Auth Scheme	If you want to use a single-sign-on authentication scheme, enable *SSO Auth Scheme* and then select which scheme to use.
Captive Portal	If you want use a captive portal to authenticate web users, enable *Captive Portal* and then select a captive portal. Enter the captive port number and select the portal type. If you select *IP* as the captive portal type, enter the captive portal IP address.
Redirecting HTTP user authentication to HTTPS	Enable *Redirecting HTTP user authentication to HTTPS* if you want HTTPS user authentication used instead of HTTP user authentication and then enter the captive portal SSL port number.
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.
Edit in CLI	Click to open a CLI console window to view and edit the setting in the CLI. If there are multiple CLI settings on the page, the CLI console shows the first setting.

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.

To configure the authentication settings in the CLI:

```
config authentication setting
   set active-auth-scheme <string>
```

```
    set sso-auth-scheme <string>
    set captive-portal <string>
    set captive-portal-port <integer value from 1 to 65535; default is 0>
    set auth-https {enable | disable}
    set captive-portal-ssl-port <integer value from 1 to 65535; default is 7831>
end
```

- `active-auth-scheme`—Active authentication method.
- `sso-auth-scheme`—SSO authentication method.
- `captive-portal`—Captive portal host name.
- `captive-portal-port`—Captive portal port number.
- `auth-https`—Enable or disable redirecting HTTP user authentication to HTTPS.
- `captive-portal-ssl-port`—Captive portal SSL port number.

Traffic shaping

A FortiProxy provides quality of service (QoS) by applying bandwidth limits and prioritization to network traffic. Traffic shaping is one technique used by the FortiProxy to provide QoS. A basic approach to traffic shaping is to prioritize higher priority traffic over lower priority traffic during periods of traffic congestion. This provides a stabilizing effect for important traffic while throttling less important traffic.

The FortiProxy delivers traffic shaping with queuing. Before a packet egresses an interface, it is first enqueued to a queue using an algorithm such as RED or FIFO. The kernel dequeues the packet based on the HTB algorithm before sending it out. When traffic exceeds the configured bandwidth limits, traffic is delayed for transport until bandwidth frees up. Traffic may be dropped if the queues are full.

Configuration methods

The following table lists the methods to configure traffic shaping on the FortiProxy and their capabilities in order of preference. If both methods are configured, the first will be preferred over the second.

Method	Traffic queuing	Traffic prioritization	Guaranteed and maximum bandwidth limits
Traffic shaping profile on page 166	Yes	Traffic is placed into classes. A total of 30 classes are available. For each class, traffic can be configured into five priority levels.	When applying a traffic shaping profile to an interface's egress shaping profile, you can configure it to use up to 100% of the interface's configured bandwidth between all the classes, regardless of the configured priority in each class. The guaranteed bandwidth is always honored.

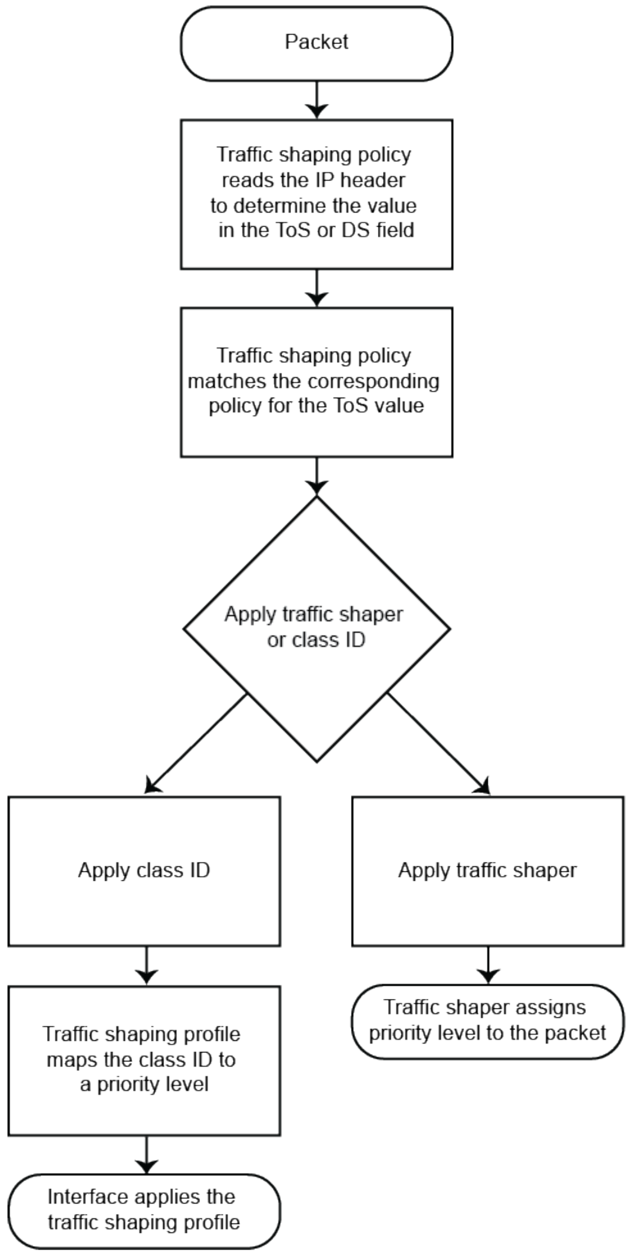
Method	Traffic queuing	Traffic prioritization	Guaranteed and maximum bandwidth limits
Traffic shaper	No	Traffic can be prioritized into the high (2), medium (3), or low (4) levels. When traffic is below the guaranteed bandwidth of the shaper, the traffic is automatically applied the critical level (1).	No hard limit on the guaranteed bandwidth. Administrators allocate guaranteed bandwidth to all the traffic shapers for an interface and ensure that the sum does not exceed the total outbandwidth of the interface. Traffic under the guaranteed bandwidth of a traffic shaper is given priority 1. If the total traffic with priority 1 exceeds the total outbandwidth, traffic can be dropped.

The following topics provide information about configuring traffic shaping:

- Traffic shaping policies on page 161
- Traffic shaping profile on page 166
- Traffic shapers on page 169
- DSCP marking in firewall shaping policies on page 178
- Examples on page 178

Traffic shaping policies

A traffic shaping policy is a rule that matches traffic to a traffic shaper or assign them to a class based on certain IP header fields and/or upper layer criteria. The matching traffic will apply a traffic shaper, class ID, or assign a DSCP DiffServ tag to the outgoing traffic. For example, it can match traffic based on source and destination IP, service, application, and URL category. One common use case is to match traffic based on the ToS or DS (differentiated services) field in the IP header. This allows Type of Service or Differentiated Services (DiffServ) tags to be read from traffic from a downstream device and prioritized accordingly on the FortiProxy based on the traffic shaper or the shaping profile applied on the interface.



The traffic shaping policies must be placed in the correct order in the traffic shaping policy list page to obtain the desired results. Policies are matched from top-down, so the traffic shaping policies should be arranged in a sequence that places the more granular policies above general policies.

The policy can be configured by going to *Policy & Objects* > *Traffic Shaping* and selecting the *Traffic Shaping Policies* tab. If the menu does not display the traffic shaping settings, go to *System* > *Feature Visibility* and enable *Traffic Shaping*.

Configuring traffic shaping policies

A traffic shaping policy can be split into two parts:

- Options used to match the traffic
- Options used to apply actions to the matched traffic

The following options can be configured for traffic matching criteria. Some options can only be configured from the CLI.

GUI option (under *Policy & Objects > Traffic Shaping > Traffic Shaping Policies*)	CLI option (under `config firewall shaping-policy`)	Description
Source		
Address	`set srcaddr <address_object>`	Select the address object to match the source IP.
Destination		
Address	`set dstaddr <address_object>`	Select the address object to match the destination IP.
Service Type	`set service-type [service|internet-service]`	Select the service type: firewall service or internet service.
Service	`set service <name1>, <name2>`	Select the firewall service or service group for the traffic.

Internet Service	`set internet-service-name <name>`
	`set internet-service-group <group>`
	`set internet-service-custom <custom>`
	`set internet-service-custom-group <custom_group>`
		Select the internet service to match the destination of the incoming traffic. Internet service currently cannot be used with destination address and service.

Schedule - NEW	`set schedule <schedule>`	Enable to select a schedule (one-time, recurring, or group).
Users	`set users <name1>, <name2>, ...`	Select the authenticated users to apply this traffic shaping policy to.
Groups	`set groups <name1>, <name2>, ...`	Select the authenticated user groups to apply this traffic shaping policy to.

The following options can be configured for actions to apply to the matched traffic:

GUI option	CLI option	Description
Outgoing interface	`set dstintf <interface>`	Select the destination interface that the traffic shaping applies to (required).
Apply shaper		

GUI option		CLI option	Description
	Shared shaper	`set traffic-shaper <shaper>`	Select the shared shaper to be applied to traffic in the ingress-to-egress direction. For example, on traffic that egresses on the wan interface, the shaper is applied to upload or outbound traffic.
	Reverse shaper	`set traffic-shaper-reverse <shaper>`	Select the reverse shaper to be applied to traffic in the egress-to-ingress direction. For example, on traffic that egresses on the wan interface, the shaper is applied to download or inbound traffic.
	Per-IP shaper	`set per-ip-shaper <shaper>`	Select the per-IP shaper. Per-IP shapers affect downloads and uploads. The allotted bandwidth applies to each individual IP. In a shared shaper, the allotted bandwidth applies to all IPs.
Assign shaping class ID			
	Traffic shaping class ID	`set class-id <class>`	Set the class ID to apply the matching traffic. Class IDs are further prioritized within a traffic shaping profile and applied to an interface.

n/a		`set diffserv-forward {enable | disable}`
		`set diffservcode-forward <code>`
		`set diffserv-reverse {enable | disable}`
		`set diffservcode-reverse <code>`
			Specify the settings to apply a DSCP tag to the forward or reverse traffic. The DiffServ code is in 6-bit binary format.
			These options can only be configured in the CLI.

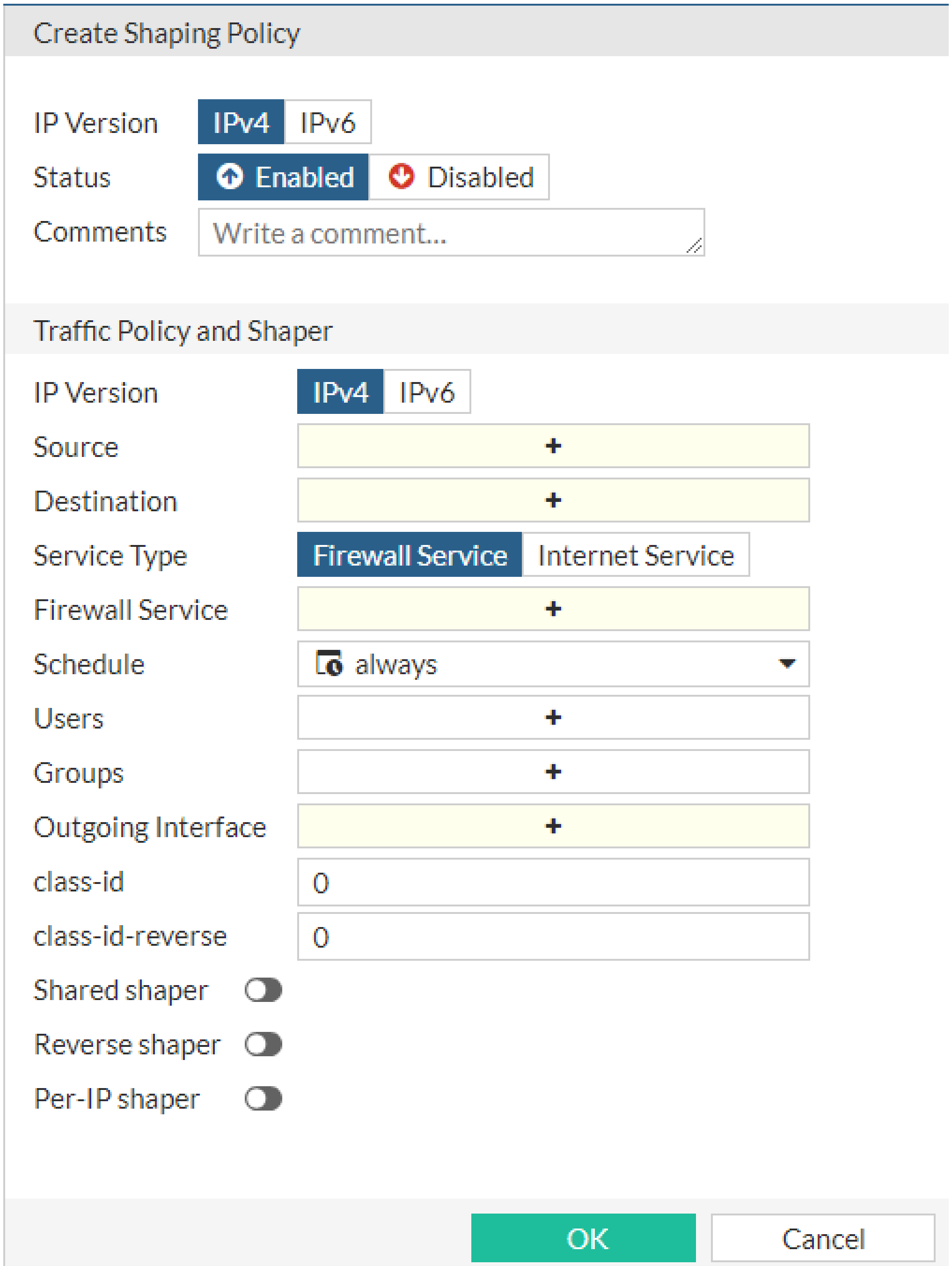
Traffic shapers and class IDs can be applied at the same time when configuring traffic shaping policies. However, to reduce the complexity, it is recommended to use one method over the other.

The following topics include examples with traffic shaping policies:

- Interface-based traffic shaping profile on page 179
- Shared traffic shaper on page 169
- Per-IP traffic shaper on page 173

Create or edit a traffic-shaping policy

Select *Create New* to open the *Create Shaping Policy* window. To change a traffic-shaping policy, select a policy and then click *Edit*.



Configure the following settings in the *New Shaping Policy* window or the *Edit Shaping Policy* window and then click *OK*:

IP Version	Select *IPv4* or *IPv6*.
Status	Policies are enabled by default. To disable to policy, click *Disabled*.
Comment	Enter any additional information that might be needed by administrators, as a reminder of the policy's purpose and scope. This setting is optional.

Source	Select or create the source address, address group, user, or user group that the traffic must match. You can select multiple sources in multiple categories.
Destination	Select or create the destination address or address group that the traffic must match. You can select multiple destinations in both categories.
Service Type	Select whether firewall services or Internet services are used for this policy.
Firewall Service	If you selected *Firewall Service* as the service type, select one or more firewall services that the traffic must match.
Internet Service	If you selected *Internet Service* as the service type, select one or more Internet services that the traffic must match.
Schedule - NEW	Select a schedule (one-time, recurring, or group) from the drop-down list for the shaping policy, which allows different traffic shaping for different days or different hours of the day without administrative intervention. Select *Create* to create a schedule. The default is *always,* which means the shaping policy is always applied. For more information, see Schedules on page 225
Users	Select one or more users that the traffic must match.
Groups	Select one or more user groups that traffic must match.
Outgoing Interface	Set this to the external interface that the traffic must match.
class-id	The class ID of a traffic shaper for outgoing packets.
class-id-reverse	The class ID of a traffic shaper for incoming packets.
Shared shaper	Enable or disable Shared traffic shaper on page 169.
Reverse shaper	Enable or disable reverse traffic shapers.
Per-IP shaper	Enable or disable Per-IP traffic shaper on page 173.
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.

Traffic shaping profile

A traffic shaping profile allows traffic shaping to be configured Up to 30 classes can be defined, with prioritization and bandwidth limits configured for each class.

Configuring traffic shaping profiles

The main steps to configure traffic shaping are:

1. Configure the traffic shaping policy, and assign matched traffic to a class (see Traffic shaping policies on page 161).
2. Create a traffic shaping profile and apply traffic bandwidth, prioritization and/or queuing per class.
3. Configure the interface outbandwidth/inbandwidth and apply a shaping profile to the interface.

Creating a traffic shaping profile

A traffic shaping profile consists of the class ID， settings per class ID, and the default class ID for traffic that does not match any traffic shaping policies. A class can be configured in the GUI as part of a traffic shaping profile or policy. In the CLI, a traffic class must be defined before it can be assigned within a traffic shaping profile. Class IDs range from 2 - 31, and they can be reused between different traffic shaping profiles.

When creating a traffic shaping profile, you can configure the following options per class.

GUI option	CLI option	Description
Default	`set default-class-id <class-id>`	Set the default class ID. Each profile must have one default class ID. The default class ID can be changed at any time.
Traffic shaping class ID	`set class-id <integer>`	Set the class ID (2 - 31).
Guaranteed bandwidth	`set guaranteed-bandwidth-percentage <integer>`	Set the percentage of the outbandwidth that will be guaranteed for the class ID.
Maximum bandwidth	`set maximum-bandwidth-percentage <integer>`	Set the percentage of the outbandwidth that will be the maximum bandwidth for the class ID.
Priority	`set priority {top | critical | high | medium | low}`	Select the priority level for the class ID.

To configure a traffic shaping profile in the GUI:

1. Go to *Policy & Objects > Traffic Shaping*, select the *Traffic Shaping Profiles* tab, and click *Create New*.
2. Enter the profile name, and optionally enter a comment.
3. In the *Traffic Shaping Classes* section, click *Create New*.
4. Configure the traffic shaping class ID settings (*Traffic shaping class ID*, *Guaranteed bandwidth*, *Maximum bandwidth*, and *Priority*).
5. Click *OK*.
6. Create more shaping classes as needed (the total guaranteed bandwidth of all classes cannot exceed 100%).
7. Click *OK*.

To configure a traffic shaping profile in the CLI:

1. Configure the shaping class:

```
config firewall traffic-class
    edit <integer>
        set class-name <string>
    next
end
```

2. Configure the shaping profile:

```
config firewall shaping-profile
    edit <name>
        set type {policing | queuing}
        set default-class-id <class-id>
        config shaping-entries
            edit <id>
                set class-id <integer>
                set priority {top | critical | high | medium | low}
                set guaranteed-bandwidth-percentage <integer>
                set maximum-bandwidth-percentage <integer>
            next
        end
    next
end
```

Configuring the interface outbandwidth and inbandwidth

You must configure the following settings on an interface that has traffic shaping applied to egressing/ingressing traffic: assign a traffic shaping profile and configure the outbound/inbound bandwidth.

Since traffic shaping is often configured on the WAN interface for egressing/ingressing traffic, the outbound/inbound bandwidth is effectively the upstream/downstream bandwidth allowed by your ISP.

To configure traffic shaping on an interface:

1. Go to *Network > Interfaces* and double-click an interface to edit it.
2. In the *Traffic Shaping* section, depending on your needs, enable *Outbound shaping profile* or *Inbound shaping profile* or both.
3. Select a profile for each enabled option.
4. Enable *Outbound bandwidth* or *Inbound shaping profile* or both, depending on your previous configuration.
5. Specify a value for each enabled option.
6. Click *OK*.

Verifying that the traffic is being shaped

In this example, three traffic classes are defined in the traffic shaping profile assigned to port1. The outbandwidth configured on port1 is 1000 Kbps. Each class has an `allocated-bandwidth`, `guaranteed-bandwidth`, `max-bandwidth`, and `current-bandwidth` value.

- The `guaranteed-bandwidth` and `max-bandwidth` are rates that are converted from the percentage of outbandwidth configured for each class. For example, `class-id` 2 has 10% `guaranteed-bandwidth`, equivalent to 100 Kbps, and 100% `max-bandwidth` equivalent to 1000 Kbps.

- The `allocated-bandwidth` displays the real-time bandwidth allocation for the traffic class based on all available factors. This value changes as traffic demand changes.
- The `current-bandwidth` displays the real-time bandwidth usage detected for the traffic class.

To verify that traffic is being shaped by the traffic shaping profile:

Enable debug flow to view the live traffic as it matches a traffic shaping policy:

```
# diagnose debug flow show function-name enable
# diagnose debug flow filter <filters>
# diagnose debug flow trace start <repeat_number>
# diagnose debug enable
```

Traffic shapers

The following topics provide more information about traffic shapers:

- Shared traffic shaper on page 169
- Per-IP traffic shaper on page 173
- Changing traffic shaper bandwidth unit of measurement on page 175
- Multi-stage DSCP marking and class ID in traffic shapers on page 176

Shared traffic shaper

Shared traffic shaper is used in a firewall shaping policy to indicate the priority and guaranteed and maximum bandwidth for a specified type of traffic use.

The maximum bandwidth indicates the largest amount of traffic allowed when using the policy. You can set the maximum bandwidth to a value between 1 and 16776000 Kbps. The GUI displays an error if any value outside this range is used. If you want to allow unlimited bandwidth, use the CLI to enter a value of 0.

The guaranteed bandwidth ensures that there is a consistent reserved bandwidth available. When setting the guaranteed bandwidth, ensure that the value is significantly less than the interface's bandwidth capacity. Otherwise, the interface will allow very little or no other traffic to pass through, potentially causing unwanted latency.

In a shared traffic shaper, the administrator can prioritize certain traffic as high, medium, or low. FortiProxy provides bandwidth to low priority connections only when high priority connections do not need the bandwidth. For example, you should assign a high traffic priority to a policy for connecting a secure web server that needs to support e-commerce traffic. You should assign less important services a low priority.

When you configure a shared traffic shaper, you can apply bandwidth shaping per policy or for all policies. By default, a shared traffic shaper applies traffic shaping evenly to all policies that use the shared traffic shaper.

When configuring a per-policy traffic shaper, FortiProxy applies the traffic shaping rules defined for each security policy individually. For example, if a per-policy traffic shaper is configured with a maximum bandwidth of 1000 Kbps, any security policies that have that traffic shaper enabled get 1000 Kbps of bandwidth each.

If a traffic shaper for all policies is configured with a maximum bandwidth of 1000 Kbps, all policies share the 1000 Kbps on a first-come, first-served basis.

The configuration is as follows:

```
config firewall shaper traffic-shaper
   edit "share1"
```

```
      set guaranteed-bandwidth 15
      set maximum-bandwidth 80000000
      set bandwidth-unit gbps
      set per-policy enable
      set diffserv enable
      set dscp-marking-method multi-stage
      set exceed-bandwidth 16
      set exceed-dscp 011111
      set maximum-dscp 111111
      set overhead 3
      set diffservcode 000110
   next
end
```

The shared traffic shaper selected in the traffic shaping policy affects traffic in the direction defined in the policy. For example, if the source port is LAN and the destination is WAN1, the traffic shaping affects the flow in this direction only, affecting the outbound traffic's upload speed. You can define the traffic shaper for the policy in the opposite direction (reverse shaper) to affect the inbound traffic's download speed. In this example, that would be from WAN1 to LAN.

Only traffic through forward traffic shapers will be included in FortiView; reverse and per-IP shapers are not included.

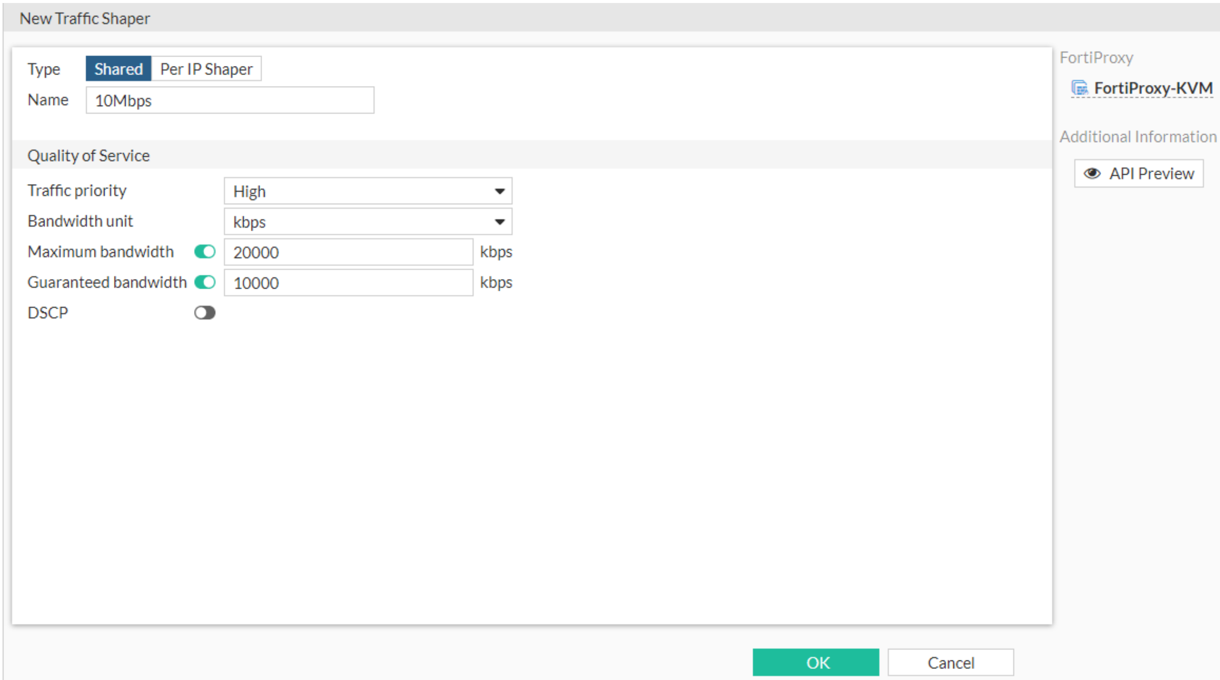
Traffic shapers can be added to a multicast policy when multicast routing is enabled.

The following example shows how to apply different speeds to different types of service. The example configures two shared traffic shapers to use in two firewall shaping policies. One policy guarantees a speed of 10 Mbps for VoIP traffic. The other policy guarantees a speed of 1 Mbps for other traffic. In the example, FortiProxy communicates with a PC using port10 and the Internet using port9.

To configure shared traffic shapers in the GUI:

1. Create a firewall policy:
   a. Go to *Policy & Objects > Policy* and click *Create New*.
   b. Set the *Name* to *Internet Access*.
   c. Set the *Incoming Interface* to *port10*.
   d. Set the *Outgoing Interface* to *port9*.
   e. Set the *Source* and *Destination* to *all*.
   f. Set the *Schedule* to *always*.
   g. Set the *Service* to *ALL*.
   h. Click *OK*.
2. Create the shared traffic shapers:
   a. Go to *Policy & Objects > Traffic Shaping*, select the *Traffic Shapers* tab, and click *Create New*.
   b. Set the *Name* to *10Mbps*. This shaper is for VoIP traffic.
   c. Set the *Traffic Priority* to *High*.
   d. Enable *Max Bandwidth* and enter *20000*.

e. Enable *Guaranteed Bandwidth* and enter *10000*.



f. Click *OK*.

g. Repeat the above steps to create another traffic shaper named *1Mbps* with the *Traffic Priority* set to *Low*, the *Max Bandwidth* set to *10000*, and the *Guaranteed Bandwidth* set to *1000*.

3. Create a firewall shaping policy for VoIP traffic:

   a. Go to *Policy & Objects > Traffic Shaping*, select the *Traffic Shaping Policies* tab, and click *Create New*.

   b. Set the *Name* to *VoIP_10Mbps_High*.

   c. Set the *Source* and *Destination* to *all*.

   d. Set the *Service* to all VoIP services.

   e. Set the *Outgoing Interface* to *port9*.

   f. Enable *Shared shaper* and select *10Mbps*.

   g. Enable *Reverse shaper* and select *10Mbps*.

   h. Click *OK*.

4. Repeat the sub-steps in step 3 to create another firewall shaping policy named *Other_1Mbps_Low* for other traffic, with the *Source* and *Destination* set to *all*, *Service* set to *ALL*, *Outgoing Interface* set to *port9*, and *Shared shaper* and *Reverse shaper* set to *1Mbps*.

To configure shared traffic shapers in the CLI:

1. Create a firewall policy:

```
config firewall policy
   edit 1
      set name "Internet Access"
      set srcintf "port10"
      set dstintf "port9"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ALL"
```

```
        set fsso disable
        set nat enable
    next
end
```

2. Create the shared traffic shapers:

```
config firewall shaper traffic-shaper
    edit "10Mbps"
        set guaranteed-bandwidth 10000
        set maximum-bandwidth 20000
    next
    edit "1Mbps"
        set guaranteed-bandwidth 1000
        set maximum-bandwidth 10000
        set priority low
    next
end
```

3. Create a firewall shaping policy:

```
config firewall shaping-policy
    edit 1
        set name "VOIP_10Mbps_High"
        set service "H323" "IRC" "MS-SQL" "MYSQL" "RTSP" "SCCP" "SIP" "SIP-MSNmessenger"
        set dstintf "port9"
        set traffic-shaper "10Mbps"
        set traffic-shaper-reverse "10Mbps"
        set srcaddr "all"
        set dstaddr "all"
    next
    edit 2
        set name "Other_1Mbps_Low"
        set service "ALL"
        set dstintf "port9"
        set traffic-shaper "1Mbps"
        set traffic-shaper-reverse "1Mbps"
        set srcaddr "all"
        set dstaddr "all"
    next
end
```

To check the statuses of shared traffic shapers:

```
# diagnose firewall shaper traffic-shaper list
name 10Mbps
maximum-bandwidth 2500 KB/sec
guaranteed-bandwidth 1250 KB/sec
current-bandwidth 0 B/sec
priority 2
tos ff
packets dropped 0
bytes dropped 0

name 1Mbps
maximum-bandwidth 1250 KB/sec
guaranteed-bandwidth 125 KB/sec
current-bandwidth 0 B/sec
priority 4
tos ff
```

```
packets dropped 0
bytes dropped 0
```

Per-IP traffic shaper

With per-IP traffic shaping, you can limit each IP address's behavior to avoid a situation where one user uses all of the available bandwidth. In addition to controlling the maximum bandwidth used per IP address, you can also define the maximum number of concurrent sessions for an IP address. For example, if you apply a per-IP shaper of 1 Mbps to your entire network, FortiProxy allocates each user/IP address 1 Mbps of bandwidth. Even if the network consists of a single user, FortiProxy allocates them 1 Mbps. If there are ten users, each user gets 1 Mbps of bandwidth, totaling 10 Mbps of outgoing traffic.

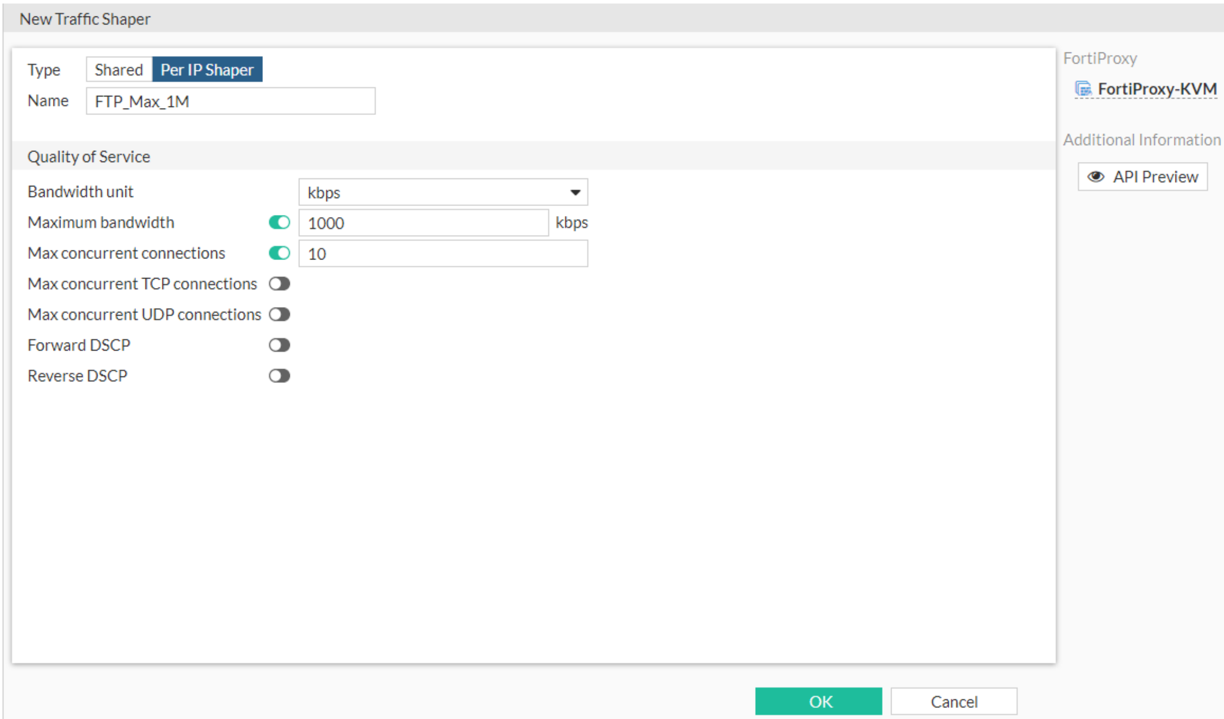
For shared shapers, all users share the set guaranteed and maximum bandwidths. For example, if you set a shared shaper for all PCs using an FTP service to 10 Mbps, all users uploading to the FTP server share the 10 Mbps.

Shared shapers affect upload speed. If you want to limit the download speed from the FTP server in the example, you must configure the shared shaper as a reverse shaper. Per-IP shapers apply the speed limit on both upload and download operations. Only traffic through forward traffic shapers will be included in FortiView; reverse and per-IP shapers are not included.

The following example shows how to apply a per-IP shaper to a traffic shaping policy. This shaper assigns each user a maximum bandwidth of 1 Mbps and allows each user to have a maximum of ten concurrent connections to the FTP server. In the example, FortiProxy communicates with users using port10 and the FTP server using port9.

To configure a per-IP traffic shaper in the GUI:

1. Create a firewall policy:
   a. Go to *Policy & Objects > IPv4 Policy* and click *Create New*.
   b. Set the *Name* to *FTP Access*.
   c. Set the *Incoming Interface* to *port10*.
   d. Set the *Outgoing Interface* to *port9*.
   e. Set the *Source* to *all*.
   f. Set the *Destination* to *FTP_Server*.
   g. Set the *Schedule* to *always*.
   h. Set the *Service* to *ALL*.
   i. Click *OK*.
2. Create the per-IP traffic shaper:
   a. Go to *Policy & Objects > Traffic Shaping*, select the *Traffic Shapers* tab, and click *Create New*.
   b. Set *Type* to *Per IP Shaper*.
   c. Enter the *Name* (*FTP_Max_1M*). This shaper is for VoIP traffic.
   d. Enable *Max Bandwidth* and enter *1000*.
   e. Enable *Max Concurrent Connections* and enter *10*. This means that each user can have up to ten concurrent connections to the FTP server.



   f. Click *OK*.
3. Create a firewall shaping policy:
   a. Go to *Policy & Objects* > *Traffic Shaping*, select the *Traffic Shaping Policies* tab, and click *Create New*.
   b. Enter the *Name* (*FTP speed 1M*).
   c. Set the *Source* to the addresses and users that require access to the FTP server.
   d. Set the *Destination* to *FTP_Server*.
   e. Set the *Service* to *ALL*.
   f. Set the *Outgoing Interface* to *port9*.
   g. Enable *Per-IP shaper* and select *FTP_Max_1M*.
   h. Click *OK*.

To configure a per-IP traffic shaper in the CLI:

1. Create a firewall policy:

```
config firewall policy
   edit 1
      set name "FTP Access"
      set srcintf "port10"
      set dstintf "port9"
      set srcaddr "all"
      set dstaddr "FTP_Server"
      set action accept
      set schedule "always"
      set service "ALL"
      set fsso disable
      set nat enable
   next
end
```

2. Create the per-IP traffic shaper:
```
config firewall shaper per-ip-shaper
  edit "FTP_Max_1M"
    set max-bandwidth 1000
    set max-concurrent-session 10
  next
end
```
3. Create a firewall shaping policy:
```
config firewall shaping-policy
  edit 1
    set name "FTP speed 1M"
    set service "ALL"
    set dstintf "port9"
    set per-ip-shaper "FTP_Max_1M"
    set srcaddr "PC1" "WinPC" "PC2"
    set dstaddr "FTP_Server"
  next
end
```

To check the status of a per-IP traffic shaper:

```
# diagnose firewall shaper per-ip-shaper list
```

The output should resemble the following:

```
name FTP_Max_1M
maximum-bandwidth 125 KB/sec
maximum-concurrent-session 10
tos ff/ff
packets dropped 0
bytes dropped 0
addr=10.1.100.11 status: bps=0 ses=3
```

Changing traffic shaper bandwidth unit of measurement

Bandwidth speeds are measured in kilobits per second (Kbps), and bytes that are sent and received are measured in megabytes (MB). In some cases, this can cause confusion depending on whether your ISP uses kilobits per second (Kbps), kilobytes per second (KBps), megabits per second (Mbps), or gigabits per second (Gbps).

You can change the unit of measurement for traffic shapers in the CLI.

To change the bandwidth unit of measurement for a shared traffic shaper:

```
config firewall shaper traffic-shaper
    edit <traffic_shaper_name>
        set bandwidth-unit {kbps | mbps | gbps}
    next
end
```

To change the bandwidth unit of measurement for a per-IP traffic shaper:

```
config firewall shaper per-ip-shaper
    edit <traffic_shaper_name>
```

```
        set bandwidth-unit {kbps | mbps | gbps}
    next
end
```

Multi-stage DSCP marking and class ID in traffic shapers

Traffic shapers have a multi-stage method so that packets are marked with a different differentiated services code point (DSCP) and `class id` at different traffic speeds. Marking packets with a different DSCP code is for the next hop to classify the packets. The FortiProxy benefits by marking packets with a different `class id`. Combined with the egress interface shaping profile, the FortiProxy can handle the traffic differently according to its `class id`.

Rule	DSCP code	Class ID
speed < guarantee bandwidth	`diffservcode`	`class id` in shaping policy
guarantee bandwidth < speed < exceed bandwidth	`exceed-dscp`	`exceed-class-id`
exceed bandwidth < speed	`maximum-dscp`	`exceed-class-id`

This example sets the following parameters:

- When the current bandwidth is less than 50 Kbps, mark packets with `diffservcode` 100000 and set `class id` to 10.
- When the current bandwidth is between 50 Kbps and 100 Kbps, mark packets with `exceed-dscp` 111000 and set `exceed-class-id` to 20.
- When the current bandwidth is more than 100 Kbps, mark packets with `maximum-dscp` 111111 and set `exceed-class-id` to 20.

To set multi-stage DSCP marking and class ID in a traffic shaper:

```
config firewall shaper traffic-shaper
    edit "50k-100k-150k"
        set guaranteed-bandwidth 50
        set maximum-bandwidth 150
        set diffserv enable
        set dscp-marking-method multi-stage
        set exceed-bandwidth 100
        set exceed-dscp 111000
        set maximum-dscp 111111
        set diffservcode 100000
    next
end
```

```
config firewall shaping-policy
     edit 1
         set service "ALL"
         set dstintf PORT2
         set srcaddr "all"
         set dstaddr "all"
         set class-id 10
     next
end
```

Traffic shapers also have an `overhead` option that defines the per-packet size overhead used in rate computation.

To set the traffic shaper overhead option:

```
config firewall shaper traffic-shaper
    edit "testing"
        set guaranteed-bandwidth 50
        set maximum-bandwidth 150
        set overhead 14 <range from 0 to 100>
    next
end
```

Example

This example shows how to mark QA traffic with a different DSCP according to real-time traffic speed.

To configure the firewall address:

```
config firewall address
    edit QA_team
        set subnet 10.1.100.0/24
    next
end
```

To configure the firewall shaper traffic shaper:

```
config firewall shaper traffic-shaper
    edit "500k-1000k-1500k"
        set guaranteed-bandwidth 500
        set maximum-bandwidth 1500
        set diffserv enable
        set dscp-marking-method multi-stage
        set exceed-bandwidth 1000
        set exceed-dscp 111000
        set maximum-dscp 111111
        set diffservcode 100000
    next
end
```

```
config firewall shaping-policy
    edit QA_team
        set service "ALL"
        set dstintf port1
        set traffic-shaper "500k-1000k-1500k"
        set traffic-shaper-reverse "500k-1000k-1500k"
        set srcaddr "QA_team"
        set dstaddr "all"
    next
end
```

DSCP marking in firewall shaping policies

Use the `diffserv-forward` and `diffserv-reverse` fields in firewall shaping policies to perform DSCP marking in firewall shaping policies to change the DSCP tag on egress traffic. Traffic is allowed or blocked according to the Differentiated Services Code Point (DSCP) values in the incoming packets. When DSCP marking on `firewall shaper traffic-shaper` and `firewall shaping-policy` both apply to the same session, `shaper traffic-shaper` overrides `shaping-policy`.

The following CLI variables in `config firewall shaping-policy` are used to mark the packets:

`diffserv-forward {enable | disable}`	Enable/disable changing a packet's DiffServ values to the value specified in `diffservcode-forward` (default = disable).
`diffservcode-forward <dscp_value>`	The value that packet's DiffServ is set to (default = 000000). This variable is only available when `diffserv-forward` is enabled.
`diffserv-reverse {enable | disable}`	Enable/disable changing a packet's reverse (reply) DiffServ values to the value specified in `diffservcode-rev` (default = disable).
`diffservcode-rev <dscp_value>`	The value that packet's reverse (reply) DiffServ is set to (default = 000000). This variable is only available when `diffserv-rev` is enabled.

Example

A FortiProxy has a traffic shaping policy to mark traffic from the QA team with a DSCP value of 100000, while reverse traffic is marked with 000011. To configure the FortiProxy:

```
config firewall shaping-policy
    edit 1
        set name "QA Team 50MB"
        set service "ALL"
        set dstintf "port3"
        set traffic-shaper "50MB/s"
        set traffic-shaper-reverse "50MB/s"
        set diffserv-forward enable
        set diffserv-reverse enable
        set srcaddr "QA"
        set dstaddr "all"
        set diffservcode-forward 100000
        set diffservcode-rev 000011
    next
end
```

Examples

This section includes the following traffic shaping configuration examples:

- Interface-based traffic shaping profile on page 179
- Ingress traffic shaping profile on page 183

Interface-based traffic shaping profile

A traffic shaping policy can be used for interface-based traffic shaping by organizing traffic into 30 class IDs. The shaping profile defines the percentage of the interface bandwidth that is allocated to each class. Each traffic class ID is shaped to the assigned speed according to the outgoing bandwidth limit configured to the interface.

Traffic classification

A shaping policy classifies traffic and organizes it into different class IDs, based on matching criteria. For traffic matching a criteria, you can choose to put it into 30 different shaping classes, identified by class ID 2 to 31.

You must select an outgoing interface for the traffic. The shaping policy is only applied when the traffic goes to one of the selected outgoing interfaces.

Criterion	Description
Source	• Address: match the source address of the traffic to the selected address or address group. • User: use the user credentials of the traffic to match the selected user or user group. At least one address, address group, or internet service must also be selected. • Internet service: match the traffic to the selected internet service. Internet services cannot be used if addresses or address or groups are used.
Destination	• Address: match the destination address of the traffic to the selected address or address group. • Internet service: match the traffic to the selected internet service. Internet services cannot be used if addresses or address or groups are used.
Schedule	Match the current date and time to the selected schedule. You can select a one-time schedule, recurring schedule, or schedule group. This setting is optional.
Service	Match the service of the traffic to the selected service or service group.
Users	Match the user of the traffic.
Groups	Match the user group(s) of the traffic.

When multiple items are selected in one criterion, it is considered a match when traffic matches any one of them.

Traffic prioritization

Shaping profiles define how different shaping classes of traffic are prioritized. For each class, you can define three prioritization strategies: guaranteed bandwidth, maximum bandwidth, and priority.

For each shaping profile, a default shaping class must be defined. Traffic is prioritized based on the default shaping group in the following two circumstances:

- All traffic to the outgoing interface that does not match to any shaping policy
- Traffic with a shaping group that is not defined in a shaping profile

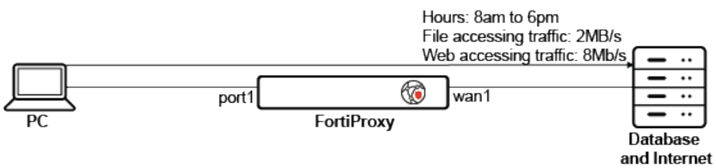
Prioritization strategy	Description
Guaranteed bandwidth	The percentage of the link speed that is reserved for the shaping group. The total guaranteed bandwidth for all shaping groups cannot exceed 100%.
Maximum bandwidth	The maximum percentage of the link speed that the shaping group can use.
Priority	The shaping class priority: top, critical, high, medium, or low. When groups are competing for bandwidth on the interface, the group with the higher priority wins.

Applying a shaping profile to an interface

Traffic shaping is accomplished by configuring the outgoing bandwidth and outgoing shaping profile on an interface. The shaping profile uses the outgoing bandwidth of the interface as the maximum link speed, and it only works when the outgoing bandwidth is configured.

This example shows how to apply interface-based traffic shaping to web and file accessing traffic according to a schedule:

- The link speed of the wan1 interface is 10 Mb/s.
- File access can use up to 2 Mb/s from 8:00 AM to 6:00 PM.
- Web access can use 8 Mb/s from 8:00 AM to 6:00 PM.



Create a recurring schedule in the GUI

To create a recurring schedule in the GUI:

1. Go to *Policy & Objects > Schedules*.
2. Click *Create New > Schedule*.
3. Configure a recurring schedule called *Day_Hours* for everyday from 8:00 AM to 6:00 PM.
4. Click *OK*.

Putting the traffic into shaping classes

To create a traffic shaping policy and class ID for web accessing traffic in the GUI:

1. Go to *Policy & Objects > Traffic Shaping*, select the *Traffic Shaping Policies* tab, and click *Create New*.
2. Configure the policy by referring to Create or edit a traffic-shaping policy on page 164. Set *Service Type* to *Firewall Service* and select web accessing services under *Firewall Service*, such as *HTTP* and *HTTPS*. Set *Outgoing interface* to *wan1*.
3. Click *OK*.

To create a traffic shaping policy and class ID for the file accessing traffic in the GUI:

1. Go to *Policy & Objects* > *Traffic Shaping*, select the *Traffic Shaping Policies* tab, and click *Create New*.
2. Configure the policy by referring to Create or edit a traffic-shaping policy on page 164. Set *Service Type* to *Firewall Service* and select file accessing services under *Firewall Service*, such as *ASF3*, *FTP* and *SMB*. Set *Outgoing interface* to *wan1*.
3. Click the *Traffic shaping class ID* drop down then click *Create*.
4. Click *OK*.

To put the traffic into shaping classes in the CLI:

1. Create a recurring schedule:

```
config firewall schedule recurring
 edit "Day_Hours"
  set start 08:00
  set end 18:00
  set day sunday monday tuesday wednesday thursday friday saturday
 next
end
```

2. Create the traffic class IDs:

```
config firewall traffic-class
    edit 3
        set class-name "Web Access"
    next
    edit 4
        set class-name "File Access"
    next
end
```

3. Create the web and file accessing traffic shaping policies:

```
config firewall shaping-policy
    edit 2
        set name "web_access_day_hours"
        set comment "Limit web accessing traffic to 8Mb/s in day time"
        set service "HTTP" "HTTPS"
        set schedule "Day_Hours"
        set dstintf "wan1"
        set class-id 3
        set srcaddr "all"
        set dstaddr "all"
    next
    edit 3
        set name "file_access_day_hours"
        set comment "Limit file accessing traffic to 2Mb/s during the day"
        set service "AFS3" "FTP" "FTP_GET" "FTP_PUT" "NFS" "SAMBA" "SMB" "TFTP"
        set schedule "Day_Hours"
        set dstintf "wan1"
        set class-id 4
        set srcaddr "all"
        set dstaddr "all"
    next
end
```

Allocating bandwidth to the shaping classes

A traffic shaping profile defines the guaranteed and maximum bandwidths each class receives. In this example, file access can use up to 2 Mb/s and web access can use 8 Mb/s.

To create a traffic shaping profile using the GUI:

1. Go to *Policy & Objects* > *Traffic Shaping*, select the *Traffic Shaping Profiles* tab, and click *Create New*.
2. Enter a name for the profile, such as *Day_Hours_Profile*.
3. Configure a default traffic shaping class:
   This class has a high priority, meaning that when the other classes have reached their guaranteed bandwidths, this default class will use the rest of the available bandwidth.
   a. Enter the class ID you specified in the *Putting the traffic into shaping classes* section.
   b. Configure the following settings, then click *OK*:

Guaranteed bandwidth	30
Maximum bandwidth	100
Priority	High

4. Configure a web accessing traffic shaping class:
   When other types of traffic are competing for bandwidth, this class is guaranteed to 6 Mb/s, or 60% of the bandwidth.
   a. In the *Traffic Shaping Classes* table click *Create New*.
   b. Configure the following settings, then click *OK*:

Traffic shaping class ID	Web Access
Guaranteed bandwidth	60
Maximum bandwidth	80
Priority	Medium

5. Configure a file accessing traffic shaping class:
   When other types of traffic are competing for bandwidth, this group is guaranteed to 1 Mb/s, or 10% of the bandwidth.
   a. In the *Traffic Shaping Classes* table click *Create New*.
   b. Configure the following settings, then click *OK*:

Traffic shaping class ID	File Access
Guaranteed bandwidth	10
Maximum bandwidth	20
Priority	Medium

6. Click *OK*.

To create a traffic shaping profile using the CLI:

```
config firewall shaping-profile
    edit "Day_Hours_Profile"
```

```
        set default-class-id 2
        config shaping-entries
            edit 1
                set class-id 2
                set guaranteed-bandwidth-percentage 30
                set maximum-bandwidth-percentage 100
            next
            edit 2
                set class-id 3
                set priority medium
                set guaranteed-bandwidth-percentage 60
                set maximum-bandwidth-percentage 80
            next
            edit 3
                set class-id 4
                set priority medium
                set guaranteed-bandwidth-percentage 10
                set maximum-bandwidth-percentage 20
            next
        end
    next
end
```

Defining the available bandwidth on an interface

In this example, the link speed of the wan1 interface is 10 Mb/s.

To set the bandwidth of the wan1 interface in the GUI:

1. Go to *Network* > *Interfaces*.
2. Edit the wan1 interface.
3. Under Traffic Shaping, enable *Outbound shaping profile* and select the profile that you just created, *Day_Hours_Profile*.
4. Enable *Outbound Bandwidth* and set it to *10000* Kbps.
5. Click *OK*.

To set the bandwidth of the wan1 interface in the CLI:

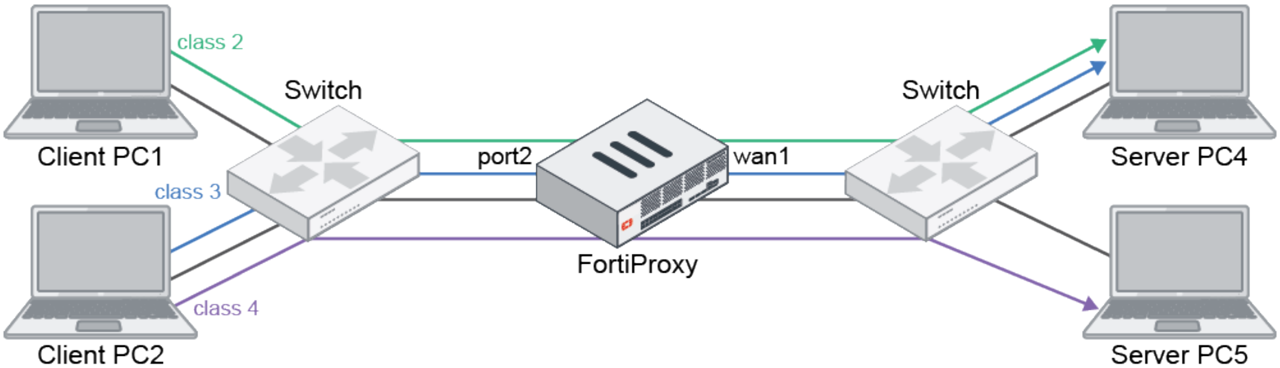
```
config system interface
    edit "wan1"
        set egress-shaping-profile "Day_Hours_Profile"
        set outbandwidth 10000
    next
end
```

Ingress traffic shaping profile

A traffic shaping profile can be applied to an interface for traffic in the ingress direction. Similar to an egress traffic shaping profile, the guaranteed bandwidth and priority of the profile will be respected when an interface receives inbound traffic. When congestion occurs, any remaining bandwidth will be allotted to classes based on priority.

Example

In this example, the port2 interface has a total inbound bandwidth of 100 Mbps. Traffic from certain clients to certain servers are assigned different classes.



IPv6 traffic from any client PCs to server PCs is assigned class 5.

For each class, the priority, guaranteed bandwidth, and maximum bandwidth are as follows:

Class	Priority	Guaranteed bandwidth	Maximum bandwidth
2	Low	10%	60%
3	High	20%	100%
4	High	30%	100%
5	Medium	10%	50%

Bandwidth will first be allotted to each class according to its guaranteed bandwidth. Then remaining available bandwidth will be allotted to class 3 and 4 first based on their priority. The allocation will be proportional to their guaranteed bandwidth ratio.

To configure ingress traffic shaping:

1. Configure the client and server addresses:

```
config firewall address
    edit "pc1"
        set subnet 10.1.100.11 255.255.255.255
    next
    edit "pc2"
        set subnet 10.1.100.22 255.255.255.255
    next
    edit "pc4"
        set subnet 172.16.200.44 255.255.255.255
    next
    edit "pc5"
        set subnet 172.16.200.55 255.255.255.255
    next
end
```

2. Configure the class IDs:

```
config firewall traffic-class
    edit 2
        set class-name "class2"
    next
    edit 3
        set class-name "class3"
    next
    edit 4
        set class-name "class4"
    next
    edit 4
        set class-name "class5"
    next
end
```

3. Configure traffic shaping policies to assign classes to each group of traffic.
   a. Configure a policy to assign traffic from PC1 to PC4 in class 2:

```
config firewall shaping-policy
    edit 1
        set name "shaping policy 1"
        set service "ALL"
        set dstintf "wan1"
        set class-id 2
        set srcaddr "pc1"
        set dstaddr "pc4"
    next
end
```

   b. Configure a policy to assign traffic from PC2 to PC4 in class 3:

```
config firewall shaping-policy
    edit 2
        set name "shaping policy 2"
        set service "ALL"
        set dstintf "wan1"
        set class-id 3
        set srcaddr "pc2"
        set dstaddr "pc4"
    next
end
```

   c. Configure a policy to assign traffic from PC2 to PC5 in class 4:

```
config firewall shaping-policy
    edit 3
        set name "shaping policy 3"
        set service "ALL"
        set dstintf "wan1"
        set class-id 4
        set srcaddr "pc2"
        set dstaddr "pc5"
    next
end
```

d. Configure a policy to assign all IPv6 traffic to class 5:

```
config firewall shaping-policy
    edit 4
        set name "shaping policy 4"
        set ip-version 6
        set service "ALL"
        set dstintf "wan1"
        set class-id 5
        set srcaddr6 "all"
        set dstaddr6 "all"
    next
end
```

4. Configure a shaping profile to set the priority, and the guaranteed and maximum bandwidth percentages for each class:

```
config firewall shaping-profile
    edit "ingShapeProfile"
        set default-class-id 2
        config shaping-entries
            edit 2
                set class-id 2
                set priority low
                set guaranteed-bandwidth-percentage 10
                set maximum-bandwidth-percentage 60
            next
            edit 3
                set class-id 3
                set guaranteed-bandwidth-percentage 20
                set maximum-bandwidth-percentage 100
            next
            edit 4
                set class-id 4
                set guaranteed-bandwidth-percentage 30
                set maximum-bandwidth-percentage 100
            next
            edit 5
                set class-id 5
                set priority medium
                set guaranteed-bandwidth-percentage 10
                set maximum-bandwidth-percentage 50
            next
        end
    next
end
```

5. Configure the inbandwidth and apply the ingress shaping profile on port2:

```
config system interface
    edit "port2"
        set ip 10.1.100.1 255.255.255.0
        set inbandwidth 100000
        set ingress-shaping-profile "ingShapeProfile"
        config ipv6
            set ip6-address 2000:10:1:100::1/64
        end
```

```
    next
end
```

Inbandwidth must be configured for traffic shaping to take effect.

6. Configure firewall policies to allow IPv4 and IPv6 traffic to go through. Since traffic shaping is for inbound traffic on port2, the policy is defined from port2 to wan1:

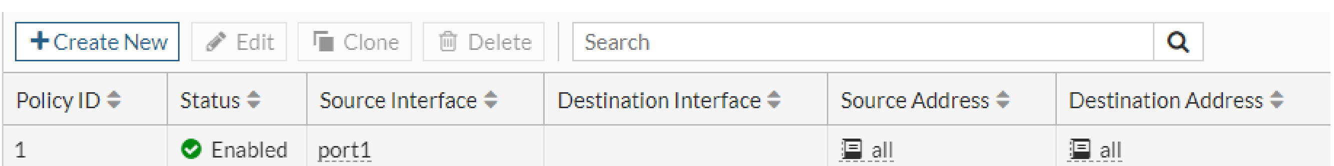
```
config firewall policy
    edit 20
        set uuid d9f9be4c-eaab-51ed-41d6-783cecc11c0c
        set srcintf "port2"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
end
```

```
config firewall policy
    edit 21
        set uuid c535a92a-eaac-51ed-6e6c-3943f8c2dc8f
        set srcintf "port2"
        set dstintf "wan1"
        set srcaddr6 "all"
        set dstaddr6 "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
end
```

Central SNAT

NAT is a process used to modify or translate either the source or destination IP address or port in a packet header. The primary use for NAT is to allow multiple network devices on a private network to be represented by a single public IP address when they browse the Internet.

The FortiProxy unit applies the NAT settings from matching central Source Network Address Translation (SNAT) policies. Go to *Policy & Objects > Central SNAT* to create a central SNAT policy.



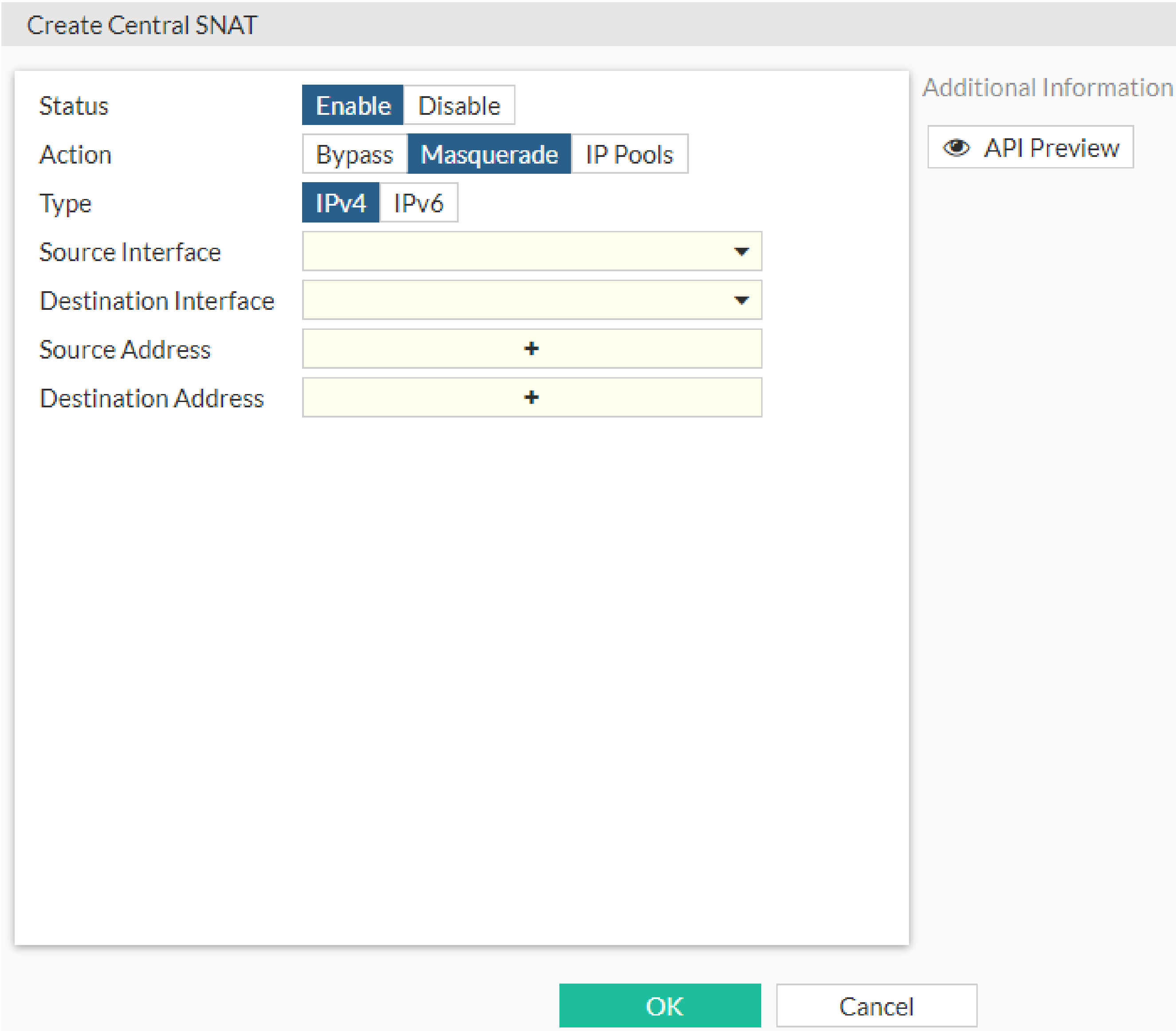
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Select to open the *Create Central SNAT* window. See Create or edit a central SNAT policy on page 188.
Edit	Edit the selected central SNAT policy. See Create or edit a central SNAT policy on page 188.
Clone	Copy an existing central SNAT policy.
Delete	Delete the selected central SNAT policy.
Search	Enter a search term to find in the list.
Policy ID	SNAT identifier.
Status	The status is either *enable* (active) or *disable* (inactive).
Source Interface	The source interface name is either a port or *any*.
Destination Interface	The destination interface name.
Source Address	The source addresses and address groups.
Destination Address	The destination addresses and address groups.
Action	The central SNAT action is *Bypass*, *Masquerade*, or *IP Pools*.
nat-ippool	The name of the NAT IP pool.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a central SNAT policy

Select *Create New* to open the *Create Central SNAT* window. To change a central SNAT policy, select the policy and then click *Edit*.



Configure the following settings in the *Create Central SNAT* window or the *Edit Central SNAT* window and then click *OK*:

Status	Select *Enable* make the central SNAT policy is active.
Action	Select one of the following options for the central SNAT action: • *Bypass*—Do not perform network address translation (NAT). • *Masquerade*—Use a single IP address to protect multiple IP addresses in a LAN. • *IP Pools*—Use an IP address from an IP pool. An IP pool defines a single IP address or a range of IP addresses to be used as the source address for the duration of the session. These assigned addresses are used instead of the IP address assigned to that FortiProxy interface.
Type	Select *IPv4* or *IPv6*.

Source Interface	Select one of the available interfaces from the drop-down list.
Destination Interface	Select one of the available interfaces from the drop-down list.
Source Address **Source IPv6 Address**	Click +. A window slides out from the right. Here, you can select from the available addresses and address groups. Select one or more items to add to the field. Clicking on an object in this window while it is highlighted removes it from the field. Multiple selections are allowed. For more information on addresses, see Addresses on page 197.
Destination Address **Destination IPv6 Address**	Click +. A window slides out from the right. Here, you can select from the available addresses and address groups. Select one or more items to add to the field. Clicking on an object in this window while it is highlighted removes it from the field. Multiple selections are allowed. For more information on addresses, see Addresses on page 197.
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.

To create a central SNAT policy in the CLI:

```
config firewall central-snat-map
   edit <policy_identifier>
      set status {enable | disable}
      set action {bypass | masquerade | ippool}
      set ipv6 {enable | disable}
      set srcintf <source_interface_name>
      set dstintf <destination_interface_name>
      set src-addr <original_address>
      set dst-addr <original_address>
   end
```

For example, to create an IPv4 central SNAT policy:

```
config firewall central-snat-map
   edit 1
      set status enable
      set action masquerade
      set ipv6 disable
      set srcintf port2
      set dstintf port1
      set src-addr "all"
      set dst-addr "all"
   end
```

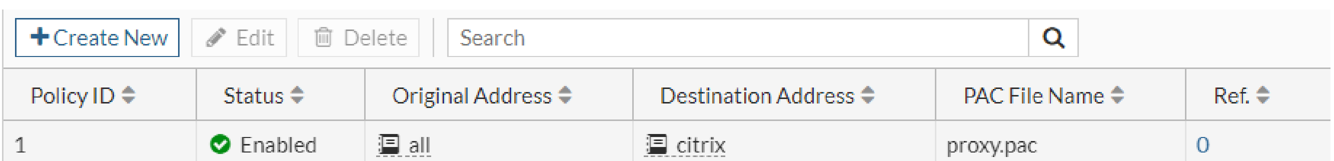
For example, to create an IPv6 central SNAT policy:

```
config firewall central-snat-map
   edit 1
      set status enable
      set action ippool
      set ipv6 enable
      set srcintf port1
      set dstintf port3
      set src-addr6 "all"
      set dst-addr6 "all"
      set nat-ippool6 "pool6"
   end
```

PAC Policy

Proxy auto-config (PAC) files automatically choose the appropriate proxy server for browsers and other user agents. Not every user in an organization has the same proxy server requirements. Supporting multiple PAC files provides granular control. To manage multiple PAC files, you use PAC policies.

To see a list of available PAC policies in the GUI, go to *Policies & Objects* > *PAC Policy*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

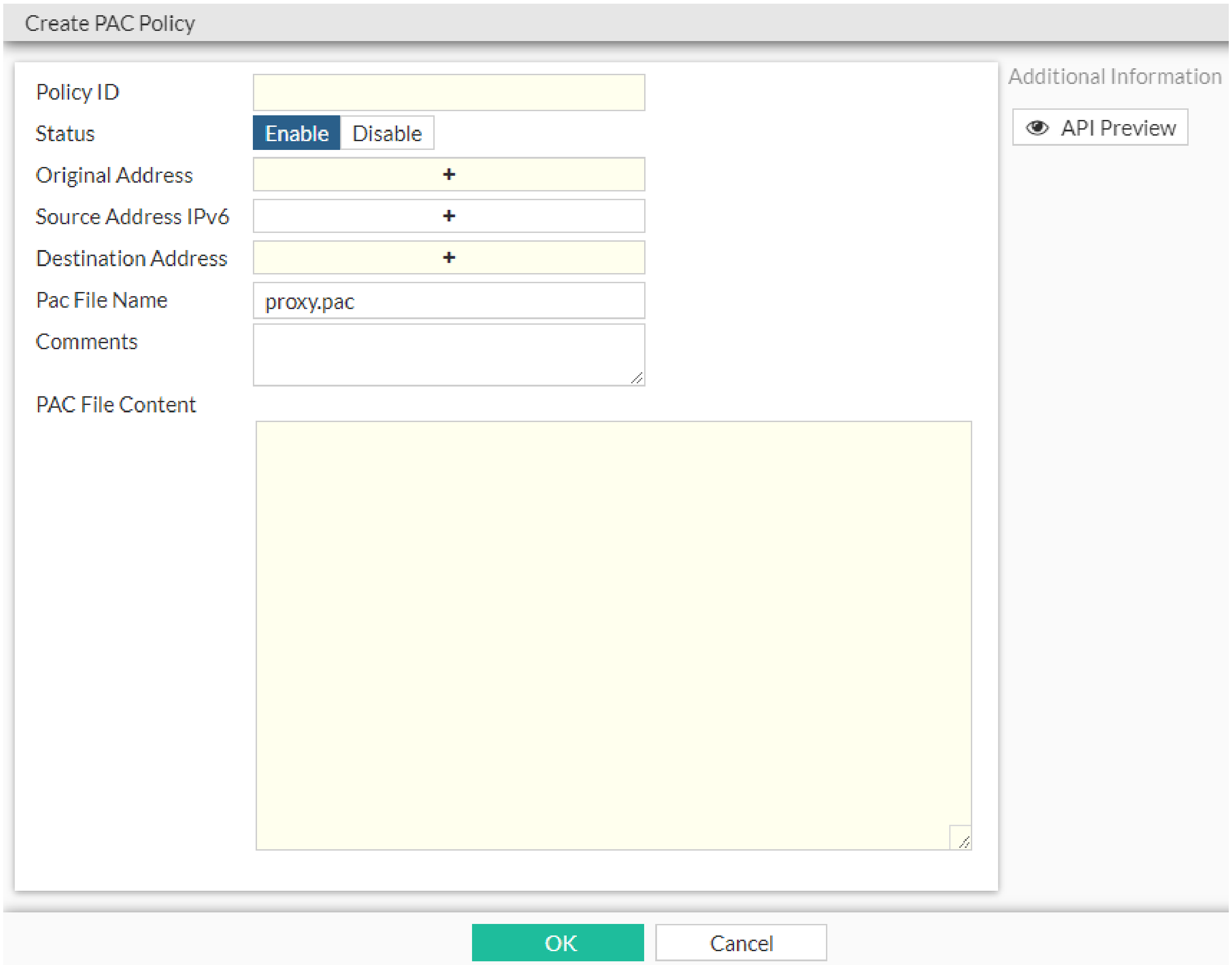
The following options are available:

Create New	Select to open the *Create PAC Policy* window. See Create or edit a PAC policy on page 192.
Edit	Edit the selected PAC policy. See Create or edit a PAC policy on page 192.
Delete	Delete the selected PAC policy.
Search	Enter a search term to find in the list.
Policy ID	The PAC policy identifier.
Status	The status is enabled or disabled.
Original Address	The source address of the initiating traffic.
Destination Address	The destination address that the policy matches.
PAC File Name	The name of the PAC file.
Ref.	Displays the number of times the object is referenced to other objects.

	To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a PAC policy

Select *Create New* to open the *Create PAC Policy* window. To change a PAC policy, select a policy and then click *Edit*.



Configure the following settings in the *Create PAC Policy* window or the *Edit PAC Policy* window and then click *OK*:

Policy ID	Enter the PAC policy identifier.
Status	Click *Enable* to make the policy active.
Original Address	Enter the source IPv4 address of the initiating traffic.
Source Address IPv6	Enter the source IPv6 address of the initiating traffic.
Destination Address	Enter the destination address that the policy matches.

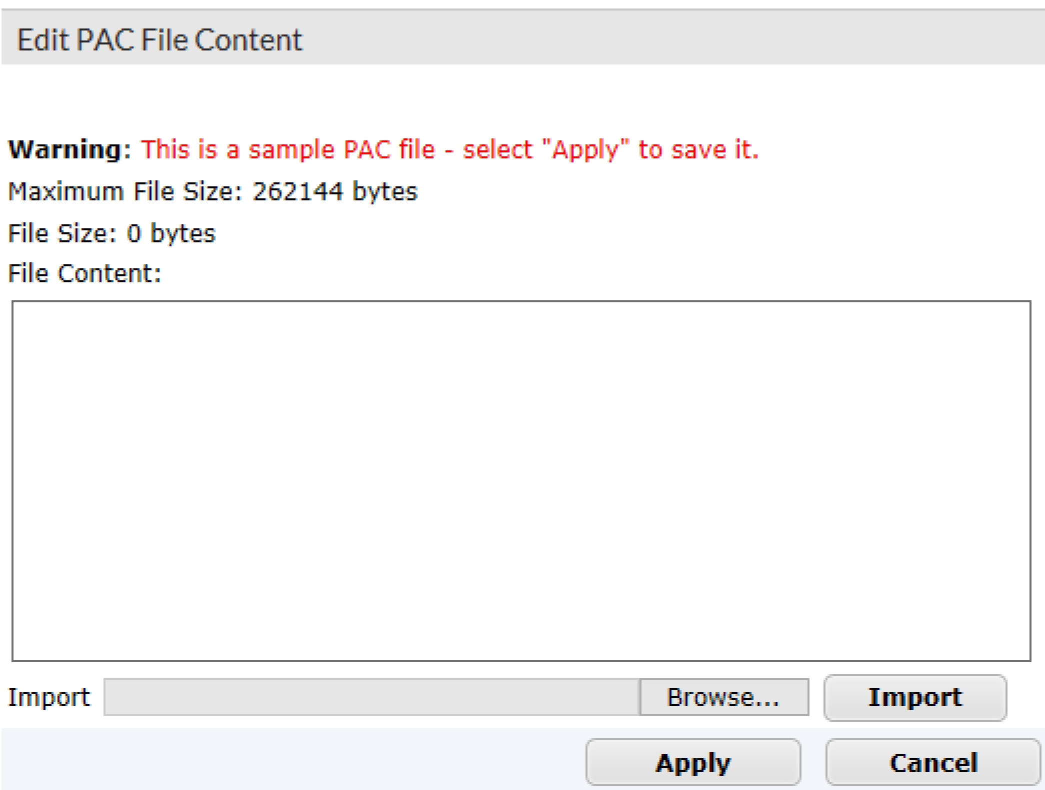
Pac File Name	Enter the name of the PAC file.
Comments	Enter an optional description of the PAC policy.
PAC File Content	Type or copy and paste a PAC file.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected 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.

Edit a PAC file

In the Create PAC Policy window or Edit PAC Policy window, click *Edit* to open the *Edit PAC File Content* window.

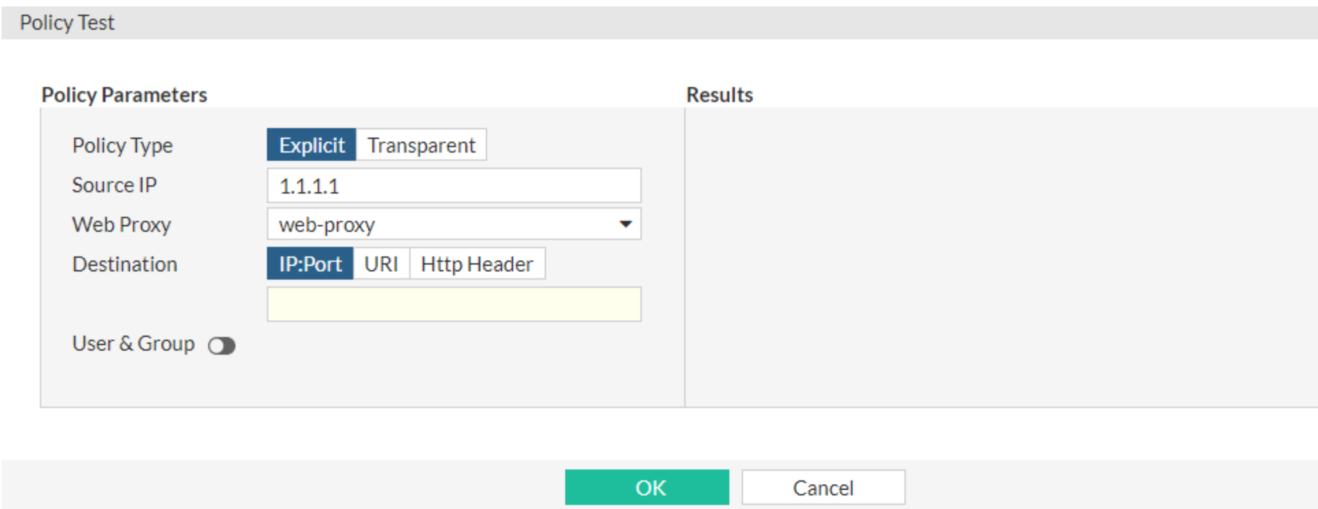


To add content to a PAC file:

1. If you have a PAC file, select *Browse*, navigate to the PAC file, select *Open,* and then select *Import*. After you import the PAC file, you can edit the content in the text box.
2. If you do not have a PAC file, you can type the content into the text box or copy and paste the content into the text box.
3. Click *Apply*.

Policy Test

You can check the configuration of explicit web proxy policies and transparent firewall policies to confirm that they are set up correctly.



The combination of policy type and source IP address forms the source traffic to test.

If a URI or HTTP header is specified as the destination, the policy test uses a DNS lookup to determine the actual IP address and port number of the destination traffic. If the client's DNS lookup differs from the device's DNS lookup, the policy used for the test might be different that the policy used on the client's traffic.

To test a policy:

1. Go to *Policy & Objects* > *Policy Test*.
2. Configure the following settings:

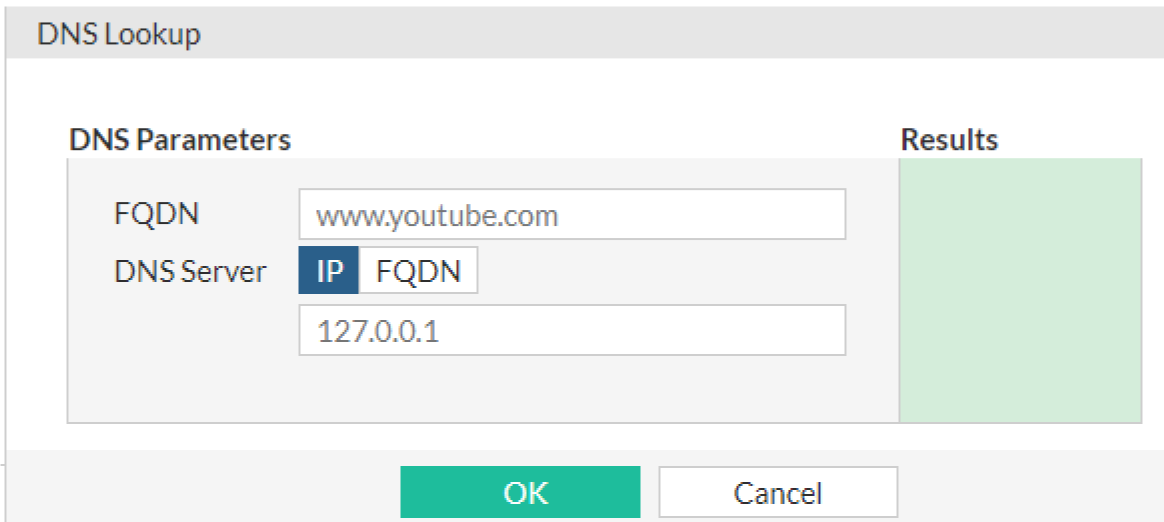
Policy Test	Select whether you want to test an *Explicit* or *Transparent* policy.
Source IP	Enter the source IP address.
Web Proxy	If you selected *Explicit*, select *web-proxy* or search for an explicit web proxy. To create an explicit web proxy, see Create or edit an explicit web proxy on page 55.
Source Interface	If you selected *Transparent*, enter the source interface.

Destination	Select *IP:Port*, *URI*, or *HTTP Header* and enter the destination.
User & Group	If you want to test a specific user or user group, enable *User & Group* and then select one user or user group.

3. Click *OK*. The results show the policy configuration if a policy matches the parameters.

DNS Lookup - NEW

You can check the associated IPs (20 entries maximum) for a specific domain (FQDN) on a specific DNS server.



To view the associated IPs for a domain on a specific DNS server:

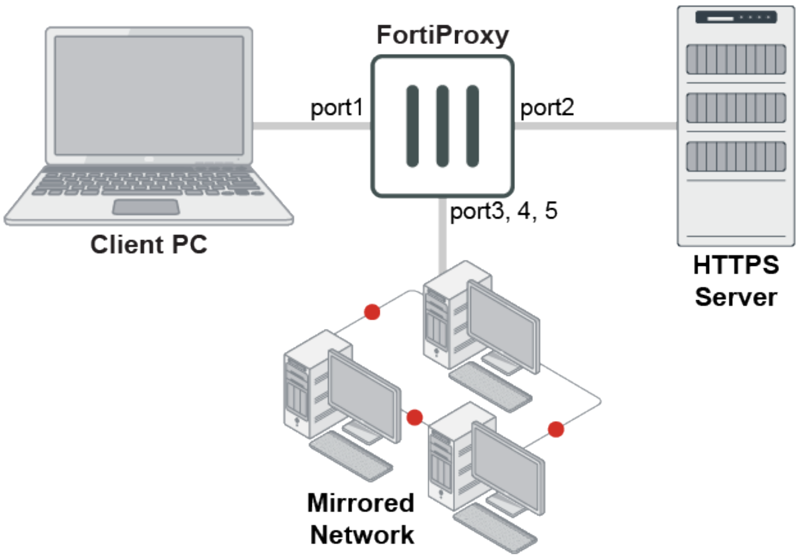
1. Go to *Policy & Objects > DNS Lookup*
2. Configure the following settings:

FQDN	Enter the domain name.
DNS Server	Select *IP* or *FQDN* and enter the source IP address or domain of the DNS server for which you want to check the associated IPs.

3. Click *OK*. The results show the associated IPs for the specified domain on the specified DNS server.

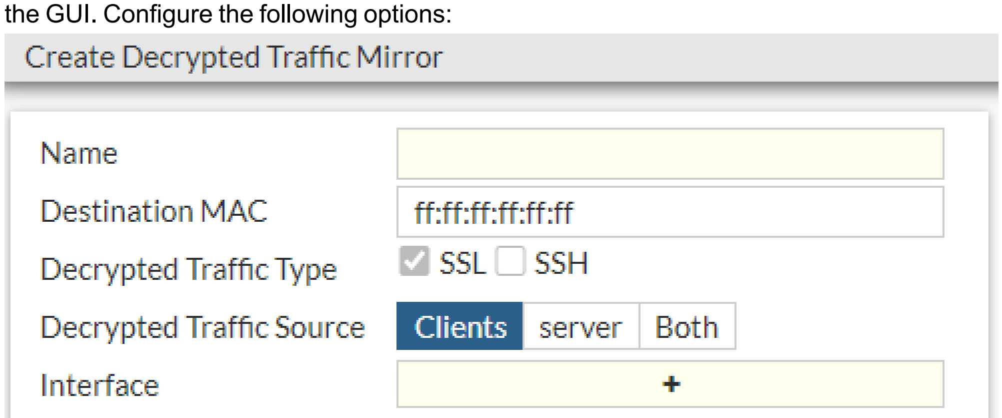
Decrypted Traffic Mirror

SSL mirroring allows the FortiProxy unit to decrypt and mirror traffic to a designated port. A decrypted traffic mirror profile can be applied to explicit, transparent, SSH tunnel, and SSH proxy policies when the custom-deep-inspection, deep-inspection, or deep-test SSL/SSH inspection security profile is selected. SSL inspection is automatically enabled when you enable a security profile on the policy configuration page.



To configure SSL mirroring in a policy:

1. Create a decrypted traffic mirror profile by selecting *Create New* under *Policy & Objects* > *Dycrypted Traffic Mirror* in the GUI. Configure the following options:



Name	Enter the name of the decrypted traffic mirror profile.
Destination MAC	Enter the destination MAC address for the mirrored traffic.
Decrypted Traffic Type	Select whether decrypted SSL traffic, decrypted SSH traffic, or both are mirrored.
Decrypted Traffic Source	Select whether decrypted client-side traffic, decrypted server-side traffic, or both are mirrored.
Interface	Select which interfaces will have decrypted traffic mirrored. Fortinet recommends that you mirror the traffic to a dedicated interface or virtual interface.
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.

Alternatively, use the `config firewall decrypted-traffic-mirror` command. For example:

```
config firewall decrypted-traffic-mirror
  edit "1"
    set dstmac ff:ff:ff:ff:ff:ff
    set traffic-type ssl ssh
    set traffic-source both
    set interface "port1"
  next
end
```

2. Configure the policy to enable SSL traffic mirroring:

```
config firewall policy
  edit 1
    set type explicit-web
    set name "All"
    set uuid 10e62d76-7c94-51ee-fa3a-ae92170cea18
    set dstintf "port1"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "webproxy"
    set explicit-web-proxy "web-proxy"
    set utm-status enable
    set logtraffic all
    set log-http-transaction all
    set decrypted-traffic-mirror "Decrypt"
    set ssl-ssh-profile "Deep_Custom".
    set webfilter-profile "default"
  next
end
```

To verify and troubleshoot issues with traffic mirroring, use the *Network* > *Packet Capture on page 120* tab to capture and analyze the mirrored traffic.

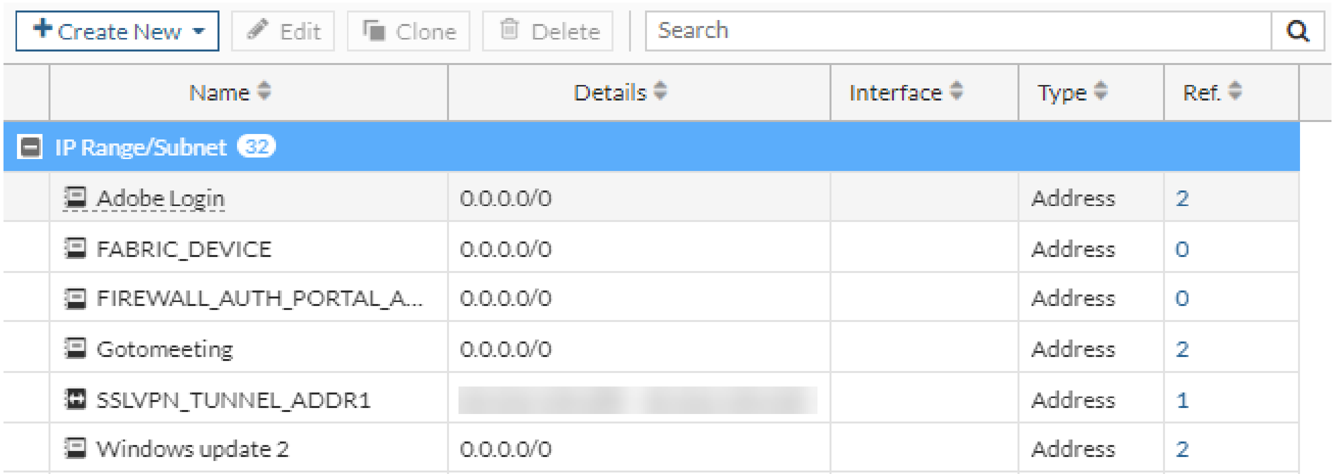
Addresses

Web cache addresses and address groups define the network addresses that you use when configuring source and destination addresses for security policies. The FortiProxy unit compares the IP addresses contained in packet headers with security policy source and destination addresses to determine if the security policy matches the traffic. Addresses can be IPv4 addresses and address ranges, IPv6 addresses, and fully qualified domain names (FQDNs).

Be careful if employing FQDN web cache addresses. Using a fully qualified domain name in a security policy, while convenient, does present some security risks because policy matching then relies on a trusted DNS server. If the DNS server becomes compromised, security policies requiring domain name resolution might no longer function properly.

Web cache addresses in the address list are grouped by type: Address, Address Group, IPv6 Address, IPv6 Address Group, Proxy Address, or Proxy Group. A FortiProxy unit's default configurations include all address, which represents any IPv4 IP address on any network. You can also add a firewall address list when configuring a security policy.

To view the address list, go to *Policy & Objects* > *Addresses*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

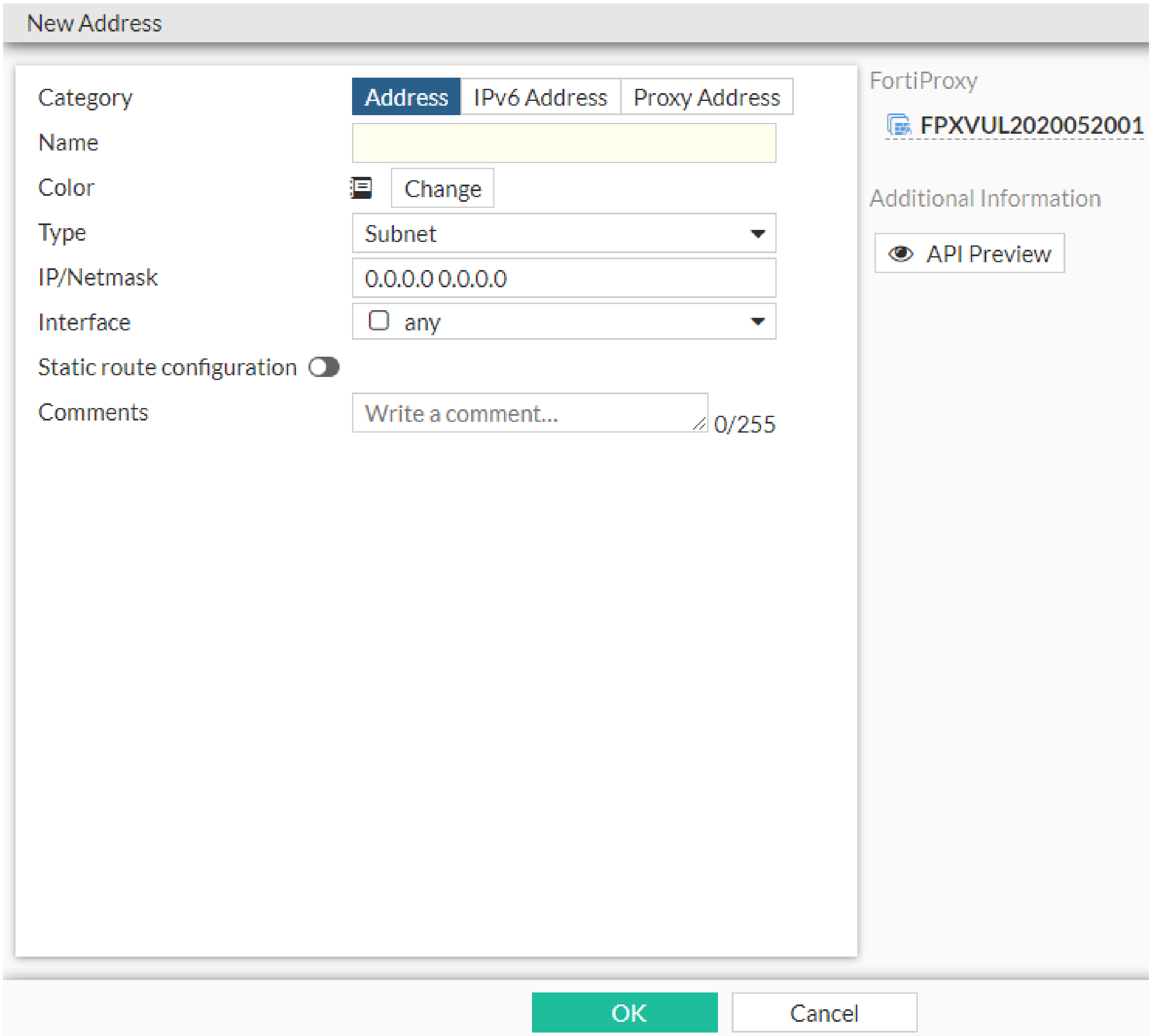
The following options are available:

Create New > Address	Add a new address. See Create or edit an address on page 199.
Create New > Address Group	Add a new address group. See Create or edit an address group on page 210.
Create New > IPv6 Address Template	Add an IPv6 address template. See Create or edit an IPv6 address template on page 212.
Edit	Edit the selected address. See Create or edit an address on page 199 or Create or edit an address group on page 210
Clone	Make a copy of the selected address or address group.
Delete	Remove the selected address or address group. This icon appears only if a policy or address group is not currently using the address.
Search	Search for text in any column.
Name	The name of the address.
Details	The domain name.
Interface	The interface to which the address is bound.
Type	Select the type of address: *FQDN*, *Geography*, *IP Range*, *Subnet*, *Wildcard FQDN*, *Dynamic SDN address*, *IPv6 Subnet*, *URL Pattern*, *Host Regex Match*, *URL Category*, *HTTP Method*, *User Agent*, *HTTP Header*, *Advanced (Source)*, or *Advanced (Destination)*.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in *Ref.*, and the *Object Usage* window appears displaying the various locations of the referenced object.
Comments	Optional description of the address.

Exclude Members	Addresses excluded from an address group.
Routable	Whether the IP address can be used for routing.

Create or edit an address

Select *Create New* > *Address* to open the *New Address* window.



To open the *Edit Address* window, select an address and then click *Edit*.

Configure the following settings in the *New Address* window or the *Edit Address* window and then click *OK*:

Category	Select *Address*, *IPv6 Address*, or *Proxy Address*.

Name	Enter a name for the IPv4 address, IPv6 address, or proxy address. Addresses must have unique names.
Color	Select *Change* to choose a color for the icon.
Type	If you selected *Address* for the category, select one of the following: • *Subnet* • *IP Range* • *FQDN* • *Geography* • *Dynamic* • *Device (MAC Address)* If you selected *IPv6 Address* for the category, select one of the following: • *IPv6 Subnet* • *IPv6 Range* • *IPv6 FQDN* • *IPv6 Geography* • *IPv6 Fabric Connector Address* • *IPv6 Template* • *Device (MAC Address)* If you selected *Proxy Address* for the category, select one of the following. Refer to Proxy address on page 202 for more information about each proxy address type. • *Host Regex Match* • *URL Pattern* • *URL Category* • *URL List* • *HTTP Method* • *User Agent* • *HTTP Header* • *Advanced (Source)* • *Advanced (Destination)*
IP/Netmask	If you selected *Subnet* as the IPv4 address type, enter the IP address and netmask.
IP Range	If you selected *IP Range* as the IPv4 address type or you selected *IPv6 Range* as the IPv6 address type, enter an IP address range separated by a hyphen. See Web cache policy address formats.
FQDN	If you selected *FQDN* as the IPv4 address type or *IPv6 FQDN* as the IPv6 address type, enter the fully qualified domain name.
Country/Region	If you selected *Geography* as the IPv4 address type or *IPv6 Geography* as the IPv6 address type, select the country or region.

Sub Type	If you selected Dynamic as the IPv4 address type, select *ClearPass*, *Fabric Connector Address*, *FortiNAC Tag*, *FortiVoice Tag*, *Fortinet Single Sign-On (FSSO)*, or *Switch Controller NAC Policy Tag*.
SPT (System Posture Token)	If you selected *ClearPass* as the *Sub Type*, select *Checkup*, *Healthy*, *Infected*, *Quarantine*, *Transient*, or *Unknown*.
SDN Connector	If you selected *Fabric Connector Address* as the *Sub Type* or *IPv6 Fabric Connector Address* as the IPv6 address type, select an existing SDN connector or create a new one. See External Connectors on page 581.
FSSO Group	If you selected *Fortinet Single Sign-On (FSSO)* as the *Sub Type*, select an existing FSSO group or create a new one. See Create or edit a user group on page 420.
MAC address	If you selected *Device (MAC Address)* as the *Sub Type* or *Type*, enter the MAC address or range of MAC addresses.
IPv6 Address	If you selected *IPv6 Subnet* as the IPv6 address type, enter the IPv6 address.
IPv6 Address Template	If you selected *IPv6 Template* as the IPv6 address type, select an existing IPv6 address template or create one. See Create or edit an IPv6 address template on page 212.
Host Type	If you selected *IPv6 Template* as the IPv6 address type, select *any* or *specific*. If you select *specific*, enter the host name.
Interface	Select the interface to which you want to bind the IPv4 address. Select *any* if you want to bind the IP address with the interface when you create a policy.
Host	Enter or select the host name.
Host Regex Pattern	If you selected *Host Regex Match* as the proxy address type, enter the appropriate string.
URL Path Regex	If you selected *URL Pattern* or *Advanced (Destination)* as the proxy address type, enter the appropriate string.
URL Category	If you selected *URL Category* or *Advanced (Destination)* as the proxy address type, select the FortiGuard web filter category or categories.
URL List	If you selected *URL List* as the proxy address type, select a URL list from the list.
Request Method	If you selected *HTTP Method* or *Advanced (Source)* as the proxy address type, select *CONNECT*, *DELETE*, *GET*, *HEAD*, *OPTIONS*, *POST*, *PUT*, or *TRACE*.
User Agent	If you selected *User Agent* or *Advanced (Source)* as the proxy address type, select a browser or browsers.
Header Name	If you selected *HTTP Header* as the proxy address type, enter the header name.
Header Regex	If you selected *HTTP Header* as the proxy address type, enter the appropriate string value.
Request Method	If you selected *Advanced (Source)* as the proxy address type, select *CONNECT*, *DELETE*, *GET*, *HEAD*, *OPTIONS*, *POST*, *PUT*, or *TRACE*.

HTTP Header	If you selected *Advanced (Source)* as the proxy address type, enter the name and value of the header.
Static Route Configuration	Enabling this feature includes the address in the listing of named addresses when setting up a static route. This option is available only when the *Type* is *FQDN*, IP Range, or *Subnet*.
Comments	Optionally, enter a description of the address.
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.

Proxy address

The following proxy address types are available for firewall policies:

- Host regex match on page 203
- URL pattern on page 203
- URL category on page 204
- URL list on page 205
- HTTP method on page 206
- HTTP header on page 208
- User agent on page 207
- Advanced (source) on page 208
- Advanced (destination) on page 209

Fast policy match

The fast policy match function improves the performance of IPv4 explicit and transparent web proxies on FortiProxy devices.

When enabled, after the firewall policies are configured, the FortiProxy builds a fast searching table based on the different firewall policy matching criteria. When fast policy matching is disabled, web proxy traffic is compared to the policies one at a time from the beginning of the policy list.

Fast policy matching is enabled by default, and can be configured with the following CLI command:

```
config web-proxy global
    set fast-policy-match {enable | disable}
end
```

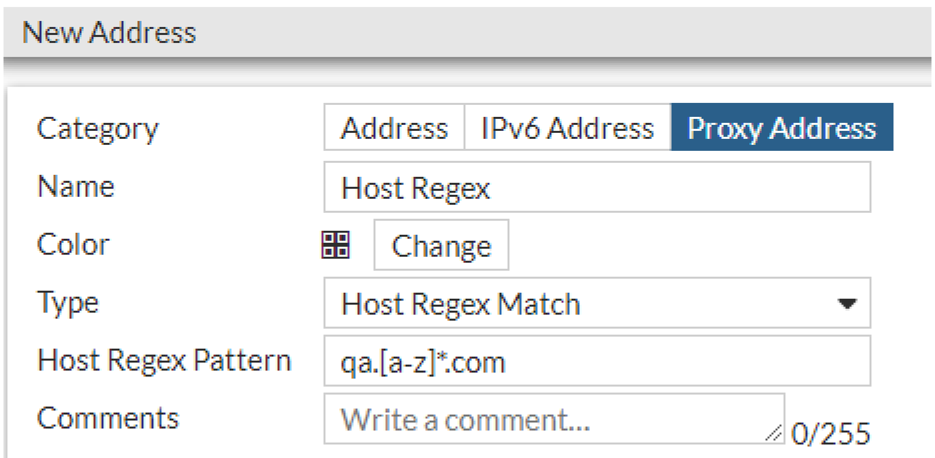
Host regex match

In this address type, a user can create a hostname as a regular expression. Once created, the hostname address can be selected as a destination of a firewall policy. This means that a policy will only allow or block requests that match the regular expression.

This example creates a host regex match address with the pattern *qa.[a-z]*.com*.

To create a host regex match address in the GUI:

1. Go to *Policy & Objects > Addresses*.
2. Click *Create New > Address*.
3. Set the following:
   - *Category* to *Proxy Address*,
   - *Name* to *Host Regex*,
   - *Type* to *Host Regex Match*, and
   - *Host Regex Pattern* to *qa.[a-z]*.com*.



4. Click *OK*.

To create a host regex match address in the CLI:

```
config firewall proxy-address
    edit "Host Regex"
        set type host-regex
        set host-regex "qa.[a-z]*.com"
    next
end
```

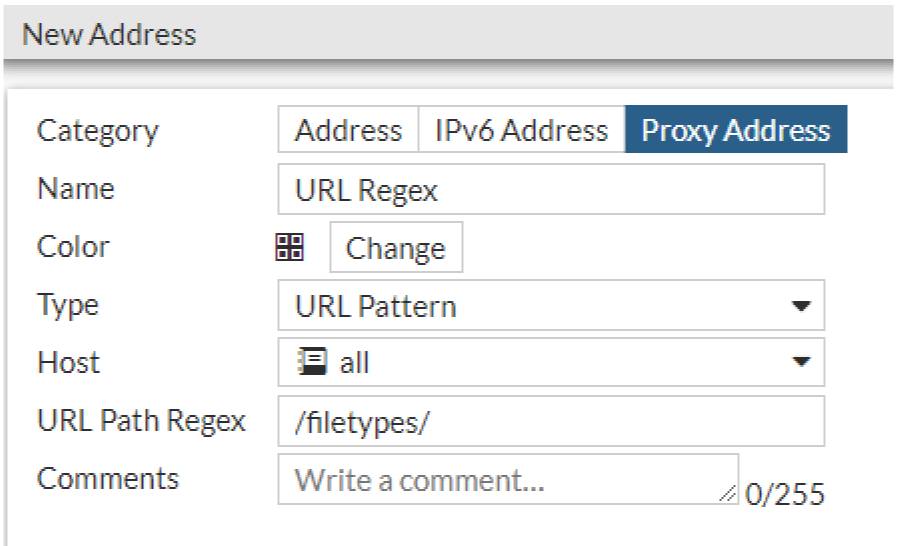
URL pattern

In this address type, a user can create a URL path as a regular expression. Once created, the path address can be selected as a destination of a firewall policy. This means that a policy will only allow or block requests that match the regular expression.

This example creates a URL pattern address with the pattern */filetypes/*.

To create a URL pattern address in the GUI:

1. Go to *Policy & Objects* > *Addresses*.
2. Click *Create New* > *Address*.
3. Set the following:
   - *Category* to *Proxy Address*,
   - *Name* to *URL Regex*,
   - *Type* to *URL Pattern*,
   - *Host* to *all*, and
   - *URL Path Regex* to */filetypes/*.



4. Click *OK*.

To create a URL pattern address in the CLI:

```
config firewall proxy-address
    edit "URL Regex"
        set type url
        set host "all"
        set path "/filetypes/"
    next
end
```

URL category

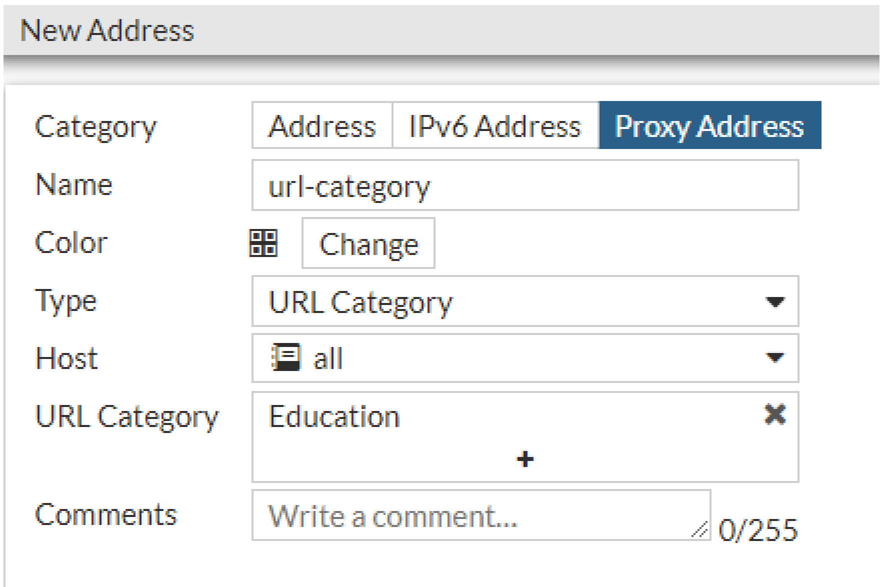
In this address type, a user can create a URL category based on a FortiGuard URL ID. Once created, the address can be selected as a destination of a firewall policy. This means that a policy will only allow or block requests that match the URL category.

The example creates a URL category address for URLs in the *Education* category. For more information about categories, see https://fortiguard.com/webfilter/categories.

For information about creating and using custom local and remote categories, see Web Rating Overrides on page 323.

To create a URL category address in the GUI:

1. Go to *Policy & Objects > Addresses*.
2. Click *Create New > Address*.
3. Set the following:
   - *Category* to *Proxy Address*,
   - *Name* to *url-category*,
   - *Type* to *URL Category*,
   - *Host* to *all*, and
   - *URL Category* to *Education*.



4. Click *OK*.

To create a URL category address in the CLI:

```
config firewall proxy-address
    edit "url-category"
        set type category
        set host "all"
        set category 30
    next
end
```

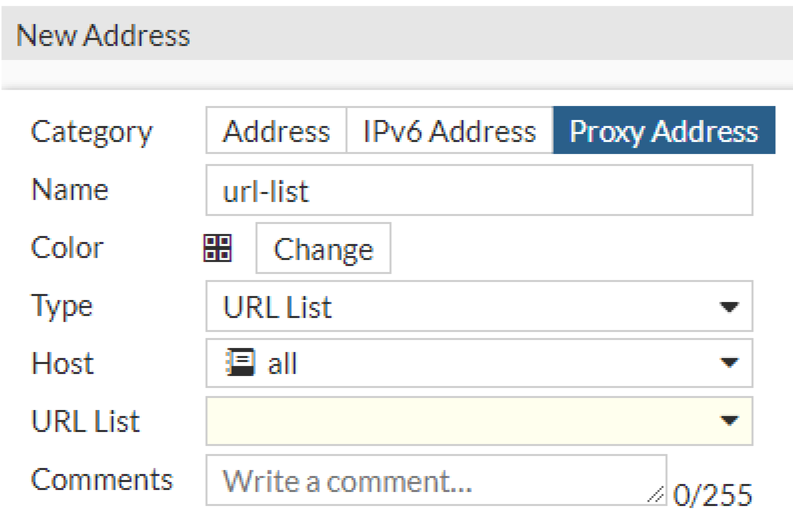
To see a list of all the categories and their numbers, when editing the address, enter `set category ?`.

URL list

In this address type, a user can create a URL list based on an existing web filter URL list that you created under *Security Profiles > Web Filter URL List*. Once created, the URL list can be selected as a destination of a firewall policy. This means that a policy will only allow or block requests that match the URL list.

To create a URL list address in the GUI:

1. Go to *Policy & Objects > Addresses*.
2. Click *Create New > Address*.
3. Set the following:
   - *Category* to *Proxy Address*,
   - *Name* to *url-list*,
   - *Type* to *URL List*,
   - *Host* to *all*, and
   - *URL List* to one that is available. If no URL list is available, create one under *Security Profiles > Web Filter URL List*.



4. Click *OK*.

To create a URL list address in the CLI:

1. If no web filter URL list is defined, use the config webfilter url-list command to define one.
2. Create a URL list address by referencing the web filter URL list:

```
config firewall proxy-address
   edit "url-list"
      set type url-list
      set host "all"
      set url list "example-list"
   next
end
```

HTTP method

In this address type, a user can create an address based on the HTTP request methods that are used. Multiple method options are supported, including: *CONNECT*, *DELETE*, *GET*, *HEAD*, *OPTIONS*, *POST*, *PUT*, and *TRACE*. Once created, the address can be selected as a source of a firewall policy. This means that a policy will only allow or block requests that match the selected HTTP method.

The example creates a HTTP method address that uses the GET method.

To create a HTTP method address in the GUI:

1. Go to *Policy & Objects > Addresses*.
2. Click *Create New > Address*.
3. Set the following:
   - *Category* to *Proxy Address*,
   - *Name* to *method_get*,
   - *Type* to *HTTP Method*,
   - *Host* to *all*, and
   - *Request Method* to *GET*.
4. Click *OK*.

To create a HTTP method address in the CLI:

```
config firewall proxy-address
    edit "method_get"
        set type method
        set host "all"
        set method get
    next
end
```

User agent

In this address type, a user can create an address based on the names of the browsers that are used as user agents. Multiple browsers are supported, such as Chrome, Firefox, Internet Explorer, and others. Once created, the address can be selected as a source of a firewall policy. This means that a policy will only allow or block requests from the specified user agent.

This example creates a user agent address for Google Chrome.

To create a user agent address in the GUI:

1. Go to *Policy & Objects > Addresses*.
2. Click *Create New > Address*.
3. Set the following:
   - *Category* to *Proxy Address*,
   - *Name* to *UA-Chrome*,
   - *Type* to *User Agent*,
   - *Host* to *all*, and
   - *User Agent* to *Google Chrome*.
4. Click *OK*.

To create a user agent address in the CLI:

```
config firewall proxy-address
    edit "UA-Chrome"
        set type ua
        set host "all"
```

```
        set ua chrome
    next
end
```

HTTP header

In this address type, a user can create a HTTP header as a regular expression. Once created, the header address can be selected as a source of a firewall policy. This means that a policy will only allow or block requests where the HTTP header matches the regular expression.

This example creates a HTTP header address with the pattern *Q[A-B]*.

To create a HTTP header address in the GUI:

1. Go to *Policy & Objects* > *Addresses*.
2. Click *Create New* > *Address*.
3. Set the following:
   - *Category* to *Proxy Address*,
   - *Name* to *HTTP-header*,
   - *Type* to *HTTP Header*,
   - *Host* to *all*,
   - *Header Name* to *Header_Test*, and
   - *Header Regex* to *Q[A-B]*.
4. Click *OK*.

To create a HTTP header address in the CLI:

```
config firewall proxy-address
    edit "method_get"
        set type header
        set host "all"
        set header-name "Header_Test"
        set header "Q[A-B]"
    next
end
```

Advanced (source)

In this address type, a user can create an address based on multiple parameters, including HTTP method, User Agent, and HTTP header. Once created, the address can be selected as a source of a firewall policy. This means that a policy will only allow or block requests that match the selected address.

This example creates an address that uses the get method, a user agent for Google Chrome, and an HTTP header with the pattern *Q[A-B]*.

To create an advanced (source) address in the GUI:

1. Go to *Policy & Objects* > *Addresses*.
2. Click *Create New* > *Address*.
3. Set the following:

- *Category* to *Proxy Address*,
- *Name* to *advanced_src*,
- *Type* to *Advanced (Source)*,
- *Host* to *all*,
- *Request Method* to *GET*,
- *User Agent* to *Google Chrome*, and
- *HTTP header* to *Header_Test* : *Q[A-B]*.

4. Click *OK*.

To create an advanced (source) address in the CLI:

```
config firewall proxy-address
    edit "advance_src"
        set type src-advanced
        set host "all"
        set method get
        set ua chrome
        config header-group
            edit 1
                set header-name "Header_Test"
                set header "Q[A-B]"
            next
        end
    next
end
```

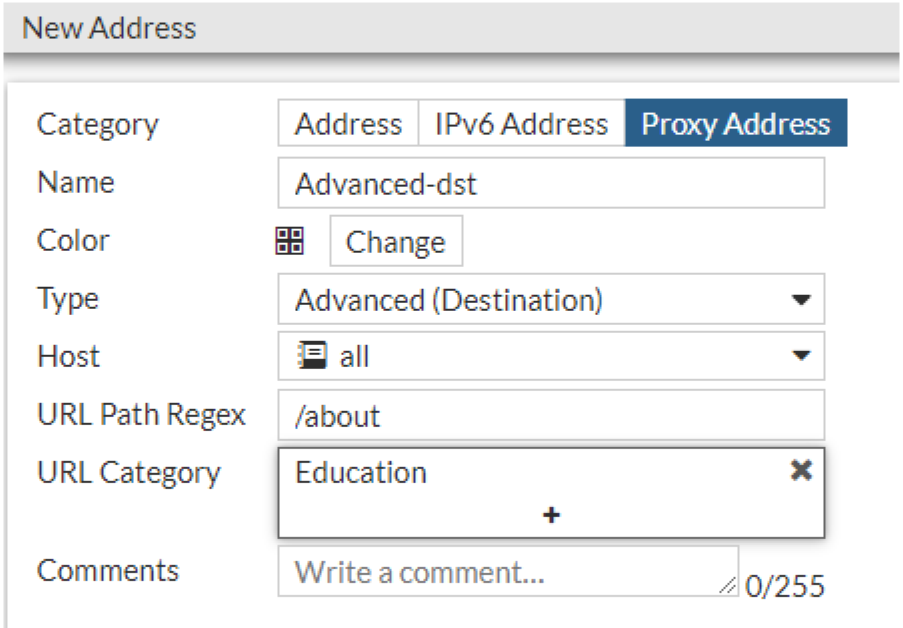
Advanced (destination)

In this address type, a user can create an address based on URL pattern and URL category parameters. Once created, the address can be selected as a destination of a firewall policy. This means that a policy will only allow or block requests that match the selected address.

This example creates an address with the URL pattern */about* that are in the *Education* category. For more information about categories, see https://fortiguard.com/webfilter/categories.

To create an advanced (destination) address in the GUI:

1. Go to *Policy & Objects* > *Addresses*.
2. Click *Create New* > *Address*.
3. Set the following:
    - *Category* to *Proxy Address*,
    - *Name* to *Advanced-dst*,
    - *Type* to *Advanced (Destination)*,
    - *Host* to *all*,
    - *URL Path Regex* to */about*, and
    - *URL Category* to *Education*.



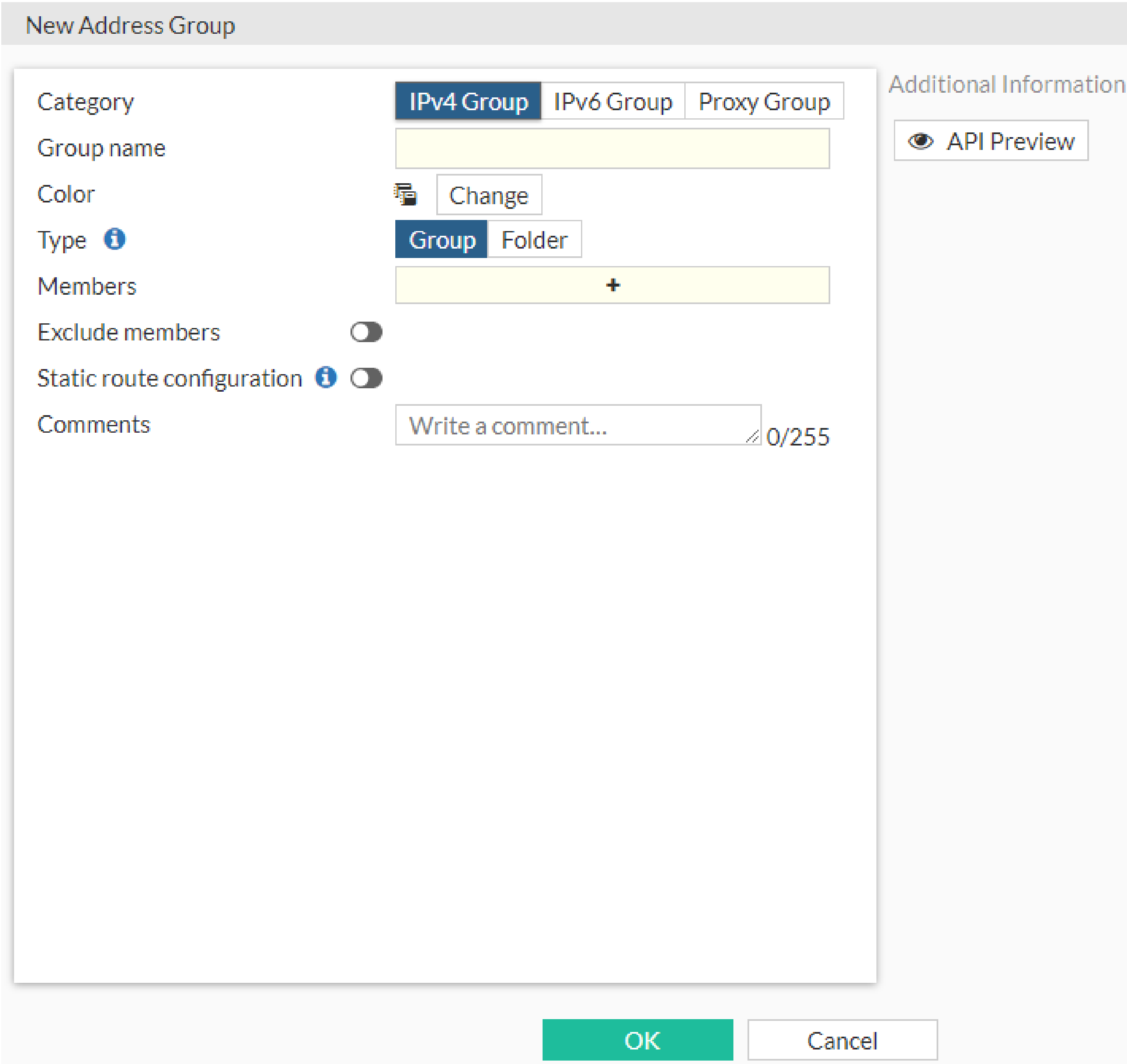
4. Click *OK*.

To create an advanced (destination) address in the CLI:

```
config firewall proxy-address
    edit "Advanced-dst"
        set type dst-advanced
        set host "ubc"
        set path "/about"
        set category 30
    next
end
```

Create or edit an address group

Select *Create New* > *Address Group* to open the *New Address Group* window.



To open the *Edit Address Group* window, select an address group and then click *Edit*.

Configure the following settings in the *New Address Group* window or the *Edit Address Group* window and then click *OK*:

Category	Select *IPv4 Group*, *IPv6 Group*, or *Proxy Group*.
Group name	Enter a name to identify the address group. Addresses, address groups, and virtual IPs must have unique names.
Color	Select *Change* to choose a color for the icon.
Type	If you selected *IPv4 Group*, select *Group* or *Folder*. If you selected *Proxy Group*, select *Source Group* or *Destination Group*.

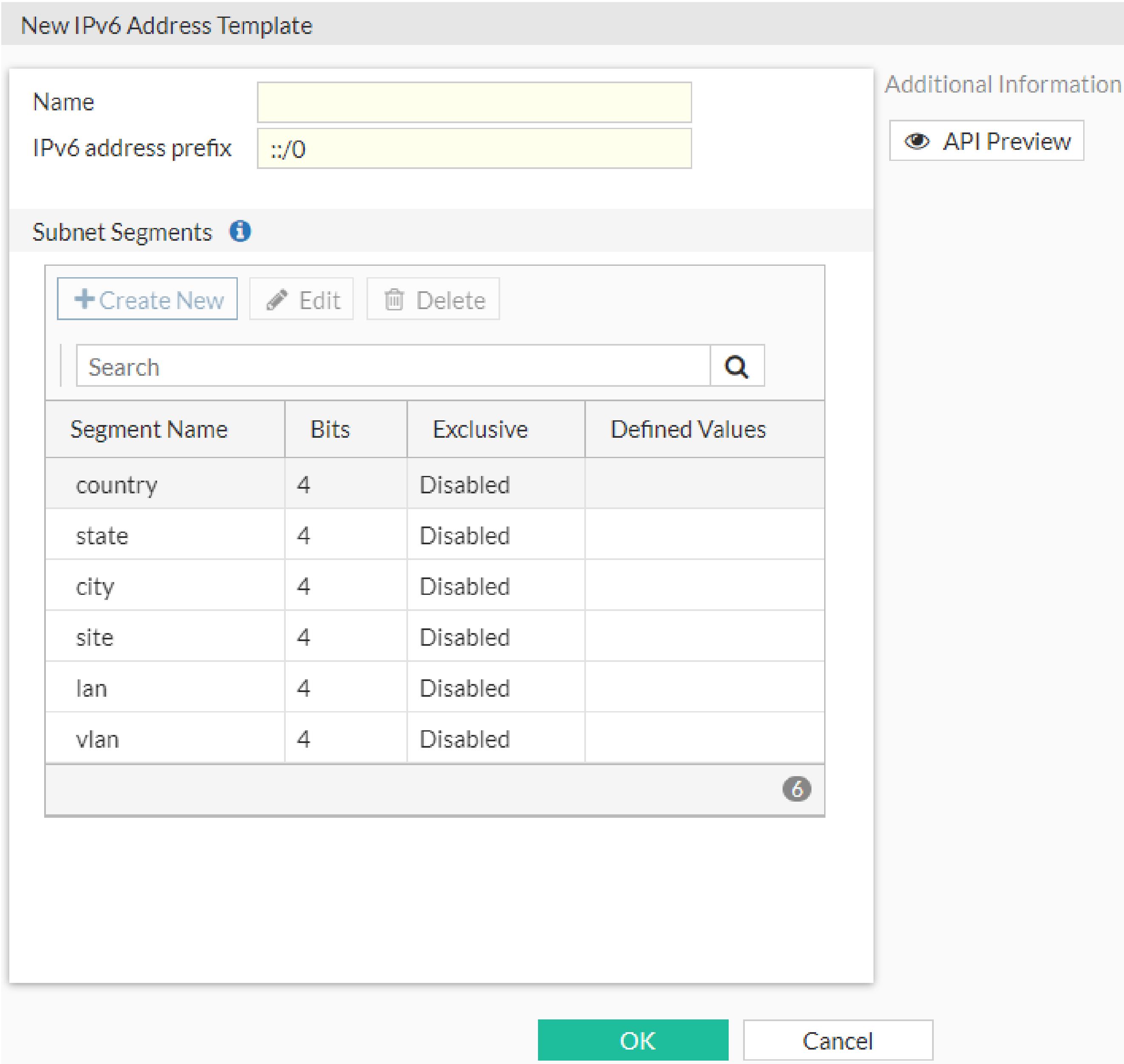
Members	Select the addresses to add to the address group. When *Category* is *Proxy Group*, select the Proxy address on page 202 or group from the list.
Exclude Members	Enable *Exclude Members* and then select the addresses to exclude from the address group.
Static Route Configuration	Enabling this feature includes the address in the listing of named addresses when setting up a static route. This option is available only if *Category* is *IPv4 Group* and every member of the address group has *Static Route Configuration* enabled.
Comments	Optionally, enter a description of the address group.
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.

Create or edit an IPv6 address template

Select *Create New* > *IPv6 Address Template* to open the *New IPv6 Address Template* window.



To open the *Edit IPv6 Address Template* window, select an IPv6 address template and then click *Edit*.

Configure the following settings in the *New IPv6 Address Template* window or the *Edit IPv6 Address Template* window and then click *OK*:

Name	Enter a name for the IPv6 address template.
IPv6 address prefix	Enter the IPv6 address prefix.
Subnet Segments	Select a maximum of six segments. Each segment can have a maximum of 16 bits.
Create New	You cannot create a subnet segment.

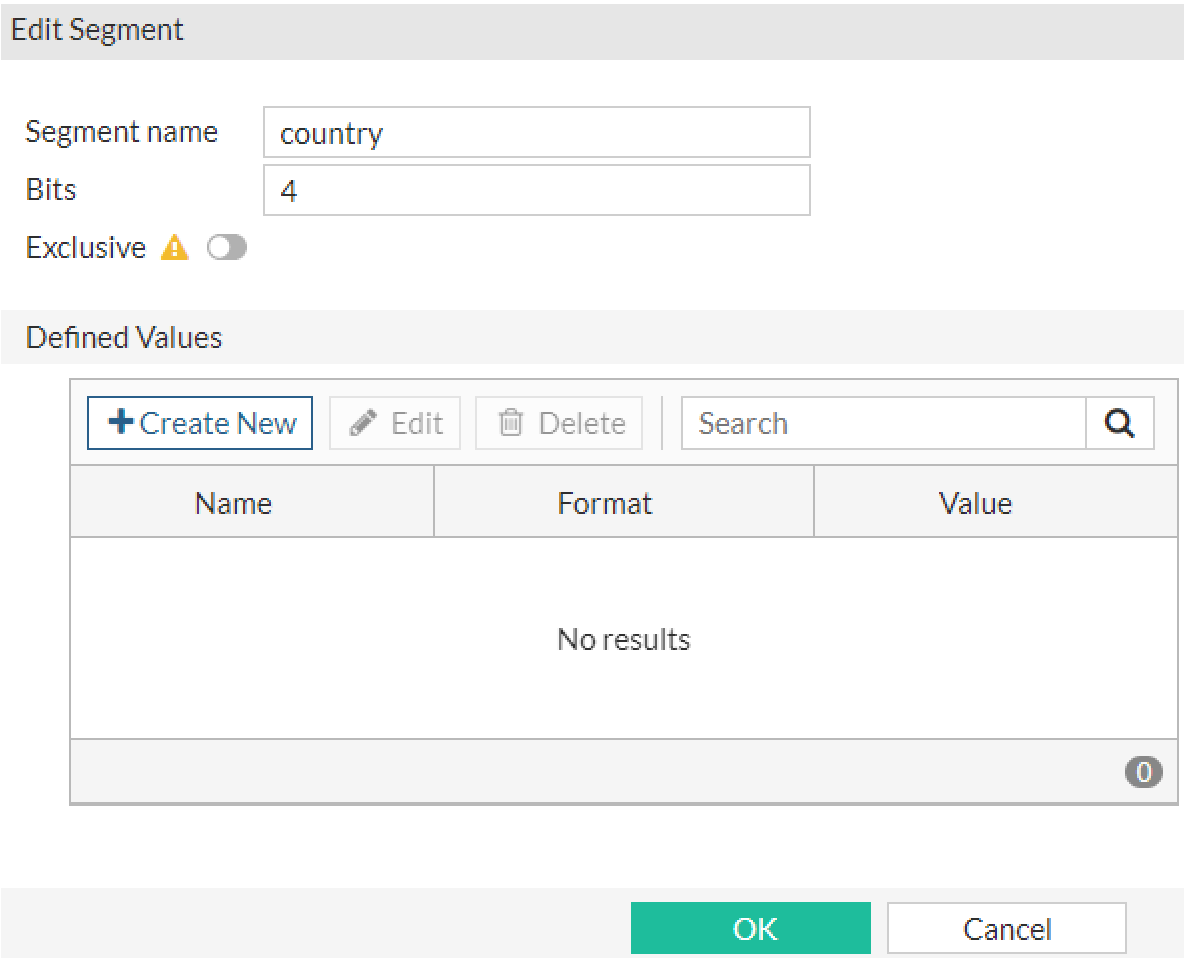
Edit	Select a subnet segment and click *Edit*. See Edit a subnet segment on page 214.
Delete	Delete the selected subnet segment.
Search	Search for text in any column.
Segment Name	The name of the subnet segment.
Bits	The number of bits used by the subnet segment.
Exclusive	*Enabled* means that the subnet segment is exclusive, and the user must select from predefined values for the segment.
Defined Values	Predefined values for an exclusive segment.
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.
References	Click to open the object usage page to show which other configuration are referencing the object.
Edit in CLI	Click to open a CLI console window to view and edit the setting in the CLI. If there are multiple CLI settings on the page, the CLI console shows the first setting.

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.

Edit a subnet segment

Select a subnet segment and click *Edit* to open the *Edit Segment* window.

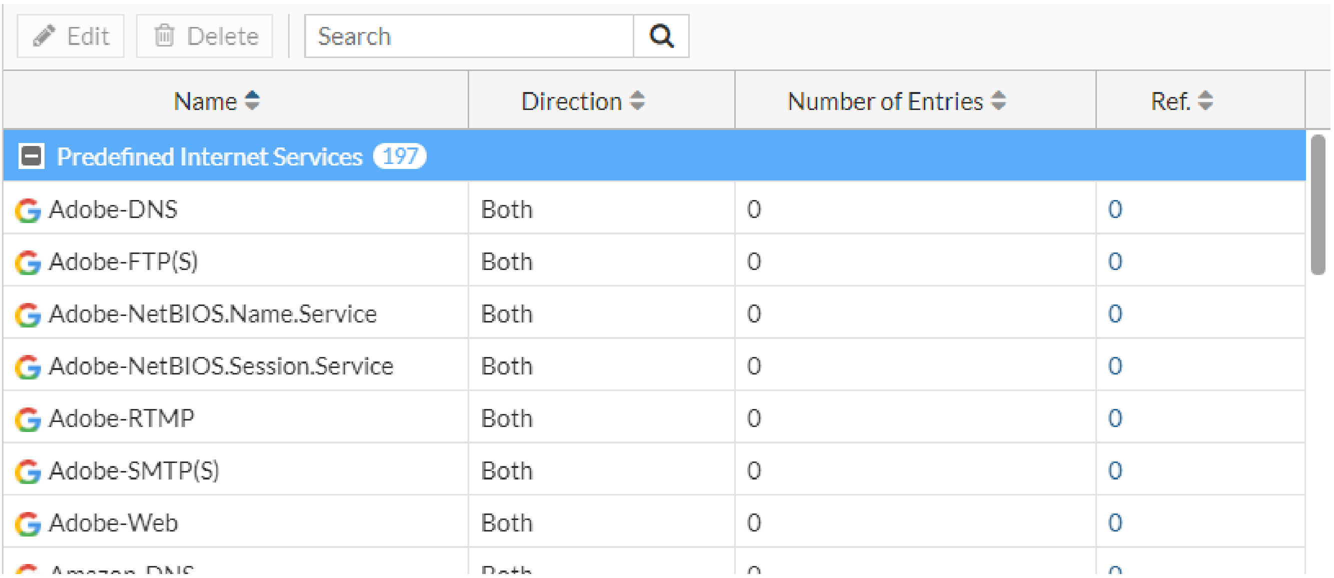


Configure the following settings in the *Edit Segment* window and then click *OK*:

Name	You can change the name of the segment.
Bits	You can change the number of bits for the segment. Each segment can have a maximum of 16 bits.
Exclusive	Enable this option to make a segment exclusive so that the user must select from predefined values for the segment. **NOTE:** You need to define at least one value before enabling *Exclusive*.
Defined Values	You can create defined values for exclusive segments.
Create New	Create the predefined values for an exclusive segment.
Edit	Select a value and then click *Edit* to change the value.
Delete	Delete the selected value.
Search	Search for text in any column.
Name	The name of the segment value.
Format	The format of the segment value.
Value	The value of the segment.

Internet Service Database

To view the Fortinet database of cloud-based applications, go to *Policy & Objects > Internet Service Database*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

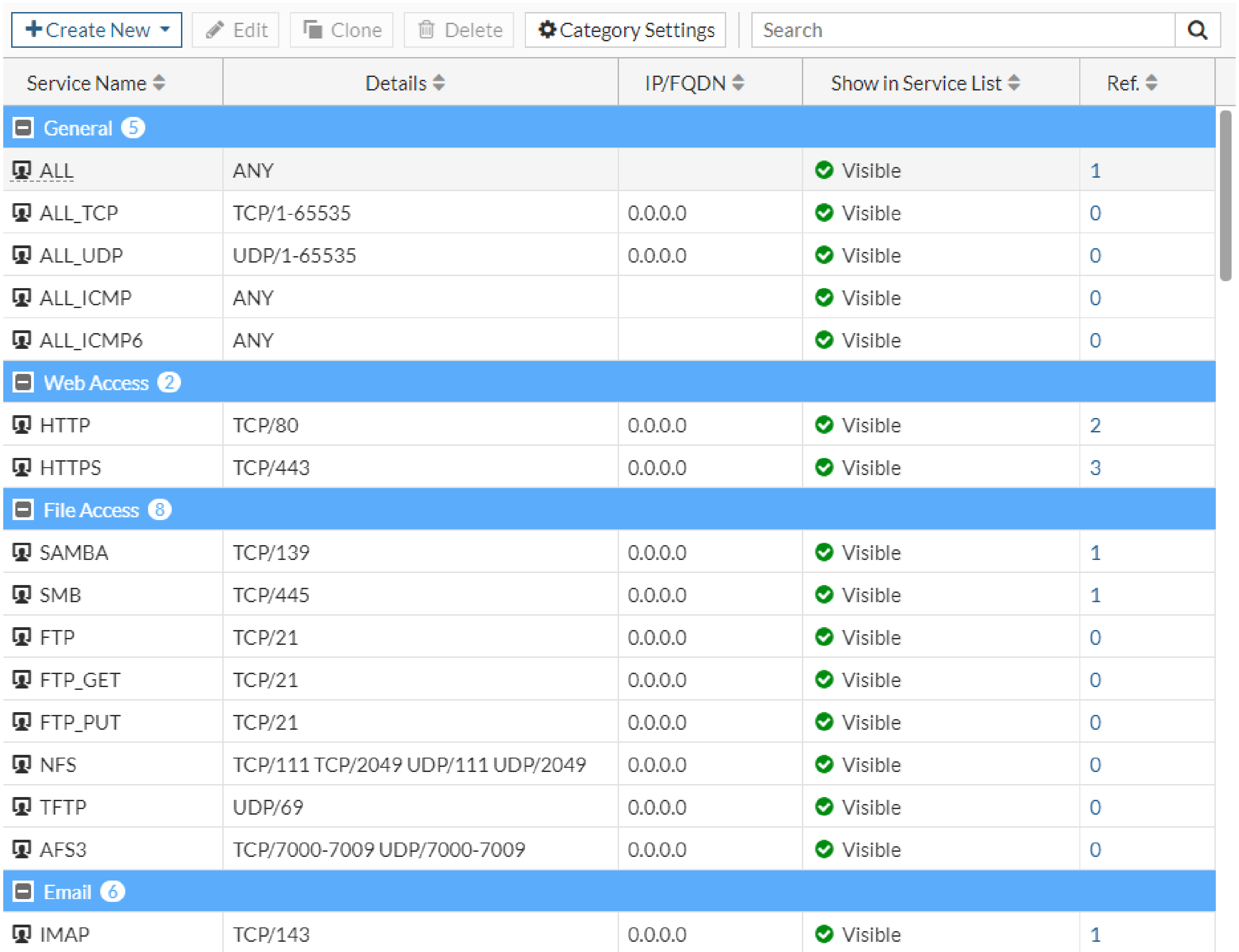
The following options are available:

Edit	Predefined Internet services cannot be changed.
Delete	Predefined Internet services cannot be deleted.
Search	Enter a search term to search the database.
Name	The name of the Internet service.
Direction	Which direction is supported for the Internet service.
Number of Entries	The number of entries in the database.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in *Ref.*, and the *Object Usage* window appears displaying the various locations of the referenced object.

Services

Web cache services define one or more protocols and port numbers associated with each service. Web cache policies use service definitions to match session types. You can organize related services into service groups to simplify your policy list.

If you need to create a web cache policy for a service that is not in the predefined service list, you can add a custom service. Custom services are configured in *Policy & Objects* > *Services*.



Service Name	Details	IP/FQDN	Show in Service List	Ref.
General 5				
ALL	ANY		Visible	1
ALL_TCP	TCP/1-65535	0.0.0.0	Visible	0
ALL_UDP	UDP/1-65535	0.0.0.0	Visible	0
ALL_ICMP	ANY		Visible	0
ALL_ICMP6	ANY		Visible	0
Web Access 2				
HTTP	TCP/80	0.0.0.0	Visible	2
HTTPS	TCP/443	0.0.0.0	Visible	3
File Access 8				
SAMBA	TCP/139	0.0.0.0	Visible	1
SMB	TCP/445	0.0.0.0	Visible	1
FTP	TCP/21	0.0.0.0	Visible	0
FTP_GET	TCP/21	0.0.0.0	Visible	0
FTP_PUT	TCP/21	0.0.0.0	Visible	0
NFS	TCP/111 TCP/2049 UDP/111 UDP/2049	0.0.0.0	Visible	0
TFTP	UDP/69	0.0.0.0	Visible	0
AFS3	TCP/7000-7009 UDP/7000-7009	0.0.0.0	Visible	0
Email 6				
IMAP	TCP/143	0.0.0.0	Visible	1

Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

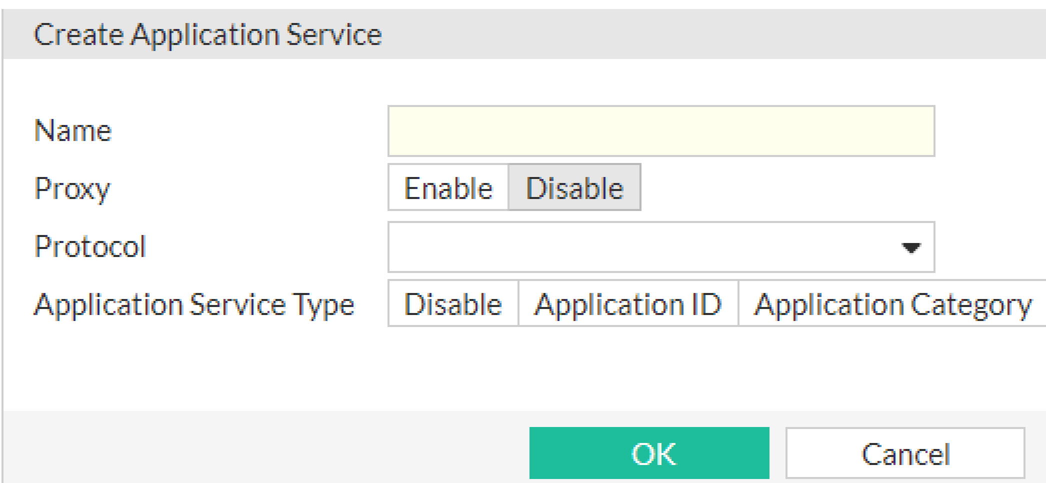
The following options are available:

Create New	Create an application service, service, service group, or category. See Create or edit an application service on page 218, Create or edit a service on page 219, Create or edit a service group on page 221, and Create a service category on page 224.
Edit	Edit the selected service.
Clone	Make a copy of the selected service.
Delete	Remove the selected custom service. This icon appears only if a service is not currently being used in a web cache policy.

Category Settings	Edit the order in which the categories are displayed in the list when viewing the list by category.
Search	Search for text in any column.
Service Name	The name of the custom service.
Details	Destination port or ports.
IP/FQDN	The IP address or FQDN of the service.
Show in Service List	Whether or not the service is shown in the service list.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in *Ref.*, and the *Object Usage* window appears displaying the various locations of the referenced object.
Comments	Optional description of the service.
Protocol	The protocol type for the service.
Type	The type of service, such as *Firewall*, *Explicit Proxy*, or *Firewall Group*.

Create or edit an application service

Select *Create New* > *Application Service* to open the *Create Application Service* window.



To open the *Edit Application Service* window, select an application service and then click *Edit*.

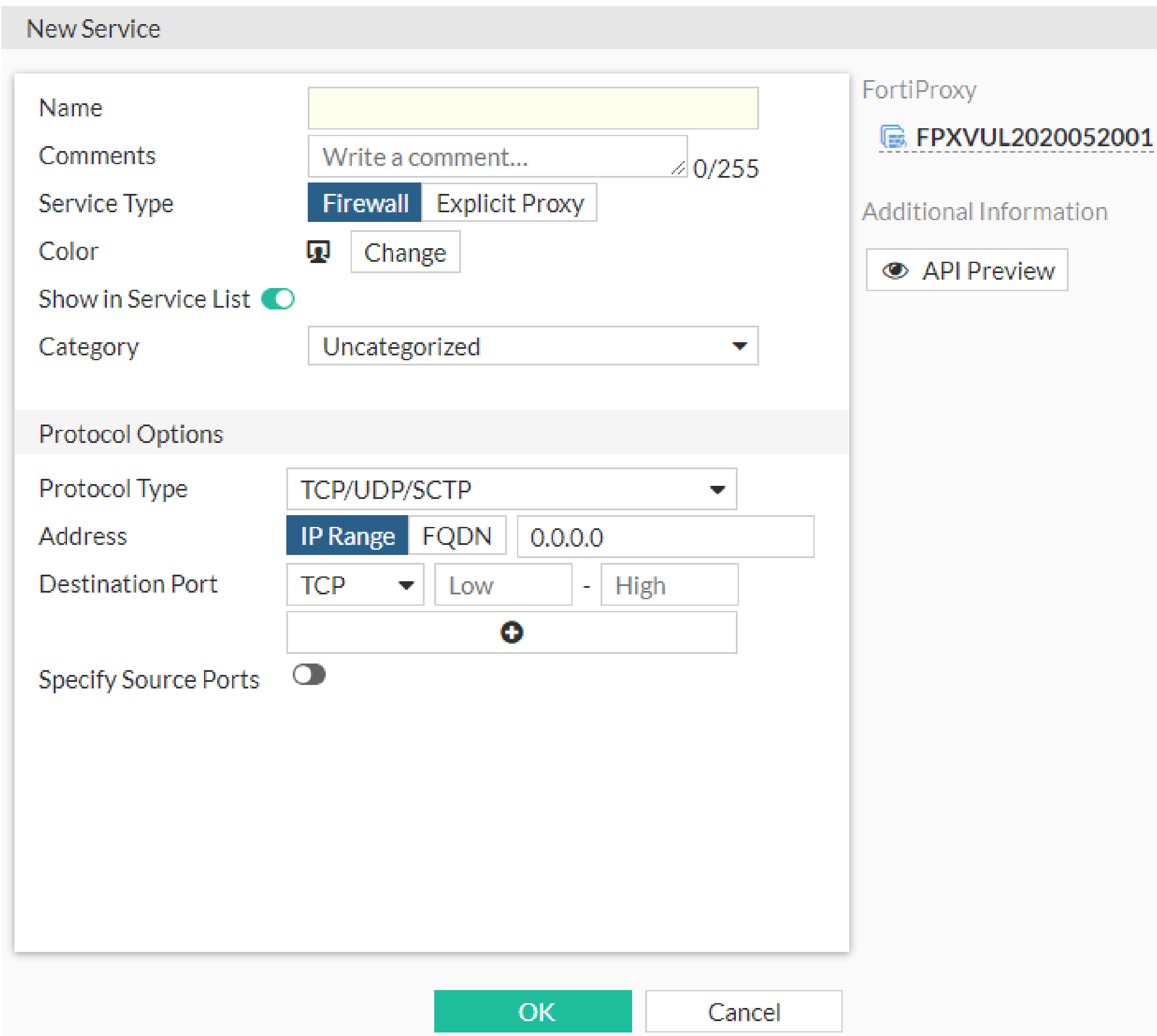
Configure the following settings in the *Create Application Service* window or *Edit Application Service* window and then click *OK*:

Name	Enter a name for the application service.
Proxy	Enable or disable the new application service.
Protocol	Select the protocol that the application service will use.

Application Service Type	Select *Disable*, *Application ID*, or *Application Category*.
Application ID	If you selected *Application ID*, click + to open the *Select Entries* window. Select one or more entries and then select *Close*.
Application category	If you selected an *Application Service Type* of *Application category*, click + to open the *Select Entries* window. Select one or more entries and then select *Close*.
TCP Port Range	If you selected *TCP/UDP/SCTP* or *ALL*, enter a range of TCP ports.

Create or edit a service

Select *Create New* > *Service* to open the *New Service* window.



To open the Edit Service window, select a service and then click *Edit.*

Configure the following settings in the *New Service* window or *Edit Service* window and then click *OK*:

Name	Enter a name for the custom service.
Comments	Optionally, enter a description of the service.
Service Type	Select the service type: *Firewall* or *Explicit Proxy*.
Color	Select *Change* to choose a color for the icon.
Show in Service List	Enable to show the service in the service list.
Category	Select the category for the service: *Uncategorized*; *Application*; *General*; *Web Access*; *File Access*; *Email*; *Network Services*; *Authentication*; *Remote Access*; *Tunneling*, *VoIP, Messaging & Other Applications*; or *Web Proxy*. You can create new service categories. See Create a service category on page 224.
Protocol Type	Select the type of protocol for the service. • If *Service Type* is *Firewall*, select one of: *TCP/UDP/SCTP*, *ICMP*, *ICMP6*, or *IP*. • If *Service Type* is *Explicit Proxy*, select one of: *ALL*, *CONNECT*, *FTP*, *HTTP*, *SOCKS_TCP*, or *SOCKS_UDP*.
Address	Select *IP Range* or *FQDN* and then enter the range of IP addresses or the FQDN for the service. Separate IP addresses with a hyphen.
Destination Port	Select *TCP*, *UDP*, or *SCTP* and then enter a range of port numbers.
Specify Source Ports	Enable and then enter a range of port numbers.
Type	Enter the ICMP type number for the ICMP protocol configuration. This option is only available if *Protocol Type* is set to *ICMP* or *ICMP6*.
Code	Enter the ICMP code number for the ICMP protocol configuration. This option is only available if *Protocol Type* is set to *ICMP* or *ICMP6*.
Protocol Number	Enter the protocol number for the IP protocol configuration. This option is only available if *Protocol Type* is set to *IP*.
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.

Create or edit a service group

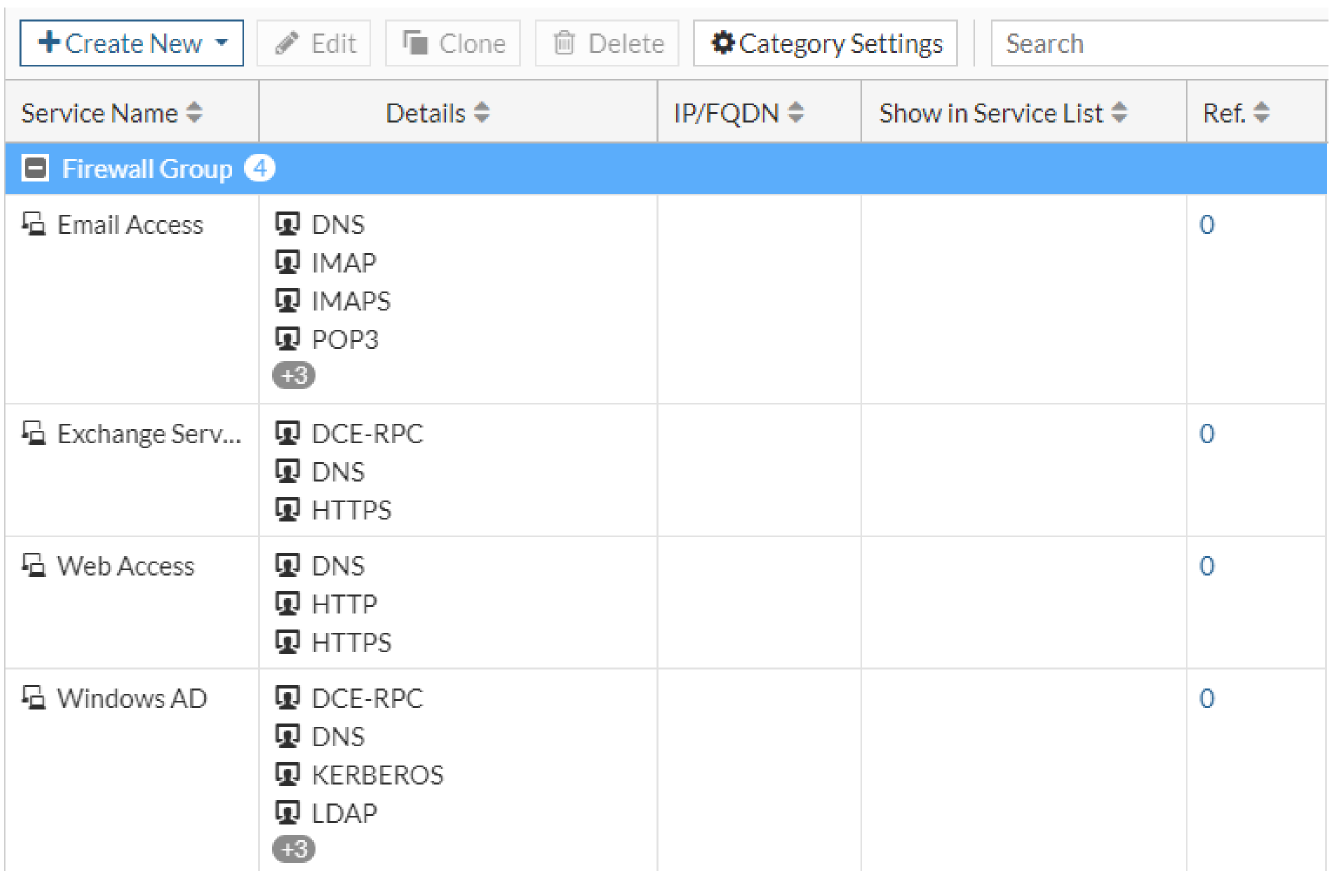
You can organize multiple services into a service group to simplify your policy list. For example, instead of having five identical policies for five different but related services, you can combine the five services into a single service group that is used by a single policy.

Service groups cannot contain other service groups.

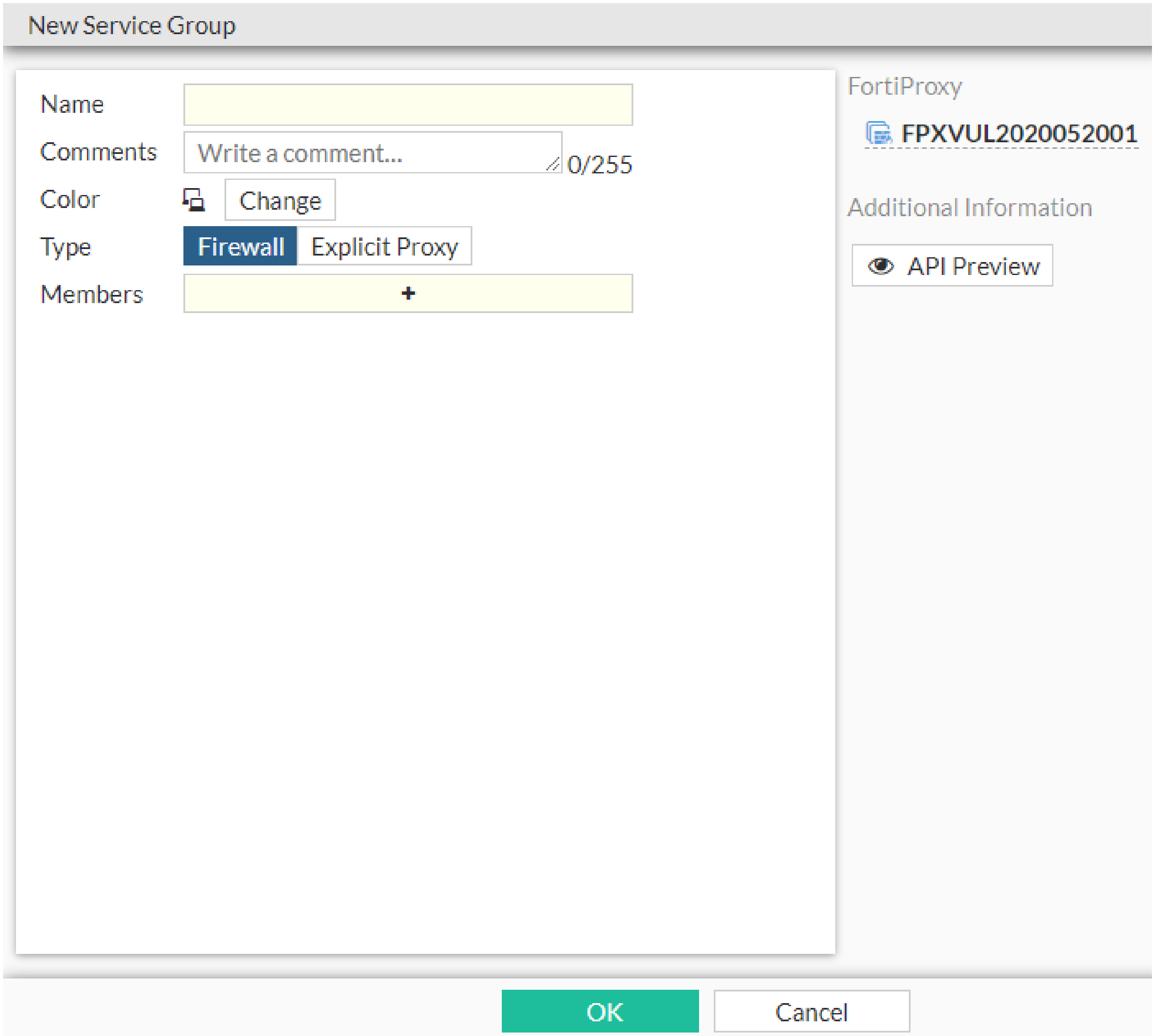
Configure a service group using the following CLI commands:

```
config firewall service group
   edit <name>
      set member              // Address group member.
      set explicit-proxy      // Enable or disable the explicit web proxy service group.
      set comment             // Comment.
      set color               // GUI icon color.
   next
end
```

Service groups are listed in the Firewall Group category.



Select *Create New > Service Group* to open the *New Service Group* window.



To open the *Edit Service Group* window, select a firewall group and then click *Edit*.

Configure the following settings in the *New Service Group* window or the *Edit Service Group* window and then click *OK*:

Name	Enter a name for the service group.
Comments	Optionally, enter a description of the service group.
Color	Select *Change* to choose a color for the icon.
Type	Select the type of service group, either *Firewall* or *Explicit Proxy*.
Members	Select the services to add to the service group.

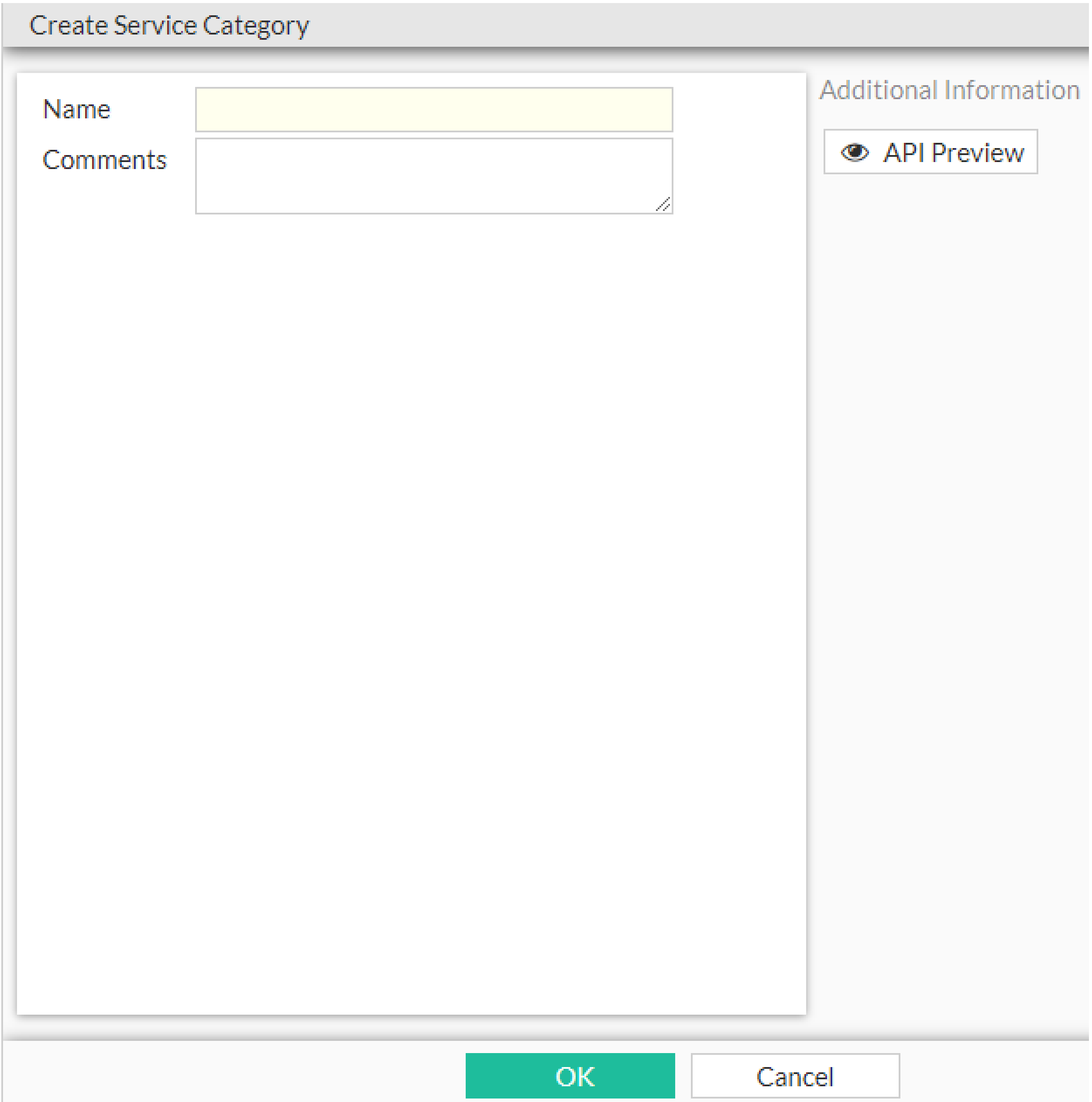
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

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.

Create a service category

1. Go to *Policy & Objects* > *Services* and select *Create New* > *Category*.



2. Enter a name for the new category in the *Name* field.
3. Optionally, enter a description of the category in the *Comments* field.
4. Click *OK* to create the new service category.

Schedules

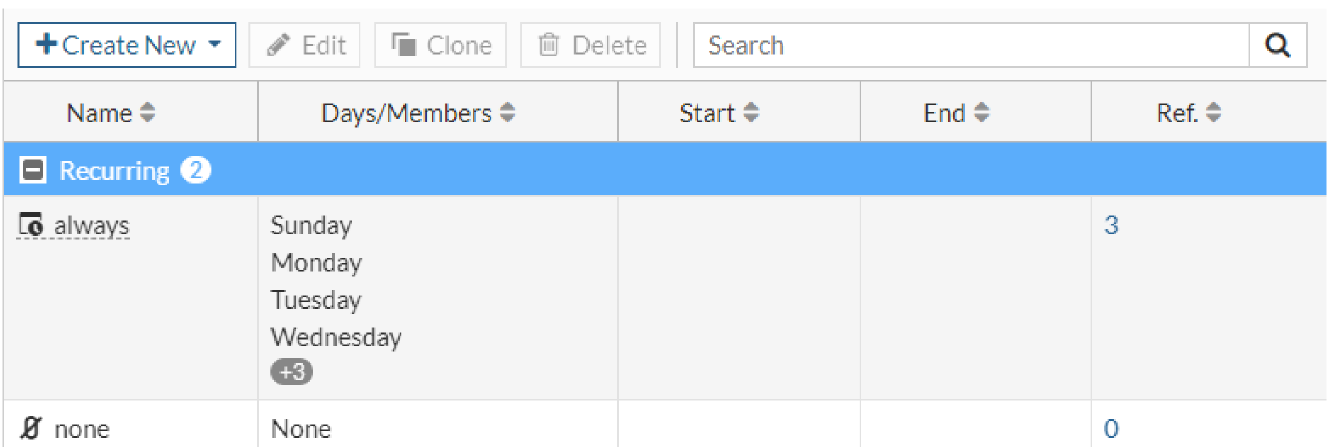
When you add security policies on a FortiProxy unit, those policies are always on, policing the traffic through the device. Schedules control when policies are in effect.

The schedule list lists all of the schedules. Recurring and one-time schedules can be created, edited, and deleted as needed.

You can create a recurring schedule that activates a policy during a specified period of time. If a recurring schedule has a stop time that is earlier than the start time, the schedule will take effect at the start time but end at the stop time on the next day. You can use this technique to create recurring schedules that run from one day to the next. To create a recurring schedule that runs for 24 hours, set the start and stop times to 00.

You can create one-time schedules, which are schedules that are in effect only once for the period of time specified in the schedule.

To manage schedules, go to *Policy & Objects > Schedules*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

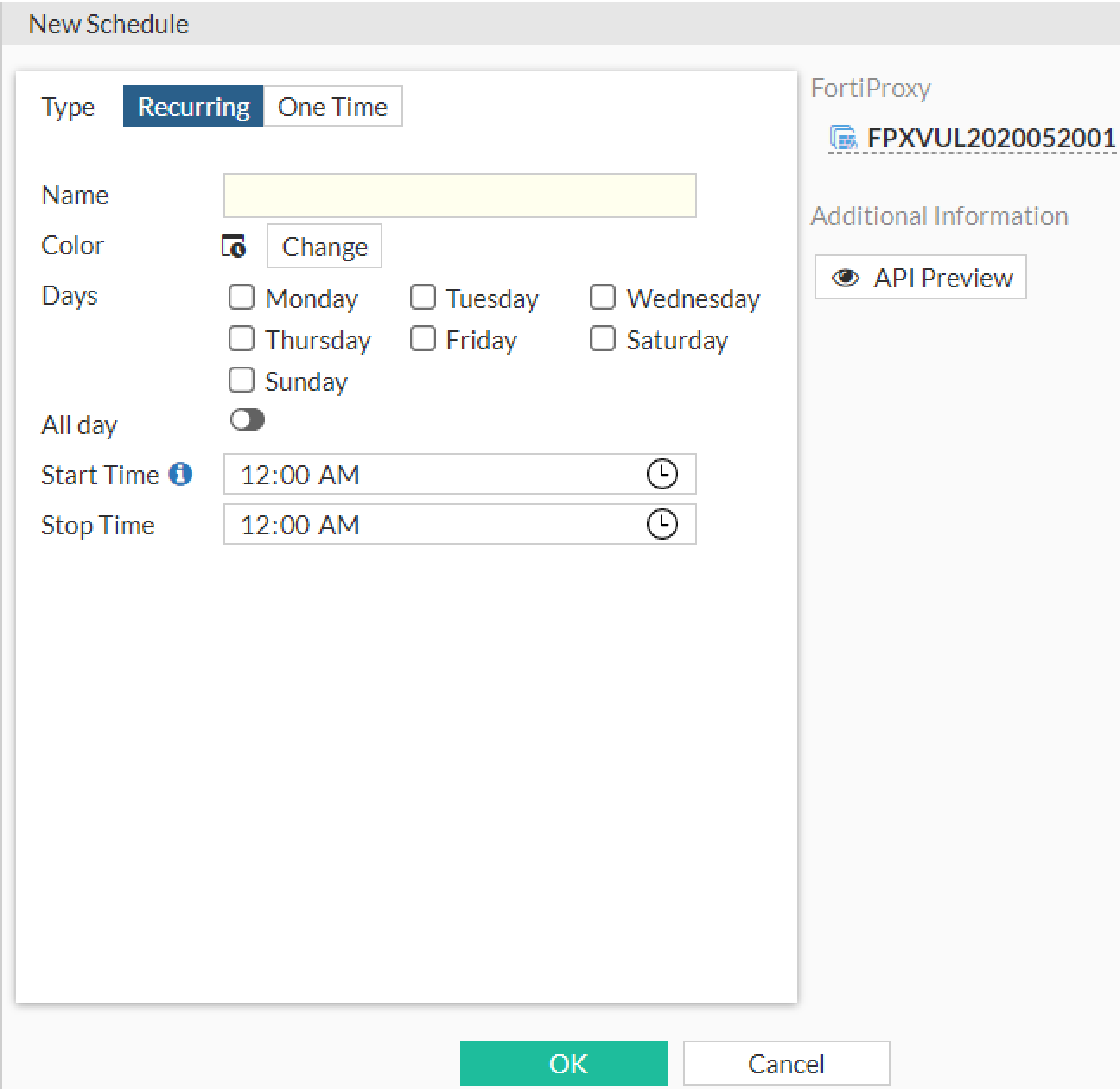
Create New	Create a schedule or a schedule group. See Create or edit a schedule on page 226 or Create or edit a schedule group on page 228.
Edit	Edit the selected schedule or schedule group. See Create or edit a schedule on page 226 or Create or edit a schedule group on page 228.
Clone	Make a copy of the selected schedule or schedule group.
Delete	Remove the selected schedule. This icon is only available if the selected schedule is not currently being used in a policy.
Search	Enter a search term to search the schedule list.
Name	The name of the schedule.
Days/Members	The days of the week that the schedule is configured to be active.

Start	The time of day that the schedule is configured to start.
End	The time of day that the schedule is configured to end.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in *Ref.*, and the *Object Usage* window appears displaying the various locations of the referenced object.
Type	The type of schedule, either *Recurring* or *One-Time*.

Create or edit a schedule

When you add security policies on a FortiProxy unit, those policies are always on, policing the traffic through the device. Schedules control when policies are in effect.

Select *Create New* > *Schedule*to open the *New Schedule* window.



To open the *Edit Schedule* window, select a schedule and then click *Edit.*

Configure the following settings in the *New Schedule* window or the *Edit Schedule* window and then click *OK*:

Type	Select *Recurring* or *One- Time*.
Name	Enter a name for the schedule.
Color	Click *Change* to choose a color for the icon.
Days	If you selected a recurring schedule, select the days of the week when the schedule will be active.

All Day	If you selected a recurring schedule and the scheduled time is the whole day, enable *All Day*. If the schedule is for specific times during the day, disable *All Day*.
Start Date	If you select a one-time schedule, select the year, month, and day that the schedule will start. The start date must be earlier than the stop date.
Start Time	If you select a recurring schedule and disable *All Day* of if you select a one-time schedule, select the start time for the schedule.
End Date	If you select a one-time schedule, select the year, month, and day that the schedule will stop. The end date must be later than the start date.
Stop Time	If you select a recurring schedule and disable *All Day* of if you select a one-time schedule, select the stop time for the schedule. If the stop time is set earlier than the start time, the stop time will be during the next day. If the start time is equal to the stop time, the schedule will run for 24 hours.
Pre-expiration event log	If you select a one-time schedule, enable this option to generate an event log before the schedule expires and then enter the number of days before the expiration that the event log will be generated, from 1 to 100.
Number of days before	If you select a one-time schedule, enter the number of days before the schedule expires to generate an event log. The range is 1-100 days).
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:

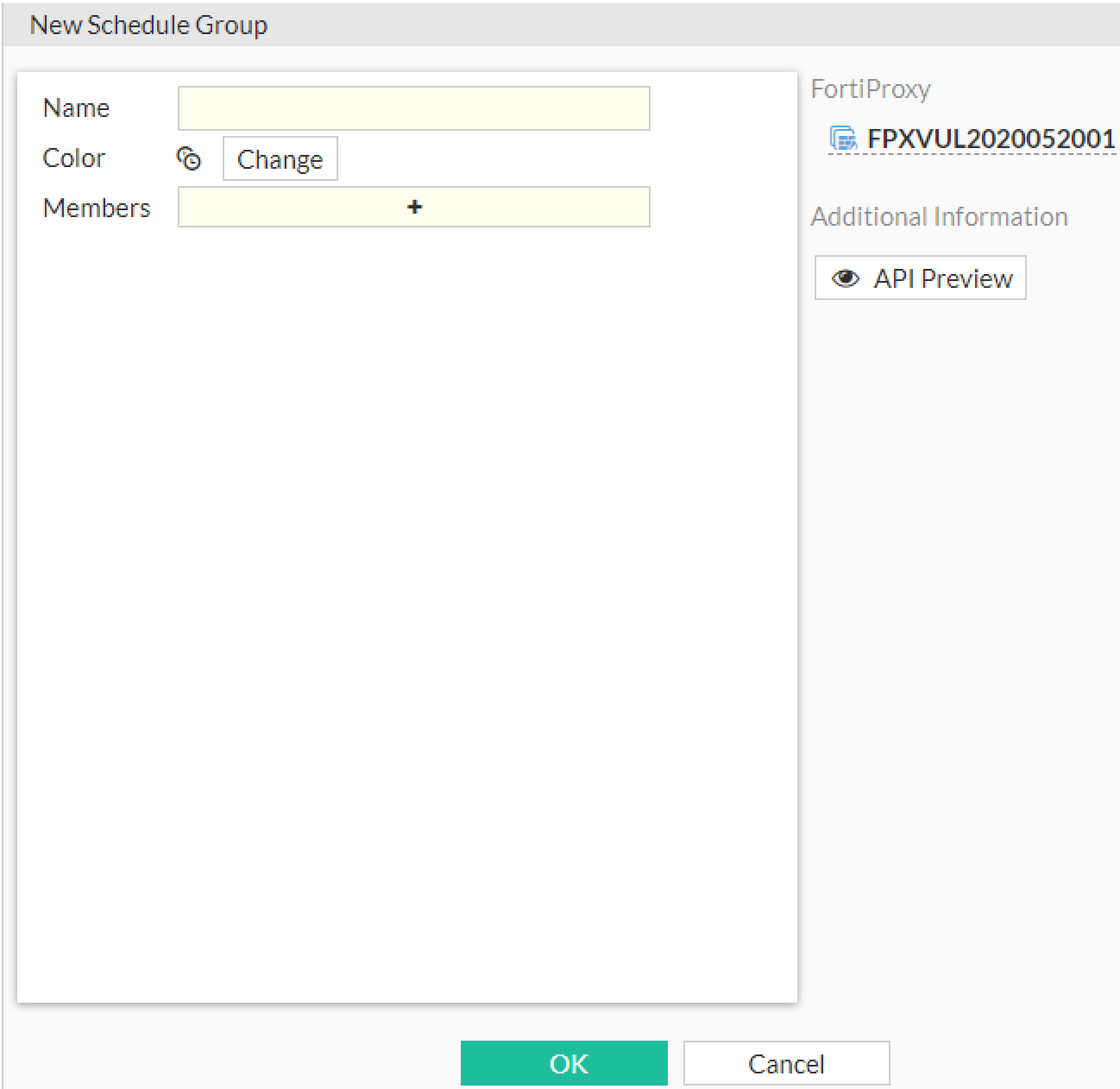
1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to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

Create or edit a schedule group

You can organize multiple schedules into a schedule group to simplify your security policy list. For example, instead of having five identical policies for five different but related schedules, you might combine the five schedules into a single schedule group that is used by a single security policy.

Schedule groups can contain both recurring and one-time schedules. Schedule groups cannot contain other schedule groups.

Select *Create New > Schedule Group*to open the *New Schedule Group* window.



To open the *Edit Schedule Group* window, select a schedule group and then click *Edit.*

Configure the following settings in the *New Schedule Group* window or the *Edit Schedule Group* window and then click *OK*:

Name	Enter the name of the schedule group.
Color	Click *Change* to choose a color for the icon.
Members	Select the schedules that you want to have included in the group from the drop-down menu.

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:

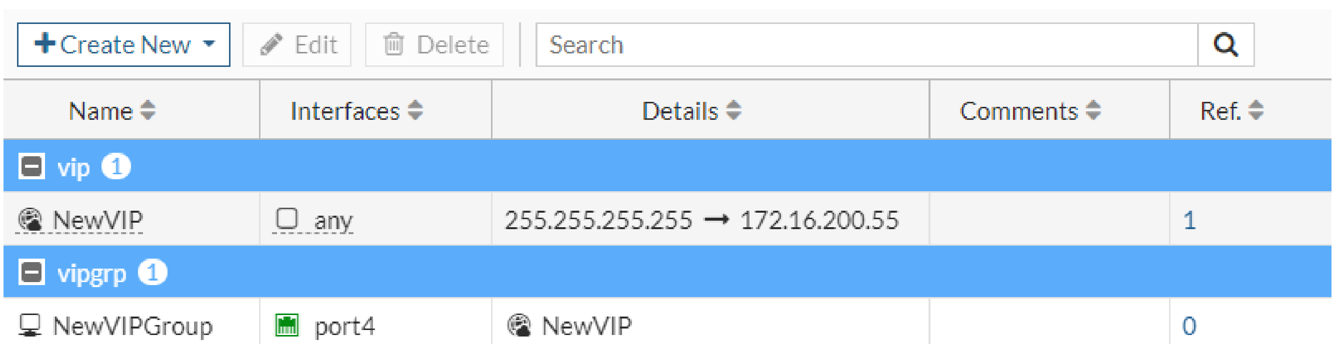
1. Click *API Preview*. The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to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

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 view the virtual IPs, go to *Policy & Objects* > *Virtual IPs*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

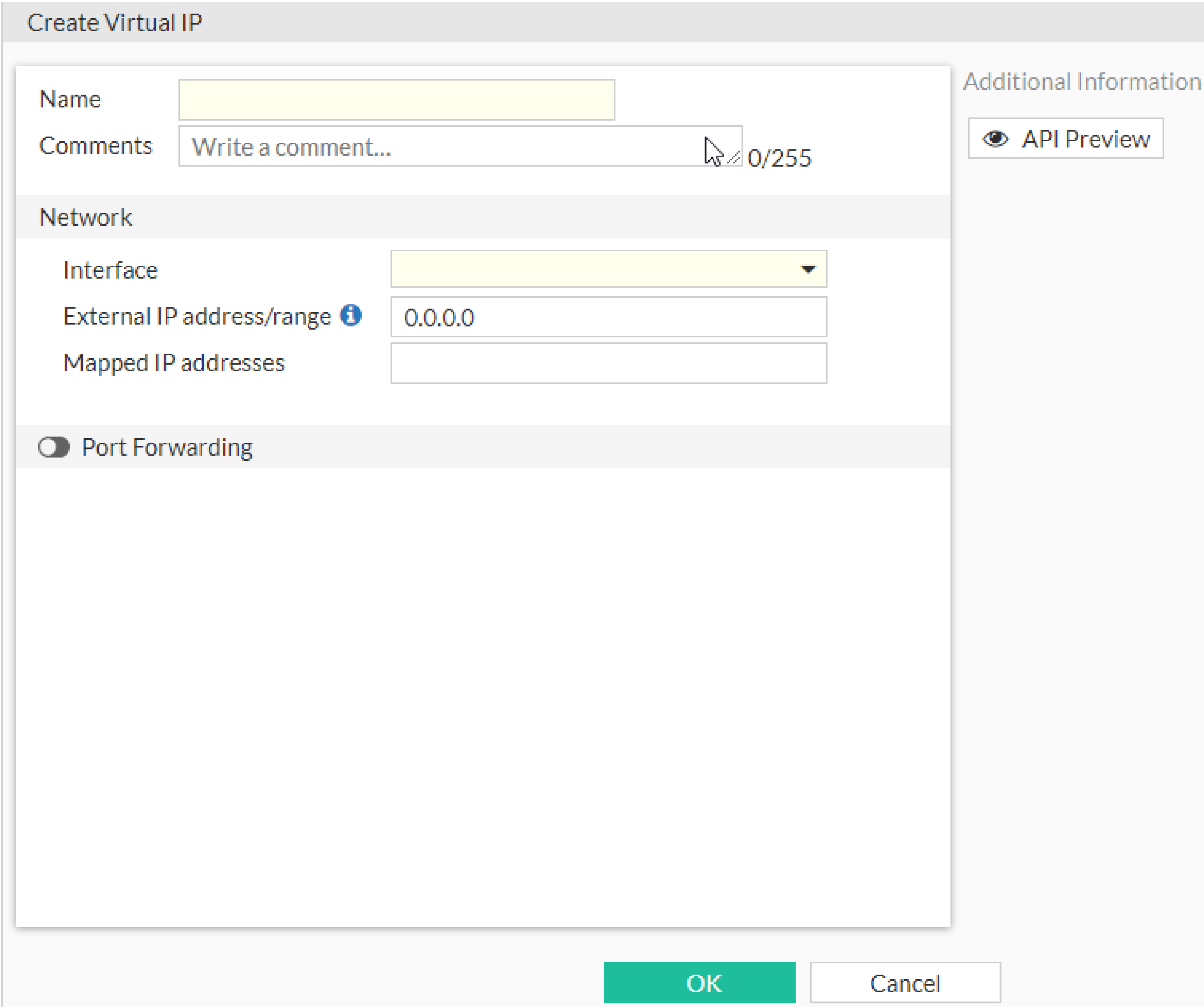
The following options are available:

Create New > Virtual IP	Add a new virtual IP. See Create or edit a virtual IP on page 231.
Create New > Virtual IP Group	Add a new virtual IP group. See Create or edit a virtual IP group on page 233.
Edit	Edit the selected virtual IP or virtual IP group. See Create or edit a virtual IP on page 231 or Create or edit a virtual IP group on page 233
Delete	Remove the selected virtual IP or virtual IP group.

Search	Search for text in any column.
Name	The name of the virtual IP or virtual IP group.
Interfaces	The domain name.
Details	The interface to which the virtual IP or virtual IP group is bound.
Comments	Optional description of the virtual IP or virtual IP group.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in *Ref.*, and the *Object Usage* window appears displaying the various locations of the referenced object.
extip	External IP address or range for the virtual IP.

Create or edit a virtual IP

Select *Create New* > *Virtual IP* to open the *Create Virtual IP* window.



To open the *Edit Virtual IP* window, select an address and then click *Edit*.

Configure the following settings in the *Create Virtual IP* window or the *Edit Virtual IP* window and then click *OK*:

Name	Enter a unique name for the virtual IP.
Comments	Optionally, enter a description of the virtual IP.
Interface	Select the interface to which you want to bind the virtual IP. Select *any* if you want to bind the virtual IP with the interface when you create a policy.
Port Forwarding	Enable or disable. If only the traffic for a specific port or port range is being forwarded, enable this setting.
Protocol	Select *TCP*, *UDP*, *SCTP*, or *ICMP* for the virtual IP to use.
External service port	Enter a port number or a range of port numbers, separated by a hyphen. This is the port(s) on the external interface of the FortiProxy (the destination port in the header of the packets).

Map to port	Enter the port number. This will be the listening port on the device located on the internal side of the network. It does not have to be the same as the external service port.
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.

To create a virtual IP in the CLI:

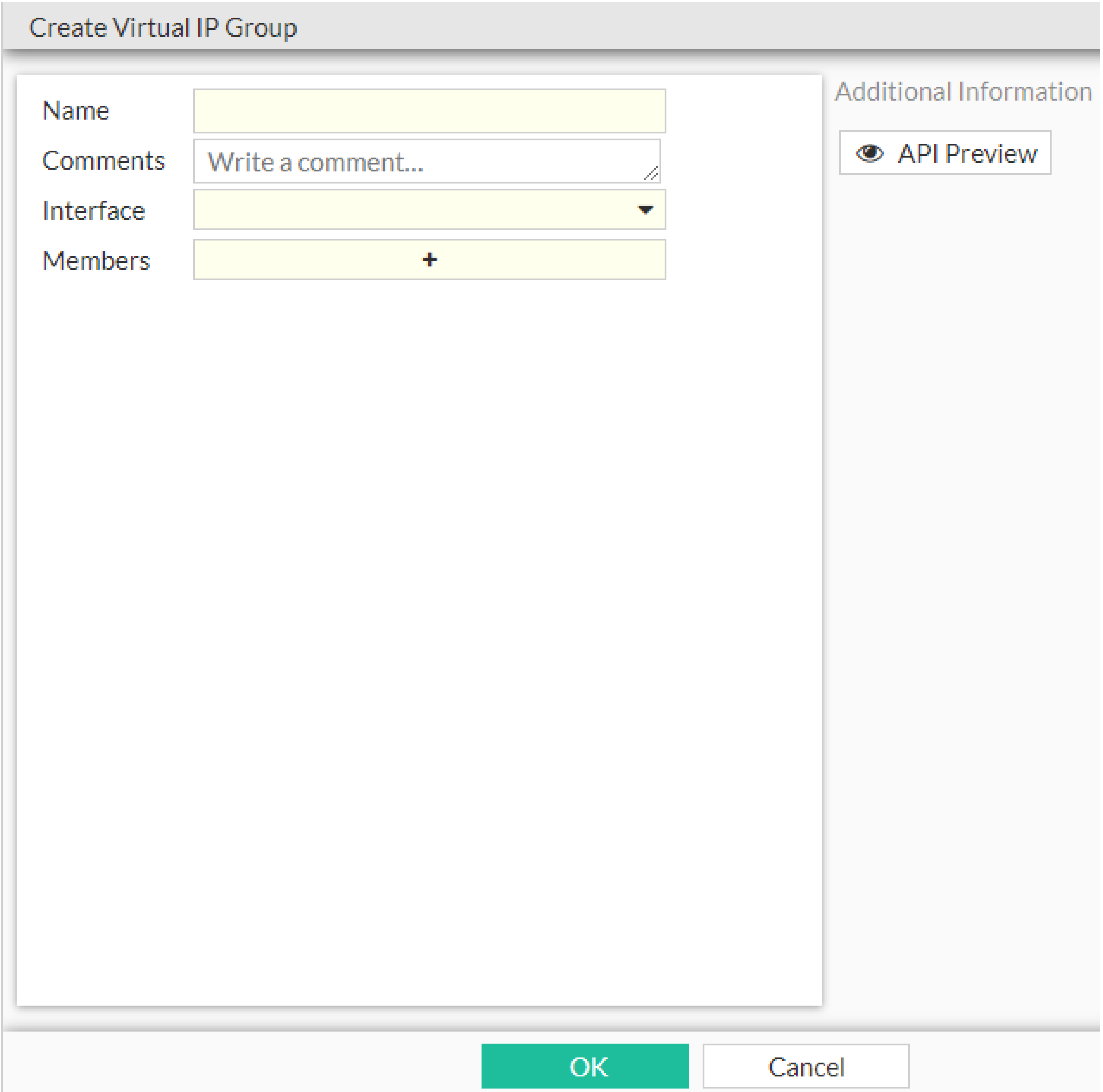
```
config firewall vip
   edit "Internal_WebServer"
      set extip 10.1.100.199
      set extintf "any"
      set mappedip "172.16.200.55"
   next
end
```

Create or edit a virtual IP group

Just like other address, Virtual IP addresses can be organized into groups for ease of administration. If you have multiple virtual IPs that are likely to be associated to common firewall policies rather than add them individually to each of the policies you can add the instead. That way, if the members of the group change then any changes made to the group will propagate to all of the policies using that group.

When using a Virtual IP address group the firewall policy will take into account all of the configured parameters of the Virtual IPs: IP addresses, ports, and port types.

Select *Create New* > *Virtual IP Group* to open the *Create Virtual IP Group* window.



To open the *Edit Virtual IP Group* window, select an address group and then click *Edit*.

Configure the following settings in the *Create Virtual IP Group* window or the *Edit Virtual IP Group* window and then click *OK*:

Name	Enter a unique name to identify the virtual IP group.
Comments	Optionally, enter a description of the virtual IP group.
Interface	Use the drop-down menu to select the interface if all of the VIPs are on the same interface. If any of the VIPS are on different interfaces or if any of them are associated with the "any" option, choose the any option for the group.

Members	Select the virtual IPs to add to the virtual IP group.
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.

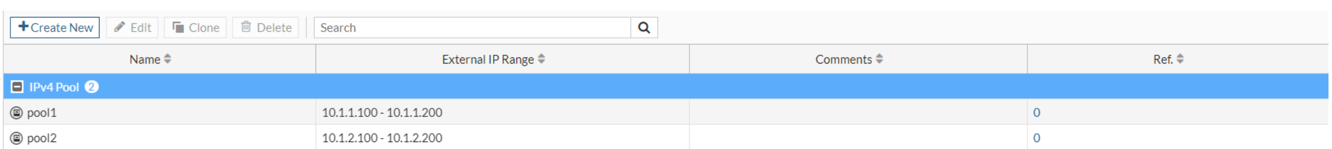
To use the API Preview:

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.

IP Pools

IP pools are a mechanism that allow sessions leaving the FortiProxy unit to use NAT. An IP pool defines a single IP address or a range of IP addresses to be used as the source address for the duration of a session. These assigned addresses are used instead of the IP address assigned to that FortiProxy interface.

To see which IP pools are configured, go to *Policy & Objects > IP Pools*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

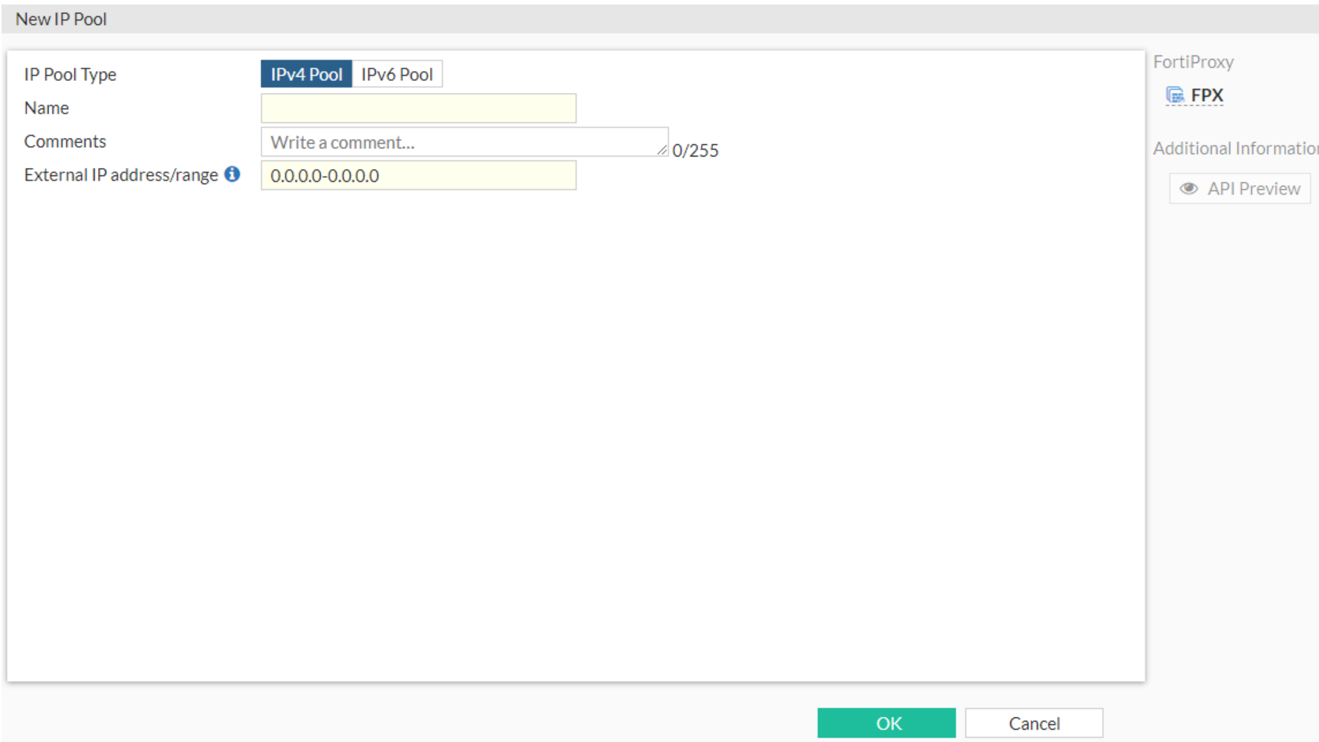
The following options are available:

Create New	Create an IP pool. See Create or edit an IP pool on page 236.
Edit	Edit the selected IP pool. See Create or edit an IP pool on page 236.
Clone	Make a copy of the selected IP pool.
Delete	Remove the selected IP pool.
Search	Enter a search term to search the IP pool list.
Name	The name of the IP pool.
External IP Range	The lowest and highest IP addresses in the range.
Comments	An optional description of the IP pool.
Ref.	Displays the number of times the object is referenced to other objects.

	To view the location of the referenced object, select the number in *Ref.*, and the *Object Usage* window appears displaying the various locations of the referenced object.

Create or edit an IP pool

Select *Create New* to open the *New IP Pool* window.



To open the *Edit IP Pool* window, select an IP pool and then click *Edit*.

Configure the following settings in the *New IP Pool* window or *Edit IP Pool* window and then click *OK*:

To create an IP pool:

IP Pool Type	Select *IPv4 Pool* if your IP pool contains IPv4 addresses or select *IPv6 Pool* if your IP pool contains IPv6 addresses.
Name	Enter a name for the IP pool in the *Name* field.
Comments	Add an optional description of the IP pool.
External IP address/range	Enter the lowest and highest IP addresses in the range. Separate IP addresses with a hyphen. If you only want a single address used, enter the same address in both fields.
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.

ZTNA

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.

Full ZTNA and IP/MAC filtering

ZTNA has two modes: Full ZTNA and IP/MAC filtering:

- Full ZTNA allows users to securely access resources through a SSL encrypted access proxy. This simplifies remote access by eliminating the use of VPNs.
- IP/MAC filtering uses ZTNA tags to provide an additional factor for identification and security posture check to implement role-based zero trust access.

ZTNA telemetry, tags, and policy enforcement

When On-net and Off-net FortiClient endpoints register to FortiClient EMS, device information, log on user information, and security posture are all shared over ZTNA telemetry with the EMS server. Clients also make a certificate signing request to obtain a client certificate from the EMS that is acting as the ZTNA Certificate Authority (CA).

Based on the client information, EMS applies matching Zero Trust tagging rules to tag the clients. These tags, and the client certificate information, are synchronized with the FortiProxy unit in real-time. This allows the FortiProxy unit to verify the client's identity using the client certificate, and grant access based on the ZTNA tags applied in the ZTNA rule.

EMS ZTNA and endpoint tags are displayed in the *Device Inventory* widget, *FortiClient* widget, and the *Asset Identity Center* page. In the backend, EMS ZTNA tags, endpoint tags, and EMS serial numbers are in the user device query API and response.

The ZTNA tag name can be used as a search criterion in the *Asset* view of the *Asset Identity Center* page.

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 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

For configuration details, see Basic ZTNA configuration on page 238.

Basic ZTNA configuration

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

1. Configure a FortiClient EMS connector on page 239
2. Configure a ZTNA server on page 241
3. Configure a ZTNA rule on page 245
4. Configure a firewall policy for full ZTNA on page 247
5. Optional authentication on page 249

To configure ZTNA in the GUI, go to *System* > *Feature Visibility* and enable *Zero Trust Network Access*.

Configure a FortiClient EMS connector

To add an on-premise FortiClient EMS server in the GUI:

1. Go to *Security Fabric* > *Fabric Connectors*.
2. Click *Create New* and click *FortiClient EMS*.
3. Enter a name for the connector and the IP address or FQDN of the EMS.
4. Click *OK*.
5. A window appears to verify the EMS server certificate. Click *Accept*.

To add an on-premise FortiClient EMS server in the CLI:

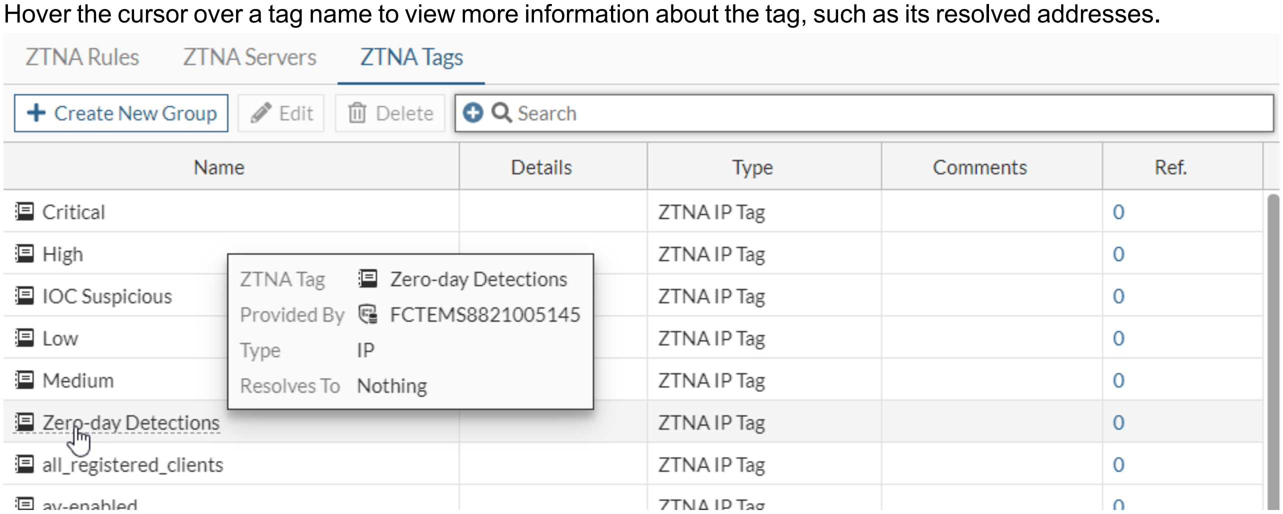
```
config endpoint-control fctems
    edit <name>
        set server <server IP or domain>
    next
end
```

ZTNA tags

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

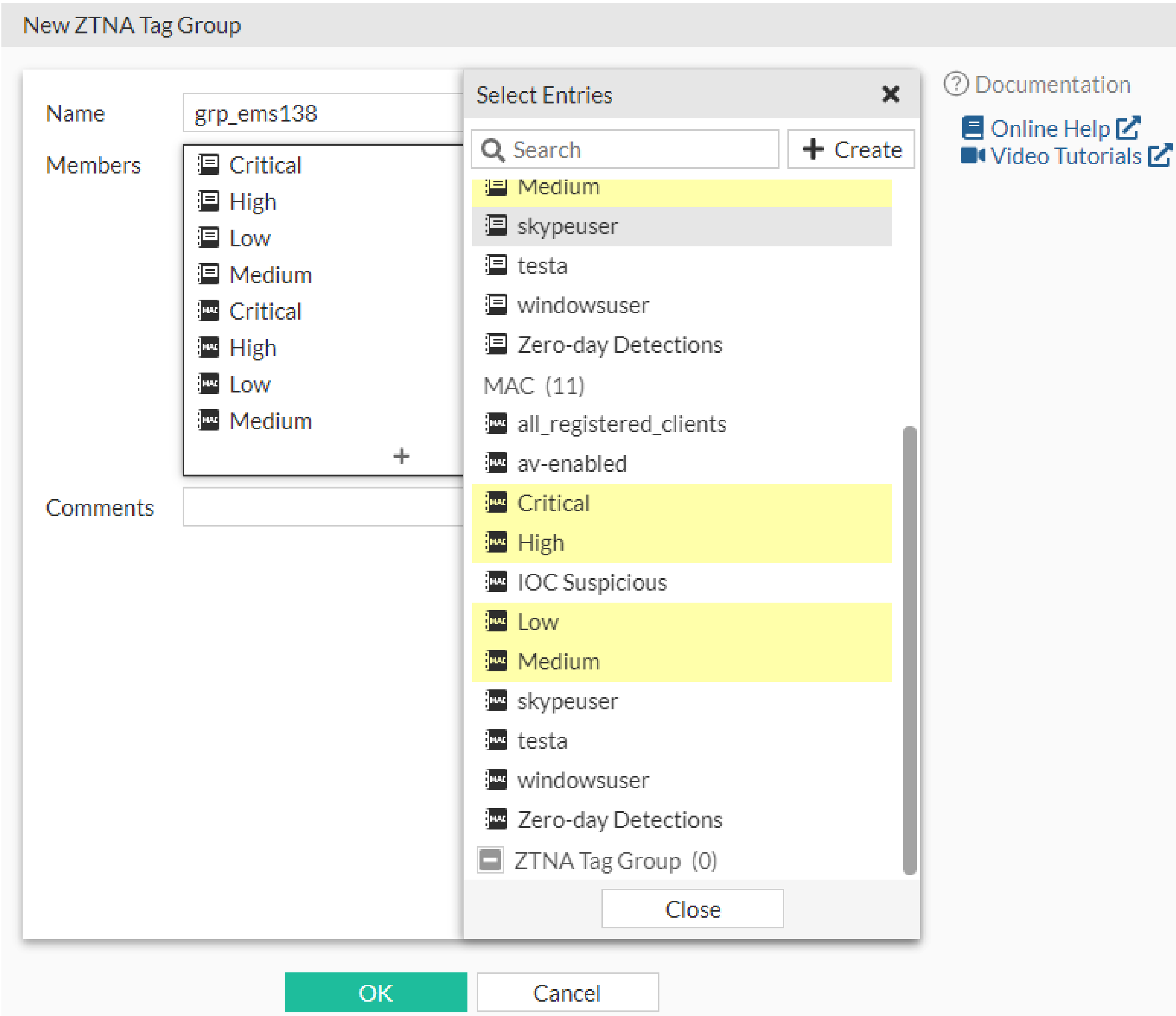
To view the synchronized ZTNA tags in the GUI:

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*.

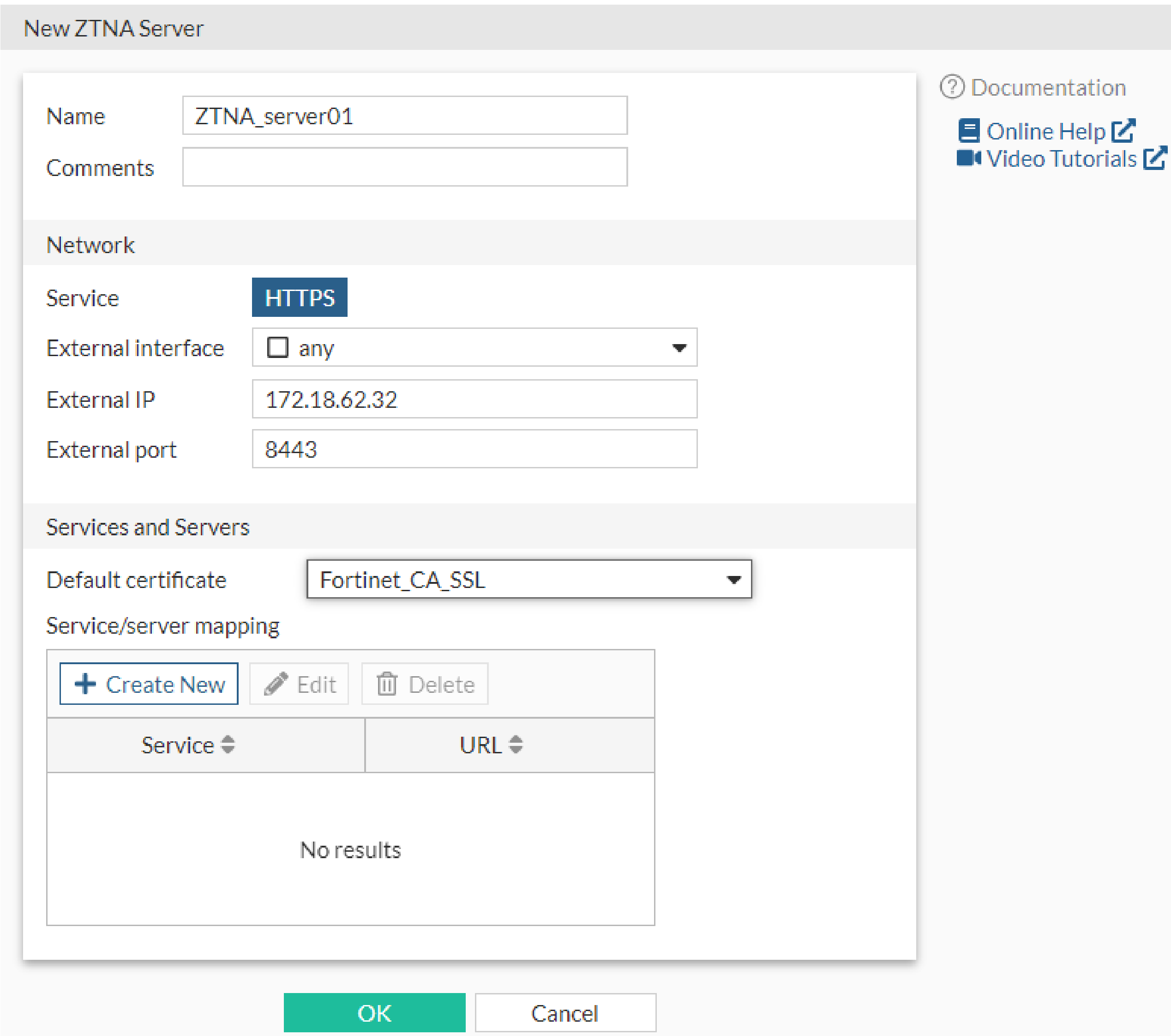
To create a ZTNA tag group in the CLI:

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

Configure a ZTNA server

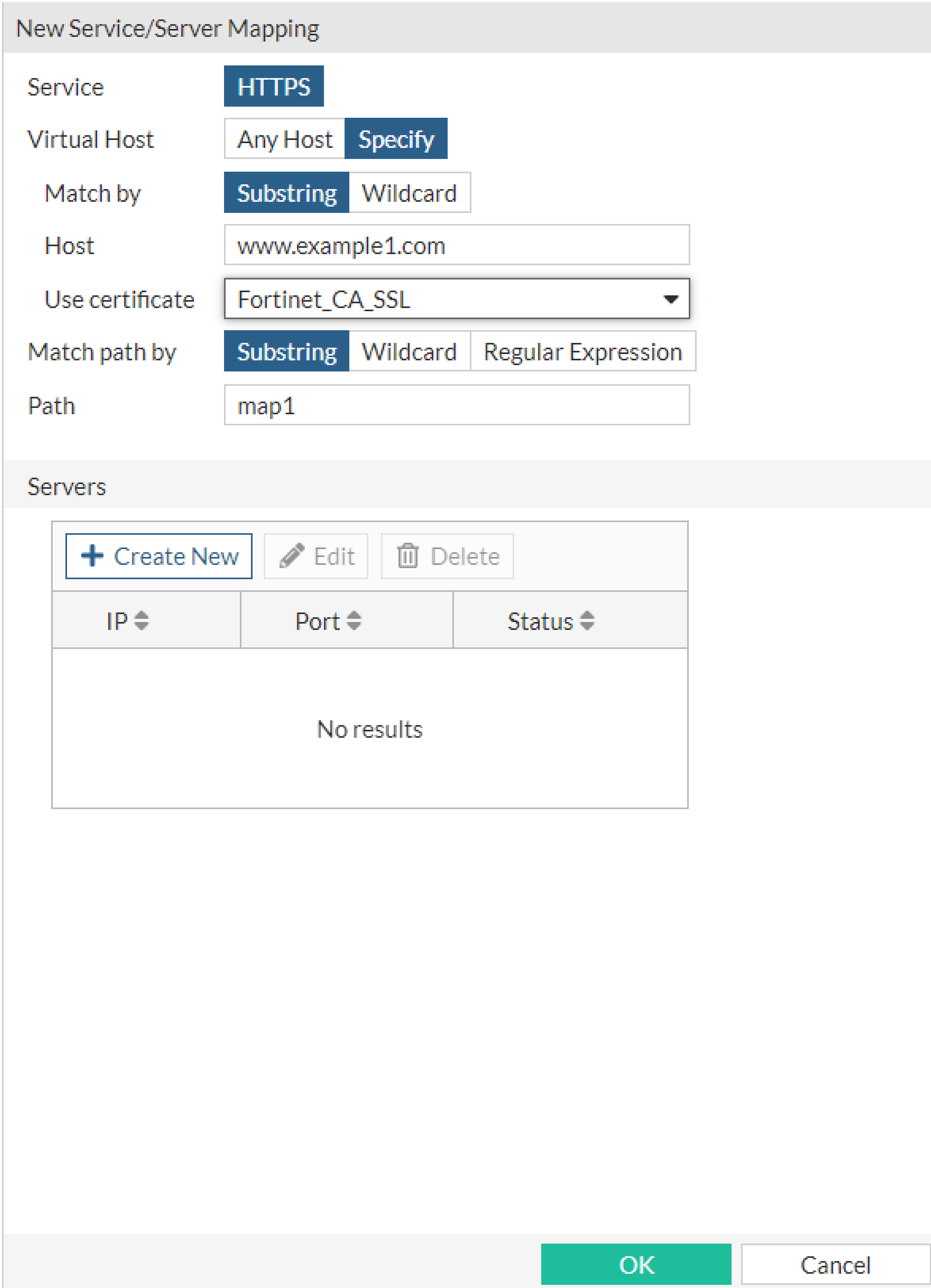
To configure a ZTNA server, define the access proxy VIP and the real servers that clients will connect to. The access proxy VIP is the FortiProxy ZTNA gateway that clients make HTTPS connections to. The service/server mappings define the virtual host matching rules and the real server mappings of the HTTPS requests.

To create a ZTNA server and access proxy VIP in the GUI:

1. Go to *Policy & Objects > ZTNA* and select the *ZTNA Servers* tab.
2. Click *Create New*.
3. Enter a name for the server.
4. Select an external interface, enter the external IP address, and select the external port that the clients will connect to.
5. Select the *Default certificate*. Clients will be presented with this certificate when they connect to the access proxy VIP.


6. Add server mapping:

a. In the *Service/server mapping* table, click *Create New*.
b. Set *Virtual Host* to *Any Host* or *Specify*.
    - *Any Host*: Any request that resolves to the access proxy VIP will be mapped to your real servers. For example, if both www.example1.com and www.example2.com resolve to the VIP, then both requests are mapped to your real servers.
    - *Specify*: Enter the name or IP address of the host that the request must match. For example, if www.example1.com is entered as the host, then only requests to www.example1.com will match.
c. Configure the path as needed.
   The path can be matched by substring, wildcard, or regular expression. For example, if the virtual host is specified as www.example1.com, and the path substring is map1, then www.example1/map1 will be matched.


New Service/Server Mapping
Service
HTTPS
Virtual Host
Any Host
Specify
Match by
Substring
Wildcard
Host
www.example1.com
Use certificate
Fortinet_CA_SSL
Match path by
Substring
Wildcard
Regular Expression
Path
map1
Servers
Create New
Edit
Delete
IP
Port
Status
No results
OK
Cancel

   d. Add a server:
      i. In the *Servers* table, click *Create New*.
      ii. Enter the server IP address and port number.
      iii. Set the server status.
      iv. Click *OK*.
      v. Add more servers as needed.
   e. Click *OK*.
   f. Add more server mappings as needed.
7. Click *OK*.

To create a ZTNA server and access proxy VIP in the CLI:

1. Configure an access proxy VIP:

```
config firewall vip
    edit <name>
        set type access-proxy
        set extip <external_IP_address>
        set extintf <external interface>
        set server-type https
        set extport <external_port_number>
        set ssl-certificate <certificate>
    next
end
```

2. If the virtual host is specified, configure the virtual host:

```
config firewall access-proxy-virtual-host
    edit <auto generated when configured from GUI>
        set ssl-certificate <certificate>
        set host <host_name_or_IP_address>
        set host-type {sub-string | wildcard}
    next
end
```

3. Configure the server and path mapping:

```
config firewall access-proxy
    edit <name>
        set vip <virtual_IP_name>
        set client-cert {enable | disable}
        set empty-cert-action {accept | block}
        config api-gateway
            edit 1
                set url-map <mapped_path>
                set service {http | https | tcp-forwarding | samlsp}
                set virtual-host <name_of_virtual_host_if_specified>
                set url-map-type {sub-string | wildcard | regex}
                config realservers
                    edit 1
                        set ip <IP_address_of_real_server>
                        set port <port>
                        set status {active | standby | disable}
                        set health-check {enable | disable}
                    next
```

```
                end
                set ldb-method static
                set persistence none
                set ssl-dh-bits 2048
                set ssl-algorithm high
                set ssl-min-version tls-1.1
                set ssl-max-version tls-1.3
            next
        end
    next
end
```

The load balance method for the real servers can only be specified in the CLI.

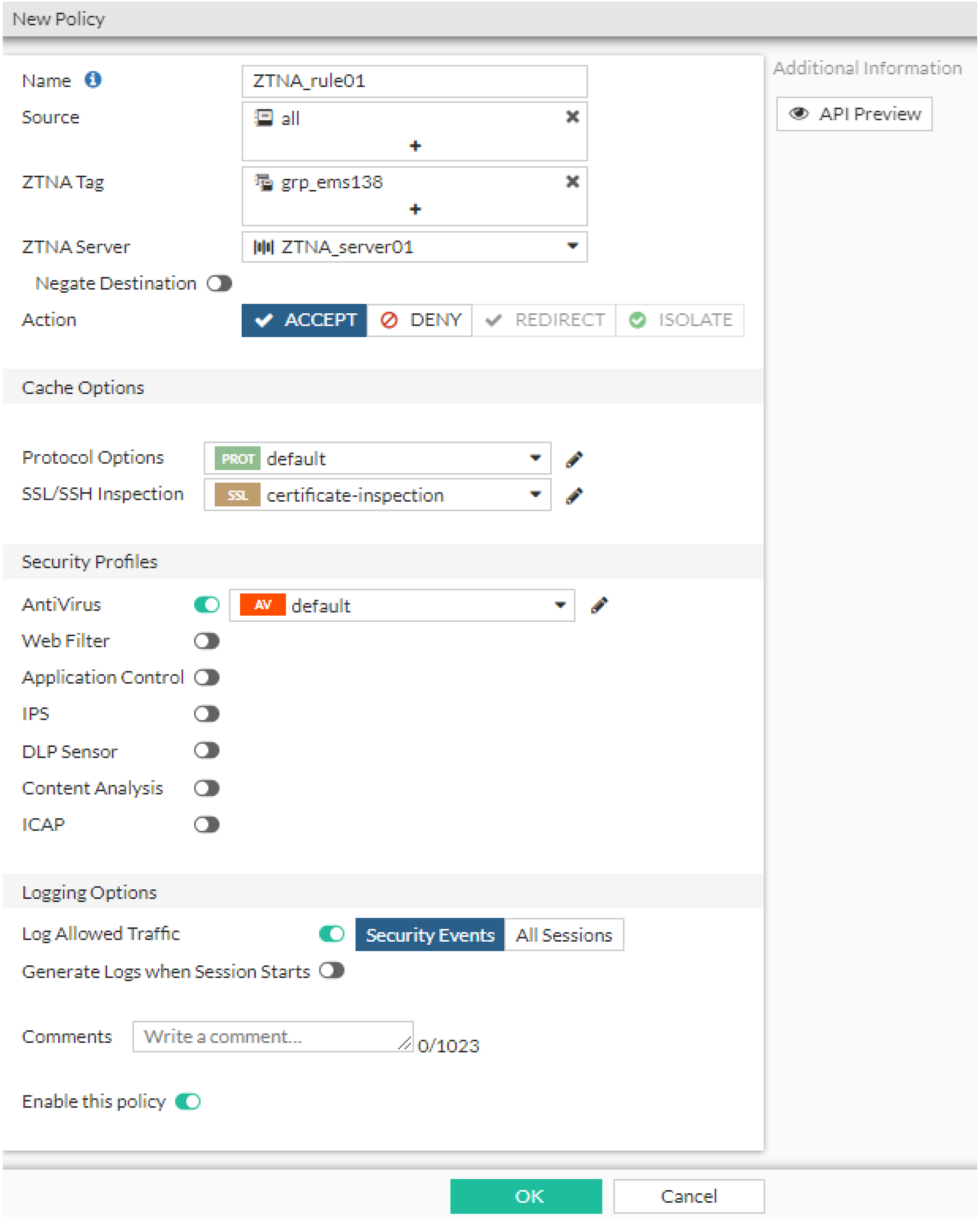
Configure a ZTNA rule

A ZTNA rule is a proxy policy used to enforce access control. ZTNA tags or tag groups can be defined to enforce zero trust role based access. Security profiles can be configured to protect this traffic.

To configure a ZTNA rule in the GUI:

1. Go to *Policy & Objects* > *ZTNA* and select the *ZTNA Rules* tab.
2. Click *Create New*.
3. Enter a name for the rule.
4. Add the ZTNA tags or tag groups that are allowed access.

5. Select the ZTNA server.



6. Configure the remaining options as needed.
7. Click *OK*.

To configure a ZTNA rule in the CLI:

```
config firewall policy
    edit 1
        set type access-proxy
        set name <ZTNA rule name>
        set access-proxy <access_proxy>
        set srcaddr "all"
        set dstaddr "all"
        set ztna-ems-tag <ZTNA_tag(s)>
        set action accept
        set schedule "always"
        set logtraffic all
        set utm-status enable
        set ssl-ssh-profile <inspection_profile>
    next
end
```

Configure a firewall policy for full ZTNA

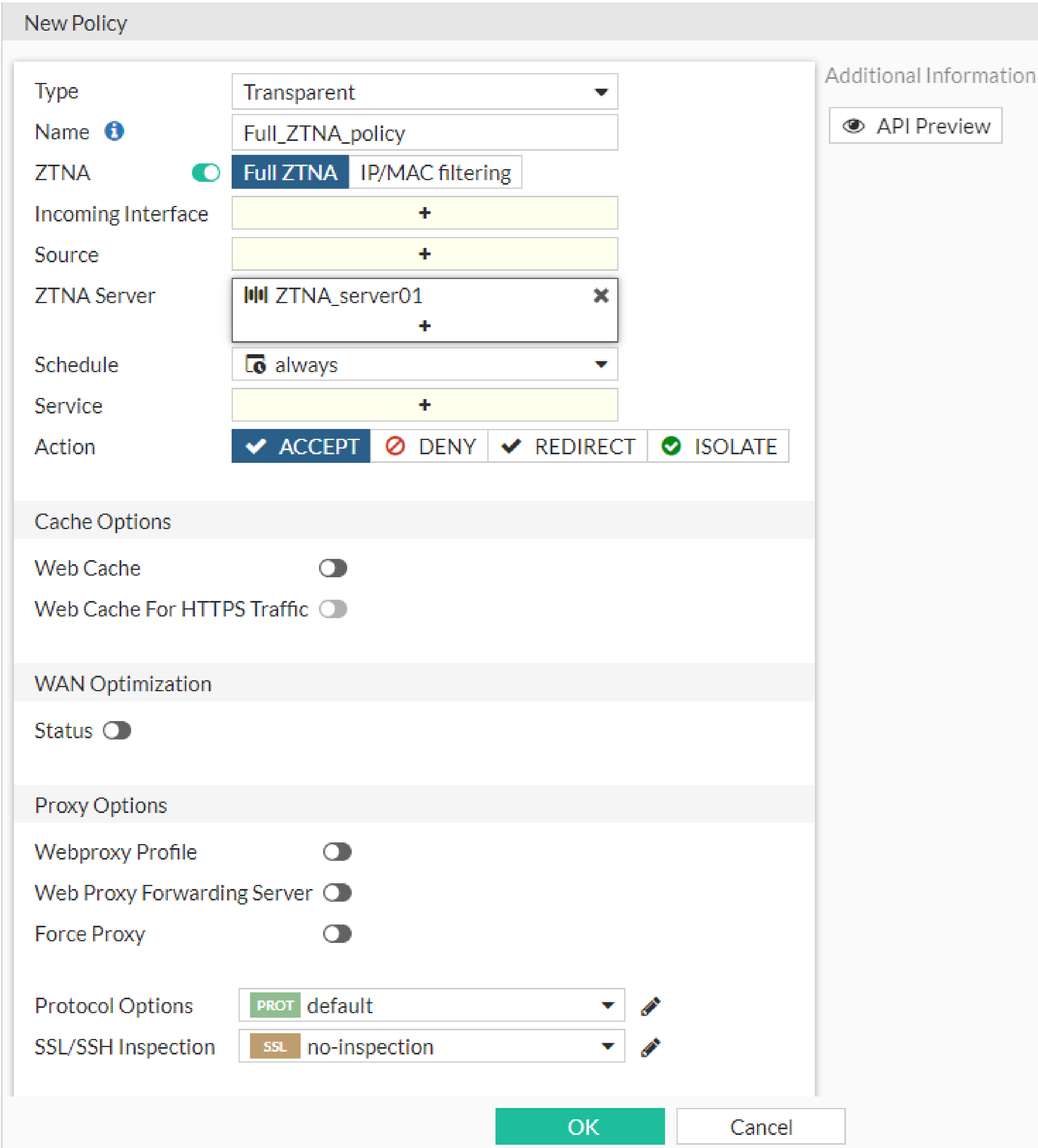
The firewall policy matches and redirects client requests to the access proxy VIP. The source interface and addresses that are allowed access to the VIP can be defined. By default, the destination is any interface, so once a policy is configured for full ZTNA, the policy list will be organized by sequence.

UTM processing of the traffic happens at the ZTNA rule.

To configure a firewall policy for full ZTNA in the GUI:

1. Go to *Policy & Objects* > *Policy* and click *Create New*.
2. Enter a name for the policy.
3. Enable *ZTNA* and select *Full ZTNA*.

4. Set *ZTNA Server* to the configured ZTNA server.



5. Configure the remaining settings as needed.
6. Click *OK*.

To configure a firewall policy for full ZTNA in the CLI:

```
config firewall policy
    edit <policy ID>
```

```
        set name <policy_name>
         set srcintf <source_interface>
         set dstintf "any"
         set srcaddr <source_address>
         set dstaddr <access_proxy_virtual_IP>
         set action accept
         set schedule "always"
         set service "ALL"
         set logtraffic all
    next
end
```

Optional authentication

To configure authentication to the access proxy, you must configure an authentication scheme and authentication rule in the CLI. They are used to authenticate proxy-based policies, similar to configuring authentication for explicit and transparent proxy.

The authentication scheme defines the method of authentication that is applied. For ZTNA, basic HTTP and SAML methods are supported. Each method has additional settings to define the data source to check against. For example, with basic HTTP authentication, a user database can reference an LDAP server, RADIUS server, local database, or other supported authentication servers that the user is authenticated against.

The authentication rule defines the proxy sources and destinations that require authentication, and which authentication scheme to apply. For ZTNA, active authentication method is supported. The active authentication method references a scheme where users are actively prompted for authentication, like with basic authentication.

After the authentication rule triggers the method to authenticate the user, a successful authentication returns the groups that the user belongs to. In the ZTNA rule and proxy policy you can define a user or user group as the allowed source. Only users that match that user or group are allowed through the proxy policy.

To configure a basic authentication scheme:

```
config authentication scheme
    edit <name>
        set method basic
        set user-database <authentication_server>
    next
end
```

To configure an authentication rule:

```
config authentication rule
    edit <name>
        set status enable
        set protocol http
        set srcintf <interface>
        set srcaddr <address>
        set dstaddr <address>
        set ip-based enable
        set active-auth-method <active_authentication_scheme>
    next
end
```

To apply a user group to a ZTNA rule in the GUI:

1. Go to *Policy & Objects* > *ZTNA* and select the *ZTNA Rules* tab.
2. Edit an existing rule or click *Create New* to create a new rule.
3. Click in the *Source* field, select the *User* tab, and select the users and user groups that will be allowed access.
4. Configure the remaining settings as required.
5. Click *OK*.

To apply a user group to a ZTNA rule in the CLI:

```
config firewall policy
    edit <policy ID>
        set name <ZTNA rule name>
        set type access-proxy
        set access-proxy <access proxy>
        set srcaddr "all"
        set dstaddr "all"
        set ztna-ems-tag <ZTNA tags>
        set action accept
        set schedule "always"
        set logtraffic all
        set groups <user group>
        set utm-status enable
        set ssl-ssh-profile <inspection profile>
    next
end
```

The authentication rule and scheme defines the method used to authenticate users. With basic HTTP authentication, a sign in prompt is shown after the client certificate prompt. After the authentication passes, the returned groups that the user is a member of are checked against the user groups that are defined in the ZTNA rule. If a group matches, then the user is allowed access after passing a posture check.

Connect a ZTNA access proxy to an SSL VPN web portal

SSL VPN web portals can be defined in ZTNA access proxy settings. The ZTNA access proxy handles the access control processes (client certificate authentication, posture check, user authentication and authorization), and establishes the HTTPS connection between the end user and the access proxy. Then, it forwards the user to the web portal where they can use predefined bookmarks to access TCP based services like HTTPS, RDP, VNC, FTP, SFTP, SSH, Telnet, and SMB. Existing SSL VPN portal configurations can be used.

The web portal service can only be configured in the CLI.

Example

In this example, a remote client connects to the ZTNA access proxy and completes the client certificate check. If successful, the remaining access control procedures are automatically completed, and the user is forwarded to the web portal. The web portal is configured with predefined bookmarks that connect to internal servers and external websites. The user can access any resource that is defined in the bookmarks to create an end-to-end connection.

To configure the SSL VPN web portal:

1. Go to *VPN > SSL-VPN Portals* and click *Create New*.
2. Enter the name *test_ssl*.
3. Disable *Tunnel Mode*.
4. Enable *Web Mode*.
5. Create the bookmarks:
   a. In the *Predefined Bookmarks* table click *Create New*.
   b. Enter the name of the service.
   c. Select the service *Type*.
   d. Enter the *URL* to access the service.
   e. Click *OK*.
   f. Repeat these steps to create other bookmarks.
6. Click *OK*.

To configure the ZTNA access proxy:

1. Configure a VIP for the ZTNA access proxy. The `ssl-certificate` can be replaced with a server certificate:
```
config firewall vip
    edit "ztna_webportal"
        set type access-proxy
        set extip 172.18.62.68
        set extintf "any"
        set server-type https
        set extport 4443
        set ssl-certificate "*.test.com"
    next
end
```
2. Configure the virtual host to be used to connect to the ZTNA access proxy. The host should resolve to the VIP's address:
```
config firewall access-proxy-virtual-host
    edit "webportal"
        set ssl-certificate "*.test.com"
        set host "web.test.com"
    next
end
```
3. Configure the ZTNA access proxy to be in web portal mode:
```
config firewall access-proxy
    edit "ztna_webportal"
        set vip "ztna_webportal"
        set client-cert enable
        config api-gateway
            edit 1
                set url-map "/webportal"
                set service web-portal
                set virtual-host "webportal"
```

```
                set ssl-vpn-web-portal "test_ssl"
            next
        end
    next
end
```

4. Apply the access proxy to a proxy policy (specify the ZTNA tags as needed):

```
config firewall proxy-policy
    edit 1
        set name "ztna_rule"
        set proxy access-proxy
        set access-proxy "ztna_webportal"
        set srcintf "any"
        set srcaddr "all"
        set dstaddr "all"
        set ztna-ems-tag "FCTEMS8821000000_High"
        set action accept
        set schedule "always"
        set logtraffic all
        set srcaddr6 "all"
        set dstaddr6 "all"
        set utm-status enable
        set profile-type group
        set profile-group "profile group1"
        set logtraffic-start enable
    next
end
```

The SSL VPN bookmarks are learned by the WAD daemon and are ready to use.

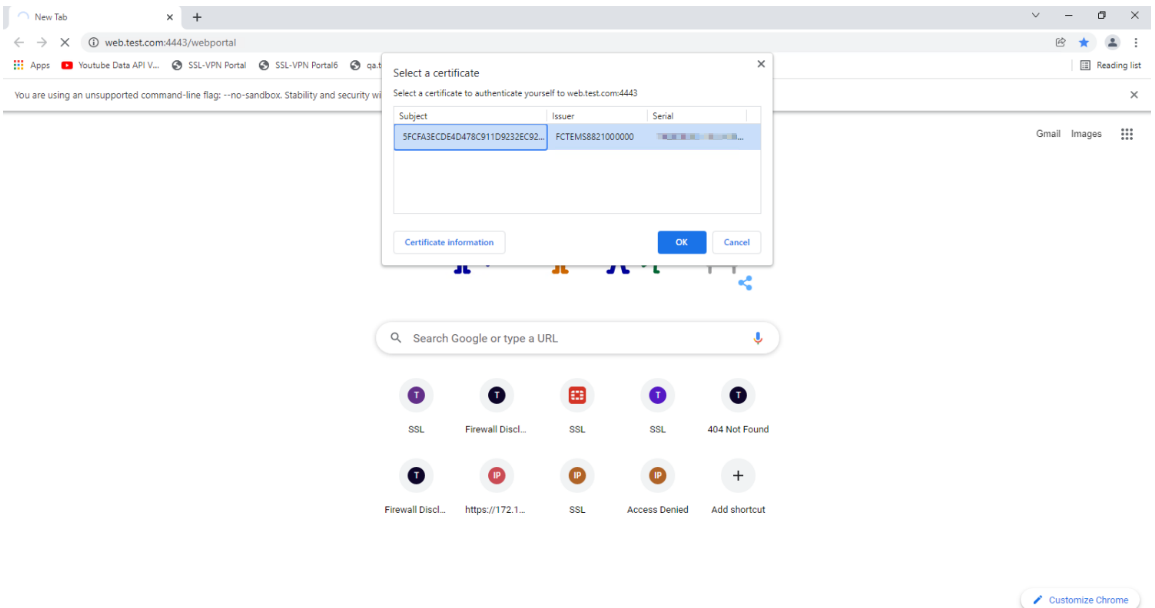
5. Verify the bookmarks:

```
# diagnose test app wad 351
[bookmark: (portal/group/name=test_ssl/gui-bookmarks/2nd HTTP)]:
    type  :1
    url   :http://httpbin.org
    host  :
    folder:
    domain:
    port  :0
[bookmark: (portal/group/name=test_ssl/gui-bookmarks/FTP)]:
    type  :4
    url   :
    host  :
    folder:172.16.200.215
    domain:
    port  :0
[bookmark: (portal/group/name=test_ssl/gui-bookmarks/HTTPS-fortinet)]:
    type  :1
    url   :https://www.fortinet.com
    host  :
    folder:
    domain:
    port  :0
[bookmark: (portal/group/name=test_ssl/gui-bookmarks/RDP)]:
    type  :9
    url   :
```

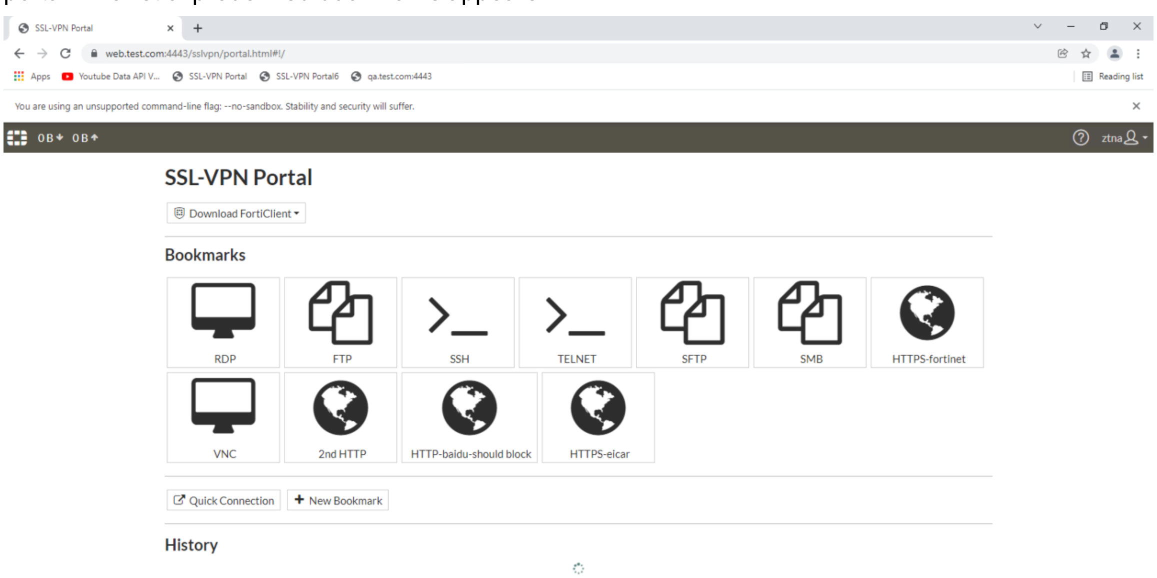
```
    host   :172.18.62.213
    folder:
    domain:
    port   :3389
...
```

To test the connection:

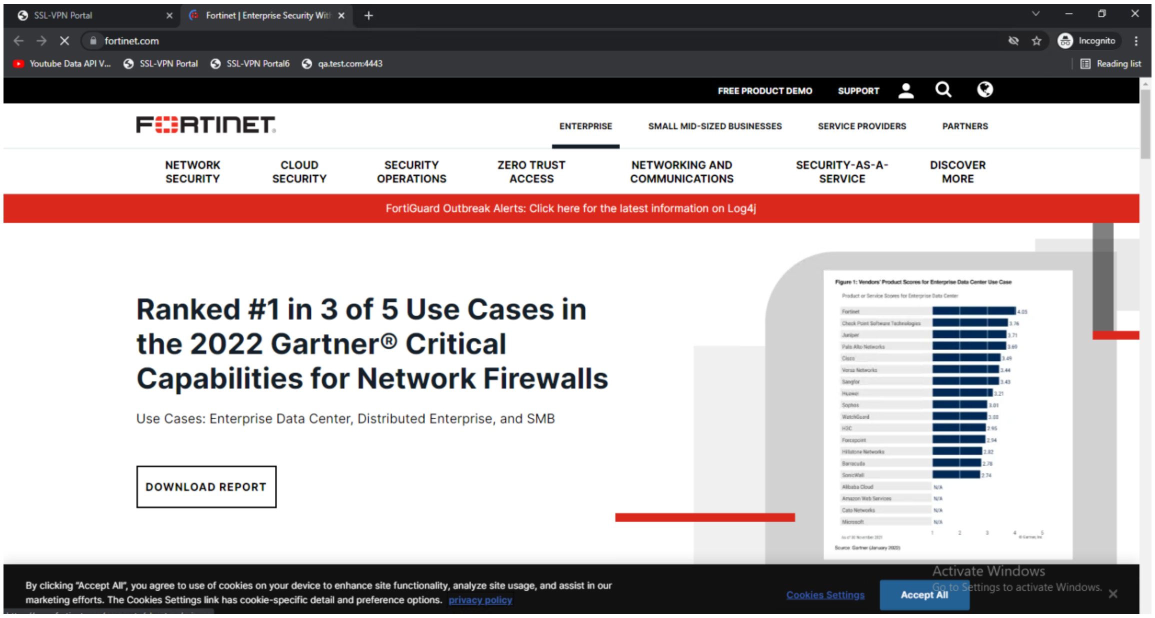
1. From the client browser, go to https://web.test.com:4443/webportal to access the ZTNA access proxy web portal.



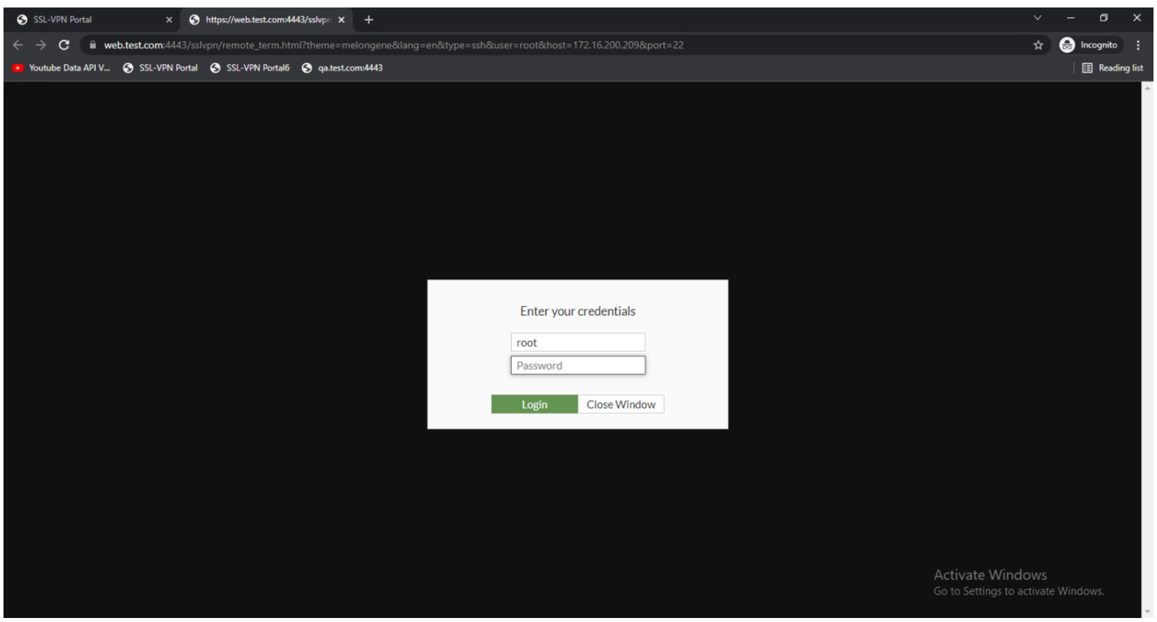
2. Once the client passes the certificate check, posture check, and access is granted, the user is redirected to the web portal. The list of predefined bookmarks appears.



3. Click a bookmark, such as *HTTPS-fortinet*. The website opens.



4. From the web portal, click another bookmark, such as *SSH*. The page opens with the credential login screen to access the server.



UTM scanning on TCP forwarding access proxy traffic

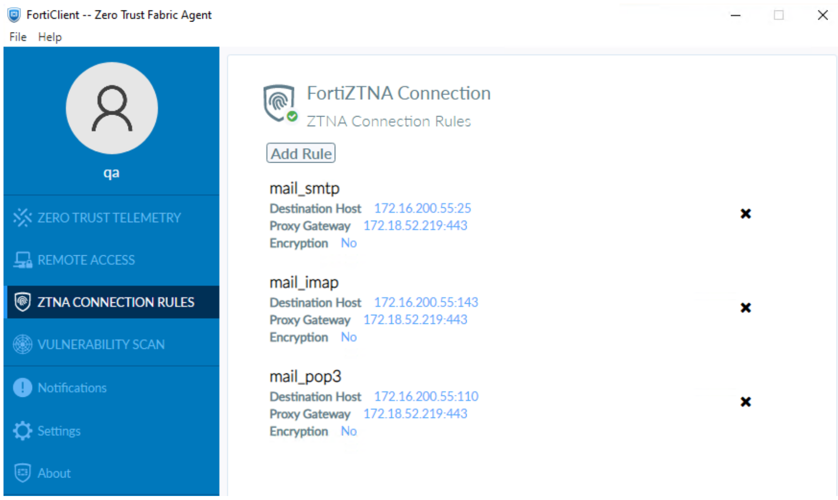
UTM scanning and deep inspection is supported for multiple protocols in a ZTNA TCP forwarding access proxy. In addition to HTTP and HTTPS, the mail protocols (SMTP, IMAP, and POP3) and file sharing protocols (SMB and CIFS) are supported.

Examples

AV scanning for normal POP3, IMAP, and SMTP traffic

To configure AV scanning for normal POP3, IMAP, and SMTP traffic:

1. In FortiClient, add ZTNA connection rules for the email server IP and POP3, IMAP, and SMTP ports.

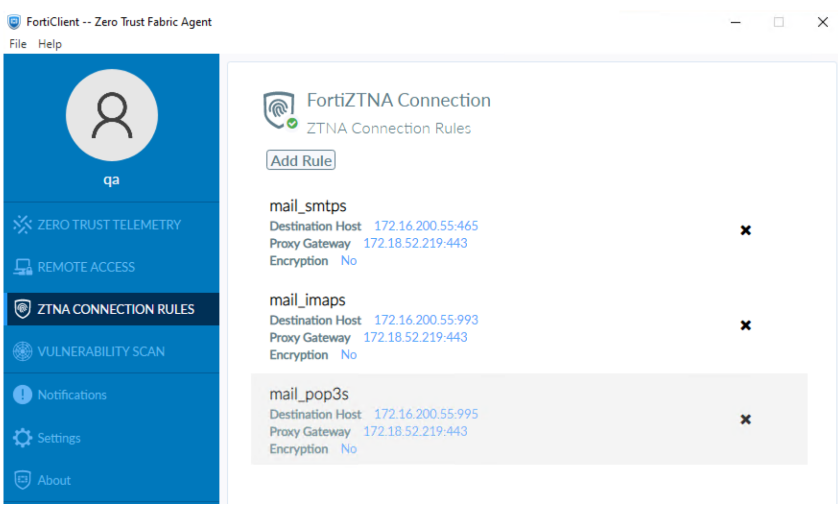


2. On the FortiProxy, configure the ZTNA TCP forwarding server to add the email server address and enable AV profile scanning in the ZTNA rules.
3. On the client PC, open Outlook app and send emails with attachments containing virus affected files.
4. The ZTNA rule on the FortiProxy blocks the email send/receive traffic and generates AV logs.

AV deep scanning for SSL encrypted POP3S, IMAPS, and SMTPS traffic

To configure AV deep scanning for SSL encrypted POP3S, IMAPS, and SMTPS traffic:

1. In FortiClient, add ZTNA connection rules for the email server IP and POP3S, IMAPS, and SMTPS ports.



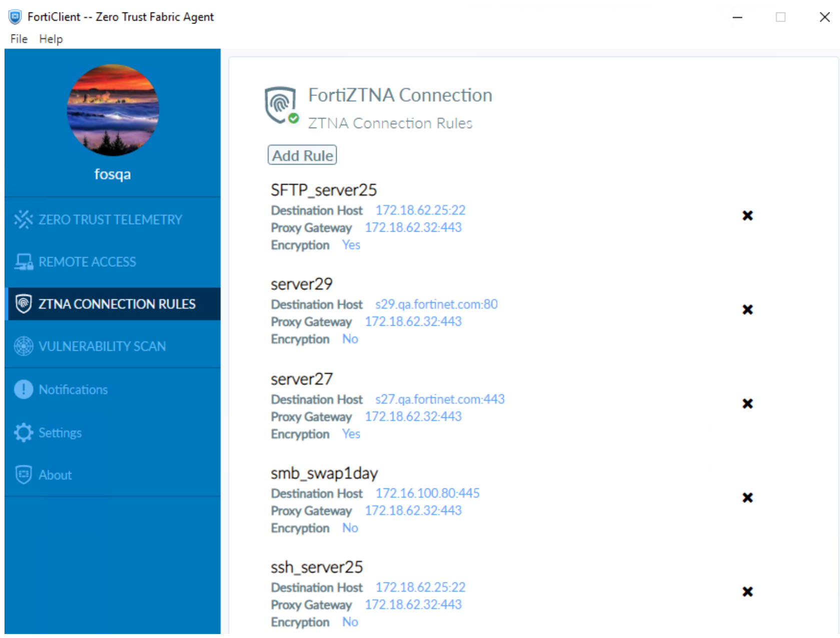
2. On the FortiProxy, configure the ZTNA TCP forwarding server to add the email server address and enable AV profile scanning in the ZTNA rules.

3. On the client PC, open Outlook app and send emails with attachments containing virus affected files.
4. The ZTNA rule on the FortiProxy blocks the email send/receive traffic and generates AV logs.

AV scanning for SMB service traffic

To configure AV scanning for SMB service traffic:

1. In FortiClient, add ZTNA connection rules for the SMB file sharing server IP and ports.



2. On the FortiProxy, configure the ZTNA TCP forwarding server to add the SMB server address and enable AV profile scanning in the ZTNA rules.
3. On the client PC, upload and download virus affected files to and from the SMB server.
4. The ZTNA rule on the FortiProxy blocks the email send/receive traffic and generates AV logs.

File filter scanning for CIFS service traffic

To configure file filter scanning for CIFS service traffic:

1. In FortiClient, add ZTNA connection rules for the CIFS server IP and port.
2. On the FortiProxy, configure the ZTNA TCP forwarding server to add the CIFA server address and enable file filter profile scanning in the ZTNA rules.
3. On the client PC, upload and download predefined file types (such as .EXE) to and from the CIFS server.
4. The ZTNA rule on the FortiProxy blocks the email send/receive traffic and generates AV logs.

Increase ZTNA and EMS tag limits

The following limits have increased for EMS server, IP addresses, and MAC addresses in EMS and ZTNA tags:

- The maximum number of EMS servers a FortiProxy can connect to increased from three to five.
- The maximum number of IP address an EMS tag can resolve increased from 1000 to over 100,000.

- The maximum number of MAC address an EMS tag can resolve increased from 1000 to 3000.

The following diagnose commands are available to verify address information:

```
# diagnose firewall fqdn <option>
```

Option	Description
`list-ip`	List IP FQDN information.
`list-mac`	List MAC FQDN information.
`list-all`	List FQDN information.
`getinfo-ip`	Get information of IP FQDN address.
`getinfo-mac`	Get information of MAC FQDN address.
`get-ip`	Get and display one IP FQDN address.
`get-mac`	Get and display one MAC FQDN address.

Use FQDN with ZTNA TCP forwarding access proxy

When defining ZTNA connection rules on FortiClient for TCP forwarding, it is sometimes desirable to configure the destination host address as an FQDN address instead of an IP address. Since the real servers are often servers in the corporate network, this layer of obfuscation prevents internal IPs from easily leaking to the public, and also makes the destination more easily recognizable by the end users.

One obstacle to overcome is getting remote hosts to resolve an internal FQDN that is typically only resolvable by an internal DNS in the corporate network. This can be solved with the following:

1. When an FQDN address is added as a destination host in a ZTNA connection rule, FortiClient creates a virtual IP for this FQDN address and adds this to the computer's host file (Windows). The same is true when a ZTNA connection rule entry is pushed from EMS.
2. The virtual IP mapped to the FQDN address is not the real address of the server. It allows applications to resolve the FQDN address to this virtual IP. FortiClient listens to any traffic destined for it and forwards the traffic using the TCP forwarding URL with FQDN to the ZTNA access proxy.
3. The access proxy will resolve the FQDN using the internal DNS on the corporate network, matching the traffic to the ZTNA real server configuration with the same domain and address.
4. If a valid ZTNA real server entry is found, traffic is forwarded to the real server.

This features requires a minimum FortiClient and FortiClient EMS version of 7.0.3.

Example

In this example, two servers in the internal network are added for TCP forwarding. The remote client configures two ZTNA connection rules, with the destination host field pointing to the FQDN addresses of the internal servers. These FQDN addresses are configured in the FortiProxy's DNS database so that they can be resolved by the FortiProxy. It is recommended to use an internal DNS server for production environments.

This example assumes that the EMS Fabric connector is already successfully connected.

To configure the TCP forwarding access proxy:

1. Go to *Policy & Objects* > *ZTNA* and select the *ZTNA Servers* tab.
2. Click *Create New*.
3. Set *Name* to *ZTNA_S1*.
4. Configure the network settings:
   a. Set *External interface* to *any*.
   b. Set *External IP* to *172.18.62.32*.
   c. Set *External port* to *443*.
5. Select the *Default certificate*. Clients will be presented with this certificate when they connect to the access proxy VIP.
6. Add server mapping:
   a. In the *Service/server mapping* table, click *Create New*.
   b. For *Service*, select *TCP Forwarding*.
   c. Add a server:
      i. In the *Servers* table click *Create New*.
      ii. Create a new FQDN address for the HTTPS server at s27.qa.fortinet.com, then click *OK*.
      iii. Apply the new address object as the address for the new server.
      iv. Click *OK*.
   d. Add another server using the same steps for s29.qa.fortinet.com.
7. Click *OK*. Now that the ZTNA server is complete, the domain settings must be configured in the CLI to map domains to the real servers.

To map domains to the real servers:

```
config firewall access-proxy
    edit "ZTNA_S1"
        set vip "ZTNA_S1"
        set client-cert enable
        config api-gateway
            edit 2
                set url-map "/tcp"
                set service tcp-forwarding
                config realservers
                    edit 4
                        set address "s27.qa.fortinet.com"
                        set domain "qa.fortinet.com"
                    next
                    edit 5
                        set address "s29.qa.fortinet.com"
                        set domain "qa.fortinet.com"
                    next
                end
            next
        end
    next
end
```

To configure the ZTNA rule:

1. Go to *Policy & Objects* > *ZTNA* and select the *ZTNA Rules* tab.
2. Click *Create New*.
3. Set *Name* to *ZTNA_TCP*.
4. Set *Incoming Interface* to *port2*.
5. Set *Source* to *all*.
6. Select the ZTNA server *ZTNA_S1*.
7. Configure the remaining options as needed.
8. Click *OK*.

To configure the DNS entries for each server:

1. Enable the DNS database visibility:
   a. Go to *System* > *Feature Visibility*.
   b. Enable *DNS Database*.
   c. Click *Apply*.
2. Go to *Network* > *DNS Service*.
3. In *DNS Database* table click *Create New*.
4. Set *DNS Zone* to *ZTNA*.
5. Set *Domain Name* to *qa.fortinet.com*.
6. Add the DNS entries:
   a. In *DNS Entries* table click *Create New*.
   b. Set *Hostname* to *s27*.
   c. Set *IP Address* to the HTTPS server address.
   d. Click *OK*.
   e. Add another DNS entry using the same steps for the s29.qa.fortinet.com HTTP server.
7. Click *OK*.

Testing the connection to the access proxy

Before connecting, users must have a ZTNA connection rule in FortiClient.

ZTNA TCP forwarding rules can be provisioned from the EMS server. See Provisioning ZTNA TCP forwarding rules via EMS for more details.

To create the ZTNA rules in FortiClient and connect:

1. From the *ZTNA Connection Rules* tab, click *Add Rule*.
2. Create a rule for the HTTPS server:
   a. Set *Rule Name* to *server27*.
   b. Set *Destination Host* to *s27.qa.fortinet.com:443*.
   c. Set *Proxy Gateway* to *172.18.62.32:443*.

   d. Disable *Encryption*.
   e. Click *Create*.
3. Create a rule for the HTTP server:
   a. Set *Rule Name* to *server29*.
   b. Set *Destination Host* to *s29.qa.fortinet.com:80*.
   c. Set *Proxy Gateway* to *172.18.62.32:443*.
   d. Disable *Encryption*.
   e. Click *Create*.
4. Upon creating the ZTNA rules, two new entries are added to the Windows PC's host file in folder C:\Windows\System32\drivers\etc. View the file, and observe the new entries for the virtual IP and FQDN pairing for each ZTNA connection rule.

```
# ----- FORTICLIENT ZTNA VIP START -----
10.235.0.1 s27.qa.fortinet.com
10.235.0.2 s29.qa.fortinet.com
# ----- FORTICLIENT ZTNA VIP END -----
```

5. The Windows PC now resolves the FQDNs to the virtual IPs, and FortiClient will listen to the traffic to these IPs and forward them to the TCP access proxy.
6. Have the remote user connect to the HTTPS and HTTP servers on a browser. After device verification, the user is able to successfully connect to the remote servers.

Security Profiles

The FortiProxy unit combines a number of security features to protect your network from threats. As a whole, these features, when included in a single Fortinet security appliance, are referred to as security profiles.

A profile is a group of settings that you can apply to one or more firewall policies. Each Security Profile feature is enabled and configured in a profile, list, or sensor. These are then selected in a security policy and the settings apply to all traffic matching the policy. For example, if you create an antivirus profile that enables antivirus scanning of HTTP traffic, and select the antivirus profile in the security policy that allows your users to access the World Wide Web, all of their web browsing traffic will be scanned for viruses.

Because you can use profiles in more than one security policy, you can configure one profile for the traffic types handled by a set of firewall policies requiring identical protection levels and types, rather than repeatedly configuring those same profile settings for each individual security policy.

For example, while traffic between trusted and untrusted networks might need strict protection, traffic between trusted internal addresses might need moderate protection. To provide the different levels of protection, you might configure two separate sets of profiles: one for traffic between trusted networks, and one for traffic between trusted and untrusted networks. FortiProxy does not modify the original payload if no security action is taken.

This section covers the following topics:

The following are brief descriptions of the security profiles and their features.

Antivirus

Your FortiProxy unit stores a virus signature database that can identify more than 15,000 individual viruses. FortiProxy models that support additional virus databases are able to identify hundreds of thousands of viruses. With a FortiGuard Antivirus subscription, the signature databases are updated whenever a new threat is discovered.

Antivirus also includes file filtering. When you specify files by type or by file name, the FortiProxy unit will block the matching files from reaching your users.

FortiProxy units with a hard drive or configured to use a FortiAnalyzer unit can store infected and blocked files that you can examine later.

Web filter

Web filtering includes a number of features you can use to protect or limit your users' activity on the web.

FortiGuard Web Filtering is a subscription service that allows you to limit access to web sites. More than 60 million web sites and two billion web pages are rated by category. You can choose to allow or block each of the 77 categories.

URL filtering can block your network users from access to URLs that you specify.

Web content filtering can restrict access to web pages based on words and phrases appearing on the web page itself. You can build lists of words and phrases, each with a score. When a web content list is selected in a web filter profile, you can specify a threshold. If a user attempts to load a web page and the score of the words on the page exceeds the threshold, the web page is blocked.

You can create overrides to web filter profiles as well.

Video filter

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.

DNS filter

The FortiProxy will inspect DNS traffic to any DNS server, so long as the policy has DNS inspection enabled. The FortiProxy will intercept DNS requests, regardless of the destination IP, and redirect it to the FortiGuard Secure DNS server—this is separate from the FortiGuard DNS server.

The Secure DNS server will resolve and rate the FQDN and send a DNS response which includes both IP and rating of the FQDN back to the FortiProxy, where it will handle the DNS response according to the DNS filter profile.

Application control

Although you can block the use of some applications by blocking the ports they use for communications, many applications do not use standard ports to communicate. Application control can detect the network traffic of more than 1,000 applications, improving your control over application communication.

You can also write custom signatures tailored to your network.

Intrusion protection

The FortiProxy Intrusion Protection System (IPS) protects your network against hacking and other attempts to exploit vulnerabilities of your systems. More than 3,000 signatures are able to detect exploits against various operating systems, host types, protocols, and applications. These exploits can be stopped before they reach your internal network.

You can also write custom signatures tailored to your network.

File filter

The file filter allows the FortiProxy unit to block files passing through based on file type based on the file's metadata only and not on file size or file content. A DLP sensor must be configured to block files based on size or content, such as SSN numbers, credit card numbers, or regular expression pattern. The file filter can be applied directly to firewall policies.

SSL/SSH inspection

SSL/SSH inspection (otherwise known as *deep inspection*) is used to scan HTTPS traffic in the same way that HTTP traffic can be scanned. This allows the FortiProxy to receive and open up the encrypted traffic on behalf of the client, then the traffic is re-encrypted and sent on to its intended destination.

Individual Deep Inspection profiles can be created, depending on the requirements of the policy. Depending on the profile, you can:

- Configure which CA certificate will be used to decrypt the SSL encrypted traffic
- Configure which SSL protocols will be inspected
- Configure which ports will be associated with which SSL protocols for inspection
- Configure whether or not to allow invalid SSL certificates
- Configure whether or not SSH traffic will be inspected

Data leak prevention

Data leak prevention (DLP) allows you to define the format of sensitive data. The FortiProxy unit can then monitor network traffic and stop sensitive information from leaving your network. Rules for U.S. social security numbers, Canadian social insurance numbers, as well as Visa, Mastercard, and American Express card numbers are included.

Order of execution of security profiles

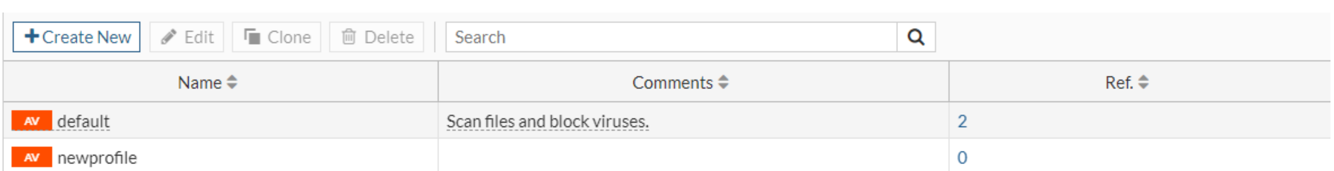
1. Check the IP ban of the UTM quarantine.
2. For transparent HTTPS traffic, process TLS ClientHello with/without SNI:
   a. Check the firewall policy to determine what to allow or deny and which security profiles to apply, including TLS inspection mode, forwarding proxy, and so on.
   b. Check the TLS exemption of deep inspection if necessary.
   c. Check the URL filtering of the web-filtering profile based on hosts learned from TLS negotiation and whether web-filter-based exemptions need to be applied.
   d. Apply TLS sanity checks.
   e. If no deep inspection is needed, forward the traffic back and force with only possible IPS scans.
3. Process the HTTP request headers for plantext HTTP or decrypted HTTPS traffic:
   a. Check the firewall policy on the HTTP request to determine whether to allow or deny and which security profiles to apply:
      i. Check the TLS inspection mode for the HTTP CONNECT request.
      ii. Determine the forwarding proxy for plantext HTTP.
   b. Check the URL filtering of the web-filtering profile based on the URL in the HTTP request.
   c. Apply the video filter profile if necessary.
   d. Apply the web application profile (WAF) on the HTTP headers if necessary.
   e. Apply the web proxy profile to the HTTP request header.
   f. Perform a botnet check in the IPS profile if necessary.

   g. Apply the ICAP profile to forward the HTTP request headers to the ICAP server.
   h. Apply the IPS sensor and Application Control profiles to the HTTP request headers.
4. Process the HTTP request streaming data of the body if the body exists:
   a. Apply the web application profile (WAF) on the HTTP request body if necessary.
   b. Apply the stream-based file filtering, web content filtering, and antivirus scanning.
   c. Apply the IPS sensor and Application Control profiles to the HTTP request body.
   d. Apply the ICAP profile to forward the HTTP request body to the ICAP server.
5. Process the HTTP request whole body if the body exists:
   a. Apply file filtering, web content filtering, antivirus scanning, and DLP to the whole HTTP request.
6. Process the HTTP response headers:
   a. Apply the web application profile (WAF) on the HTTP headers if necessary.
   b. Apply the web proxy profile to the HTTP response headers.
   c. Apply the ICAP profile to forward the HTTP response headers to the ICAP server.
   d. Apply the IPS sensor and Application Control profiles to the HTTP response headers.
7. Process the HTTP response streaming data of the body if the body exists:
   a. Apply the web application profile (WAF) on the HTTP response body if necessary.
   b. Apply the stream-based file filtering, web content filtering, and antivirus scanning.
   c. Apply the IPS sensor and Application Control profiles to the HTTP response body.
   d. Apply the ICAP profile to forward the HTTP response body to the ICAP server.
8. Process the HTTP response whole body if the body exists:
   a. Apply file filtering, web content filtering, antivirus scanning, and DLP to the whole HTTP response.

AntiVirus

An antivirus profile contains specific configuration information that defines how the traffic within a policy is examined and what action can be taken based on the examination. Multiple antivirus profiles can be created for different antivirus scanning requirements. These profiles can then be applied to firewall policies.

To view available antivirus profiles, go to *Security Profiles > AntiVirus*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

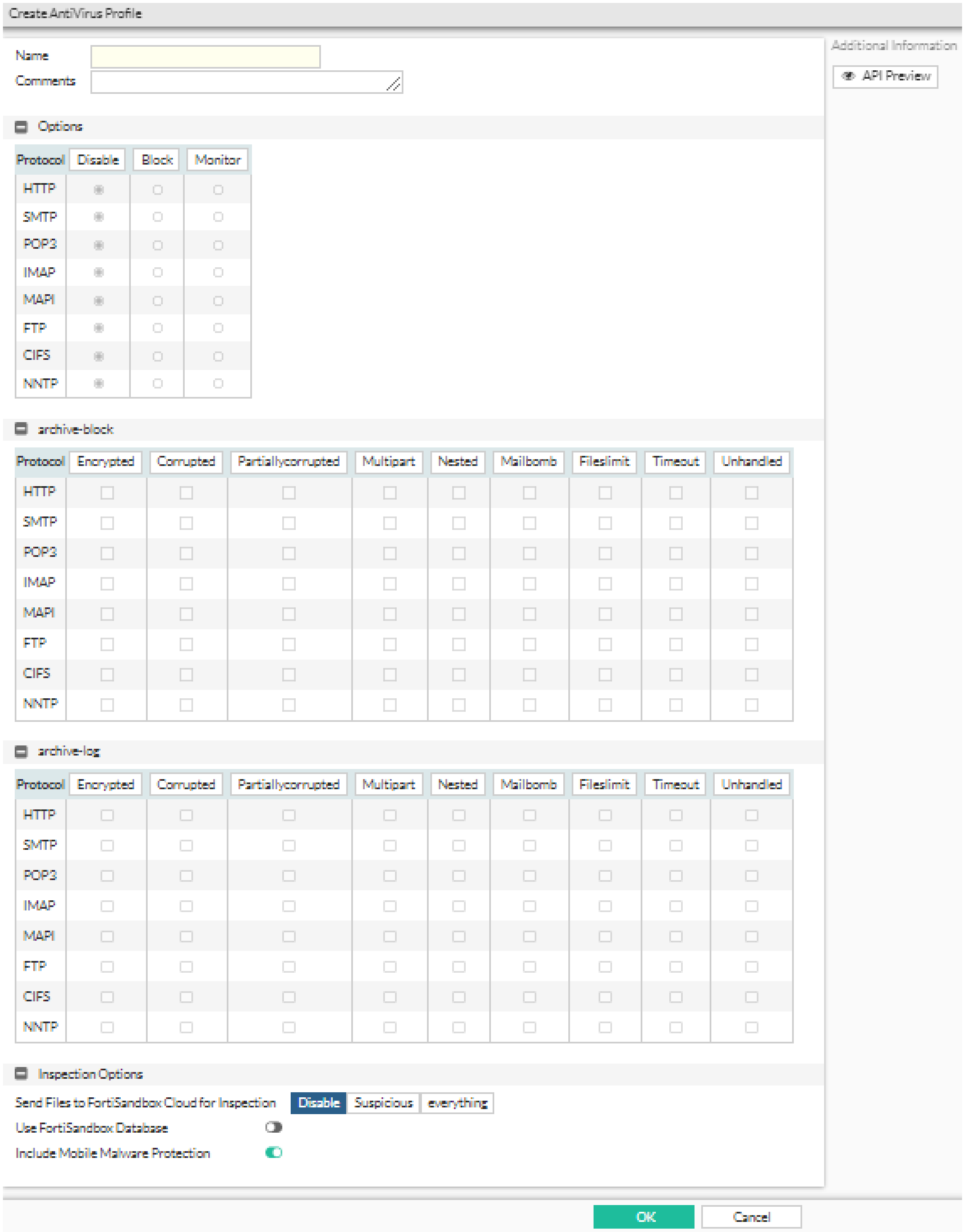
The following options are available:

Create New	Create an antivirus profile. See Create or edit an antivirus profile on page 265.
Edit	Modify the selected antivirus profile. See Create or edit an antivirus profile on page 265.

Clone	Make a copy of the selected antivirus profile.
Delete	Remove the selected antivirus profile.
Search	Enter a search term to find in the list.
Name	The name of the antivirus profile.
Comments	An optional description of the antivirus profile.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit an antivirus profile

Click *Create New* to open the *Create AntiVirus Profile* window.



Select an antivirus profile and then click *Edit* to open the *Edit AntiVirus Profile* window.

Configure the following settings in the *Create AntiVirus Profile* window and then click *OK*:

Name	Enter the name of the antivirus profile.

Comments	Optionally, enter a description of the profile.
Options	For each protocol, enable or disable antivirus scanning, blocking, and monitoring.
Outbreak Prevention	FortiGuard Virus Outbreak Protection Service (VOS) allows the FortiProxy antivirus database to be subsidized with third-party malware hash signatures curated by FortiGuard. The hash signatures are obtained from FortiGuard's Global Threat Intelligence database. The antivirus database queries FortiGuard with the hash of a scanned file. If FortiGuard returns a match, the scanned file is deemed to be malicious. Enabling the AV engine scan is not required to use this feature.
Scanning Files by FortiNDR Server	For each protocol, select to disable, block, or monitor. Refer to Using FortiNDR inline scanning with antivirus on page 273 for more details. This option is available only when a FortiNDR server is connected.
Content Disarm	Content disarm and reconstruction (CDR) allows the FortiProxy unit to sanitize Microsoft Office documents and PDF files (including those that are in ZIP archives) by removing active content, such as hyperlinks, embedded media, JavaScript, macros, and so on from the files (disarm) without affecting the integrity of its textual content (reconstruction). It allows network administrators to protect their users from malicious document files. Files processed by CDR can be stored locally for quarantine on FortiAnalyzer, FortiSandbox, or FortiProxy models with a hard disk. The original copies can also be obtained in the event of a false positive. CDR is supported on HTTP, SMTP, POP3, and IMAP. **NOTE:** SMTP splice and client-comfort mode are not supported.
Archive Block	For each protocol, select the file types to block.
Archive Log	For each protocol, select the file types to log.
Send Files to FortiSandbox Cloud for Inspection	If you want files to be inspected by FortiSandbox Cloud, select *Suspicious* or *everything*. Refer to Using FortiSandbox post-transfer scanning with antivirus on page 271 for more details.
Use FortiSandbox Database	Enable this option to use the FortiSandbox database.
Include Mobile Malware Protection	Enable this option to protect mobile devices from malware.
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.

Stream-based antivirus scan for FTP, SFTP, and SCP

Stream-based antivirus scanning 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. 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
```

Configuring 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 to sanitize Microsoft Office documents and PDF files (including those that are in ZIP archives) by removing active content, such as hyperlinks, embedded media, JavaScript, macros, and so on from the files (disarm) without affecting the integrity of its textual content (reconstruction). It allows network administrators to protect their users from malicious document files.

Files processed by CDR can be stored locally for quarantine on FortiAnalyzer, FortiSandbox, or FortiProxy models with a hard disk. The original copies can also be obtained in the event of a false positive.

CDR is supported on HTTP, SMTP, POP3, and IMAP. **NOTE:** SMTP splice and client-comfort mode are not supported.

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.

To configure CDR:

1. Go to Security Profiles > AntiVirus.
2. Edit an antivirus profile or create a new one.
3. Under *Content Disarm*, enable the options that you want.
4. Select a quarantine location from the available options:
   - *FortiSandbox*—Saves the original document file to a connected FortiSandbox.
   - *File Quarantine*—Saves the original document file to disk (if possible) or a connected FortiAnalyzer based on the FortiProxy log settings (`config log fortianalyzer setting`).
   - *Discard*—The default setting, which discards the original document file.
5. Select the action that is taken when an error occurs:
   - *Block*—Block file when there is a CDR error.
   - *Log Only*—Log the CDR error but allow the file to pass.
   - *Ignore*—When there is a CDR error, let the file pass but do not log the error.
6. Click *OK*.

To edit the CDR detection parameters:

By default, stripping of all active Microsoft Office and PDF content types are enabled. In this example, stripping macros in Microsoft Office documents is disabled.

```
config antivirus profile
   edit <antivirus_profile_name>
      config content-disarm
         set office-macro disable
         set detect-only {enable | disable}
         set cover-page {enable | disable}
         set error-action {block | log-only | ignore}
      end
   next
end
```

Where:

detect-only	Only detect disarmable files, do not alter content. Disabled by default.
cover-page	Attach a cover page to the file’s content when the file has been processed by CDR. Enabled by default.

Using FortiSandbox post-transfer scanning with antivirus

Antivirus profiles can submit potential zero-day viruses to FortiSandbox for inspection. Based on FortiSandbox's analysis, the FortiProxy can supplement its own antivirus database with FortiSandbox's threat intelligence to detect files determined as malicious or suspicious. This augments the FortiProxy antivirus with zero-day detection.

The FortiProxy first examines the file for any known viruses. When a match is found, the file is tagged as known malware. If no match is found, the files are forwarded to FortiSandbox using the following options:

- *All Supported Files*: all files matching the file types defined in the scan profile of the FortiSandbox are forwarded.
- *Suspicious Files Only*: files classified by the antivirus as having any possibility of active content are forwarded to FortiSandbox. When using FortiGate Cloud Sandbox, we recommend selecting this option due to its submission limits.
- *None*: files are not forwarded to FortiSandbox.

To enable FortiSandbox inspection in an antivirus profile:

1. Go to *Security Profiles > AntiVirus*.
2. Create, edit, or clone an antivirus profile.
3. In the *Inspection Options* section, set *Send files to FortiSandbox for inspection* to either *Suspicious* or *everything*.
4. Optionally, for *Do not submit files matching types and Patterns*, click the + to exclude certain file types from being sent to FortiSandbox.
5. Optionally, for *Do not submit files matching types and Patterns*, click the + to enter a wildcard pattern to exclude files from being sent to FortiSandbox.
6. Enable *Use FortiSandbox Database*.
7. Click *OK*.

FortiProxy diagnostics

To view the detection count:

```
# diagnose test application quarantined 7
Total: 0

Statistics:
        vfid: 0, detected: 2, clean: 1252, risk_low: 6, risk_med: 2, risk_high: 1, limit_
reached:0
```

To verify the address is configured correctly:

```
# diagnose test application quarantined 1
…
fortisandbox-fsb1 is enabled: analytics, realtime=yes, taskfull=no
addr=172.18.52.154/514, source-ip=0.0.0.0, keep-alive=no. ssl_opt=3, hmac_alg=0
…
```

To run the diagnostics for real-time debugging:

```
# diagnose debug application quarantined -1
# diagnose debug enable
```

To check the FortiGate Cloud server status:

```
# diagnose test application forticldd 3
…
    Active APTServer status:  up
```

To view FortiGate Cloud Sandbox submission statistics for advanced debugging:

```
# diagnose test application quarantined 2
```

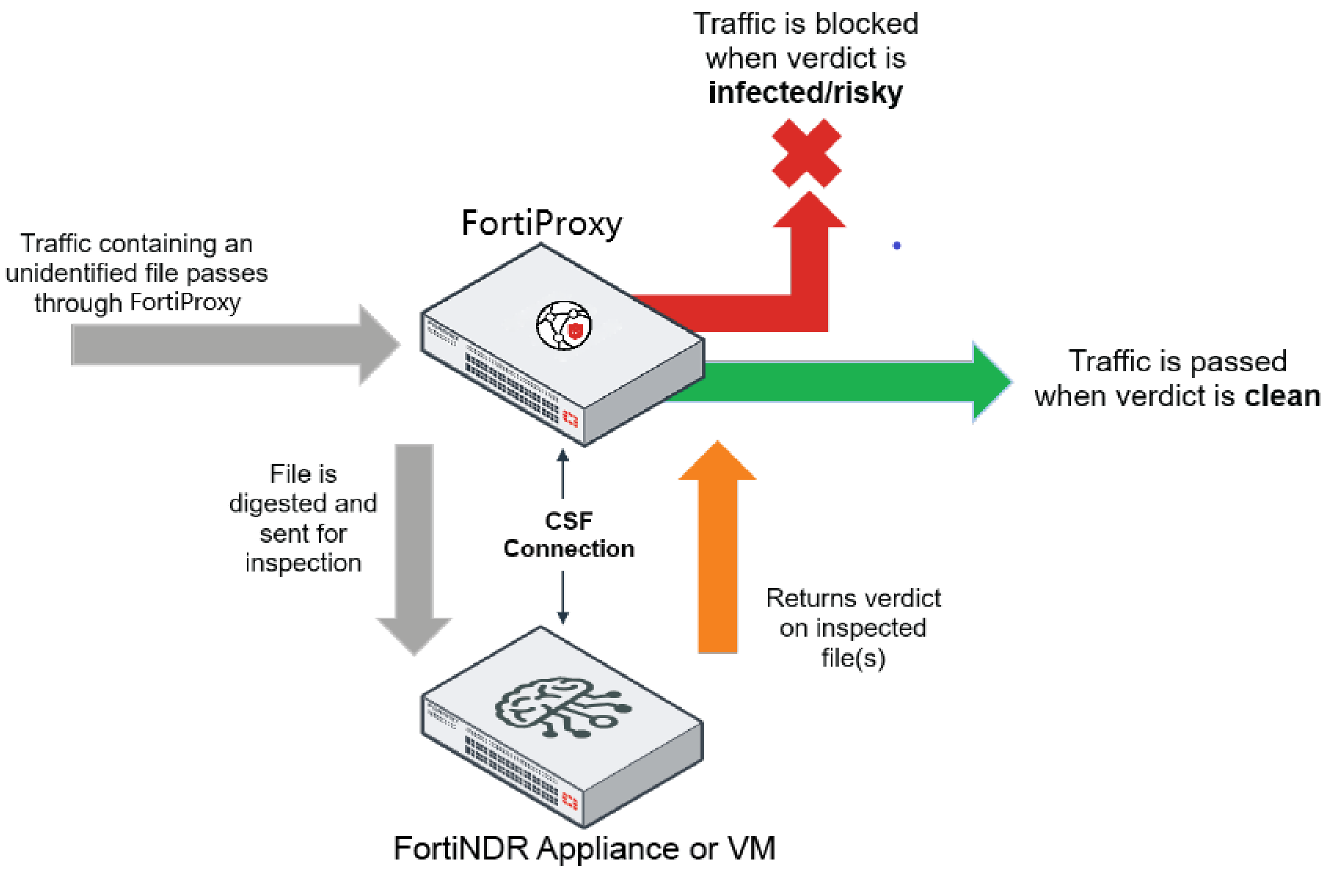
FortiSandbox diagnostics

To run the OFTP debug for advanced debugging:

```
# diagnose-debug device <client serial number>
```

Using FortiNDR inline scanning with antivirus

FortiNDR (formerly FortiAI) can be used with antivirus profiles in FortiProxy. FortiNDR inspects high-risk files and issues a verdict to the firewall based on how close the file features match those of malware. When enabled, FortiNDR can log, block, ignore, or monitor (allow) the file based on the verdict.



A licensed FortiNDR appliance with version 1.5.1 or later is required to use this feature.

To configure FortiNDR inline inspection with an AV profile:

1. Configure FortiNDR to join a Security Fabric in FortiProxy:
   a. Enable Security Fabric on FortiProxy using the following command:

   ```
   config system csf
          set status enable
          set group-name "fabric-ai"
   end
   ```

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

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

   c. In FortiNDR, configure the device to join the Security Fabric:

   ```
   config system csf
          set status enable
          set upstream-ip 10.6.30.14
          set managment-ip 10.6.30.251
   end
   ```

   d. Authorize the FortiNDR in FortiProxy:

   ```
   config system csf
          config trusted-list
                  edit "FAIVMSTM21000000"
                          set authorization-type certificate
                          set certificate "********************"
                  next
          end
   end
   ```

2. In the FortiProxy CLI, enable inline inspection:

   ```
   config system fortindr
       set status enable
   end
   ```

3. Configure an AV profile in FortiProxy to use inline inspection and block detected infections (see also Create or edit an antivirus profile on page 265):

   ```
   config antivirus profile
       edit "av"
           set feature-set proxy
           config http
               set fortindr block
           end
           config ftp
               set fortindr block
           end
           config imap
               set fortindr block
           end
           config pop3
               set fortindr block
   ```

```
        end
        config smtp
            set fortindr block
        end
        config mapi
            set fortindr block
        end
        config nntp
            set fortindr block
        end
        config cifs
            set fortindr block
        end
        config ssh
            set fortindr block
        end
    next
end
```

4. Add the AV profile to a policy. See Create or edit a policy on page 134.
   When potential infections are blocked by FortiNDR inline inspection, a replacement message appears. See Replacement Messages on page 492 for more information.

Sample log

```
date=2021-04-29 time=15:12:07 eventtime=1619734327633022960 tz="-0700" logid="0209008221"
type="utm" subtype="virus" eventtype="fortindr" level="notice" vd="vdom1" policyid=1
msg="Detected by FortiNDR." action="monitored" service="HTTP" sessionid=13312
srcip=10.1.100.221 dstip=172.16.200.224 srcport=50792 dstport=80 srcintf="wan2"
srcintfrole="wan" dstintf="wan1" dstintfrole="wan" proto=6 direction="incoming"
filename="detected_samples.zip" quarskip="File-was-not-quarantined"
virus="MSIL/Kryptik.KVH!tr" dtype="fortindr"
ref="http://www.fortinet.com/ve?vn=MSIL%2FKryptik.KVH%21tr" virusid=0
url="http://172.16.200.224/avengine_ai/detected_samples.zip" profile="av"
agent="curl/7.68.0" analyticssubmit="false" crscore=50 craction=2 crlevel="critical"
```

FortiNDR inline inspection with other AV inspection methods

The following inspection logic applies when FortiNDR inline inspection is enabled simultaneously with other AV inspection methods. The AV engine inspection and its verdict always takes precedence because of performance. The actual behavior depends on which inspected protocol is used.

HTTP, FTP, SSH, and CIFS protocols:

1. AV engine scan; AV database and FortiSandbox database (if applicable).
   a. FortiNDR inline inspection occurs simultaneously.
2. AV engine machine learning detection for WinPE PUPs (potentially unwanted programs).
   a. FortiNDR inline inspection occurs simultaneously.
3. Outbreak prevention and external hash list resources.
   a. FortiNDR inline inspection occurs simultaneously.

If any AV inspection method returns an infected verdict, the FortiNDR inspection is aborted.

POP3, IMAP, SMTP, NNTP, and MAPI protocols:

1. AV engine scan; AV database and FortiSandbox database (if applicable).
2. AV engine machine learning detection for WinPE PUPs (potentially unwanted programs).
   a. FortiNDR inline inspection occurs simultaneously.
3. Outbreak prevention and external hash list resources.
   a. FortiNDR inline inspection occurs simultaneously.

In an AV profile, use `set fortindr-error-action {log-only | block | ignore}` to configure the action to take if FortiNDR encounters an error.

Accepted file types

The following file types are sent to FortiNDR for inline inspection:

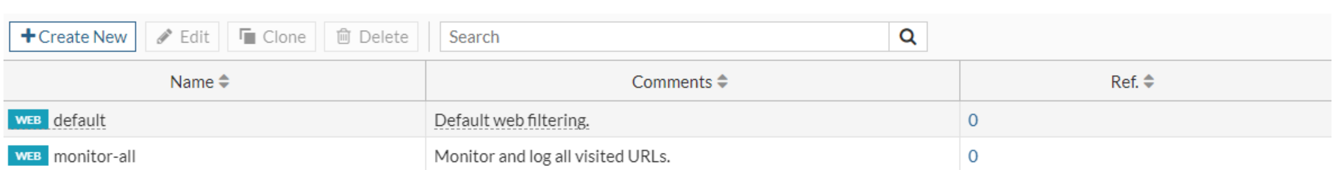
7Z	HTML	RTF
ARJ	JS	TAR
BZIP	LZH	VBA
BZIP2	LZW	VBS
CAB	MS Office documents (XML and non-XML)	WinPE (EXE)
ELF	PDF	XZ
GZIP	RAR	ZIP

Web Filter

This section describes how to configure web filters for HTTP traffic and configure URL filters to allow or block caching of specific URLs.

After you configure a web filter profile, you can apply it to a policy. A profile is specific information that defines how the traffic within a policy is examined and what action can be taken based on the examination.

To view available web filter profiles, go to *Security Profiles* > *Web Filter*.



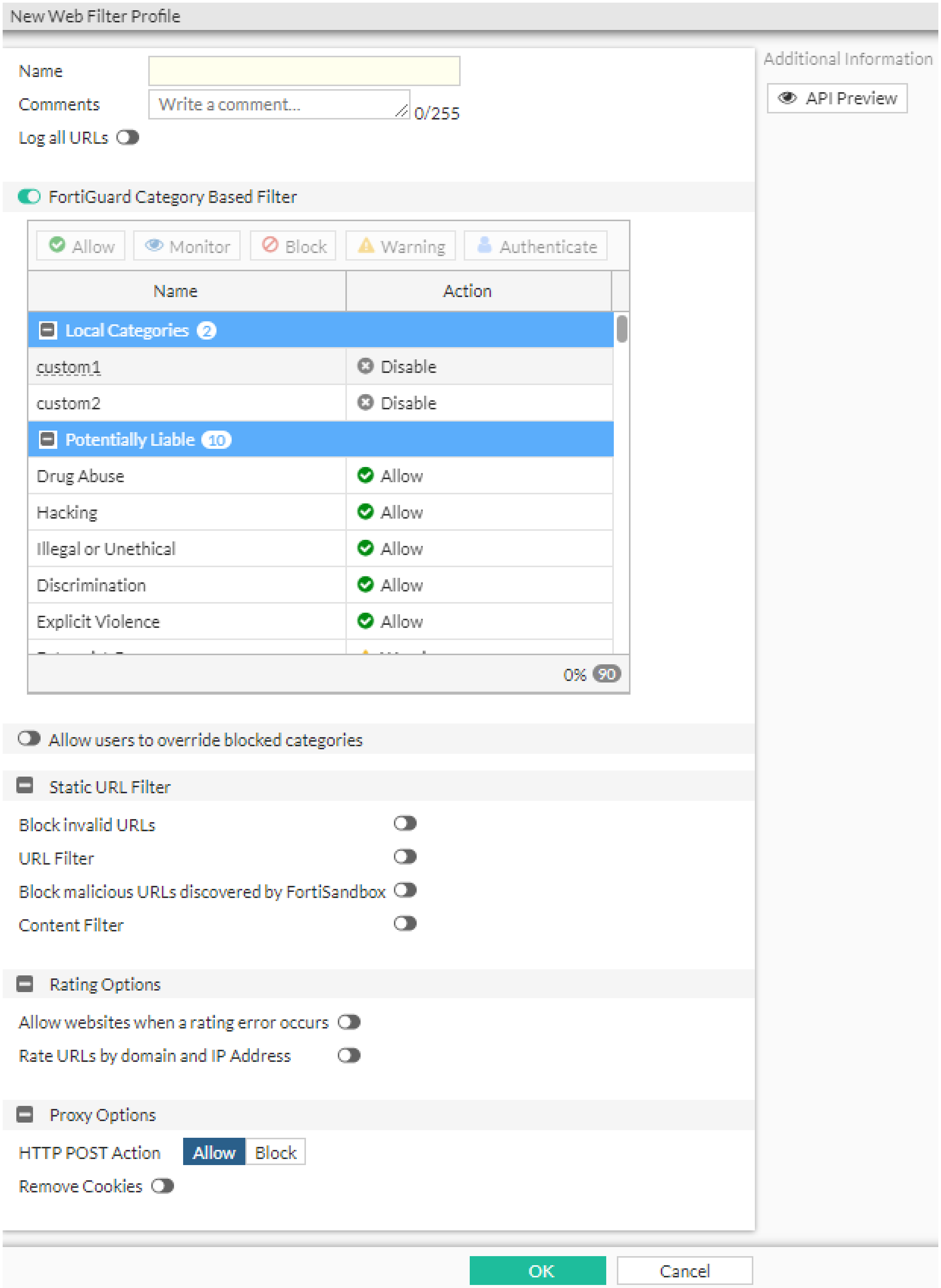
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a web filter profile. See Create or edit a web filter profile on page 277.
Edit	Modify the selected web filter profile. See Create or edit a web filter profile on page 277.
Clone	Make a copy of the selected web filter profile.
Delete	Remove the selected web filter profile.
Search	Enter a search term to find in the web filter profile list.
Name	The name of the web filter profile.
Comments	An optional description of the web filter profile.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a web filter profile

Click *Create New* to open the *Create Web Filter Profile* window.


New Web Filter Profile
Name
Comments
Write a comment...
0/255
Log all URLs
Additional Information
API Preview
FortiGuard Category Based Filter
Allow
Monitor
Block
Warning
Authenticate
Name
Action
Local Categories 2
custom1
Disable
custom2
Disable
Potentially Liable 10
Drug Abuse
Allow
Hacking
Allow
Illegal or Unethical
Allow
Discrimination
Allow
Explicit Violence
Allow
0% 90
Allow users to override blocked categories
Static URL Filter
Block invalid URLs
URL Filter
Block malicious URLs discovered by FortiSandbox
Content Filter
Rating Options
Allow websites when a rating error occurs
Rate URLs by domain and IP Address
Proxy Options
HTTP POST Action
Allow
Block
Remove Cookies
OK
Cancel

Select a web filter profile and then click *Edit* to open the *Edit Web Filter Profile* window.

Configure the following settings in the *Create Web Filter Profile* window and then click *OK*:

Name	The name of the web filter profile.
Comments	Optional description of the web filter profile.
Log all URLs	Enable if you want all URLs to be logged.
FortiGuard category based filter	Enable to use FortiGuard categories. If the device is not licensed for the FortiGuard web-filtering service, traffic can be blocked by enabling this option.
Allow/Monitor/Block/Warning/Authentication	Select the action for each FortiGuard category: *Allow*, *Monitor*, *Block*, *Warning*, or *Authenticate*. You can enter a category to search for.
Allow users to override blocked categories	Enable this option if you want users to be able to override blocked categories.
Groups that can override	Select the user groups that will be able to override blocked categories. This option is available only if *Allow users to override blocked categories* is enabled.
Profile Name	Select which web filter profile to change blocked categories to. This option is available only if *Allow users to override blocked categories* is enabled.
Switch applies to	Select whether the new web filter profile applies to a *User*, *User Groups*, or *IP* or whether to *Ask*. The user or user groups must be specified as the *Source* in firewall policies using this profile. This option is available only if *Allow users to override blocked categories* is enabled.
Switch Duration	Select whether blocked categories can be overridden for a predefined period or to *Ask*. This option is available only if *Allow users to override blocked categories* is enabled.
day(s)/hour(s)/minute(s)	Select how long users can override blocked categories. This option is available only if *Allow users to override blocked categories* is enabled and the *Switch Duration* is set to *Predefined*.
Static URL Filter	
Block invalid URLs	Enable to block web sites when their SSL certificate CN field does not contain a valid domain name.
URL Filter	Enable and then create or edit a URL filter. See Create or edit a URL filter on page 283.

Block malicious URLs discovered by FortiSandbox	Enable to block malicious URLs discovered by FortiSandbox.
Content Filter	Enable and then create or edit a content filter to block access to web pages that include the specified patterns. See Create or edit a content filter on page 284.
Rating Options	
Allow websites when a rating error occurs	Enable to allow access to web pages that return a rating error from the web filter service. If your unit is temporarily unable to contact the FortiGuard service, this setting determines what access the unit allows until contact is re-established. If enabled, users will have full unfiltered access to all web sites. If disabled, users will not be allowed access to any web sites.
Rate URLs by domain and IP Address	Enable to have the unit request site ratings by URL and IP address separately, providing additional security against attempts to bypass the FortiGuard Web Filter. FortiGuard Web Filter ratings for IP addresses are not updated as quickly as ratings for URLs. This difference can sometimes cause the unit to allow access to sites that should be blocked or to block sites that should be allowed.
Proxy Options	
HTTP POST Action	Select whether to *Allow* or *Block* HTTP POST traffic. HTTP POST is the command used by your browser when you send information, such as a form you have filled-out or a file you are uploading, to a web server.
Remove Cookies	Enable to filter cookies from web traffic. Web sites using cookies might not function properly with this enabled.
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.

Using 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.

Configuring user-name-only credential matching

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
```

Configuring different custom pattern types for user names and passwords

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.

Create or edit a URL filter

You can allow or block access to specific web sites by adding them to the URL filter list. You add the web sites by using patterns containing text and regular expressions. The FortiProxy unit allows or blocks web pages matching any specified URLs or patterns and displays a replacement message instead.

Web site blocking does not block access to other services that users can access with a web browser. For example, web site blocking does not block access to ftp://ftp.example.com. Instead, use firewall policies to deny ftp connections.

When adding a URL to the web site filter list, follow these rules:

- Type a top-level URL or IP address to control access to all pages on a web site. For example, www.example.com or 192.168.144.155 controls access to all pages at these web sites.
- Enter a top-level URL followed by the path and file name to control access to a single page on a web site. For example, www.example.com/monkey.html or 192.168.144.155/monkey.html controls access to the monkey page on this web site.
- To control access to all pages with a URL that ends with example.com, add example.com to the filter list. For example, adding example.com controls access to www.example.com, mail.example.com, www.finance.example.com, and so on.
- Control access to all URLs that match patterns using text and regular expressions (or wildcard characters). For example, example.* matches example.com, example.org, example.net and so on.

URLs with an action set to exempt or pass are not scanned for viruses. If users on the network download files through the FortiProxy unit from a trusted web site, add the URL of this web site to the URL filter list with an action to pass it, so the unit does not scan files downloaded from this URL.

To create a URL filter:

1. Go to *Security Profiles* > *Web Filter*.
2. Click *Create New* or select a web filter profile and then click *Edit*.
3. Enable *URL Filter*.
4. In the *URL Filter* table, click *Create New*. The *New URL Filter* window opens.
5. Enter the URL to filter in the *URL* field. Enter a top-level domain suffix (for example, “com” without the leading period) to block access to all web sites with this suffix.
6. Select the type of pattern to match: *Simple*, *Reg. Expression*, or *Wildcard*.

7. Select the action to take when the pattern is matched:
   - *Exempt*: Allow trusted traffic to bypass the antivirus proxy operations.
   - *Block*: Block access to any URLs matching the URL pattern and display a replacement message. SeeReplacement Messages on page 492.
   - *Allow*: Allow access to any URL that matches the URL pattern.
   - *Monitor*: Monitor traffic to and from URLs matching the URL pattern.
8. Enable or disable the status of the filter to make the filter active or inactive.
9. Enter the referrer host name.
10. Click *OK* to save the URL filter.
11. Click *OK* to save the changes to the web filter profile.

To edit a URL filter:

1. Go to *Security Profiles* > *Web Filter*.
2. Click *Create New* or select a web filter profile and then click *Edit*.
3. In the URL Filter table, double-click on a filter or select the filter and then click *Edit* in the toolbar.
4. Edit the filter settings as required.
5. Click *OK* to save your changes to the URL filter.
6. Click *OK* to save the changes to the web filter profile.

Create or edit a content filter

Content filters can be added or edited, as required.

To create a web content filter:

1. Go to *Security Profiles* > *Web Filter*.
2. Click *Create New* or select a web filter profile and then click *Edit*.
3. In the *Static URL Filter* section, enable *Content Filter*.
4. Select *Create New*.
5. Select the *Pattern Type*, either *Wildcard* or *Regular Expression*.
6. Enter the content *Pattern* to match.
7. Select the *Language* from the drop-down menu.
8. Select *Block* or *Exempt*.
9. Enable the *Status*.
10. Click *OK*.

To edit a web content filter:

1. Go to *Security Profiles* > *Web Filter*.
2. Click *Create New* or select a web filter profile and then click *Edit*.
3. In the *Static URL Filter* section, enable *Content Filter*.
4. Select the content filter you want to edit and then click *Edit* from the toolbar. The *Edit Web Content Filter* window opens.
5. Edit the information as required and then click *OK* to apply your changes.

FortiGuard filter

The FortiGuard filter enhances the web filter features by sorting billions of web pages into a wide range of categories that users can allow or block.

The FortiGuard Web Filtering service includes over 45 million individual website ratings that apply to more than two billion pages. When the FortiGuard filter is enabled in a web filter profile and applied to firewall policies, if a request for a web page appears in traffic controlled by one of the firewall policies, the URL is sent to the nearest FortiGuard server. The URL category or rating is returned. If the category is blocked, the FortiProxy shows a replacement message in place of the requested page. If the category is not blocked, the page request is sent to the requested URL as normal.

To use this service, you must have a valid FortiGuard license.

The following actions are available:

FortiGuard web filter action	Description
Allow	Permit access to the sites in the category.
Monitor	Permit and log access to sites in the category. User quotas can be enabled for this option.
Block	Prevent access to the sites in the category. Users trying to access a blocked site see a replacement message indicating the site is blocked.
Warning	Display a message to the user allowing them to continue if they choose.
Authenticate	Require the user to authenticate with the FortiProxy before allowing access to the category or category group.
Disable	Remove the category from the from the web filter profile. This option is only available for local or remote categories from the right-click menu.

FortiGuard web filter categories

FortiGuard has many web filter categories, including two local categories and a special remote category:

- All URL categories—See Web Filter Categories.
- Local categories— See Web Rating Overrides on page 323.
- Remote category

The priority of categories is local category > external category > FortiGuard built-in category. If a URL is configured as a local category, it only follows the behavior of the local category and not the external or FortiGuard built-in category.

Blocking a web category

The following example shows how to block a website based on its category. The Information Technology category (category 52) will be blocked.

To block a category in the GUI:

1. Go to *Security Profiles > Web Filter* and click *Create New*, or edit an existing profile.
2. In the *FortiGuard category based filter* section, select *Information Technology*, then click *Block*.

3. Configure the remaining settings as needed.
4. Click *OK*.

To block a category in the CLI:

```
config webfilter profile
    edit "webfilter"
        config ftgd-wf
            unset options
            config filters
                edit 1
                    set category 52
                    set action block
                next
            end
        end
    next
end
```

To verify that the category is blocked:

1. Go to a website that belongs to the blocked category, such as www.fortinet.com.
   The page should be blocked and display a replacement message.

To view the log of a blocked website in the GUI:

1. Go to *Log & Report > Security Events*.
2. Click the *Web Filter* card name.
3. Select an entry with *blocked* in the *Action* column and click *Details*.

To view the log of a blocked website in the CLI:

```
# execute log filter category utm-webfilter
# execute log display

4: date=2023-08-08 time=13:25:31 eventtime=1691526331836645153 tz="-0700" logid="0316013056"
type="utm" subtype="webfilter" eventtype="ftgd_blk" level="warning" vd="root" policyid=1
poluuid="4a4b9d00-e471-51ed-71ec-c1a3bc8f773c" policytype="policy" sessionid=254529
srcip=1.1.1.2 srcport=60836 srccountry="Australia" srcintf="internal7" srcintfrole="lan"
srcuuid="45eec070-e471-51ed-4b1c-930f37c5d882" dstip=44.240.173.227 dstport=443
dstcountry="United States" dstintf="wan1" dstintfrole="wan" dstuuid="45eec070-e471-51ed-
4b1c-930f37c5d882" proto=6 service="HTTPS" hostname="www.fortinet.com" profile="default"
action="blocked" reqtype="direct" url="https://www.fortinet.com/" sentbyte=517 rcvdbyte=0
direction="outgoing" msg="URL belongs to a denied category in policy" ratemethod="domain"
cat=52 catdesc="Information Technology"
```

Allowing users to override blocked categories

There is an option to allow users with valid credentials to override blocked categories.

To allow users to override blocked categories in the GUI:

1. Go to *Security Profiles* > *Web Filter* and click *Create New*, or edit an existing profile.
2. Enable *Allow users to override blocked categories*.
3. Enter information in the following fields:
   - *Groups that can override*
   - *Profile name*
   - *Switch applies to*
   - *Switch Duration*
4. Configure the other settings as needed.
5. Click *OK*.

To allow users to override blocked categories in the CLI:

```
config webfilter profile
    edit "webfilter"
        set ovrd-perm bannedword-override urlfilter-override fortiguard-wf-override
contenttype-check-override
        config override
            set ovrd-user-group "radius_group"
            set profile "webfilter"
        end
        config ftgd-wf
            unset options
        end
    next
end
```

Issuing a warning on a web category

The following example shows how to issue a warning when a user visits a website in a specific category (Information Technology, category 52).

To configure a warning for a category in the GUI:

1. Go to *Security Profiles* > *Web Filter* and click *Create New*, or edit an existing profile.
2. In the *FortiGuard category based filter* section, select *Information Technology*, then click *Warning*.
3. Set the *Warning Interval*, then click *OK*.
   The warning interval is the amount of time until the warning appears again after the user proceeds past it.
4. Configure the remaining settings as needed.
5. Click *OK*.

To configure a warning for a category in the CLI:

```
config webfilter profile
    edit "webfilter"
        config ftgd-wf
            unset options
            config filters
```

```
                edit 1
                    set category 52
                    set action warning
                next
            end
        end
    next
end
```

To verify that the warning works:

1. Go to a website that belongs to the category, such as www.fortinet.com.
2. On the warning page, click *Proceed* or *Go Back*.

Authenticating a web category

The following example shows how to authenticate a website based on its category (Information Technology, category 52).

To authenticate a category in the GUI:

1. Go to *Security Profiles* > *Web Filter* and edit or create a new web filter profile.
2. In the *FortiGuard category based filter* section, select *Information Technology*, then click *Authenticate*.
3. Set the *Warning Interval* and select one or more user groups, then click *OK*.
4. Configure the remaining settings as needed.
5. Click *OK*.

To authenticate a category in the CLI:

```
config webfilter profile
    edit "webfilter"
        config ftgd-wf
            unset options
            config filters
                edit 1
                    set category 52
                    set action authenticate
                    set auth-usr-grp "local_group"
                next
            end
        end
    next
end
```

To verify that you have configured authentication:

1. Go to a website that belongs to the category, such as www.fortinet.com.
2. On the warning page, click *Proceed*.
3. Enter the username and password for the configured user group, then click *Continue*.

Customizing the replacement message page

When the category action is *Block*, *Warning*, or *Authenticate*, you can customize the replacement message page that a user sees.

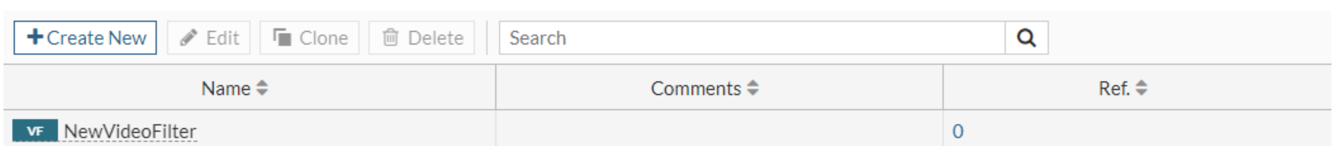
To customize the replacement message page:

1. Go to *Security Profiles* > *Web Filter* and edit or create a new web filter profile.
2. In the *FortiGuard category based filter* section, right-click on a category and select *Customize*.
3. Select a *Replacement Message Group*. See Replacement Message Groups on page 500 for details.
4. Optionally, click *Edit FortiGuard Block Page* or *Edit FortiGuard Warning Page* to make modifications.
5. Click *Save*.
6. Configure the remaining settings as needed.
7. Click *OK*.

Video Filter

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 view available video filter profiles, go to *Security Profiles* > *Video Filter*.



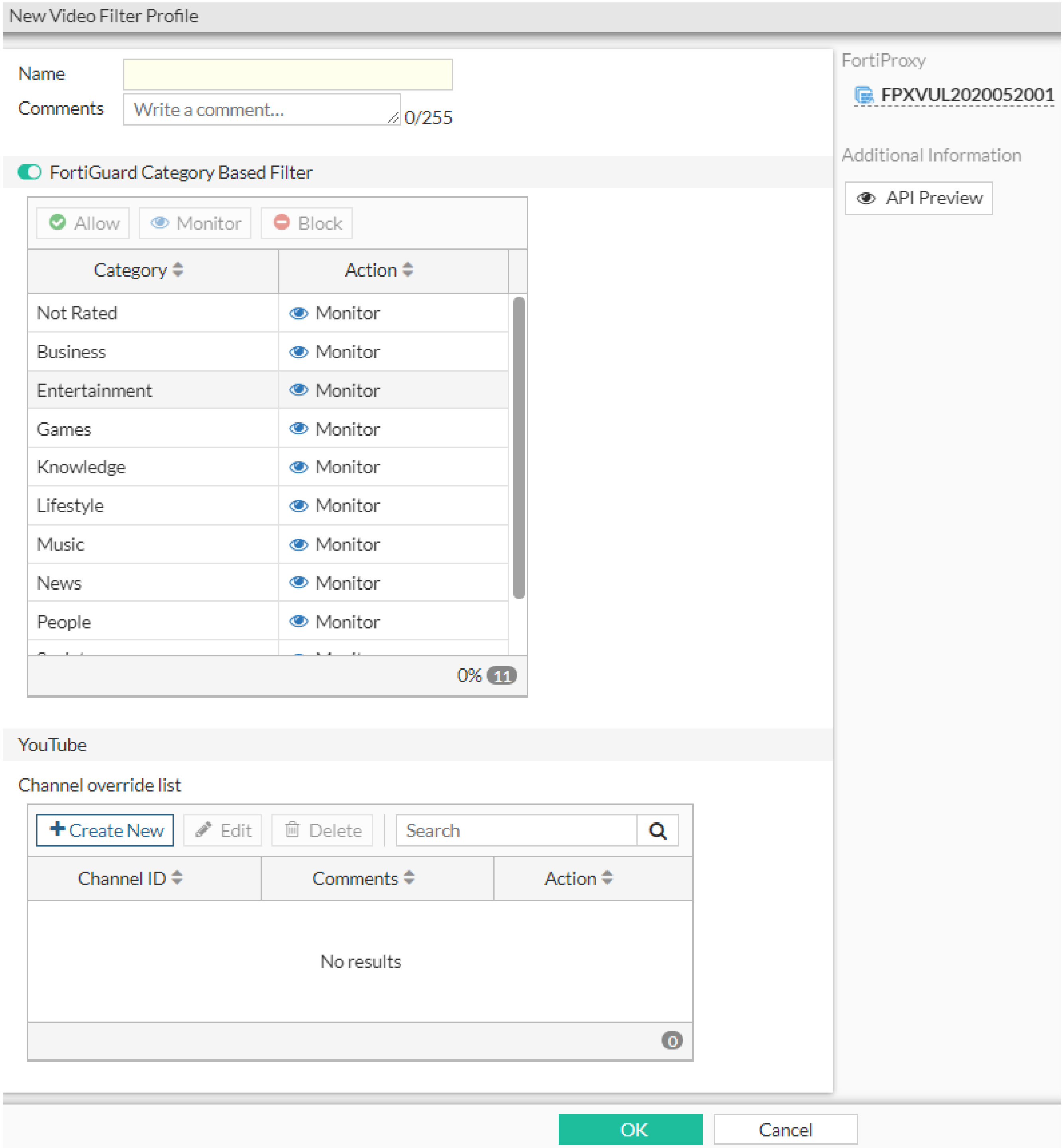
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a video filter profile. See Create or edit a video filter profile on page 290.
Edit	Modify the selected video filter profile. See Create or edit a video filter profile on page 290.
Clone	Make a copy of the selected video filter profile.
Delete	Remove the selected video filter profile.
Search	Enter a search term to find in the video filter profile list.
Name	The name of the video filter profile.
Comments	An optional description of the video filter profile.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a video filter profile

Click *Create New* to open the *New Video Filter Profile* window.



Select a video filter profile and then click *Edit* to open the *Edit Video Filter Profile* window.

Configure the following settings in the *New Video Filter Profile* window and then click *OK*:

Name	The name of the video filter profile.
Comments	Optional description of thevideo filter profile.
FortiGuard category based filter	Enable to use FortiGuard categories. If the device is not licensed for the FortiGuard web-filtering service, traffic can be blocked by enabling this option.
Allow/Monitor/Block	Select the action for each FortiGuard category: *Allow*, *Monitor*, or *Block*.
YouTube	
Channel override list	Create or edit a YouTube channel override list. See Create or edit a channel override entry on page 292.
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.

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
```

Create or edit a channel override entry

You can override the video filter with channel override entries.

To create a channel override entry:

1. Go to *Security Profiles* > *Video Filter*.
2. Click *Create New* or select a video filter profile and then click *Edit*.
3. Click *Create New*. The *New Channel override Entry* window opens.
4. Enter the YouTube channel ID.
5. Enter a description of the YouTube channel.
6. Select the action to take when the pattern is matched:
   - *Allow*: Allow access to the YouTube channel.
   - *Monitor*: Monitor traffic to and from the YouTube channel.
   - *Block*: Block access to the YouTube channel and display a replacement message. SeeReplacement Messages on page 492.
7. Click *OK* to save the channel override entry.
8. Click *OK* to save the changes to the video filter profile.

To edit a channel override entry:

1. Go to *Security Profiles* > *Video Filter*.
2. Click *Create New* or select a video filter profile and then click *Edit*.
3. Select a channel override entry and then click *Edit*.
4. Edit the entry settings as required.
5. Click *OK* to save your changes to the channel override entry.
6. Click *OK* to save the changes to the video filter profile.

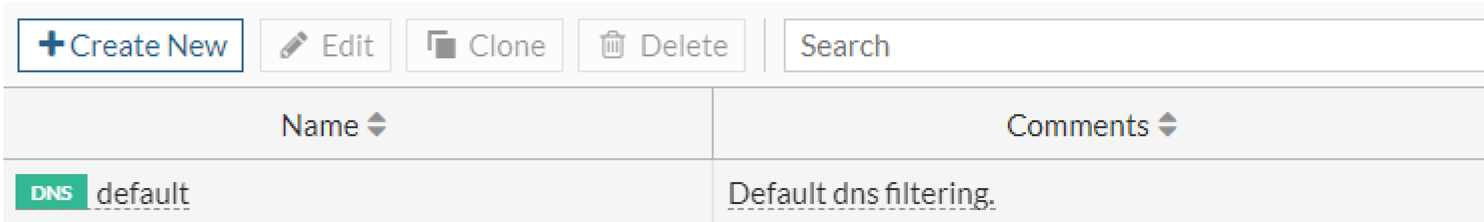
DNS Filter

You can configure DNS filtering to allow, block, or monitor access to web content according to FortiGuard categories. When DNS filtering is enabled, your FortiProxy unit must use the FortiGuard DNS service for DNS lookups. DNS lookup requests sent to the FortiGuard DNS service return with an IP address and a domain rating that includes the FortiGuard category of the web page.

If that FortiGuard category is set to block, the result of the DNS lookup is not returned to the requester. If the category is set to redirect, then the address returned to the requester points at a FortiGuard redirect page.

You can also allow or monitor access based on the FortiGuard category.

To view available DNS filter profiles, go to *Security Profiles* > *DNS Filter*.



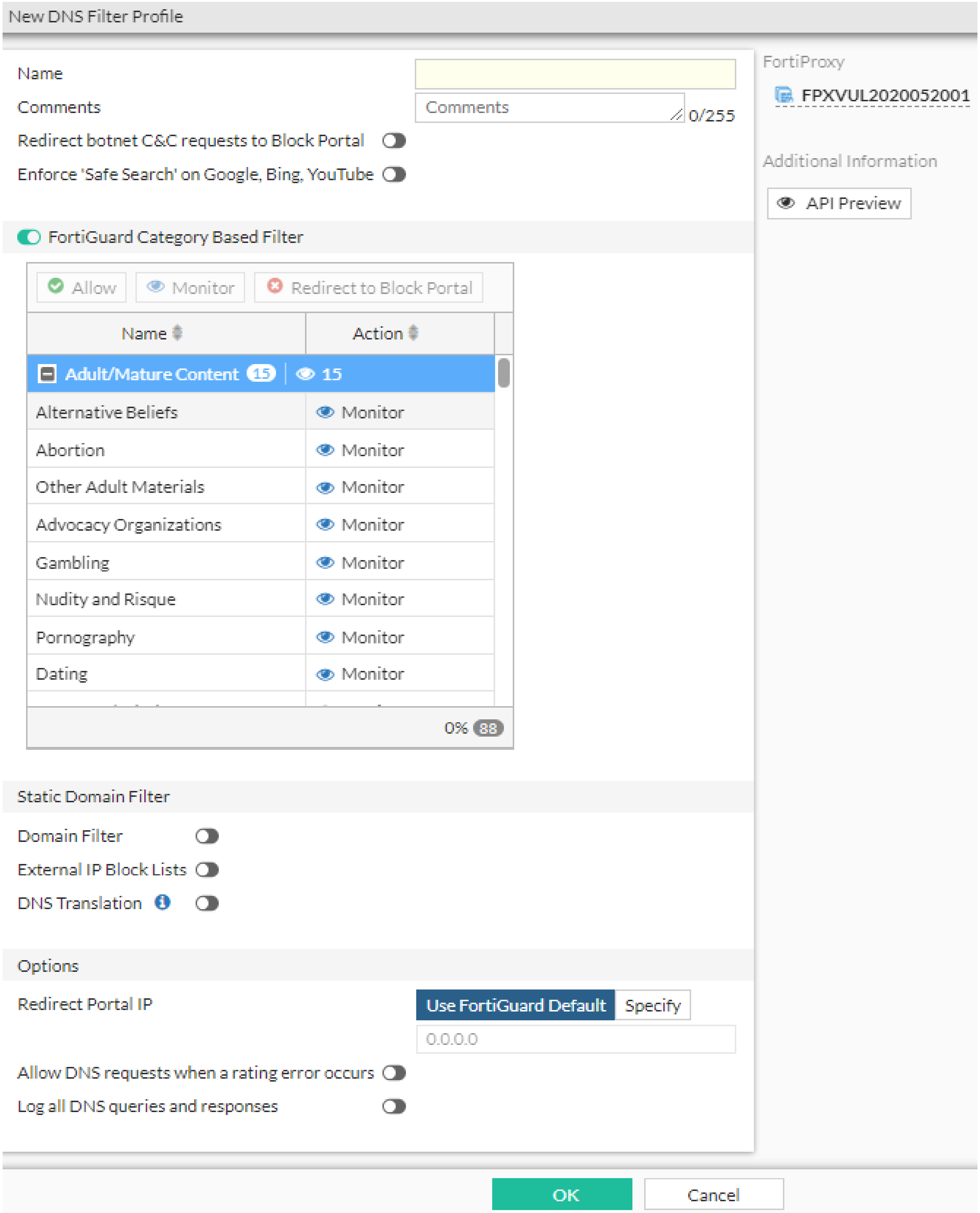
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a DNS filter profile. See Create or edit a DNS filter profile on page 293.
Edit	Modify the selected DNS filter profile. See Create or edit a DNS filter profile on page 293.
Clone	Make a copy of the selected DNS filter profile.
Delete	Remove the selected DNS filter profile.
Search	Enter a search term to find in the DNS filter list.
Name	The name of the DNS filter profile.
Comments	An optional description of the DNS filter profile.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a DNS filter profile

Click *Create New* to open the *New DNS Filter Profile* window.


New DNS Filter Profile
Name
Comments
Comments
0/255
Redirect botnet C&C requests to Block Portal
Enforce 'Safe Search' on Google, Bing, YouTube
FortiGuard Category Based Filter
Allow
Monitor
Redirect to Block Portal
Name
Action
Adult/Mature Content 15
15
Alternative Beliefs
Monitor
Abortion
Monitor
Other Adult Materials
Monitor
Advocacy Organizations
Monitor
Gambling
Monitor
Nudity and Risque
Monitor
Pornography
Monitor
Dating
Monitor
0% 88
Static Domain Filter
Domain Filter
External IP Block Lists
DNS Translation
Options
Redirect Portal IP
Use FortiGuard Default
Specify
0.0.0.0
Allow DNS requests when a rating error occurs
Log all DNS queries and responses
FortiProxy
FPXVUL2020052001
Additional Information
API Preview
OK
Cancel

Configure the following settings and then click *OK*:

Name	The name of the DNS filter profile.
Comments	Optional description of the DNS filter profile.
Redirect botnet C&C requests to Block Portal	FortiGuard Service continually updates the botnet C&C domain list. The botnet C&C domain blocking feature can block the botnet website access at the DNS name resolving stage. This provides additional protection for your network.
Enforce 'Safe search' on Google, Bing, YouTube	The DNS safe search option helps avoid explicit and inappropriate results in the Google, Bing, and YouTube search engines. The FortiProxy responds with content filtered by the search engine.
Restrict YouTube Access	Select the *Strict* or *Moderate* level of restriction for YouTube access. This option is available only if *Enforce 'Safe search' on Google, Bing, YouTube* is enabled.
FortiGuard category based filter	Enable if you want to use FortiGuard categories. If the device is not licensed for the FortiGuard web-filtering service, traffic can be blocked by enabling this option.
Allow/Monitor/Redirect to Block Portal	Select the action for each FortiGuard category: *Allow*, *Monitor*, or *Redirect to Block Portal*.
Static Domain Filter	
Domain Filter	Enable to create or edit domain filters. See Create or edit a domain filter on page 296.
External IP Block Lists	Enable to create or select a list of external IP addresses to block. See External Connectors on page 581.
DNS Translation	This setting allows you to translate a DNS resolved IP address to another IP address you specify on a per-policy basis. See Create or edit a DNS translation entry on page 297.
Options	
Redirect Portal IP	If you want the FortiProxy unit to use the portal IP address to replace the resolved IP address in the DNS response packet, select *Use FortiGuard Default* or *Specify*. If you select *Specify*, enter the portal IP address.
Allow DNS requests when a rating error occurs	Enable to allow access to domains that return a rating error from the web filter service. If your unit is temporarily unable to contact the FortiGuard service, this setting determines what access the unit allows until contact is re-established. If enabled, users will have full unfiltered access to all domains. If disabled, users will not be allowed access to any domains.
Log all DNS queries and responses	Enable if you want DNS queries and responses logged.
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.

To edit a DNS filter profile:

1. Go to *Security Profiles > DNS Filter*.
2. Select the profile you want to edit and then click *Edit* from the toolbar or double-click on the profile name in the list. The *Edit DNS Filter Profile* window opens.
3. Edit the information as required and then select *OK* to save your changes.

Create or edit a domain filter

The DNS static domain filter allows you to block, exempt, or monitor DNS requests by using IPS to look inside DNS packets and match the domain being looked up with the domains on the static URL filter list. If there is a match the DNS request can be blocked, exempted, monitored, or allowed.

If blocked, the DNS request is blocked and so the user cannot look up the address and connect to the site.

If exempted, access to the site is allowed even if another method is used to block it.

To create a domain filter:

1. Go to *Security Profiles > DNS Filter*.
2. Click *Create New* or select a DNS filter profile and then click *Edit*.
3. Enable *Domain Filter*.
4. In the *Domain Filter* table, select *Create New*. The *Create Domain Filter* window opens.
5. Enter the domain to filter in the *Domain* field. Enter a top-level domain suffix (for example, “com” without the leading period) to block access to all web sites with this suffix.
6. Select the type of pattern to match: *Simple*, *Reg. Expression*, or *Wildcard*.
7. Select the action to take when the pattern is matched:
   - *Redirect to Block Portal*: If a DNS query domain name rating belongs to the block category, the query is blocked and redirected.
   - *Allow*: Allow access to any domain that matches the domain pattern.
   - *Monitor*: Monitor traffic to and from domains matching the domain pattern.
8. Enable or disable the status of the filter to make the filter active or inactive.
9. Click *OK* to save the domain filter.
10. Click *OK* to save the DNS filter profile.

To edit a domain filter:

1. Go to *Security Profiles > DNS Filter*.
2. Click *Create New* or select a DNS filter profile and then click *Edit*.

3. Enable *Domain Filter*.
4. In the Domain Filter table, double-click on a filter or select the filter and then click *Edit* in the toolbar.
5. Edit the filter settings as required.
6. Click *OK* to save your changes to the domain filter.
7. Click *OK* to save the DNS filter profile.

Create or edit a DNS translation entry

This setting allows you to translate a DNS resolved IP address to another IP address you specify on a per-policy basis.

For example, website A has a public address of 1.2.3.4. However, when your internal network users visit this website, you want them to connect to the internal host 192.168.3.4. You can use DNS translation to translate the DNS resolved address 1.2.3.4 to 192.168.3.4. Reverse use of DNS translation is also applicable. For example, if you want a public DNS query of your internal server to get a public IP address, then you can translate a DNS resolved private IP to a public IP address.

To create a DNS translation entry:

1. Go to *Security Profiles* > *DNS Filter* and enable *DNS Translation*.
2. In the *DNS Translation* table, select *Create New*. The *New DNS Translation* window opens.
3. Select the type of IP address to translate, either *IPv4* or *IPv6*.
4. In the *Original Destination* field, enter the domain's original IP address.
5. In the *Translation Destination* field, enter the IP address that you want used instead of the original IP address.
6. Enter the network mask.
7. Enable or disable the status.
8. Click *OK* to save the DNS translation entry.
9. Click *OK* to save the DNS filter profile.

To edit a DNS translation entry:

1. Go to *Security Profiles* > *DNS Filter* and enable *DNS Translation*.
2. In the *DNS Translation* table, double-click on an entry or select an entry and then click *Edit* in the toolbar.
3. Edit the settings as required.
4. Click *OK* to save the DNS translation entry.
5. Click *OK* to save the DNS filter profile.

Application Control

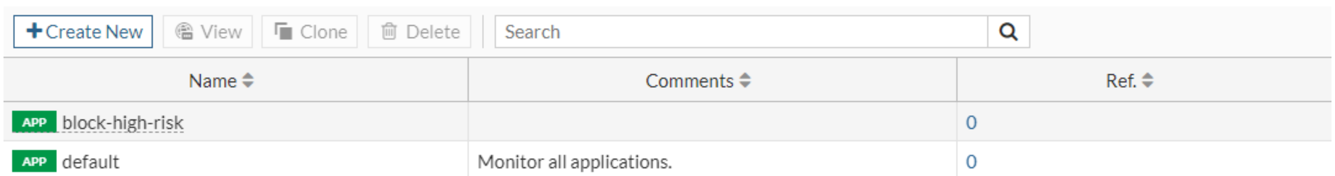
Using the Application Control feature, your FortiProxy unit can detect and take action against network traffic depending on the application generating the traffic. Based on FortiProxy Intrusion Protection protocol decoders, application control is a user-friendly and powerful way to use Intrusion Protection features to log and manage the behavior of application traffic passing through the FortiProxy unit. Application control uses IPS protocol decoders that can analyze network traffic to detect application traffic even if the traffic uses nonstandard ports or protocols. Application control supports detection for traffic using HTTP protocol (versions 1.0, 1.1, and 2.0).

The FortiProxy unit can recognize the network traffic generated by a large number of applications. You can create application control sensors that specify the action to take with the traffic of the applications you need to manage and the network on which they are active, and then add application control sensors to the firewall policies that control the network traffic you need to monitor.

Fortinet is constantly adding to the list of applications detected through maintenance of the FortiGuard Application Control Database. This database is part of the FortiGuard Intrusion Protection System Database because intrusion protection protocol decoders are used for application control and both of these databases have the same version number.

You can see the complete list of applications supported by FortiGuard Application Control on the FortiGuard site or https://fortiguard.com/appcontrol. This web page lists all of the supported applications. You can select any application name to see details about the application.

To view available application sensors, go to *Security Profiles > Application Control*.



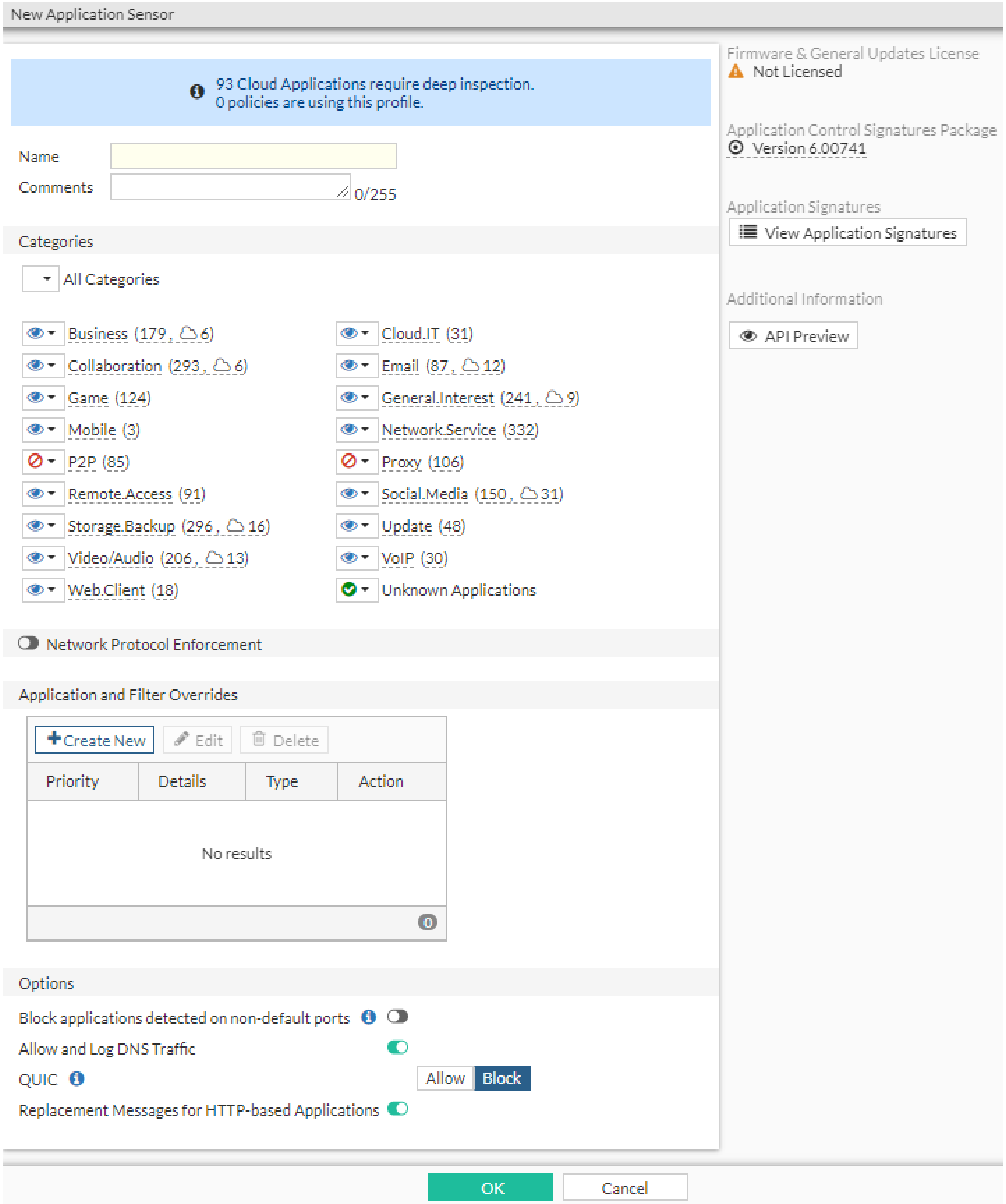
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create an application sensor. See Create or edit an application sensor on page 298.
Edit	Modify the selected application sensor. See Create or edit an application sensor on page 298.
Clone	Make a copy of the selected application sensor.
Delete	Remove the selected application sensor.
Search	Enter a search term to search the application sensor list.
Name	The name of the application sensor.
Comments	An optional description of the application sensor.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit an application sensor

To create an application sensor, click *Create New*.


New Application Sensor
93 Cloud Applications require deep inspection.
0 policies are using this profile.
Name
Comments
0/255
Categories
All Categories
Business (179, 6)
Cloud.IT (31)
Collaboration (293, 6)
Email (87, 12)
Game (124)
General.Interest (241, 9)
Mobile (3)
Network.Service (332)
P2P (85)
Proxy (106)
Remote.Access (91)
Social.Media (150, 31)
Storage.Backup (296, 16)
Update (48)
Video/Audio (206, 13)
VoIP (30)
Web.Client (18)
Unknown Applications
Network Protocol Enforcement
Application and Filter Overrides
Create New
Edit
Delete
Priority
Details
Type
Action
No results
0
Options
Block applications detected on non-default ports
Allow and Log DNS Traffic
QUIC
Allow
Block
Replacement Messages for HTTP-based Applications
Firmware & General Updates License
Not Licensed
Application Control Signatures Package
Version 6.00741
Application Signatures
View Application Signatures
Additional Information
API Preview
OK
Cancel

Configure the following settings and then select *OK*:

Name	The name of the application sensor.
Comments	Optional description of the application sensor.
Categories	Select an action for *All Categories* or for each category of applications: • *Monitor*—This action allows the targeted traffic to continue on through the FortiProxy unit but logs the traffic for analysis. • *Allow*—This action allows the targeted traffic to continue on through the FortiProxy unit. • *Block*—This action prevents all traffic from reaching the application and logs all occurrences. • *Quarantine*—This action allows you to quarantine or block access to an application for a specified duration that can be entered in days, hours, and minutes. The default is 5 minutes. You can also select *View Signatures* or *View Cloud Signatures* to see a list of signatures for some categories.
Network Protocol Enforcement	Enable and configure network services on certain ports and determine the violation action. SeeCreate or edit a default network service on page 301. Protocol enforcement allows you to configure networking services (for example, FTP, HTTP, and HTTPS) on known ports (for example, 21, 80, or 43). For protocols that have not been added to the allowlist for certain ports, the IPS engine performs the violation action to block, allow, or monitor that traffic.
Application and Filter Overrides	Application overrides allow you to choose individual applications. To add an application override, see Add or edit an application override on page 302. Filter overrides can be added based on behavior, application category, popularity, protocol, risk, technology, or vendor subtypes. To add a filter override, see Add or edit a filter override on page 302.
Allow and Log DNS Traffic	Enable to allow DNS traffic.
Block applications detected on non-default ports	For monitor and allow actions, applications are blocked if they are detected on nondefault ports (as defined in FortiGuard application signatures). Block actions still block all traffic for the application, regardless of port.
QUIC	Select *Allow* if you want the FortiProxy unit to inspect Google Chrome packets for a QUIC header. Select *Block* to force Google Chrome to use HTTP2/TLS 1.2.
Replacement Messages for HTTP-based Applications	Enable to display replacement messages for HTTP-based applications.
View Application Signatures	Select to see a list of predefined application signatures. To create an application signature, see Create or edit an application signature on page 318.
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.

To edit an application sensor:

1. From the application sensor list, select the sensor that you need to edit and then click *Edit* from the toolbar or double-click on the sensor name in the list. The *Edit Application Sensor* window opens.
2. Edit the information as required and then select *OK* to save your changes.

Create or edit a default network service

Protocol enforcement allows you to configure networking services (e.g. FTP, HTTP, HTTPS) on known ports (e.g. 21, 80, 443). For protocols that are not allowlisted under select ports, the IPS engine performs the violation action to block, allow, or monitor that traffic.

This feature can be used in the following scenarios:

- When one protocol dissector confirms the service of network traffic, protocol enforcement can check whether the confirmed service is allowlisted under the server port. If it is not allowlisted, the traffic is considered a violation and IPS can take the action specified in the configuration (block or monitor it).
- When there is no confirmed service for the network traffic, the traffic is considered a service violation if IPS dissectors rule out all of the services enforced under its server port.

In an applicable profile, a default-network-service list can be created to associate well known ports with accepted services.

Default network services can be added or edited, as required.

To create a default network service:

1. Go to *Security Profiles > Application Control*.
2. Click *Create New* or select an application sensor and then click *Edit*.
3. Enable *Network Protocol Enforcement*.
4. In the *Network Protocol Enforcement* section, select *Create New*.
5. Enter a port number.
6. Enter one or more protocols to allow on the specified port.
7. Select to block or monitor protocols that are not specified in the *Enforce protocols* field.
8. Click *OK*.

To edit a default network service:

1. Go to *Security Profiles > Application Control*.
2. Click *Create New* or select an application sensor and then click *Edit*.
3. Enable *Network Protocol Enforcement*.

4. Select the default network service that you want to edit and then click *Edit* from the toolbar. The *Edit Default Network Service* window opens.
5. Edit the information as required and then click *OK* to apply your changes.

Add or edit an application override

Application overrides can be added or edited as required.

To add predefined signatures:

1. Go to *Security Profiles > Application Control*.
2. Click *Create New* or select an application sensor and then click *Edit*.
3. In the *Application and Filter Overrides* section, click *Create New*.
4. Select *Application* for the override type.
5. Select the action to take: *Monitor*, *Allow*, *Block*, or *Quarantine*.
6. Use the search field to narrow down the list of possible signatures by a series of attributes.
7. Click *OK*.

To edit a predefined signature:

1. Go to *Security Profiles > Application Control*.
2. Click *Create New* or select an application sensor and then click *Edit*.
3. In the *Application and Filter Overrides* section, select the application override to edit and then click *Edit* from the toolbar.
4. Edit the information as required and then click *OK* to apply your changes.

Add or edit a filter override

Filters overrides can be added or edited as required.

To create a filter override:

1. Go to *Security Profiles > Application Control*.
2. Click *Create New* or select an application sensor and then click *Edit*.
3. In the *Application and Filter Overrides* section, click *Create New*.
4. Select *Filter* for the override type.
5. Select the action to take: *Monitor*, *Allow*, *Block*, or *Quarantine*.
6. Use the search field to narrow down the list of possible filters by a series of attributes.
7. Click *OK*.

To edit a filter override:

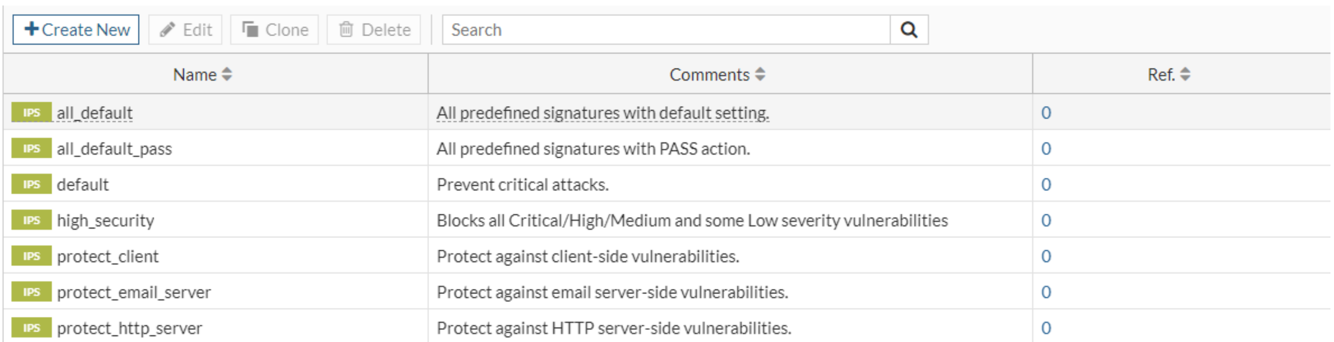
1. Go to *Security Profiles > Application Control*.
2. Click *Create New* or select an application sensor and then click *Edit*.
3. In the *Application and Filter Overrides* section, select the filter override to edit and then click *Edit* from the toolbar.
4. Edit the information as required and then click *OK* to apply your changes.

Intrusion Prevention

The Intrusion Prevention System (IPS) combines signature detection and prevention with low latency and excellent reliability. With intrusion protection, you can create multiple IPS sensors, each containing a complete configuration based on signatures. Then, you can apply any IPS sensor to any security policy.

This section describes how to configure the Intrusion Prevention settings.

To view available IPS sensors, go to *Security Profiles > Intrusion Prevention*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

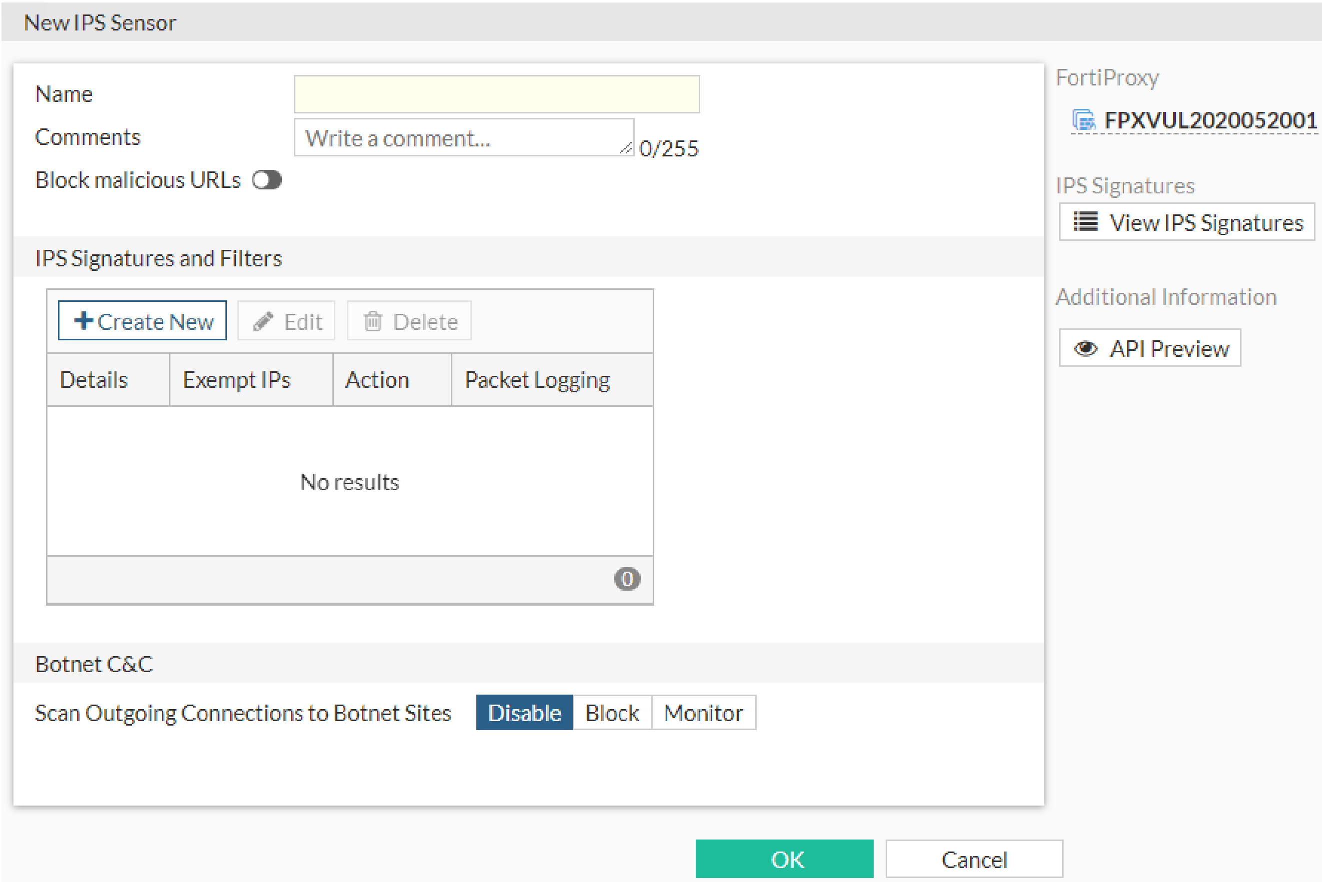
Create New	Create an IPS sensor. See Create or edit an IPS sensor on page 303.
Edit	Modify the selected IPS sensor. See Create or edit an IPS sensor on page 303.
Clone	Make a copy of the selected IPS sensor.
Delete	Remove the selected IPS sensor.
Search	Enter a search term to find in the IPS sensor list.
Name	The name of the IPS sensor.
Comments	An optional description of the IPS sensor.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit an IPS sensor

The Intrusion Prevention System (IPS) combines signature detection and prevention with low latency and excellent reliability. With intrusion protection, you can create multiple IPS sensors, each containing a complete configuration based on signatures. Then, you can apply any IPS sensor to any security policy.

IPS sensors can be added, edited, cloned, and deleted as required.

To create an IPS sensor, go to *Security Profiles > Intrusion Prevention* and click *Create New*.



Configure the following settings and then select *OK* to save your changes:

Name	The name of the IPS sensor.
Comments	Optional description of the IPS sensor.
Block malicious URLs	Enable this setting to block malicious URLs that FortiSandbox finds. Your FortiProxy unit must be connected to a registered FortiSandbox.
IPS Signatures and Filters	Add or edit an IPS signature or filter. See Add or edit an IPS signature or filter on page 305. While individual signatures can be added to a sensor, a filter allows you to add multiple signatures to a sensor by specifying the characteristics of the signatures to be added.
Scan Outgoing Connections to Botnet Sites	Select *Block* or *Monitor* to enable botnet blocking across all traffic that matches the policy.
View IPS Signatures	Select to see a list of predefined IPS signatures. To create an IPS signature, see Create or edit an IPS signature on page 322.
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.

To edit an IPS sensor:

1. From the IPS sensor list, select the sensor that you need to edit and then click *Edit* from the toolbar or double-click on the sensor name in the list. The *Edit IPS Sensor* window opens.
2. Edit the information as required and then select *OK* to save your changes.

Add or edit an IPS signature or filter

You can add or edit IPS signatures and filters.

To create a filter:

1. Go to *Security Profiles* > *Intrusion Prevention*.
2. In the *IPS Signatures and Filters* section, select *Create New*.
3. In the *Add Signatures* window, select *Filter*.
4. For the action, select *Allow*, *Monitor*, *Block*, *Reset*, *Default*, or *Quarantine*.
5. Enable or disable packet logging.
6. Enable the status to make the filter active.
7. Use the *Filter* field to select filters.
8. Use the search field to narrow down the list of possible signatures by a series of attributes.
9. Click *OK*.

To create a signature:

1. Go to *Security Profiles* > *Intrusion Prevention*.
2. In the *IPS Signatures and Filters* section, select *Create New*.
3. In the *Add Signatures* window, select *Signature*.
4. For the action, select *Allow*, *Monitor*, *Block*, *Reset*, *Default*, or *Quarantine*.
5. Enable or disable packet logging.
6. Enable the status to make the filter active.
7. Select *Default* or *Specify* for the rate-based settings. If you select *Specify*, enter the number of incidents per minute in the *Threshold* field, enter the number of seconds after which the block will be removed in the *Duration (seconds)* field, and select whether the rate-based settings use the source IP address, the destination IP address, or any IP address.
8. If you want to exempt certain IP addresses from the signature, click *Edit IP Exemptions* and add the source IP address and netmask and the destination IP address and netmask.
9. Use the search field to narrow down the list of possible signatures by a series of attributes.
10. Click *OK*.

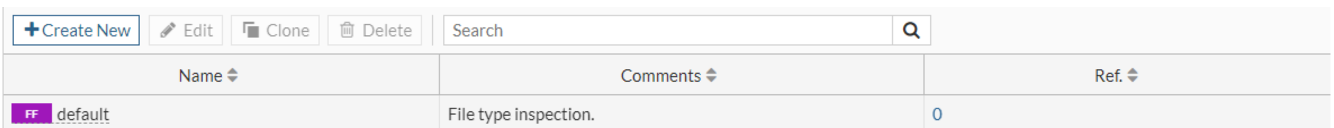
To edit a filter or signature:

1. Go to *Security Profiles > Intrusion Prevention*.
2. In the *IPS Filters* section, select the filter or signature that you want to edit and then click *Edit* from the toolbar.
3. Edit the information as required and then select *OK* to apply your changes.

File Filter

The file filter allows the FortiProxy unit to block files passing through based on file type based on the file's metadata only and not on file size or file content. A DLP sensor must be configured to block files based on size or content, such as SSN numbers, credit card numbers, or regular expression pattern. The file filter can be applied directly to firewall policies.

To view available file filter profiles, go to *Security Profiles > File Filter*.



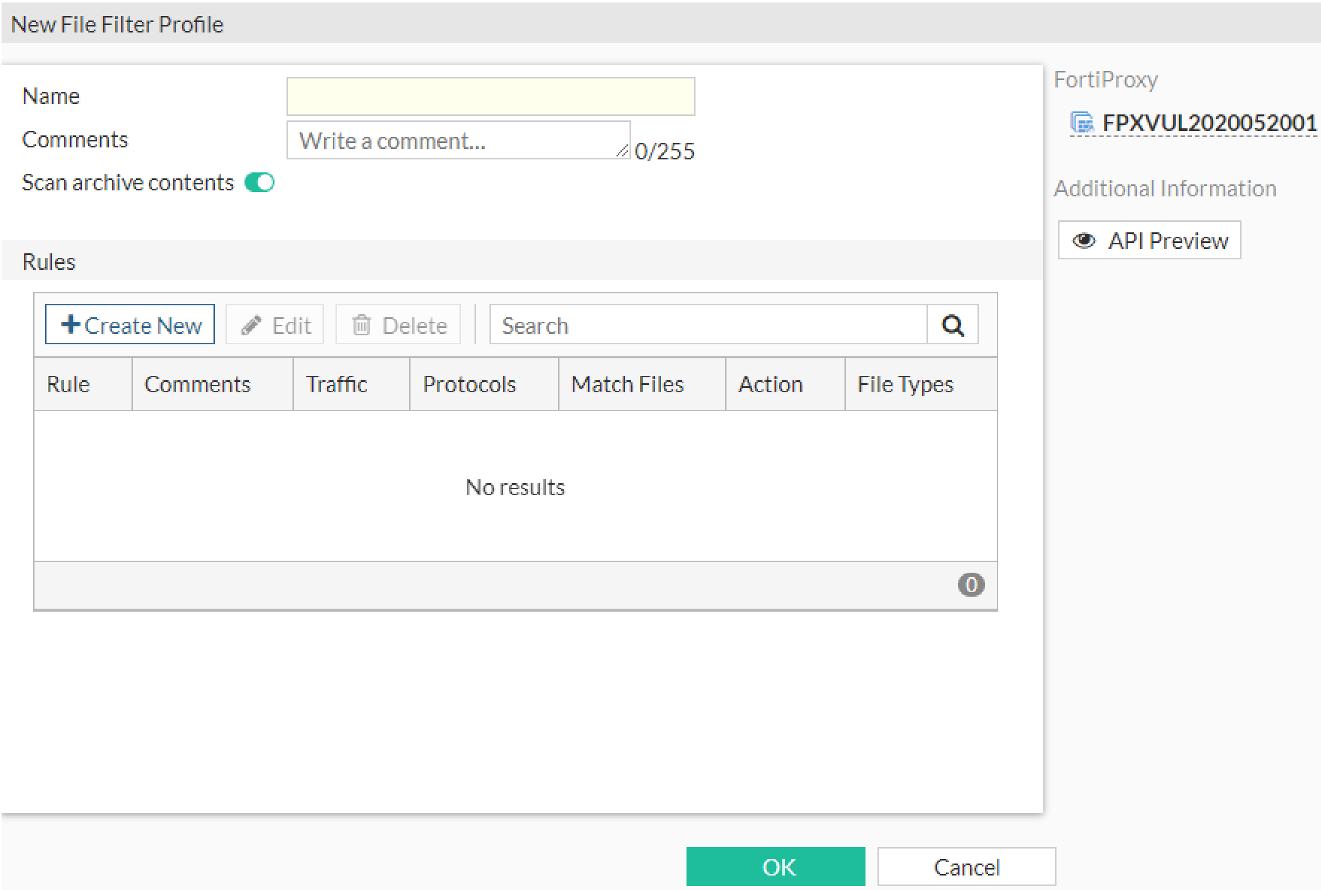
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a file filter profile. See Create or edit a file filter profile on page 306.
Edit	Modify the selected file filter profile. See Create or edit a file filter profile on page 306.
Clone	Make a copy of the selected file filter profile.
Delete	Remove the selected file filter profile.
Search	Enter a search term to find in the file filter profile list.
Name	The name of the file filter profile.
Comments	An optional description of the file filter profile.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.
Scan Archive Contents	Whether the scanning of archive contents has been enabled or disabled.

Create or edit a file filter profile

Click *Create New* to open the *New File Filter Profile* window.



Select a file filter profile and then click *Edit* to open the *Edit File Filter Profile* window.

Configure the following settings in the *New File Filter Profile* window and then click *OK*:

Name	The name of the file filter profile.
Comments	Optional description of the file filter profile.
Scan archive contents	Enable if you want the archive contents to be scanned.
Rules	Create or edit file filter rules. See Create or edit a file filter rule on page 308.
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.

Create or edit a file filter rule

You can create or edit rules for the file filter profile.

To create a file filter rule:

1. Go to *Security Profiles* > *File Filter*.
2. Click *Create New* or select a file filter profile and then click *Edit*.
3. In the *Rules* table, select *Create New*. The *Create New File Filter Rule* window opens.
4. Enter the name of the file filter rule.
5. Enter an optional description of the file filter rule.
6. Select one or more protocols.
7. Select *Incoming*, *Outgoing*, or *Both*.
8. Enable *Password-protected only* if you want to just match password-protected files.
9. Select the file types to match.
10. Select the action to take when the rule is matched:
    - *Block*: Block access to any file that matches the rule.
    - *Monitor*: Monitor traffic to and from files matching the rule.
11. Click *OK* to save the file filter rule.
12. Click *OK* to save the file filter profile.

To edit a file filter rule:

1. Go to *Security Profiles* > *File Filter*.
2. Click *Create New* or select a file filter profile and then click *Edit*.
3. In the *Rules* table, double-click on a rule or select the rule and then click *Edit* in the toolbar.
4. Edit the rule settings as required.
5. Click *OK* to save your changes to the file filter rule.
6. Click *OK* to save the file filter profile.

SSL/SSH Inspection

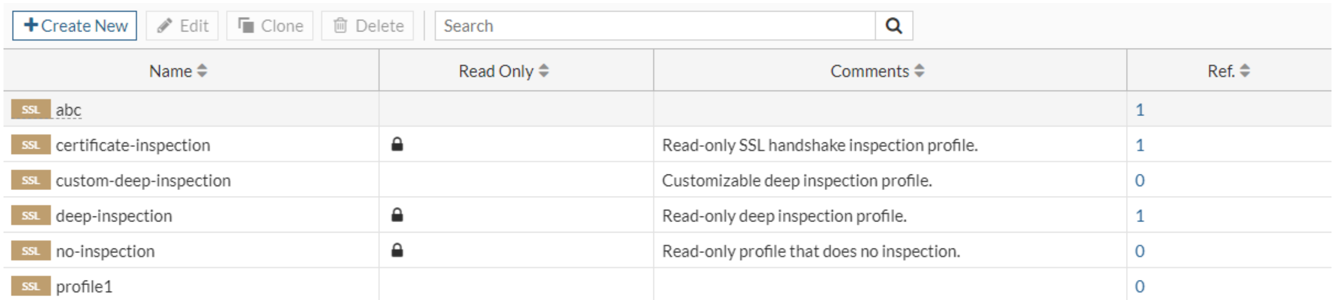
Secure sockets layer (SSL) content scanning and inspection allows you to apply antivirus scanning, web filtering, and email filtering to encrypted traffic. You can apply SSL inspection profiles to firewall policies.

Deep inspection (also known as SSL/SSH inspection) is typically applied to outbound policies where destinations are unknown. Depending on your policy requirements, you can configure the following:

- Which CA certificate will be used to decrypt the SSL encrypted traffic
- Which SSL protocols will be inspected
- Which ports will be associated with which SSL protocols for inspection
- Whether or not to allow invalid SSL certificates
- Whether or not SSH traffic will be inspected
- Which addresses or web category allowlists can bypass SSL inspection

SSL/SSH inspection profile

To view the available SSL/SSH inspection profiles, go to *Security Profiles > SSL/SSH Inspection*.



Name	Read Only	Comments	Ref.
abc			1
certificate-inspection	🔒	Read-only SSL handshake inspection profile.	1
custom-deep-inspection		Customizable deep inspection profile.	0
deep-inspection	🔒	Read-only deep inspection profile.	1
no-inspection	🔒	Read-only profile that does no inspection.	0
profile1			0

Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create an SSL/SSH inspection profile. See Create or edit an SSL/SSH inspection profile on page 309.
Edit	Modify the selected SSL/SSH inspection profile. See Create or edit an SSL/SSH inspection profile on page 309.
Clone	Make a copy of the selected SSL/SSH inspection profile.
Delete	Remove the selected SSL/SSH inspection profile.
Search	Enter a search term to find in the SSL/SSH inspection profile list.
Name	The name of the SSL/SSH inspection profile.
Read Only	The `certificate-inspection`, `deep-inspection`, and `no-inspection` profiles are read only and cannot be edited.
Comments	An optional description of the SSL/SSH inspection profile.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

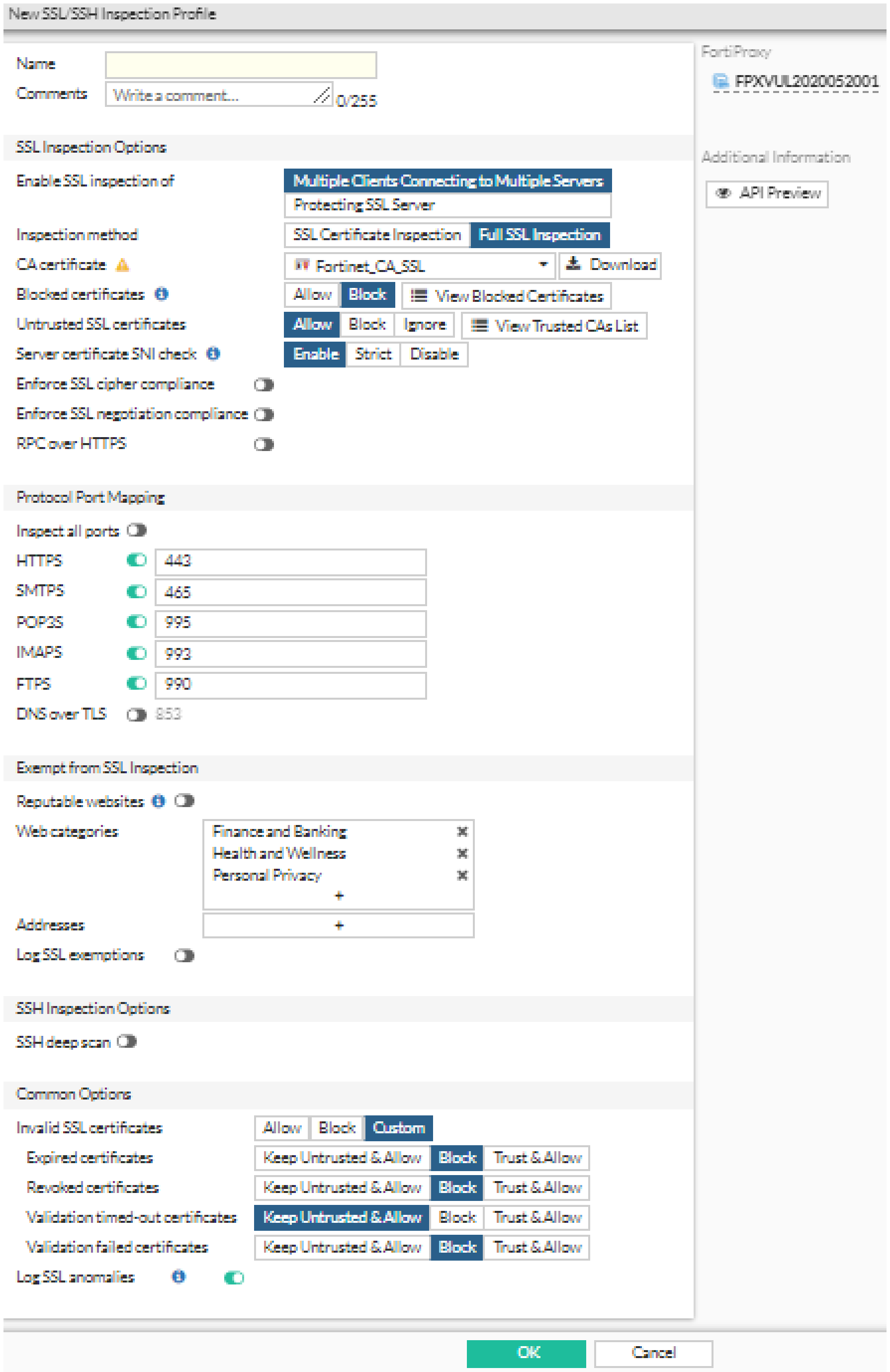
Create or edit an SSL/SSH inspection profile

The FortiProxy unit includes four preloaded SSL/SSH inspection profiles, three of which are read-only and can be cloned:

- `certificate-inspection`
- `deep-inspection`
- `no-inspection`

The `custom-deep-inspection` profile can be edited, or you can create your own SSL/SSH inspection profiles.

To create an SSL/SSH inspection profile, go to *Security Profiles > SSL/SSH Inspection* and click *Create New*.



Configure the following settings and then click *OK* to save your changes:

Name	Give the profile an easily identifiable name that references its intent.
Comments	Enter any additional information that might be needed by administrators, as a reminder of the profile's purpose and scope. This setting is optional.
SSL Inspection Options	

Enable SSL Inspection of	• *Multiple Clients Connecting to Multiple Servers*—Select this option for generic policies where the destination is unknown. The *Exempt from SSL Inspection* and *Common Options* options are only available with this option enabled. • *Protecting SSL Server*—Select this option when setting up a profile customized for a specific SSL server with a specific certificate.
Server certificate	Click + and select a certificate or click *Create* to import a certificate. This option is available only when *Protecting SSL Server* is selected.
Inspection Method	This option is available only when *Multiple Clients Connecting to Multiple Servers* is selected. • *SSL Certificate Inspection*—Only inspects the certificate, not the contents of the traffic. • *Full SSL Inspection*—Inspects all of the traffic.
CA Certificate	Select a CA certificate from the drop-down menu or select *Download Certificate*.You need to have the certificate installed in your browser, or you might see certificate warnings. This option is available only when *Multiple Clients Connecting to Multiple Servers* is selected.
Blocked certificates	The FortiProxy unit receives Botnet C&C SSL connections from FortiGuard that contain SHA1 fingerprints of malicious certificates. By default, these certificates are blocked. Click *View Blocked Certificates* to see a detailed list.
Untrusted SSL certificates	Configure the action to take when a server certificate is not issued by a trusted CA. • *Allow*: Allow the untrusted server certificate. This is the default value. • *Block*: Block the session. • *Ignore*: This option is for Full SSL inspection only. It re-signs the server certificate as trusted. When configured in the GUI for certificate inspection, it has no effect, and the setting is not saved. Click *View Trusted CAs List* to see a list of the factory bundled and user imported CAs that are trusted by the FortiProxy unit.
Server certificate SNI check	Check the SNI in the hello message with the CN or SAN field in the returned server certificate. • *Enable*: If mismatched, use the CN in the server certificate to do URL filtering. • *Strict*: If mismatched, close the connection. • *Disable*: Server certificate SNI check is disabled.
Enforce SSL cipher compliance	Enable to enforce SSL cipher compliance.
Enforce SSL negotiation compliance	Enable to enforce SSL negotiation compliance.
RPC over HTTPS	Enable to allow RPC over HTTPS.

Protocol Port Mapping	To optimize the resources of the unit, enable or disable the mapping and inspection of protocols. The default port numbers are automatically filled in, but you can change them.
Exempt from SSL Inspection	Exempt web categories or specific addresses from SSL inspection. This section is available only when *Multiple Clients Connecting to Multiple Servers* and a protocol under *Protocol Port Mapping* are enabled.
Reputable Websites	Enable this option to exempt any websites identified by FortiGuard as reputable.
Web Categories	By default, the categories of *Finance and Banking*, *Health and Wellness*, and *Personal Privacy* have been added because they are most likely to require a specific certificate. Click + to add web categories to be exempt from SSL inspection.
Addresses	Click + to add web addresses to be exempt from SSL inspection.
Log SSL exemptions	Enable this option to log all SSL exemptions.
SSH Inspection Options	
SSH Deep Scan	Enable to perform SSH deep scan and then enter the SSH port to use for the SSH deep scan.
Common Options	This section is available only when *Multiple Clients Connecting to Multiple Servers* is selected.
Invalid SSL Certificates	• Select *Allow* to allow traffic with invalid certificate. • Select *Block* to block traffic with an invalid certificate. • Select *Custom* to display more options.
Expired certificates	Select the action to take when the server certificate is expired. The default action is block. This option is available only when *Custom* is selected.
Revoked certificates	Select the action to take when the server certificate is revoked. The default action is block. This option is available only when *Custom* is selected.
Validation timed-out certificates	Select the action to take when the server certificate validation times out. The default action is to keep untrusted and allow. This option is available only when *Custom* is selected.
Validation failed certificates	Select the action to take when the server certificate validation fails. The default action is block. This option is available only when *Custom* is selected.
Log SSL anomalies	Enable this option to record traffic sessions containing untrusted or expired certificates.
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.

SSL options can be configured in SSL/SSH profiles even when the protocol is disabled

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.

DNS inspection with DoT and DoH

DNS over TLS (DoT) and DNS over HTTPS (DoH) are supported in DNS inspection. The WAD is able to handle DoT and DoH and redirect DNS queries to the DNS proxy for further inspection.

To configure DNS inspection of DoT and DoH queries in the CLI:

1. Configure the SSL-SSH profile:

```
config firewall ssl-ssh-profile
    edit "ssl"
        config dot
            set status deep-inspection
            set client-certificate bypass
            set unsupported-ssl-version block
            set unsupported-ssl-cipher allow
            set unsupported-ssl-negotiation allow
            set expired-server-cert block
            set revoked-server-cert block
            set untrusted-server-cert allow
            set cert-validation-timeout allow
            set cert-validation-failure block
        end
    next
end
```

2. Configure the DNS filter profile:

```
config dnsfilter profile
    edit "dnsfilter"
        config ftgd-dns
            config filters
                edit 1
```

```
                    set category 30
                    set action block
                next
            end
        end
        set block-botnet enable
    next
end
```

3. Configure the firewall policy:

```
config firewall policy
    edit 1
        set srcintf "port1"
        set dstintf "port3"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set profile-protocol-options "protocol"
        set ssl-ssh-profile "ssl"
        set webfilter-profile "webfilter"
        set dnsfilter-profile "dnsfilter"
    next
end
```

Client authentication with an SSL client certificate for the Original Content Server

FortiProxy can provide a client certificate for authentication to the Original Content Server on behalf of a user.

To use the SSL client certificate for server authentication:

- Set the client certificate to `inspect` under the `config https` command.
- Set the status of the SSL client certificate to `keyring-list` or `ca-sign`.
  - The `keyring-list` setting matches the user name to the Common Name of the SSL client certificate in the keyring list for authenticated users. See SSL Keyring on page 93.
  - The `ca-sign` setting provides an SSL client certificate signed by a configured CA for authenticated users. The signed client certificate has the Common Name set to the authenticated user's user name.

  By default, the status of the SSL client certificate is set to `do-not-offer`, which means that the SSL client certificate is not provided.

To provide an SSL client certificate from the keyring list:

```
config firewall ssl-ssh-profile
   edit <profile_name>
      config https
         set client-certificate inspect
      end
      config ssl-client-certificate
         set status keyring-list
         set keyring-list <keyring_list_used_to_find_client_certificate>
      end
   next
end
```

To provide an SSL client certificate signed by a CA:

```
config firewall ssl-ssh-profile
   edit <profile_name>
      config https
         set client-certificate inspect
      end
      config ssl-client-certificate
         set status ca-sign
         set caname <CA_certficate_used_to_sign_client_certificate>
      end
   next
end
```

Use the FortiProxy CLI to specify which keyring list to use for the SSL client certificate. The universally unique identifiers (UUIDs) are automatically assigned. See SSL Keyring on page 93 for information about uploading keyring lists.

To specify the keyring list to use for the SSL client certificate:

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

Disable IP-based URL rating

You can disable IP-based URL rating for SSL-exemption and proxy-address objects. By default, IP -based URL rating is enabled.

To configure IP-based URL rating in an SSL/SSH inspection profile:

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

To configure IP-based URL rating in web proxy settings:

```
config firewall profile-protocol-options
    edit <protocol>
        config http
            set address-ip-rating {enable | disable}
        end
    next
end
```

Application Signatures

The FortiProxy predefined signatures cover common attacks. If you use an unusual or specialized application or an uncommon platform, add custom signatures based on the security alerts released by the application and platform vendors.

You can create custom IPS signatures and custom application signatures to further extend protection. For example, you can use custom IPS signatures to protect unusual or specialized applications or even custom platforms from known and unknown attacks.

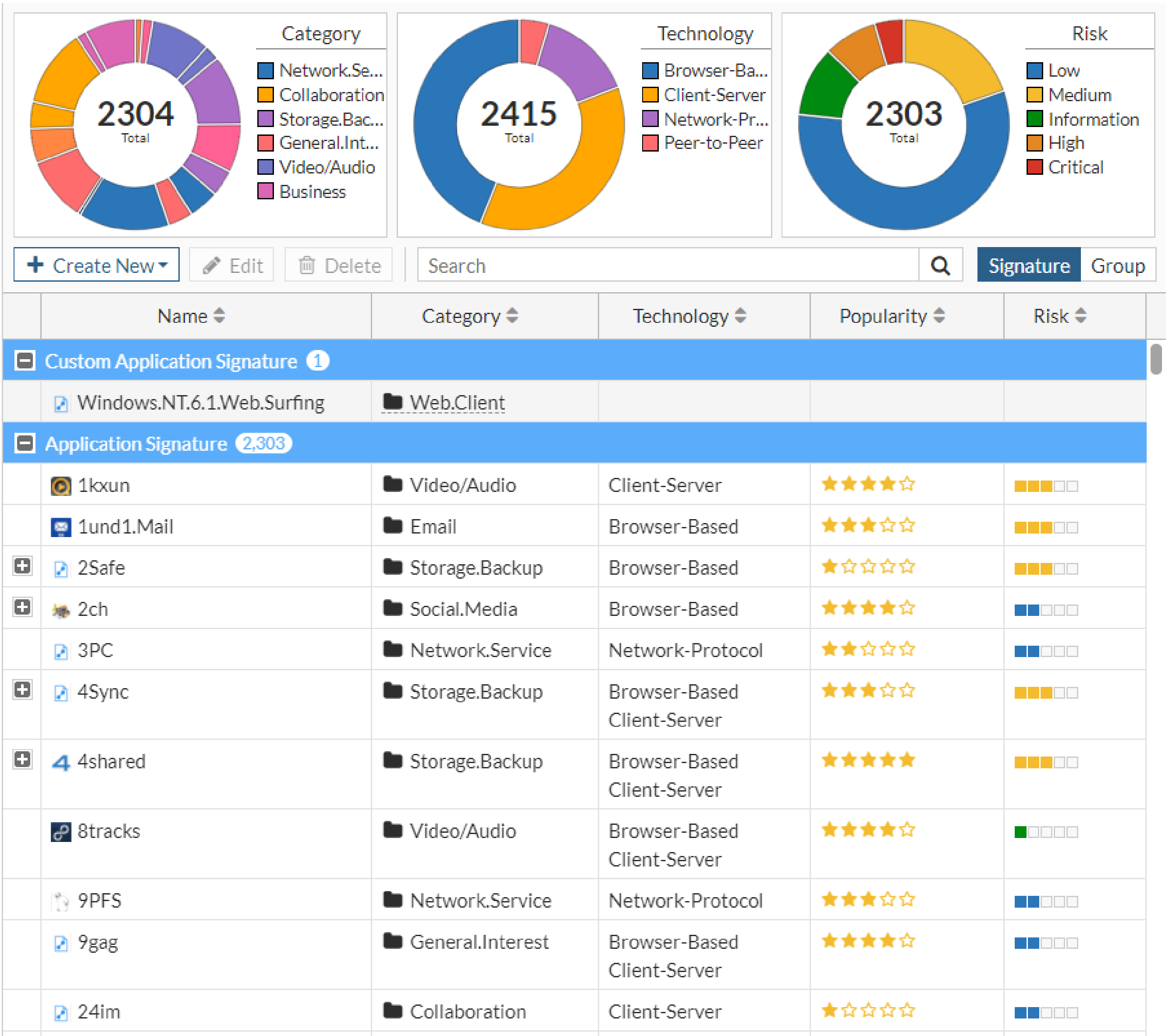
All custom signatures follow a particular syntax. Each begins with a header and is followed by one or more keywords. A custom signature definition is limited to a maximum length of 512 characters. A definition can be a single line or span multiple lines connected by a backslash (\) at the end of each line.

A custom signature definition begins with a header, followed by a set of keyword/value pairs enclosed by parenthesis [( )]. The keyword and value pairs are separated by a semicolon (;) and consist of a keyword and a value separated by a space. The following is the basic format of a definition:

```
HEADER (KEYWORD VALUE;)
```

You can use as many keyword/value pairs as required within the 512-character limit.

To view the available custom application signatures, go to *Security Profiles > Application Signatures* and click *Signature*. Custom application signatures are listed under a separate heading in the table. To create a custom application signature, see Create or edit an application signature on page 318.



To view the available custom application groups, go to *Security Profiles > Application Signatures* and click *Group*.To create a custom application group, see Create or edit an application group on page 319.

Create or edit an application signature

If you have to detect an application that is not already in the application list, you can create an application signature:

1. Go to *Security Profiles > Application Signatures* and select *Create New > Custom Application Signature*. You can also go to *Security Profiles > Application Control*, click *Create New*, click *View Application Signatures*, and select *Create New > Custom Application Signature*.
2. Enter a name (no spaces) for the application signature in the *Name* field.
3. Enter a brief description in the *Comments* field.

4. Enter the text for the signature in the *Signature* field. The syntax for signatures is described in Valid syntax on page 319.
5. Click *OK*.

You can edit application signatures that you have created. Select the application signature and then click *Edit*.

Valid syntax

The following table shows the valid characters and basic structure. For details about each keyword and its associated values, see Custom signature keywords on page 613.

Field	Valid Characters	Usage
HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.
KEYWORD	Each keyword must start with a pair of dashes (--) and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword identifies a parameter.
VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. **NOTE:** If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	The value is set specifically for a parameter identified by a keyword.

Create or edit an application group

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 comment <string>
      set type {application | filter}
      set application <application_ID>
      set category <2 | 3 | 5-8 | 12 | 15 | 17 | 21-23 | 25 | 26 | 28-32>
      set risk <1-5>
      set protocols <0-47 | all>
      set vendor <0-25 | all>
      set technology <all | 0-4>
      set behavior <all | 2 | 5 | 6 | 9>
      set popularity <1-6>
```

```
   next
end
```

To create an application group:

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

To edit an application group:

1. Go to *Security Profiles > Application Signatures*.
2. Select *Group*.
3. Select a group name and click *Edit*.
4. Make your changes.
5. Click *OK*.

IPS Signatures

The FortiProxy predefined signatures cover common attacks. If you use an unusual or specialized application or an uncommon platform, add custom signatures based on the security alerts released by the application and platform vendors.

You can create custom IPS signatures and custom application signatures to further extend protection. For example, you can use custom IPS signatures to protect unusual or specialized applications or even custom platforms from known and unknown attacks.

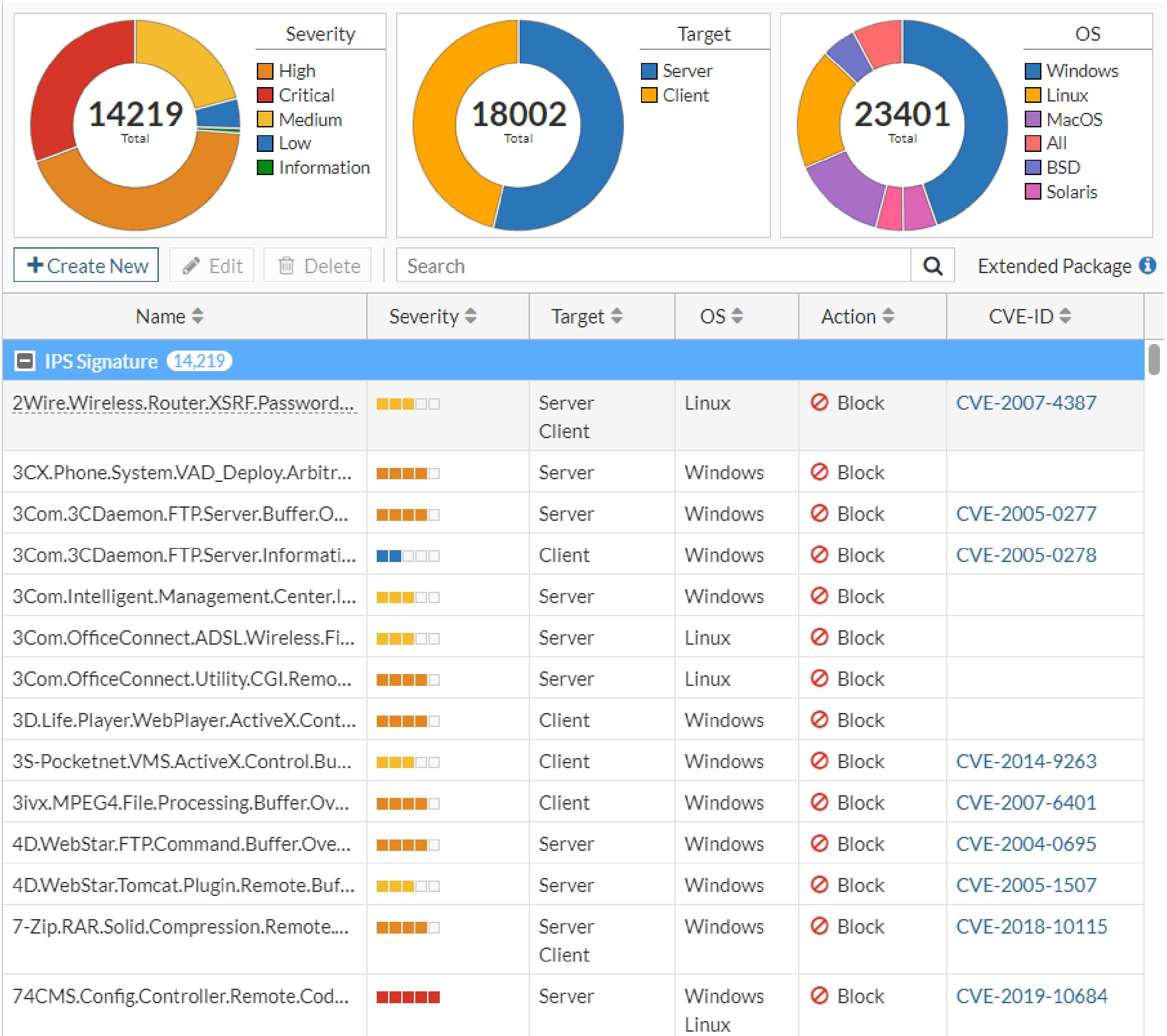
All custom signatures follow a particular syntax. Each begins with a header and is followed by one or more keywords. A custom signature definition is limited to a maximum length of 512 characters. A definition can be a single line or span multiple lines connected by a backslash (\) at the end of each line.

A custom signature definition begins with a header, followed by a set of keyword/value pairs enclosed by parenthesis [( )]. The keyword and value pairs are separated by a semicolon (;) and consist of a keyword and a value separated by a space. The following is the basic format of a definition:

```
HEADER (KEYWORD VALUE;)
```

You can use as many keyword/value pairs as required within the 512-character limit.

To view the available custom IPS signatures, go to *Security Profiles > IPS Signatures*. Custom IPS signatures are listed under a separate heading inthe table.



To create a custom IPS signature, see Create or edit an IPS signature on page 322.

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.

Create or edit an IPS signature

You can create an IPS signature.

To create an IPS signature:

1. Go to *Security Profiles* > *IPS Signatures* and click *Create New*. You can also go to *Security Profiles* > *Intrusion Prevention*, click *Create New,* click *View IPS Signatures*, and click *Create New*.
2. Enter a name (no spaces) for the IPS signature in the *Name* field.
3. Enter a brief description in the *Comments* field
4. Enter the text for the signature in the *Signature* field. The syntax for signatures is described in Valid syntax on page 322.
5. Click *OK*.

You can also edit IPS signatures that you have created. Select the IPS signature and then click *Edit*.

Valid syntax

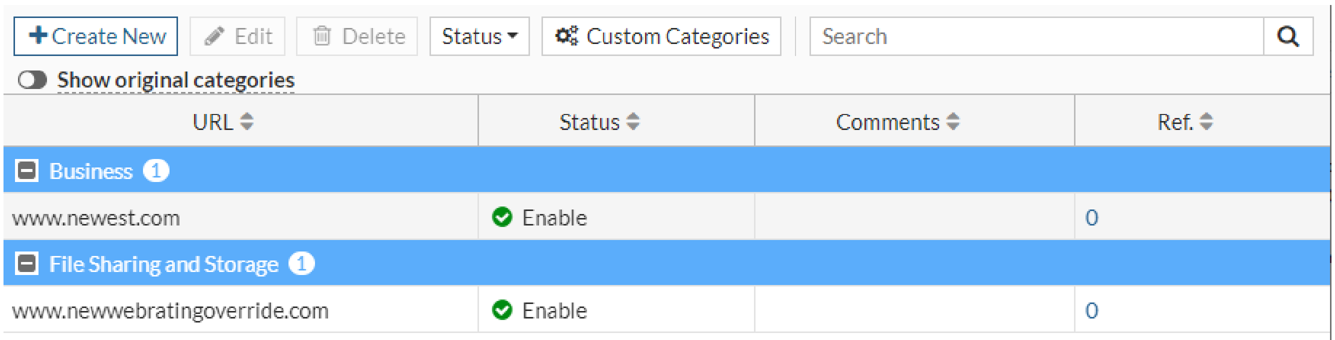
The following table shows the valid characters and basic structure. For details about each keyword and its associated values, see Custom signature keywords on page 613.

Field	Valid Characters	Usage
HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.
KEYWORD	Each keyword must start with a pair of dashes (--) and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword identifies a parameter.
VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. **NOTE:** If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	The value is set specifically for a parameter identified by a keyword.

Web Rating Overrides

This feature allows you to override the FortiGuard web filtering. You can change the rating for a web site and control access to the site without affecting the rest of the sites in the original category.

To override the FortiGuard web rating, go to *Security Profiles > Web Rating Overrides*.



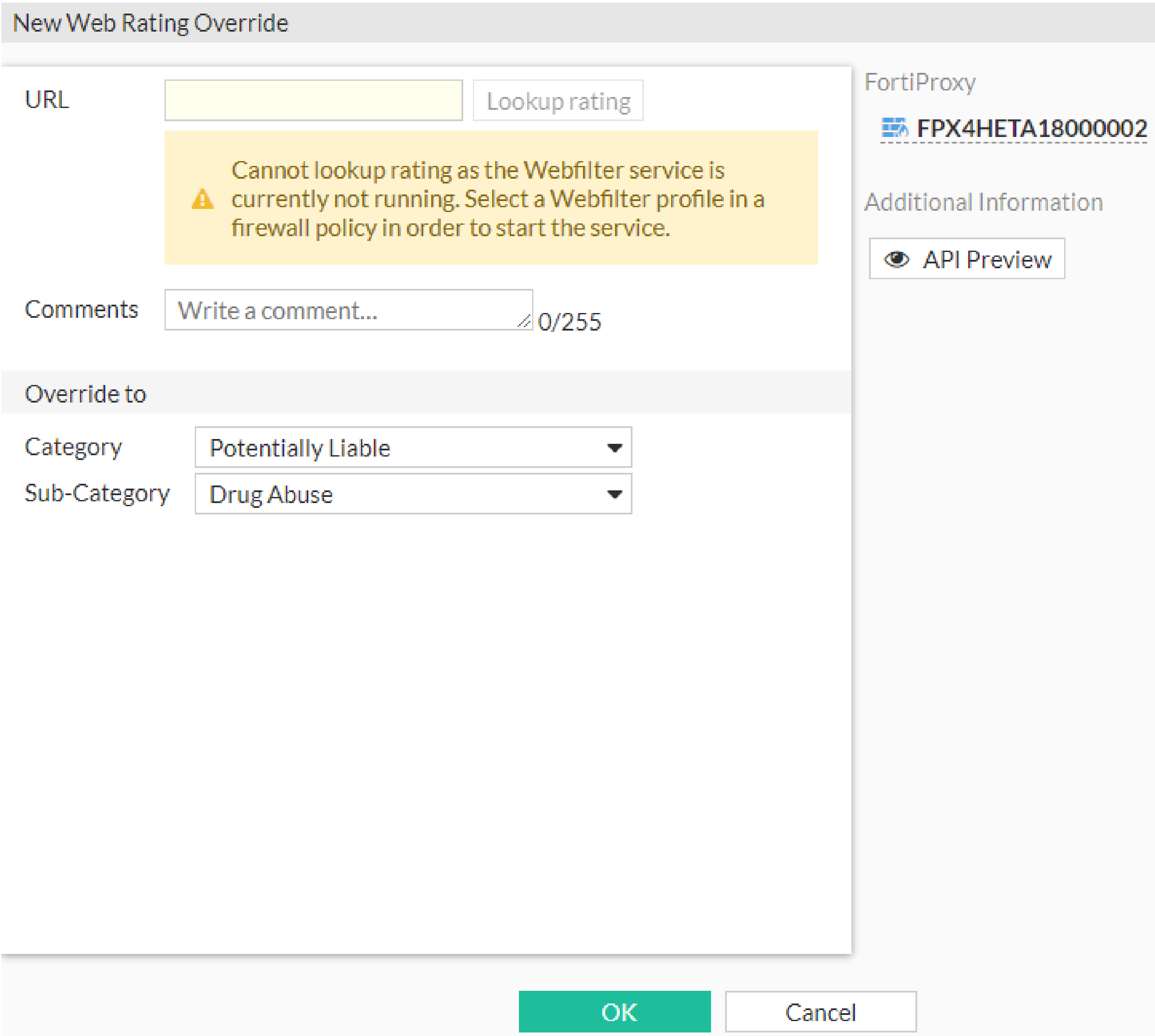
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a web rating override. See Create or edit a web rating override on page 324.
Edit	Modify the selected web rating override. See Create or edit a web rating override on page 324.
Delete	Remove the selected web rating override.
Status	Select *Enable* or *Disable* to make the override active or inactive.
Custom Categories	Select to create a custom category for groups of URLs. See Create or edit a custom category on page 325.
Search	Enter a search term to find in the web rating override list.
Show original categories	Enable to add the *Original Category* column, which shows the categories that are being overridden.
URL	The URL of a web site.
Status	Whether the override is enabled or disabled.
Comments	An optional description of the web rating override
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.
Override Category	The new category for the web site.
Original Category	The category that the web site originally belonged to.

Create or edit a web rating override

Click *Create New* to open the *New Web Rating Override* window.



To open the *Edit Web Rating Override* window, select a web rating override from the list and then click *Edit*.

Configure the following settings and then click *OK* to save your changes:

URL	Enter the URL of a website.
Lookup Rating	Click to find the FortiGuard rating if it exists for the URL you entered.
Comments	Enter an optional description of the web rating override.
Category	Select the new category for the website.

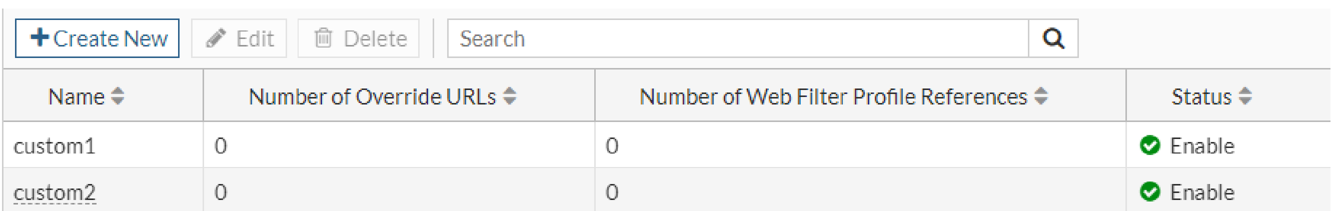
Sub-Category	Select a more narrowly defined option within the category that you selected for the website.
API Preview	The API Preview allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available 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.

Create or edit a custom category

Click *Custom Categories* to open the *Custom Categories* window.



To create a category for a group of web sites:

1. Go to *Security Profiles > Web Rating Overrides*.
2. Click *Custom Categories*. The *Custom Categories* window opens.
3. Click *Create New*.
4. Enter the name of the custom category.
5. Click *Enable* to make the custom category active.
6. Click *OK*.

To use the new category, select the *Custom Categories* category in the *New Web Rating Override* window or the *Edit Web Rating Override* window. The new categories are listed in the *Sub-Category* drop-down menu.

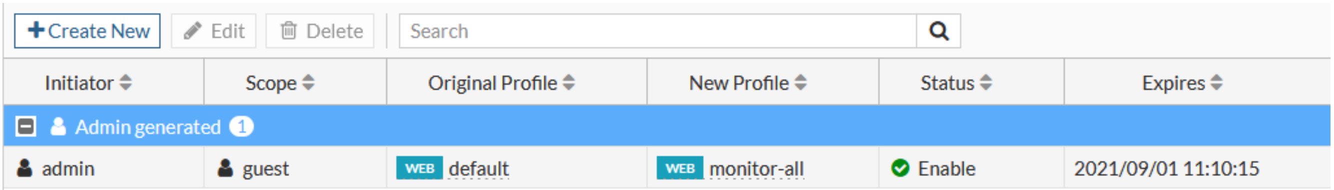
To edit a custom category, select a category from the list and then click *Edit*.

Web Profile Overrides

Administrators can grant temporary access to sites that are otherwise blocked by a web filter profile. You can grant temporary access to a user, user group, or source IP address. You can set the time limit by selecting a date and time. The default is 15 minutes.

When the administrative web profile override is enabled, a blocked access page or replacement message does not appear, and authentication is not required.

To override the web filter profile, go to *Security Profiles > Web Profile Overrides*.



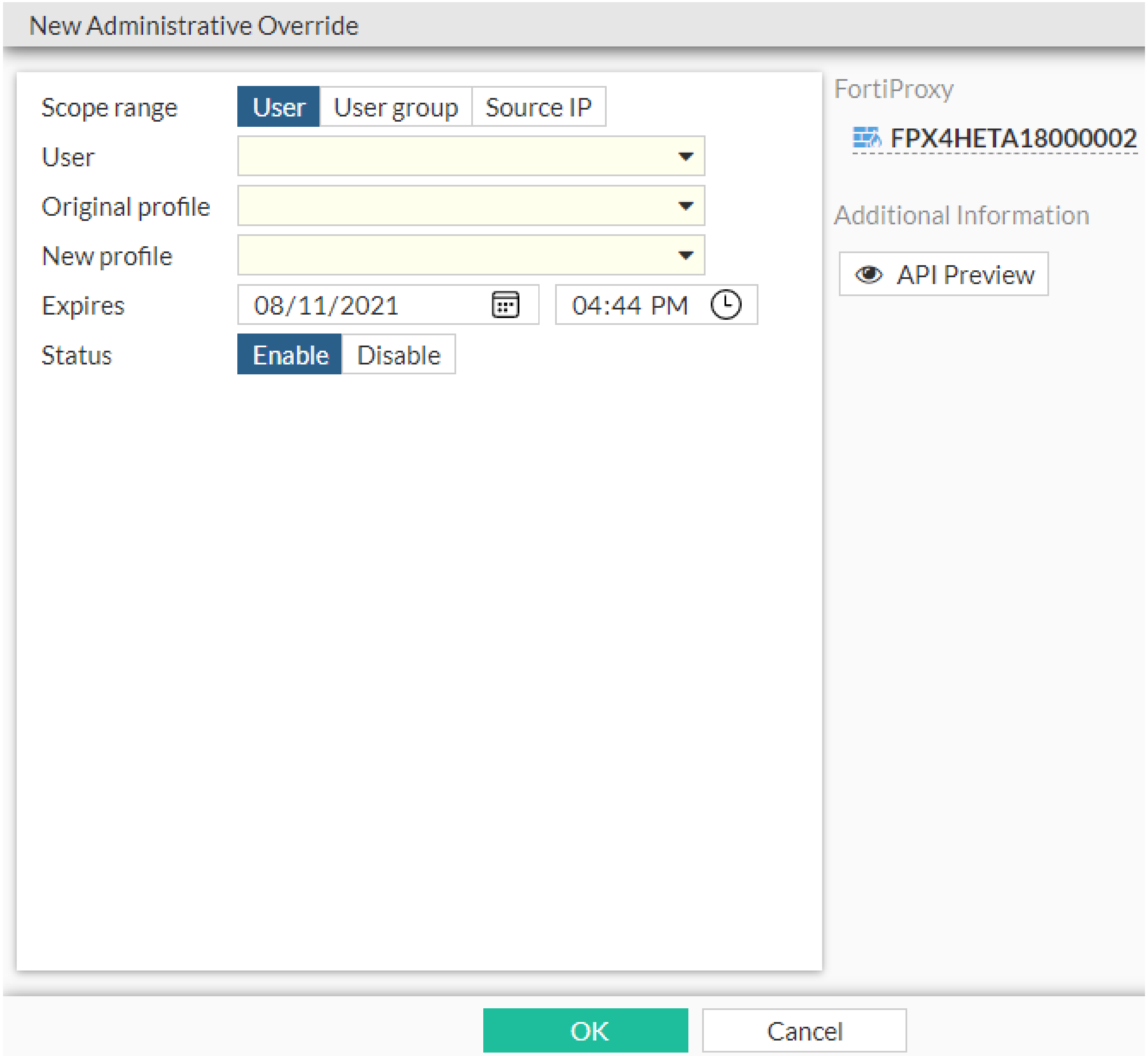
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a web profile override. See Create or edit a web profile override on page 326.
Edit	Modify the selected web profile override. See Create or edit a web profile override on page 326.
Delete	Remove the selected web profile override.
Search	Enter a search term to find in the web profile override list.
Initiator	The user who created the web profile override.
Scope	The scope is a user, a user group, or a source IP address.
Original Profile	The web filter profile that is being overridden.
New Profile	The web filter profile that is overriding the original web filter profile.
Status	Whether the override is enabled or disabled.
Expires	The day and time when the override ends.

Create or edit a web profile override

Click *Create New* to open the *New Administrative Override* window.



To open the *Edit Administrative Override* window, select a web profile override from the list and then click *Edit*.

Configure the following settings and then click *OK* to save your changes:

Scope range	Select one of the following scope ranges: • *User*: Authentication for permission to override is based on whether or not the user is using a specific user account. • *User group*: Authentication for permission to override is based on whether or not the user account supplied as a credential is a member of the specified user group. • *Source IP*: Authentication for permission to override is based on the IP address of the computer that was used to authenticate. This would be used for computers that have multiple users. For example, if a user logs on to the

	computer, engages the override by using their credentials, and then logs off, anyone who logs on with an account on that computer would be using the alternate override web filter profile.
User	If you selected *User* for the scope range, select or create the user. See Create a user on page 414.
User group	If you selected *User group* for the scope range, select or create the user group. See Create or edit a user group on page 420.
Source IP	If you selected *Source IP* for the scope range, enter the source IP address.
Original profile	Select or create a web filter profile to override. See Create or edit a web filter profile on page 277.
New profile	Select or create a web filter profile that will override the original web filter profile. See Create or edit a web filter profile on page 277.
Expires	Select the date and time when the override ends.
Status	Enable to make the override active.
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.
References	Click to open the object usage page to show which other configuration are referencing the object.
Edit in CLI	Click to open a CLI console window to view and edit the setting in the CLI. If there are multiple CLI settings on the page, the CLI console shows the first setting.

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.

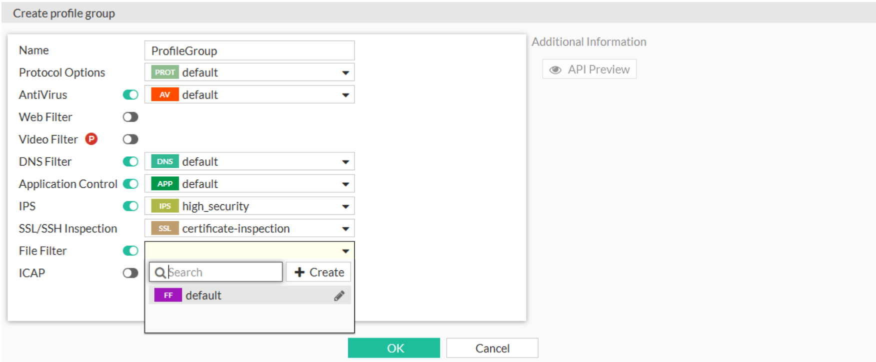
Profile Groups

Profile groups are used to group security profiles of different types together, and can be used in policies instead of individual profiles.

To create a profile group in the GUI:

1. Go to *Security Profiles* > *Profile Groups* and click *Create New*.
2. Enter a name for the group.
3. Select the *Protocol Options* from the drop-down list.

4. Enable the required profile types and select a profile for each.



5. Click *OK*.

To create a profile group in the CLI:

```
config firewall profile-group
    edit <name>
        set profile-protocol-options <options>
        set ssl-ssh-profile {certificate-inspection | custom-deep-inspection | deep-
inspection | no-inspection}
        set av-profile <profile>
        set ia-profile <profile>
        set webfilter-profile <profile>
        set dnsfilter-profile <profile>
        set emailfilter-profile <profile>
        set dlp-sensor <sensor>
        set file-filter-profile <profile>
        set ips-sensor <sensor>
        set application-list <list>
        set icap-profile <profile>
        set cifs-profile <profile>
        set videofilter-profile <profile>
        set ssh-filter-profile <profile>
    next
end
```

To use a profile group in a policy:

```
config firewall policy
    edit <policy>
        set profile-type group
        set profile-group <group>
    next
end
```

Data Leak Prevention

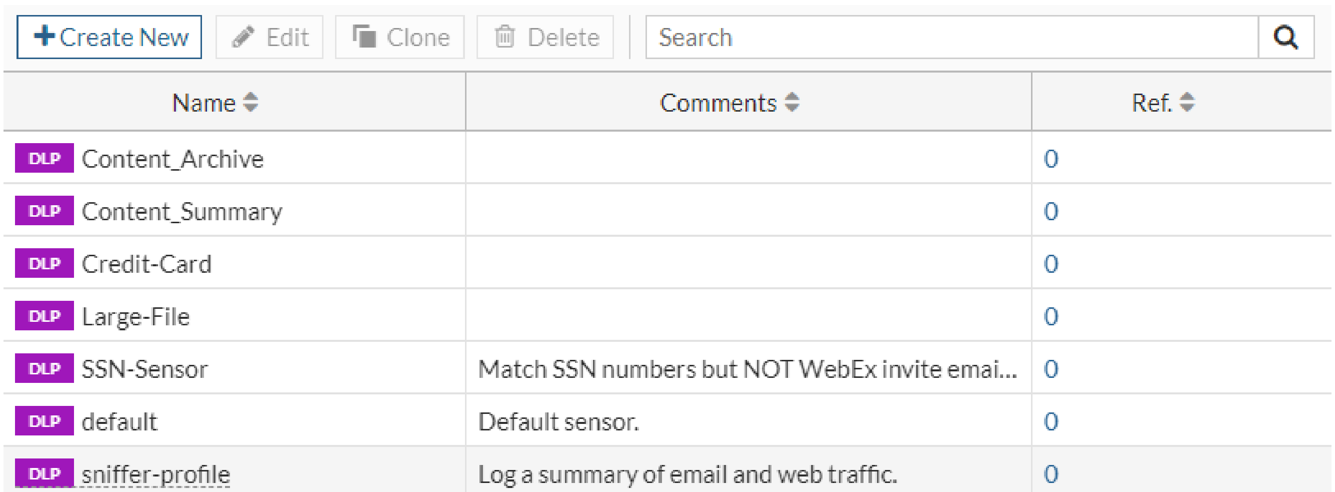
The data leak prevention (DLP) system allows you to prevent sensitive data from leaving your network. After sensitive data patterns are defined, data matching the patterns will either be blocked or logged and then allowed.

The DLP system is configured by creating filters based on various attributes and expressions within DLP sensors and then assigning the sensors to security policies.

DLP can also be used to prevent unwanted data from entering your network and to archive content passing through the FortiProxy device.

A DLP sensor is a package of filters. To use DLP, select and enable a DLP sensor in a security policy. The traffic controlled by the security policy will be searched for the patterns defined in the filters contained in the DLP sensor. Matching traffic will be passed or blocked according to the filters.

To view available DLP sensors, go to *Security Profiles > Data Leak Prevention*.



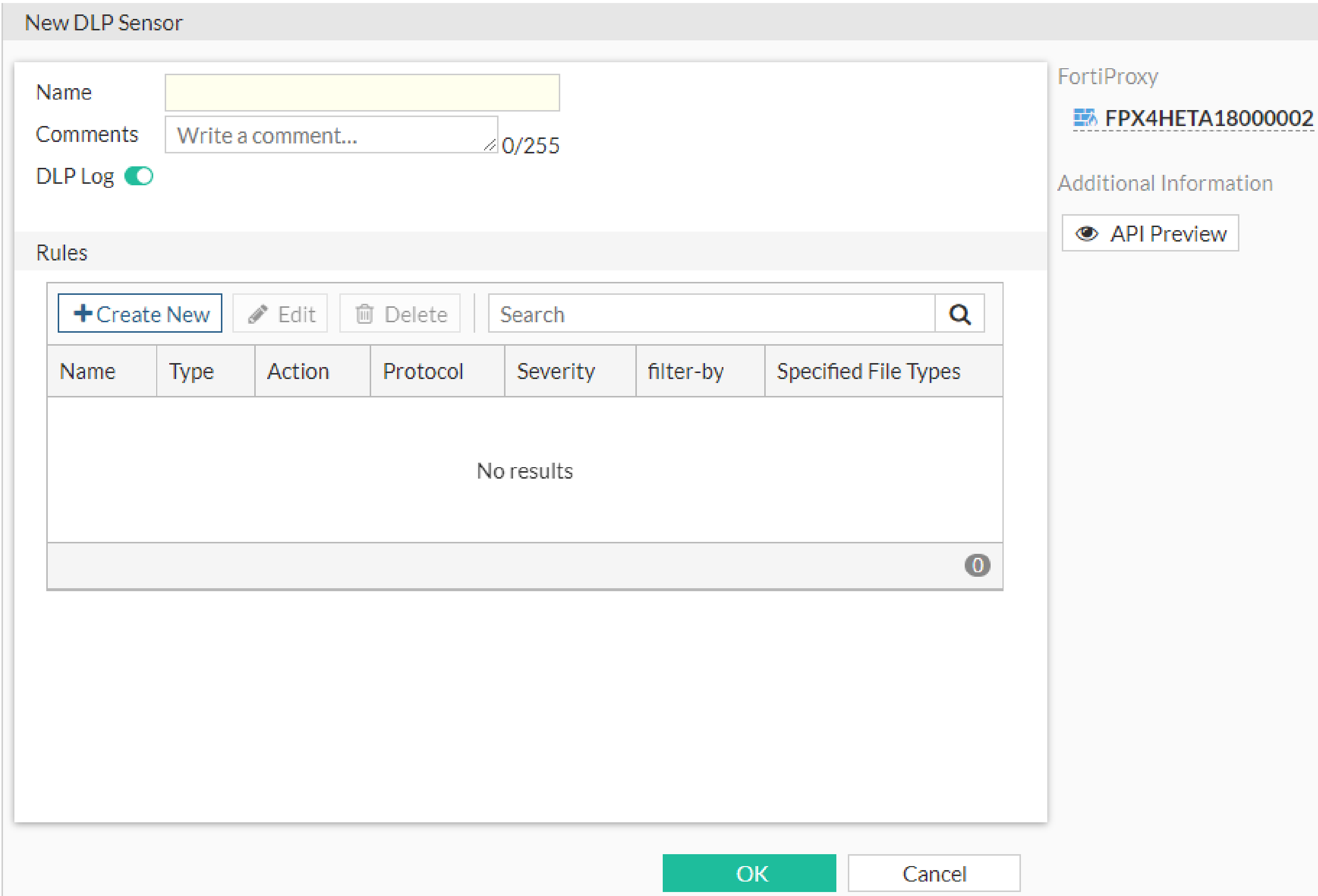
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a DLP sensor. See Create or edit a DLP sensor on page 331.
Edit	Modify the selected DLP sensor. See Create or edit a DLP sensor on page 331.
Clone	Make a copy of a DLP sensor.
Delete	Remove the selected DLP sensor.
Search	Search for text in any column.
Name	The name of the DLP sensor.
Comments	Optional description of the sensor.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.
DLP Log	Logging when data matches the configured patterns is enabled or disabled.

Create or edit a DLP sensor

To configure a DLP sensor, go to *Security Profiles > Data Leak Prevention* and click *Create New*.



Configure the following settings and select *OK* to save your changes:

Name	Enter he name of the DLP sensor.
Comments	An optional description of the DLP sensor.
DLP Log	Enable if you want a log entry when data matches the configured patterns.
Rules	Create or edit DLP filter rules. See Create or edit a DLP filter rule on page 333.

To create a DLP sensor:

1. Go to *Security Profiles > Data Leak Prevention* and click *Create New*. The *New DLP Sensor* window opens.
2. Enter a name for the new sensor in the *Name* field and, optionally, enter a description of the sensor in the *Comments* field.
3. Enable *DLP Log* if you want a log entry when data matches the configured patterns.
4. Add DLP filter rules to the sensor. See Create or edit a DLP filter rule on page 333.
5. Click *OK* to create the new sensor.

To edit a DLP sensor:

1. Go to *Security Profiles* > *Data Leak Prevention*.
2. Select a DLP sensor and then click *Edit*. The *Edit DLP Sensor* window opens.
3. Edit the DLP sensor name and comments as required.
4. Enable or disable *DLP Log*.
5. Edit, create, or delete DLP filter rules as required. See Create or edit a DLP filter rule on page 333.
6. Click *OK* to save your changes.

DLP archiving

DLP is typically used to prevent sensitive information from getting out of your company network, but it can also be used to record network use. This is called DLP archiving. The DLP engine examines email, FTP, NNTP, and web traffic. Enabling archiving for rules when you add them to sensors directs the FortiProxy unit to record all occurrences of these traffic types when they are detected by the sensor.

Because the archive setting is configured for each rule in a sensor, you can have a single sensor that archives only the things you want.

You can archive Email, FTP, HTTP, and session control content:

- Email content includes IMAP, POP3, and SMTP sessions. Email content can also include email messages tagged as spam by Email filtering. If your unit supports SSL content scanning and inspection, email content can also include IMAPS, POP3S, and SMTPS sessions.
- HTTP content includes HTTP sessions. If your unit supports SSL content scanning and inspection HTTP content can also include HTTPS sessions.

DLP archives are saved to a FortiAnalyzer unit or the FortiGuard Analysis and Management Service (subscription required).

You can use DLP archiving to collect and view historical logs that have been archived to a FortiAnalyzer unit or the FortiGuard Analysis and Management Service. DLP archiving is available for FortiAnalyzer when you add a FortiAnalyzer unit to the Fortinet configuration. The FortiGuard Analysis server becomes available when you subscribe to the FortiGuard Analysis and Management Service.

Two sample DLP sensors are provided with DLP archiving capabilities enabled. If you select the `Content_Summary` sensor in a security policy, it will save a summary DLP archive of all traffic the security policy handles. Similarly, the `Content_Archive` sensor will save a full DLP archive of all traffic handled the security policy you apply it to. These two sensors are configured to detect all traffic of the supported types and archive them.

NOTE: You can see these sensors in the GUI but the configuration is only visible through the CLI; DLP archiving is set in the CLI only.

To enable the DLP archiving:

```
config dlp sensor
   edit <name of sensor>
      set summary-proto smtp pop3 imap http-get http-post ftp nntp mapi cifs
   next
end
```

Create or edit a DLP filter rule

Each DLP sensor must have one or more DLP filter rules configured within it. Filters can examine traffic for the following:

- Known files using DLP fingerprints
- Files of a particular name or type
- Files larger than a specified size
- Data matching a specified regular expression
- Traffic matching an advanced or compound rule

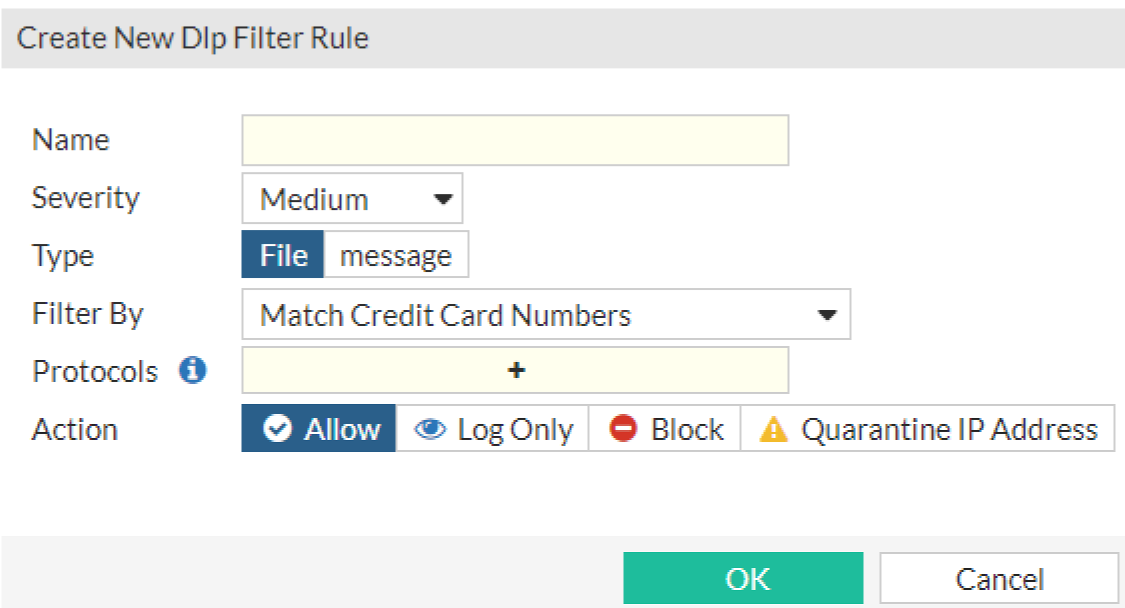
File filters allow you to block files based on their file names and types. When a file filter list is applied to a DLP sensor filter, the network traffic is examined against the list entries, and, if the sensor filter is triggered, the predefined action is taken by the DLP sensor filter.

The general steps for configuring filters are as follows:

1. Create a DLP sensor.
2. Add DLP filter rules to filter either messages or specific file types.
3. Select the DLP sensor in a security policy.

To create a DLP filter rule in the GUI:

Select *Create New* to open the *Create New Dlp Filter Rule* window.



To open the *Edit Dlp Filter Rule* window, select a filter and then click *Edit*.

Configure the following settings in the *Create New Dlp Filter Rule* window or the *Edit Dlp Filter Rule* window and then click *OK*.

Name	Enter a name for the DLP filter rule.

Severity	Select a severity for the DLP filter rule: *Information*, *Low*, *Medium*, *High,* or *Critical*.
Type	Select *File* or *message* to filter based on file attributes or to filter for specific messages.
Filter By	Select the filter from the drop-down list.
Regular Expression	Enter the pattern that network traffic is examined for. See Regular expressions on page 338.
File Pattern	Select or create a DLP file pattern. See File types on page 338.
File Size	Enter the maximum file size in kilobytes. See File size on page 336.
Company Identifier	Enter the company identifier. The company identifier is to make sure that you are only blocking watermarks that your company has placed on the files, not watermarks with the same name by other companies. See Watermarking on page 338.
Protocols	Select one or more protocols that the filter will examine. This allows resources to be optimized by only examining relevant traffic. The available protocols are *HTTP-POST*, *IMAP*, *MAPI*, *NNTP*, *POP3*, and *SMTP*.
Action	Select an action to take if the filter is triggered. Available actions are *Allow*, *Log Only*, *Block*, and *Quarantine IP Address*.
Allow	No action is taken when the filter is triggered.
Log Only	When the filter is triggered, the match is logged, but no other action is taken.
Block	Traffic matching the filter is blocked and replaced with a replacement message. See Replacement Messages on page 492.
Quarantine IP Address	Block access for any IP address that sends traffic matching the filter. The IP address is added to the banned user list, and an appropriate replacement message is sent for all connection attempts until the quarantine time expires. Enter the amount of time that the IP address will be quarantined for (>= 1 minute).

Basic DLP filter types

You can configure four basic filter types:

- File types
- File size
- Regular expression
- Credit card and SSN

File type and name

A file type filter allows you to block, allow, log, or quarantine based on the file type specified in the file filter list.

To configure file type and name filtering using the CLI:

1. Create a file pattern to filter files based on the file name patter or file type:
```
config dlp filepattern
   edit <filepattern_entry_integer>
      set name <string>
         config entries
            edit <file pattern>
               set filter-type <type | pattern>
               set file-type <file type>
            next
         end
   next
end
```
   For example, to filter for GIFs and PDFs:
```
config dlp filepattern
   edit 11
      set name “sample_config”
         config entries
            edit "*.gif"
               set filter-type pattern
            next
            edit "pdf"
               set filter-type type
               set file-type pdf
         next
      end
   next
end
```
2. Attach the file pattern to a DLP sensor, and specify the protocols and actions:
```
config dlp sensor
   edit <string>
      config filter
         edit <integer>
            set name <string>
            set proto {smtp | pop3 | imap | http-get | http-post | ftp | nntp | mapi}
            set filter-by file-type
            set file-type 1 <-- Previously configured file pattern
            set action {allow | log-only| block | quarantine-ip}
         next
      end
   next
end
```

To configure file type and name filtering using the GUI:

1. Go to *Security Profiles > Data Leak Prevention*.
2. Click *Create New*. The *New DLP Sensor* window opens.
3. Click *Create New* in the *Rules* table. The *Create New Dlp Filter Rule* window opens.
4. Set *Type* to *File* and select *Match a DLP File Pattern*.
5. Select or create a file pattern. See Create or edit a DLP file pattern on page 340.
6. Click + and select one or more protocols from the side pane.

7. Select the action.
8. Click *OK* to save the new filter.

File size

A file size filter checks for files that exceed the specific size, and performs the DLP sensor's configured action on them.

To configure file size filtering using the CLI:

```
config dlp sensor
   edit <string>
      config filter
         edit <integer>
            set name <string>
            set proto {smtp | pop3 | imap | http-get | http-post | ftp | nntp | mapi}
            set filter-by file-size <-- Match any file over with a size over the threshold
            set file-type 1 <-- Previously configured file pattern
            set action {allow | log-only| block | quarantine-ip}
         next
      end
   next
end
```

To configure file size filtering using the GUI:

1. Go to *Security Profiles > Data Leak Prevention*.
2. Click *Create New*. The *New DLP Sensor* window opens.
3. Click *Create New* in the *Rules* table. The *Create New Dlp Filter Rule* window opens.
4. Set *Type* to *File* and select *Match Any File Over Size*.
5. Enter the maximum file size, in kilobytes, in the *File Size* field.
6. Click + and select one or more protocols from the side pane.
7. Select the action.
8. Select one of and then click *OK*.

Regular expression

A regular expression filter is used to filter files or messages based on the configured regular expression pattern.

To configure regular expression filtering using the CLI:

```
config dlp sensor
   edit <string>
      config filter
         edit <integer>
            set name <string>
            set type {file | message} <-- Check contents of a file or of messages, web pages,
                and so on
            set proto {smtp | pop3 | imap | http-get | http-post | ftp | nntp | mapi}
            set filter-by regexp <-- Use a regular expression to match content
            set regexp <regexp> <-- Input a regular expression pattern
            set action {allow | log-only| block | quarantine-ip}
         next
```

```
      end
   next
end
```

To configure regular expression filtering using the GUI:

1. Go to *Security Profiles > Data Leak Prevention*.
2. Click *Create New*. The *New DLP Sensor* page opens.
3. Click *Create New* in the *Rules* table. The *Create New Dlp Filter Rule* window opens.
4. For filtering regular expressions in files, set *Type* to *File*. For filtering in messages, set *Type* to *message*.
5. Select *Match a Regular Expression*.
6. Enter the regular expression string in the *Regular Expression* field.
7. Click + and select one or more protocols from the side pane.
8. Select the action.
9. Click *OK*.

Credit card and SSN

The credit card sensor can match the credit card number formats used by American Express, Mastercard, and Visa. It can be used to filter files or messages.

The SSN sensor can be used to filter files or messages for Social Security Numbers.

To configure credit card or SSN filtering using the CLI:

```
config dlp sensor
   edit <string>
      config filter
         edit <integer>
            set name <string>
            set type {file | message} <-- Check contents of a file, or of messages, web
                  pages, etc.
            set proto {smtp | pop3 | imap | http-get | http-post | ftp | nntp | mapi}
            set filter-by < credit-card | ssn > <-- Match credit cards or social security
                  numbers
            set action {allow | log-only| block | quarantine-ip}
         next
      end
   next
end
```

To configure credit card or SSN filtering using the GUI:

1. Go to *Security Profiles > Data Leak Prevention*.
2. Click *Create New*. The *New DLP Sensor* page opens.
3. Click *Create New* in the *Rules* table. The *Create New Dlp Filter Rule* window opens.
4. For filtering in files, set *Type* to *File*. For filtering in messages, set *Type* to *message*.
5. Select *Match Credit Card Numbers* or *Match Social Security Numbers*.
6. Click + and select one or more protocols from the side pane.

7. Select the action.
8. Click *OK*.

Regular expressions

Network traffic is examined for the pattern described by the regular expression specified in the DLP sensor filters. Fortinet uses a variation of the Perl Compatible Regular Expressions (PCRE) library. For some examples of Perl expressions, see Perl regular expressions on page 604. For more information about using Perl regular expressions, go to http://perldoc.perl.org/perlretut.html.

By adding multiple filters containing regular expressions to a sensor, a dictionary can be developed within the sensor. The filters can include expressions that accommodate complex variations of words or target phrases. Within the sensors, each expression can be assigned a different action, allowing for a very granular implementation.

File types

- Archive (7z)
- Archive (arj)
- Archive (bzip)
- Archive (bzip2)
- Archive (cab)
- Archive (gzip)
- Archive (lzh)
- Archive (rar)
- Archive (tar)
- Archive (xz)
- Archive (zip)
- Audio (avi)
- Audio (mp3)
- Audio (wav)
- Audio (wma)
- Batch File (bat)
- BMP Image (bmp)
- Common Console Document (msc)
- Encoded Data (base64)
- Encoded Data (binhex)
- Encoded Data (mime)
- Encoded Data (uue)
- Executable (elf)
- Executable (exe)
- GIF Image (gif)
- HTML Application (hta)
- HTML File (html)
- Ignored File Type (ignored)
- Java Application Descriptor (jad)
- Java Class File (class)
- Java Compiled Bytecode (cod)
- JavaScript File (javascript)
- JPEG Image (jpeg)
- Microsoft Active Mime Object (activemime)
- Microsoft Office (msoffice)
- Microsoft Office (msofficex)
- Packer (aspack)
- Packer (fsg)
- Packer (petite)
- Packer (upx)
- PalmOS Application (prc)
- PDF (pdf)
- PNG Image (png)
- Real Media Streaming (rm)
- Symbian Installer System File (sis)
- TIFF Image (tiff)
- Torrent (torrent)
- Unknown File Type (unknown)
- Video (mov)
- Video (mpeg)
- Windows Help File (hlp)
- Windows Installer Package (msi)

Watermarking

Watermarking is essentially marking files with a digital pattern to mark the file as being proprietary to a specific company. Fortinet provides a Linux-based utility that applies a digital watermark to files. The utility adds a small (approximately 100 bytes) pattern to the file that is recognized by the DLP watermark filter. The pattern is invisible to the end user.

When watermarking a file, verify that the pattern matches a category found on the FortiProxy firewall. For example, if you are going to watermark a file with the sensitivity level of “Secret” you should verify that “Secret” is a sensitivity level that has been assigned in the FortiProxy unit.

Company identifier and sensitivity

The company identifier is to make sure that you are only blocking watermarks that your company has placed on the files, not watermarks with the same name by other companies.

If you are using watermarking on your files, you can use the watermark sensitivity filter to check for watermarks that correspond to sensitivity categories that you have set up.

Software versions

Before planning on using watermarking software it is always best to verify that the software will work with your OS. Currently, the only utility available to watermark files is a Linux-based command line tool. It is available for download from the Fortinet Customer Service & Support website, with a valid support contract and access to the site. To access the file:

1. Sign into the Fortinet Customer Service & Support website.
2. Go to https://support.fortinet.com/Download/FirmwareImages.aspx.
3. Navigate to the image file path for WATERMARK.
4. Download the `fortinet-watermark-linux.out` file.

File types

The watermark utility does not work with every file type. The following file types are supported by the watermark tool: .txt; .pdf; .doc; .xls; .ppt; .docx; pptx; and, .xlsx.

Syntax of the watermark utility

The tool is executed in a Linux environment by passing in files or directories of files to insert a watermark.

Usage:

```
watermark_linux_amd64 <options> -f <file name> -i <identifier> -l <sensitivity level>
watermark_linux_amd64 <options> -d <directory> -i <identifier> -l <sensitivity level>
```

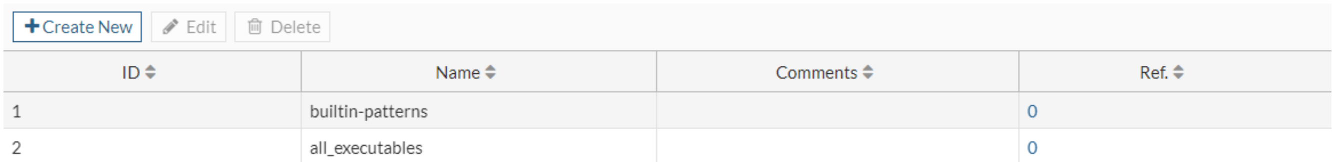
Options:

```
        -h print help
        -I inplace watermarking (do not copy file)
        -o output file (or directory in directory mode)
        -e encode <to non-readable>
        -i add watermark identifier
        -l add watermark sensitivity level
        -D delete watermark identifier
        -L delete watermark sensitivity level
```

DLP File Pattern

DLP file patterns match selected file types and file patterns. They are used as DLP filter rules in DLP sensors.

To view available DLP file patterns, go to *Security Profiles > DLP File Pattern*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a DLP file pattern. See Create or edit a DLP file pattern on page 340.
Edit	Modify the selected DLP file pattern. See Create or edit a DLP file pattern on page 340.
Delete	Remove the selected DLP file pattern.
ID	Identifier for the DLP file pattern.
Name	The name of the DLP file pattern.
Comments	An optional description of the DLP file pattern.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a DLP file pattern

You can create or edit DLP file patterns.

To create a DLP file pattern:

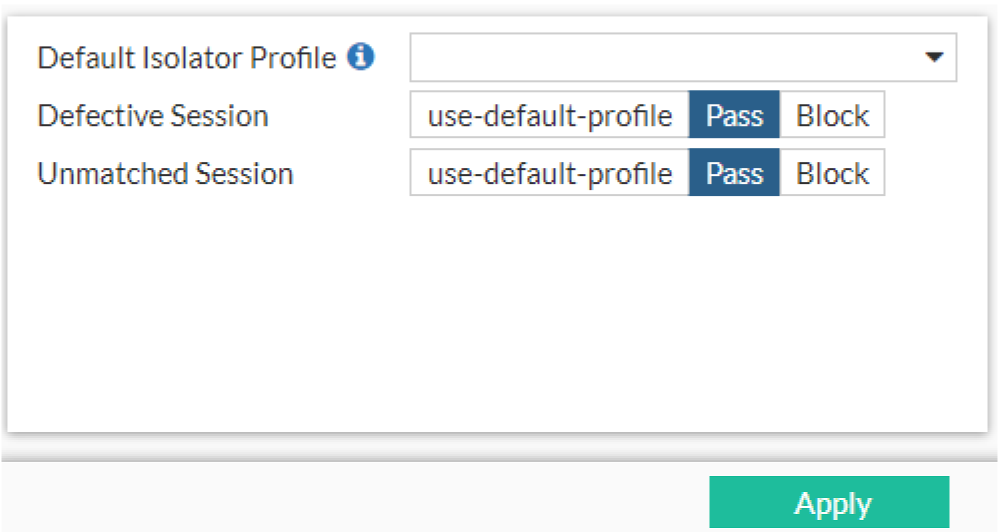
1. Go to *Security Profiles > DLP File Pattern*.
2. Click *Create New*. The *Create DLP File Pattern* window opens.
3. Enter an identifier for the DLP file pattern.
4. Enter a name for the DLP file pattern.
5. Enter an optional description of the DLP file pattern.
6. Select one or more file types.
7. Enter one or more file patterns.
8. Click *OK* to save the DLP file pattern.

To edit a DLP file pattern:

1. Go to *Security Profiles* > *DLP File Pattern*.
2. Select a DLP file pattern and then click *Edit*.
3. Edit the settings as required.
4. Click *OK* to save your changes to the DLP file pattern.

Isolator Setting - NEW

Configure the default isolator profile and/or configure the action to perform on rating requests for isolator sessions that do not match any existing policies (unmatched-session) or have missing information (defective-session).



To configure isolator settings in the GUI, go to *Security Profiles* > *Isolator Setting*, configure the following options, and click *Apply*.

Default Isolator Profile	Select a profile that will used when no policy is matched. You can select an existing isolator profile from the list or create a new one. By default, no profile is selected.
Defective Session	Select the action to perform on rating requests for isolator sessions that do not match any existing policies. • Use the action defined in the default isolator profile. • Bypass defective sessions • Block defective sessions
Unmatched Session	Select the action to perform on rating requests for isolator sessions that have missing information. • Use the action defined in the default isolator profile. • Bypass unmatched sessions • Block unmatched sessions

To configure isolator settings in the CLI, use the `config isolator setting` command.

Content Analyses

Content Analysis Service is an automated computer vision AI that detects visual threats including pornography, extremism, and graphic violence. Content Analysis empowers your application with AI content moderation that recognizes threats in images.

Internet Content Adaptation Protocol (ICAP) allows for the offloading of certain processes to a separate server so that your FortiProxy firewall can optimize its resources and maintain the best level of performance possible.

This section covers the following topics:

Image Analysis

Content Analysis is a licensed feature, powered by AI that detects visual threats including pornography, extremism, graphic violence, and other inappropriate Not Safe for Work (NSFW) visual content. This service is a real-time analysis of the content passing through the FortiProxy unit. The Content Analysis Service uses advanced artificial intelligence that delivers unparalleled accuracy with near zero false positives, all in a matter of milliseconds. After inappropriate NSFW content is detected, such content can be optionally blocked or reported. Unlike early heuristic-based technologies the AI-powered Content Analysis Service has been extensively trained and developed, and more NSFW-relevant Threat Categories are being added as they become available.

In general, the procedure is similar to the HTTP antivirus scanning procedure.

When a client HTTP requests an image, the HTTP header content-type determines the image type. Then the WAD process holds the image content from the server for scanning before sending it to the client.

If the scan results are larger than the configurable threshold, the requested image is blocked, and the client receives a replacement image. This replacement image keeps the same image type and size if you enable the option to re-size images. The FortiProxy unit stores the results to improve performance for future requests.

The default settings provide a good balance, but they might require some adjustment in some instances.

To use Content Analysis, you need to set up at least one profile and apply it to a policy. Content Analysis profiles are configured under *Content Analyses* > *Image Analyses*.

+ Create New | Edit | Delete

Name	Image Skip Size	Rating Error Action	Comments	Ref.
default	1	Pass	Analyze image content	0

Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a Content Analysis profile. See Create or edit an Image Analysis profile on page 343.
Edit	Modify the selected Content Analysis profile. See Create or edit an Image Analysis profile on page 343.
Delete	Remove the selected Content Analysis profile.
Name	The name of the Content Analysis profile.
Image Skip Size	Enter a value between 0 and 2,048. This value represents the size of image that will be skipped by the image scan unit, in kilobytes. Images that are too small are difficult to scan and are more likely to be rated incorrectly by the image scan engine. The default value is 1.
Rating Error Action	Set to either *Pass* or *Block* the image when it exceeds the rating threshold. The default is *Pass*.
Comments	An optional description of the Content Analysis profile.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Validating Content Analysis

You can use the following debug commands to validate the service licensing and image cache:

`get system fortiguard`—Display licensing information.

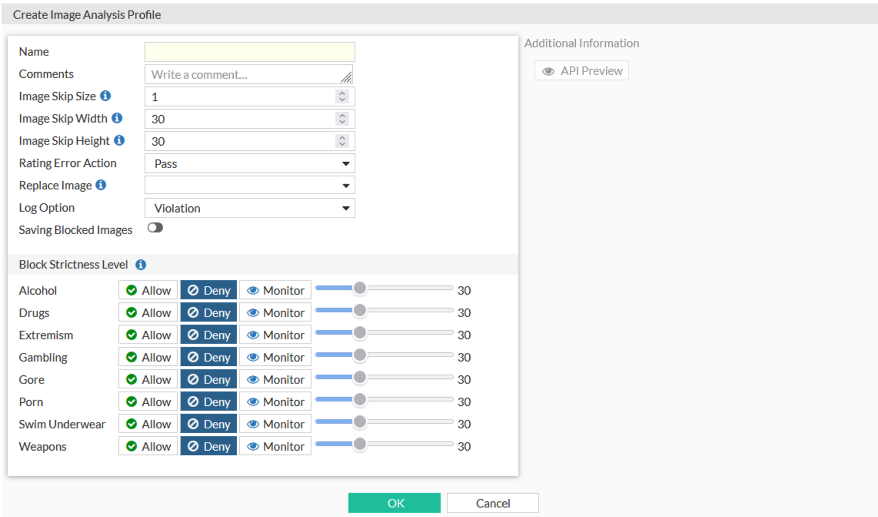
`diagnose test application wad 143`—Display image cache.

`diagnose test application wad 144`—Clear image cache.

You need a license to display and clear the image cache; otherwise, these commands are not available.

Create or edit an Image Analysis profile

Select *Create New* to open the *Create Image Analysis Profile* window.



To open the *Edit Image Analysis Profile* window, select a profile and then click *Edit*.

Configure the following settings and then click *OK*:

Name	Enter a name for this profile.
Comments	Optional description of the profile.
Image Skip Size	Enter a value between 0 and 2,048. This value represents the image size that will be skipped by the image scan unit, in kilobytes. Images that are too small are difficult to scan and are more likely to be rated incorrectly by the image scan engine. The default value is 1.
Image Skip Width	This value represents the image width that will be skipped by the image scan unit, in pixels. Images that are too small are difficult to scan and are more likely to be rated incorrectly by the image scan engine. The default value is 30 pixels; the minimum value is 5 pixels.
Image Skip Height	This value represents the image height that will be skipped by the image scan unit, in pixels. Images that are too small are difficult to scan and are more likely to be rated incorrectly by the image scan engine. The default value is 30 pixels; the minimum value is 5 pixels.
Rating Error Action	Set to either *Pass* or *Block* the image when it exceeds the rating threshold. The default is *Pass*.
Replace Image	Select a replacement image. **NOTE:** The file type must be `.jpeg`. To specify the replacement image, go to *System > Replacement Messages* and select *Manage Images*.
Log Option	Select *All* to log all content or *Violation* to log content that exceeds any of the strictness levels.
Saving Blocked Images	Enable to save blocked images.

Block Strictness Level	For each category, select to *Allow*, *Deny*, or *Monitor* content that exceeds the strictness level, and set the level between 0 and 100. The higher the image score, the more chance of the image being explicit. The challenge with this setting is that if you set it too high, it will block legitimate images. If you set it too low, it will allow explicit images through. If the image score is above this setting, the *Rating Error Action* is taken. The default value is 30.
Alcohol	The alcohol category is designed to identify images containing alcoholic brands and beverages, people drinking alcohol, frat parties, keg stands, bars and nightclubs, party aftermaths, shots, beer pong, kegs, and plastic cups associated with drinking.
Drugs	The drugs category is designed to identify images containing illegal and legal drugs, drug use, drug paraphernalia, and plants and symbols relating to drugs.
Extremism	The extremism category is designed to identify images containing terrorist militants, beheadings, executions, propaganda, acts of terrorism, KKK rallies, Hitler, insignia related to Nazism, KKK, ISIS, and white supremacy icons.
Gambling	The gambling category is designed to identify images containing gambling.
Gore	The gore or graphic violence category is designed to identify images containing gore, graphic violence, self-harm, suicide, horrific imagery, bloody wounds, accident victims, shooting victims, beatings, mutilation, decapitation, and images that contain blood and guts.
Porn	The pornography category is designed to identify images and videos containing commercial pornography, amateur pornography, sexting selfies, nudity, sex acts, grayscale pornographic images, sexually explicit cartoons, and manga.
Swim Underwear	The swim and underwear, or risqué, category is designed to identify images containing people wearing swimwear or beachwear, underwear, and lingerie.
Weapons	The weapons category is designed to identify images containing rifles, machine guns, handguns, grenade launchers, swords, knives, and people holding handheld weapons.

Alternatively, use the `config image-analyzer profile` command to configure an image analysis profile in the CLI.

ICAP Profile

Internet Content Adaptation Protocol (ICAP) is an application layer protocol that is used to offload tasks from the firewall to separate, specialized servers. For more information see RFC 3507.

If you enable ICAP in a policy, HTTP and HTTPS (if HTTPS inspection is supported) traffic that is intercepted by the policy is transferred to the ICAP server specified by the selected ICAP profile. Responses from the ICAP server are returned to the FortiProxy, and then forwarded to their destination

By default, ICAP is not visible in the GUI. See Feature Visibility on page 506 for instructions on making it visible.

The ICAP Profile page allows you to view and configure ICAP profiles, which you can then apply to a policy.

If you enable ICAP in a security policy, HTTP traffic intercepted by the policy is transferred to the ICAP servers in the ICAP profile added to the policy. The FortiProxy unit acts as the surrogate and carries the ICAP responses from the ICAP server to the ICAP client. The ICAP client then responds back, and the FortiProxy unit determines the action that should be taken with these ICAP responses and requests.

You can configure ICAP profiles under *Content Analyses > ICAP Profile*.

+ Create New | Edit | Delete

Name	Request	Response	Streaming Content Bypass	Ref.
ICAP default	Disable	Disable	Disable	0
ICAP icap_fpx2_test	Enable	Enable	Enable	0
ICAP icap_test	Enable	Enable	Enable	0
ICAP new	Disable	Disable	Disable	0

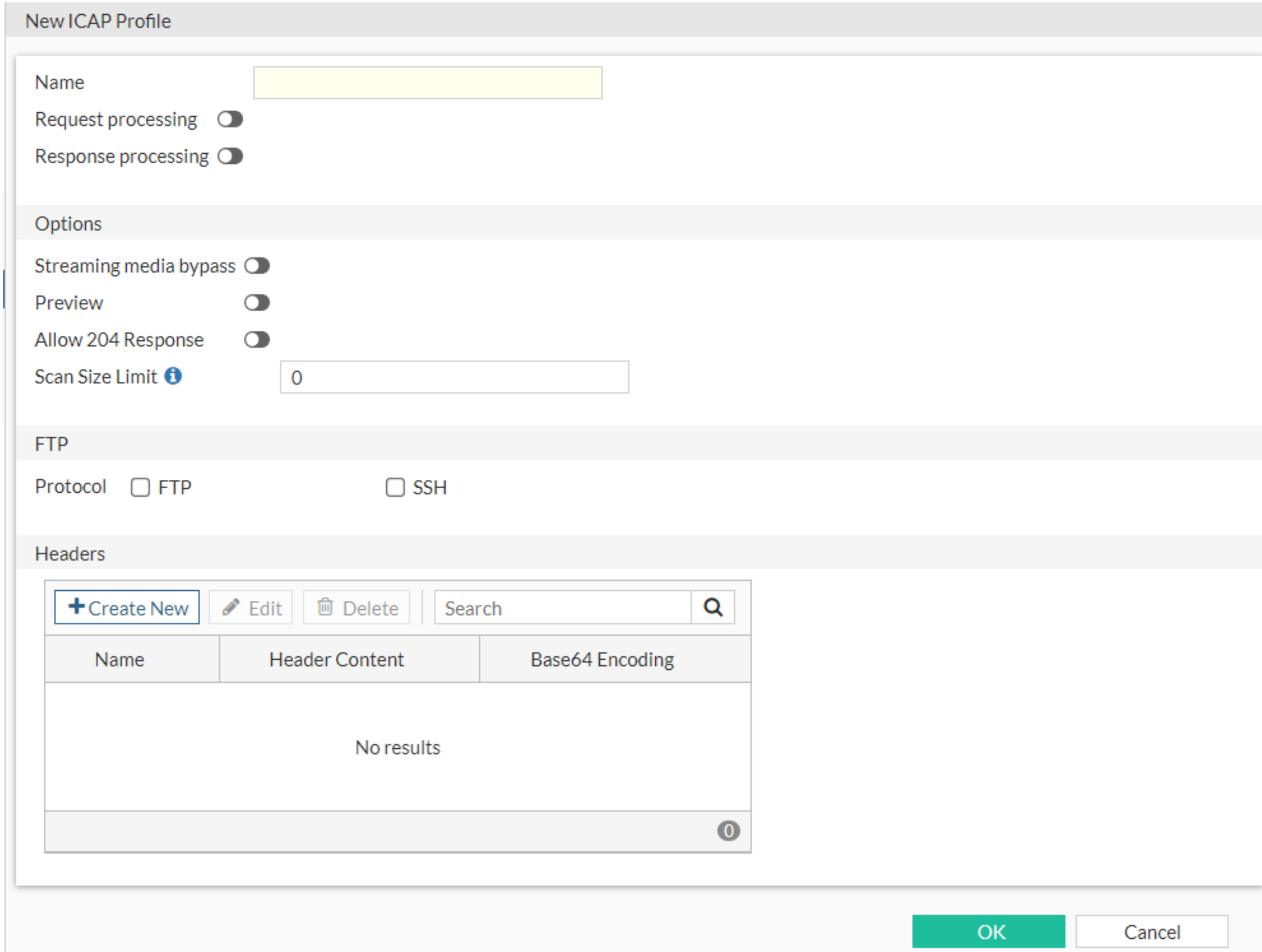
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create an ICAP profile. See Create or edit an ICAP profile on page 346.
Edit	Edit an ICAP profile. See Create or edit an ICAP profile on page 346.
Delete	Delete a profile or profiles.
Name	The name of the ICAP profile.
Request	Whether request processing is enabled or disabled.
Response	Whether response processing is enabled or disabled.
Streaming Content Bypass	Whether streaming media is allowed (enabled) to ignore offloading to the ICAP server.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit an ICAP profile

Select *Create New* to open the *New ICAP Profile* window.



To open the *Edit ICAP Profile* window, select an ICAP profile and then click *Edit*.

Configure the following settings in the *New ICAP Profile* window or *Edit ICAP Profile* window and then click *OK*:

Name	Specify a name for the ICAP profile. After you create an ICAP profile, you cannot change the name.
Request Processing	Enable or disable request processing. When enabled, you can further configure the following options: • **Server**—Select an existing server from the list or create a new server. • **Path**—Path to the processing component on the server, such as `/proprietary_code/content-filter/`. • **Method**—Allowed HTTP methods that will be sent to ICAP server for further processing. Click the *Add* button to add more methods to the list. Click the *Delete* button on the right of a method to delete it from the list. • **On failure**—Action to take if the ICAP server cannot be contacted when processing an HTTP request. • *Error*—HTTP or FTP traffic reports an error and is blocked when the ICAP server is down.

	• *Bypass*—HTTP or FTP traffic can still pass through when the ICAP server is down.

Response Processing	Enable or disable response processing.
	When enabled, you can further configure the following options:
	• **Server**—Select an existing server from the list or create a new server.
	• **Path**—Path to the processing component on the server, such as `/proprietary_code/content-filter/`.
	• **On failure**—Action to take if the ICAP server cannot be contacted when processing an HTTP response.
	  • *Error*—HTTP or FTP traffic reports an error and is blocked when the ICAP server is down.
	  • *Bypass*—HTTP or FTP traffic can still pass through when the ICAP server is down.

Streaming Media Bypass	Specify whether to bypass offloading of streaming media to the ICAP server. When enabled, streaming media is not offloaded to the ICAP server.
Preview	Enable preview of data to the ICAP server. When enabled, you can further configure the *Preview Data Length*, which is the preview data length to be sent to the ICAP server.
Allow 204 Response	Specify whether to allow 204 response. When enabled, you can further configure the *204 Size Limit*.
Scan Size Limit	Specify the ICAP server scan size limit for a single request within the range of 0-4096 (MB). The default is 0 MB, which means unlimited.

Protocol	Select the FTP protocol: FTP or SSH. You can select both.
	When a protocol is enabled, you can further configure the following options:
	• **Server**—Select an existing server from the list or create a new server.
	• **On failure**—Action to take if the FTP server cannot be contacted when processing an FTP request.
	  • *Error*—FTP traffic reports an error and is blocked when the FTP server is down.
	  • *Bypass*—FTP traffic can still pass through when the FTP server is down.
	• **Path**—Path to the processing component on the server, such as `/proprietary_code/content-filter/`.

Headers	View existing ICAP headers or create a new ICAP header using the *Create New* button. When creating a new ICAP header, specify the following options in the *Create Header* window: • **Name**—Name of the HTTP forwarded header. • **Header Content**—HTTP header content. • **Base64 Encoding**—Enable or disable base64 encoding of HTTP content.

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.

ICAP server response extension headers

ICAP server responses can be configured to include X-Virus-ID, X-Infection-Found, and X-Violation-Found extension headers.

```
config icap local-server
    edit 1
        config icap-service
            edit 1
                set extension-headers {X-Virus-id X-Infection-Found X-Violation-Found}
            next
        end
    next
end
```

`X-Virus-id`	Enable X-Virus-ID ICAP extension header.
`X-Infection-Found`	Enable X-Infection-Found ICAP extension header.
`X-Violation-Found`	Enable X-Violation-Found ICAP extension header.

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

You can 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 = 10)>
```

```
    next
end
```

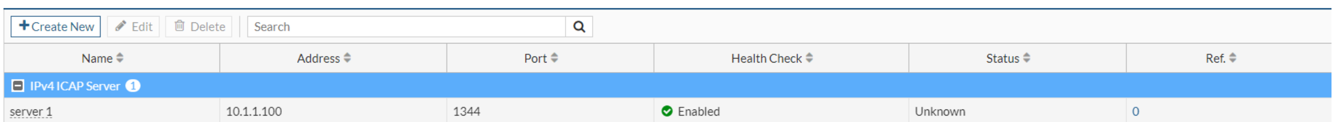
Timeout configuration for the FortiProxy ICAP client

You can 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 = 30)>
    next
end
```

ICAP Remote Server

To view the list of ICAP remote servers, go to *Content Analyses > ICAP Remote Servers*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

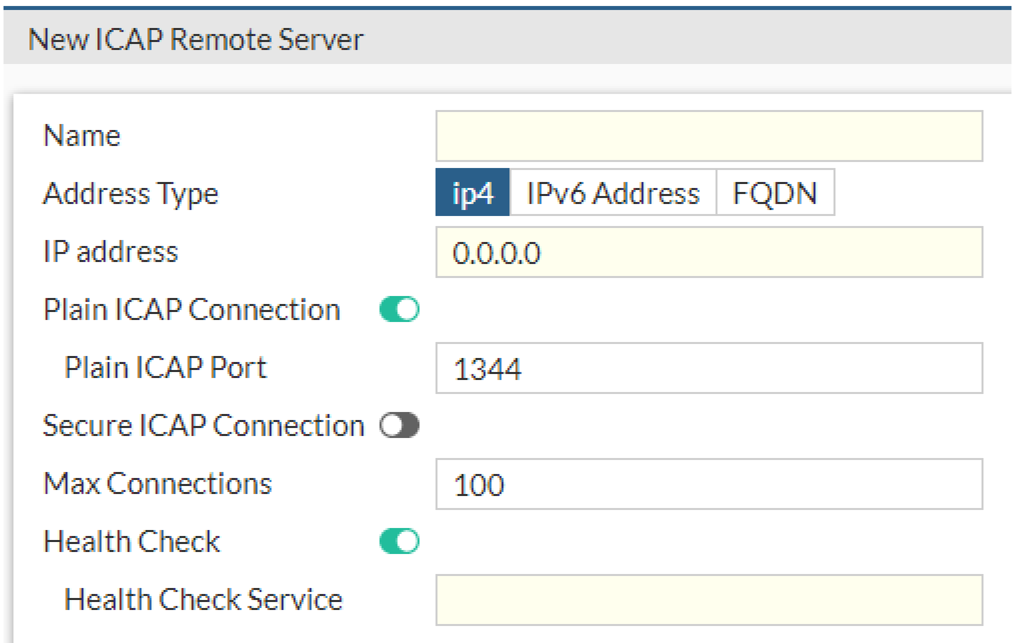
The following options are available:

Create New	Create an ICAP remote server. See Create or edit an ICAP remote server on page 351.
Edit	Edit an ICAP remote server. See Create or edit an ICAP remote server on page 351.
Delete	Delete an ICAP remote server or servers.
Name	The name of the ICAP remote server.
Address	The IP address of the ICAP remote server.
Port	The port number that the ICAP remote server is using.
Health Check	Indicates whether health check is enabled or disabled for the ICAP remote server.
Status	Health status of the ICAP remote server, which can be *Online*, *Offline*, or *Unknown*.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

The health check options are added in FortiProxy 7.2.3.

Create or edit an ICAP remote server

Select *Create New* to open the *New ICAP Remote Server* window.



To open the *Edit ICAP Remote Server* window, select a server and then click *Edit*.

Configure the following settings in the *New ICAP Remote Server* window or *Edit ICAP Remote Server* window and then click *OK*:

Name	Enter a name for the ICAP remote server. After you create an ICAP remote server, you cannot change the name.
Address Type	Select *IPv4* or *IPv6 Address* or *FQDN*.
IP Address/IPv6 Address/FQDN	Enter the IPv4 or IPv6 address or the Fully Qualified Domain Name (FQDN) for the ICAP remote server.
Plain ICAP Connection	Enable or disable unsecure connection from the FortiProxy unit to the remote ICAP server.
Secure ICAP Connection	Enable or disable secure SSL connection from the FortiProxy unit to the remote ICAP server.
Plain/Secure ICAP Port	Enter the TCP port number used by the ICAP remote server, from 1 to 65,535. The default is 1344.

Certificate	Select the CA certificate. This option is available only if you enable *Secure ICAP Connection*.
Max Connections	Enter the maximum number of concurrent connections to the ICAP remote server. Must not be less than wad-workercount. The default is 100. The valid value range is 0-4294967295.
Health Check	Enable or disable ICAP remote server health checking. When enabled, FortiProxy attempts to connect to the remote ICAP server to verify that the server is operating normally and generates an event log each time the ICAP server health check fails or goes back online. The default is disabled.
Health Check Service	Enter the ICAP service name to use for health checks.

To configure an ICAP remote server via CLI:

```
config icap remote-sever
   edit <server_name>
      set addr-type [ip4|ip6|fqdn]
      set ip-address {ipv4-address-any}
      set ip6-address {ipv6-address}
      set fqdn {string}
      set port {integer}
      set max-connections {integer}
      set secure [disable|enable]
      set ssl-cert {string}
      set healthcheck [disable|enable]
      set healthcheck-service {string}
   next
end
```

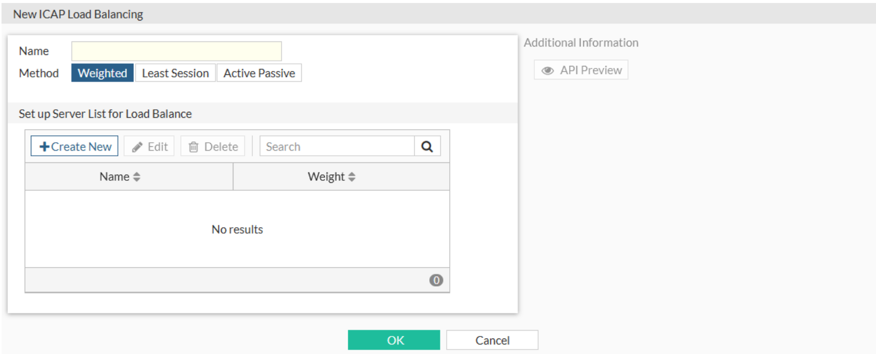
The health check options are added in FortiProxy 7.2.3.

ICAP Load Balancing

ICAP load balancing can be configure the balance the traffic load to ICAP servers based on assigned weights, send new sessions to the ICAP server with the lowest session count, or send new sessions to the active ICAP server with the highest weight.

To configure an ICAP load balancing in the GUI:

1. Go to *Content Analyses > ICAP Load Balancing* and click *Create New*.



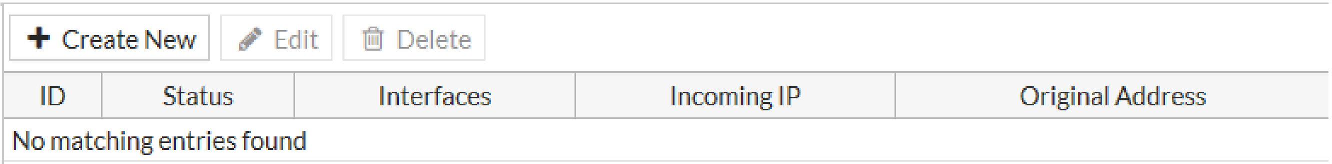
2. Enter a name for the ICAP load-balancing configuration.
3. Select the load-balancing method:
   - *Weighted*: Balance the traffic load to ICAP servers based on the assigned weights.
   - *Least Session*: Send new sessions to the ICAP server with the lowest session count.
   - *Active Passive*: Send new sessions to the active ICAP server with the highest weight.
4. To create a server list for load balancing:
   a. Click *Create New* in the *Set up Server List for Load Balance* table.
   b. Select or create a remote server. See ICAP Remote Server on page 350 for information.
   c. Enter a weight for the remote server.
   d. Click *OK*.
   e. Add more servers as required.
5. Click *OK*.

To configure an ICAP load balancing in the CLI:

```
config icap remote-server-group
    edit <name>
        set ldb-method {weighted | least-session | active-passive}
        config server-list
            edit <ICAP_remote_server>
                set weight <integer>
            next
        end
    next
end
```

ICAP Local Server

To view the list of ICAP local servers, go to *Content Analyses> ICAP Local Servers*.



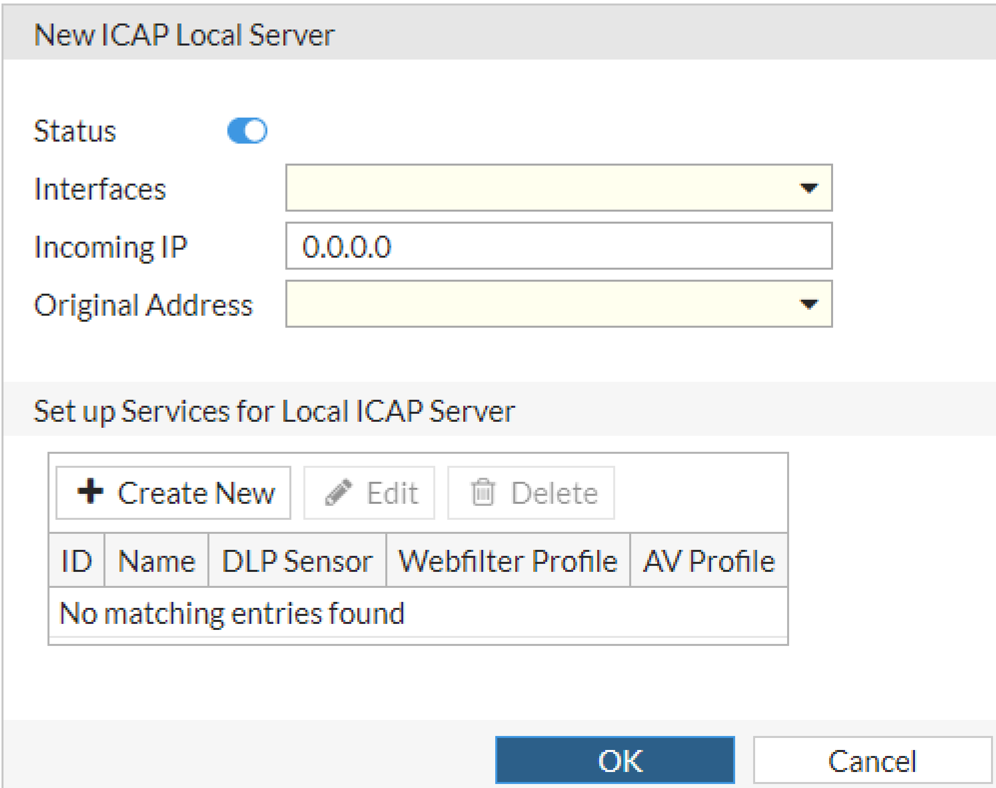
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create an ICAP local server. See Create or edit an ICAP local server on page 354.
Edit	Edit an ICAP local server. See Create or edit an ICAP local server on page 354.
Delete	Delete an ICAP local server or servers.
ID	The identifier for the ICAP local server.
Status	Whether the server is active.
Interfaces	The interface that the ICAP local server will use.
Incoming IP	The IP address that the ICAP local server will use.
Original Address	The original address.

Create or edit an ICAP local server

Select *Create New* to open the New ICAP Local Server window.



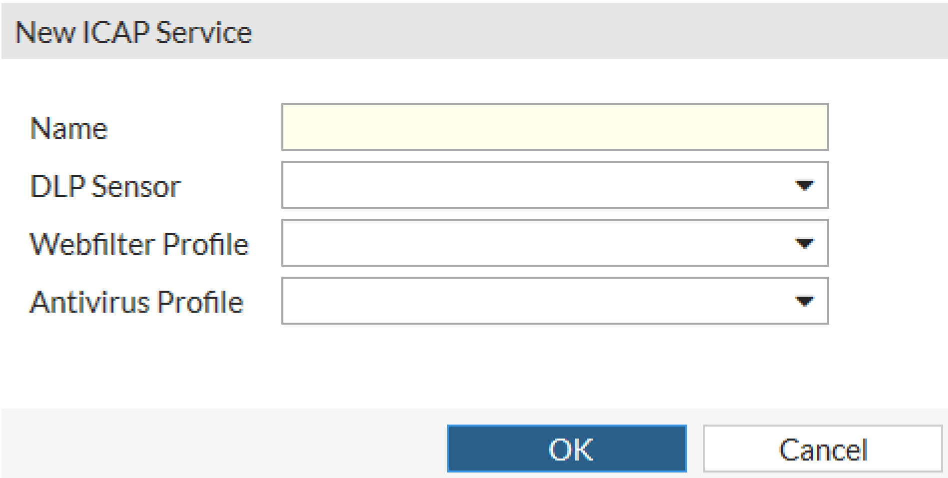
To open the Edit ICAP Local Server window, select a server and then click *Edit*.

Configure the following settings in the New ICAP Local Server window or Edit ICAP Local Server window and then click *OK*:

Status	Enable or disable this ICAP local server.
Interfaces	Select an interface for the ICAP local server to use.
Incoming IP	Enter an IP address for the ICAP local server to use.
Original Address	Select the original address.
Create New	Create an ICAP service. See Create or edit an ICAP service on page 356.
Edit	Edit an ICAP service. See Create or edit an ICAP service on page 356.
Delete	Delete an ICAP service.
ID	The identifier for the ICAP service.
Name	The name of the ICAP service.
DLP Sensor	The DLP sensor used by the ICAP service.
Webfilter Profile	The web filter profile used by the ICAP service.
AV Profile	The antivirus profile used by the ICAP service.

Create or edit an ICAP service

Select *Create New* to open the New ICAP Service window.



To open the Edit ICAP Service window, select an ICAP service and then click *Edit*.

Configure the following settings in the New ICAP Service window or Edit ICAP Service window and then click *OK*:

Name	Enter the name of the ICAP service.
DLP Sensor	Select the DLP sensor that the ICAP service will use. See Create or edit a DLP sensor on page 331.
Webfilter Profile	Select the web filter profile that the ICAP service will use. See Create or edit a web filter profile on page 277.
AV Profile	Select the antivirus profile that the ICAP service will use. See Create or edit an antivirus profile on page 265.

ICAP scanning with FTP

Transferred files can be forwarded to the ICAP server for further processing using FTP.

To configure ICAP scanning with FTP in the GUI:

1. Configure an ICAP remote server.
2. Create an ICAP profile that references the server.

- Select *FTP* in *Protocol*.
- Select the server you created in step 1 in *Server*.

3. Enable and configure explicit FTP Proxy on page 81.
4. Create an explicit FTP proxy policy that uses the ICAP profile.

- Select *FTP* under *Type* for an explicit FTP proxy policy.
- Select *ACCEPT* for *Action* to enable the *Security Profiles* options. You can then enable *ICAP* and select the ICAP profile you configured in step 2 from the dropdown list.

To configure ICAP scanning with FTP in the CLI:

1. Configure an ICAP remote server:

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

   See config icap remote-server in the CLI guide for more details.
2. Create an ICAP profile that references the server:

```
config icap profile
    edit "icapFTP"
        set file-transfer ftp
        set file-transfer-server "icap1"
        set file-transfer-failure error
        set file-transfer-path "ftpicap"
    next
end
```

   See config icap profile in the CLI guide for more details.
3. Enable and configure explicit FTP Proxy:

```
config ftp-proxy explicit
    set status [enable|disable]
    set incoming-port {user}
    set incoming-ip {ipv4-address-any}
    set outgoing-ip {ipv4-address-any}
    set sec-default-action [accept|deny]
    set server-data-mode [client|passive]
    set ssl [enable|disable]
    set ssl-cert {string}
    set ssl-dh-bits [768|1024|...]
    set ssl-algorithm [high|medium|...]
end
```

   See config ftp-proxy explicit in the CLI guide for more details.
4. Create an explicit FTP proxy policy that uses the ICAP profile:

```
config firewall policy
    edit 1
        set type explicit-ftp
        set name "test"
        set dstintf "any"
        set srcaddr "all"
```

```
            set dstaddr "all"
            set action accept
            set schedule "always"
            set ssl-ssh-profile "certificate-inspection"
            set utm-status enable
            set icap-profile "icapFTP"
        next
    end
```

See config firewall policy in the CLI guide for more details.

WAN Optimization

You can add WAN optimization to improve traffic performance and efficiency as it crosses the WAN. For more information about WAN optimization, see WAN optimization on page 20.

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.

This section describes the following:

- Profiles on page 359
- Peers on page 363
- Authentication Groups on page 364

Profiles

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 the following:

- Protocol optimization—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—Byte caching caches files and other data on FortiProxy units to reduce the amount of data transmitted across the WAN.
- Web caching—Web caching stores web pages on FortiProxy units to reduce latency and delays between the WAN and web servers.
- SSL offloading—SSL offloading offloads SSL decryption and encryption from web servers onto FortiProxy SSL acceleration hardware.
- Secure tunneling—Secure tunneling secures traffic as it crosses the WAN.

You can apply different combinations of these WAN optimization techniques to a single traffic stream depending on the traffic type. For example, you can apply byte caching and secure tunneling to any TCP traffic. For HTTP and HTTPS traffic, you can also apply protocol optimization and web caching.

You can view the list of WAN optimization profiles by going to *WAN Optimization* > *Profiles* and selecting the List icon (the farthest right of the three icons in the upper right of the window; it resembles a page with some lines on it) in the *Edit WAN Optimization Profile* page toolbar.

+ Create New | Edit | Delete

Name	Ports	Transparent	Authentication Group	Comments
default	CIFS/445 FTP/21 HTTP/80 MAPI/135 TCP/1-65535	Enabled	NewAuthGroup	Default WANopt profile.

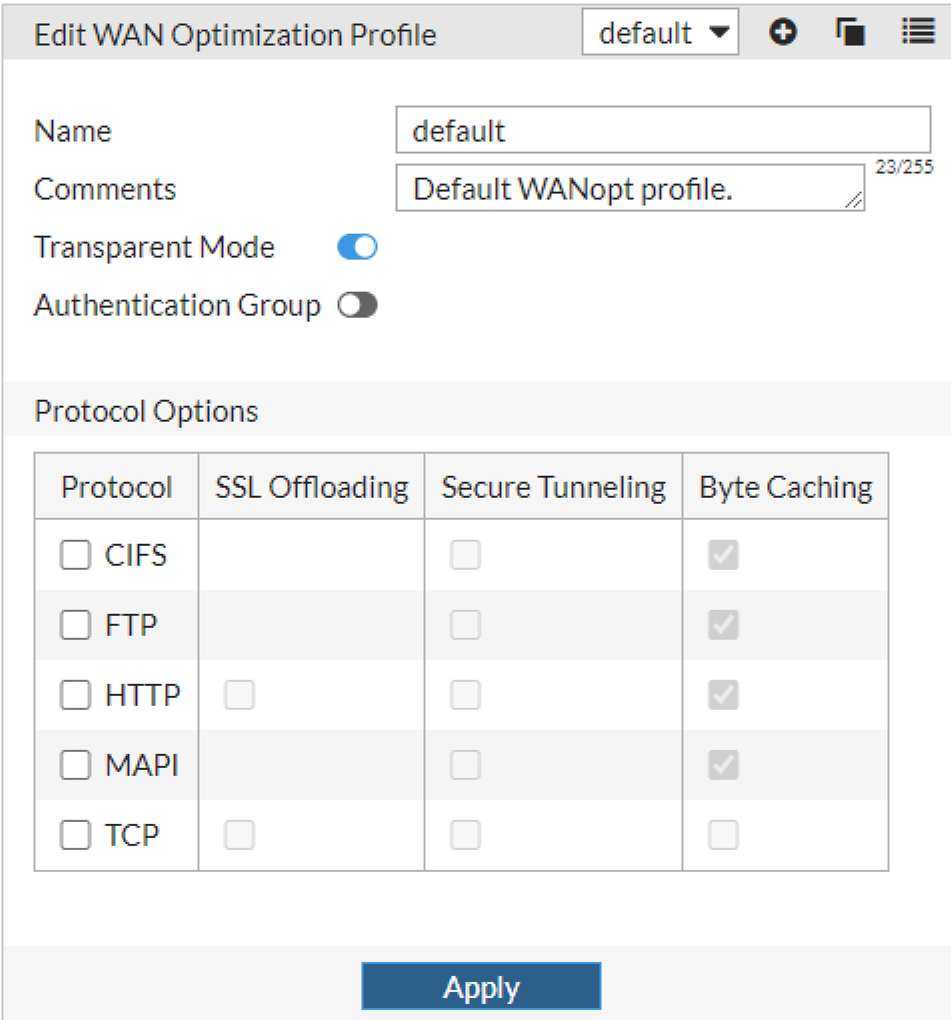
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a WAN optimization profile. See Create or edit a WAN optimization profile on page 360.
Edit	Modify the profile. See Create or edit a WAN optimization profile on page 360.
Delete	Remove the profile.
Name	The name of the WAN optimization profile.
Ports	The ports used by the profile.
Transparent	Whether the WAN optimization transparent mode is enabled. For more information about the WAN optimization transparent mode, see WAN optimization transparent mode on page 20.
Authentication Group	The authentication group used by the profile, if any. See Authentication Groups on page 364.
Comments	Optional description of the WAN optimization profile.

Create or edit a WAN optimization profile

To configure WAN optimization profiles, go to *WAN Optimization* > *Profiles*. The *Edit WAN Optimization Profile* page is displayed.



Configure the following settings and then select *Apply* to save your changes:

drop-down list	Select a profile to edit from the drop-down list. See To create a WAN optimization profile: on page 362.
Create New icon	Create a WAN optimization profile. See To edit a WAN optimization profile: on page 362.
Clone icon	Clone the current profile. See To clone a WAN optimization profile: on page 362.
List icon	View the WAN optimization profile list. See Profiles on page 359.
Name	Enter a name for the WAN optimization profile.
Comments	Optionally, enter a description of the profile.
Transparent Mode	Enable or disable transparent mode. For more information about the WAN optimization transparent mode, see WAN optimization transparent mode on page 20.

Authentication Group	Enable to select the authentication group from the drop-down list that will be applied to the WAN optimization profile. To create an authentication group, see Create or edit an authentication group on page 365.
Protocol	Select the protocols that are enabled for this profile: *CIFS*, *FTP*, *HTTP*, *MAPI*, and *TCP*. **NOTE:** The FortiProxy unit supports WAN optimization for SMBv1, SMBv2 and SMBv3 (unencrypted only) protocols.
SSL Offloading	Select to enable SSL offloading. SSL offloading offloads SSL decryption and encryption from web servers onto FortiProxy SSL acceleration hardware. It is only available for HTTP and TCP protocols.
Secure Tunneling	Select to enable secure tunneling. To use secure tunneling, it must be enabled for a protocol, and an authentication group must be added. The authentication group specifies the certificate or pre-shared key used to set up the secure tunnel. The *Peer Acceptance* setting of the authentication group does not affect secure tunneling. The FortiProxy units at each end of the secure tunnel must have the same authentication group with the same name and the same configuration, including the same pre-shared key or certificate.
Byte Caching	Select to enable byte caching. Byte caching breaks large units of application data (for example, a file being downloaded from a web page) into small chunks of data, labeling each chunk of data with a hash of the chunk and storing those chunks and their hashes in a database. The database is stored on a WAN optimization storage device.

You can add, edit, clone, and delete WAN optimization profiles.

To create a WAN optimization profile:

1. From either the *Edit WAN Optimization Profile* page or the WAN optimization profile list, select *Create New*.
2. Enter the required information and then click *OK* to create the new WAN optimization profile.

To edit a WAN optimization profile:

1. From the *Edit WAN Optimization Profile* page, select the profile you need to edit from the profile drop-down list.
   Alternatively, from the profile list, either select the profile you want to edit and then click *Edit* from the toolbar or double-click on the profile name in the list. The *Edit WAN Optimization Profile* page opens.
2. Edit the information as required and then select *Apply* to apply your changes.

To clone a WAN optimization profile:

1. From the *Edit WAN Optimization Profile* page, select the profile you need to clone from the profile drop-down list.
2. Select *Clone* from the toolbar.
3. Enter a name for the profile in the dialog box and then click *OK*.
4. Edit the clone as required.

To delete a profile or profiles:

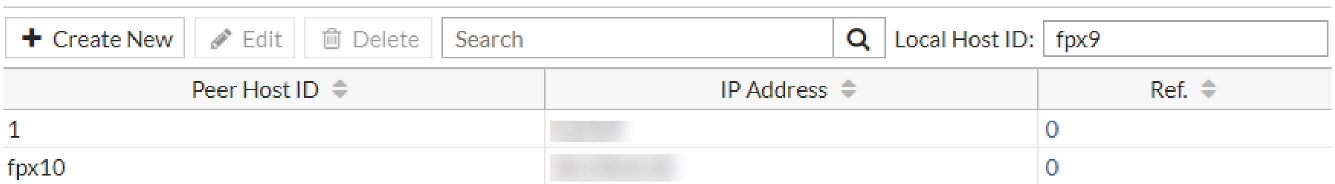
1. From the profile list, select the profile or profiles that you want to delete.
2. Click *Delete* from the toolbar.
3. Click *OK* in the confirmation dialog box to delete the selected profile or profiles.

Peers

The client-side and server-side FortiProxy units are called WAN optimization peers because all of the FortiProxy units in a WAN optimization network have the same peer relationship with each other. The client and server roles relate to how a session is started. Any FortiProxy unit configured for WAN optimization can be both a client-side and a server-side FortiProxy unit at the same time, depending on the direction of the traffic. Client-side FortiProxy units initiate WAN optimization sessions, and server-side FortiProxy units respond to the session requests. Any FortiProxy unit can be a client-side FortiProxy unit for some sessions and a server-side FortiProxy unit for others.

To identify all of the WAN optimization peers that a FortiProxy unit can perform WAN optimization with, host IDs and IP addresses of all of the peers are added to the FortiProxy unit configuration. The peer IP address is actually the IP address of the peer unit interface that communicates with the FortiProxy unit.

Go to *WAN Optimization > Peer Settings* to view the WAN optimization peer list.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

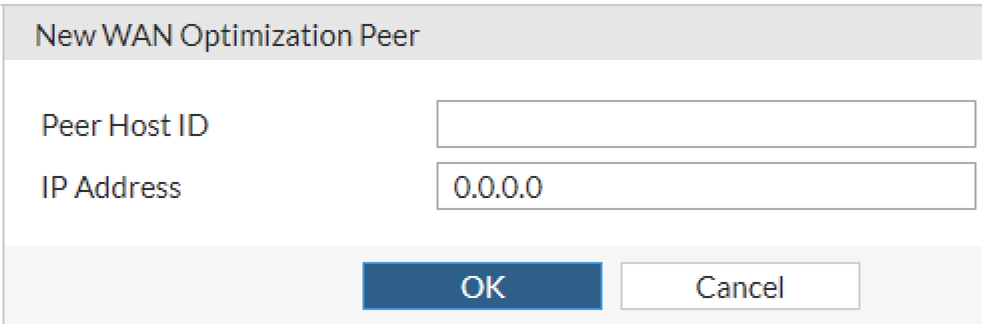
The following options are available:

Create New	Create a WAN optimization peer. See To create a WAN optimization peer: on page 364.
Edit	Edit a WAN optimization peer. See To create a WAN optimization peer: on page 364.
Delete	Delete a WAN optimization peer or peers.
Search	Enter a search term to search for in the peer list.
Local Host ID	The local host identifier. Enter an identifier and then select *Apply* to apply the identifier.
Peer Host ID	The peer host identifier of the WAN optimization peer.
IP Address	The IP address of the peer.
Ref.	Displays the number of times the object is referenced to other objects.

To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a WAN optimization peer

To create a WAN optimization peer:

1. From the peer list, select *Create New* in the toolbar.
   The *New WAN Optimization Peer* window opens.
   

2. Enter the *Peer Host ID* and *IP Address*.
3. Click *OK* to create the new peer.

To edit a WAN optimization peer:

1. Select the peer that you want to edit in the peer list and then click *Edit* from the toolbar or double-click on the peer in the peer list. The *Edit WAN Optimization Peer* window opens.
2. Edit the peer as required and click *OK* to apply your changes.

To delete a WAN optimization peer or peers:

1. Select the peer or peers that you want to delete in the peer list.
2. Click *Delete* from the toolbar.
3. Click *OK* in the confirmation dialog box to delete the selected peer or peers.

Authentication Groups

You need to add authentication groups to support authentication and secure tunneling between WAN optimization peers.

To perform authentication, WAN optimization peers use a certificate or a pre-shared key added to an authentication group, so they can identify each other before forming a WAN optimization tunnel. Both peers must have an authentication group with the same name and settings. The authentication group is added to a peer-to-peer or active rule on the client-side FortiProxy unit. When the server-side FortiProxy unit receives a tunnel start request that includes an authentication group from the client-side unit, the server-side unit finds an authentication group in its configuration with the same name. If both authentication groups have the same certificate or pre-shared key, the peers can authenticate and set up the tunnel.

Go to *WAN Optimization > Authentication* to manage the authentication groups.

+ Create New | Edit | Delete | Search

Name	Authentication Method	Peer(s)	Ref.
NewAuthenticationGroup	Certificate (Fortinet_CA_SSL)	Any	0

Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

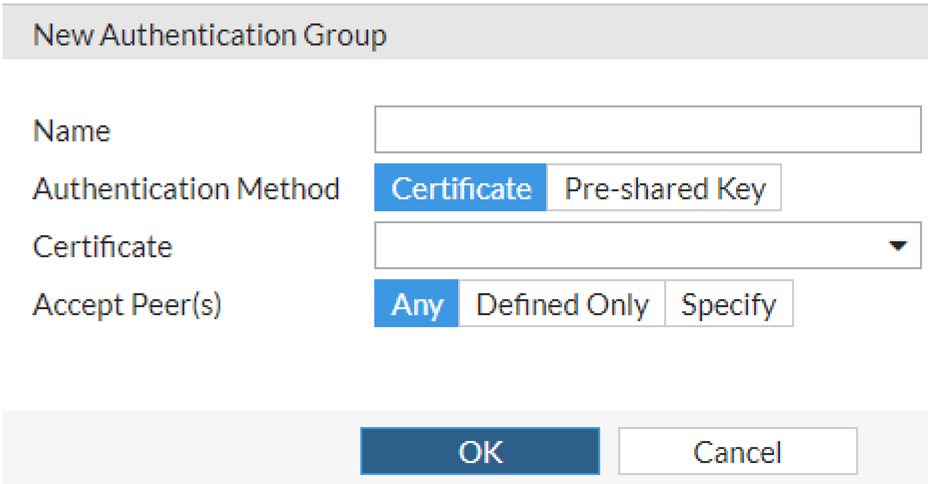
The following options are available:

Create New	Create an authentication group. See Create or edit an authentication group on page 365.
Edit	Edit an authentication group. See Create or edit an authentication group on page 365.
Delete	Delete an authentication group or groups.
Search	Enter a search term to search for in the group list.
Name	The name of the authentication group.
Authentication Method	The authentication used by the group, either *Certificate* or *Pre-shared key*.
Peer(s)	The peer or peers in the authentication group.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit an authentication group

To create an authentication group:

1. Go to *WAN Optimization > Authentication*.
2. Select *Create New* from the toolbar.
   The *New Authentication Group* window opens.



3. Enter the following information:

Name	Enter a name for the authentication group.
Authentication Method	Select the authentication method to use. • *Certificate*: Use a certificate to authenticate and encrypt WAN optimization tunnels. Then select a local certificate that has been added to this FortiProxy unit from the drop-down list. • *Pre-shared Key*: Use a pre-shared key or password to authenticate and encrypt WAN optimization tunnels. Then enter the password (or pre-shared key) in the *Password* field. Other FortiProxy units that participate in WAN optimization tunnels with this unit must have an authentication group with the same name and password. The password must contain at least 6 printable characters and should be known only by network administrators. For optimum protection against currently known attacks, the key should consist of a minimum of 16 alphanumeric characters.
Certificate	Select a local certificate from the drop-down list.
Pre-shared Key	Enter the pre-shared key.
Accept Peer(s)	Select the peer acceptance method for the authentication group. • *Any*: If you do not know the peer host IDs or IP addresses of the peers that will use this authentication group. This setting is most often used for WAN optimization with FortiProxy units that do not have static IP addresses, such as units that use DHCP. • *Defined Only*: Authenticate with peers that have added to the peer list only. • *Specify*: Select a peer from the drop-down list to authenticate with the selected peer only. Select *Create New* from the drop-down list to create a peer; see Create or edit a WAN optimization peer on page 364.

4. Click *OK* to create the new authentication group.

   The authentication group can now be added to WAN optimization profiles to apply the authentication settings in the authentication group to the profile. See Create or edit a WAN optimization profile on page 360.

To edit an authentication group:

1. Go to *WAN Optimization > Authentication*.
2. Select the group you want to edit and then click *Edit* from the toolbar or double-click on the group in the authentication group list.
   The *Edit Authentication Group* window opens.
3. Edit the group information as required and click *OK* to apply your changes.

To delete an authentication group or groups:

1. Go to *WAN Optimization > Authentication*.
2. Select the group or groups that you want to delete.
3. Click *Delete* from the toolbar.
4. Click *OK* in the confirmation dialog box to delete the selected group or groups.

Web Cache

You can use web caching to cache web pages from any web server. All traffic between a client network and one or more web servers is then 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.

In a standard web caching configuration, the FortiProxy unit caches pages for users on a client network. A router sends HTTP traffic to be cached to the FortiProxy unit.

You can also create a reverse proxy web caching configuration where the FortiProxy unit is dedicated to providing web caching for a single web server or server farm. In this second configuration, one or more FortiProxy units can be installed between the server network, and the WAN or Internet or traffic to be cached can be routed to the FortiProxy units.

This section describes the following:

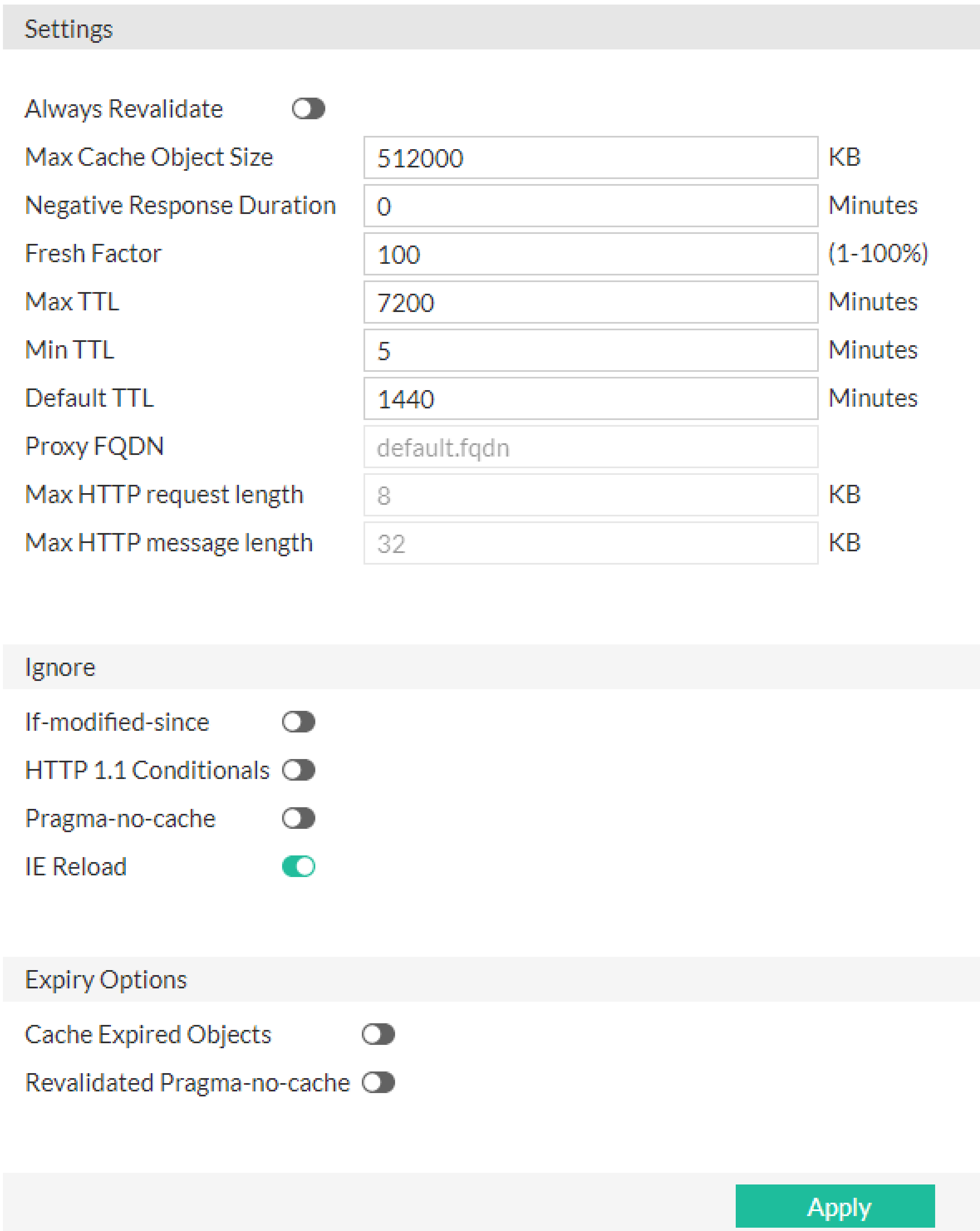
- Settings on page 368
- Prefetch URLs on page 372
- Reverse Cache Server on page 374
- Prefetch File on page 375
- WCCP Settings on page 378
- User Agent on page 385

Settings

You can optimize web cache settings to improve performance and exempt specific URL patterns from caching and/or forward them to a web proxy server.

In most cases, the default settings for the WAN optimization web cache are acceptable. However, you might want to change them to improve performance or optimize the cache for your configuration.

Go to *Web Cache > Settings* to configure web cache settings.



Configure the following settings and then select *Apply* to save your changes:

Always Revalidate	Always re-validate requested cached objects with content on the server before serving them to the client.

Max Cache Object Size	The maximum size of objects (files) that are cached (the default is 512,000 KB). Objects that are larger than this size are still delivered to the client but are not stored in the FortiProxy web cache.
Negative Response Duration	The amount of time, in minutes, that the FortiProxy unit caches error responses from web servers (default is 0 minutes). The content server might send a client error code (4xx HTTP response) or a server error code (5xx HTTP response) as a response to some requests. If the web cache is configured to cache these negative responses, it returns that response in subsequent requests for that page or image for the specified number of minutes, regardless of the actual object status.
Fresh Factor	For cached objects that do not have an expiry time, the web cache periodically checks the server to see if the objects have expired. The higher the fresh factor, the less often the checks occur (default is 100%). For example, if you set *Max TTL* and *Default TTL* to 7,200 minutes (5 days) and set *Fresh Factor* to 20, the web cache checks the cached objects 5 times before they expire, but, if you set the *Fresh Factor* to 100, the web cache will only check once.
Max TTL	The maximum amount of time (Time to Live), in minutes, an object can stay in the web cache without the cache checking to see if it has expired on the server. From 1 to 5,256,000 minutes (one year) (default is 7,200 minutes).
Min TTL	The minimum amount of time an object can stay in the web cache before the web cache checks to see if it has expired on the server. From 1 to 5,256,000 minutes (default is 5 minutes).
Default TTL	The default expiry time for objects that do not have an expiry time set by the web server. From 1 to 5,256,000 minutes (default is 1,440 minutes).
Proxy FQDN	This setting cannot be changed from the default: *default.fqdn*.
Max HTTP request length	This setting cannot be changed from the default: *4KB*.
Max HTTP message length	This setting cannot be changed from the default: *32KB*.
Ignore	
If-modified-since	If the time specified by the if-modified-since (IMS) header in the client's conditional request is greater than the last modified time of the object in the cache, it is a strong indication that the copy in the cache is stale. If so, HTTP does a conditional GET to the original content source, based on the last modified time of the cached object. Enable ignoring if-modified-since to override this behavior.
HTTP 1.1 Conditionals	HTTP 1.1 provides additional controls to the client for the behavior of caches toward stale objects. Depending on various cache-control headers, the FortiProxy unit can be forced to consult the OCS before serving the object from the cache. For more information about the behavior of cache-control header values, see RFC 2616. Enable ignoring HTTP 1.1 conditionals to override this behavior.

Pragma-no-cache	Typically, if a client sends an HTTP GET request with a pragma no-cache (PNC) or cache-control no-cache header, a cache must consult the OCS before serving the content. This behavior means that the unit always re-fetches the entire object from the OCS, even if the cached copy of the object is fresh. Because of this behavior, PNC requests can degrade performance and increase server-side bandwidth use. Enable ignoring Pragma-no-cache so that the PNC header from the client request is ignored. The FortiProxy unit treats the request as if the PNC header is not present.
IE Reload	Some versions of Internet Explorer issue Accept / header instead of Pragma no-cache header when you select *Refresh*. When an Accept header has only the / value, the FortiProxy unit treats it as a PNC header if it is a type-N object. Enable ignoring IE reload to cause the FortiProxy unit to ignore the PNC interpretation of the Accept / header.
Expiry Options	
Cache Expired Objects	Enable to cache expired type-1 objects (if all other conditions make the object cacheable).
Revalidated Pragma-no-cache	The PNC header in a request can affect how efficiently the device uses bandwidth. If you do not want to completely ignore PNC in client requests by selecting *Ignore > Pragma-no-cache*, you can lower the impact on bandwidth usage with this option. When selected, a client's nonconditional PNC-GET request results in a conditional GET request sent to the OCS if the object is already in the cache. This gives the OCS a chance to return the *304 Not Modified* response, which consumes less server-side bandwidth because the OCS has not been forced to return full content. By default, *Revalidate Pragma-no-cache* is disabled and is not affected by changes in the top-level profile. When the Substitute Get for PNC configuration is enabled, the revalidate PNC configuration has no effect. Most download managers make byte-range requests with a PNC header. To serve such requests from the cache, you need to also configure byte-range support when you configure the *Revalidate pragma-no-cache* option.

HTTP traffic caching reports

Another way to review traffic caching is to generate top-entry reports with the following CLI commands:

```
config system global
   set http-view {enable | disable}
end
```

After enabling top-entry reports, you can execute and generate six different kinds of reports, depending upon what statistics you are interested in. Enter the following command:

```
execute http-view report {00 | 01 | 02 | 03 | 04 | 05}
```

Enter the two-digit value for the report that you want generated:

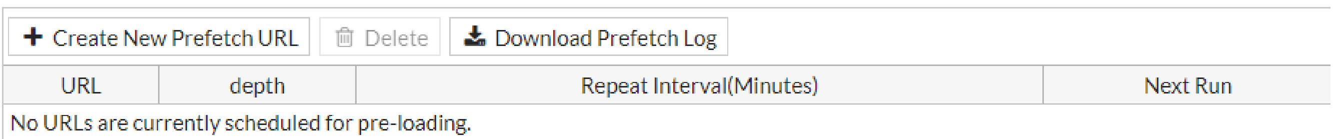
- **00:** Top entries by total HTTP requests
- **01:** Top entries by bandwidth consumed
- **02:** Top entries by cacheable percent of total requests
- **03:** Top entries by cache hit percent of total requests
- **04:** Top entries by cache hit percent of cacheable requests
- **05:** Top entries by bandwidth saved with cache hits

Each generated report shows the appropriate domain traffic within the last hour.

Prefetch URLs

To improve the speed of your system, you can specify URLs to preload.

To see the list of prefetch files of URLs to preload, go to *Web Cache > Prefetch URLs*.



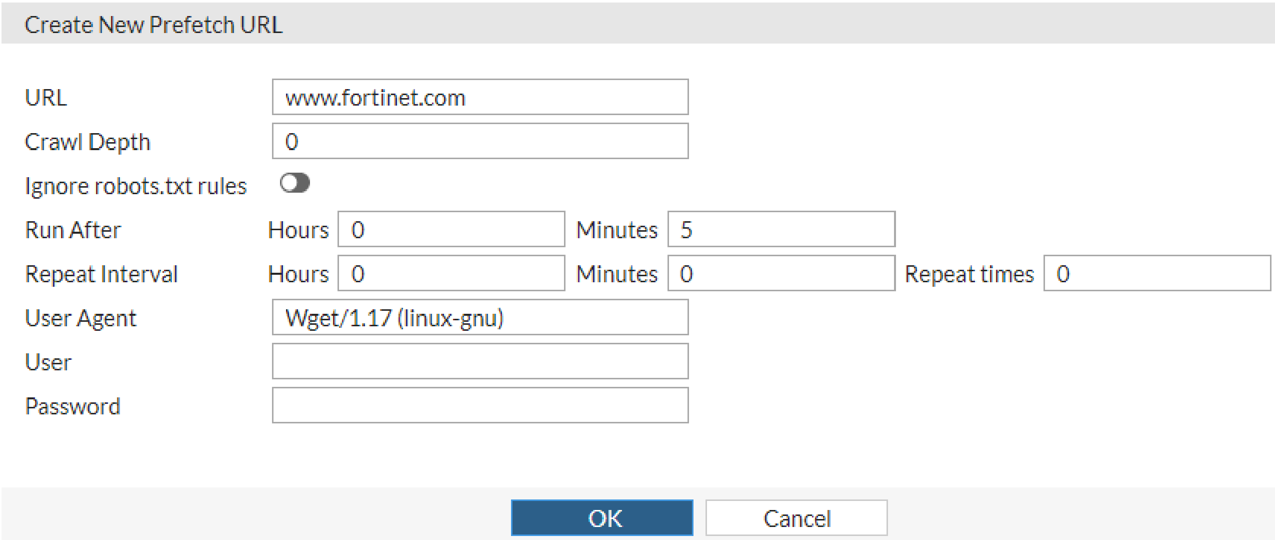
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New Prefetch URL	Add a new prefetch file. See To create a prefetch file: on page 372.
Edit	Edit the selected prefetch file. See To edit a prefetch file: on page 373.
Delete	Delete the selected prefetch file. See To delete a prefetch file or files: on page 373.
Download Prefetch Log	Select to download the prefetch log.
URL	The URLs to preload.
Depth	How many levels deep to preload.
Repeat Interval (Minutes)	How often, in minutes, to preload the URLs.
Next Run	When the URLs will be preloaded next.

To create a prefetch file:

1. Go to *Web Cache > Prefetch URLs* and select *Create New Prefetch URL* from the toolbar. The *Create New Prefetch URL* window opens.



2. Configure the following settings:

URL	Enter the URLs to preload. Separate multiple URLS with a semicolon.
Crawl Depth	Enter how many levels deep to preload the URLs.
Ignore robots.txt rules	Enable to ignore the rules found in the `robots.txt` file.
Run After	Select when the URL is preloaded the first time.
Repeat Interval	Enter how often to preload the URLs and how many times to preload the URLs.
User Agent	The name of the computer program to use to preload the URLs.
User	The user name for the user agent.
Password	The password for the user agent.

3. Click *OK* to create the new prefetch file.

To edit a prefetch file:

1. Go to *Web Cache > Prefetch URLs*.
2. Select the file that you want to edit and then click *Edit* from the toolbar or double-click on the file in the table. The *Edit Reverse Cache Prefetch* window opens.
3. Edit the information as required, then click *OK* to apply your changes.

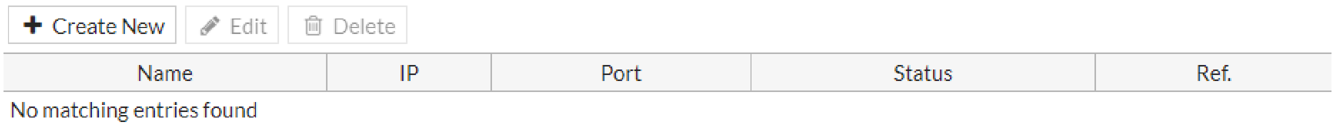
To delete a prefetch file or files:

1. Go to *Web Cache > Prefetch URLs*.
2. Select the file or files that you want to delete.
3. Click *Delete* from the toolbar.
4. Click *OK* in the confirmation dialog box to delete the selected file or files.

Reverse Cache Server

If you want to use reverse proxy web-caching, you need to configure a reverse cache server. For more information about reverse proxy web caching, see Web-caching topologies on page 26.

To see the list of reverse cache servers, go to *Web Cache > Reverse Cache Server*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

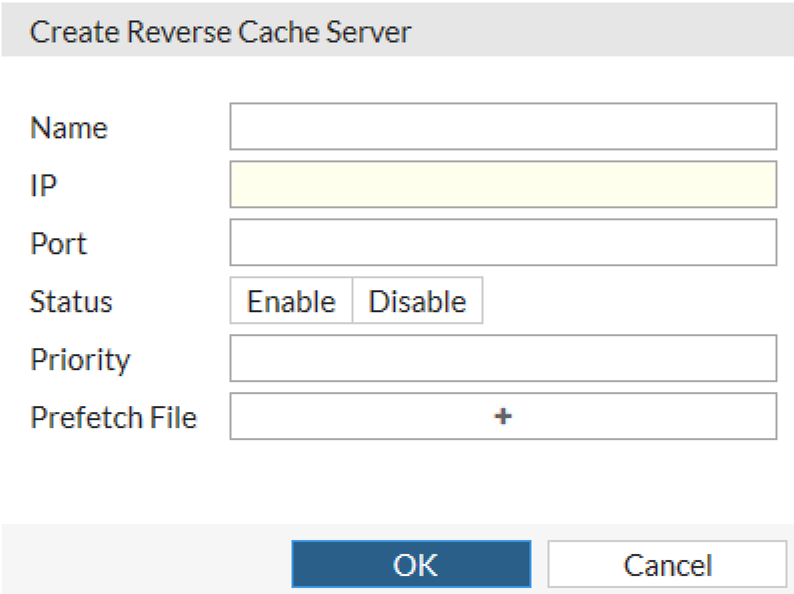
The following options are available:

Create New	Add a new reverse cache server. See Create or edit a reverse cache server on page 374.
Edit	Edit the selected reverse cache server. See Create or edit a reverse cache server on page 374.
Delete	Delete the selected reverse cache server.
Name	The name of the reverse cache server.
IP	The IP address of the reverse cache server.
Port	The port number that the reverse cache server is using.
Status	The status is *Enabled* or *Disabled*.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a reverse cache server

To create a reverse cache server:

1. Go to *Web Cache > Reverse Cache Server* and select *Create New* from the toolbar. The *Create Reverse Cache Server* window opens.



2. Configure the following settings:

Name	Enter a name for the reverse cache server.
IP	Enter the IP address of the reverse cache server.
Port	Enter the port number that the reverse cache server will use.
Status	Enable or disable the reverse cache server.
Priority	Enter a number to indicate the priority of the reverse cache server.
Prefetch File	If you created a prefetch file of URLs that you want preloaded, select + to open the Select Entries window and then select the prefetch file. To create a prefetch file, see Prefetch URLs on page 372.

3. Click *OK* to create the reverse cache server.

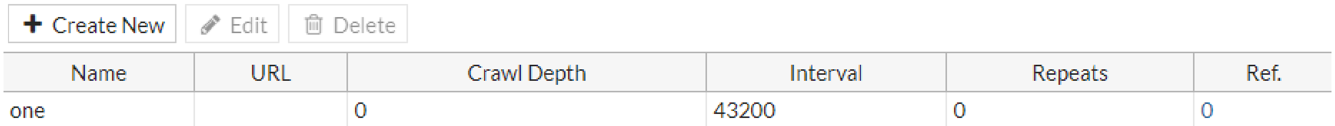
To edit a reverse cache server:

1. Go to *Web Cache* > *Reverse Cache Server*.
2. Select the server you want to edit and then click *Edit* from the toolbar or double-click on the server in the table. The *Edit Reverse Cache Server* window opens.
3. Edit the information as required and then click *OK* to apply your changes.

Prefetch File

Use the prefetch file to specify which URLs to preload.

To see the list of prefetch files, go to *Web Cache* > *Prefetch File*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

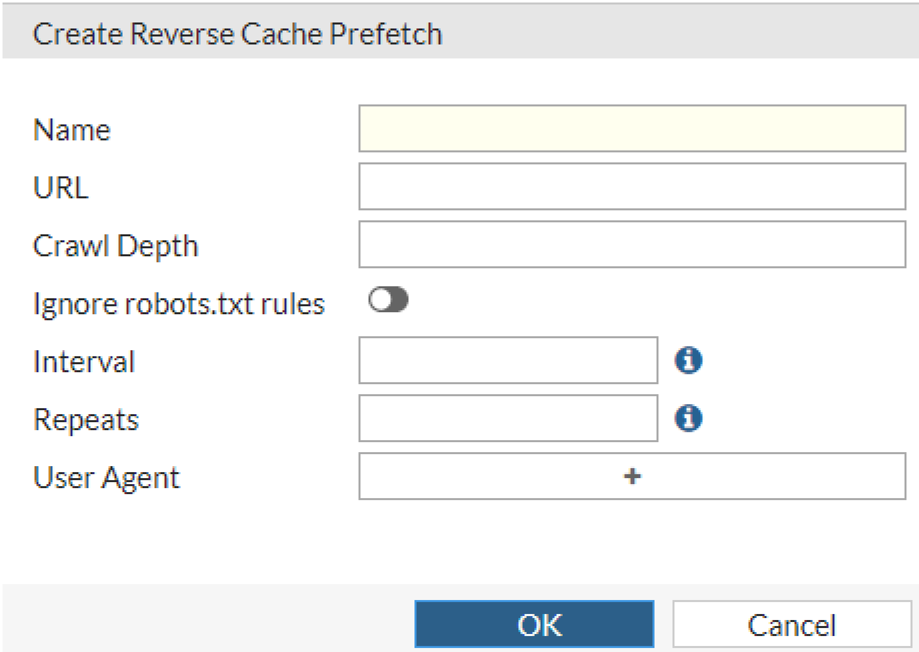
The following options are available:

Create New	Add a new prefetch file. See Create or edit a prefetch file on page 376.
Edit	Edit the selected prefetch file. See Create or edit a prefetch file on page 376.
Delete	Delete the selected reverse cache prefetch file.
Name	The name of the reverse cache prefetch file.
URL	The URLs to preload.
Crawl Depth	How many levels deep to preload.
Interval	How often, in seconds, to preload the URLs.
Repeats	How many times to preload the URLs. The value range is 0-4,200,000,000.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a prefetch file

To create a prefetch file:

1. Go to *Web Cache > Prefetch File* and select *Create New* from the toolbar.
   The *Create Reverse Cache Prefetch* window opens.



2. Configure the following settings:

Name	Enter a name for the reverse cache prefetch file.
URL	Enter the URLs to preload. Separate multiple URLS with a semicolon.
Crawl Depth	Enter how many levels deep to preload the URLs.
Ignore robots.txt rules	Enable to ignore the rules found in the `robots.txt` file.
Interval	Enter how often, in seconds, to preload the URLs.
Repeats	Enter how many times to preload the URLs. The value range is 0-4,200,000,000.
User Agent	The name of the computer program to use to preload the URLs. To create a user agent, see Create or edit a user agent on page 386.

3. Click *OK* to create the new reverse cache prefetch file.

To edit a prefetch file:

1. Go to *Web Cache > Prefetch File*.
2. Select the file that you want to edit and then click *Edit* from the toolbar or double-click on the file in the table.
   The *Edit Reverse Cache Prefetch* window opens.
3. Edit the information as required, then click *OK* to apply your changes.

WCCP Settings

WCCP can be used to provide web caching with load balancing and fault tolerance. In a WCCP configuration, a WCCP server receives HTTP requests from users' web browsers and redirects the requests to one or more WCCP clients. The clients either return cached content or request new content from the destination web servers, before caching it and returning it to the server. The server then returns the content to the original requester. If a WCCP configuration includes multiple WCCP clients, the WCCP server balances traffic among the clients and can detect when a client fails and redirects traffic to still operating clients. WCCP is described by the Web Cache Communication Protocol internet draft.

You can purge specific cached content with a CLI command. See Purging specific cached content for details.

FortiProxy units operate as WCCP clients and support WCCPv2. FortiProxy units use UDP port 2048 for WCCP communication, with user traffic encapsulated in GRE-mode or L2-mode.

This section describes the following:

WCCP service groups, numbers, IDs, and well-known services

A FortiProxy unit configured as a WCCP client can include multiple client configurations. Each of these configurations is called a WCCP service group. A service group consists of one or more FortiProxy units configured as WCCP servers (or routers) and one or more FortiProxy WCCP clients working together to cache a specific type of traffic. The service group configuration includes information about the type of traffic to be cached, the addresses of the WCCP clients and servers, and other information about the service.

A service group is identified with a numeric WCCP service ID (or service number) in the range 0 to 255. All of the servers and clients in the same WCCP service group must have service group configurations with the same WCCP service ID.

The value of the service ID provides some information about the type of traffic to be cached by the service group. Service IDs in the range 0 to 50 are reserved for well-known services. A well-known service is any service that is defined by the WCCP standard as being well known. Because the service is well known, you just need to specify the service ID to identify the traffic to be cached.

Even though the well-known service ID range is 0 to 50, only one well known service has been defined. Its service ID is 0, which is used for caching HTTP (web) traffic.

To configure WCCP to cache HTTP sessions, you can add a service group to the FortiProxy WCCP router and FortiProxy WCCP clients with a service ID of 0. No other information about the type of traffic to cache needs to be added to the service group.

Because service IDs 1 to 50 are reserved for well-known services and because these services are not defined yet, you should not add service groups with IDs in the range 1 to 50.

FortiProxy allows you to add service groups with IDs between 1 and 50. However, because these service groups have not been assigned as well-known services, they will not cache any sessions. Service groups with IDs 51 to 255 allow you to set the port numbers and protocol number of the traffic to be cached. So you can use service groups with IDs 51 to 255 to cache different kinds of traffic based on port numbers and protocol number of the traffic. Service groups 1 to 50 however, do not allow you to set port or protocol numbers, so they cannot be used to cache any traffic.

To cache traffic other than HTTP traffic you must add service groups with IDs in the range 51 to 255. These service group configurations must include the port numbers and protocol number of the traffic to be cached. It is the port and protocol number configuration in the service group that determines what traffic will be cached by WCCP.

WCCP configuration overview

To configure WCCP, you must create a service group that includes FortiProxy units configured as WCCP servers and FortiProxy units configured as WCCP clients. WCCP servers intercept sessions to be cached (for example, sessions from users browsing the web from a private network). To intercept sessions to be cached, the WCCP server must include a firewall policy that accepts sessions to be cached, and WCCP must be enabled in this firewall policy.

The server must have an interface configured for WCCP communication with WCCP clients. That interface sends and receives encapsulated GRE or L2 traffic to and from WCCP clients. The server must also include a WCCP service group that includes a service ID and the addresses of the WCCP clients, as well as other WCCP configuration options.

To use a FortiProxy unit as a WCCP client, you must configure an interface on the unit for WCCP communication. The client sends and receives encapsulated GRE traffic to and from the WCCP server using this interface.

The client must also include a WCCP service group with a service ID that matches a service ID on the server. The client service group also includes the IP address of the servers in the service group and specifies the port numbers and protocol number of the sessions that will be cached on the FortiProxy unit.

When the client receives sessions from the server on its WCCP interface, it either returns cached content over the WCCP interface or connects to the destination web servers using the appropriate interface, based on the client routing configuration. Content received from web servers is then cached by the client and returned to the WCCP server over the WCCP link. The server then returns the received content to the initial requesting user’s web browser.

Finally, you might also need to configure routing on the FortiProxy server unit and FortiProxy client units, and you might need to add additional firewall policies to the server to accept sessions not cached by WCCP.

Example: Caching HTTP sessions

In this example configuration, a FortiProxy unit is operating as an Internet firewall for a private network. The port39 interface of the FortiProxy unit is connected to the Internet, and the port38 interface is connected to the internal network.

All HTTP traffic on port80 that is received at the port38 interface of the FortiProxy unit is accepted by a port39-to-port38 firewall policy with WCCP enabled. All other traffic received at the port2 interface is allowed to connect to the Internet by adding a general port38-to-port39 firewall policy below the HTTP-on-port-80 firewall policy.

A WCCP service group is added to the FortiProxy unit with a service ID of 0 for caching HTTP traffic on port80. The port1 interface of the FortiProxy unit is configured for WCCP communication.

A FortiProxy unit connects to the Internet through the FortiProxy unit. To allow for this, a port1-to-port39 firewall policy is added to the FortiProxy unit.

NOTE: The WCCP client can operate in L2 mode. The WCCP client firewall policy must specify which ingress interface is receiving the L2-forwarded traffic. This is different from GRE-mode, which uses the w.root interface.

Configure the WCCP client

You can configure the WCCP client in the GUI or CLI.

To configure the FortiProxy unit as a WCCP client using the GUI:

1. Go to *Network > Interfaces*.
2. Select an interface and then click *Edit*. If there are no interfaces in the list, select *Create New*.
3. Move the slider for *Enable WCCP Protocol* to enable WCCP on this interface and Click *OK* to save your changes.
4. Go to *Web Cache > WCCP Settings* and select *Create New*.
5. Configure the following settings:

Server ID	Enter the WCCP service group identifier. Enter *90* for the example network.
Cache ID	Enter the IP address that is known by all web cache routers. Enter *10.51.101.10* for the example network.
Router List	Enter the IP addresses of potential cache servers. Enter *10.51.101.100* for the example network.
Authentication	Enable or disable MD5 authentication. Select *Disable* for the example network.
Cache Engine Method	Select the method for forwarding traffic to the routers and for returning traffic to the cache engine, either *GRE* or *L2*. Select *GRE* or *L2* for the example network.
Assignment Method	Select the preferred assignment method for the hash key, either *HASH* or *MASK*. Select *HASH* or *MASK* for the example network.

6. Click *OK* to create the WCCP client.

To configure the FortiProxy unit as a WCCP client using the CLI:

Use the following steps to configure the FortiProxy unit as the WCCP client for the example network. The example steps only describe the WCCP-related configuration.

1. Enable the L2 mode:
```
config system wccp
   edit <Service-ID>
      set cache-engine-method L2
   next
end
```
2. Configure the FortiProxy unit to operate as a WCCP client:
```
config system settings
   set wccp-cache-engine enable
end
```

> You cannot enter the `wccp-cache-engine enable` command if you have already added a WCCP service group. When you enter this command, an interface named w.root is added to the FortiProxy configuration. All traffic redirected from a WCCP router is considered to be received at this interface of the FortiProxy unit operating as a WCCP client. A default route to this interface with lowest priority is added.

3. Enable WCCP on the aggregate interface aggr1:
```
config system interface
   edit aggr1
      set ip 192.168.1.2 255.255.255.0
      set allowaccess ping https ssh snmp http telnet
      set type aggregate
      set explicit-web-proxy enable
      set member port1 port4
      set wccp enable
end
```
4. Add a WCCP service group with service ID 0:
```
config system wccp
   edit 0
      set router-list 192.168.1.2
      set cache-id 192.168.1.1
end
```
5. Add a port-w.root-to-aggr1 firewall policy that accepts HTTP traffic on port80 and is configured for WCCP:
```
config firewall policy
   edit 1
      set srcintf w.root
      set dstintf aggr1
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service HTTP
      set webcache enable
end
```

```
config firewall central-snat-map
   edit 1
      set masquerade enable
      set srcintf w.root
      set dstintf aggr1
      set orig-addr "all"
```

```
      set dst-addr "all"
   next
end
```

NOTE: If the FortiProxy is operating in L2 mode, the firewall policy must specify the ingress interface where L2-forwarded traffic is being received:

```
config firewall policy
   edit 1
      set srcintf <port x>
      set dstintf <port y>
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service HTTP
      set webcache enable
end

config firewall central-snat-map
   edit 1
      set masquerade enable
      set srcintf <port x>
      set dstintf <port y>
      set orig-addr "all"
      set dst-addr "all"
   next
end
```

Verify the WCCP status

After setting up the FortiProxy unit as the WCCP client, you should verify to confirm that it is configured correctly.

```
diagnose test application wccp 2
   root: work mode:cache working NAT first_phy_id=8
      interface list:
         intf=aggr1, gid=8 phy_id=8
      service list:
         service: 0, cache_id=192.168.1.2, group=0.0.0.0, auth(no)
            forward=1, return=1, assign=1.
         router list:
            192.168.1.1
         port list:
            ecache_id=192.168.1.2

diagnose test application wccp 6
   service-0 in root
   erouter_list: 1 routers in total
      0. 192.168.1.1
      receive_id:23573 change_number:2
      cache servers seen by this router:
         0. 192.168.1.2 weight:0 (*Designated Web Cache)
```

WCCP packet flow

The following packet flow sequence assumes you have configured a FortiProxy unit to be a WCCP server and one or more FortiProxy units to be WCCP clients.

1. A user's web browser sends a request for web content.
2. The FortiProxy unit configured as a WCCP server includes a firewall policy that intercepts the request and forwards it to a FortiProxy WCCP client.
3. The firewall policy can apply UTM features to traffic accepted by the policy.
4. The FortiProxy WCCP client receives the WCCP session.
5. The client either returns requested content to the WCCP server if it is already cached or connects to the destination web server, receives and caches the content, and then returns it to the WCCP server.
6. The WCCP server returns the requested content to the user's web browser.
7. The WCCP router returns the request to the client web browser. The client web browser is not aware that all this is taking place and does not have to be configured to use a web proxy.

Configure forward and return methods and adding authentication

The WCCP forwarding method determines how intercepted traffic is transmitted from the WCCP router to the WCCP cache engine. FortiProxy units use GRE forwarding.

GRE forwarding encapsulates the intercepted packet in an IP GRE header with a source IP address of the WCCP router and a destination IP address of the target WCCP cache engine. The result is a tunnel that allows the WCCP router to be multiple hops away from the WCCP cache server.

By default, the WCCP communication between the router and cache servers is unencrypted. If you are concerned about attackers sniffing the information in the WCCP stream, you can use the following command to enable hash-based authentication of the WCCP traffic. You must enable authentication on the router and the cache engines, and all must have the same password.

```
config system wccp
   edit 1
      set authentication enable
      set password <password>
end
```

Purging specific cached content

You can purge specific cached content with the following CLI command:

```
execute webcache delete [pattern_type] [pattern_string]
```

For *[pattern_type]*, there are three choices:

- `simple`—a simple string following the pattern [domain_string]:[port_string]/[path_string]
- `wildcard`—a wild-card match following the pattern [domain_wildcard]:[port_wildcard]/[path_wildcard]
- `regexp`—a Perl regular expression

To delete all cached content from www.domain.com/path:

```
execute webcache delete simple www.domain.com:80/path
```

To delete all content from .com www sites

```
execute webcache delete wildcard www.*.com:*/*
```

To verify the status of a purge request

```
execute webcache delete status
```

WCCP messages

When the WCCP service is active on a web cache server, it periodically sends a WCCP HERE I AM broadcast or unicast message to the FortiProxy unit operating as a WCCP router. This message contains the following information:

- Web cache identity (the IP address of the web cache server)
- Service information (the service group to join)

If the information received in this message matches what is expected, the FortiProxy unit replies with a WCCP I SEE YOU message that contains the following details:

- Router identity (the FortiProxy unit's IP address)
- Sent to IP (the web cache IP addresses to which the packets are addressed)

When both ends receive these two messages, the connection is established, the service group is formed, and the designated web cache is elected.

Troubleshooting WCCP

Two types of debug commands are available for debugging or troubleshooting a WCCP connection between a FortiProxy unit operating as a WCCP router and its FortiProxy WCCP cache engines.

Real-time debugging

The following commands can capture live WCCP messages:

```
diagnose debug enable
diagnose debug application wccpd <debug level>
```

Application debugging

The following commands display information about WCCP operations:

```
get test wccpd <integer>
diagnose test application wccpd <integer>
```

Where `<integer>` is a value between 1 and 5:

1. Display WCCP statistics
2. Display WCCP configuration
3. Display WCCP cache servers
4. Display WCCP services
5. Display WCCP assignment

Enter the following command to view the debugging output:

```
diagnose test application wccpd 3
```

Sample output from a successful WCCP connection:

```
service-0 in root: num=1, usable=1
cache server ID:
len=44, addr=172.16.78.8, weight=4135, status=0
rcv_id=6547, usable=1, fm=1, nq=0, dev=3(k3),
to=192.168.11.55
ch_no=0, num_router=1:
192.168.11.55
```

Sample output from the same command from an unsuccessful WCCP connection (because of a service group password mismatch):

```
service-0 in root: num=0, usable=0
diag debug application wccpd -1
Sample output:
wccp_on_recv()-98: root recv: num=160, dev=3(3),
172.16.78.8->192.168.11.55
wccp2_receive_pkt()-1124: len=160, type=10, ver=0200,
length=152
wccp2_receive_pkt()-1150: found component:t=0, len=20
wccp2_receive_pkt()-1150: found component:t=1, len=24
wccp2_receive_pkt()-1150: found component:t=3, len=44
wccp2_receive_pkt()-1150: found component:t=5, len=20
wccp2_receive_pkt()-1150: found component:t=8, len=24
wccp2_check_security_info()-326: MD5 check failed
```

User Agent

You can specify which computer programs are used to preload URLs. Multiple browsers are supported, such as Chrome, Safari, Firefox, and Internet Explorer. After you define a user agent, you can select it when you create prefetch URLs or reverse cache prefetch URLs.

To see the list of user agents, go to *Web Cache* > *User Agent*.

+ Create New | Edit | Delete

Name	User Agent	Ref.
Google	Google	0
Internet Explorer	Internet Explorer	0
Safari	Safari	0

Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

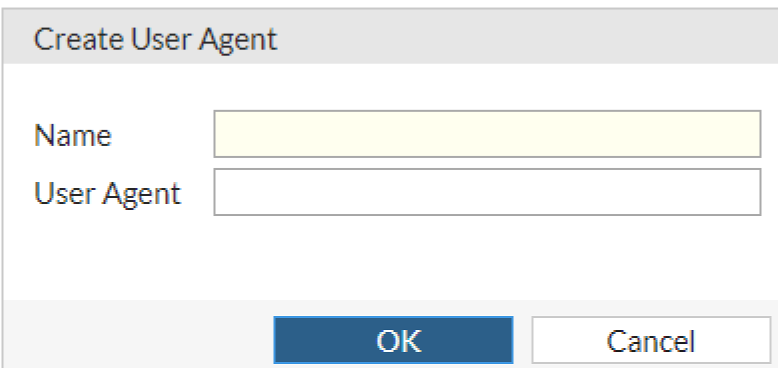
The following options are available:

Create New	Add a new user agent. See Create or edit a user agent on page 386.
Edit	Edit the selected user agent. See Create or edit a user agent on page 386.
Delete	Delete the selected user agent.
Name	The name of the user agent.
User Agent	The name of the computer program to use to preload the URLs.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a user agent

To create a user agent:

1. Go to *Web Cache > User Agent* and select *Create New* from the toolbar. The *Create User Agent* window opens.



2. Configure the following settings:

Name	Enter a name for the user agent.
User Agent	Enter the name of the browser.

3. Click *OK* to create the new user agent.

To edit a user agent:

1. Go to *Web Cache > User Agent*.
2. Select the user agent you want to edit and then click *Edit* from the toolbar or double-click on the server in the table. The *Edit User Agent* window opens.
3. Edit the information as required and then click *OK* to apply your changes.

VPN

The *VPN* menu allows you to configure IPsec VPN and SSL-VPN.

The following topics are included in this section:

IPsec VPN

Virtual Private Network (VPN) technology enables remote users to connect to private computer networks to gain access to their resources in a secure way. For example, an employee traveling or working from home can use a VPN to securely access the office network through the Internet.

Instead of remotely logging on to a private network using an unencrypted and insecure Internet connection, the use of a VPN ensures that unauthorized parties cannot access the office network and cannot intercept any of the information that is exchanged between the employee and the office. It is also common to use a VPN to connect the private networks of two or more offices.

Fortinet offers VPN capabilities in the FortiProxy Unified Threat Management (UTM) appliance and in the FortiClient Endpoint Security suite of applications. A FortiProxy unit can be installed on a private network, and FortiClient software can be installed on the user’s computer. It is also possible to use a FortiProxy unit to connect to the private network instead of using FortiClient software.

SSL-VPN

As organizations have grown and become more complex, secure remote access to network resources has become critical for day-to-day operations. In addition, businesses are expected to provide clients with efficient, convenient services including knowledge bases and customer portals. Employees traveling across the country or around the world require timely and comprehensive access to network resources. As a result of the growing need for providing remote/mobile clients with easy, cost-effective and secure access to a multitude of resources, the concept of a Virtual Private Network (VPN) was developed.

SSL VPNs establish connectivity using SSL, which functions at Levels 4-5 (Transport and Session layers). Information is encapsulated at Levels 6-7 (Presentation and Application layers), and SSL VPNs communicate at the highest levels in the OSI model. SSL is not strictly a Virtual Private Network (VPN) technology that allows clients to connect to remote networks in a secure way. A VPN is a secure logical network created from physically separate networks. VPNs use encryption and other security methods to ensure that only authorized users can access the network. VPNs also ensure that the data transmitted between computers cannot be intercepted by unauthorized users. When data is encoded and transmitted over the Internet, the data is said to be sent through a “VPN tunnel.” A VPN tunnel is a non-application oriented tunnel that allows the users and networks to exchange a wide range of traffic regardless of application or protocol.

The advantages of a VPN over an actual physical private network are two-fold. Rather than utilizing expensive leased lines or other infrastructure, you use the relatively inexpensive, high-bandwidth Internet. Perhaps more important though is the universal availability of the Internet. In most areas, access to the Internet is readily obtainable without any special arrangements or long wait times.

SSL (Secure Sockets Layer) as HTTPS is supported by most web browsers for exchanging sensitive information securely between a web server and a client. SSL establishes an encrypted link, ensuring that all data passed between the web server and the browser remains private and secure. SSL protection is initiated automatically when a user (client) connects to a web server that is SSL-enabled. Once the successful connection is established, the browser encrypts all the information before it leaves the computer. When the information reaches its destination, it is decrypted using a secret (private) key. Any data sent back is first encrypted, and is decrypted when it reaches the client.

FortiProxy supports the SSL and TLS versions defined in the following table.

SSL and TLS version support table

Version	RFC
SSL 2.0	RFC 6176
SSL 3.0	RFC 6101
TLS 1.0	RFC 2246
TLS 1.1	RFC 4346
TLS 1.2	RFC 5246

IPsec Tunnels

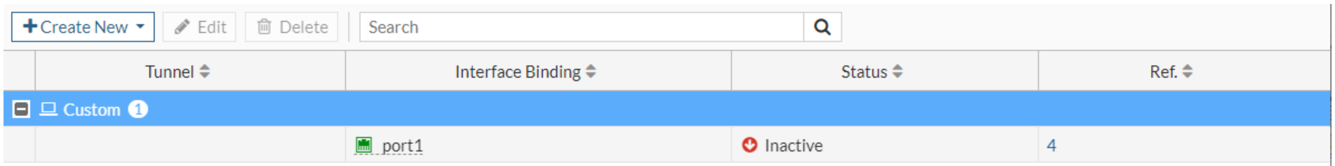
The data path between a user’s computer and a private network through a VPN is referred to as a tunnel. Like a physical tunnel, the data path is accessible only at both ends. In the telecommuting scenario, the tunnel runs between the FortiClient application on the user’s PC, or a FortiProxy unit or other network device and the FortiProxy unit on the office private network.

Encapsulation makes this possible. IPsec packets pass from one end of the tunnel to the other and contain data packets that are exchanged between the local user and the remote private network. Encryption of the data packets ensures that any third-party who intercepts the IPsec packets can not access the data.

You can create a VPN tunnel between:

- A PC equipped with the FortiClient application and a FortiProxy unit
- Two FortiProxy units
- Third-party VPN software and a FortiProxy unit

To view a list of IPsec tunnels, go to *VPN > IPsec Tunnels*. After you create an IPsec VPN tunnel, it appears in the VPN tunnel list.



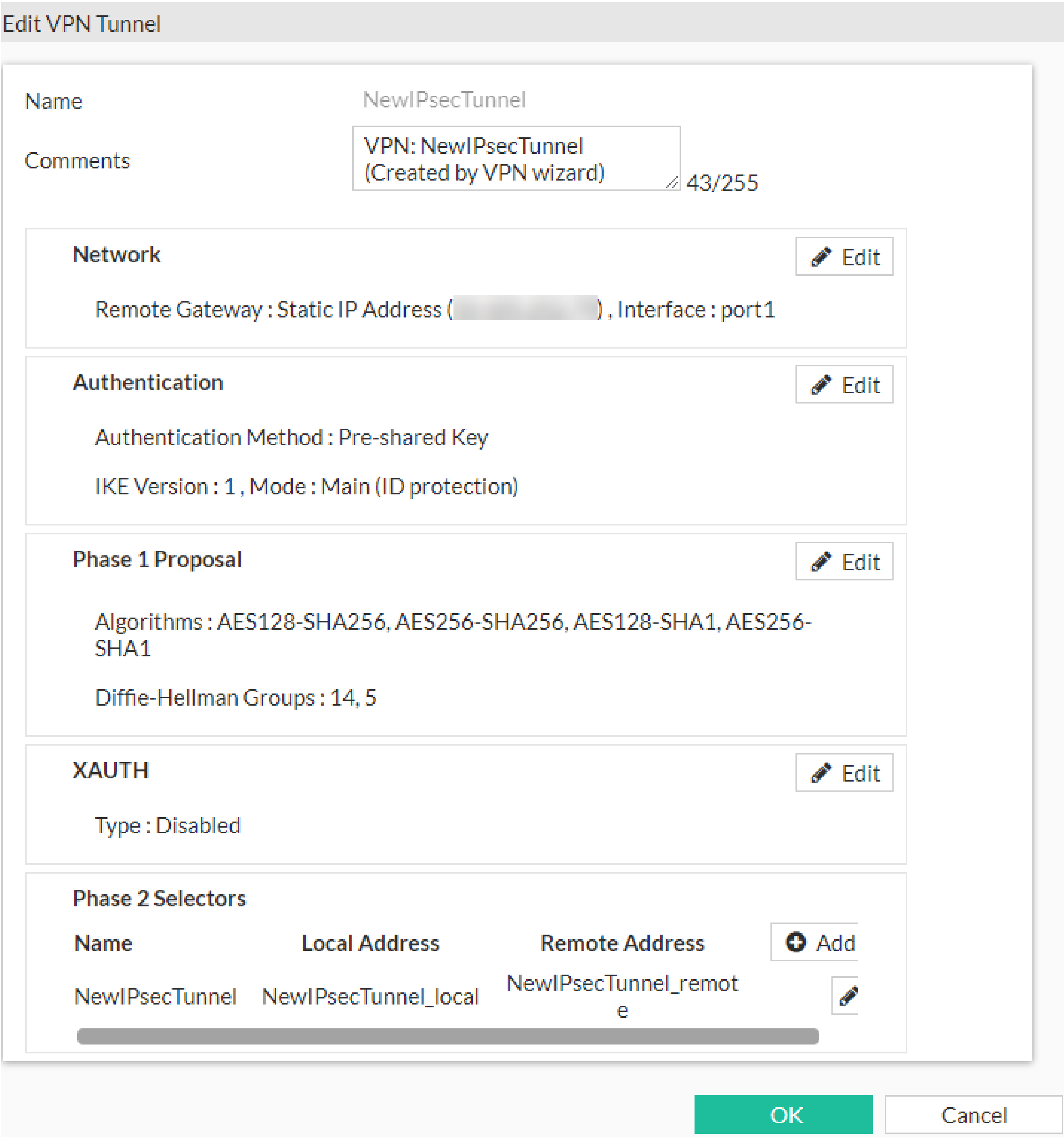
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New > IPsec Tunnel	Run the IPsec Wizard and create an IPsec tunnel. See IPsec Wizard on page 393.
Edit	Edit an IPsec tunnel. See Edit an IPsec tunnel on page 389.
Delete	Delete the selected IPsec tunnel.
Search	Enter a search term to find in the list.
Tunnel	The name of the IPsec tunnel.
Interface Binding	Select the name of the interface through which remote peers connect to the FortiProxy unit.
Status	The status is *Active* or *Inactive*.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.
Aggregate Weight	The aggregate weight.
Comments	An optional description of the IPsec tunnel.
IKE Version	The default IKE version is 1.
Mode	The mode is *Aggressive* or *Main (ID Protection)*: • *Main (ID Protection)*—The Phase 1 parameters are exchanged in multiple rounds with encrypted authentication information. • *Aggressive*—The Phase 1 parameters are exchanged in single message with authentication information that is not encrypted.
Phase 2 Selectors	The name of phase 2.

Edit an IPsec tunnel

Select an IPsec tunnel and then click *Edit* to open the Edit VPN Tunnel page.



Configure the following settings in the Edit VPN Tunnel page. After each editing a section, select the checkmark icon to save your changes. After you make all of your changes, click *OK*.

Name	The name of the IPsec tunnel cannot be changed.
Comments	An optional description of the IPsec tunnel.

Network	Select *Edit* to make changes.
IP Version	This option is set to *IPv4*.
Remote Gateway	This option is set to *Static IP Address* for a remote peer that has a static IP address.
IP Address	Enter the IP address of the remote peer.
Interface	Select the name of the interface through which remote peers connect to the FortiProxy unit.
Local Gateway	Enable this option to configure a local gateway and then select *Primary IP*, *Secondary IP*, or *Specify*. Enter or select the IP address.
NAT Traversal	Select *Enable* if a NAT device exists between the local FortiProxy unit. and the VPN peer or client. The local FortiProxy unit and the VPN peer or client must have the same NAT traversal setting (both selected or both cleared) to connect reliably. Additionally, you can force IPsec to use NAT traversal. If this option is set to *Forced*, the FortiProxy unit uses a port value of zero when constructing the NAT discovery hash for the peer. This causes the peer to think it is behind a NAT device, and it will use UDP encapsulation for IPsec, even if no NAT is present. This approach maintains interoperability with any IPsec implementation that supports the NAT-T RFC.
Keepalive Frequency	If you selected *Enable* or *Forced* for the NAT traversal, enter a keep-alive frequency.
Forward Error Correction	Select *Egress* or *Ingress*.
Add route	Select *Enabled* if you want to add a route.
Auto discovery sender	Select *Enabled* to automatically discover the sender.
Auto discover receiver	Select *Enabled* to automatically discover the receiver.
Authentication	Select *Edit* to make changes.
Method	Select *Pre-shared Key* or *Signature*: • *Pre-shared Key*—A preshared key contains at least six random alphanumeric characters. Users of the VPN must obtain the preshared key from the person who manages the VPN server and add the preshared key to their VPN client configuration. • *Signature*—Use one or more certificates for authentication.
Pre-shared Key	If you selected *Pre-shared Key* for the authentication method, enter the pre-shared key that the FortiProxy unit will use to authenticate itself to the remote peer or dial-up client during Phase 1 negotiations. You must define the same key at the remote peer or client. The key must contain at least 6 printable characters. For optimum protection against currently known attacks, the key must consist of a minimum of 16 randomly chosen alphanumeric characters. The limit is 128 characters.

Certificate Name	If you selected *Signature* for the authentication method, select + and then select one or more certificates that the FortiProxy unit will use to authenticate itself.
Version	IKE version 1 is selected by default.
Mode	Select *Aggressive* or *Main (ID protection)*: • *Main (ID protection)*—The Phase 1 parameters are exchanged in multiple rounds with encrypted authentication information. • *Aggressive*—The Phase 1 parameters are exchanged in single message with authentication information that is not encrypted.
Phase 1 Proposal	Select *Edit* to make changes. Select *Add* to get another row of Encryption and Authentication options.
Encryption	Select *DES*, *3DES*, *AES128*, *AES192*, *AES256* to use as the encryption algorithm.
Authentication	Select *MD5*, *SHA1*, *SHA256*, *SHA384*, or *SHA512* to use for authentication.
Diffie-Hellman Groups	Select one or more Diffie-Hellman (DH) asymmetric key algorithms for public key cryptography.
Key Lifetime (seconds)	Enter the time (in seconds) that must pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The key lifetime can be from 120 to 172,800 seconds.
Local ID	A Local ID is an alphanumeric value.
XAUTH	Select *Edit* to make changes.
Type	Select *Client* to require an additional user name and password for authentication.
Username	If you selected *Client*, enter a user name for authentication.
Password	If you selected *Client*, enter a password for authentication.
Phase 2 Selectors	Select *Add* to enter new phase-2 information.
Name	Enter the Phase-2 name.
Comments	An optional description of the VPN tunnel.
Local Address	Select *Subnet*, *IP Range*, *IP Address*, *Named Address,IPv6 Subnet*, *IPv6 Range*, *IPv6 Address*, or *Named IPv6 Address* and then enter the specified information.
Remote Address	Select *Subnet*, *IP Range*, *IP Address*, *Named Address,IPv6 Subnet*, *IPv6 Range*, *IPv6 Address*, or *Named IPv6 Address* and then enter the specified information.
Phase 2 Proposal	Select *Add* to get another row of Encryption and Authentication options.
Encryption	Select *DES*, *3DES*, *AES128*, *AES128GCM*, *AES192*, *AES256* or *CHACHA20POLY1305* to use as the encryption algorithm.
Authentication	Select *MD5*, *SHA1*, *SHA256*, *SHA384*, or *SHA512* to use for authentication.
Enable Replay Detection	Replay attacks occur when an unauthorized party intercepts a series of IPsec packets and replays them back into the tunnel.

Enable Perfect Forward Secrecy (PFS)	Enable for PFS.
Local Port	Select *All* or enter the local port number.
Remote Port	Select *All* or enter the remote port number.
Protocol	Select *All* or enter the protocol number.
Auto-negotiate	Enable the option if you want the tunnel to be automatically renegotiated when the tunnel expires.
Autokey Keep Alive	Select the check box if you want the tunnel to remain active when no data is being processed.
Key Lifetime	Select the method for determining when the Phase 2 key expires: *Seconds*, *Kilobytes*, or *Both*. If you select *Both*, the key expires when either the time has passed or the number of kilobytes have been processed.
Seconds	If you selected *Seconds* or *Both* for the key lifetime, enter the number of seconds.
Kilobytes	If you selected *Kilobytes* or *Both* for the key lifetime, enter the number of kilobytes.

IPsec Wizard

To set up an IPsec VPN:

1. Go to *VPN > IPsec Wizard*.
2. Configure the VPN setup and then select *Next*:

Name	Enter a unique descriptive name (15 characters or less) for the VPN tunnel.
Template Type	Select *Site to Site* or *Custom*: • *Site to Site*—Static tunnel between this FortiProxy unit and a remote FortiProxy unit through the Internet. • *Custom*—No template. See Create a custom VPN tunnel on page 395.
NAT Configuration	If you selected *Site to Site*, select *No NAT between sites*, *This site is behind NAT*, or *The remote site is behind NAT*.
Remote Device type	If you selected *Site to Site*, select *FortiProxy* or *Cisco*.

3. Configure the authentication and then select *Next*:

Remote Device	If you selected *Site to Site* for the template type, select *IP Address* or *Dynamic DNS*.
Remote IP Address	If you selected *IP Address* for the remote address, enter the IP address of the remote peer.
FQDN	If you selected *Dynamic DNS* for the remote address, enter the domain name of the remote peer.

Outgoing Interface	If you selected *Site to Site* for the template type, select the outgoing interface from the drop-down list.
Incoming Interface	If you selected *Remote Access* for the template type, select the incoming interface from the drop-down list.
Authentication Method	Select *Pre-shared Key* or *Signature*: • *Pre-shared Key*—A preshared key contains at least six random alphanumeric characters. Users of the VPN must obtain the preshared key from the person who manages the VPN server and add the preshared key to their VPN client configuration. • *Signature*—Use one or more certificates for authentication.
Pre-shared Key	If you selected *Pre-shared Key* for the authentication method, enter the pre-shared key that the FortiProxy unit will use to authenticate itself to the remote peer or dial-up client during Phase 1 negotiations. You must define the same key at the remote peer or client. The key must contain at least 6 printable characters. For optimum protection against currently known attacks, the key must consist of a minimum of 16 randomly chosen alphanumeric characters. The limit is 128 characters.
Certificate Name	If you selected *Signature* for the authentication method, select + and then select one or more certificates that the FortiProxy unit will use to authenticate itself.
Peer Certificate CA	If you selected *Signature* for the authentication method, select a peer certificate authority.

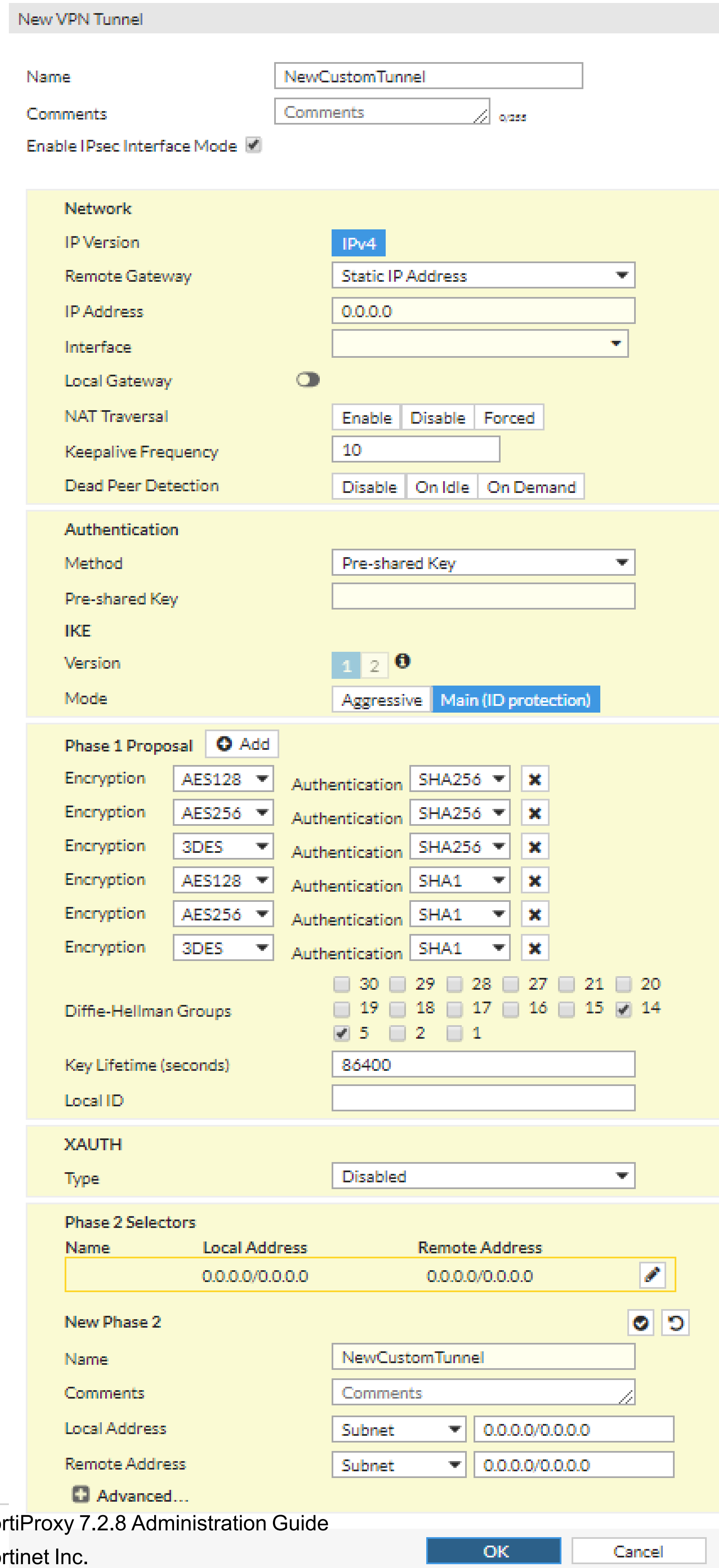
4. Configure the policy and routing settings:

Local Interface	Select the name of the interface through which remote peers or dial-up clients connect to the FortiProxy unit.
Local Subnets	If you selected *Site to Site* for the template type, enter a local subnet. Select + to enter another local subnet.
Remote Subnets	Enter a remote subnet. Select + to enter another remote subnet.
Internet Access	Select *None*, *Share Local*, or *Use Remote*. • *None*—Site-to-site devices communicate over the VPN, but Internet access does not require VPN. • *Share Local*—Allow the remote site to use this FortiProxy as an Internet gateway. • *Use Remote*—This FortiProxy unit will use a tunnel for Internet access from the remote location.
Shared WAN	If you selected *Share Local* for Internet access, select the WAN interface.
Local Gateway	If you selected *Use Remote* for Internet access, enter the local gateway address.

5. Select *Create*.
6. Select *Add Another* to start at the beginning of the IPsec Wizard or select *Show Tunnel List* to see the available IPsec tunnels.

Create a custom VPN tunnel

If you select *Custom* for the template type in the IPsec Wizard and then select *Next*, the New VPN Tunnel window opens.


New VPN Tunnel
Name
NewCustomTunnel
Comments
Comments
0/255
Enable IPsec Interface Mode
Network
IP Version
IPv4
Remote Gateway
Static IP Address
IP Address
0.0.0.0
Interface
Local Gateway
NAT Traversal
Enable
Disable
Forced
Keepalive Frequency
10
Dead Peer Detection
Disable
On Idle
On Demand
Authentication
Method
Pre-shared Key
Pre-shared Key
IKE
Version
1
2
Mode
Aggressive
Main (ID protection)
Phase 1 Proposal
Add
Encryption AES128 Authentication SHA256
Encryption AES256 Authentication SHA256
Encryption 3DES Authentication SHA256
Encryption AES128 Authentication SHA1
Encryption AES256 Authentication SHA1
Encryption 3DES Authentication SHA1
Diffie-Hellman Groups
30 29 28 27 21 20
19 18 17 16 15 14
5 2 1
Key Lifetime (seconds)
86400
Local ID
XAUTH
Type
Disabled
Phase 2 Selectors
Name
Local Address
Remote Address
0.0.0.0/0.0.0.0
0.0.0.0/0.0.0.0
New Phase 2
Name
NewCustomTunnel
Comments
Comments
Local Address
Subnet
0.0.0.0/0.0.0.0
Remote Address
Subnet
0.0.0.0/0.0.0.0
Advanced...
OK
Cancel

Configure the following settings and then click *OK*:

Name	Type a name for the Phase 1 definition.
Comments	An optional description of the VPN tunnel.
Enable IPsec Interface Mode	Select this option if you want to create an IPsec VPN tunnel.
IP Version	This option is set to *IPv4*.
Remote Gateway	This option is set to *Static IP Address* for a remote peer that has a static IP address.
IP Address	Enter the IP address of the remote peer.
Interface	Select the name of the interface through which remote peers connect to the FortiProxy unit.
Local Gateway	Enable this option to configure a local gateway and then select *Primary IP*, *Secondary IP*, or *Specify*. Enter or select the IP address.
NAT Traversal	Select *Enable* if a NAT device exists between the local FortiProxy unit. and the VPN peer or client. The local FortiProxy unit and the VPN peer or client must have the same NAT traversal setting (both selected or both cleared) to connect reliably. Additionally, you can force IPsec to use NAT traversal. If this option is set to *Forced*, the FortiProxy unit uses a port value of zero when constructing the NAT discovery hash for the peer. This causes the peer to think it is behind a NAT device, and it will use UDP encapsulation for IPsec, even if no NAT is present. This approach maintains interoperability with any IPsec implementation that supports the NAT-T RFC.
Keepalive Frequency	If you selected *Enable* or *Force*d for the NAT traversal, enter a keep-alive frequency.
Dead Peer Detection	Select *On Idle* to reestablish VPN tunnels on idle connections and clean up dead IKE peers if required. You can use this option to receive notification whenever a tunnel goes up or down, or to keep the tunnel connection open when no traffic is being generated inside the tunnel. With *On Idle* or *On Demand* selected, you can use the `config vpn ipsec phase1` (tunnel mode) or `config vpn ipsec phase1-interface` (interface mode) CLI command to optionally specify a retry count and a retry interval.
Method	Select *Pre-shared Key* or *Signature*: • *Pre-shared Key*—A preshared key contains at least six random alphanumeric characters. Users of the VPN must obtain the preshared key from the person who manages the VPN server and add the preshared key to their VPN client configuration. • *Signature*—Use one or more certificates for authentication.
Pre-shared Key	If you selected *Pre-shared Key* for the authentication method, enter the pre-shared key that the FortiProxy unit will use to authenticate itself to the remote peer or dial-up client during Phase 1 negotiations. You must define the same key at the remote peer or client.

	The key must contain at least 6 printable characters. For optimum protection against currently known attacks, the key must consist of a minimum of 16 randomly chosen alphanumeric characters. The limit is 128 characters.
Certificate Name	If you selected *Signature* for the authentication method, select + and then select one or more certificates that the FortiProxy unit will use to authenticate itself.
Version	IKE version 1 is selected by default.
Mode	Select *Aggressive* or *Main (ID protection)*: • *Main (ID protection)*—The Phase 1 parameters are exchanged in multiple rounds with encrypted authentication information. • *Aggressive*—The Phase 1 parameters are exchanged in single message with authentication information that is not encrypted.
Accept Types	If you selected *Pre-shared Key* for the authentication method and selected aggressive mode, select *Any peer ID* or *Specific peer ID*. If you select *Specific peer ID*, enter the peer ID. If you selected *Signature* for the authentication method, select *Any peer ID*, *Specific peer ID*, or *Peer certificate*.
Peer ID	If you selected *Any peer ID*, enter the peer ID.
Peer certificate	If you selected *Peer certificate* for the authentication method, select the certificate.
Phase 1 Proposal	Select *Add* to get another row of Encryption and Authentication options.
Encryption	Select *DES*, *3DES*, *AES128*, *AES192*, and *AES256* to use as the encryption algorithm. *AES256* is the most secure; *DES* is the least secure.
Authentication	Select *MD5*, *SHA1*, *SHA256*, *SHA384*, *SHA512*, or *SHA256* to use for authentication.
Diffie-Hellman Groups	Select one or more Diffie-Hellman (DH) asymmetric key algorithms for public key cryptography.
Key Lifetime (seconds)	Enter the time (in seconds) that must pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The key lifetime can be from 120 to 172,800 seconds.
Local ID	A Local ID is an alphanumeric value.
Type	Select *Client* to require an additional user name and password for authentication.
User Name	If you selected *Client*, enter a user name for authentication.
Password	If you selected *Client*, enter a password for authentication.
Name	By default, the Phase-2 name is the same as the Phase-1 name.
Comments	An optional description of the VPN tunnel.
Local Address	Select *Subnet*, *IP Range*, *IP Address*, *Named Address,IPv6 Subnet*, *IPv6 Range*, *IPv6 Address*, or *Named IPv6 Address* and then enter the specified information.

Remote Address	Select *Subnet*, *IP Range*, *IP Address*, *Named Address,IPv6 Subnet*, *IPv6 Range*, *IPv6 Address*, or *Named IPv6 Address* and then enter the specified information.
Phase 2 Proposal	Select *Add* to get another row of Encryption and Authentication options.
Encryption	Select *NULL*, *DES*, *3DES*, *AES128*, *AES128GCM*, *AES192*, *AES256*, or *AES256GCM* to use as the encryption algorithm. *NULL* is the least secure; *AES256GCM* is the most secure.
Authentication	Select *NULL*, *MD5*, *SHA1*, *SHA256*, *SHA384*, or *SHA512* to use for authentication.
Enable Replay Detection	Replay attacks occur when an unauthorized party intercepts a series of IPsec packets and replays them back into the tunnel.
Enable Perfect Forward Secrecy (PFS)	Perfect forward secrecy (PFS) improves security by forcing a new Diffie-Hellman exchange whenever keylife expires.
Local Port	Select *All* or enter the local port number.
Remote Port	Select *All* or enter the remote port number.
Protocol	Select *All* or enter the protocol number.
Auto-negotiate	Enable the option if you want the tunnel to be automatically renegotiated when the tunnel expires.
Autokey Keep Alive	Select the check box if you want the tunnel to remain active when no data is being processed.
Key Lifetime	Select the method for determining when the Phase 2 key expires: *Seconds*, *Kilobytes*, or *Both*. If you select *Both*, the key expires when either the time has passed or the number of kilobytes have been processed.
Seconds	If you selected *Seconds* or *Both* for the key lifetime, enter the number of seconds.
Kilobytes	If you selected *Kilobytes* or *Both* for the key lifetime, enter the number of kilobytes.

IPsec Tunnel Template

Several tunnel templates are available in the IPsec VPN Wizard that cover a variety of different types of IPsec VPN. Go to *VPN > IPsec Tunnel Template* to see a list and descriptions of these templates:

- Site to Site - FortiProxy
- Site to Site - Cisco

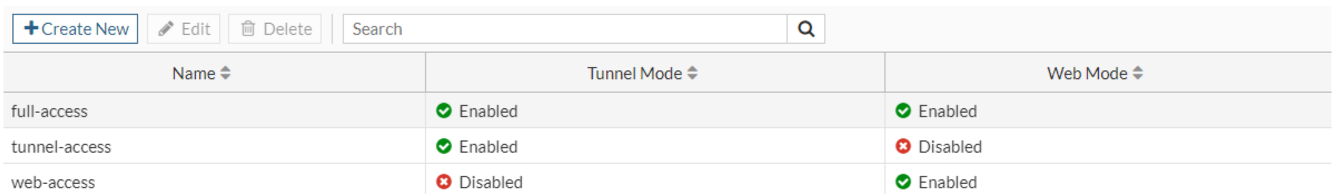
Select a template and then select *View* to see the template details.

SSL-VPN Portals

The SSL-VPN portal enables remote users to access internal network resources through a secure channel using a web browser. FortiProxy administrators can configure login privileges for system users as well as the network resources that are available to the users.

This step in the configuration of the SSL-VPN tunnel sets up the infrastructure; the addressing, encryption, and certificates needed to make the initial connection to the FortiProxy unit. This step is also where you configure what the remote user sees with a successful connection. The portal view defines the resources available to the remote users and the functionality they have on the network.

Go to *VPN > SSL-VPN Portals* to see a list of available SSL-VPN portals.



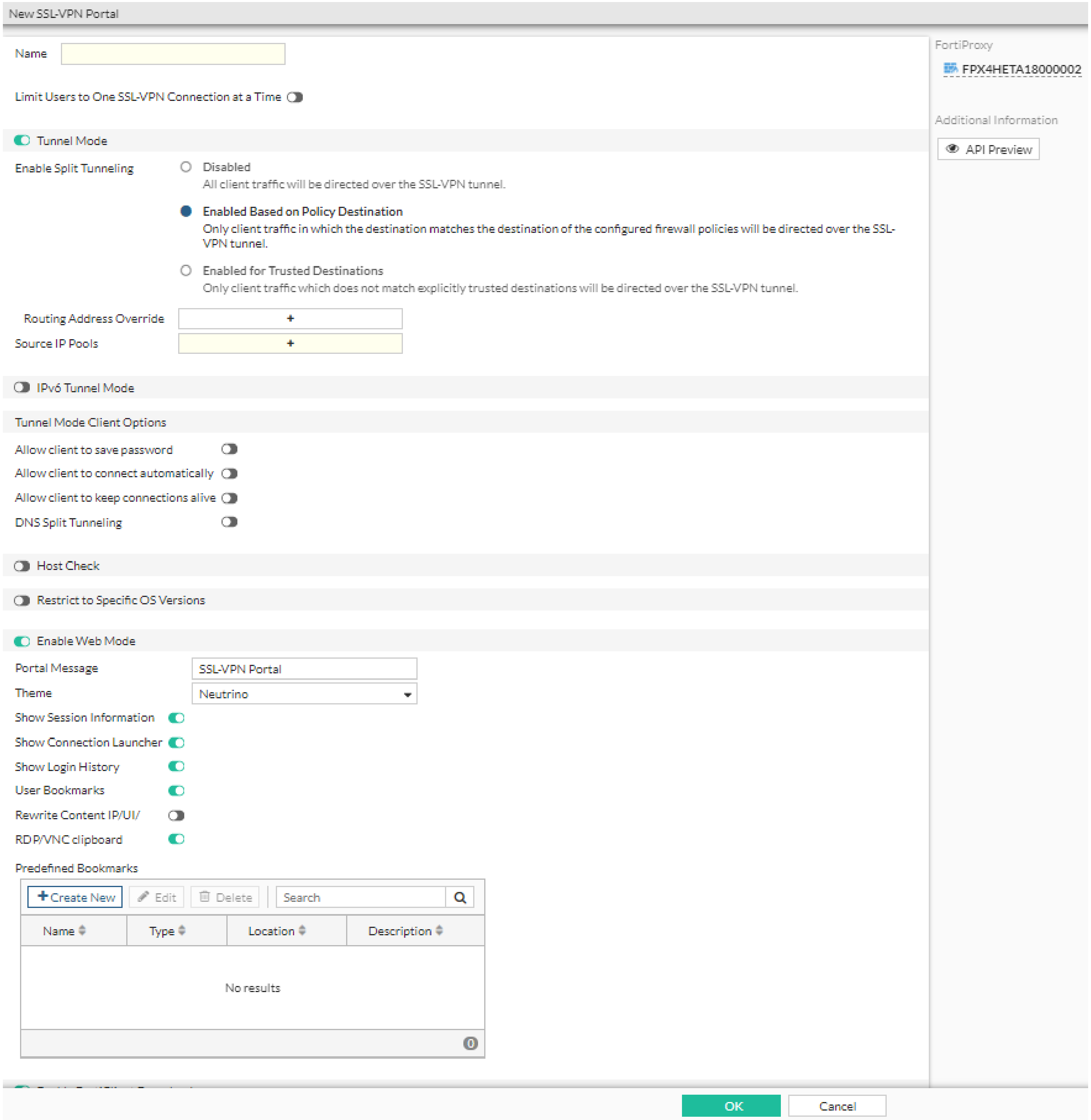
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create an SSL-VPN portal. See Create or edit an SSL-VPN portal on page 400.
Edit	Edit an SSL-VPN portal. See Create or edit an SSL-VPN portal on page 400.
Delete	Delete an SSL-VPN portal.
Search	Enter a search term to find in the list.
Name	The name for the portal.
Tunnel Mode	Whether this portal is using tunnel mode.
Web Mode	Whether this portal is using web-only mode.
IPv6 Tunnel Mode	Whether this portal is using IPv6 tunnel mode.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit an SSL-VPN portal

Select *Create New* to open the *New SSL-VPN Portal* page.



Select an SSL-VPN portal from the list and then click *Edit* to open the *Edit SSL-VPN Portal* page.

Configure the following settings in the *New SSL-VPN Portal* page or *Edit SSL-VPN Portal* page and then click *OK*:

Name	The name for the portal. After you create the SSL-VPN portal, the name cannot be changed.

Limit Users to One SSL-VPN Connection at a Time	You can set the SSL VPN tunnel such that each user can only log into the tunnel one time concurrently per user per login. That is, after logging into the portal, they cannot go to another system and log in with the same credentials again. This option is disabled by default.
Tunnel Mode	Enable to determine how tunnel-mode clients are assigned IPv4 addresses.
Enable Split Tunneling	If you want to use split tunneling, select *Enabled Based on Policy Destination* or *Enabled for Trusted Destinations*.
Routing Address Override	If you enable split tunneling, you are required to set the routing address, which is the address that your corporate network is using. Traffic intended for the routing address is not split from the tunnel.
Source IP Pools	Select an IP pool for users to acquire an IP address when connecting to the portal. There is always a default pool available if you do not create your own.
IPv6 Tunnel Mode	Move the slider to determine how tunnel-mode clients are assigned IPv6 addresses.
Enable IPv6 Split Tunneling	Select *Disabled*, *Enabled Based on Policy Destination*, or *Enabled for Trusted Destinations*.
IPv6 Routing Address Override	If you enable split tunneling, you are required to set the IPv6 routing address, which is the address that your corporate network is using. Traffic intended for the routing address is not split from the tunnel.
Source IPv6 Pools	Select an IPv6 pool for users to acquire an IP address when connecting to the portal. There is always a default pool available if you do not create your own.
Allow client to save password	When enabled, if the user selects this option, their password is stored on the user's computer and will automatically populate each time they connect to the VPN.
Allow client to connect automatically	When enabled, if the user selects this option, when the FortiClient application is launched, for example after a reboot or system startup, FortiClient will automatically attempt to connect to the VPN tunnel.
Allow client to keep connections alive	When enabled, if the user selects this option, the FortiClient should try to reconnect once it detects the VPN connection is down unexpectedly (not manually disconnected by user).
DNS Split Tunneling	Enable and then create or edit the DNS entry. See Create or edit a DNS entry on page 404.
Host Check	Enable and then select *Realtime AntiVirus*, *Firewall*, or *Enable both*.
Restrict to Specific OS Versions	Enable or disable.
Enable Web Mode	Enable for web-mode access.
Portal Message	This is a text header that appears on the top of the web portal.
Theme	Select a color styling specifically for the web portal.

Show Session Information	The *Show Session Information* widget displays the login name of the user, the amount of time the user has been logged in and the inbound and outbound traffic statistics.
Show Connection Launcher	Displays the *Connection Launcher* widget in the web portal.
Show Login History	Select to include user login history on the web portal.
User Bookmarks	Enable to allow users to add their own bookmarks in the web portal.
Rewrite Content IP/UI/	Enable or disable whether the content can be rewritten.
FDP/VNC clipboard	Enable or disable the FDP/VNC clipboard.
Create New	Create a bookmark. See Create or edit a bookmark on page 404.
Edit	Edit a selected bookmark. See Create or edit a bookmark on page 404.
Delete	Delete a selected bookmark.
Search	Enter a search term to find in the list.
Enable FortiClient Download	Enable to allow users to customize the download URL for FortiClient.
Download Method	If you enable FortiClient download, select whether FortiClient will directly download or use SSL-VPN proxy.
Customize Download Location	Enable to change the download location.
Windows	Enable to specify the Windows download location.
Mac	Enable to specify the Mac download location.

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*.

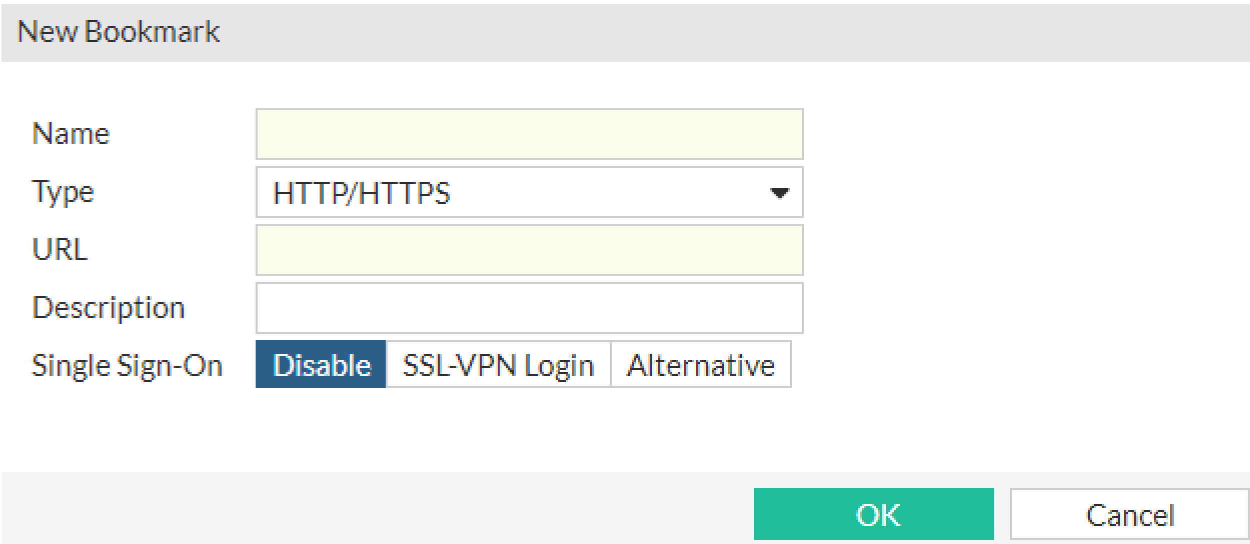
To disable the RDP/VNC clipboard in the CLI:

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

Create or edit a bookmark

A web bookmark can include login credentials to automatically log the SSL-VPN user into the website. When the administrator configures bookmarks, the website credentials must be the same as the user's SSL-VPN credentials. Users configuring their own bookmarks can specify alternative credentials for the website.

Select *Create New* to open the *New Bookmark* page.



Select a bookmark from the list and then click *Edit* to open the *Edit Bookmark* page.

Configure the following settings in the *New Bookmark* page or *Edit Bookmark* page and then click *OK*:

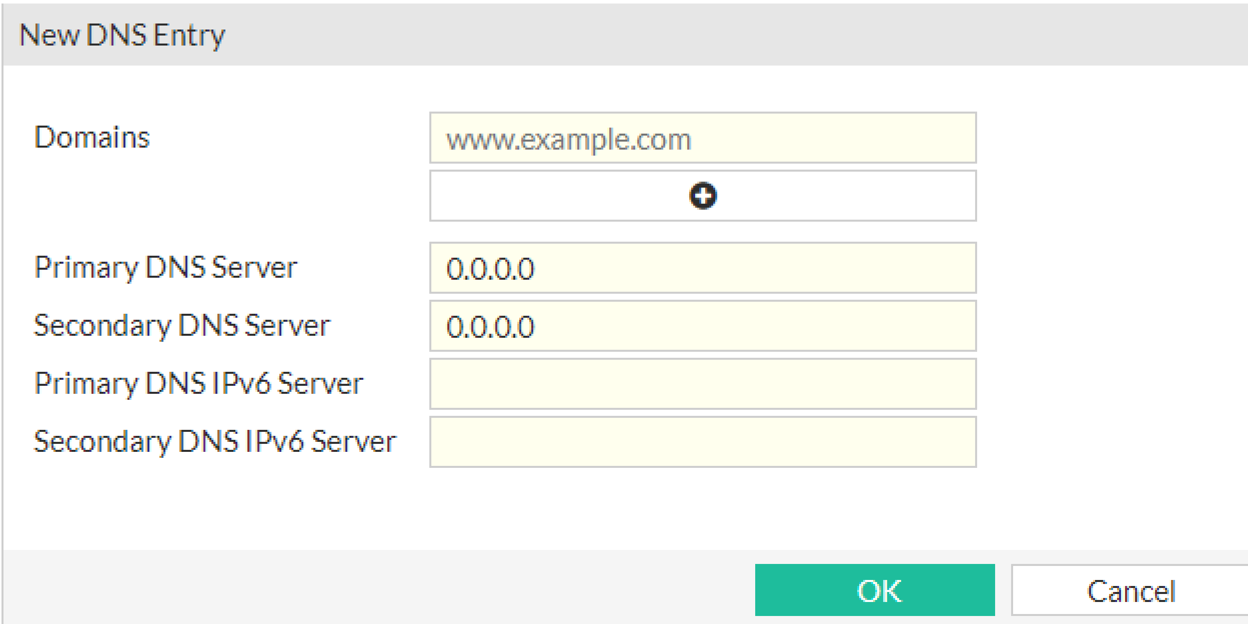
Name	Enter a name for the bookmark.
Type	Select the type of link from the drop-down list: *HTTP/HTTPS*, *FTP*, *RDP*, *SFTP*, *SMB/CIFS*, *SSH*, *TELNET*, or *VNC*.
URL	Enter the URL for the bookmark.
Description	Enter a brief description of the link.
Single Sign-On	If you want to use single sign-on, select *SSL-VPN Login* or *Alternative*.
SSO Form Data	If you selected *SSL-VPN Login* for SSO, select whether you want to use SSO form data.
Form Key	If you enabled *SSO Form Data*, enter the SSO form key.
Form Value	If you enabled *SSO Form Data*, enter one or more form values.
Username	If you selected *Alternative* for SSO, enter a user name for signing in.
Password	If you selected *Alternative* for SSO, enter a password for signing in.

Create or edit a DNS entry

You can create or edit a DNS entry for the SSL-VPN portal.

To create a DNS entry:

1. Go to *VPN* > *SSL-VPN Portals* and, under *Tunnel Mode Client Options*, enable *DNS Split Tunneling*.
2. In the *Split DNS* table, select *Create New*. The *New DNS Entry* window opens.



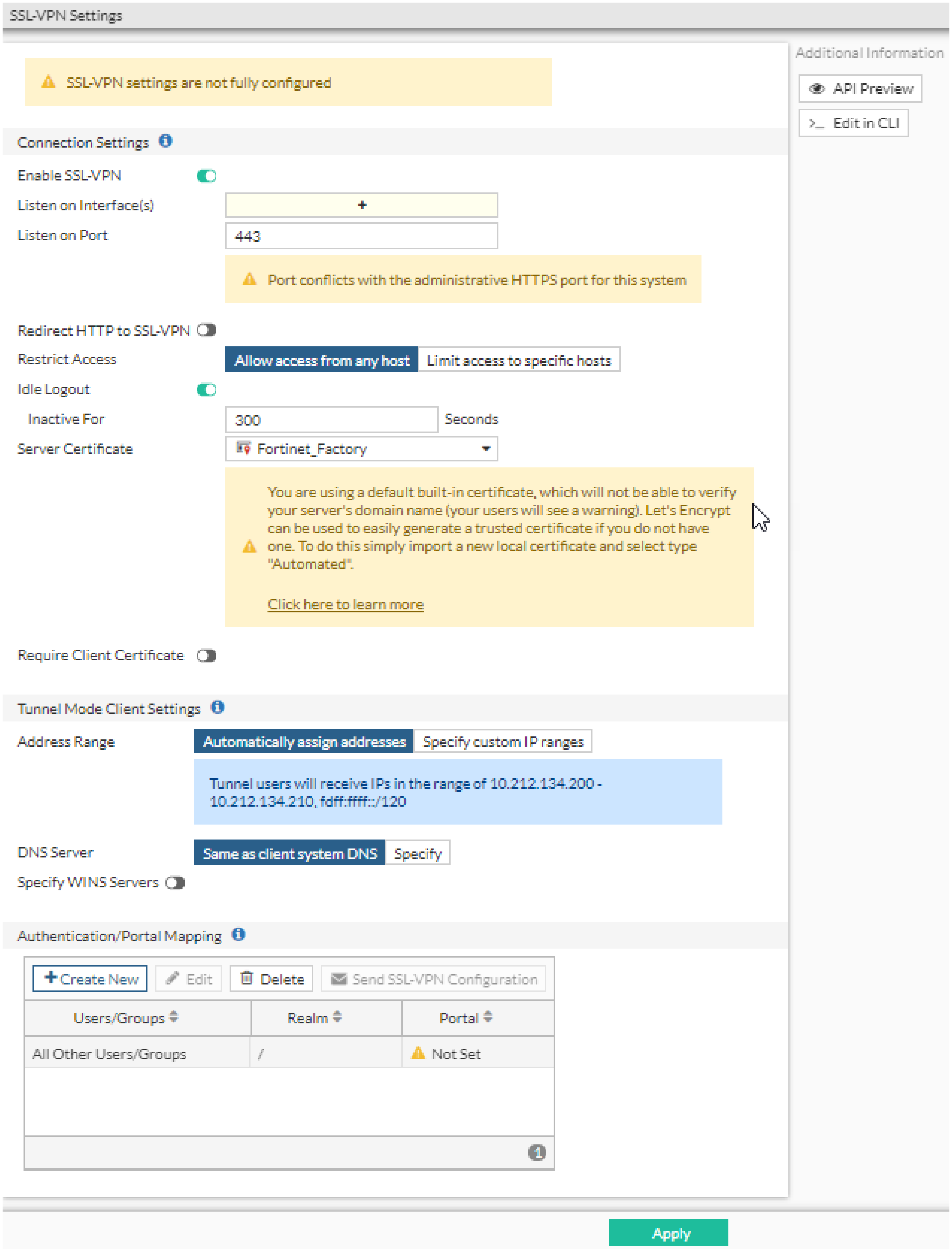
3. Enter one or more domains for the DNS entry.
4. Enter the IPv4 address of the primary DNS server.
5. Enter the IPv4 address of the secondary DNS server.
6. Enter the IPv6 address of the primary DNS server.
7. Enter the IPv6 address of the secondary DNS server.
8. Click *OK* to save your DNS entry. The new DNS entry is added to the table.
9. Click *OK* to save your changes to the SSL-VPN portal.

To edit a DNS entry:

1. Go to *VPN* > *SSL-VPN Portals* and, under *Tunnel Mode Client Options*, enable *DNS Split Tunneling*.
2. Select a DNS entry and then click *Edit*.
3. In the *Edit DNS Entry* page, make your changes.
4. Click *OK* to save your changes to the DNS entry.
5. Click *OK* to save your changes to the SSL-VPN portal.

SSL-VPN Settings

To configure the basic SSL-VPN settings for encryption and login options, go to *VPN* > *SSL-VPN Settings*.


SSL-VPN Settings
Additional Information
API Preview
Edit in CLI
SSL-VPN settings are not fully configured
Connection Settings
Enable SSL-VPN
Listen on Interface(s)
Listen on Port
443
Port conflicts with the administrative HTTPS port for this system
Redirect HTTP to SSL-VPN
Restrict Access
Allow access from any host
Limit access to specific hosts
Idle Logout
Inactive For
300
Seconds
Server Certificate
Fortinet_Factory
You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). Let's Encrypt can be used to easily generate a trusted certificate if you do not have one. To do this simply import a new local certificate and select type "Automated".
Click here to learn more
Require Client Certificate
Tunnel Mode Client Settings
Address Range
Automatically assign addresses
Specify custom IP ranges
Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210, fdff:ffff::/120
DNS Server
Same as client system DNS
Specify
Specify WINS Servers
Authentication/Portal Mapping
Create New
Edit
Delete
Send SSL-VPN Configuration
Users/Groups
Realm
Portal
All Other Users/Groups
/
Not Set
1
Apply

Configure the following settings and then select *Apply*:

Enable SSL-VPN	Enable to use SSL-VPN.
Listen on Interface(s)	Select + to choose one or more interfaces that the FortiProxy unit will use to listen for SSL-VPN tunnel requests. This is generally your external interface.
Listen on Port	Enter the port number for HTTPS access.
Redirect HTTP to SSL-VPN	Move the slider to redirect the admin HTTP port to the admin HTTPS port.
Restrict Access	Restrict accessibility to either *Allow access from any host* or to *Limit access to specific hosts*.
Hosts	If you selected *Limit access to specific hosts*, enter the hosts.
Idle Logout	Enable if you want the user to log in again after the connection is inactive for the specified number of seconds.
Inactive For	Type the period of time (in seconds) that the connection can remain inactive before the user must log in again. The range is from 10 to 28800 seconds. Setting the value to 0 will disable the idle connection timeout. This setting applies to the SSL-VPN session. The interface does not time out when web application sessions or tunnels are up.
Server Certificate	Select the signed server certificate to use for authentication. If you leave the default setting (*Fortinet_Factory*), the FortiProxy unit offers its built-in certificate from Fortinet to remote clients when they connect. A warning appears that recommends you generate a trusted certificate and import it for use.
Require Client Certificate	Select to use group certificates for authenticating remote clients. When the remote client initiates a connection, the FortiProxy unit prompts the client
Address Range	Select *Automatically assign addresses* or *Specify custom IP ranges*.
IP Ranges	If you selected *Specify custom IP ranges*, select the range or subnet firewall addresses that represent IP address ranges reserved for tunnel-mode SSL VPN clients.
DNS Server	Select *Same as client system DNS* or *Specify*.
DNS Server #1	If you select *Specify*, you can enter up to two DNS servers (IPv4 or IPv6) to be provided for the use of clients.
DNS Server #2	If you select *Specify*, you can enter up to two DNS servers (IPv4 or IPv6) to be provided for the use of clients.
IPv6 DNS Server #1	If you select *Specify*, you can enter up to two DNS servers (IPv4 or IPv6) to be provided for the use of clients.
IPv6 DNS Server #2	If you select *Specify*, you can enter up to two DNS servers (IPv4 or IPv6) to be provided for the use of clients.
Specify WINS Servers	Move the slider to access options for entering up to two WINS servers (IPv4 or IPv6) to be provided for the use of clients.

WINS Server #1	If you enabled *Specify WINS Server*, you can enter up to two WINS servers (IPv4 or IPv6) to be provided for the use of clients.
WINS Server #2	If you enabled *Specify WINS Server*, you can enter up to two WINS servers (IPv4 or IPv6) to be provided for the use of clients.
IPv6 WINS Server #1	If you enabled *Specify WINS Server*, you can enter up to two WINS servers (IPv4 or IPv6) to be provided for the use of clients.
IPv6 WINS Server #2	If you enabled *Specify WINS Server*, you can enter up to two WINS servers (IPv4 or IPv6) to be provided for the use of clients.
Create New	Creates an authentication/portal mapping. See Create or edit an authentication/portal mapping on page 409.
Edit	Modifies the selected authentication/portal mapping. See Create or edit an authentication/portal mapping on page 409.
Delete	Removes the selected authentication/portal mapping.
Send SSL-VPN Configuration	Click to email the SSL-VPN configuration.
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.
Edit in CLI	Click to open a CLI console window to view and edit the setting in the CLI. If there are multiple CLI settings on the page, the CLI console shows the first setting.

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.

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.

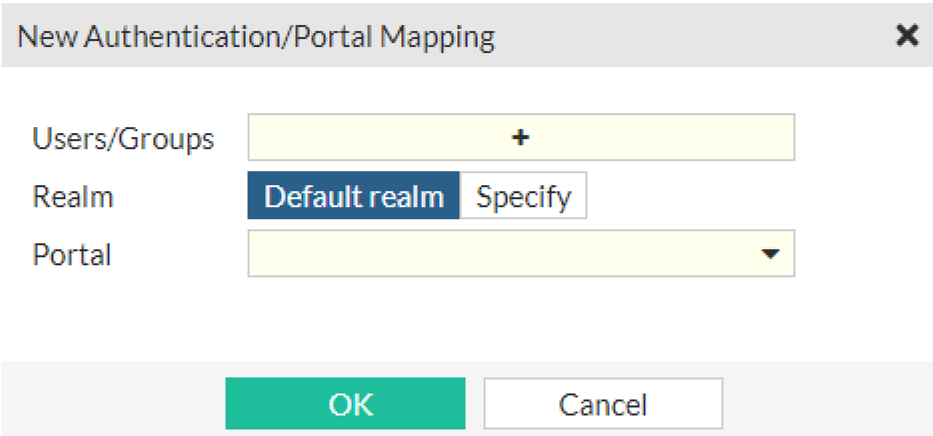
Users connecting in web mode can connect to the web portal over IPv4 or IPv6. They can access bookmarks in either IPv4 or IPv6, depending on the preferred DNS setting of the web portal.

To enable dual stack in the CLI:

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

Create or edit an authentication/portal mapping

Select *Create New* to open the New Authentication/Portal Mapping page.



Configure the following settings and then click *OK*:

Users/Groups	Select + to choose which users and user groups to add.
Realm	Select *Default realm* or *Specify.* If you select *Specify*, select a realm from the drop-down list.
Portal	Select an SSL-VPN portal from the drop-down list. To create an SSL-VPN portal, see Create or edit an SSL-VPN portal on page 400.

SSL-VPN Personal Bookmarks

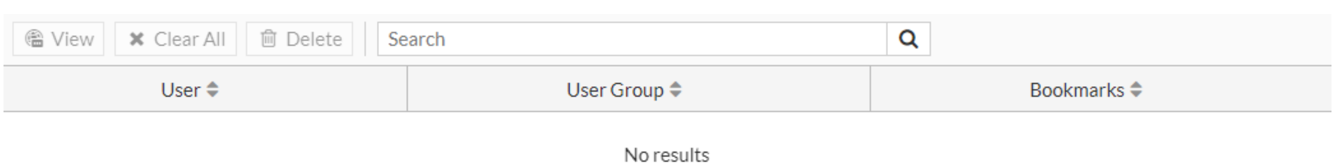
The administrator has the ability to view bookmarks the remote client has added to the remote client's SSL-VPN login in the bookmarks widget. This enables the administrator to monitor and, if needed, remove unwanted bookmarks that do not meet with corporate policy.

To view and maintain remote client bookmarks, go to *VPN > SSL-VPN Personal Bookmarks*.

To enable personal bookmarks:

1. Go to *System > Feature Visibility*.
2. Enable *SSL-VPN Personal Bookmark Management*.
3. Click *Apply*.

To view the list of personal bookmarks, go to *VPN > SSL-VPN Personal Bookmarks*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

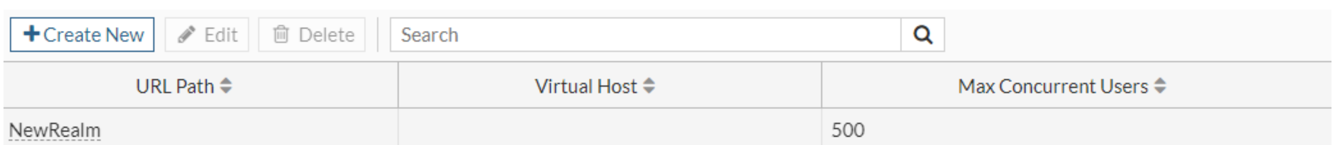
The following options are available:

View	Select a bookmark and then select *View* to see the bookmark target.
Clear All	Select *Clear All* to delete all personal bookmarks.
Delete	Select a bookmark and then select *Delete* to remove the selected bookmark.
Search	Enter a search term to find in the list.
User	The user who created the bookmark.
User Group	The user groups that have access to the bookmark.
Bookmarks	The IP address source.

SSL-VPN Realms

You can go to *VPN > SSL-VPN Realms* and create custom login pages for your SSL-VPN users. You can use this feature to customize the SSL-VPN login page for your users and also to create multiple SSL-VPN logins for different user groups.

To view the list of available SSL-VPN realms, go to *VPN > SSL-VPN Realms*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

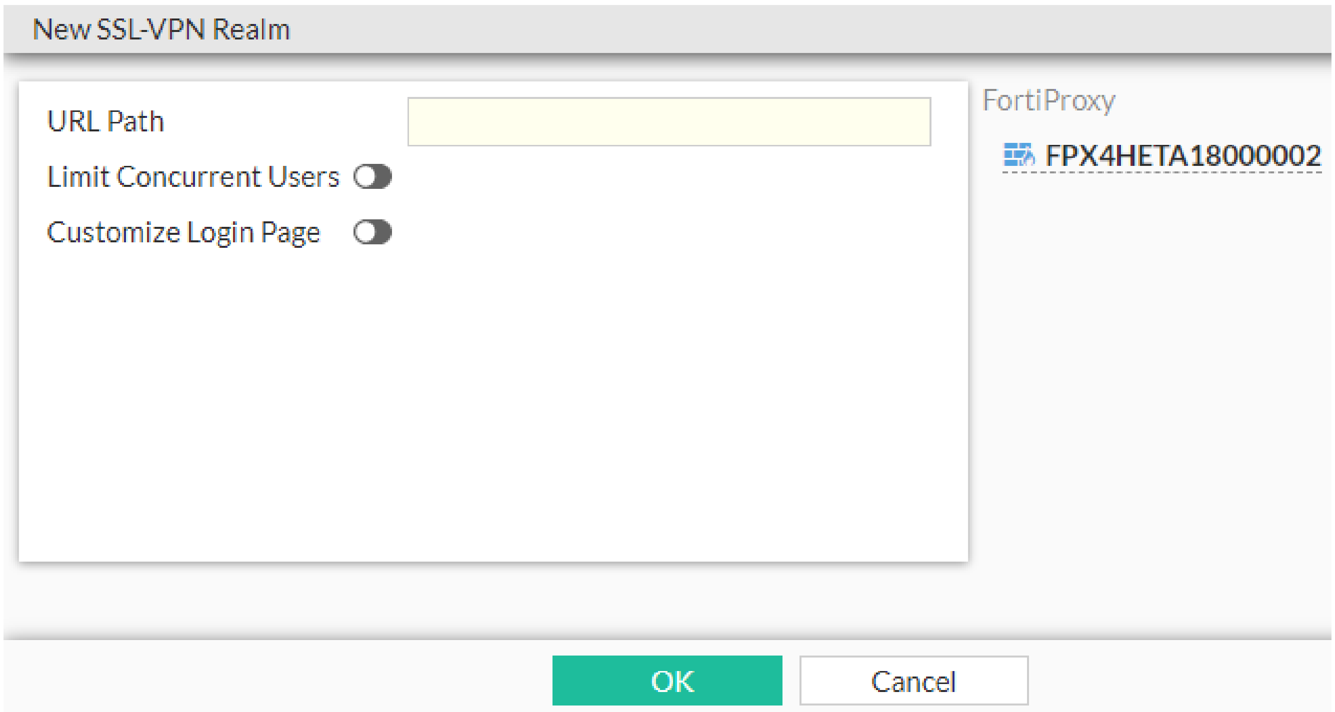
The following options are available:

Create New	Create an SSL-VPN realm. See Create or edit an SSL-VPN realm on page 411.
Edit	Modify the selected SSL-VPN realm. See Create or edit an SSL-VPN realm on page 411.
Delete	Delete the selected SSL-VPN realm.
Search	Enterr a search term to find in the list.
URL Path	The actual path for the custom login page.
Virtual Host	The virtual host name for this realm.
Max Concurrent Users	The maximum number of users that can access the custom login at any given time.

Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit an SSL-VPN realm

Select *Create New* to open the *New SSL-VPN Realm* window.



Select an SSL-VPN realm and then click *Edit* to open the *Edit SSL-VPN Realm* window.

Configure the following settings in the *New SSL-VPN Realm* window or *Edit SSL-VPN Realm* window and then click *OK*:

URL Path	Enter the URL path to access the SSL-VPN login page. Do not include “http://”.
Limit Concurrent Users	Move the slider to limit the number of users that can access the custom login at any given time and then enter the maximum number of users.
Customize Login Page	*Enable* if you want to change the login page for the SSL-VPN realm, click *Edit*, and then make your changes in the *text/html* column.
Restore Defaults	Select this option to undo your changes to the login page.

To configure SSL-VPN realms using the GUI:

1. Configure a custom SSL VPN login by going to *VPN > SSL-VPN Realms* and selecting *Create New*. Users access different portals depending on the URL they enter.
2. Configure the settings and click *OK*.

3. After adding the custom login, you must associate it with the users that will access the custom login. Go to *VPN > SSL-VPN Settings*. Under *Authentication/Portal Mapping*, select *Create New* and select the user groups and the associated realm.
4. Click *OK* to save the authentication/portal mapping.
5. Click *Apply* to save your changes to the SSL-VPN settings.

User & Authentication

The *User & Authentication* menu allows you to configure user accounts, user groups, guests, authentication settings, and FortiTokens.

FortiProxy units support the use of external authentication servers. An authentication server can provide password checking for selected FortiProxy users, or it can be added as a member of a FortiProxy user group.

NOTE: If you are going to use authentication servers, you must configure the servers before you configure the FortiProxy users or user groups that require them.

This section describes the following topics:

- User Definition on page 413
- User Groups on page 418
- Guest Management on page 422
- LDAP Servers on page 424
- RADIUS Servers on page 427
- TACACS+ Servers on page 429
- Kerberos on page 432
- SAML on page 433
- FortiTokens on page 437

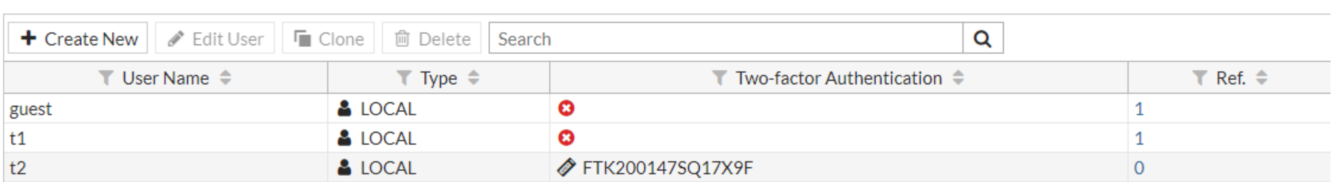
User Definition

A user is defined in a user account that consists of a user name, password and, in some cases, other information that can be configured on the unit or on an external authentication server. Users can access resources that require authentication only if they are members of an allowed user group.

A local user is a user configured on a unit. The user can be authenticated with a password stored on the unit or with a password stored on an authentication server. The user name must match a user account stored on the unit, and the user name and password must match a user account stored on the authentication server associated with the user.

Go to *User & Authentication* > *User Definition* and select *Create New* to create new users with the *Users/Groups Creation Wizard*.

To configure users, go to *User & Authentication* > *User Definition*.



User Name	Type	Two-factor Authentication	Ref.
guest	LOCAL		1
t1	LOCAL		1
t2	LOCAL	FTK200147SQ17X9F	0

Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Run the Users/Groups Creation Wizard and create a user. You can also use the wizard to create new groups. See Create a user on page 414.
Edit User	Edit a user. See Edit a user on page 417.
Clone	Make a copy of a user.
Delete	Delete a user or users.
Search	Enter a search term to find in the user list.
User Name	The name of the user.
Type	The type of user, such as *Local* or *LDAP*.
Two-factor Authentication	Displays whether the user has token two-factor authentication enabled.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create a user

Use the *Users/Groups Creation Wizard* to create user accounts. From the *User Definition* page, select *Create New* to start the wizard.

To create a local user:

1. In the *User Type* page, select *Local User* and then select *Next*.
2. In the *Login Credentials* page, enter a user name and password for the new user and then select *Next*.
3. In the *Contact Info* page, enter an email address for the user and then select *Next*. Alternatively, you can supply the user’s SMS contact information. To assign a FortiToken to the user, enable *Two-factor Authentication* and select a token from the drop-down menu provided. The *Contact Info* page is optional.
4. In the *Extra Info* page, select *Enabled* to make the new user active. To place the user into a group, enable *User Group* and then select a group from the drop-down menu. For information on user groups, see Create or edit a user group on page 420.
5. Select *Submit* to create the new local user.

To create a remote RADIUS user:

1. In the *User Type* page, select *Remote RADIUS User* and then select *Next*.
2. In the *RADIUS Server* page, enter a user name, select a RADIUS server from the drop-down menu, and then select *Next*. For information on RADIUS servers, see Create or edit a RADIUS server on page 428.
3. In the *Contact Info* page, enter an email address for the user and then select *Next*. Alternatively, you can supply the user’s SMS contact information. To assign a FortiToken to the user, enable *Two-factor Authentication* and select a token from the drop-down menu provided. The *Contact Info* page is optional.
4. In the *Extra Info* page, select *Enabled* to enable the new user. To place the user into a group, enable *User Group* and then select a group from the drop-down menu. For information on user groups, see Create or edit a user group

on page 420.

5. Select *Submit* to create the new RADIUS user.

To create a remote TACACS+ user:

By default, the *TACACS+ Servers* option under *User & Device* is not visible unless you add a server using the following CLI command:

```
config user tacacs+
    edit <name>
        set server <IP_address>
    next
end
```

1. In the *User Type* page, select *Remote TACACS+ User* and then select *Next*.
2. In the *TACACS+ Server* page, enter a user name, select a TACACS+ server from the drop-down menu, and then select *Next*. For information on TACACS+ servers, see Create or edit a TACACS server on page 431
3. In the *Contact Info* page, enter an email address for the user and then select *Next*. Alternatively, you can supply the user's SMS contact information. To assign a FortiToken to the user, enable *Two-factor Authentication* and select a token from the drop-down menu provided. The *Contact Info* page is optional.
4. In the *Extra Info* page, select *Enabled* to enable the new user. To place the user into a group, enable *User Group* and then select a group from the drop-down menu. For information on user groups, see Create or edit a user group on page 420.
5. Select *Submit* to create the new TACACS+ user.

To create a remote LDAP user:

1. In the *User Type* page, select *Remote LDAP User* and then select *Next*.
2. In the *LDAP Server* page, select an existing LDAP server from the drop-down menu or create an LDAP server and then select *Next*. To create an LDAP server, select the *Create New* icon in the drop-down menu, enter the required information, and then click *OK*. For information on LDAP servers, see Create or edit an LDAP server on page 425.
3. In the *Remote Users* page, enter and apply the LDAP filter, enter a search term to search the server, and select a user from the results.
4. Select *Submit* to create the remote LDAP user.

To use Fortinet Single Sign-On (FSSO):

1. In the *User Type* page, select *FSSO* and then select *Next*.
2. In the *Remote Groups* page, select the FSSO agent, select an AD group, and then select *Next*.

   To create an AD group, see To create an AD group:.
3. In the *Local Group* page, select *Choose Existing* or *Create New*.

   If you select *Choose Existing*, select the FSSO group name from the drop-down menu.

   If you select *Create New*, enter the name of the FSSO group in the field.
4. Select *Submit* to use FSSO.
5. Click *OK* in the confirmation dialog box.

To create an AD group:

```
config user adgrp
   edit <AD_group_name>
      set server-name <FSSO_agent_name>
   next
end
```

For example:

```
config user adgrp
   edit adgroup1
      set server-name NewFSSOserver
   next
end
```

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
```

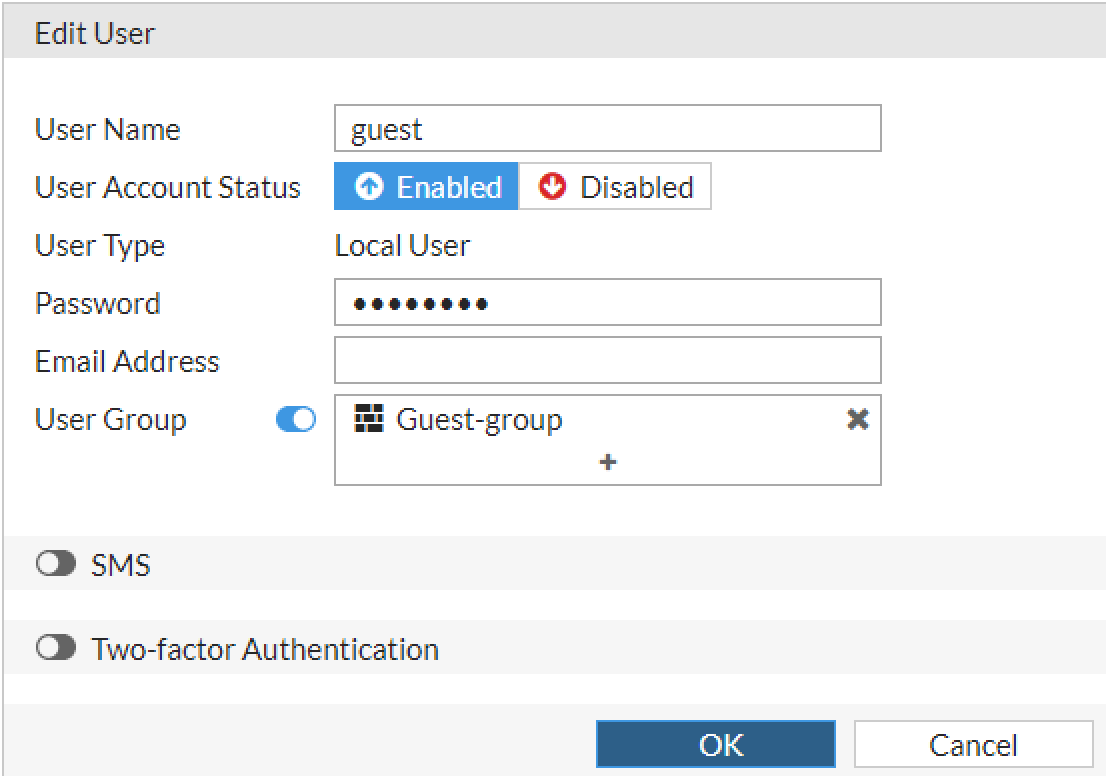
To configure Active Directory in LDS mode:

```
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
```

Edit a user

To edit a user:

1. Select the user you want to edit and then click *Edit User* from the toolbar or double-click on the user in the table. The *Edit User* window opens.



2. Edit the user information as required or select *Disabled* to disable the user account.
3. Click *OK* to apply your changes.

User Groups

A user group is a list of user identities. An identity can be one of the following:

- a local user account (user name and password) stored on the Fortinet unit
- a local user account with a password stored on a RADIUS, LDAP, or TACACS+ server
- a RADIUS, LDAP, or TACACS+ server (all identities on the server can authenticate)
- a user or user group defined on a Directory Service server

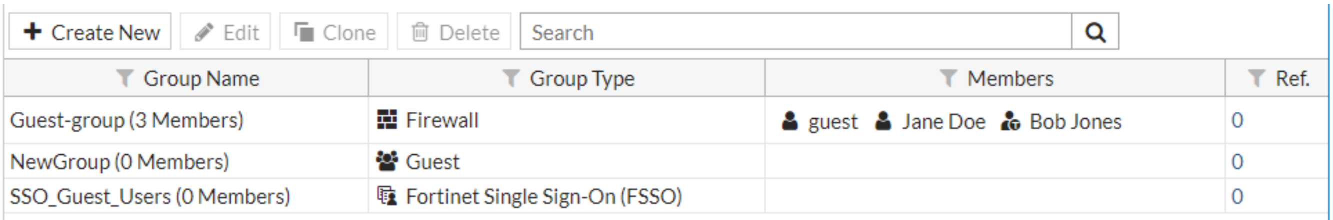
There are four types of user groups:

- Firewall
- Fortinet Single Sign-On (FSSO)
- RADIUS Single Sign-On (RSSO)
- Guest

For each resource that requires authentication, you specify which user groups are permitted access. You need to determine the number and membership of user groups appropriate to your authentication needs.

Users that are associated with multiple groups have access to all services within those user groups. This access is only available in the CLI with the `auth-multi-group` command, which is enabled by default. This feature checks all groups a user belongs to for firewall authentication.

To configure user groups, go to *User & Authentication > User Groups*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

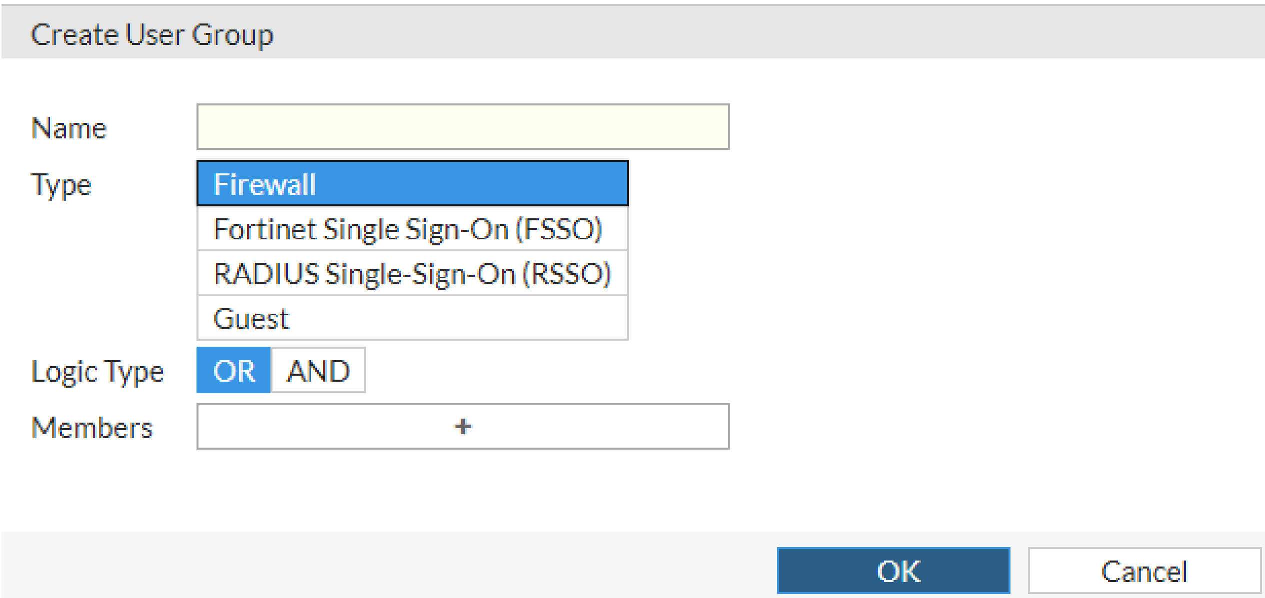
The following options are available:

Create New	Create a user group. See Create or edit a user group on page 420.
Edit	Edit a user group. See Create or edit a user group on page 420.
Clone	Make a copy of a user group.
Delete	Delete a group or groups.
Search	Enter a search term to search the user group list.
Group Name	The name of the user group.
Group Type	The type of group: *Firewall*, *Fortinet Single Sign-On (FSSO)*, *RADIUS Single-Sign-On (RSSO)*, or *Guest*.
Members	The names of the members in the group.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a user group

To create a user group:

1. In the user group list, select *Create New* from the toolbar. The *Create User Group* window opens.



2. Enter a name for the group in the *Name* field.
3. Select the group type in the *Type* field, one of: *Firewall*, *Fortinet Single Sign-On (FSSO)*, *RADIUS Single-Sign-On (RSSO)*, or *Guest*.
4. Enter the following information, depending on the group type selected:

Firewall	This type of group can be selected in any security policy that requires firewall authentication.
Logic Type	Select whether OR or AND logic is used for matching memberships of a user group.
Members	If you selected a Firewall user group, select users to add to the group from the drop-down list.
Fortinet Single Sign-On (FSSO)	This type of group can be selected in any security policy that requires FSSO authentication.
Logic Type	Select whether OR or AND logic is used for matching memberships of a user group.
Members	If you selected the FSSO user group, select users to add to the group from the drop-down list.
RADIUS Single Sign-On (RSSO)	This type of group can be selected in any security policy that requires RSSO authentication.
RADIUS Attribute Value	If you selected the RSSO user group, enter the RADIUS attribute value. This value matches the value from the RADIUS Accounting-Start attribute.

Guest	This type of group can be selected in any security policy that allows guest authentication.
Batch Guest Account Creation	If you selected the Guest user group, enable the creation of batches of guest accounts. When enabled, only the *Maximum Accounts*, *Start Countdown*, and *Time* options are available.
User ID	If you selected the Guest user group, select a user identifier option: • *Email*: The user identifier is emailed. • *Auto Generated*: The user identifier is generated automatically. • *Specify*: The user identifier must be specified.
Maximum Accounts	If you selected the Guest user group, enable *Maximum Accounts* to limit how many accounts exist and then enter the maximum number in the field.
Require Name	If you selected the Guest user group, enable *Require Name* to require names for guests.
Require Email	If you selected the Guest user group, enable *Require Email* to require email addresses for guests.
Require SMS	If you selected the Guest user group, enable *Require SMS* to require SMS contact information for guests.
Password	If you selected the Guest user group, enable *Password* to require passwords for guests and then select a password option: • *Auto Generated*: The password is generated automatically. • *Specify*: The password must be specified.
Sponsor	If you selected the Guest user group, enable *Sponsor* and select *Required* to make a sponsor a requirement for guests.
Company	If you selected the Guest user group, enable *Company* and select *Required* to make a company a requirement for guests.
Start Countdown	If you selected the Guest user group, select when the expiration countdown begins for the user group, either *On account Creation* or *After first login*.
Time	If you selected the Guest user group, select the expiration time for the user group in *Days*, *Hours*, *Minutes*, and *Seconds*.

5. Click *OK* to create the new user group.

To edit a user group:

1. Select the group you want to edit and then click *Edit* from the toolbar or double-click on the group in the table. The *Edit User Group* window opens.
2. Edit the information as required and then click *OK* to apply your changes.

Guest Management

Visitors to your premises might need user accounts on your network for the duration of their stay. If you are hosting a large event such as a conference, you might need to create many such temporary accounts. The FortiProxy Guest Management feature is designed for this purpose.

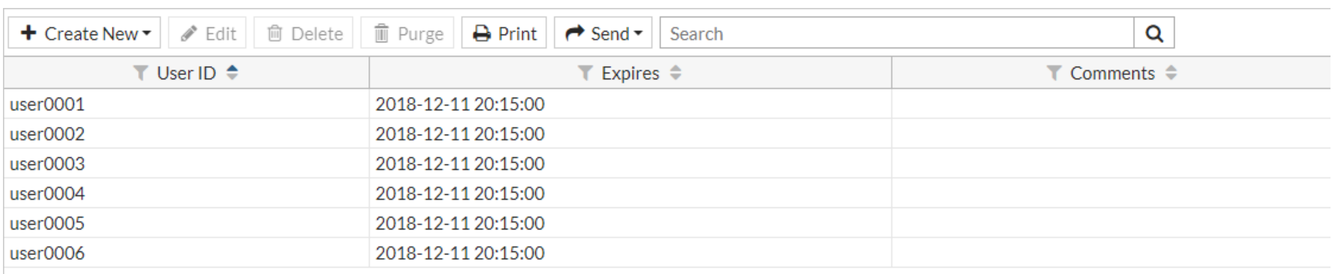
A guest user account User ID can be the user's email address, a randomly generated string, or an ID that the administrator assigns. Similarly, the password can be administrator-assigned or randomly generated.

You can create many guest accounts at the same time using randomly generated User IDs and passwords. This reduces administrator workload for large events.

To set up guest user access, you need to create at least one guest user group and add guest user accounts. Optionally, you can create a guest management administrator whose only function is the creation of guest accounts in specific guest user groups. Otherwise, any administrator can do guest management.

To manage guest access, go to *User & Authentication > Guest Management*.

NOTE: You must create a user group with the Guest group type before the toolbar is displayed on the Guest Management page.



User ID	Expires	Comments
user0001	2018-12-11 20:15:00	
user0002	2018-12-11 20:15:00	
user0003	2018-12-11 20:15:00	
user0004	2018-12-11 20:15:00	
user0005	2018-12-11 20:15:00	
user0006	2018-12-11 20:15:00	

Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

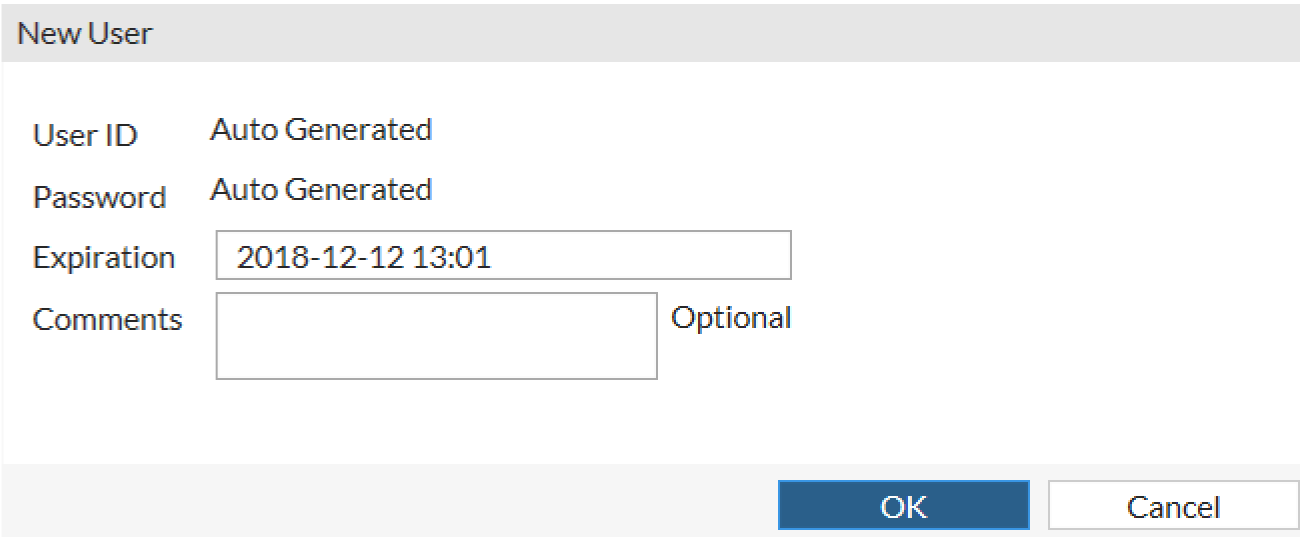
The following options are available:

Create New > User	Create a guest user account. See Create or edit a guest user account on page 423.
Create New > Multiple Users	Create more than one guest user account at the same time. See Create multiple guest user accounts on page 423.
Edit	Modify a guest user account. See Create or edit a guest user account on page 423.
Delete	Remove the selected guest user account.
Purge	Remove all expired accounts from the list.
Print	Print the network guest access credentials, including the user identifiers, passwords, and expiration date and time.
Search	Enter a search term to find in the guest user list
User ID	An automatically generated number to identify the guest user.

Expires	Date and time when the guest user account becomes inactive.
Comments	An optional description of the guest user account.

Create or edit a guest user account

Select *Create New* > *User* to open the *New User* page.



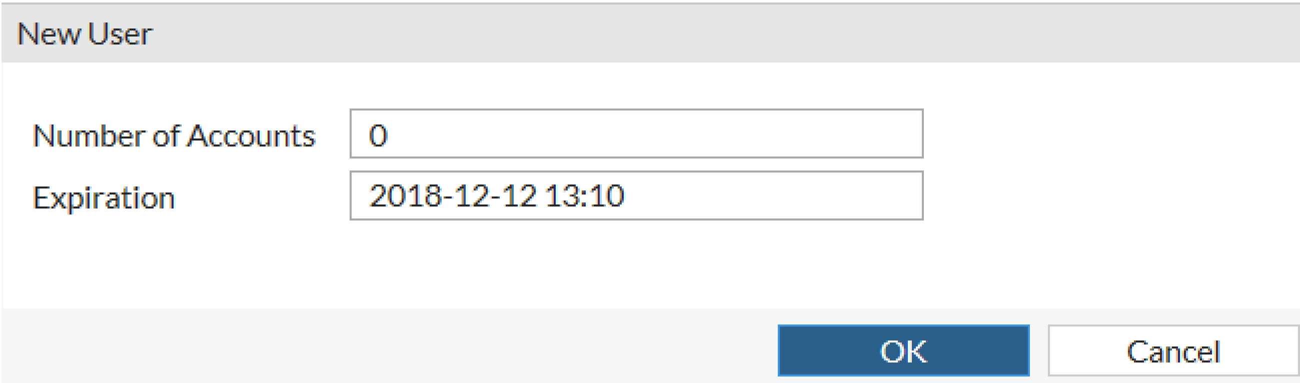
Select a guest user account and then click *Edit* to open the *Edit User* page.

Configure the following settings in the *New User* page or *Edit User* page and then click *OK*:

User ID	The user identifier is automatically generated when you create a guest user account, but you can edit it.
Password	The password is automatically generated when you create a guest user account, but you can edit it.
Expiration	Date and time when the guest user account becomes inactive.
Comments	An optional description of the guest user account.

Create multiple guest user accounts

Select *Create New* > *Multiple Users* to open the *New User* page.



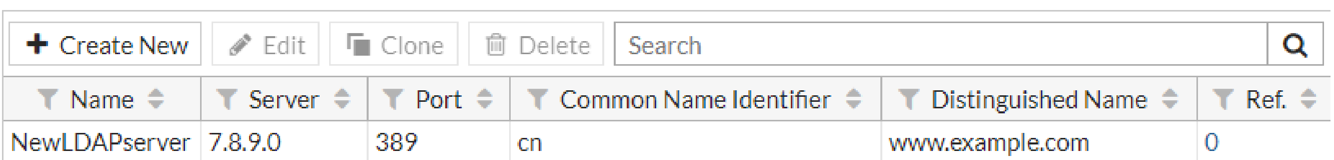
Configure the following settings in the *New User* page and then click *OK*:

Number of Accounts	Enter the number of guest user accounts that you want to create.
Expiration	Date and time when the guest user accounts become inactive.

LDAP Servers

LDAP is an Internet protocol used to maintain authentication data that can include departments, people, groups of people, passwords, email addresses, and printers. LDAP consists of a data-representation scheme, a set of defined operations, and a request/response network.

To manage LDAP servers, go to *User & Authentication > LDAP Servers*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

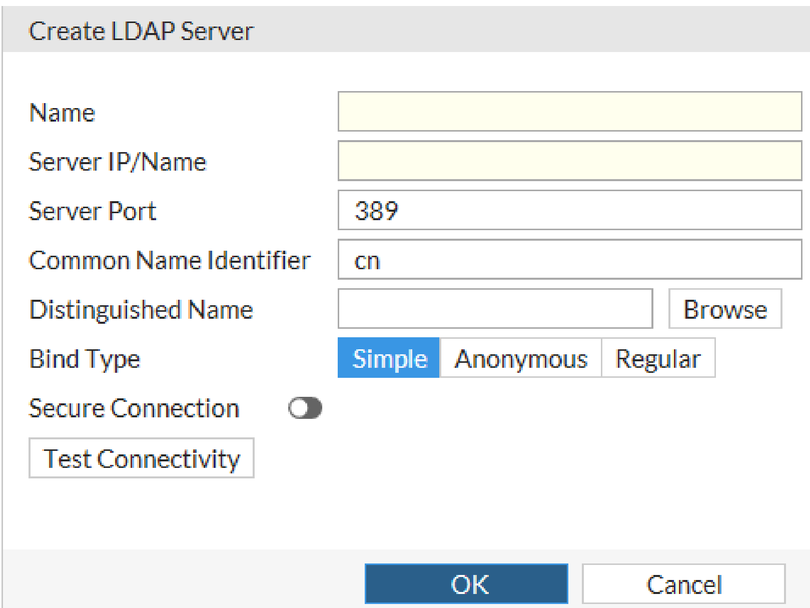
Create New	Create an LDAP server. See Create or edit an LDAP server on page 425.
Edit	Modify an LDAP server. See Create or edit an LDAP server on page 425.
Clone	Make a copy of an LDAP server.
Delete	Remove a server or servers.
Search	Enter a search term to find in the LDAP server list.
Name	The name that identifies the LDAP server on the Fortinet unit.
Server	The domain name or IP address of the LDAP server.

Port	The TCP port used to communicate with the LDAP server. By default, LDAP uses port 389.
Common Name Identifier	The common name identifier for the LDAP server.
Distinguished Name	The base distinguished name for the server using the correct X.500 or LDAP format. The unit passes this distinguished name unchanged to the server.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit an LDAP server

To add a new LDAP server:

1. In the LDAP server list, select *Create New* from the toolbar. The *Create LDAP Server* window opens.



2. Configure the following:

Name	Enter the name that identifies the LDAP server on the FortiProxy unit.
Server IP/Name	Enter the domain name or IP address of the LDAP server.
Server Port	Enter the TCP port used to communicate with the LDAP server. By default, LDAP uses port 389. If you use a secure LDAP server, the default port changes if you select *Secure Connection*.
Common Name Identifier	Enter the common name identifier for the LDAP server. The maximum number of characters is 20.
Distinguished Name	Enter the base distinguished name for the server using the correct X.500 or LDAP format. The unit passes this distinguished name unchanged to the server. The maximum number of characters is 512. You can also select *Browse* to contact and retrieve the specified LDAP server.
Bind Type	Select the type of binding for LDAP authentication. • *Simple*: Connect directly to the LDAP server with user name/password authentication. • *Anonymous*: Connect as an anonymous user on the LDAP server and then retrieve the user name/password and compare them to given values. • *Regular*: Connect to the LDAP server directly with user name and password and then receive acceptance or rejection based on search of given values. Enter the user name and password of the user to be authenticated in the *Username* and *Password* fields.
Secure Connection	Enable to use a secure LDAP server connection for authentication.
Protocol	If you enabled *Secure Connection*, select a secure LDAP protocol to use for authentication, either *STARTTLS* or *LDAPS*. Depending on your selection, the server port changes to the default port for the selected protocol: • *STARTTLS*: port 389 • *LDAPS*: port 636
Certificate	If you enabled *Secure Connection*,select a certificate to use for authentication from the list.
Test Connectivity	Select *Test Connectivity* to test if the LDAP server can be contacted.

3. Click *OK* to create the new LDAP server.

To edit an LDAP server:

1. Select the LDAP server you want to edit and then click *Edit* from the toolbar or double-click on the address in the address table. The *Edit LDAP Server* window opens.
2. Edit the server information as required and click *OK* to apply your changes.

Creating an administrator that can be authenticated by an LDAP server

You can configure a least privileges user account (read access only) in Active Directory for FortiProxy admin users which can be authenticated by an LDAP server:

1. Configure an LDAP server. See Create or edit an LDAP server on page 425. Alternatively, use the `configure user ldap` command.
2. To allow only a particular group of members to login to the FortiProxy as administrators, configure an LDAP user group under *User & Authentication* > *User Group* to limit the access. Alternatively, use the `configure user group` command.
3. Configure an administrator to authenticate with the LDAP server under *System* > *Administrators*. See Administrators on page 445. Alternatively, use the `config system admin` command.
4. Verify the configuration is successful by accessing the FortiProxy GUI using the credentials of the configured LDAP user(s).

RADIUS Servers

RADIUS is a broadly supported client server protocol that provides centralized authentication, authorization, and accounting functions. RADIUS clients are built into gateways that allow access to networks such as Virtual Private Network (VPN) servers, Network Access Servers (NASs), as well as network switches and firewalls that use authentication. FortiProxy units fall into the last category.

RADIUS servers use UDP packets to communicate with the RADIUS clients on the network to do the following:

- Authenticate users before allowing them access to the network
- Authorize access to resources by appropriate users
- Account or bill for those resources that are used

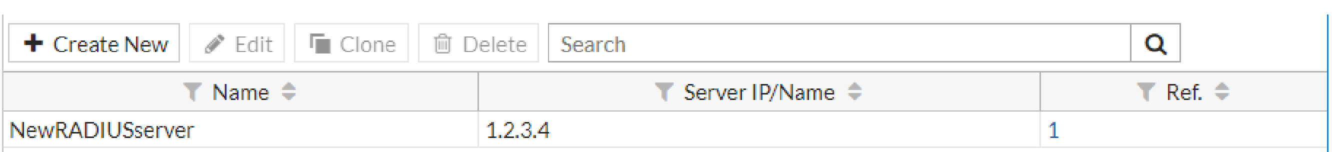
RADIUS servers are currently defined by RFC 2865 (RADIUS) and RFC 2866 (Accounting). They listen on either UDP ports 1812 (authentication) and 1813 (accounting) or ports 1645 (authentication) and 1646 (accounting) requests. RADIUS servers exist for all major operating systems.

You must configure the RADIUS server to accept the FortiProxy unit as a client. FortiProxy units use the authentication and accounting functions of the RADIUS server.

When a configured user attempts to access the network, the FortiProxy unit forwards the authentication request to the RADIUS server, which then matches the user name and password remotely. After authentication succeeds, the RADIUS server passes the Authorization Granted message to the FortiProxy unit, which then grants the user permission to access the network.

The RADIUS server uses a “shared secret” key, along with MD5 hashing, to encrypt information passed between RADIUS servers and clients, including the FortiProxy unit. Typically, only user credentials are encrypted.

To manage RADIUS servers, go to *User & Authentication* > *RADIUS Servers*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

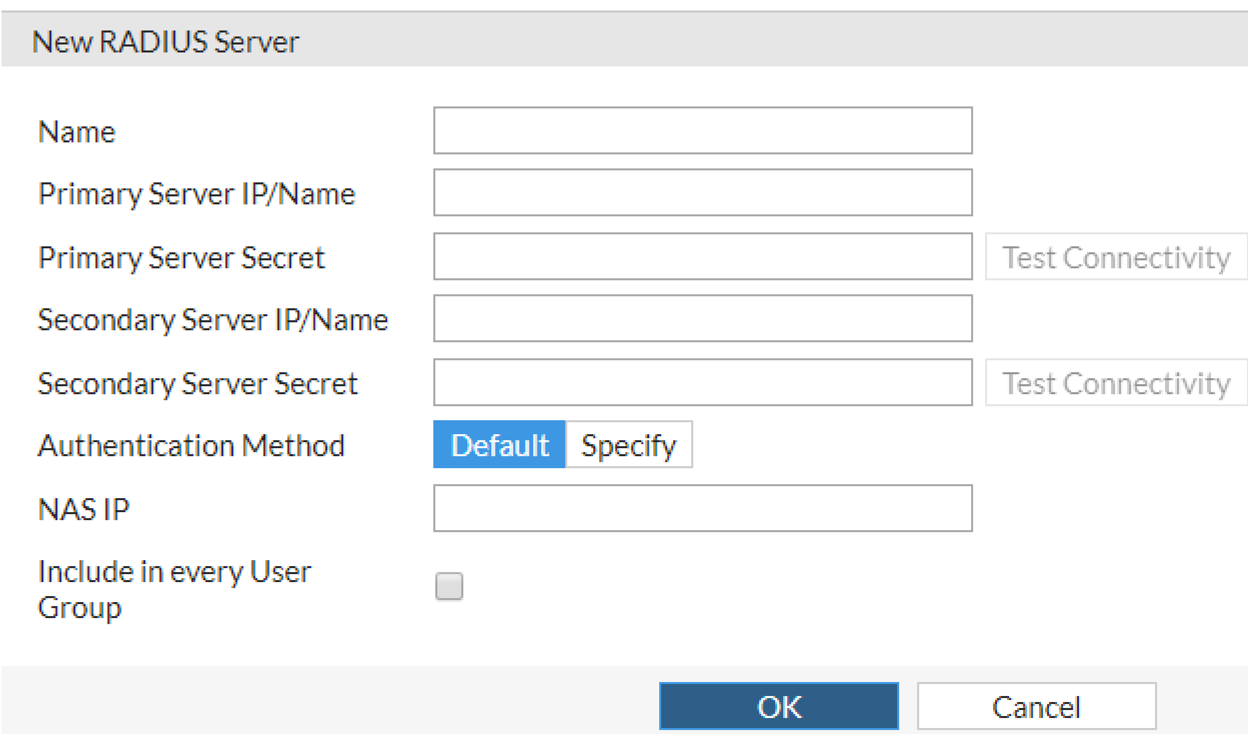
The following options are available:

Create New	Create a RADIUS server. See Create or edit a RADIUS server on page 428.
Edit	Modify a RADIUS server. See Create or edit a RADIUS server on page 428.
Clone	Make a copy of a RADIUS server.
Delete	Remove a server or servers.
Search	Enter a search term to find in the RADIUS server list.
Name	The name that identifies the RADIUS server on the unit.
Server IP/Name	The domain name or IP address of the primary and, if applicable, secondary, RADIUS server.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a RADIUS server

To add a RADIUS server:

1. In the RADIUS server list, select *Create New* from the toolbar. The *New RADIUS Server* window opens.



2. Configure the following:

Name	Enter the name that is used to identify the RADIUS server on the FortiProxy unit.
Primary Server IP/Name	Enter the domain name or IP address of the primary RADIUS server.
Primary Server Secret	Enter the RADIUS server secret key for the primary RADIUS server. The primary server secret key length can be up to a maximum of 16 characters. For security reason, it is recommended that the server secret key be the maximum length.
Test Connectivity	Select *Test Connectivity* to test if the primary and secondary RADIUS servers can be contacted using the domain name or IP address and secret provided.
Secondary Server IP/Name	Enter the domain name or IP address of the secondary RADIUS server, if applicable.
Secondary Server Secret	Enter the RADIUS server secret key for the secondary RADIUS server. The secondary server secret key can be up to a maximum length of 16 characters.
Authentication Method	Select *Default* to authenticate with the default method. Select *Specify* to override the default authentication method and then select the protocol from the list: *MSCHAP-v2*, *MS-CHAP*, *CHAP*, or *PAP*.
NAS IP	Optionally, enter the NAS IP address (RADIUS Attribute 31, outlined in RFC 2548). In this configuration, the FortiProxy unit is the NAS, which is how the RADIUS server registers all valid servers that use its records. If you do not enter an IP address, the IP address that the Fortinet interface uses to communicate with the RADIUS server is applied.
Include in every User Group	Enable to have the RADIUS server automatically included in all user groups.

3. Click *OK* to create the new RADIUS server.

To edit a RADIUS server:

1. Select the RADIUS server you want to edit and then click *Edit* from the toolbar or double-click on the address in the address table. The *Edit RADIUS Server* window opens.
2. Edit the server information as required and click *OK* to apply your changes.

TACACS+ Servers

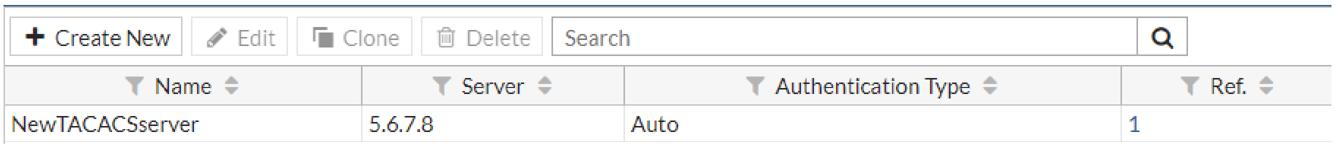
TACACS+ is a remote authentication protocol that provides access control for routers, network access servers, and other networked computing devices through one or more centralized servers. TACACS+ allows a client to accept a user name and password and send a query to a TACACS+ authentication server. The server host determines whether to accept or deny the request and sends a response back that allows or denies the user access to the network.

TACACS+ offers fully encrypted packet bodies and supports both IP and AppleTalk protocols. TACACS+ uses TCP port 49, which is seen as more reliable than RADIUS's UDP.

By default, the *TACACS+ Servers* option under *User & Device* is not visible unless you add a server using the following CLI command:

```
config user tacacs+
    edit <name>
        set server <IP_address>
    next
end
```

To manage TACACS+ servers, go to *User & Authentication > TACACS+ Servers*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

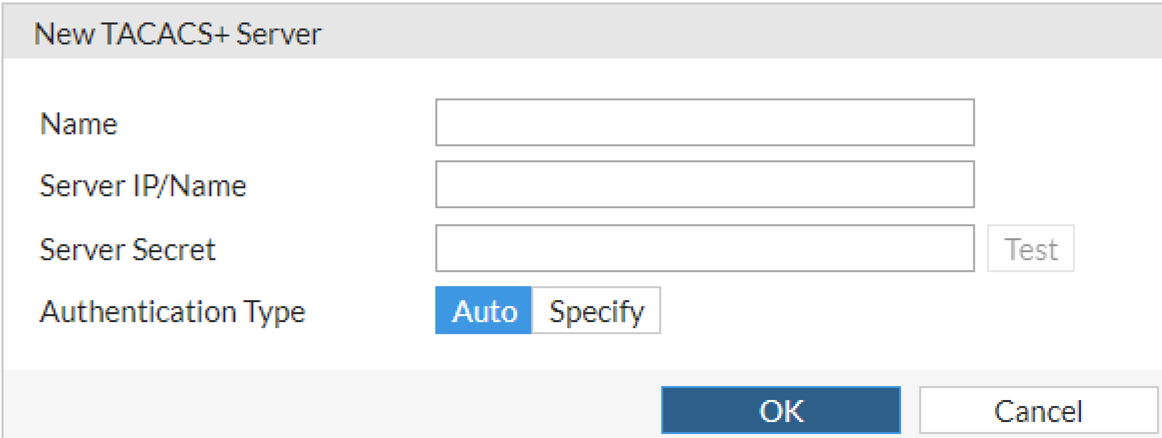
The following options are available:

Create New	Create a TACACS+ server. See Create or edit a TACACS server on page 431.
Edit	Modify a TACACS+ server. See Create or edit a TACACS server on page 431.
Clone	Make a copy of a TACACS+ server.
Delete	Remove a server or servers.
Search	Enter a search term to find in the TACACS+ server list.
Name	The name that identifies the TACACS+ server on the unit.
Server	The domain name or IP address of the TACACS+ server.
Authentication Type	The authentication type used by the server.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a TACACS server

To add a TACACS+ server:

1. In the TACACS+ server list, select *Create New* from the toolbar. The *New TACACS+ Server* window opens.



2. Configure the following:

Name	Enter the name of the TACACS+ server.
Server IP/Name	Enter the server domain name or IP address of the TACACS+ server.
Server Secret	Enter the key to access the TACACS+ server. The server key can be a maximum of 16 characters in length.
Authentication Type	Select the authentication type to use for the TACACS+ server: Auto, MSCHAP, CHAP, PAP, or ASCII. Auto authenticates using PAP, MSCHAP, and CHAP, in that order. For more information, see Authentication protocols.

3. Click *OK* to create the new TACACS+ server.

To edit a TACACS+ server:

1. Select the TACACS+ server you want to edit and then click *Edit* from the toolbar or double-click on the address in the address table. The *Edit TACACS+ Server* window opens.
2. Edit the server information as required and click *OK* to apply your changes.

Authentication protocols

ASCII	Machine-independent technique that uses representations of English characters. Requires user to type a user name and password that are sent in clear text (unencrypted) and matched with an entry in the user database, which is stored in ASCII format.
PAP	Password Authentication Protocol (PAP). Used to authenticate PPP connections. Transmits passwords and other user information in clear text.

CHAP	Challenge-Handshake Authentication Protocol (CHAP). Provides the same functionality as PAP but is more secure because it does not send the password and other user information over the network to the security server.
MSCHAP	Microsoft Challenge-Handshake Authentication Protocol v1 (MSCHAP). Microsoft-specific version of CHAP.
Auto	The default protocol configuration, Auto, uses PAP, MSCHAP, and CHAP, in that order.

Kerberos

Kerberos authentication is a method for authenticating both explicit web proxy and transparent web proxy users. It has several advantages over NTLM challenge response:

- Does not require FSSO/AD agents to be deployed across domains.
- Requires fewer round-trips than NTLM SSO, making it less latency sensitive.
- Is (probably) more scalable than challenge response.
- Uses existing Windows domain components rather than added components.
- NTLM may still be used as a fallback for non-Kerberos clients.

To configure Kerberos authentication service, go to *User & Authentication > Kerberos*.

Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

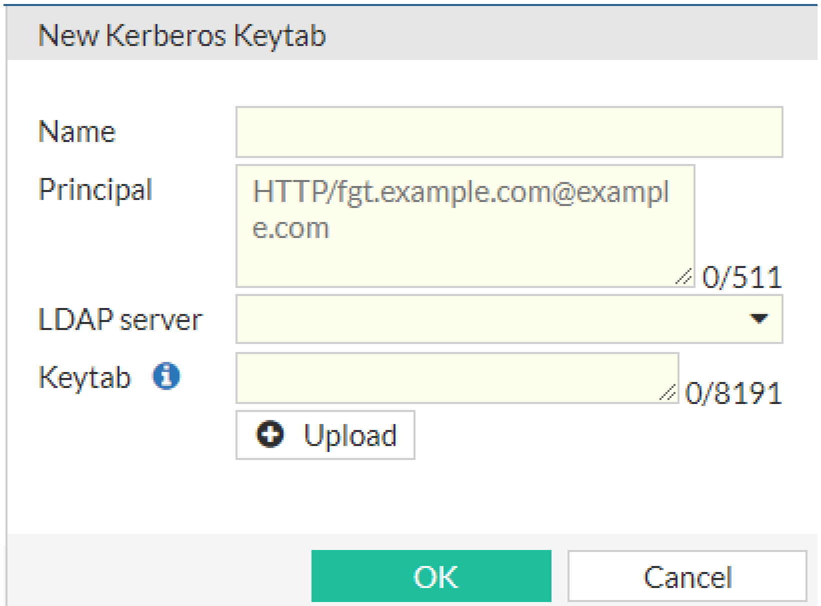
The following options are available:

Create New	Create a Kerberos authentication service. See Create or edit a Kerberos authentication service on page 433.
Edit	Modify a Kerberos authentication service. See Create or edit a Kerberos authentication service on page 433.
Delete	Remove a Kerberos authentication service or services.
Name	The name of the Kerberos authentication service.
Principal	The server domain name of the Kerberos authentication service.
LDAP Server	The name of the LDAP server used for authorization.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit a Kerberos authentication service

To add a new Kerberos authentication service:

1. In the Kerberos service list, select *Create New* from the toolbar. The *New Kerberos Keytab* window opens.



2. Configure the following:

Name	Enter the name of the Kerberos authentication service.
Principal	Enter the server domain name of the Kerberos authentication service.
LDAP server	Enter the name of the LDAP server used for authorization.
Keytab	Select *Upload* and then navigate to the file that contains the shared secret. Use the `ktpass` command (found on Windows servers and many domain workstations) to generate the Kerberos keytab.

3. Click *OK* to create the new Kerberos authentication service.

To edit the Kerberos authentication service:

1. Select the Kerberos authentication service you want to edit and then click *Edit* from the toolbar or double-click on the service in the service table. The *Edit Kerberos Keytab* window opens.
2. Edit the service information as required and click *OK* to apply your changes.

SAML

Security Assertion Markup Language (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization data between two security domains: an Identity Provider (IdP) and a Service Provider (SP). The FortiProxy unit supports the SAML protocol and will act as a Service Provider.

In SAML-SP authentication, the FortiProxy unit redirects unauthenticated users to the IdP (FortiAuthenticator, Okta Identity, Microsoft ADFS, or similar) for authentication. After the user is authenticated with the IdP, the user is redirected to the FortiProxy unit with SAML assertion information using the POST method. The assertion information includes the authentication result, user name, and group in attribute assertions (or claim in terms of ADFS). Based on that information, the FortiProxy unit executes both authentication and authorization (matching the user to the group). If the IdP is Microsoft ADFS, the FortiProxy unit supports resolving the user group information through the LDAP query with Kerberos or NTLM authentication.

To manage SAML servers, go to *User & Authentication* > *SAML*.

Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

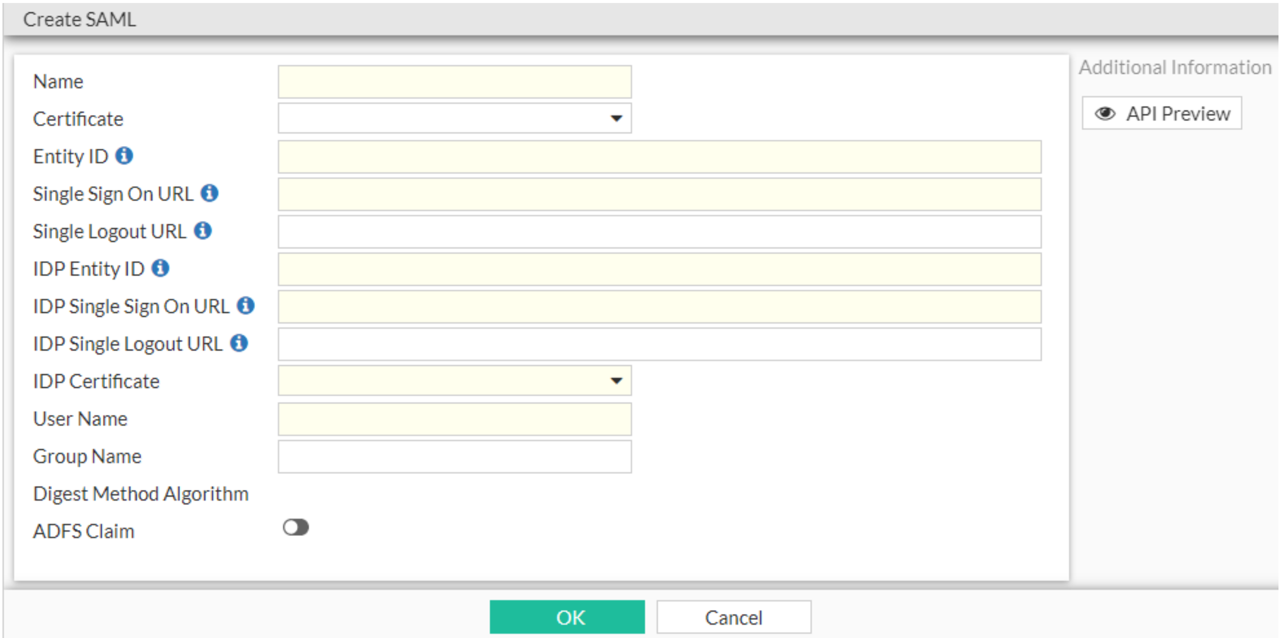
The following options are available:

Create New	Create a SAML server. See Create or edit a SAML server on page 435.
Edit	Modify a SAML server. See Create or edit a SAML server on page 435.
Delete	Remove a server or servers.
Name	The name that identifies the SAML server on the Fortinet unit.
Entity ID	The SP entity identifier.
Single Sign On URL	The SP single sign-on URL.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.
ADFS Claim	Enable or disable the ADFS claim for the user and group attributes in the assertion statement.
digest-method	Which algorithm is used for the digest method.
Group Claim Type	The group claim in the assertion statement.
Group Name	The group name in assertion statement.
IDP Entity ID	The IDP entity identifier.
IDP Single Logout URL	The IDP single logout URL.
IDP Single Sign On URL	The IDP single sign-on URL.
Single Logout URL	The SP single logout URL.
User Claim Type	The user name claim in the assertion statement.
User Name	The user name in the assertion statement.

Create or edit a SAML server

To add a new SAML server in the GUI:

1. In the SAML server list, click *Create New* from the toolbar. The *Create SAML* window opens.



2. Configure the following:

Name	Enter the name that identifies the SAML server on the FortiProxy unit.
Certificate	Select the certificate to sign SAML messages.
Entity ID	Enter the service provider entity identifier. The URL must start with `http://` or `https://`.
Single Sign On URL	Enter the service provider single sign-on URL. The URL must start with `http://` or `https://`.
Single Logout URL	Enter the service provider single logout URL. The URL must start with `http://` or `https://`.
IDP Entity ID	Enter t he identity provider entity identifier. The URL must start with `http://` or `https://`.
IDP Single Sign On URL	Enter the identity provider single sign-on UR. The URL must start with `http://` or `https://`.
IDP Single Logout URL	Enter the identity provider single logout URL. The URL must start with `http://` or `https://`.
IDP Certificate	Enter the identity provider certificate name.
User Name	Enter the user name in the assertion statement.
Group Name	Enter the group name in the assertion statement.
Digest Method Algorithm	Select the algorithm used for the digest method.
ADFS Claim	Enable or disable the ADFS claim for the user and group attributes in the assertion statement.
User Claim Type	Select the user name claim in the assertion statement.
Group Claim Type	Select the group claim in the assertion statement.

3. Click *OK* to create the new SAML server.

To add a new SAML server in the CLI:

```
config user saml
   edit <SAML_server_entry_name>
      set cert <certificate_to_sign_SAML_messages>
      set entity-id <service_provider_entity_ID>
      set single-sign-on-url <service_provider_single_sign-on_URL>
      set single-logout-url <service_provider_single_logout_URL>
      set idp-entity-id <identity_provider_entity_ID>
      set idp-single-sign-on-url <identity_provider_single_sign-on_URL>
      set idp-single-logout-url <identity_provider_single_logout_URL>
      set idp-cert <identity_provider_certificate_name>
      set user-name <user_name_in_assertion_statement>
      set group-name <group_name_in_assertion_statement>
      set algo {sha1 | sh256}
      set adfs-claim {enable | disable}
      set limit-relaystate {enable | disable}
      set user-claim-type {email | given-name | name | upn | common-name | email-adfs-1x |
           group | upn-adfs-1x | role | sur-name | ppid | name-identifier | authentication-
```

```
            method | deny-only-group-sid | deny-only-primary-sid | deny-only-primary-group-
            sid | group-sid | primary-group-sid | primary-sid | windows-account-name }
        set group-claim-type {email | given-name | name | upn | common-name | email-adfs-1x |
            group | upn-adfs-1x | role | sur-name | ppid | name-identifier | authentication-
            method | deny-only-group-sid | deny-only-primary-sid | deny-only-primary-group-
            sid | group-sid | primary-group-sid | primary-sid | windows-account-name}
    next
end
```

To edit a SAML: server:

1. Select the SAML server you want to edit and then click *Edit* from the toolbar. The *Edit SAML* window opens.
2. Edit the server information as required and click *OK* to apply your changes.

FortiTokens

FortiToken is a disconnected one-time password (OTP) generator. It is a small physical device with a button that when pressed displays a six digit authentication code. This code is entered with a user's username and password as two-factor authentication. The code displayed changes every 60 seconds, and, when not in use, the LCD screen is blanked to extend the battery life.

There is also a mobile phone application, FortiToken Mobile, that performs much the same function.

FortiTokens have a small hole in one end. This is intended for a lanyard to be inserted so the device can be worn around the neck, or easily stored with other electronic devices. Do not put the FortiToken on a key ring as the metal ring and other metal objects can damage it. The FortiToken is an electronic device like a cell phone and must be treated with similar care.

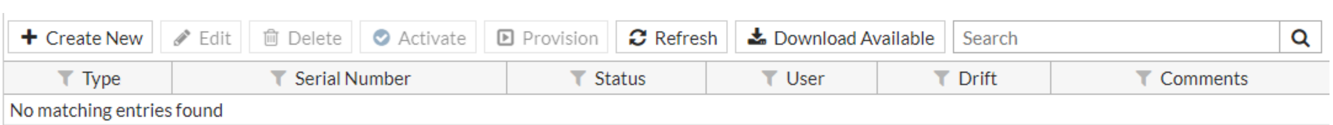
Any time information about the FortiToken is transmitted, it is encrypted. When the FortiProxy unit receives the code that matches the serial number for a particular FortiToken, it is delivered and stored encrypted. This is in keeping with the Fortinet's commitment to keeping your network highly secured.

FortiTokens can be added to user accounts that are local, IPsec VPN, SSL VPN, and even Administrators. See Associate FortiTokens with accounts on page 442.

A FortiToken can be associated with only one account on one FortiProxy unit.

If a user loses the FortiToken, it can be locked out using the FortiProxy unit so it will not be used to falsely access the network. Later if found, that FortiToken can be unlocked on the FortiProxy unit to allow access once again. See FortiToken maintenance on page 443.

To view a list of available FortiTokens, go to *User & Device* > *FortiTokens*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Add a FortiToken to your FortiProxy unit. See Add or edit a FortiToken on page 440.
Edit	Modify a FortiToken that was added to your FortiProxy unit. See Add or edit a FortiToken on page 440.
Delete	Remove a FortiToken from the list.
Activate	Activate a FortiToken that was added to your FortiProxy unit. See Activate a FortiToken on the FortiProxy unit on page 441.
Provision	Notify the FortiToken provisioning server that the token has been assigned for subsequent activation. The provisioning server sends an activation code to the end user.
Refresh	Update the data displayed.
Download Available	Download FortiToken information.
Search	Enter a search term to find in the FortiToken list.
Type	The FortiToken type can be *Hard Token* or *Mobile Token*.
Serial Number	The FortiToken serial number.
Status	Whether the FortiToken has been assigned or activated.
User	The user associated with the FortiToken.
Drift	How many minutes the FortiToken time differs from the time on the FortiProxy unit.
Comments	An optional description of the FortiToken.
License	The license for the mobile token.

FortiToken authentication process

There are three tasks to complete before FortiTokens can be used to authenticate accounts:

1. Add or edit a FortiToken on page 440
2. Activate a FortiToken on the FortiProxy unit on page 441
3. Associate FortiTokens with accounts on page 442

The following are the steps during FortiToken two-factor authentication:

1. The user attempts to access a network resource.
2. The FortiProxy unit matches the traffic to an authentication security policy, and the FortiProxy unit prompts the user for user name and password.
3. The user enters the user name and password.
4. The FortiProxy unit verifies the information, and, if valid, prompts the user for the FortiToken code.
5. The user gets the current code from their FortiToken device.
6. The user enters current code at the prompt.
7. The FortiProxy unit verifies the FortiToken code, and, if valid, allows access to the network resources such as the Internet.

The following steps are needed only if the time on the FortiToken has drifted and needs to be re-synchronized with the time on the FortiProxy unit.

8. If time on FortiToken has drifted, the FortiProxy unit will prompt the user to enter a second code to confirm.
9. User gets the next code from their FortiToken device.
10. User enters the second code at the prompt.
11. The FortiProxy unit uses both codes to update its clock to match the FortiToken and then proceeds as in step 7.

When configured, the FortiProxy unit accepts the user name and password, authenticates them either locally or remotely, and prompts the user for the FortiToken code. The FortiProxy unit then authenticates the FortiToken code. When FortiToken authentication is enabled, the prompt field for entering the FortiToken code is automatically added to the authentication screens.

Even when an Administrator is logging in through a serial or Telnet connection and their account is linked to a FortiToken, that Administrator will be prompted for the token’s code at each login.

If you have attempted to add invalid FortiToken serial numbers, there will be no error message. The serial numbers will simply not be added to the list.

FortiToken Mobile Push

A command under `config system ftm-push` allows you to configure the FortiToken Mobile Push services server IP address and port number. The Push service is provided by Apple (APNS) and Google (GCM) for iPhone and Android smartphones respectively. This service prevents tokens from becoming locked after an already enabled two-factor authentication user has been disabled.

CLI syntax

```
config system ftm-push
   set server-ip <ip-address>
   set server-port [1-65535] // Default is 4433.
   set status <enable | disable>
end
```

NOTE: The `server-ip` is the public IP address of the FortiProxy interface that the FTM will call back to; it is the IP address used by the FortiProxy for incoming FTM calls.

In addition, FTM Push is supported on administrator login and SSL VPN login for both iOS and Android. If an SSL VPN user authenticates with their token, then logs out and attempts to reauthenticate again within a minute, a new message displays showing “Please wait x seconds to login again.” This replaces a previous error/permission denied message.

The “x” value depends on the calculation of how much time is left in the current time step.

CLI syntax

```
config system interface
   edit <name>
      set allowaccess ftm
   next
end
```

The FortiProxy unit supports FTM Push notifications initiated by FortiAuthenticator when users are attempting to authenticate through a VPN and/or RADIUS (with FortiAuthenticator as the RADIUS server).

Migrate FortiToken Mobile users from FortiProxy to FortiToken Cloud

The `execute fortitoken-cloud migrate-ftm <license> <vdom>` command allows the migration of FortiToken Mobile users from the FortiProxy unit to FortiToken Cloud. The FortiToken Cloud account must be using a time-based subscription license. A request must be made to Fortinet Customer Service to initiate and pre-authorize the transfer. All current active FortiToken Mobile users will be migrated to the FortiToken Cloud license with no changes to the FortiToken Mobile serial number. The FortiProxy user or administrator's two-factor setting is automatically converted from `fortitoken` to `fortitoken-cloud`. After migration, end users will be able to authenticate as before without any changes to their FortiToken mobile app. See Migrate FTM tokens to FortiToken Cloud for more information.

Add or edit a FortiToken

Before one or more FortiTokens can be used to authenticate logons, they must be added to the FortiProxy unit. The import feature is used to enter many FortiToken serial numbers at one time. The serial number file must be a text file with one FortiToken serial number per line.

Both FortiToken Mobile and physical FortiTokens store their encryption seeds on the cloud; therefore, you will only be able to register them to a single FortiProxy unit or FortiAuthenticator unit.

Because FortiToken-200CD seed files are stored on the CD, these tokens can be registered on multiple FortiProxy units and/or FortiAuthenticator units, but *not* simultaneously.

To manually add a FortiToken to the FortiProxy using the web-based manager:

1. Go to *User & Authentication > FortiTokens*.
2. Select *Create New*.
3. In *Type*, select *Hard Token* or *Mobile Token*.
4. Enter one or more FortiToken serial numbers (hard token) or activation codes (mobile token).
5. Click *OK*.

For mobile token, you receive the activation code in the license certificate after you purchase a license.

To import multiple FortiTokens to the FortiProxy unit using the web-based manager:

1. Go to *User & Authentication > FortiTokens*.
2. Select *Create New*.
3. In *Type*, select *Hard Token*.
4. Select *Import*.

5. Select *Serial Number File* or *Seed File*, depending on which file you have.
6. Select *Upload* and browse to the local file location on your local computer.
7. Select *Open*. The file is imported.
8. Click *OK*.

To import FortiTokens to the FortiProxy unit from external Sources using the CLI:

FortiToken seed files (both physical and mobile versions) can be imported from either FTP or TFTP servers, or a USB drive, allowing seed files to be imported from an external source more easily:

```
execute fortitoken import ftp <file name> <ip>[:ftp port] <Enter> <user> <password>
execute fortitoken import tftp <file name> <ip>
execute fortitoken import usb <file name>
```

To import seed files for FortiToken Mobile, replace `fortitoken` with `fortitoken-mobile`.

To add two FortiTokens to the FortiProxy unit using the CLI:

```
config user fortitoken
   edit <serial_number>
   next
   edit <serial_number2>
   next
end
```

To edit the settings for a FortiToken:

1. Go to *User & Authentication > FortiTokens*.
2. Select a FortiToken from the list.
3. Select *Edit*.
4. Change the comments and serial number as needed.
5. Click *OK*.

Activate a FortiToken on the FortiProxy unit

After one or more FortiTokens have been added to the FortiProxy unit, they must be activated before being available to be associated with accounts. The process of activation involves the FortiProxy unit querying FortiGuard servers about the validity of each FortiToken. The serial number and information is encrypted before it is sent for added security.

A FortiProxy unit requires a connection to FortiGuard servers to activate a FortiToken.

To activate a FortiToken on the FortiProxy unit using the web-based manager:

1. Go to *User & Authentication > FortiTokens*.
2. Select one or more FortiTokens with a status of *Available*.
3. Right-click the FortiToken entry and select *Activate*.
4. Select *Refresh*. The status of selected FortiTokens will change to *Activated*.

The selected FortiTokens are now available for use with user and admin accounts.

To activate a FortiToken on the FortiProxy unit using the CLI:

```
config user fortitoken
   edit <token_serial_number>
      set status active
   next
end
```

Associate FortiTokens with accounts

The final step before using the FortiTokens to authenticate logons is associating a FortiToken with an account. The accounts can be local user or administrator accounts.

NOTE: You cannot delete a FortiToken from the FortiToken list page if it is associated with a user account.

To add a FortiToken to a local user account using web-based manager:

1. Ensure that your FortiToken serial number has been added to the FortiProxy unit successfully, and its status is *Available*.
2. Go to *User & Authentication > User Definition*, select the user account, and then click *Edit User*.
3. Enter the user’s *Email Address*.
4. Enable Two-factor Authentication.
5. Select the user's FortiToken serial number from the *Token* list.
6. Click *OK*.

For mobile token, select *Send Activation Code* to be sent to the email address configured previously. The user will use this code to activate the mobile token. An *Email Service* has to be set under *System > Advanced* to send the activation code.

To add a FortiToken to a local user account using the CLI:

```
config user local
   edit <username>
      set type password
      set passwd "myPassword"
      set two-factor fortitoken
      set fortitoken <serial_number>
      set email-to "username@example.com"
      set status enable
   next
end
```

To add a FortiToken to an administrator account using the web-based manager:

1. Ensure that your FortiToken serial number has been added to the FortiProxy unit successfully, and its status is *Available*.
2. Go to *System* > *Administrators* , select *admin*, and then click *Edit*. This account is assumed to be configured except for two-factor authentication.
3. Enter admin's *Email Address*.
4. Enable *Two-factor Authentication*.
5. Select the user's FortiToken serial number from the *Token* list.
6. Click *OK*.

For mobile token, select *Send Activation Code* to be sent to the email address configured previously. The admin will use this code to activate the mobile token. An *Email Service* has to be set under *System* > *Advanced* to send the activation code.

To add a FortiToken to an administrator account using the CLI:

```
config system admin
   edit <username>
      set password "myPassword"
      set two-factor fortitoken
      set fortitoken <serial_number>
      set email-to "username@example.com"
   next
end
```

The `fortitoken` keyword is not visible until `fortitoken` is selected for the `two-factor` option.

Before a new FortiToken can be used, you might need to synchronize it due to clock drift.

FortiToken maintenance

After FortiTokens are entered into the FortiProxy unit, there are only two tasks to maintain them—changing the status and synchronizing them if they drift.

To change the status of a FortiToken between Activated and Locked using the CLI:

```
config user fortitoken
   edit <token_serial_num>
      set status lock
   next
end
```

Any user attempting to login using this FortiToken will not be able to authenticate.

To list the drift on all FortiTokens configured on this FortiProxy unit using the CLI:

```
# diag fortitoken info
FORTITOKEN DRIFT STATUS
FTK2000BHV1KRZCC 0 token already activated, and seed won't be returned
FTK2001C5YCRRVEE 0 token already activated, and seed won't be returned
FTKMOB4B94972FBA 0 provisioned
FTKMOB4BA4BE9B84 0 new
Total activated token: 0
Total global activated token: 0
Token server status: reachable
```

This command lists the serial number and drift for each FortiToken configured on this FortiProxy unit. This command is useful to check if it is necessary to synchronize the FortiProxy unit with any particular FortiTokens.

System

The *System* menu provides submenus for three areas: system administration, system configuration, and certificates.

System administration covers the following topics:

- Administrators on page 445
- Admin Profiles on page 451
- Firmware on page 454
- Settings on page 455

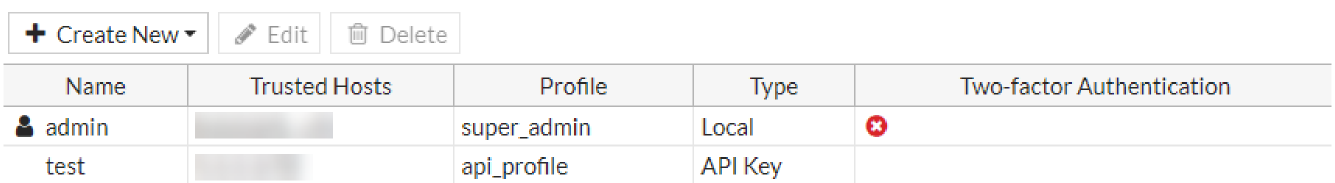
System configuration covers the following topics:

- HA on page 469
- SNMP on page 481
- Replacement Messages on page 492
- Replacement Message Groups on page 500
- FortiGuard on page 502
- Feature Visibility on page 506

Certificates on page 508 covers generating, editing, deleting, importing, viewing, and downloading certificates.

Administrators

Administrators are configured in *System > Administrators*. There is already a default administrator account on the unit named `admin` that uses the super_admin administrator profile.



Name	Trusted Hosts	Profile	Type	Two-factor Authentication
admin		super_admin	Local	
test		api_profile	API Key	

Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

You need to use the default `admin` account, an account with the super_admin admin profile, or an administrator with read-write access control to add new administrator accounts and control their permission levels. If you log in with an administrator account that does not have the super_admin admin profile, the administrators list shows only the administrators for the current virtual domain.

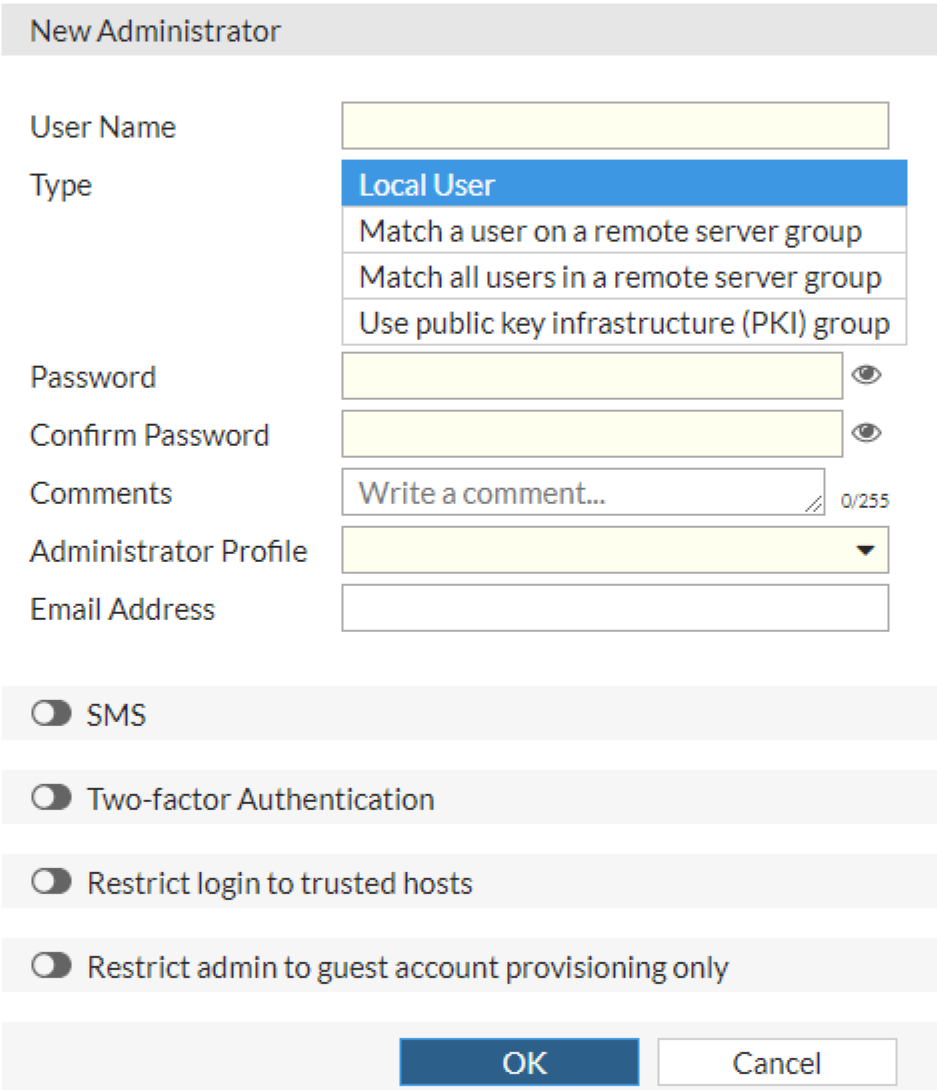
The *Administrators* page lists the default super_admin administrator account, and all administrator accounts that you have created. The following options are available:

Create New	Creates a new administrator account. See Create or edit an administrator on page 446 or Create or edit a REST API administrator on page 449.

Edit	Modifies settings within an administrator's account. When you select *Edit*, the *Edit Administrator* page opens. See Create or edit an administrator on page 446 or Create or edit a REST API administrator on page 449.
Delete	Remove an administrator account. You cannot delete the original *admin* account until you create another user with the super_admin profile, log out of the *admin* account, and log in with the alternate user that has the super_admin profile. To remove multiple administrator accounts, select multiple rows in the list by holding down the Ctrl or Shift keys and then select *Delete*.
Name	The login name for an administrator account.
Trusted Hosts	The IP address and netmask of trusted hosts from which the administrator can log in.
Profile	The admin profile for the administrator.
Type	The type of authentication for this administrator, one of the following: • *Local*: Authentication of an account with a local password stored on the FortiProxy unit. • *Remote*: Authentication of a specific account on a RADIUS, Lightweight Directory Access Protocol (LDAP), or Terminal Access Controller Access-Control System (TACACS+) server. • *Remote+Wildcard*: Authentication of any account on an LDAP, RADIUS, or TACACS+ server. • *PKI*: PKI-based certificate authentication of an account.
Two-factor Authentication	FortiProxy supports FortiToken and FortiToken Mobile. FortiToken Mobile is a Fortinet application that enables you to generate One Time Passwords (OTPs) on a mobile device for FortiProxy two-factor authentication. The user's mobile device and the FortiProxy unit must be connected to the Internet to activate FortiToken mobile. Once activated, users can generate OTPs on their mobile device without having network access. FortiToken Mobile is available for iOS and Android devices from their respective Application stores. No cellular network is required for activation.
Comments	A description of the administrator account.

Create or edit an administrator

Select *Create New > Administrator* to open the *New Administrator* page. It provides settings for configuring an administrator account. When you are configuring an administrator account, you can enable authentication for an admin from an LDAP, RADIUS, or local server.



Select an administrator and then click *Edit* to open the Edit Administrator page.

Configure the following settings in the New Administrator page or Edit Administrator page and then click *OK*:

User Name	Enter the login name for the administrator account. The name of the administrator should not contain the characters `<`, `>`, `(`, `)`, `#`, `"`, or `'`. Using these characters in the administrator account name can result in a cross-site scripting (XSS) vulnerability.
Type	Select the type of administrator account. • *Local User*—Select to create a local administrator account. • *Match a user on a remote server group*—Select to authenticate the administrator using a RADIUS, LDAP, or TACACS+ server. Server authentication for administrators must be configured first. • *Match all users on a remote server group*—Select to authenticate all users using a specific RADIUS, LDAP, or TACACS+ server. Server authentication for administrators must be configured first.

	• *Use public key infrastructure (PKI) group*—Select to enable certificate-based authentication for the administrator. Only one administrator can be logged in with PKI authentication enabled.
Password	Enter a password for the administrator account. For improved security, the password should be at least 6 characters long. Select the eye icon to view the password. This option is only available if *Type* is *Local User*.
Confirm Password	Type the password for the administrator account a second time to confirm that you have typed it correctly. Select the eye icon to view the password. This option is not available if *Type* is *Use public key infrastructure (PKI) group*.
Backup Password	Enter a backup password for the administrator account. For improved security, the password should be at least 6 characters long. Select the eye icon to view the password. This option is only available if *Type* is *Match a user on a remote server group* or *Match all users in a remote server group*.
Comments	Optionally, enter comments about the administrator account.
Administrator Profile	Select an administrator profile to use for the new administrator. To create an administrator profile, see Create or edit an administrator profile on page 452.
Email Address	If email is used for two-factor authentication, provide the email address at which the user will receive token password codes.
Remote User Group	Select the administrator user group that includes the remote server/PKI (peer) users as members of the *Remote User Group*. The administrator user group cannot be deleted after the group is selected for authentication. This option is only available if *Type* is *Match a user on a remote server group* or *Match all users in a remote server group*.
PKI Group	Select to allow all accounts on the RADIUS, LDAP, or TACACS+ server to be administrators. This option is only available if *Type* is *Use public key infrastructure (PKI) group*.
SMS	If SMS is used for two-factor authentication, enable *SMS* and provide the country dial code and SMS cell phone number at which the user will receive token password codes.
Restrict login to trusted hosts	Enable to restrict this administrator login to specific trusted hosts and then enter the IPv4 or IPv6 addresses and netmasks of the trusted hosts. You can specify up to 10 trusted hosts and 10 IPv6 trusted hosts.
Restrict admin to guest account provisioning only	Enable to create a guest management administrator and then select the name of the guest group.

Regular (password) authentication for administrators

You can use a password stored on the local unit to authenticate an administrator. When you select *Local User* for *Type*, you will see *Local* as the entry in the *Type* column when you view the list of administrators.

Using trusted hosts

Setting trusted hosts for all of your administrators increases the security of your network by further restricting administrative access. In addition to knowing the password, an administrator can connect only through the subnet or subnets that you specify. You can even restrict an administrator to a single IP address if you define only one trusted host IP address with a netmask of 255.255.255.255.

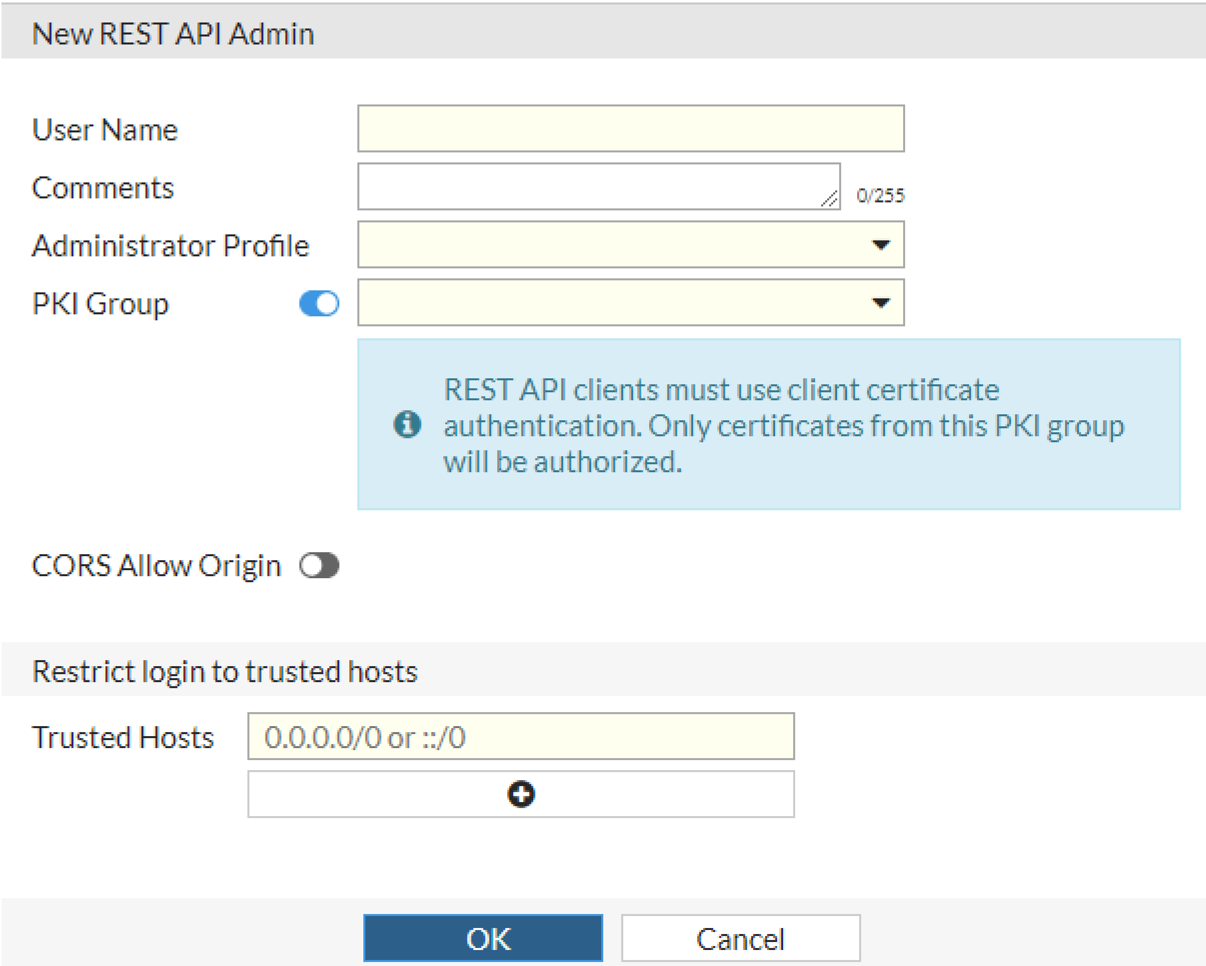
When you set trusted hosts for all administrators, the unit does not respond to administrative access attempts from any other hosts. This provides the highest security. If you leave even one administrator unrestricted, the unit accepts administrative access attempts on any interface that has administrative access enabled, potentially exposing the unit to attempts to gain unauthorized access.

The trusted hosts you define apply to the GUI, Ping, SNMP, and the CLI when accessed through Telnet or SSH. CLI access through the console port is not affected.

The trusted host addresses all default to 0.0.0.0/0.0.0.0. If you set one of the zero addresses to a nonzero address, the other zero addresses will be ignored. The only way to use a wildcard entry is to leave the trusted hosts at 0.0.0.0/0.0.0.0. However, this configuration is less secure.

Create or edit a REST API administrator

Select *Create New > REST API Admin* to open the *New REST API Admin* page. It provides settings for configuring a REST API administrator account.



Select a REST API administrator and then click *Edit* to open the Edit REST API Admin page.

Configure the following settings in the New REST API Admin page or Edit REST API Admin page and then click *OK*:

User Name	Enter the login name for the administrator account. The name of the administrator should not contain the characters `<`, `>`, `(`, `)`, `#`, `"`, or `'`. Using these characters in the administrator account name can result in a cross-site scripting (XSS) vulnerability.
Comments	Optionally, enter comments about the administrator account.
Administrator Profile	Select an administrator profile to use for the new administrator. To create an administrator profile, see Create or edit an administrator profile on page 452.
PKI Group	Enable this option for REST API clients and then select which PKI group to accept.
CORS Allow Origin	Enable this option for cross-origin resource sharing (CORS) and then specify the URL that can access the REST API.
Trusted Hosts	Enter the trusted hosts allowed to log in to the REST API.

Using trusted hosts

Setting trusted hosts for all of your administrators increases the security of your network by further restricting administrative access. In addition to knowing the password, an administrator can connect only through the subnet or subnets that you specify. You can even restrict an administrator to a single IP address if you define only one trusted host IP address with a netmask of 255.255.255.255.

When you set trusted hosts for all administrators, the unit does not respond to administrative access attempts from any other hosts. This provides the highest security. If you leave even one administrator unrestricted, the unit accepts administrative access attempts on any interface that has administrative access enabled, potentially exposing the unit to attempts to gain unauthorized access.

The trusted hosts you define apply to the GUI, Ping, SNMP, and the CLI when accessed through Telnet or SSH. CLI access through the console port is not affected.

The trusted host addresses all default to 0.0.0.0/0.0.0.0. If you set one of the zero addresses to a nonzero address, the other zero addresses will be ignored. The only way to use a wildcard entry is to leave the trusted hosts at 0.0.0.0/0.0.0.0. However, this configuration is less secure.

Admin Profiles

Each administrator account belongs to an admin profile. The admin profile separates FortiProxy features into access control categories for which an administrator with read-write access can enable none (deny), read-only, or read-write access.

Read-only access for a GUI page enables the administrator to view that page. However, the administrator needs write access to change the settings on the page.

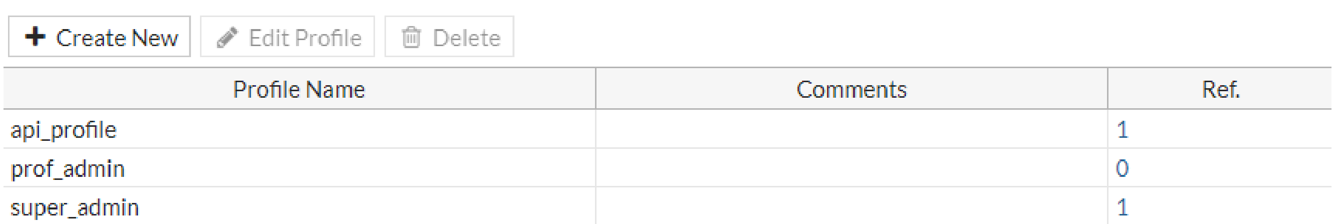
The admin profile has a similar effect on administrator access to CLI commands. You can access `get` and `show` commands with *Read Only* access, but access to `config` commands requires *Read-Write* access.

When an administrator has read-only access to a feature, the administrator can access the GUI page for that feature but cannot make changes to the configuration. There are no *Create* or *Apply* buttons, and lists display only the *View* icon instead of icons for *Edit*, *Delete*, or other modification commands.

You need to use the admin account or an account with read-write access to create or edit admin profiles.

The *Admin Profile* page lists all administration profiles that you created as well as the default admin profiles. On this page, you can edit, delete, or create an admin profile.

To view administrator profiles, go to *System > Admin Profiles*.



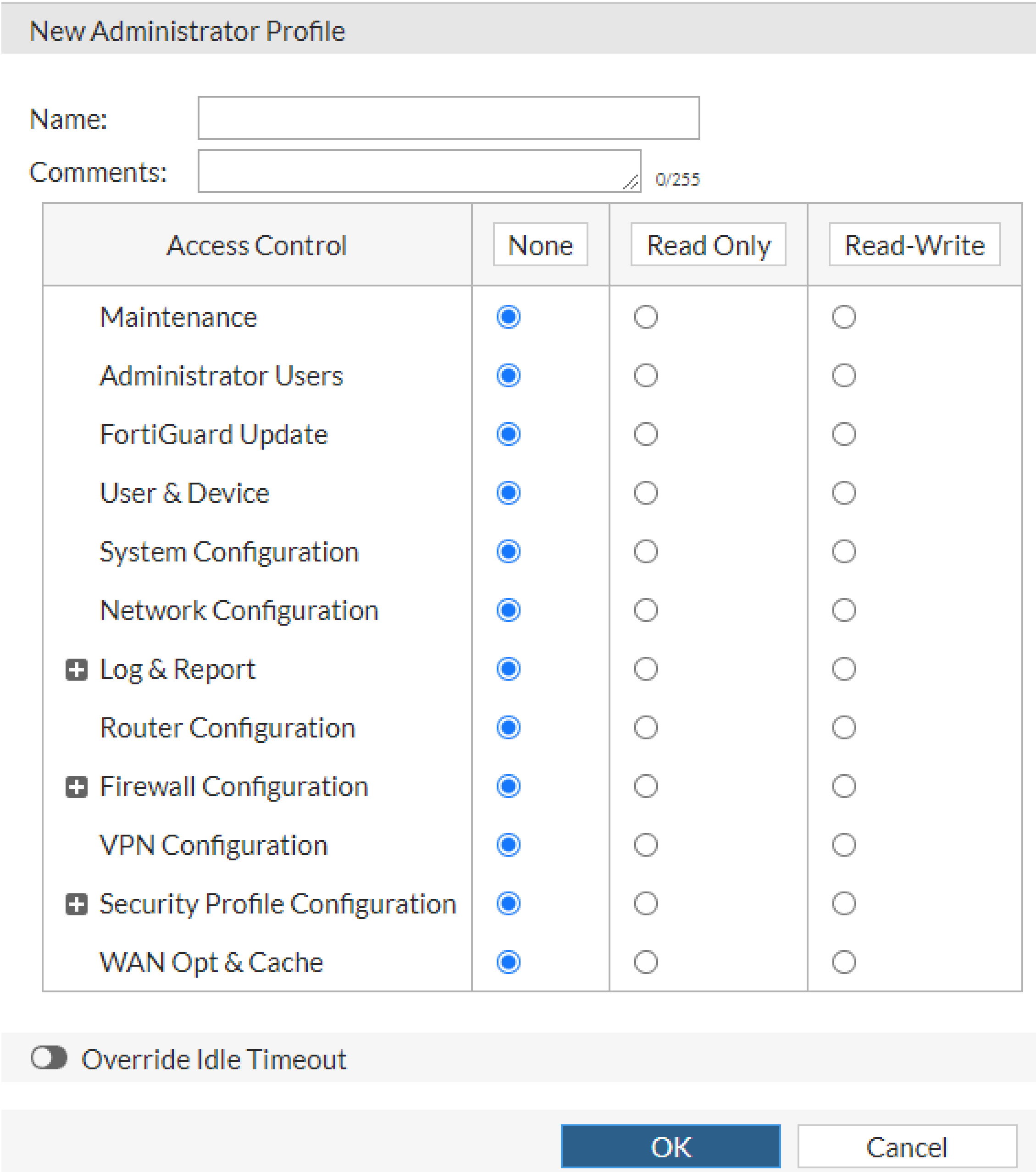
Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Creates an administrator profile. See Create or edit an administrator profile on page 452.
Edit Profile	Modifies the selected administrator profile. When you click *Edit Profile*, the Edit Administrator Profile page opens. See Create or edit an administrator profile on page 452. **NOTE:** You cannot edit the super_admin profile.
Delete	Removes the admin profile from the list on the page. You cannot delete an admin profile that has administrators assigned to it. To remove multiple admin profiles, select multiple rows in the list by holding down the Ctrl or Shift keys and then select *Delete*.
Profile Name	The name of the admin profile.
Comments	Comments about the admin profile.
Ref.	Displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in Ref.; the *Object Usage* window opens and displays the various locations of the referenced object.

Create or edit an administrator profile

Select *Create New* to open the *New Administrator Profile* page. It provides settings for configuring an administrator profile.



Select an administrator profile and then click *Edit Profile* to open the *Edit Administrator Profile* page.

Configure the following settings in the New Administrator Profile page or Edit Administrator Profile page and then click *OK*.

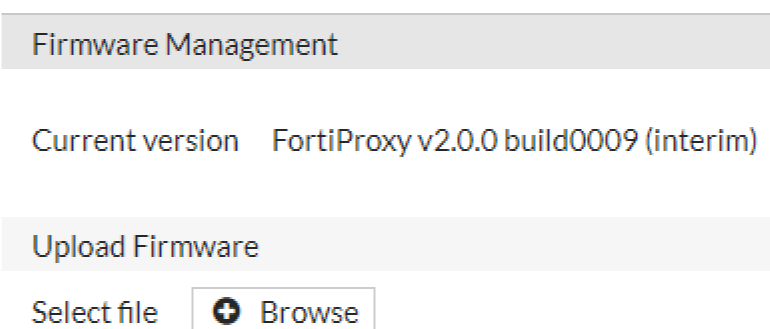
NOTE: You cannot edit the super_admin profile.

Name	Enter a name for the new administrator profile. After an administrator profile is created, you cannot change the name.
Comments	Optionally, add comments about the administrator profile.
Access Control	List of the items that can customize access control settings if configured.

None	Deny access for the *Access Control* category.
Read Only	Enable read-only access for the *Access Control* category.
Read-Write	Allow read-write access for the *Access Control* category.
Access Control (categories)	Make specific access control selections as required. • Maintenance • Administrator Users • FortiGuard Update • User & Device • System Configuration • Network Configuration • Log & Report • Router Configuration • Firewall Configuration • VPN Configuration • Security Profile Configuration • WAN Opt & Cache
Override Idle Timeout	Enable to change how many minutes the FortiProxy unit is idle before the session closes.
Timeout	Select *Idle Countdown* to specify the number of minutes that the system is idle before the session closes. Select *Never Timeout* to prevent the FortiProxy unit from closing idle sessions.
Idle	Enter the number of minutes that the FortiProxy unit is idle before the session closes. The default is 10 minutes.

Firmware

Go to *System > Firmware* to check the current firmware version and to upload firmware from your computer or from FortiGuard.



To upload a new firmware image from your computer:

1. Go to *System* > *Firmware* and select *Browse*.
2. Select the file on your PC and select *Open*.
3. Select *Backup Config and Upgrade*. Your system will reboot.

Settings

Use the system settings to configure general settings for administration access, password policies, system time settings, and display settings.

Go to *System* > *Settings* to configure system settings.

Configure the following settings and then select *Apply*:

System Settings	
Host name	The host name of the FortiProxy unit. The only administrators that can change a host name are administrators whose admin profiles permit system configuration write access. If the FortiProxy unit is part of an HA cluster, you should use a unique host name to distinguish the FortiProxy unit from others in the cluster.
System Time	
Time Zone	Select the time zone of your FortiProxy unit.
Set Time	Select either *NTP*, *PTP*, or *Manual settings*. • *NTP*: To use an NTP server other than FortiGuard, the CLI must be used. In the *Sync interval* field, enter how often, in minutes, that the device synchronizes its time with the NTP server. • *PTP*: • Set the *Mode* to *Multicast* or *Hybrid*. • Select the *Delay mechanism*: *E2E* or *P2P*. • Set the *Request interval*, in seconds. • Select the *Interface*. • *Manual settings*: Manually enter the *Date*, and *Time*.
Setup device as local NTP server	Enable to configure the FortiProxy as a local NTP server. This option is not available if *Set Time* is *PTP*. In the *Listen on Interfaces* field, set the interface or interfaces that the FortiProxy will listen for NTP requests on.
Administration Settings	
HTTP port	Enter the TCP port to be used for administrative HTTP access. The default is 80.
Redirect to HTTPS	Enable *Redirect to HTTPS* to force redirection from HTTP to HTTPS.

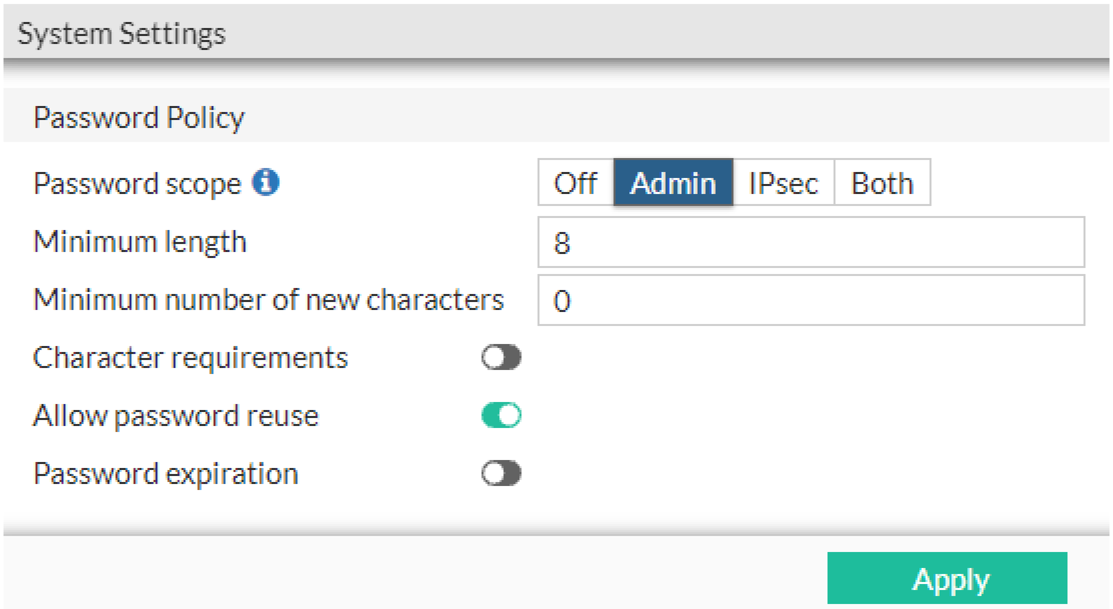
HTTPS port	Enter the TCP port to be used for administrative HTTPS access. The default is 443.
HTTPS server certificate	Select *Fortinet_Factory* or search for a certificate.
SSH port	Enter the TCP port to be used for administrative SSH access. The default is 22.
Telnet port	Enter the TCP port to be used for administrative Telnet access. The default is 23.
Idle timeout	Change the time after which the GUI logs out idle system administration settings, from 1 to 480 minutes.
ACME interface	Select the interface that the ACME client will listen to for challenges to provision and renew certificates.
Allow concurrent sessions	Concurrent administrator sessions occur when multiple people concurrently access the FortiProxy unit using the same administrator account. This behavior is allowed by default.
Password Policy	
Password Scope	Select *Admin*, *IPsec*, or *Both* to change the policy for the administrator password. Select *Off* to apply no policy for the administrator password
Minimum Length	If you select *Admin*, *IPsec*, or *Both*, set the minimum acceptable length for passwords, from 8 to 128 characters.
Character requirements	If you select *Admin*, *IPsec*, or *Both*, select to enable special character types, upper or lower case letters, or numbers. Enter information for one or all of the following. Each selected type must occur at least once in the password. • *Upper case*—A, B, C, ... Z • *Lower case*—a, b, c, ... z • *Numbers (0-9)*—0, 1, 2, ... 9 • *Special*—@, ?, #, ... %
Allow password reuse	If you select *Admin*, you can select this option to allow passwords to be reused.
Password expiration	If you select *Admin*, *IPsec*, or *Both*, you can require administrators to change the password after a specified number of days. Enter the number of days in the field. The default is 90 days.
View Settings	
Language	The language the GUI uses: *English*, *French*, *Spanish*, *Portuguese*, *Japanese*, *Traditional Chinese*, *Simplified Chinese*, or *Korean*. You should select the language that the operating system of the management computer uses.
Date/Time display	Display the time in either the *FortiProxy timezone* or the *Browser timezone*.
System Operation Settings	
Virtual Domains	Enable or disable VDOMs.

Defining the password policy with a minimum character change

Administrators can 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
```

Trusted platform module support

On supported FortiProxy hardware devices, the Trusted Platform Module (TPM) can be used to protect your password and key against malicious software and phishing attacks. The dedicated module hardens the FortiProxy by generating, storing, and authenticating cryptographic keys. To help prevent tampering, the chip is soldered on the motherboard to reduce the risk of data transaction interceptions from attackers.

By default, the TPM is disabled. To enable it, you must set the 32 hexadecimal digit master-encryption-password which encrypts sensitive data on the FortiProxy using AES128-CBC. With the password, TPM generates a 2048-bit primary key to secure the master-encryption-password through RSA-2048 encryption. The master-encryption-password protects the data. The primary key protects the master-encryption-password.

The TPM module does not encrypt the disk drive of eligible FortiProxy units.

The primary key binds the encrypted configuration file to a specific FortiProxy unit and never leaves the TPM. When backing up the configuration, the TPM uses the primary key to encrypt the master-encryption-password in the configuration file. When restoring a configuration that includes a TPM protected master-encryption-password:

- If TPM is disabled, then the configuration cannot be restored.
- If TPM is enabled but has a different master-encryption-password than the configuration file, then the configuration cannot be restored.
- If TPM is enabled and the master-encryption-password is the same in the configuration file, then the configuration can be restored.

For information on backing up and restoring the configuration, see Automatic backup to an FTP or TFTP server on page 608.

Passwords and keys that can be encrypted by the master-encryption-key include:

- Admin password
- Alert email user's password
- BGP and other routing related configurations
- External resource
- FortiGuard proxy password
- FortiToken/FortiToken Mobile’s seed
- HA password
- IPsec pre-shared key
- Link Monitor, server side password
- Local certificate's private key
- Local, LDAP. RADIUS, FSSO, and other user category related passwords
- Modem/PPPoE
- NST password
- NTP Password
- SDN connector, server side password
- SNMP
- Wireless Security related password

In HA configurations, each cluster member must use the same master-encryption-key so that the HA cluster can form and its members can synchronize their configurations.

To check if your FortiProxy device has a TPM:

Verify all the following commands exist. Otherwise, the platform does not support it.

```
# diagnose hardware test info
List of test cases:
    bios: sysid
```

```
    bios: checksum
    bios: license
    bios: detect

# diagnose hardware deviceinfo tpm
TPM capability information of fixed properties:
=========================================================
TPM_PT_FAMILY_INDICATOR: 2.0
TPM_PT_LEVEL: 0
TPM_PT_REVISION: 138
TPM_PT_DAY_OF_YEAR: 8
TPM_PT_YEAR: 2018
TPM_PT_MANUFACTURER: NTC
# diagnose hardware test tpm
=========== Fortinet Hardware Test Report ===================
TPM
TPM Device Detection......................................... PASS
================= Fortinet Hardware Test PASSED ==============
# diagnose tpm
get-property Get TPM properties. [Take 0-1 arg(s)]
get-var-property Get TPM var properties.
read-clock Read TPM internal clock.
shutdown-prepare Prepare for TPM power cycle.
selftest Perform self tests.
generate-random-number Generate a 4-byte random number
SHA-1 HASH a sequence of num with SHA-1 algo
SHA-256 HASH a sequence of num with SHA-256 algo
```

To enable TPM and input the master-encryption-password:

```
config system global
    set private-data-encryption enable
end
Please type your private data encryption key (32 hexadecimal numbers):
********************************
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
********************************
Your private data encryption key is accepted.
```

VDOM

Virtual Domains (VDOMs) are used to divide a single FortiProxy into two or more virtual units that function independently. VDOMs can provide separate firewall policies and security profiles. In NAT mode, they provide separate routing configurations. When multi VDOM mode is enabled, the default VDOM is the *root* VDOM, and it cannot be deleted.

Multiple VDOMs allow users to combine NAT and transparent mode on a single FortiProxy; VDOMs can be independently configured to operate in NAT or transparent mode. In transparent mode, it is recommended to configure a dedicated management interface when out-of-band management is required. See Transparent mode management on page 467.

By default, most FortiProxy units support 5 VDOMs.

Global settings are configured outside of a VDOM. They effect the entire FortiProxy, and include settings such as interfaces, firmware, HA, and so on. Global settings should only be changed by top level administrators. Both VDOM specific and global security profiles can be created. Global security profiles are configured in the global VDOM, and can be used by any VDOM and have *g-* appended to their names to differentiate them from VDOM specific profiles.

Administrative users can be configured to have global access, or access to specific VDOMs. See Administrators on page 445 for more information about administrators.

Global administrators have complete visibility and access because the scope of their role is to manage the entire physical FortiProxy device. To create a global administrator that has access to all VDOMs and access to global settings, it must be created at the global level and must use the *super_admin* administrator profile. See Create Global VDOM administrators on page 462 for configuration details.

Per-VDOM administrators are unable to view global settings or VDOMs that are not assigned to them because the scope of their role is restricted to managing specific VDOMs only. They can only access the FortiProxy through interfaces that are assigned to the VDOM that they are assigned to. The interface must also be configured to allow management access. They can also connect to the FortiProxy using the console port. See Create per-VDOM administrators on page 462 for configuration details.

Configuration

VDOMs can be configured in the GUI and the CLI.

The following topics provide information on general VDOM configurations:

- Enable multi VDOM mode on page 460
- Disable multi VDOM mode on page 461
- Create VDOMs on page 461
- Delete VDOMs on page 462
- Create Global VDOM administrators on page 462
- Create per-VDOM administrators on page 462
- Assign interfaces to a VDOM on page 463
- Global and per-VDOM resources on page 464
- Inter-VDOM routing on page 466

To ensure that no VDOMs are accidentally configured in the CLI, prompts can be enabled. These prompts will display to ask for confirmation that the VDOM is meant to be configured in the CLI.

To configure confirmation prompts:

```
config system global
    set edit-vdom-prompt enable
end
```

Enable multi VDOM mode

To enable VDOMs in the GUI:

1. Go to *System > Settings*.
2. In the *System Operation Settings* sections, enable *Virtual Domains*.

3. Click *OK*.
   You will be logged out of the device when VDOM mode is enabled.

To enable VDOMs in the CLI:

```
config system global
    set vdom-mode multi-vdom
end
```

You will be logged out of the device when VDOM mode is enabled.

Disable multi VDOM mode

All non-root VDOMs must be deleted before multi VDOM mode can be disabled.

To disable VDOMs in the GUI:

1. In the Global VDOM, go to *System* > *Settings*.
2. Disable *Virtual Domains*.
3. Click *Apply*.

To disable VDOMs in the CLI:

```
config global
    config system global
        set vdom-mode no-vdom
    end
end
```

Create VDOMs

To create VDOMs in the GUI:

1. In the Global VDOM, go to *System* > *VDOM*.
2. Click *Create New*.
3. In the *Virtual Domain* field, enter a name for the VDOM.
4. Optionally, enter a comment describing the VDOM.
5. Click *OK*.

To create VDOMs in the CLI:

```
config global
    config vdom
        edit <vdom_a>
        next
        edit <vdom_b>
        next
    end
end
```

Delete VDOMs

The root VDOM and VDOMs that are referenced in the current configuration cannot be deleted.

To delete a VDOM in the GUI:

1. In the Global VDOM, go to *System* > *VDOM*.
2. Select the VDOM that you need delete.
3. Click *Delete*.
4. Click *OK*.

To delete a VDOM in the CLI:

```
config vdom
    delete <vdom>
end
```

Create Global VDOM administrators

Global administrators have complete visibility and access because the scope of their role is to manage the entire physical FortiProxy device. When global administrators log into the GUI, from the *VDOM: Global* view they will see all pages for global settings shared between VDOMs, and VDOM-specific settings.

To create a global administrator that has access to all VDOMs and access to global settings, it must be created at the global level and must use the *super_admin* administrator profile.

To create a Global VDOM administrator in the GUI:

1. In the Global VDOM, go to *System* > *Administrators* and click *Create New* > *Administrator*.
2. Fill in the required information, setting the *Type* as *Local User*.
3. Set Administrator profile to *super_admin* or *super_admin_readonly*.
4. Click *OK*.

To create a Global VDOM administrator using the CLI:

```
config global
    config system admin
        edit <name>
            set accprofile "super_admin"
        next
    end
end
```

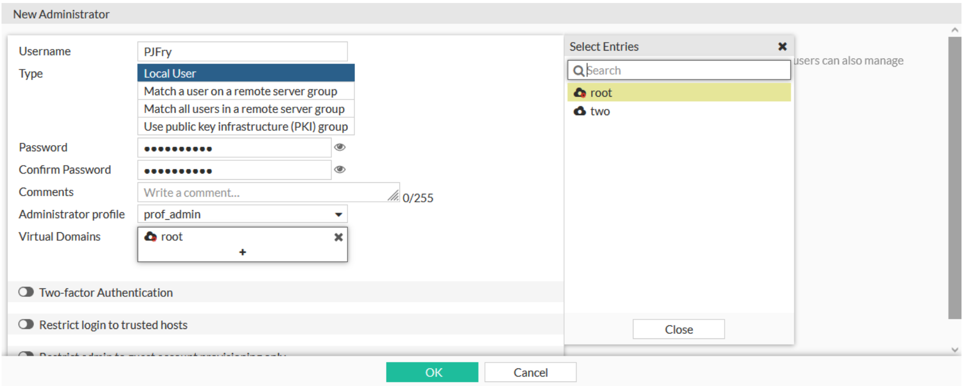
Create per-VDOM administrators

Per-VDOM administrators can be created that can access only the administrative or traffic VDOM. These administrators must use the *prof_admin*, *admin_no_access*, or a custom administrator profile.

To assign an administrator to multiple VDOMs, they must be created at the global level. When creating an administrator at the VDOM level, the *super_admin* administrator profile cannot be used.

To create a per-VDOM administrator in the GUI:

1. In the Global VDOM, go to *System > Administrators* and click *Create New > Administrator*.
2. Fill in the required information, setting the *Type* as *Local User*.
3. In the *Virtual Domains* field, add the VDOMs that the administrator will be assigned to.



4. Click *OK*.

To create a per-VDOM administrator using the CLI:

```
config global
    config system admin
        edit <name>
            set accprofile <profile>
            set vdom <vdom(s)>
            ...
        next
    end
end
```

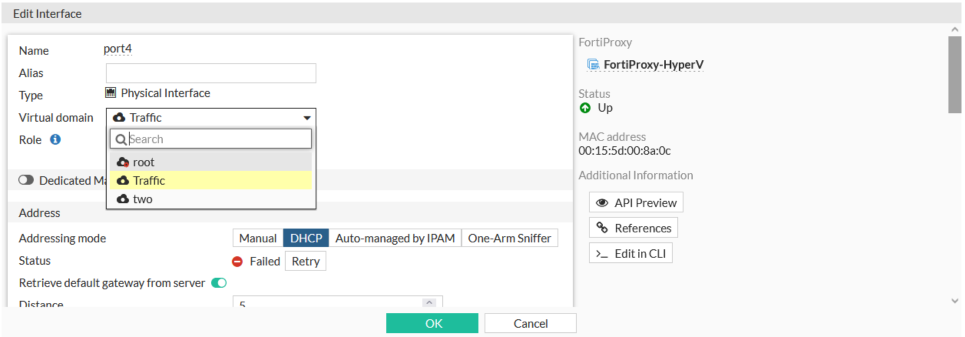
Assign interfaces to a VDOM

An interface can only be assigned to one of the VDOMs. An interface cannot be moved if it is referenced in an existing configuration. By default, all interfaces belong to the root VDOM.

In the GUI, the interface list *Ref.* column shows if the interface is referenced in an existing configuration, and allows you to quickly access and edit those references.

To assign an interface to a VDOM in the GUI:

1. In the Global VDOM, go to *Network > Interfaces*.
2. Select the interface that will be assigned to a VDOM and click *Edit*.
3. Select the VDOM that the interface will be assigned to from the *Virtual Domain* list.



4. Click *OK*.

To assign an interface to a VDOM using the CLI:

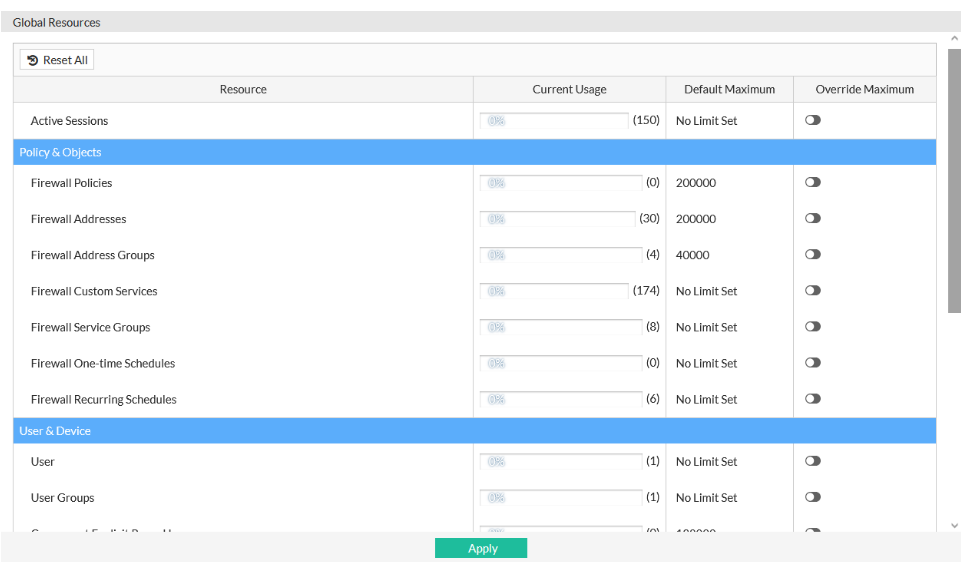
```
config global
    config system interface
        edit <interface>
            set vdom <vdom>
        next
    end
end
```

Global and per-VDOM resources

Global resources apply to resources that are shared by the whole FortiProxy, while per-VDOM resources are specific to each VDOM.

To configure global resources in the GUI:

1. In the Global VDOM, go to *System > Global Resources*.
2. Enable the resource's override in the *Override Maximum* column, then enter the override value.



3. Click *Apply*.

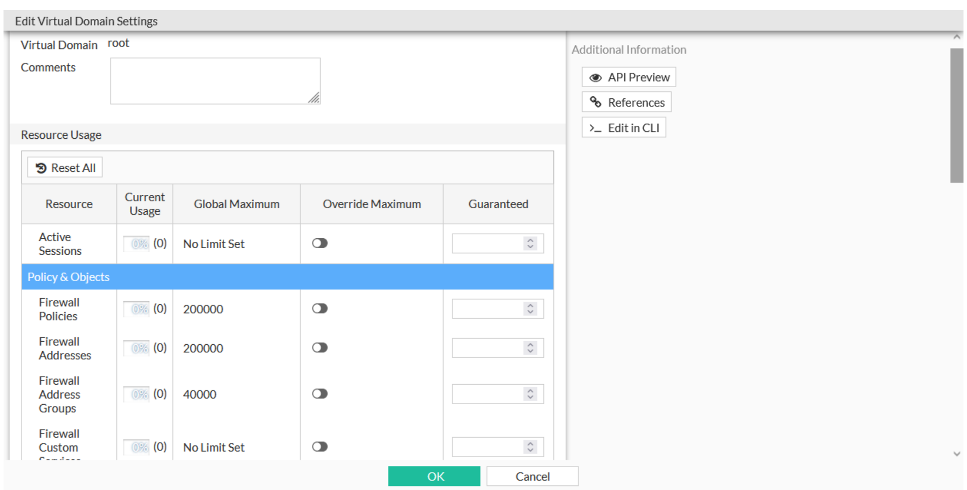
   To reset all of the override values, click *Reset All*.

To configure global resources in the CLI:

```
config global
    config system resource-limits
        set log-disk-quota <integer>
        set session <integer>
        set ipsec-phase1-interface <integer>
        set ipsec-phase2-interface <integer>
        set firewall-policy <integer>
        set firewall-address <integer>
        set firewall-addrgrp <integer>
        set custom-service <integer>
        set service-group <integer>
        set onetime-schedule <integer>
        set recurring-schedule <integer>
        set user <integer>
        set user-group <integer>
        set sslvpn <integer>
        set proxy <integer>
        set log-disk-quota <integer>
    end
end
```

To configure per-VDOM resources in the GUI:

1. In the *Global* VDOM, go to *System > VDOM*.
2. Select the VDOM whose resources need to be configured and click *Edit*.
3. Enable the resource's override in the *Override Maximum* column, then enter the override value.
4. Optionally, enter a value in the *Guaranteed* column.



5. Click *OK*.

   To reset all of the override values, click *Reset All*.

To configure per-VDOM resources in the CLI:

```
config vdom
    edit <vdom>
        config system vdom-property
```

```
            edit <vdom>
                set session <max-number> [guaranteed-number]
                set ipsec-phase1-interface <max-number> [guaranteed-number]
                set ipsec-phase2-interface <max-number> [guaranteed-number]
                set firewall-policy <max-number> [guaranteed-number]
                set firewall-address <max-number> [guaranteed-number]
                set firewall-addrgrp <max-number> [guaranteed-number]
                set custom-service <max-number> [guaranteed-number]
                set service-group <max-number> [guaranteed-number]
                set onetime-schedule <max-number> [guaranteed-number]
                set recurring-schedule <max-number> [guaranteed-number]
                set user <max-number> [guaranteed-number]
                set user-group <max-number> [guaranteed-number]
                set sslvpn <max-number> [guaranteed-number]
                set proxy <max-number> [guaranteed-number]
                set log-disk-quota <integer>
            next
        end
    next
end
```

Inter-VDOM routing

VDOM links allow VDOMs to communicate internally without using additional physical interfaces. VDOM link does not support traffic offload.

A VDOM link cannot share the same name as a VDOM.

To configure a VDOM link in the GUI:

1. In the *Global* VDOM, go to *Network > Interfaces*.
2. Click *Create New > VDOM Link*.
3. Configure the fields, including the *Name*, *Virtual Domain*, IP information, *Administrative Access*, and so on, then click *OK*.

To configure a VDOM link in the CLI:

```
config global
    config system vdom-link
        edit "<vdom-link-name>"
            set type {ppp | ethernet}
        next
    end
    config system interface
        edit "<vdom-link-name0>"
            set vdom "<VDOM Name>"
            set type vdom-link
        next
        edit "<vdom-link-name1>"
            set vdom "<VDOM Name>"
            set type vdom-link
```

```
        next
    end
end
```

To delete a VDOM link in the GUI:

1. In the *Global* VDOM, go to *Network* > *Interfaces*.
2. Select a *VDOM Link* and click *Delete*.

To delete a VDOM link in the CLI:

```
config global
    config system vdom-link
        delete <VDOM-LINK-Name>
    end
end
```

Transparent mode management

In transparent mode, you can assign a single IP address to the FortiProxy for remote management access and configure multiple static routes for in-band management. When out-of-band management is required, it is recommended to configure a dedicated management interface.

The management interface supports only the following protocols for outgoing traffic: SNMP, NTP, LOG, Radius, FTP, TFTP, Telnet. To allow the management interface to handle outgoing traffic with an unsupported protocol, you must configure multiple VDOM on page 459s and dedicate the root VDOM to management traffic, which means assigning the management interface to the root VDOM while keeping all other interfaces for in-band traffic to user VDOMs.

In-band management

The management IP address is bound to all ports or VLANs that belong to the same bridge group. Remote access services are subject to the same rules as in NAT mode, and must be enabled on each interface.

To configure the management IP address:

```
config system settings
    set opmode transparent
    set manageip 10.1.1.100/255.255.255.0
end
config router static
    edit 1
        set gateway 10.1.1.254
    next
end
config system interface
    edit port1
        set allowaccess ping ssh https snmp
```

```
    next
end
```

To add a second IP address for management and additional default routes:

```
config system settings
    set manageip 192.168.182.136/255.255.254.0 10.1.1.1/255.255.255.0
end
config router static
    edit 1
        set gateway 192.168.183.254
    next
    edit 2
        set gateway 10.1.1.254
    next
end
```

Out-of-band management

When an interface is dedicated to management purposes only, it is removed from default switch group and becomes an isolated routing port. When the FortiProxy is running in transparent mode, it is recommended that one physical interface be kept as an out-of-band management interface to avoid layer 2 loops and allow for more routing flexibility.

The management interface must have IP connectivity to the management and monitoring network subnets.

To dedicate an interface to management:

1. Dedicate the interface to management:

```
config system interface
    edit port2
        set dedicated-to management
        set ip 192.168.1.10 255.255.255.0
        set allowaccess ping ssh https snmp
    next
end
```

2. Configure static routed to the management and monitoring subnets:

```
config router static
    edit 1
        set gateway 192.168.183.254
    next
    edit 2
        set dst 172.18.1.0 255.255.255.0
        set gateway 192.168.1.10 next
        set device "port2"
        set comment "To_MGMT_Monitoring_subnets"
    next
end
```

HA

NOTE: The HA clustering members must be the same hardware model running the same software version. The seat license does not have to be identical across HA devices but is highly recommended in case of failure.

FortiProxy high availability (HA) provides a system management solution that synchronizes configuration changes among the clustering members. You can fine-tune the performance of the HA cluster to change how a cluster forms and shares information among clustering members.

The HA heartbeat keeps cluster units communicating with each other. The heartbeat consists of hello packets that are sent at regular intervals by the heartbeat interface of all cluster units. These hello packets describe the state of the cluster unit and are used by other cluster units to keep all the units synchronized.

HA heartbeat packets are non-TCP packets that use Ethertype values 0x8890, 0x8891, and 0x8893. The default time interval between HA heartbeats is 200 ms.

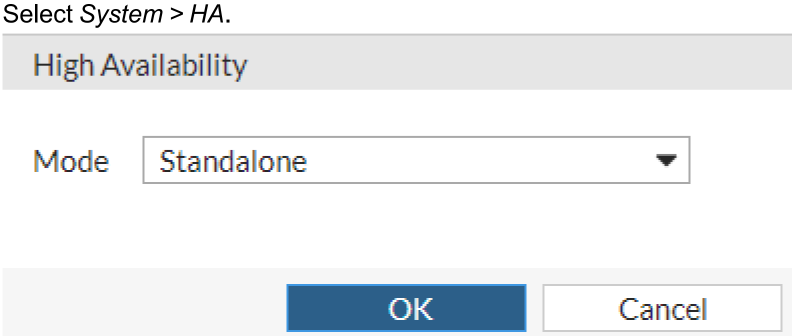
Your FortiProxy device can be configured as a standalone unit or you can configure two FortiProxy devices in the Active-Passive mode for failover protection. In active-passive mode, the FortiProxy shares available seats among the HA cluster (hardware and VM) by default. The primary FortiProxy unit automatically claims all license entitlements from all members in the HA cluster (hardware or VM). When a member joins the cluster, its associated entitlements are added to the primary unit. When a member leaves the cluster, its associated entitlements are removed from the primary unit. When the primary unit goes down, the secondary device with the highest priority becomes the primary and assumes all the license entitlements.

NOTE: If you are using vSwitches:

- In Config-Sync mode, you need to select the promiscuous mode and accept MAC address changes on the VLANs or port groups of the heartbeat vSwitch. For the data interface's vSwitch, you can use the default vSwitch setting.
- In Active-Passive mode, you need to select the promiscuous mode and accept MAC address changes on the VLANs or port groups of the heartbeat vSwitch. For the data interface's vSwitch, the security setting must be the same as the heartbeat vSwitch.

To configure an HA cluster or to view the cluster member list in the GUI:

1. Select *System > HA*.



2. Configure the following settings and then click *OK*:

Mode	Select the mode from the drop-down menu. • *Standalone*—This option disables HA mode. No further configuration options are available. • *Config-Sync*

	• *Active-Passive*—Select this option for the root of a security fabric group for license sharing.
Device priority	You can set a different device priority for each cluster member to control the order in which cluster units become the primary unit (HA primary) when the primary unit fails. The device with the highest device priority becomes the primary unit. The default value is 128.
Cluster Settings	
Group name	Enter a name to identify the cluster. Must be the same for all members for authentication and membership identification.
Password	Select *Change* to enter a password to identify the HA cluster. The maximum password length is 15 characters. The password must be the same for all cluster FortiProxy units before the FortiProxy units can form the HA cluster. When the cluster is operating, you can add a password, if required. Two clusters on the same network must have different passwords.
Monitor interfaces	Select the specific ports to monitor. If a monitored interface fails or is disconnected from its network, the interface leaves the cluster and a link failover occurs. The link failover causes the cluster to reroute the traffic being processed by that interface to the same interface of another cluster that still has a connection to the network. This other cluster becomes the new primary unit.
Heartbeat Interfaces	Select to enable or disable the HA heartbeat communication for each interface in the cluster and then set the heartbeat interface priority. The heartbeat interface with the highest priority processes all heartbeat traffic. You must select at least one heartbeat interface. If the interface functioning as the heartbeat fails, the heartbeat is transferred to another interface configured as a heartbeat interface. If heartbeat communication is interrupted, the cluster stops processing traffic. Priority ranges from 0 to 512. Select + enter another management interface.
Management Interface Reservation	Enable or disable the management interface reservation. You can provide direct management access to individual cluster units by reserving a management interface as part of the HA configuration. After this management interface is reserved, you can configure a different IP address, administrative access, and other interface settings for this interface for each cluster unit. You can also specify static routing settings for this interface. Then by connecting this interface of each cluster unit to your network, you can manage each cluster unit separately from a different IP address. Refer to HA cluster out-of-band management on page 476 for detailed instructions about configuring a management interface for an HA cluster. **Interface**: Select the management interface. **Gateway**: Enter the IPv4 address for the remote gateway.

	IPv6 gateway	Enter the IPv6 address for the remote gateway.
	Destination subnet	Enter the destination subnet.
Unicast Heartbeat	Enable the unicast HA heartbeat in virtual machine (VM) environments that do not support broadcast communication. By default, the device notifies peers by multicasting which allows all devices sharing the same group credentials (name and password) in the LAN to join the HA group automatically.	
	Unicast Heartbeat Peer IP	Enter the IP address of the HA heartbeat interface of the other FortiProxy VM in the HA cluster.

To configure an HA cluster in the CLI:

```
config system ha
   set group-name {string}
   set password {password}
   set mode [standalone|config-sync-only|...]
   set hbdev <INTERFACE_NAME> <PRIORITY>
   set override enable
   set priority <PRIORITY>
   set unicast-hb enable
   set unicast-hb-peerip <PEER_IP>
end
```

Parameter	Description	Type	Size	Default
group-name	Cluster group name. Must be the same for all members for authentication and membership identification.	string	Maximum length: 32	
password	Cluster password. Must be the same for all members for authentication and membership identification.	password	Not Specified	
mode	HA mode. Must be the same for all members. FGSP requires standalone.	option	-	standalone
	Option / **Description** *standalone*: Disable HA feature. *config-sync-only*: Enable Config sync only *active-passive*: Enable Active-passive mode. This mode enables license sharing.			
hbdev	Heartbeat interfaces. HA devices notify and identify each other through heart beat. The heartbeat interface must be the same for all members. You can also specify multiple interfaces: `set hbdev <INTF_NAME_1> <PRIORITY_1> <INTF_NAME_2> <PRIORITY_2> ...` • `<INTERFACE_NAME>` means the interface name	user	Not Specified	

Parameter	Description	Type	Size	Default
	as configured in config system interface. • <PRIORITY> means the search priority when there are multiple interfaces.			
(Optional) override	Enable and increase the priority of the unit that should always be primary. When disabled (default), the active (primary) unit is automatically determined based on its uptime etc.	option	-	disable
(Optional) priority	Increase the priority of the unit to make it the primary unit .	integer	Minimum value: 0 Maximum value: 255	128
(Optional) unicast-hb	Enable the unicast HA heartbeat in virtual machine (VM) environments that do not support broadcast communication. By default, the device notifies peers by multicasting which allows all devices sharing the same group credentials (name and password) in the LAN to join the HA group automatically.			
(Optional) unicast-hb-peerip	Unicast heartbeat peer IP, which is the IP address of the HA heartbeat interface of the other FortiProxy VM in the HA cluster.	ipv4-address	Not Specified	0.0.0.0

Refer to the config system ha topic in the CLI guide for more details about other available configurations for HA setup.

To view HA cluster information in the CLI:

- Run the `get system ha status` command to see the synchronization status of the HA cluster. For synchronized HA peers, the status should be `in-sync` in `Configuration Status`.
- Run the `diag system ha status` command to see the license serial number of connected peer devices.

HA multiple unicast peers

You can configure up to eight unicast Config-Sync HA clusters. Unicast configuration synchronization is supported on layer 3, allowing peers to be synchronized in cloud environments that do not support layer-2 networking. Configuring a unicast gateway allows peers to be in different subnets.

For example:

```
config system ha
   set mode config-sync-only
   set hbdev "port1" 50
   set override enable
   set unicast-status enable
   set unicast-gateway 10.0.0.1
   config unicast-peers
      edit 1
         set peer-ip 192.168.76.13
      next
```

```
      .........
   end
end
```

Note:

- Use the `set unicast-hb enable` command for a one-to-one unicast Active-Passive HA cluster or Config-Sync HA cluster.
- Use the *set unicast-status*, `set unicast-gateway`, and `config unicast-peers` commands for multiple peers in a Config-Sync HA cluster.

Cache Collaboration

When deployed in a cluster, depending on the deployed architecture, requests for the same URL might have hit each cache device and been cached separately on each. Methods are available to mitigate this through load balancing with FortiADC or WCCP.

FortiProxy has the Cache Collaboration feature, where the storage of all devices within the FortiProxy HA Cluster is accessible as a shared entity. This feature allows content cached by one device to be shared by other FortiProxy devices within the cluster, significantly increasing the cache rate.

CLI syntax

```
config wanopt cache-service
   set prefer-senario {balance | prefer-speed | prefer-cache} // Default is balance.
   set collaboration {enable | disable} // Default is disable.
   set device-id <name>
   set acceptable-connections {any | peers} // Default is any.
end
```

HA virtual cluster setup

Virtual clustering provides failover protection between two instances of one or more VDOMs operating on two FortiProxies that are in a virtual cluster. A standard virtual cluster consists of FortiProxies that are operating in active-passive HA mode with multiple VDOMs enabled.

Active-passive virtual clustering uses VDOM partitioning to send traffic for some VDOMs to the primary FortiProxy and traffic for other VDOMs to the secondary FortiProxies. Traffic distribution between FortiProxies can potentially improve throughput. If a failure occurs and only one FortiProxy continues to operate, all traffic fails over to that FortiProxy, similar to normal HA. If the failed FortiProxies rejoin the cluster, the configured traffic distribution is restored.

In an active-passive virtual cluster of two FortiProxies, the primary and secondary FortiProxies share traffic processing according to the VDOM partitioning configuration. If you add a third or fourth FortiProxy, the primary and first secondary FortiProxy process all traffic and the other one or two FortiProxies operate in standby mode. If the primary or first secondary FortiProxy fails, one of the other FortiProxies becomes the new primary or secondary FortiProxy and begins processing traffic.

Separation of VDOM traffic

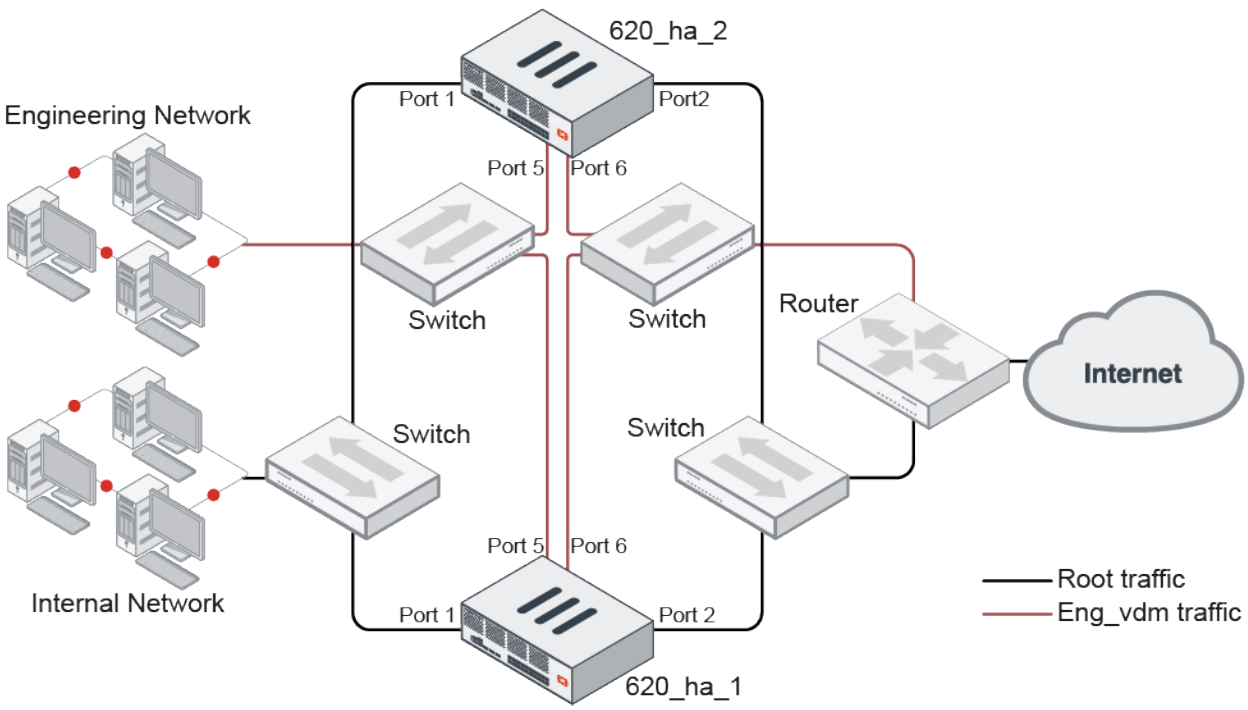
Virtual clustering creates a cluster between instances of each VDOM on the two FortiProxies in the virtual cluster. All traffic to and from a given VDOM is sent to one of the FortiProxies where it stays within its VDOM and is only processed by that VDOM. One FortiProxy is the primary FortiProxy for each VDOM and one FortiProxy is the secondary FortiProxy for each VDOM. The primary FortiProxy processes all traffic for its VDOMs; the secondary FortiProxy processes all traffic for its VDOMs.

Virtual clustering and heartbeat interfaces

The HA heartbeat provides the same HA services in a virtual clustering configuration as in a standard HA configuration. One set of HA heartbeat interfaces provides HA heartbeat services for all of the VDOMs in the cluster. You do not have to add a heartbeat interface for each VDOM.

Example

This example shows a virtual cluster configuration consisting of two FortiProxies. The virtual cluster has two VDOMs, Root and End_vdm.



The root VDOM can only be associated with virtual cluster 1.

To set up an HA virtual cluster using the GUI:

1. Make all the necessary connections as shown in the topology diagram.
2. Log into one of the FortiProxies.
3. Go to *System > HA* and set the following options:

Mode	Active-Passive

Device priority	128 or higher
Group name	Example_cluster
Heartbeat interfaces	ha1 and ha2

Except for the device priority, these settings must be the same on all FortiProxies in the cluster.

4. Leave the remaining settings as their default values. They can be changed after the cluster is in operation.
5. Click *OK*.
   The FortiProxy negotiates to establish an HA cluster. Connectivity with the FortiProxy may be temporarily lost as the HA cluster negotiates and changes the MAC addresses of the FortiProxy's interfaces.
6. Factory reset the other FortiProxy that will be in the cluster, configure GUI access, then repeat steps 1 to 5, omitting setting the device priority, to join the cluster.
7. Go to *System* > *Settings* and enable *Virtual Domains*.
8. Click *Apply*. You will be logged out of the FortiProxy.
9. Log back into the FortiProxy, ensure that you are in the global VDOM, and go to *System* > *VDOM*.
10. Create two new VDOMs, such as VD1 and VD2:
    a. Click *Create New*. The *New Virtual Domain* page opens.
    b. Enter a name for the VDOM in the *Virtual Domain* field, then click *OK* to create the VDOM.
    c. Repeat these steps to create a second new VDOM.
11. Implement a virtual cluster by moving the new VDOMs to *Virtual cluster 2*:
    a. Go to *System* > *HA*.
    b. Enable *VDOM Partitioning*.
    c. Click on the *Virtual cluster 2* field and select the new VDOMs.
    d. Click *OK*.

To set up an HA virtual cluster using the CLI:

1. Make all the necessary connections as shown in the topology diagram.
2. Set up a regular A-P cluster. See HA on page 469.
3. Enable VDOMs:

```
config system global
    set vdom-mode multi-vdom
end
```

   You will be logged out of the FortiProxy.
4. Create two VDOMs:

```
config vdom
    edit VD1
    next
    edit VD2
    next
end
```

5. Reconfigure the HA settings to be a virtual cluster:

```
config global
    config system ha
        set vcluster2 enable
        config secondary-vcluster
            set vdom "VD1" "VD2"
```

```
            end
        end
    end
```

HA cluster out-of-band management

To provide direct management access to all cluster units, a management interface can be reserved as port of the HA configuration. After the management interface is reserved, the various interface settings, such as the IP address and administrative access, can be configured for each individual cluster unit. These settings are not synchronized to other cluster units. Connect the management interface of each cluster unit to your network to individually manage each unit with its unique IP address.

- Reserved management interfaces provide direct management access to each cluster unit, and give each cluster unit a different identity on your network. This simplifies using external services, such as SNMP, to monitor and manage each cluster units.
- Reserved management interfaces are not assigned HA virtual MAC addresses. They retain the permanent hardware address of the physical interface, unless you manually change it using the `config system interface` command.
- Reserved management interfaces and their IP addresses should not be used for managing a cluster using FortiManager. To manage a FortiGate HA cluster with FortiManager, use the IP address of one of the cluster unit interfaces.
- Configuration changes to a reserved management interface are not synchronized to other cluster units. Other configuration changes are automatically synchronized to all cluster units.

For outgoing traffic, the management interface supports only the following protocols: SNMP, NTP, LOG, Radius, FTP, TFTP, telnet. For the management interface to handle outgoing traffic with an unsupported protocol, you must configure multiple VDOM on page 459s and dedicate the root VDOM to management traffic, which means assigning the management interface and the ha-sync interface to the root VDOM while keeping all other interfaces for in-band traffic to user VDOMs.

Management interface

Enable HTTPS or HTTP administrative access on the reserved management interfaces to connect to the GUI of each cluster unit. On secondary units, the GUI has the same features as the primary unit, except for unit specific information, for example:

- The *System Information* widget on the Dashboard shows the secondary unit's serial number, and also the same cluster information as on the primary unit.
- In the cluster list at *System* > *HA*, you can change the HA configuration for the unit that you are logged into, but you can only change the host name and device priority for the primary unit and other secondary units.
- The system events logs show logs for the device that you are logged into. To view logs for other cluster units, including the primary unit, use the cluster member list at *System* > *HA*.

Enable SNMP administrative access on a reserved management interface to use SNMP to monitor each cluster unit using the interface's IP address. Direct management of cluster members must also be enabled, see Configuration example on page 477.

Enable SSH or TELNET administrative access on the reserved management interfaces to connect to the CLI of each cluster unit. The CLI prompt includes the host of the cluster unit that you are connected to. Use the `execute ha manage` command to connect to other cluster unit CLIs.

SNMP, remote authentication server and other management services

By default, management services such as SNMP, remote authentication (LDAP, RADIUS, TACACS+, and others), remote logging, and others use a cluster interface. This means that communication from each cluster unit comes from a cluster interface, and not from an individual cluster unit's interface or the HA reserved management interface.

You can configure HA reserved management interfaces to be used for communication with management services by enabling the `ha-direct` option. This separates management traffic for each cluster unit, and allows each unit to be individually managed. This is especially useful when cluster units are in different physical locations.

The following management features will then use the HA reserved management interface:

- SNMP queries and traps
- Remote authentication and certificate verification
- Communication with FortiSandbox
- Remote logging

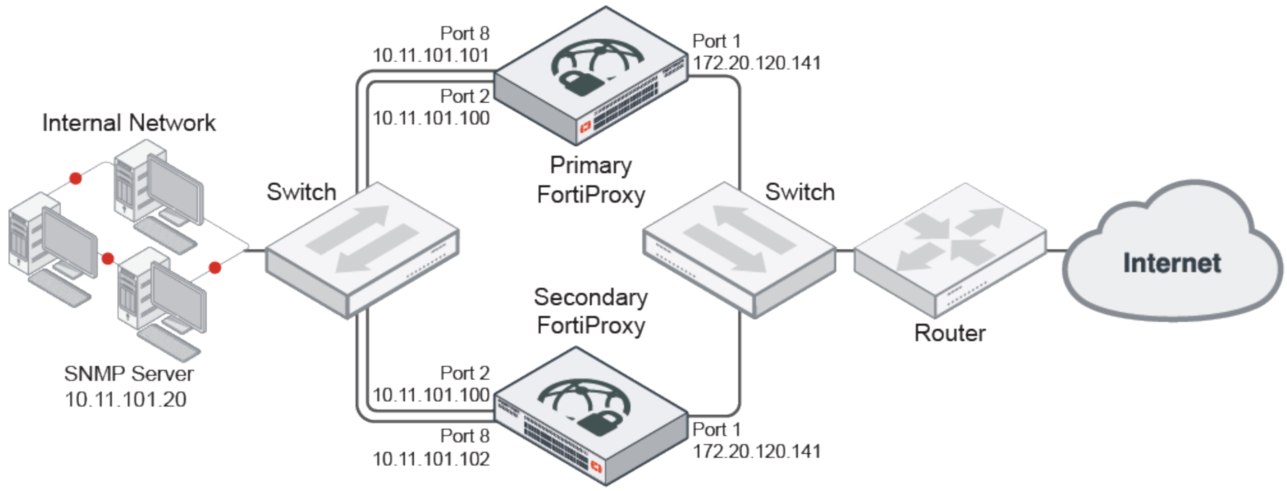
To use the HA reserved management interface for management:

```
config system ha
    set ha-direct enable
end
```

SNMP requires `ha-direct` to be configured under SNMP settings only. See below for more configuration options.

Configuration example

This example describes how to configure SNMP remote management of individual cluster units using an HA reserved management interface. The configuration consists of two FortiProxy units already operating as a cluster.



Two FortiProxy units are already operating in a cluster. On each unit, port8 is connected to the internal network through a switch and configured as an out-of-band reserved management interface.

Administrative access and default route for HA management interface

To configure the primary unit's reserved management interface, configure an IP address and management access on port8. Then, configure the necessary HA settings to enable the HA reserved management interface and its route.

To configure the secondary unit's reserved management interface, access the unit's CLI through the primary unit, and configure an IP address, management access on port8, and the necessary HA settings. Configuration changes to the reserved management interface are not synchronized to other cluster units.

To configure the primary unit reserved management interface in CLI:

1. From a computer on the internal network, connect to the CLI at 10.11.101.100 on port2.
2. Change the port8 IP address and management access:

```
config system interface
    edit port8
        set ip 10.11.101.101/24
        set allowaccess https ping ssh snmp
    next
end
```

3. Configure the HA settings for the HA reserved management interface by defining a default route to route to the gateway 10.11.101.2:

```
config system ha
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface port8
            set gateway 10.11.101.2
            set gateway6 2001:db8:0:2::20
        next
    end
end
```

You can now log into the primary unit's GUI by browsing to https://10.11.101.101. You can also log into the primary unit's CLI by using an SSH client to connect to 10.11.101.101.

To configure secondary unit reserved management interfaces to allow HTTPS, SSH, and ICMP access:

1. From a computer on the internal network, connect to the primary unit's CLI.
2. Connect to the secondary unit with the following command:

```
execute ha manage <unit id> <username> <password>
```

3. Change the port8 IP address and management access:

```
config system interface
    edit port8
        set ip 10.11.101.102/24
        set allowaccess https ping ssh snmp
    next
end
```

4. Configure the HA settings for the HA reserved management interface by defining a default route to route to the gateway 10.11.101.2:

```
config system ha
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface port8
            set gateway 10.11.101.2
            set gateway6 2001:db8:0:2::20
        next
    end
end
```

You can now log into the secondary unit's GUI by browsing to https://10.11.101.102. You can also log into the secondary unit's CLI by using an SSH client to connect to 10.11.101.102.

SNMP monitoring

The SNMP server can get status information from the cluster members. To use the reserved management interfaces, you must add at least one HA direct management host to an SNMP community. If the SNMP configuration includes SNMP users with user names and passwords, HA direct management must be enabled for the users. The SNMP configuration is synchronized to all cluster units.

To configure the cluster for SNMP management using the reserved management interfaces:

1. Add an SNMP community with a host for the reserved management interface of each cluster member. The host includes the IP address of the SNMP server.

```
config system snmp community
    edit 1
        set name "Community"
        config hosts
            edit 1
                set ip 10.11.101.20 255.255.255.255
                set ha-direct enable
            next
```

```
        end
    next
end
```

Enabling `ha-direct` in a non-HA environment will make SNMP unusable.

2. Add an SNMP user for the reserved management interface:

```
config system snmp user
    edit "1"
        set notify-hosts 10.11.101.20
        set ha-direct enable
    next
end
```

3. Configure remaining settings as required.

To get CPU, memory, and network usage information from the SNMP manager for each cluster unit using the reserved management IP addresses:

1. Connect to the SNMP manager CLI.
2. Get resource usage information for the primary unit using the MIB fields:

```
snmpget -v2c -c Community 10.11.101.101 fgHaStatsCpuUsage
snmpget -v2c -c Community 10.11.101.101 fgHaStatsMemUsage
snmpget -v2c -c Community 10.11.101.101 fgHaStatsNetUsage
```

3. Get resource usage information for the primary unit using the OIDs:

```
snmpget -v2c -c Community 10.11.101.101 1.3.6.1.4.1.12356.101.13.2.1.1.3.1
snmpget -v2c -c Community 10.11.101.101 1.3.6.1.4.1.12356.101.13.2.1.1.4.1
snmpget -v2c -c Community 10.11.101.101 1.3.6.1.4.1.12356.101.13.2.1.1.5.1
```

4. Get resource usage information for the secondary unit using the MIB fields:

```
snmpget -v2c -c Community 10.11.101.102 fgHaStatsCpuUsage
snmpget -v2c -c Community 10.11.101.102 fgHaStatsMemUsage
snmpget -v2c -c Community 10.11.101.102 fgHaStatsNetUsage
```

5. Get resource usage information for the primary unit using the OIDs:

```
snmpget -v2c -c Community 10.11.101.102 1.3.6.1.4.1.12356.101.13.2.1.1.3.1
snmpget -v2c -c Community 10.11.101.102 1.3.6.1.4.1.12356.101.13.2.1.1.4.1
snmpget -v2c -c Community 10.11.101.102 1.3.6.1.4.1.12356.101.13.2.1.1.5.1
```

Remote authentication over dedicated HA management interface

If a dedicated management interface is configured on each cluster unit, and authentication on a remote server is used (administrator log in, firewall authentication, SSL VPN access, and so on), then the FortiProxy units can contact the remote authentication server using the HA management interface if `ha-direct` is enabled.

This shows an example configuration for a remote system administrator:

```
config system ha
    set group-id 110
```

```
    set group-name "leo_fpx_ha_11"
    set mode active-passive
    set hbdev "port5" 50
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "port4"
            set gateway 10.150.0.3
        next
    end
    set override enable
    set priority 111
    set unicast-hb enable
    set unicast-hb-peerip 10.150.51.12
end

config system admin
    edit "leo_rad"
        set remote-auth enable
        set accprofile "prof_admin"
        set remote-group "radius_grp_mgmt"
    next
end

config user radius
    edit "radius_mgmt"
        set server "10.150.0.111"
        set secret ************
    next
end

config user group
    edit "radius_grp_mgmt"
        set member "radius_mgmt"
    next
end
```

SNMP

The Simple Network Management Protocol (SNMP) allows you to monitor hardware on your network. You can configure the hardware, such as the FortiProxy SNMP agent, to report system information and traps.

SNMP traps alert you to events that happen, such as a log disk becoming full, or a virus being detected. These traps are sent to the SNMP managers. An SNMP manager (or host) is typically a computer running an application that can read the incoming traps and event messages from the agent and can send out SNMP queries to the SNMP agents. A FortiManager unit can act as an SNMP manager to one or more FortiProxy units.

By using an SNMP manager, you can access SNMP traps and data from any FortiProxy interface configured for SNMP management access. Part of configuring an SNMP manager is to list it as a host in a community on the FortiProxy unit it will be monitoring. Otherwise, the SNMP monitor will not receive any traps from, and be unable to query, that FortiProxy unit.

When using SNMP, you must also ensure you have added the correct Management Information Base (MIB) files to the unit, regardless of whether or not your SNMP manager already includes standard and private MIBs in a ready-to-use, compiled database. A MIB is a text file that describes a list of SNMP data objects used by the SNMP manager. See Fortinet MIBs on page 485 for more information.

The FortiProxy SNMP implementation is read-only. SNMP v1, v2c, and v3 compliant SNMP managers have read-only access to FortiProxy system information through queries and can receive trap messages from the unit.

The FortiProxy SNMP v3 implementation includes support for queries, traps, authentication, and privacy. Authentication and encryption are configured in the CLI.

FortiProxy supports Low crypto (LENC) mode for LENC models.

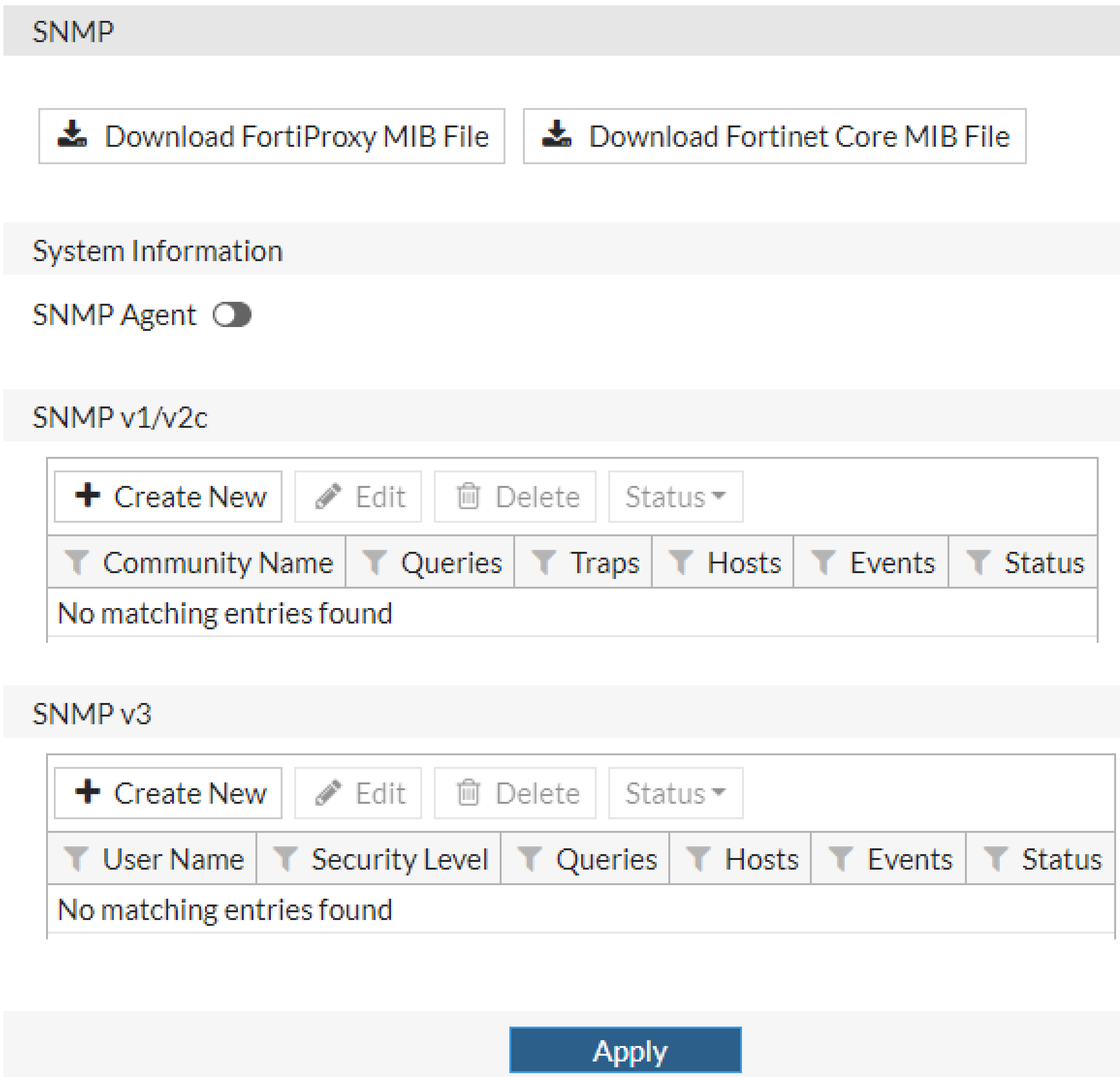
Before a remote SNMP manager can connect to the FortiProxy agent, you must configure one or more FortiProxy interfaces to accept SNMP connections. Interfaces are configured in *Network > Interfaces*. See Interfaces on page 95.

For security reasons, Fortinet recommends that neither “public” nor “private” be used for SNMP community names.

When the unit is in virtual domain mode, SNMP traps can only be sent on interfaces in the management virtual domain.

If you want to allow SNMP access on an interface, you must go to *Network > Interfaces* and select *SNMP* in the *Access* field in the settings for the interface that you want the SNMP manager to connect to.

For SNMP configuration, go to *System > SNMP*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

Configure the following settings and select *Apply*:

Download FortiProxy MIB File	Download the FortiProxy MIB file. See Fortinet MIBs on page 485.
Download Fortinet Core MIB File	Download the Fortinet MIB file. See Fortinet MIBs on page 485.
SNMP Agent	Enable the FortiProxy SNMP agent. See SNMP agent on page 486.
SNMP v1/v2c	Lists the communities for SNMP v1/v2c. From within this section, you can create, edit or remove SNMP communities.
Create New	Creates a new SNMP community. When you select *Create New*, the *New SNMP Community* page opens. See Create or edit an SNMP community on page 486.

Edit	Modifies settings within an SNMP community. When you click *Edit*, the *Edit SNMP Community* page opens.
Delete	Removes an SNMP community from the list. To remove multiple SNMP communities, select multiple rows in the list by holding down the Ctrl or Shift keys and then select *Delete*.
Status	Enable or disable the SNMP community.
Community Name	The name of the community.
Queries	Indicates whether queries protocols (v1 and v2c) are enabled or disabled. A check mark indicates that queries are enabled; a gray x indicates that queries are disabled. If one query is disabled and another one enabled, there will still be a check mark.
Traps	Indicates whether trap protocols (v1 and v2c) are enabled or disabled. A check mark indicates that traps are enabled; a gray x indicates that traps are disabled. If one query is disabled and another one enabled, there will still be a check mark.
Hosts	Number of hosts that are part of the SNMP community.
Events	Number of events that have occurred.
Status	Indicates whether the SNMP community is enabled or disabled.
SNMP v3	Lists the SNMP v3 users. From within this section, you can edit, create or remove an SNMP v3 user.
Create New	Creates a new SNMP v3 user. When you select *Create New*, the *Create New SNMP User* page opens. See Create or edit an SNMP user on page 490.
Edit	Modifies settings within the SNMP v3 user. When you click *Edit*, the *Edit SNMP User* page opens.
Delete	Removes an SNMP v3 user from the page. To remove multiple SNMP v3 users, select multiple rows in the list by holding down the Ctrl or Shift keys and then select *Delete*.
Status	Enable or disable the SNMP v3 user.
User Name	The name of the SNMP v3 user.
Security Level	The security level of the user.
Queries	Indicates whether queries are enabled or disabled. A green check mark indicates that queries are enabled; a gray x indicates that queries are disabled.
Hosts	Number of hosts.
Events	Number of SNMP events associated with the SNMPv3 user.
Status	Indicates whether the SNMPv3 user is enabled or disabled.

Fortinet MIBs

The FortiProxy SNMP agent supports Fortinet proprietary MIBs, as well as standard RFC 1213 and RFC 2665 MIBs. RFC support includes support for the parts of RFC 2665 (Ethernet-like MIB) and the parts of RFC 1213 (MIB II) that apply to FortiProxy unit configuration.

There are two MIB files for FortiProxy units; both files are required for proper SNMP data collection:

- The Fortinet MIB: contains traps, fields, and information that is common to all Fortinet products.
- The FortiProxy MIB: contains traps, fields, and information that is specific to FortiProxy units.

The Fortinet and FortiProxy MIB files are available for download on the Fortinet Customer Support site. Each Fortinet product has its own MIB—if you use other Fortinet products, you need to download their MIB files as well.

The Fortinet MIB and FortiProxy MIB, along with the two RFC MIBs, are listed in the table in this section.

To download the MIB files, go to *System* > *SNMP* and select a MIB link in the SNMP section. See SNMP on page 481.

Your SNMP manager may already include standard and private MIBs in a compiled database that is ready to use. You must add the Fortinet proprietary MIB to this database to have access to the Fortinet-specific information.

MIB files are updated for each version of FortiProxy. When upgrading the firmware, ensure that you update the Fortinet FortiProxy MIB file compiled in your SNMP manager as well.

MIB file name	Description
FORTINET-CORE-MIB.mib	The Fortinet MIB includes all system configuration information and trap information that is common to all Fortinet products. Your SNMP manager requires this information to monitor FortiProxy unit configuration settings and receive traps from the FortiProxy SNMP agent.
FORTINET-FORTIPROXY-MIB.mib	The FortiProxy MIB includes all system configuration information and trap information that is specific to FortiProxy units. Your SNMP manager requires this information to monitor FortiProxy configuration settings and receive traps from the FortiProxy SNMP agent. FortiManager systems require this MIB to monitor FortiProxy units.

SNMP get command syntax

Normally, to get configuration and status information for a FortiProxy unit, an SNMP manager would use an SNMP get command to get the information in a MIB field. The SNMP get command syntax would be similar to:

```
snmpget -v2c -c <community_name> <address_ipv4> {<OID> | <MIB_field>}
```

where:

- <community_name> refers to the SNMP community name added to the FortiProxy configuration. You can add more than one community name to a FortiProxy SNMP configuration. The most commonly used community name is public. For security reasons, Fortinet recommends that neither public nor private be used for SNMP community names.
- <address_ipv4> is the IP address of the FortiProxy interface that the SNMP manager connects to
- {<OID> | <MIB_field>} is the object identifier for the MIB field or the MIB field name itself.

For example, to query the firmware version running on the FortiProxy unit, the following command could be issued:

```
snmpget -v2c -c public 10.10.10.1 1.3.6.1.4.1.12356.109.4.1.1.0
```

In this example, the community name is `public`, the IP address of the interface configured for SNMP management access is `10.10.10.1`. The firmware version is queried using the MIB field `fchSysVersion`, the OID for which is `1.3.6.1.4.1.12356.109.4.1.1.0`.

The value returned is a string with a value of `v2.0,build0225,130213`.

SNMP agent

The FortiProxy SNMP agent must be enabled before configuring other SNMP options. Enter information about the FortiProxy unit to identify it so that when your SNMP manager receives traps from the FortiProxy unit, you will know which unit sent the information.

To configure the SNMP agent in the GUI:

1. Go to *System* > *SNMP*.
2. Enable the SNMP agent by moving the slider in the SNMP Agent field.
3. Enter a descriptive name for the agent. The description can be up to 35 characters long.
4. Enter the physical location of the unit. The system location description can be up to 35 characters long.
5. Enter the contact information for the person responsible for this FortiProxy unit. The contact information can be up to 35 characters.
6. Click *Apply* to save your changes.

To configure the SNMP agent with the CLI:

Enter the following CLI commands:

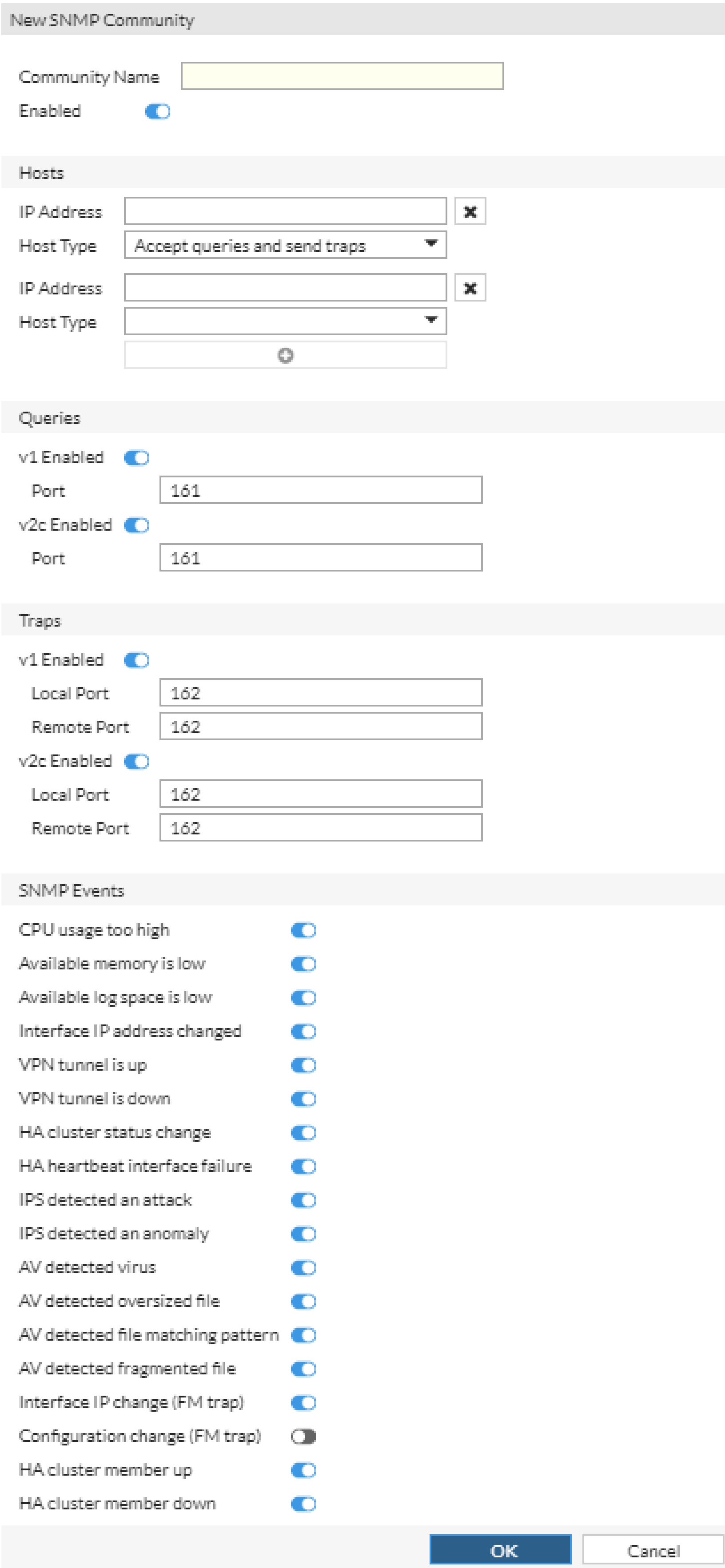
```
config system snmp sysinfo
   set status enable
   set contact-info <contact_information>
   set description <description_of_FortiProxy>
   set location <FortiProxy_location>
end
```

Create or edit an SNMP community

An SNMP community is a grouping of devices for network administration purposes. Within that SNMP community, devices can communicate by sending and receiving traps and other information. One device can belong to multiple communities, such as one administrator terminal monitoring both a firewall SNMP and a printer SNMP community.

Add SNMP communities to your FortiProxy unit so that SNMP managers can view system information and receive SNMP traps. You can add up to three SNMP communities. Each community can have a different configuration for SNMP queries and traps and can be configured to monitor the FortiProxy unit for a different set of events. You can also add the IP addresses of up to eight SNMP managers to each community.

Selecting *Create New* on the *SNMP v1/v2c* table opens the *New SNMP Community* page, which provides settings for configuring a new SNMP community. Selecting a community from the list and selecting *Edit* opens the *Edit SNMP Community* page.

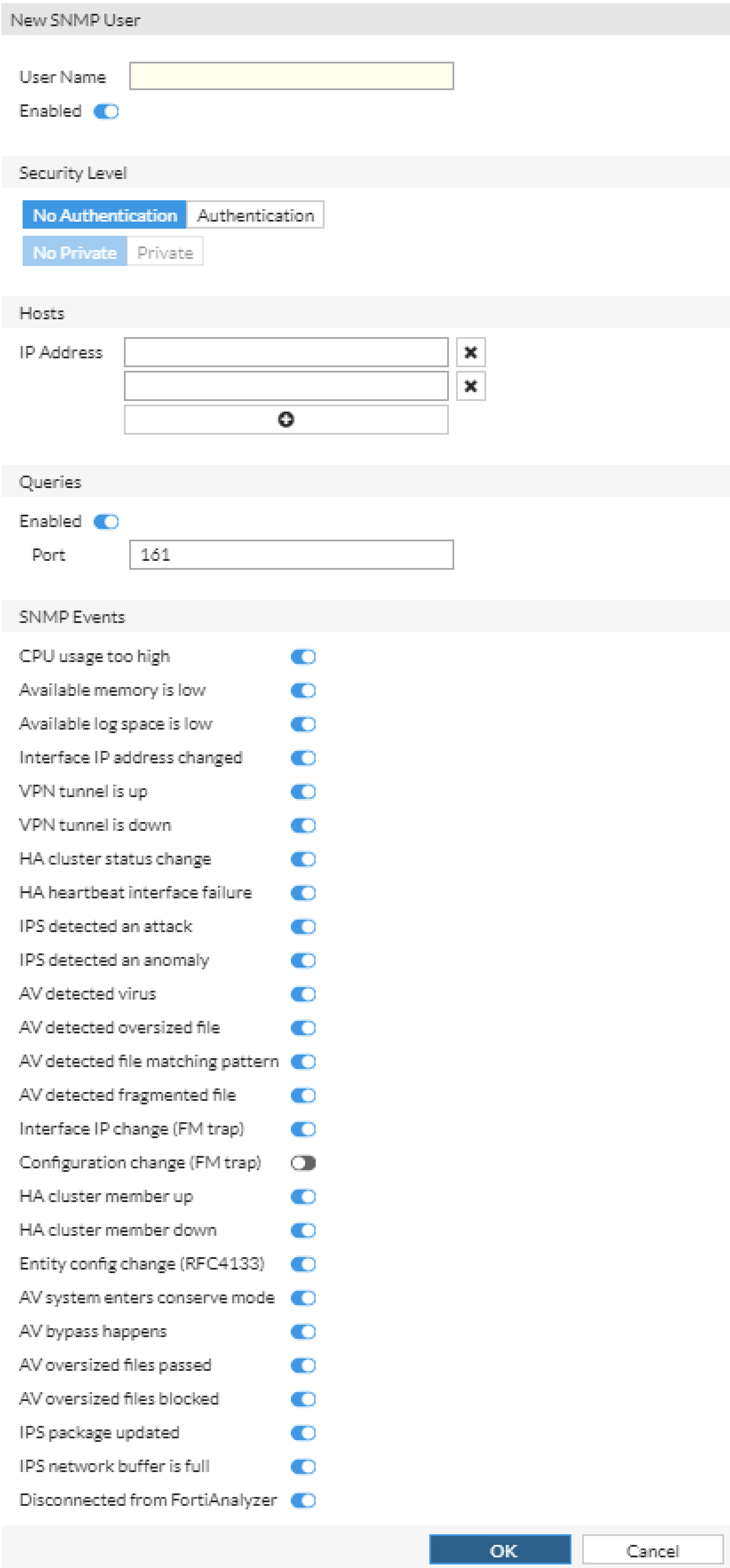

New SNMP Community
Community Name
Enabled
Hosts
IP Address
Host Type
Accept queries and send traps
IP Address
Host Type
Queries
v1 Enabled
Port
161
v2c Enabled
Port
161
Traps
v1 Enabled
Local Port
162
Remote Port
162
v2c Enabled
Local Port
162
Remote Port
162
SNMP Events
CPU usage too high
Available memory is low
Available log space is low
Interface IP address changed
VPN tunnel is up
VPN tunnel is down
HA cluster status change
HA heartbeat interface failure
IPS detected an attack
IPS detected an anomaly
AV detected virus
AV detected oversized file
AV detected file matching pattern
AV detected fragmented file
Interface IP change (FM trap)
Configuration change (FM trap)
HA cluster member up
HA cluster member down
OK
Cancel

Configure the following settings in the New SNMP Community page or Edit SNMP Community page and click *OK*:

Community Name	Enter a name to identify the SNMP community. After you create the SNMP community, you cannot edit the name.
Enabled	Enable or disable the SNMP community.
Hosts	Settings for configuring the hosts of an SNMP community.
IP Address	Enter the IP address/netmask of the SNMP managers that can use the settings in this SNMP community to monitor the unit. You can also set the IP address to 0.0.0.0 to so that any SNMP manager can use this SNMP community.
Host Type	Select one of the following: *Accept queries and send traps*, *Accept queries only*, or *Send traps only*
X	Removes an SNMP manager from the list within the *Hosts* section.
+	Select to add a blank line to the Hosts list. You can add up to 16 SNMP managers to a single community.
Queries	Settings for configuring queries for both SNMP v1 and v2c.
v1 Enabled	Enable or disable SNMP v1 queries.
Port	Enter the port number (161 by default) that the SNMP managers in this community use for SNMP v1 and SNMP v2c queries to receive configuration information from the unit. The SNMP client software and the unit must use the same port for queries.
v2c Enabled	Enable or disable SNMP v2c queries.
Traps	Settings for configuring local and remote ports for both v1 and v2c.
v1 Enabled	Enable or disable SNMP v1 traps.
Local Port	Enter the remote port numbers (162 by default) that the unit uses to send SNMP v1 or SNMP v2c traps to the SNMP managers in this community. The SNMP client software and the unit must use the same port for traps.
Remote Port	Enter the remote port number (162 by default) that the unit uses to send SNMP traps to the SNMP managers in this community. The SNMP client software and the unit must use the same port for traps.
v2c Enabled	Enable or disable SNMP v2c traps.
SNMP Events	Enable each SNMP event for which the unit should send traps to the SNMP managers in this community. **Note:** The *CPU usage too high* trap's sensitivity is slightly reduced by spreading values out over 8 polling cycles. This reduction prevents sharp spikes due to CPU intensive short-term events such as changing a policy.

Create or edit an SNMP user

Selecting *Create New* on the *SNMP v3* table opens the *New SNMP User* page, which provides settings for configuring a new SNMP v3 user. Selecting a user name from the route list and selecting *Edit* opens the *Edit SNMP User* page.

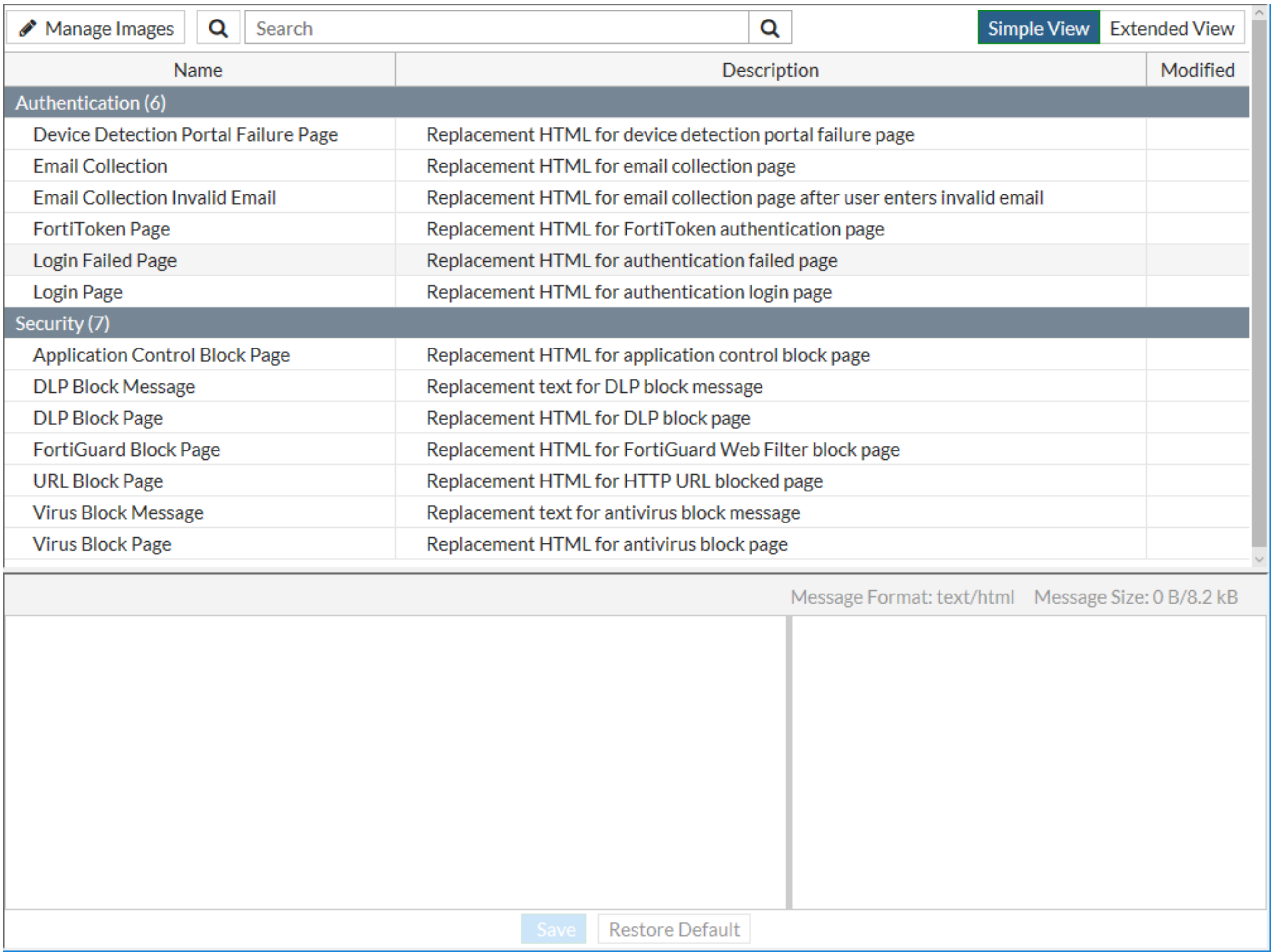

New SNMP User
User Name
Enabled
Security Level
No Authentication
Authentication
No Private
Private
Hosts
IP Address
Queries
Enabled
Port
161
SNMP Events
CPU usage too high
Available memory is low
Available log space is low
Interface IP address changed
VPN tunnel is up
VPN tunnel is down
HA cluster status change
HA heartbeat interface failure
IPS detected an attack
IPS detected an anomaly
AV detected virus
AV detected oversized file
AV detected file matching pattern
AV detected fragmented file
Interface IP change (FM trap)
Configuration change (FM trap)
HA cluster member up
HA cluster member down
Entity config change (RFC4133)
AV system enters conserve mode
AV bypass happens
AV oversized files passed
AV oversized files blocked
IPS package updated
IPS network buffer is full
Disconnected from FortiAnalyzer
OK
Cancel

Configure the following settings in the New SNMP User page or Edit SNMP User page and click *OK*:

User Name	Enter the name of the user. After you create an SNMP user, you cannot change the user name.
Enabled	Toggle the slider to enable or disable this SNMP user.
Security Level	Select the type of security level the user will have: • *No Authentication* • *Authentication* and *No Private*—Enter the authentication algorithm and password to use. • *Authentication* and *Private*—Enter the authentication algorithm and password to use.
Authentication Algorithm	If the security level is set to *Authentication* and *No Private*, you can select *MD5* or *SHA1* for the authentication algorithm. If the security level is set to *Authentication* and *Private*, you can select *AES*, *DES*, *AES256*, or *AES256 Cisco* for the authentication algorithm.
Password	If the security level is set to *Authentication*, select *Change* and enter a password in the *Password* field.
Hosts	Settings for configuring the hosts of an SNMP community.
IP Address	Enter the IP address of the notification host. If you want to add more than one host, select + to add another host. Up to 16 hosts can be added. Select *X* to delete any hosts.
Queries	Settings for configuring queries for both SNMP v1 and v2c.
Enabled	Enable or disable the query. By default, the query is enabled.
Port	Enter the port number in the *Port* field (161 by default).
SNMP Events	Select the SNMP events that will be associated with the user.

Replacement Messages

Go to *System* > *Replacement Messages* to customize replacement pages as needed.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Manage Images	Select to view the available images and their respective tags and add new images. By default, images are embedded in replacement messages instead of using a URL.
	To use a URL:
	`config webfilter fortiguard`
	`    set embed-image disable`
	`end`

Search	Enter a search term to search the replacement message list.
Simple View or Extended View	Select the view: • *Simple View* displays a selection of *Security* and *Authentication* messages. • *Extended View* displays all messages. See the table at the end of this section for a list of all the messages.

Name	The message name.
Description	The message description.
Modified	A check mark is shown when the message has been modified.
Save	Save any customizations that you made to the message.
Restore Default	Restore the message back to its default state.
Preview	A preview of how the message looks.
Message HTML	The HTML code for the message that you can edit.

The following table outlines all of the messages that can be customized, as shown in *Extended View*:

Category	Messages	Description
Administrator	Post-login Disclaimer Message	Replacement message for post-login disclaimer.
	Pre-login Disclaimer Message	Replacement message for pre-login disclaimer.
Alert Email	alertmail-block	Alert email text for block incidents.
	alertmail-crit-event	Alert email text for critical event notification.
	alertmail-disk-full	Alert email text for disk-full events.
	alertmail-nids-event	Alert email text for IPS events.
	alertmail-virus	Alert email text for virus incidents.

Category	Messages	Description
Authentication	Authentication Rejection Page	Replacement HTML for authentication rejection page.
	Authentication Success Page	Replacement HTML for authentication success page.
	Block Notification Page	Replacement HTML for block notification page.
	Certificate Password Page	Replacement HTML for certificate password page.
	Declined Disclaimer Page	Replacement HTML for user declined disclaimer page.
	Declined Quarantine Page	Replacement HTML for user declined quarantine page.
	Disclaimer Page	Replacement HTML for authentication disclaimer page.
	Email Collection	Replacement HTML for email collection page.
	Email Collection Invalid Email	Replacement HTML for email collection page after user enters invalid email.
	Email Token Page	Replacement HTML for email-token authentication page.
	FortiToken Page	Replacement HTML for FortiToken authentication page.
	Guest User Email Template	Replacement text for guest-user credentials email message.
	Guest User Print Template	Replacement HTML for guest-user credentials print out.
	Keepalive Page	Replacement HTML for authentication keep-alive page.
	Login Challenge Page	Replacement HTML for authentication login-challenge page.
	Login Failed Page	Replacement HTML for authentication failed page.
	Login Page	Replacement HTML for authentication login page.
	Next FortiToken Page	Replacement HTML for next FortiToken authentication page.
	Password Expiration Page	Replacement HTML for password expiration page.
	Portal Page	Replacement HTML for post-authentication portal page.
	Quarantine Notification Page	Replacement HTML for quarantine notification page.
	SAML Login Page	Replacement HTML for SAML authentication login page.
	SMS Token Page	Replacement HTML for SMS-token authentication page.
	Success Message	Replacement text for authentication success message.
	Two-Factor Login Failed	Replacement HTML for two-factor authentication failed page.
	Two-Factor Login Page	Replacement HTML for two-factor authentication login page.
Automation	Automation Alert Email	Replacement HTML for automation alert email.
Device Detection Portal	Device Detection Portal Failure Page	Replacement HTML for device detection portal failure page.

Category	Messages	Description
Email	AV Engine Load Error Email Block Message	Replacement text for email blocked because the antivirus engine failed. to load.
	Email Decompressed Attachment Oversize Block Message	Replacement text indicating the removal of an oversized decompressed attachment from email.
	Email DLP Ban	Replacement text for emails blocked due to data leak detection.
	Email DLP Subject	Replacement text for subject of emails blocked due to data leak detection.
	Email File Block Message	Replacement text for message indicating removal of blocked attachment from email.
	Email File Size Block Message	Replacement text for message indicating removal of oversized attachment from email.
	Partial Email Block Message	Replacement text for emails rejected because they are fragmented.
	SMTP Decompressed Attachment Oversize Block Message	SMTP rejection text indicating rejection due to an oversized decompressed attachment.
	SMTP File Block Message	Replacement text for emails rejected due to blocked attachments.
	SMTP File Size Message	Replacement text for emails rejected due to file size limit.
FortiGuard Web Filtering	FortiGuard Block Page	Replacement HTML for FortiGuard web filter block page.
	FortiGuard HTTP Error Page	Replacement HTML for FortiGuard web filter HTTP error page.
	FortiGuard Override Page	Replacement HTML for FortiGuard web filter override page.
	FortiGuard Quota Page	Replacement HTML for FortiGuard web filter quota exceeded block page.
	FortiGuard Warning Page	Replacement HTML for FortiGuard web filter warning page.

Category	Messages	Description
FTP	Archive Block Message	Replacement text for FTP archive file block message.
	AV Engine Load Error Block Message	Replacement text for FTP blocked because the antivirus engine failed to load.
	Block Message	Replacement text for FTP permission-denied block message.
	DLP Ban Message	Replacement text for FTP data-leak detected ban message.
	Explicit Banner Message	Replacement text for explicit FTP proxy banner message.
	File Size Block Message	Replacement text for FTP oversized file block message.
HTTP	AntiPhish Block Message	Replacement HTML for AntiPhish credential block message.
	Archive Block Message	Replacement HTML for HTTP archive block message.
	Block Message	Replacement HTML for HTTP file block message.
	Blocked Certificate Message	Replacement HTML for blocked certificate message.
	Content Block Message	Replacement HTML for HTTP content-type block message.
	Content Block Page	Replacement HTML for HTTP file content block page.
	Content Upload Block Page	Replacement HTML for HTTP file upload content block page.
	DLP Ban Message	Replacement HTML for HTTP data-leak detected ban message.
	Invalid Certificate Message	Replacement HTML for HTTP invalid certificate message.
	Oversized File Message	Replacement HTML for HTTP oversized file block message.
	Oversized Upload Message	Replacement HTML for HTTP oversized file upload block message.
	POST Block Message	Replacement HTML for HTTP POST block message.
	Previously Infected Block Page	Replacement HTML for HTTP URL previously infected block page.
	Switching Protocols Blocked	Replacement HTML for HTTP Switching Protocols Blocked page.
	Untrusted Certificate Message	Replacement HTML for untrusted certificate message.
	Upload Archive Block Message	Replacement HTML for HTTP archive upload block message.
	Upload Block Message	Replacement HTML for HTTP file upload block message.
	URL Block Page	Replacement HTML for HTTP URL blocked page.
	URL Filter Error Message	Replacement HTML for HTTP web filter service error message.

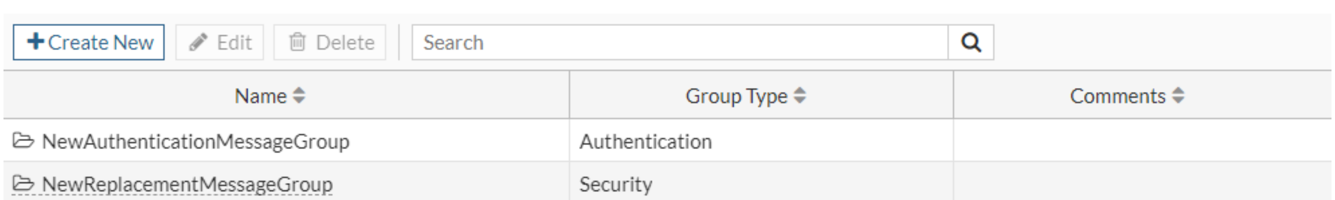
Category	Messages	Description
ICAP	icap-req-resp	Replacement HTML for HTTP POST action block message.
	ICAP REQMOD Response	Replacement message for ICAP REQMOD Response.
	icap-server-service	Replacement HTML for HTTP service action block message.
Network Quarantine	Network Quarantine Administrative Block Page	Replacement HTML for network quarantine administrative block page.
	Network Quarantine Application Block Page	Replacement HTML for network quarantine application block page.
	Network Quarantine AV Block Page	Replacement HTML for network quarantine antivirus block page.
	Network Quarantine DLP Block Page	Replacement HTML for network quarantine DLP block page.
	Network Quarantine DOS Block Page	Replacement HTML for network quarantine DOS block page.
	Network Quarantine IPS Block Page	Replacement HTML for network quarantine IPS block page.
NNTP	NNTP AV Engine Load Error Block Message	Replacement text for NNTP article blocked because the antivirus engine failed to load.
	NNTP Decompressed File Oversize Block Message	Replacement text indicating the removal of an oversized decompressed file.
	NNTP DLP Ban Message	Replacement text for NNTP user banned by data leak prevention.
	NNTP DLP Block Message	Replacement text for body of NNTP message blocked by data leak prevention.
	NNTP DLP Block Subject	Replacement text for subject of NNTP message blocked by data leak prevention.
	NNTP File Size Block Message	Replacement text for NNTP article too large block message.

Category	Messages	Description
Security	Application Control Block Page	Replacement HTML for Application Control block page.
	DLP Block Message	Replacement text for DLP block message.
	DLP Block Page	Replacement HTML for DLP block page.
	IPS Scan Failure Block Page	Replacement HTML for IPS scan failure block page.
	IPS Sensor Block Page	Replacement HTML for IPS sensor block page.
	Virus Block Message	Replacement text for antivirus block message.
	Virus Block Page	Replacement HTML for antivirus block page.
	Virus Upload Block Page	Replacement HTML for virus infected file upload block page.
	Web Application Firewall Block Page	Replacement HTML for web application firewall block page.
	Windows Executable Block Page	Replacement text for blocked Windows executables.
Spam	ASE Block Message	Replacement text for emails blocked due to detection by Advanced Antispam Engine (ASE).
	Banned Word Block Message	Replacement text for emails blocked due to prohibited content (banned words) in message.
	DNSBL Block Message	Replacement text for emails blocked due to detection by antispam DNSBL.
	False-Positive Submit Message	Replacement text for email submit message as false-positive message.
	FortiGuard Block Message	Replacement text for emails blocked due to IP blacklist by FortiGuard.
	HELO Block Message	Replacement text for emails blocked due to HELO check.
	IP Blacklist Message	Replacement text for emails blocked due to blacklisted sending IP addresses.
	MIME Header Block Message	Replacement text for emails blocked due to invalid MIME header.
	Reverse DNS Block Message	Replacement text for emails blocked due to invalid return domain.
	Sender Address Block Message	Replacement text for emails blocked due to blacklisted sender address.

Category	Messages	Description
SSL-VPN	Hostcheck Error Message	Replacement text for host-checking error message.
	SSL-VPN Limit Page	Replacement HTML for SSL-VPN connection limit exceeded page.
	SSL-VPN Login Page	Replacement HTML for SSL-VPN login page.
	SSL-VPN Portal Header	Replacement HTML for SSL-VPN portal page header.
	SSL-VPN Provision User Email	Replacement HTML for SSL-VPN provision user email template
	SSL-VPN Provision User SMS	Replacement text for SSL-VPN provision user SMS template
Traffic Quota	Traffic Quota Limit Exceeded Page	Replacement HTML for traffic quota limit exceeded block page.
Web-proxy	Web-proxy Authentication Failed Page	Replacement HTML for web-proxy authentication failed page.
	Web-proxy Authorization Failed Page	Replacement HTML for web-proxy authorization failed page.
	Web-proxy Block Page	Replacement HTML for web-proxy block page.
	Web-proxy Challenge Page	Replacement HTML for web-proxy authentication required block page.
	Web-proxy HTTP Error Page	Replacement HTML for web-proxy HTTP error page.
	Web-proxy IP Blackout Page	Replacement HTML for web-proxy IP Blackout page.
	Web-proxy User Limit Page	Replacement HTML for web-proxy user limit block page.
	Web-proxy ZTNA block page	Replacement HTML for web-proxy ZTNA block page.

Replacement Message Groups

Go to *System > Replacement Message Groups* to configure custom replacement message groups.



To create a custom replacement message group in the GUI:

1. Click *Create New*.
2. In the *Name* field, enter a name for the custom replacement message group.

3. In the *Comments* field, enter an optional description of the custom replacement message group.
4. Select *Security* or *Authentication*.
5. Click *OK*.

To create a custom replacement message group in the CLI:

```
config system replacemsg-group
    edit <name>
        set comment <string>
        set group-type {utm | auth}
        config {webproxy | auth}
            edit <msg-type>
                set buffer <string>
                set header {none | http | 8bit}
                set format {none | text | html}
            next
        end
    next
end
```

Custom ZTNA virtual host replacement message

Custom messages can be configured for each ZTNA virtual host, to be shown when verification fails. The ZTNA detail tag (`%%ZTNA_DETAIL_TAG%%`) can be included to show the reason for the verification failure.

To use a custom replacement message:

1. Configure a replacement message group that includes the ZTNA detail tag in the message:

```
config system replacemsg-group
    edit "test-vhost"
        set comment ''
        set group-type utm
        config webproxy
            edit "ztna-block"
                set buffer "This is a test message: %%ZTNA_DETAIL_TAG%%"
                set header http
                set format html
            next
        end
    next
end
```

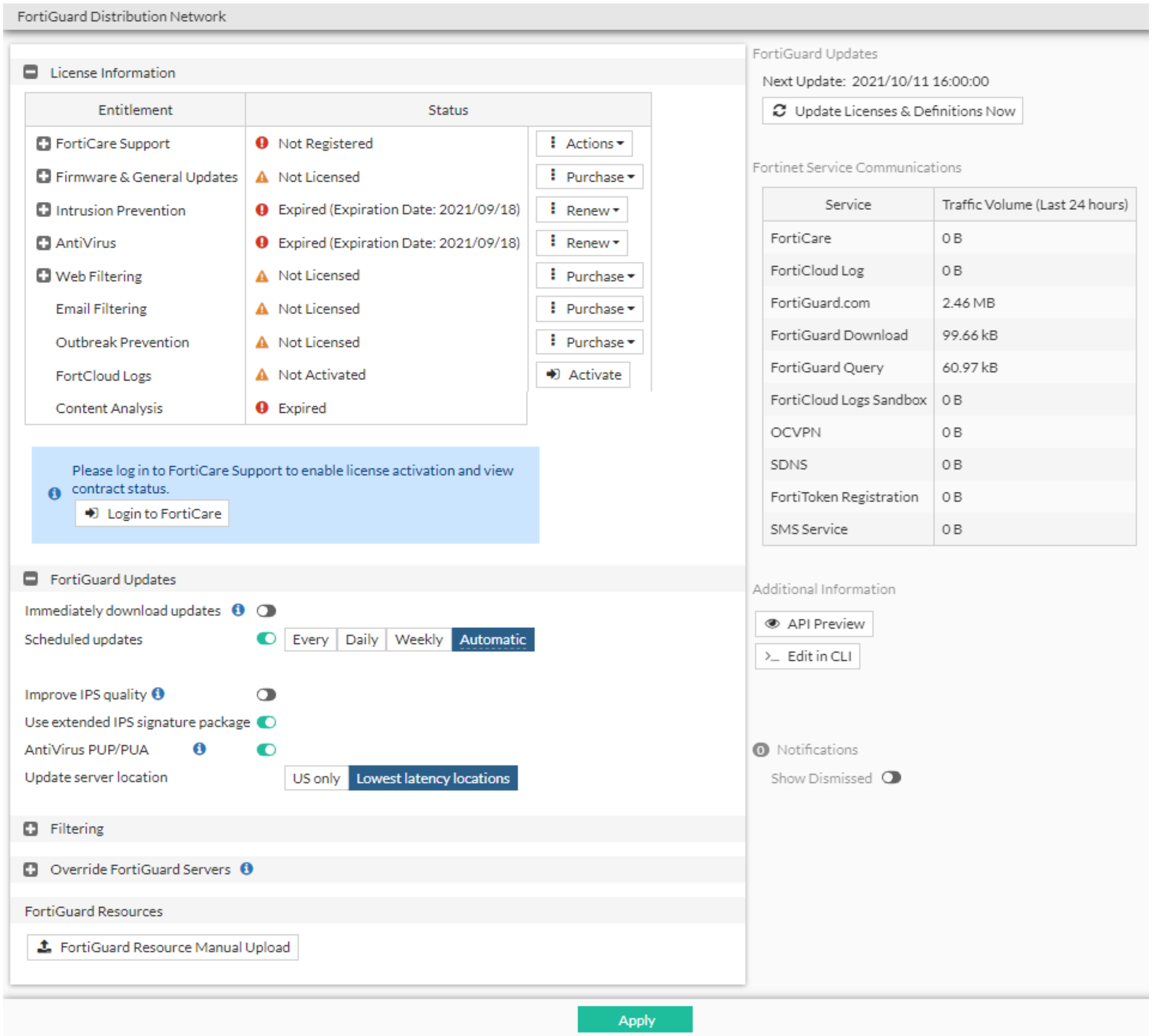
2. Apply the replacement message group to a virtual host:

```
config firewall access-proxy-virtual-host
    edit "test"
        set host "10.1.200.102"
        set replacemsg-group "test-vhost"
    next
end
```

FortiGuard

The *FortiGuard Distribution Network* page provides information and configuration settings for FortiGuard subscription services. For more information about FortiGuard services, see FortiGuard Labs.

To view and configure FortiGuard connections, go to *System > FortiGuard*.



Configure the following settings and select *Apply*:

FortiCare Support	The availability or status of your unit's support contract. The status can be *Unreachable*, *Not Registered*, or *Valid Contract*. Select *Launch Portal* to log in to FortiCloud.

	You can update your registration status by selecting *Register* and loading the license file from a location on your management computer.
Application Control Signatures	Application Control is a free FortiGuard service. Application Control allows you to identify and control applications on networks and endpoints regardless of port, protocol, and IP address used. It gives you unmatched visibility and control over application traffic, even traffic from unknown applications and sources. Although the Application Control profile can be used for free, signature database updates require a valid FortiGuard subscription. To update the database of Application Control signatures, select *Upgrade Database*.
IPS	The FortiGuard Intrusion Prevention System (IPS) uses a customizable database of more than 4000 known threats to stop attacks that evade conventional firewall defenses. It also provides behavior-based heuristics, enabling the system to recognize threats when no signature has yet been developed. It also provides more than 1000 application identity signatures for complete Application Control. To update the IPS database, select *Upgrade Database*.
AntiVirus	The FortiGuard AntiVirus Service provides fully automated updates to ensure protection against the latest content level threats. It employs advanced virus, spyware, and heuristic detection engines to prevent both new and evolving threats from gaining access to your network and protects against vulnerabilities. To update the antivirus database, select *Upgrade Database*.
Industrial DB	The FortiGuard Industrial Security Service provides in-line protection and proactive filtering of malicious and unauthorized network traffic; it enforces security policies tailored to industrial environments, protocols, and equipment. To update the industrial database, select *Upgrade Database*.
Web Filtering	Web Filtering provides Web URL filtering to block access to harmful, inappropriate, and dangerous web sites that may contain phishing/pharming attacks, malware such as spyware, or objectionable content that can expose your organization to legal liability. Based on automatic research tools and targeted research analysis, real-time updates enable you to apply highly-granular policies that filter web access based on 78 web content categories, over 45 million rated web sites, and more than two billion web pages—all continuously updated.
Virtual Machine	To upload or check your virtual machine license, select *FortiProxy VM License*.
Content Analysis	FortiGuard Content Analysis Service is a licensed feature for the real-time analysis of images to detect adult content. Detection of adult content in images uses various patented techniques (not just color-based), including limb and body part detection, body position, and so on. When adult content is detected, such content can be optionally blocked or reported.
Antivirus & IPS Updates	
Accept push updates	Enable to allow updates sent automatically to your FortiProxy. New definitions are added as soon as they are released by FortiGuard. If a specific override push IP address is required, select *Use override push IP* and enter an IP address and port number in the required fields.
Use override push	This option is available only when *Accept push updates* is enabled.

	Enable to configure an override server if you cannot connect to the FDN or if your organization provides updates using their own FortiGuard server. Enter the IP address and port of the NAT device in front of your FortiProxy. FDN connects to this device when attempting to reach the FortiProxy. The NAT device must be configured to forward the FDN traffic to the FortiProxy unit on UDP port 9443.
Scheduled Updates	Enable to receive scheduled updates and then select when the updates occur: *Every* 1-23 hours, *Daily* at a specific hour, or *Weekly* on a specific day at a specific hour.
Improve IPS quality	Enable to help Fortinet maintain and improve IPS signatures. The information sent to the FortiGuard servers when an attack occurs and can be used to keep the database current as variants of attacks evolve.
Use extended IPS signature package	Some models have access to an extended IPS database.
Update AV & IPS Definitions	Select to manually initiate an FDN update.
Update Server Location	
US only/Lowest latency locations	Select whether to access FortiGuard servers within the United States or the quickest FortiGuard servers.
Filtering	
Web Filter Cache	Enable the web filter cache. Enter the number of minutes the FortiProxy unit stores blocked IP addresses or URLs locally, saving time and network access traffic by not checking the FortiGuard server. After the specified time, the FortiProxy unit contacts the FDN server to verify a web address.
Clear Web Filter Cache	Select to manually delete the contents of the web filter cache.
FortiGuard Filtering Protocol	Select the protocol to use to contact the FortiGuard servers, either *HTTPS* or *UDP*.
FortiGuard Filtering Port	Select the port assignments for contacting the FortiGuard servers, either the default port (53) or the alternate port (8888).
Filtering Services Availability	Indicates the status of filtering service. Select *Check Again* if the filtering service is not available and then click *OK* in the confirmation dialog box. A warning is displayed if the FortiProxy unit does not have a valid license.
Request re-evaluation of a URL's category	Select to re-evaluate a URL’s category rating using the Fortinet Live URL Rating Support (opens in a new browser window).
Override FortiGuard Servers	By default, the FortiProxy unit updates signature packages and queries rating servers using public FortiGuard servers. You can override this list of servers. You can also disable communication with public FortiGuard servers.
Create New	Select to display the *Create New Override FortiGuard Server* page.

Edit	Select a server in the list and click *Edit* to display the *Edit Override FortiGuard Server* page.
Delete	Select a server in the list and select *Delete* to remove one of the servers in the list. To remove multiple servers, select multiple rows in the list by holding down the Ctrl or Shift keys and then select *Delete*.

Setting automatic updates for FortiGuard packages

The default auto-update schedule for FortiGuard packages has been updated. Previously, the frequency was a reoccurring random interval within two hours. You can select an update frequency of `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
```

FortiGuard Outbreak Prevention

FortiGuard Virus Outbreak Protection Service (VOS) allows the FortiProxy antivirus database to be subsidized with third-party malware hash signatures curated by FortiGuard. The hash signatures are obtained from FortiGuard's Global Threat Intelligence database. The antivirus database queries FortiGuard with the hash of a scanned file. If FortiGuard returns a match, the scanned file is deemed to be malicious. Enabling the AV engine scan is not required to use this feature.

NOTE: The FortiProxy unit must be registered with a valid FortiGuard outbreak prevention license.

To verify FortiGuard antivirus license information:

Go to *System* > *FortiGuard* and locate the *Outbreak Prevention* section in the *License Information* table.

To enable FortiGuard outbreak prevention:

1. Go to *Security Profiles* > *AntiVirus*.
2. Edit an antivirus profile or create a new one.
3. Under *Outbreak Protection*, enable *Block* or *Monitor* for each protocol.
4. Click *OK*.

Antiphish pattern database

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:

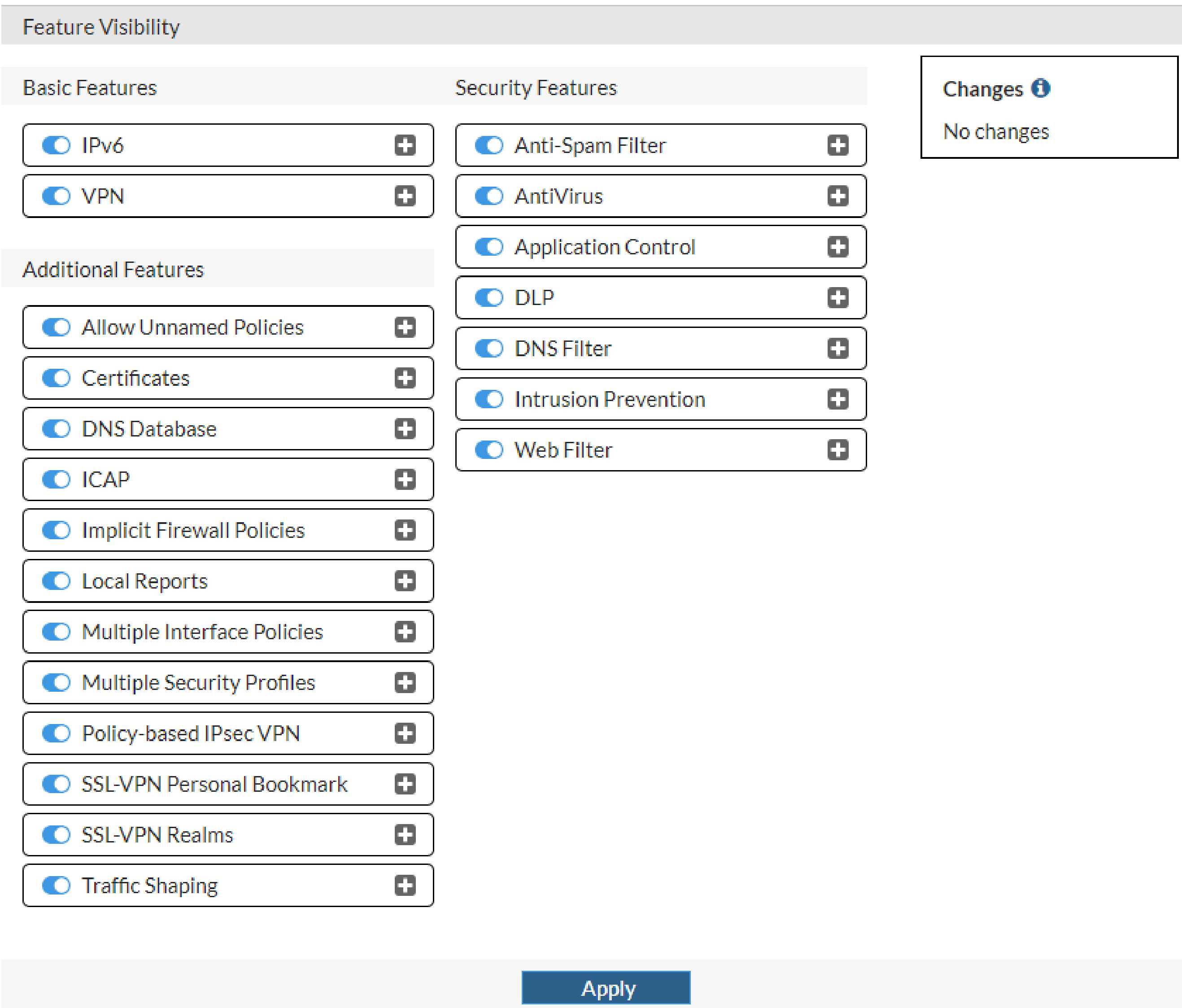
```
# diagnose autoupdate versions
...
AntiPhish Pattern DB
```

```
---------
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
```

Feature Visibility

Various FortiProxy features can be enabled or disabled as required. Disable features are not shown in the GUI.

Go to *System > Feature Visibility* to configure which features are available.



The following options can be turned on or off by toggling the sliders:

IPv6	Allows you to configure the following IPv6 features from the GUI: network interface addresses, trusted hosts for administration, static routes, policy routes, security policies, and firewall addresses.
VPN	Creates secure communication channels between networks and allows remote users to safely connect to secure private networks using SSL-VPN, IPsec VPN, and FortiClient. Adds the *VPN > IPsec Tunnels* and *VPN > SSL-VPN Settings* menus.
Allow Unnamed Policies	Relaxes the requirement for every policy to have a name when created in GUI.
Certificates	Controls the visibility of the *System > Certificates* menu. Allows you to change the certificates used for SSL inspection, SSL load balancing, SSL-VPN, IPsec VPN, and authentication. If *Certificates* is not enabled, default FortiProxy certificates are used.
ICAP	Controls the visibility of the *Content Analyses > ICAP Profile*, *Content Analyses > ICAP Remote Servers*, and *Content Analyses > ICAP Local Servers* pages. Allows you to offload services to an external server. These services can include: ad insertion, virus scanning, content and language translation, HTTP header or URL manipulation, and content filtering. You can also use this feature to set up profiles and add them to security policies.
Local Reports	Controls whether you cna view PDF security reports in the GUI.
Implicit Firewall Policies	Firewall policy lists end with an implicit policy that denies all traffic. Enable this feature to see these policies on firewall policy lists in the GUI. You can edit an implicit policy and enable logging to record log messages when the implicit policy denies a session.
Multiple Interface Policies	Allows the configuration of policies with multiple source/destination interfaces.
Multiple Security Profiles	Allows you to create more than one antivirus profile, web filter profile, application sensor, IPS sensor, antispam profile, DLP sensor, VoIP profile (if enabled), and ICAP profile (if enabled). You can also select the individual UTM profiles in security policies. Enable multiple UTM profiles if you need different levels of UTM protection for different traffic streams.
Policy-based IPsec VPN	Configures policy-based IPsec tunnels. When enabled, an option is added when creating phase 1 IPsec tunnels to determine if they are interface based or policy based. There will also be an option added under *Policy & Objects > Policy* to select IPsec as a subtype for VPN policies, and an option to select the IPsec tunnel to use.
SSL-VPN Personal Bookmark	Allows you to view personal bookmarks added by SSL-VPN users to their portal pages. Adds the *VPN > SSL-VPN Personal Bookmarks* menu. Also allows you to delete users' personal bookmarks.
SSL-VPN Realms	Allows you to create customized realms for different SSL-VPN users and groups. Adds the *VPN > SSL-VPN Realm*s menu. Allows you to associate realms with users and groups in the Authentication/Portal Mapping table under *VPN > SSL-VPN Settings*.

Traffic Shaping	Allows you to configure policies to define how specific types of traffic are shaped by the FortiProxy unit.
Anti-Spam Filter	Controls the visibility of the *Security Profiles > Anti-Spam* menu. Allows you to detect and filter spam. Set up anti-spam profiles (under *Security Profiles > Anti-Spam*) and add them to firewall policies. Some features require a subscription to FortiGuard Anti-Spam.
AntiVirus	Controls the visibility of the *Security Profiles > AntiVirus* menu. Allows you to remove viruses, analyze suspicious files with FortiSandbox, and apply botnet protection to network traffic. Set up antivirus profiles (*Security Profiles > AntiVirus*) and add them to firewall policies. This feature requires a subscription to FortiGuard AntiVirus.
Application Control	Controls the visibility of the *Security Profiles > Application Control* menu. Allows you to visualize and control the applications on your network. Set up application sensors (under *Security Profiles > Application Control*) and add them to firewall policies. This feature requires a subscription to Application Control Signatures.
DLP	Controls the visibility of the *Security Profiles > Data Leak Prevention* menu. Allows you to prevent sensitive data, like credit card and social security numbers, from leaving or entering your network. Set up DLP sensors (under *Security Profiles > Data Leak Prevention*) and add them to firewall policies.
DNS Filter	Controls the visibility of the *Security Profiles > DNS Filter* menu. Allows you to apply DNS category filtering, URL filtering to control a user's access to web resources. Set up DNS filter profiles (under *Security Profiles > DNS Filter*) and add them to firewall policies or add them to a DNS server on a FortiProxy interface. Some features require a subscription to FortiGuard Web Filtering.
Intrusion Prevention	Controls the visibility of the *Security Profiles > Intrusion Prevention* menu. Allows you to detect and block network-based attacks. You can set up IPS sensors (under *Security Profiles > Intrusion Prevention*) and add them to security policies. This feature requires a subscription to FortiGuard IPS.
Web Filter	Controls the visibility of the *Security Profiles > Web Filter* menu. Allows you to apply web category filtering, URL filtering, and content filtering to control user's access to web resources. You can set up web filter profiles (*Security Profiles > Web Filter*) and add them to firewall policies. Some features require a subscription to FortiGuard Web Filtering.

Certificates

FortiProxy uses three types of certificates:

- **Local**: Local certificates are issued for a specific server or web site. They are usually very specific, and often for an internal enterprise network.
- **CA**: External CA certificates are similar to local certificates, but apply to a broader range of addresses or to whole

company. A CA certificate would be issued for an entire web domain, instead of just a single web page.
- **Remote**: Remote certificates are public certificates without private keys.

The FortiProxy unit generates a certificate request based on the information entered to identify the FortiProxy unit. After generating a certificate request, it can be downloaded and then forward to a CA.

The certificate page also enables you to export certificates for authentication, importing, and viewing.

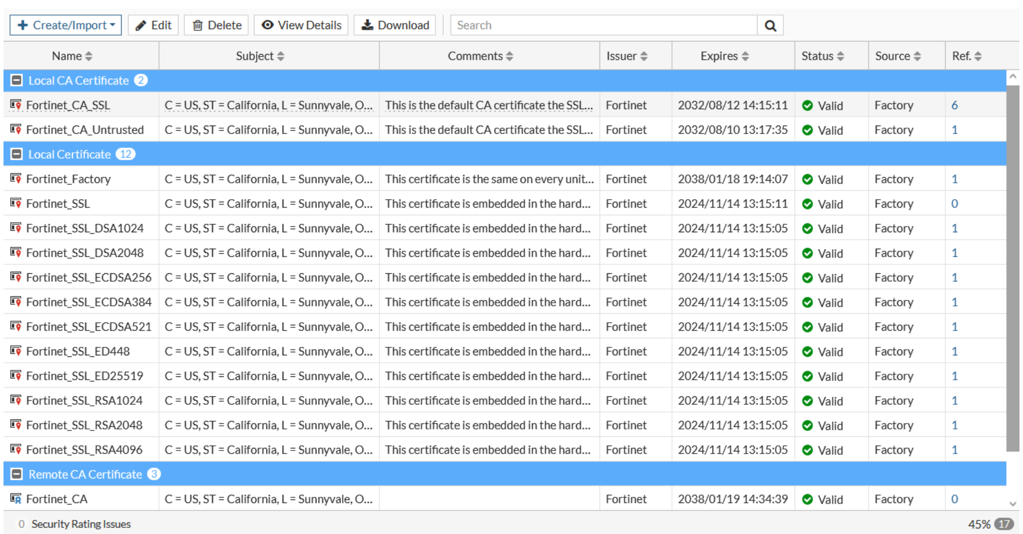
The certificates feature is hidden by default in FortiProxy. In the GUI, go to *System* > *Feature Visibility* and enable *Certificates*.

The following topics provide information about certificates:

- Certificate list on page 509
- Certificate Signing Requests on page 510
- Import a local certificate on page 513
- Import a CA certificate on page 516
- Upload a remote certificate on page 516
- Import a CRL on page 516
- View certificate details on page 517
- Default certificate authority on page 517

Certificate list

To see a list of certificates that have been imported, go to *System* > *Certificates*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create Import	• Create or import a local certificate (see Import a local certificate on page 513) • Generate a CSR (see Certificate Signing Requests on page 510) • Import a CA certificate (see Import a CA certificate on page 516)

	• Upload a remote certificate (see Upload a remote certificate on page 516) • Import a CRL (see Import a CRL on page 516)
Edit	Highlight a certificate and select to edit the certificate comments. This command is only available on some certificates.
Delete	Select a certificate and select *Delete* to remove the selected certificate or CSR. Click *OK* in the confirmation dialog box to proceed with the delete action. To remove multiple certificates or CSRs, select multiple rows in the list by holding down the Ctrl or Shift keys and then select *Delete*.
View Details	View a certificate. See View certificate details on page 517.
Download	Select a certificate or CSR and then select *Download* to download that certificate or CSR to your management computer.
Search	Enter a search term to search the certificate list.
Name	The name of the certificate.
Subject	The subject of the certificate.
Comments	Comments.
Issuer	The issuer of the certificate.
Expires	Displays the certificate's expiration date and time.
Status	The status of the certificate or CSR. • *OK*: the certificate is okay. • *NOT AVAILABLE*: the certificate is not available, or the request was rejected. • *PENDING*: the certificate request is pending.
Source	The source of a certificate can be *Factory*, *User*, or *FortiGuard*.
Ref.	Displays the number of times the certificate or CSR is referenced to other objects. To view the location of the referenced object, select the number in *Ref.*, and the *Object Usage* window appears displaying the various locations of the referenced object.

Certificate Signing Requests

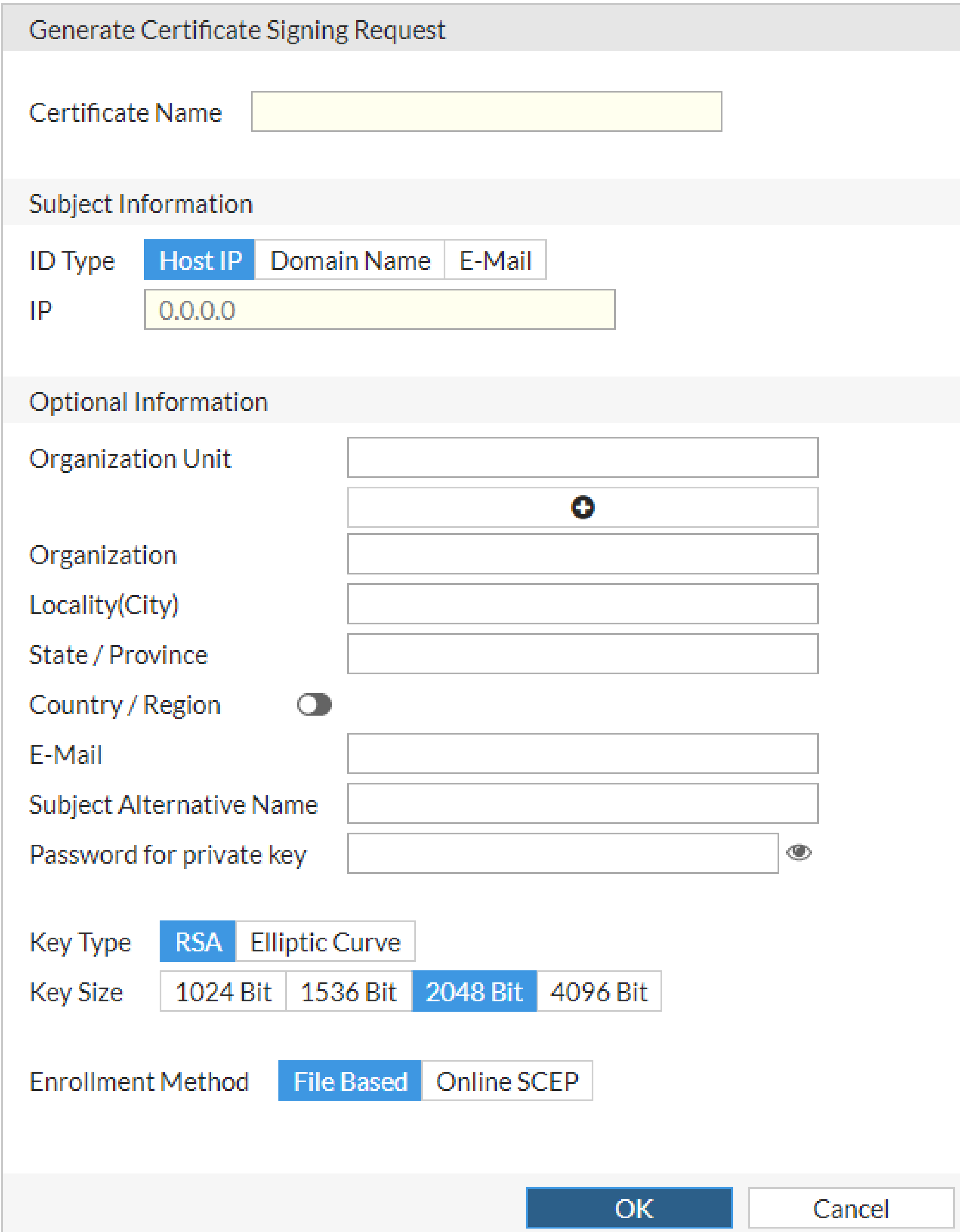
Whether you create certificates locally or obtain them from an external certificate service, you need to generate a Certificate Signing Request (CSR).

When a CSR is generated, a private and public key pair is created for the FortiProxy unit. The generated request includes the public key of the device, and information such as the unit's public static IP address, domain name, or email address. The device's private key remains confidential on the unit.

After the request is submitted to a CA, the CA verifies the information and register the contact information on a digital certificate that contains a serial number, an expiration date, and the public key of the CA. The CA then signs the certificate, after which you can install the certificate on the FortiProxy device.

To generate a CSR:

1. Go to *System* > *Certificates* and click *Create/Import* > *Generate CSR*. The *Generate Certificate Signing Request* page opens.



2. Enter the following information:

Certificate Name	Enter a unique name for the certificate request, such as the host name or the serial number of the device. Do not include spaces in the certificate to ensure compatibility as a PKCS12 file.
Subject Information	Select the ID type: • *Host IP*: Select if the unit has a static IP address. Enter the device’s IP address in the *IP* field. • *Domain Name*: Enter the device’s domain name or FQDN in the *Domain Name* field. • *E-mail*: Enter the email address of the device’s administrator in the *E-mail* field.
Optional Information	Optional information to further identify the device.
Organization Unit	Enter the name of the department. Up to 5 OUs can be added.
Organization	Enter the legal name of the company or organization.
Locality (City)	Enter the name of the city where the unit is located.
State/Province	Enter the name of the state or province where the unit is located.
Country/Region	Enable and then enter the country where the unit is located. Select from the drop-down list.
E-Mail	Enter the contact email address.
Subject Alternative Name	Enter one or more alternative names, separated by commas, for which the certificate is also valid. An alternative name can be: email address, IP address, URI, DNS name, or a directory name. Each name must be preceded by its type, for example: IP:1/2/3/4, or URL: http://your.url.here/.
Password for private key	Enter a password for the private key.
Key Type	Select *RSA* or *Elliptic Curve*. The default is *RSA*.
Key Size	If you selected *RSA* for the *Key Type*, select the key size: *1024 Bit*, *1536 Bit*, *2048 Bit*, or *4096 Bit*. The default is *2048 Bit*. Larger key sizes are more secure but slower to generate.
Curve Name	If you selected *Elliptic Curve* for the *Key Type*, select the curve name: *secp256r1*, *secp384r1*, or *secp521r1*.
Enrollment Method	Select the enrollment method. The default is *File Based*. • *File Based*: Generate the certificate request. • *Online SCEP*: Obtain a signed, Simple Certificate Enrollment Protocol (SCEP) based certificate automatically over the network. Enter the CA server URL and challenge password in their respective fields.

3. Click *OK* to generate the CSR.

Import a local certificate

Local certificates are issued for a specific server, or web site. Generally they are very specific, and often for an internal enterprise network. For example, a personal web site for John Smith at www.example.com (such as http://www.example.com/home/jsmith) would have its own local certificate.

These can optionally be just the certificate file or also include a private key file and PEM passphrase for added security.

Signed local certificates can be imported to the FortiProxy unit.

To import a local certificate:

1. Go to *System* > *Certificates* and click *Create/Import* > *Certificate*. The *Import Certificate* page opens.
2. Select the *Type*:
   - If the *Type* is *Local Certificate*, select *Upload* and locate the certificate file on your computer.
   - If the *Type* is *PKCS #12 Certificate*, select *Upload* and locate the certificate with key file on your computer. Select *Change* to enter the password in the *Password* field.
   - If the *Type* is *Certificate*, select *Upload* and locate the certificate file on your computer. Select *Upload* and locate the key file on your computer. Select *Change* to enter the password in the *Password* field.
3. Click *OK* to import the certificate.

ACME certificate support

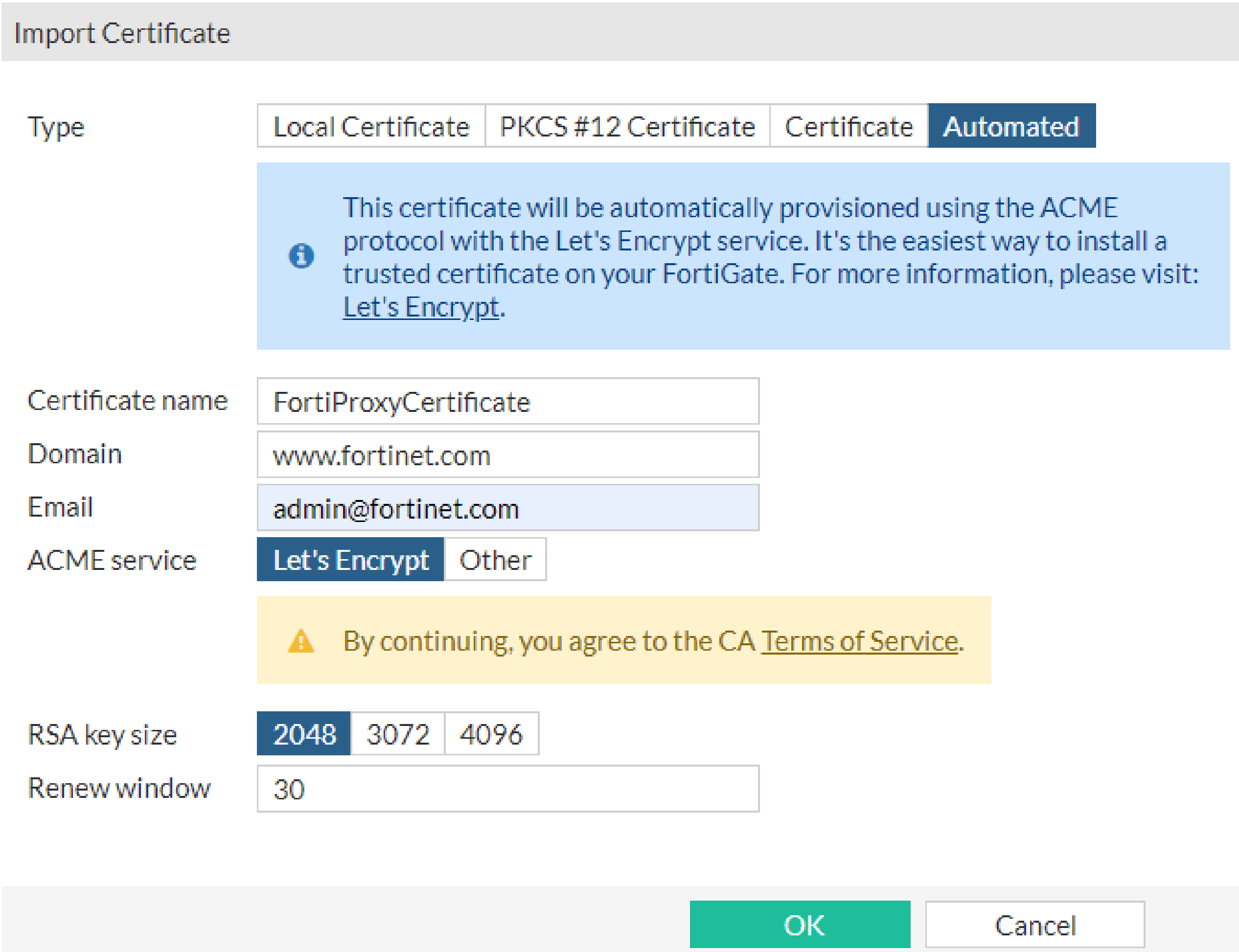
The Automated Certificate Management Environment (ACME), as defined in RFC 8555, is used by the public Let's Encrypt certificate authority (https://letsencrypt.org) to provide free SSL server certificates. The FortiProxy unit can be configured to use certificates that are manged by Let's Encrypt, and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

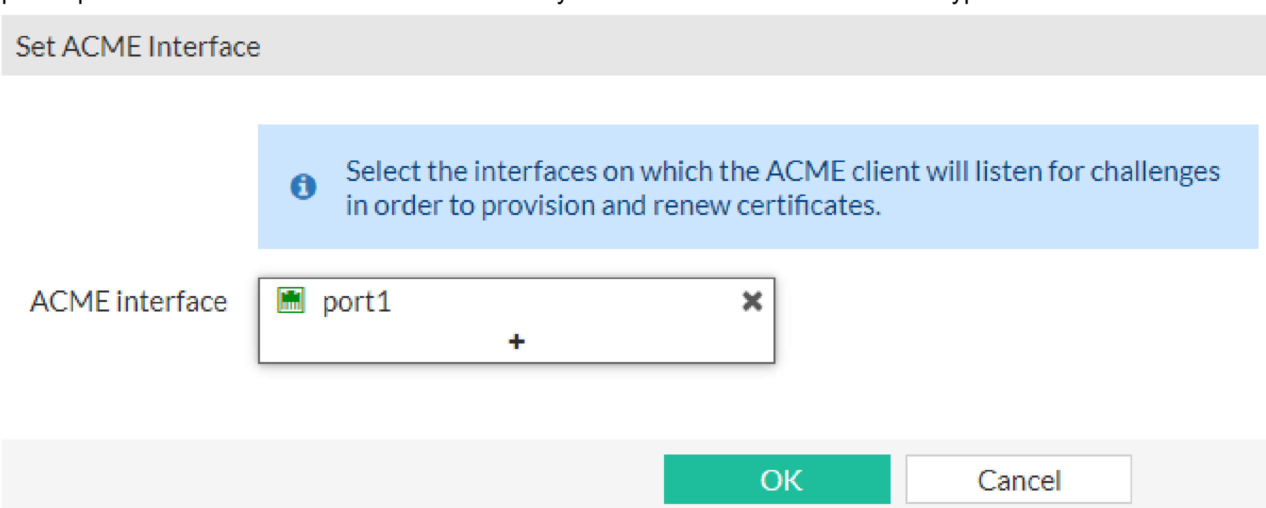
NOTE: To configure certificates in the GUI, go to *System* > *Feature Visibility* and enable *Certificates*.

To import an ACME certificate in the GUI:

1. Go to *System* > *Certificates* and click *Create/Import* > *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.

Import a CA certificate

CA root certificates are similar to local certificates, however they apply to a broader range of addresses or to whole company; they are one step higher up in the organizational chain. Using the local certificate example, a CA root certificate would be issued for all of www.example.com instead of just the smaller single web page.

CA certificates can be imported to the FortiProxy unit.

To import a CA certificate:

1. From the Certificates page, select *Import* > *CA Certificate*. The *Import CA Certificate* page opens.
2. Select the *Type*:
   - If you select *Online SCEP* (Simple Certificate Enrollment Protocol), enter the URL of the SCEP server and optional CA identifier.
   - If you select *File*, select *Upload* and locate the certificate file on your computer.
3. Click *OK* to import the certificate.

Upload a remote certificate

Remote certificates are public certificates without a private key. Remote certificates can be uploaded to the FortiProxy unit.

To upload a remote certificate:

1. From the Certificates page, select *Import* > *Remote Certificate*. The *Upload Remote Certificate* page opens.
2. Select *Upload* and locate the certificate file on your computer.
3. Click *OK* to upload the certificate.

Import a CRL

Certificate revocation list (CRL) is a list of certificates that have been revoked and are no longer usable. This list includes certificates that have expired, been stolen, or otherwise compromised. If your certificate is on this list, it will not be accepted. CRLs are maintained by the CA that issues the certificates and includes the date and time when the next CRL will be issued as well as a sequence number to help ensure you have the most current version of the CRL.

CRLs can be imported to the FortiProxy unit.

To import a certificate revocation list:

1. From the Certificates page, select *Import* > *CRL*. The *Import CRL* page opens.
2. Select *File Based* or *Online Updating*.

If you select *File Based*, select *Upload* and locate the certificate file on your computer. If you select *Online Updating*, configure the following settings:
- *HTTP:* If you enable HTTP updating, enter the URL of the HTTP server.
- *LDAP:* If you enable LDAP updating, select or search for the LDAP server, enter the user name, and select *Change* to enter the password in the *Password* field.
- *SCEP:* If you enable SCEP updating, select a local certificate for SCEP communication for the online CRL and enter the URL of the SCEP server.

3. Click *OK* to import the CRL.

View certificate details

Certificate details can be viewed by selecting a certificate and then selecting *View Details* from the toolbar.

The following information is displayed:

Certificate Name	The name of the certificate.
Serial Number	The serial number of the certificate.
Subject Information	The subject information of the certificate, including: • *Common Name (CN)* • *Organization (O)* • *Organization Unit (OU)* • *Locality (L)* • *State (ST)* • *Country (C)* • *Email Address*
Issuer	The issuer information of the certificate, including most of the information from *Subject Information*.
Validity Period	Displays the *Valid From* and the expiration *Valid To* date of the certificate. The certificate should be renewed before this expiration date.
Fingerprints	The identifying fingerprint of the certificate.
Extension	The certificate extension information.

Select *Close* to return to the certificate list.

Default certificate authority

The default certificate authorities (CA) can be configured. By default, web-proxy and ssl-ssh-profile use the default CAs:

```
config firewall ssl default-certificate
    set default-ca "Fortinet_CA_SSL"
    set default-untrusted-ca "Fortinet_CA_Untrusted"
    set default-server-cert "Fortinet_Factory"
end
```

```
config web-proxy global
    set ssl-cert "default-server-cert"
```

```
    set ssl-ca-cert "default-ca"
end

confir firewall ssl-ssh-profile
    edit 1
        set caname "default-ca"
        set untrusted-caname "default-untrusted-ca"
    next
end
```

The CA can be changed by either changing the default, or by setting a specific CA for the web-proxy or ssl-ssh-profile. For example, to change the web-proxy CAs, but not the defaults:

```
config web-proxy global
    set ssl-cert "Personal_Server_CA"
    set ssl-ca-cert "Personal_CA"
end
```

Integrating FortiFroxy with SafeNet Luna Network HSM

A hardware security module (HSM) is a dedicated device for managing digital keys and performing cryptographic operations. An HSM can be a plug-in card or an external device directly connected to a computer or network server. Purposefully designed to protect the crypto-key life cycle, HSMs have been used by some of the world's most security-conscious entities to protect their cryptographic infrastructure by securely managing, processing, and storing cryptographic keys inside a hardened, tamper-resistant device.

Because of their strengths in securing cryptographic keys and provisioning encryption, decryption, authentication, and digital signing services for a wide range of applications, HSMs have been used by enterprises worldwide to safeguard their online transactions, identities, and applications.

Starting from Version 2.0, FortiProxy has integrated with SafeNet Luna Network HSM. It enables you to retrieve a per-connection, SSL session key from the HSM server instead of loading the private key and certificate stored on FortiProxy. The HSM integration supports active-passive and active-active HA modes but not active-passive configuration synchronization (config-sync). You can sync local certificate using HSM to peer FortiProxy appliances but the local certificate may NOT function properly on peer FortiProxy appliances.

To integrate FortiFroxy with SafeNet Luna Network HSM:

1. Check if the FortiProxy has already registered with the HSM by running the following command on HSM: ssh admin@<hsm_ip>.
   If the FortiProxy IP is listed under the HSM client list, clear up existing configuration by running the following commands:
   - client revokePartition -client <fortiproxy_ip> -partition fortiproxy
   - client delete -client <fortiproxy_ip> -force
2. Create and initialize a new HSM partition that uses password authentication using the partition create command on HSM. HSM partition is a global configuration that can be used from individual VDOMs.

   This is the partition FortiProxy uses on the HSM server. You can create more than one partition, but all the partitions are assigned to the same client. For more information, see SafeNet Luna Network HSM documentation.

3. Retrieve the server certificate file from the HSM server using the SCP utility and the following command:
   ```
   scp <hsm_username>@<hsm_ip>:server.pem /usr/lunasa/bin/server_<hsm_ip>.pem
   ```
4. Configure the HSM by running the `config system nethsm` command on the FortiProxy. You need to specify the HSM server certificate and the partition name/password. See config
   ```
   config system nethsm
      set status enable
      set interface "port1"
      config servers
         edit "us_hsm"
            set server "172.30.30.13"
            set server-cert "copy over the HSM server certificate from previous step"
            set htl disable
      next
   end
      config slots
         edit "fortiproxy"
            set id <partition name on the HSM server>
            set password <partition password on the HSM server>
         next
      end
   end
   ```
   The HSM configuration also generates a default FortiProxy client certificate, which can be displayed by running the `execute nethsm client-cert-show` command. To re-generate the client certificate, run the `execute nethsm client-cert-create` command.
5. Export the FortiProxy client certificate to local PC using the following command: `execute nethsm client-cert-export`.
6. Send the FortiProxy client certificate to the HSM using the SCP utility and the following command:
   ```
   scp <fortiproxy_ip>.pem admin@<hsm_ip>:
   ```
7. Connect to the HSM server using an admin account via SSH and register a client for FortiProxy on the HSM server using the following command:
   `lunash:> client register -c <client_name> -ip <fortiproxy_ip>`, where `<client_name>` is the name you specify that identifies the client.
   You can verify the client registration using the `exe nethsm diagnose` command.
8. Assign the client you registered to the partition you've created in step 2 above using the following command:
   `lunash:> client assignPartition -client <client_name> -partition <partition_name>`
   You can verify the assignment using the following command:
   `lunash:> client show -client <client_name>`
9. Repeat the client assignment process for any additional partitions you've created for FortiProxy.
10. In FortiProxy, generate a certificate-signing request that includes the HSM's configuration information.
    The CSR generation process creates a private key on both the HSM and FortiProxy. The private key on the HSM is the "real" key that secures communication when FortiProxy uses the signed certificate. The key found on the FortiProxy is to indicate the HSM server information when you upload the certificate to FortiProxy.
11. Download the certificate request (`.csr`) file under *System* > *Certificates* > *Local Certificates* in FortiProxy.
12. Upload the certificate request (`.csr`) file to your certificate authority (CA) under *System* > *Certificates* > *Create/Import* > *CA Certificate*. See Import a CA certificate on page 516.
13. Upload the HSM server certificate (that you obtained in step 3) under *System* > *Certificates* > *Create/Import* > *Certificate*. See Import a local certificate on page 513.
14. You can then use the HSM server in a policy or server pool configuration by referencing the HSM certificate.
15. In case of any server or client changes, you must re-configure the FortiProxy-HSM integration which involves deleting the intermediate CA, deleting the server and partitions, and then reset the configuration using the `exe nethsm reset` command on FortiProxy.

16. To configure FortiProxy HA with SafeNet Network HSM, follow the steps below:

   a. Enable HA with HSM by running the following command on the FortiProxy:
```
config system nethsm
set ha enable
```
   b. Disable Network Trust Links (NTLs) IP check (ntls ipcheck) on the HSM server.

   c. Configure multiple HSM servers with the same software version and multiple partitions with the same domain name and password. Refer to the steps above for instructions about creating one single HSM server or partition. Alternatively, use the `config system nethsm` command on the FortiProxy to set up the HA cluster with HSM:
```
config system nethsm
   set ha enable
      config hagroups
         edit "hagroup1"
            set member "partition_1" "partition_2"
         next
      end
   end
end
config slots
   edit “partition_1”
      set id 0
      set password <password>
         next
         edit “partition_2”
            set id 1
            set password <password>
         next
         edit “hagroup1” <<<< virtual slot created by background process, which is
               used to create the CSR>
      set id 5
      set password <password>
   next
end
```
   d. Register each client to all HSM servers. Refer to the steps above for instructions about registering a client to an HSM server.

Security Fabric

The Fortinet Security Fabric provides a visionary approach to security that allows your organization to deliver intelligent, powerful, and seamless security. Fortinet offers security solutions for endpoints, access points, network elements, the data center, applications, cloud, and data, designed to work together as an integrated security fabric that can be integrated, analyzed, and managed to provide end-to-end protection for your network. Your organization can also add third-party products that are members of the Fortinet Fabric-Ready Partner Program to the Security Fabric.

All elements in the Security Fabric work together as a team to share policy, threat intelligence, and application flow information. This collaborative approach expands network visibility and provides fast threat detection in real time and the ability to initiate and synchronize a coordinated response, no matter which part of the network is being compromised. The Security Fabric allows your network to automatically see and dynamically isolate affected devices, partition network segments, update rules, push out new policies, and remove malware.

The Security Fabric is designed to cover the entire attack surface and provide you with complete visibility into your network. It allows you to collect, share, and correlate threat intelligence between security and network devices, centrally manage and orchestrate policies, automatically synchronize resources to enforce policies, and coordinate a response to threats detected anywhere across the extended network. The unified management interface provides you with cooperative security alerts, recommendations, audit reports, and full policy control across the Security Fabric that will give you confidence that your network is secure.

This section describes the following topics:

- Fabric Connectors on page 576
- External Connectors on page 581
- Asset Identity Center on page 585

Automation stitches

Automation stitches automate the activities between the different components in the Security Fabric, which decreases the response times to security events. Events from any source in the Security Fabric can be monitored, and action responses can be set up to any destination.

> Automation stitches can also be used on FortiProxy devices that are not part of a Security Fabric.

An automation stitch consists of two parts: the trigger and the actions. The trigger is the condition or event on the FortiProxy that activates the action, for example, a specific log, or a failed log in attempt. The action is what the FortiProxy does in response to the trigger.

Automation stitches that use cloud-based actions (AWS Lambda, Azure Function, Google Cloud Function, and AliCloud Function) have the option to delay an action after the previous action is completed.

Diagnose commands are available in the CLI to test, log, and display the stitch history and settings.

Automation stitches can only be created on the root FortiProxy in a Security Fabric.

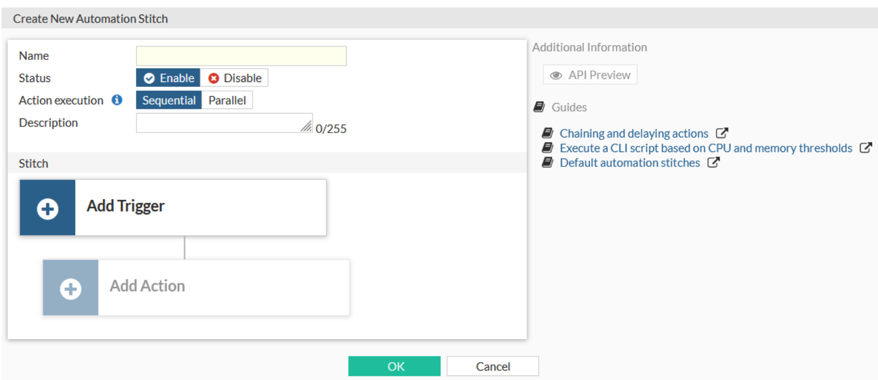
Creating automation stitches

To create an automation stitch, a trigger event and a response action or actions are selected. Automation stitches can be tested after they are created.

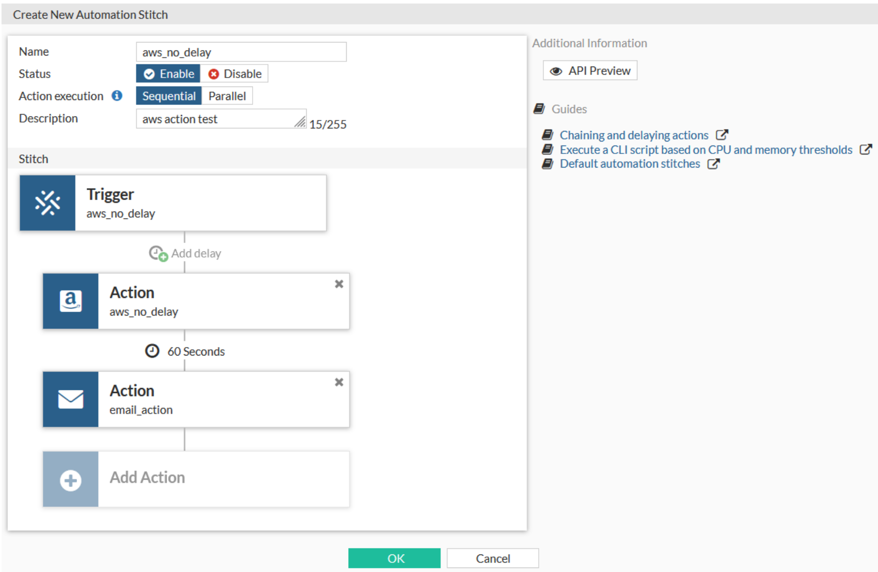
In the GUI, go to *Security Fabric > Automation*, select the *Stitch* tab, and click *Create New*. Automation stitches, actions, and triggers are configured in separate dialogs.

The stitch *Action execution* can be set to either *Sequential* or *Parallel*. In sequential execution, actions will execute one after another with a delay (if specified). If one action fails, then the action chain stops. This is the default setting. In parallel execution, all actions will execute immediately when the stitch is triggered.

When creating a stitch, clicking *Add Trigger* and *Add Action* displays the lists of available triggers and actions, and the option to create new ones.



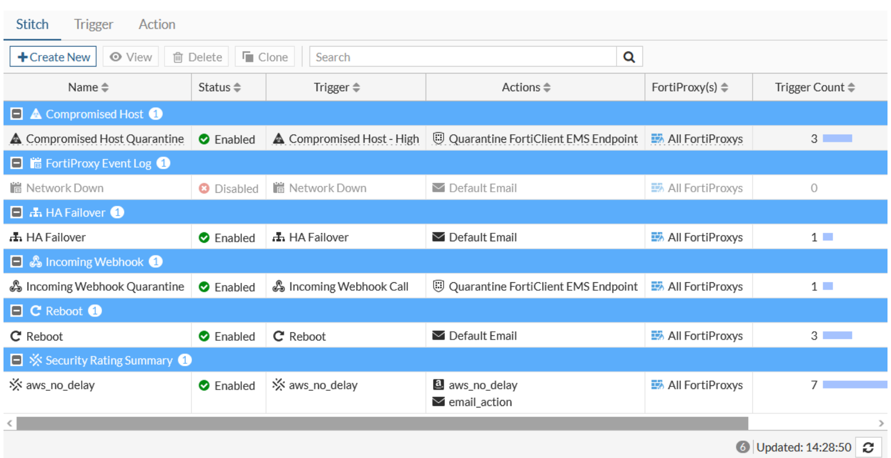
Once the stitch is configured, a process diagram of the trigger, actions, and delays is displayed. A delay can be added before an action if *Sequential* action execution is used. Executing the next action can be delayed by up to 3600 seconds (one hour).



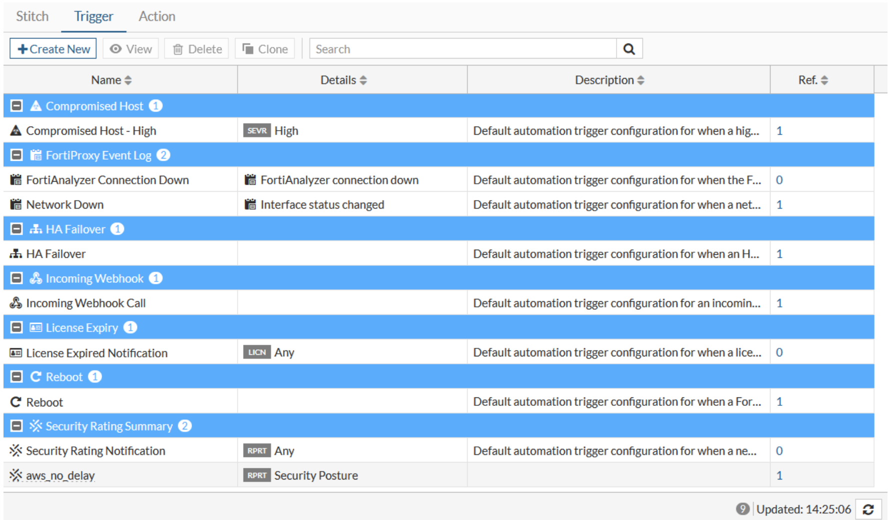
Triggers and actions can be configured separately, and then added to an automation stitch.

Tabs on the Automation page

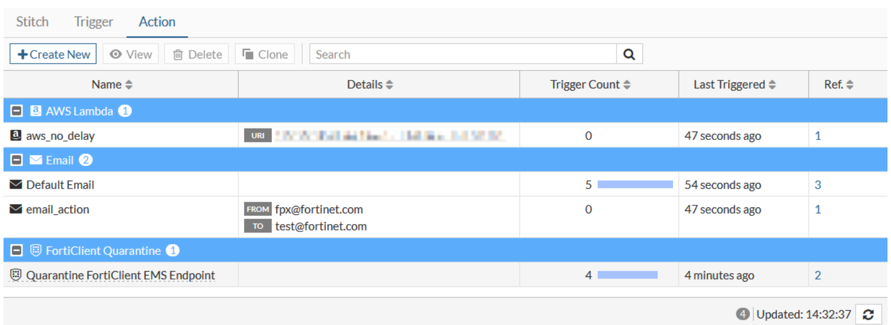
On the *Security Fabric > Automation* page, there are tabs for *Stitch*, *Trigger*, and *Action*. The *Stitch* tab is the default view that lists the trigger and actions used in each stitch. Individual triggers and actions can be created or edited in the corresponding tabs.



Click *Trigger* to view the list of triggers.



Click *Action* to view the list of actions.



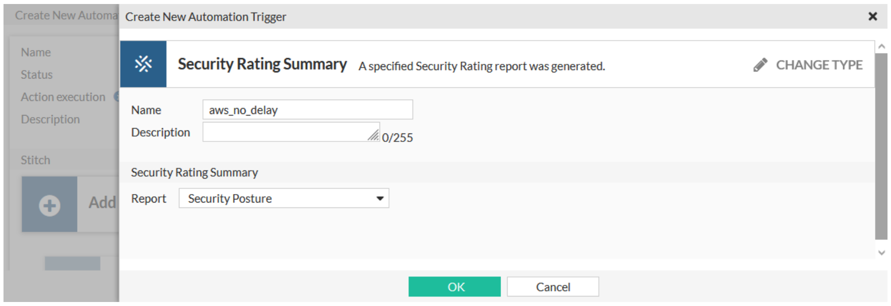
Sample configuration

The following example shows how to configure a Security Rating Summary automation stitch with AWS Lambda and Email actions. There is a 60-second delay before the Email action.

To configure the automation stitch in the GUI:

1. Go to *Security Fabric > Automation*, select the *Stitch* tab, and click *Create New*.
2. Enter the stitch name and description.
3. Configure the trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *Security Rating Summary*.
   c. Enter the following:

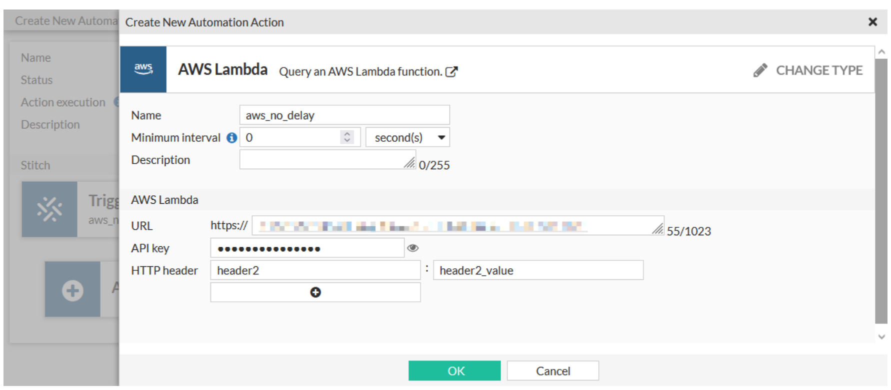
Name	*aws_no_delay*
Report	*Security Posture*



d. Click *OK*.
e. Select the trigger in the list and click *Apply*.

4. Configure the AWS Lambda function action:
   a. Click *Add Action*.
   b. Click *Create* and select *AWS Lambda*.
   c. Enter the following:

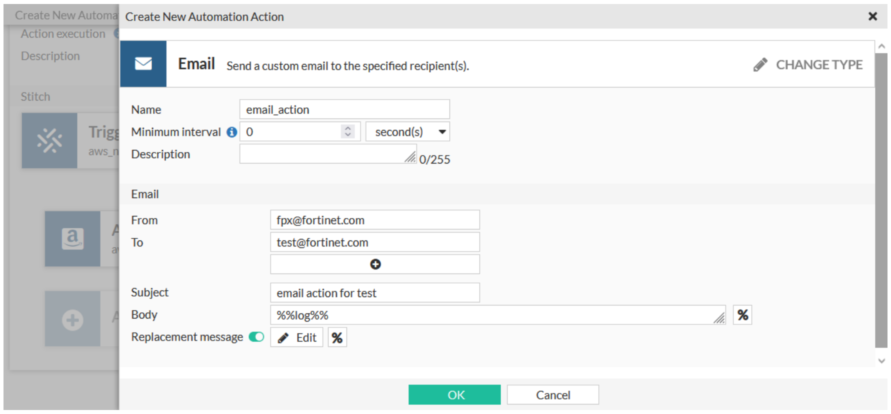
Name	*aws_no_delay*
URL	Enter the request API URI
API key	Enter the API key
HTTP header	*header2 : header2_value*



   d. Click *OK*.
   e. Select the action in the list and click *Apply*.

5. Configure the Email notification action:
   a. Click *Add Action*.
   b. Click *Create* and select *Email*.
   c. Enter the following:

Name	*email_action*
To	Enter an email address
Subject	*email action for test*
Replacement message	Enable



d. Click *OK*.
e. Select the action in the list and click *Apply*.
6. Click the *Add delay* located between both actions. Enter *60* and click *OK*.
7. Click *OK*.

To configure the automation stitch in the CLI:

1. Configure the trigger:

```
config system automation-trigger
    edit "aws_no_delay"
        set event-type security-rating-summary
    next
end
```

2. Configure the actions:

```
config system automation-action
    edit "aws_no_delay"
        set action-type aws-lambda
        set aws-api-key xxxxxxxxxxxx
        set uri "xxxxxxxxxx.execute-api.us-east-1.amazonaws.com/xxxxxxxxxx"
        set headers "header2:header2_value"
    next
    edit "email_action"
        set action-type email
        set email-to "test@fortinet.com"
        set email-from "fpx@fortinet.com"
        set email-subject "email action for test"
        set replacement-message enable
    next
end
```

3. Configure the stitch:

```
config system automation-stitch
    edit "aws_no_delay"
        set description "aws action test"
        set trigger "aws_no_delay"
        config actions
            edit 1
                set action "aws_no_delay"
```

```
                    set required enable
                next
                edit 2
                    set action "email_action"
                    set delay 60
                    set required enable
                next
            end
        next
    end
```

Testing automation stitches

In the GUI, go to *Security Fabric > Automation*, select the *Stitch* tab, right-click on the automation stitch, and select *Test Automation Stitch*.

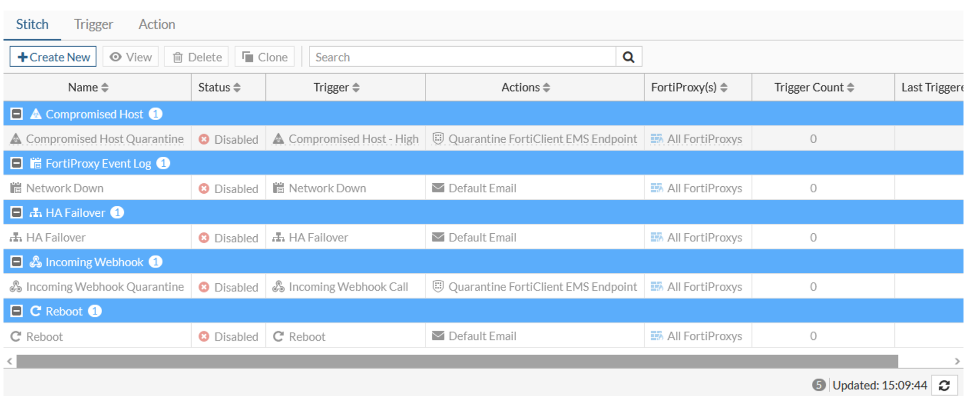
In the CLI, enter `diagnose automation test <automation-stitch name>`.

Default automation stitches

The following default automation stitches are included in FortiProxy:

- Compromised Host Quarantine
- Network Down
- HA Failover
- Incoming Webhook Quarantine
- Reboot

To view and edit the automation stitches in the GUI, go to *Security Fabric > Automation* and select the *Stitch* tab..



CLI configurations

Compromised Host Quarantine

```
config system automation-action
    edit "Quarantine FortiClient EMS Endpoint"
        set description "Default automation action configuration for quarantining a
FortiClient EMS endpoing device."
        set action-type quarantine-forticlient
```

```
    next
end

config system automation-trigger
    edit "Compromised Host - High"
        set description "Default automation trigger configuration for when a high severity
compromised host is detected."
    next
end

config system automation-stitch
    edit "Compromised Host Quarantine"
        set description "Default automation stitch to quarantine a high severity compromised
host on FortiClient EMS."
        set status disable
        set trigger "Compromised Host - High"
        config actions
            edit 1
                set action "Quarantine FortiClient EMS Endpoint"
            next
        end
    next
end
```

Network Down

```
config system automation-action
     edit "Default Email"
        set description "Default automation action configuration for sending an email with
basic information on the log event."
        set action-type email
        set email-subject "%%log.logdesc%%"
    next
end

config system automation-trigger
    edit "Network Down"
        set description "Default automation trigger configuration for when a network
connection goes down."
        set event-type event-log
        set logid 20099
        config fields
            edit 1
                set name "status"
                set value "DOWN"
            next
        end
    next
end

config system automation-stitch
    edit "Network Down"
        set description "Default automation stitch to send an email when a network goes
down."
        set status disable
        set trigger "Network Down"
        config actions
            edit 1
```

```
                set action "Default Email"
            next
        end
    next
end
```

HA Failover

```
config system automation-action
    edit "Default Email"
        set description "Default automation action configuration for sending an email with
basic information on the log event."
        set action-type email
        set email-subject "%%log.logdesc%%"
    next
end
```

```
config system automation-trigger
    edit "HA Failover"
        set description "Default automation trigger configuration for when an HA failover
occurs."
        set event-type ha-failover
    next
end
```

```
config system automation-stitch
    edit "HA Failover"
        set description "Default automation stitch to send an email when a HA failover is
detected."
        set status disable
        set trigger "HA Failover"
        config actions
            edit 1
                set action "Default Email"
            next
        end
    next
end
```

Incoming Webhook Quarantine

```
config system automation-action
    edit "Quarantine FortiClient EMS Endpoint"
        set description "Default automation action configuration for quarantining a
FortiClient EMS endpoing device."
        set action-type quarantine-forticlient
    next
end
```

```
config system automation-trigger
    edit "Incoming Webhook Call"
        set description "Default automation trigger configuration for an incoming webhook."
        set event-type incoming-webhook
    next
end
```

```
config system automation-stitch
    edit "Incoming Webhook Quarantine"
        set description "Default automation stitch to quarantine a provided MAC address on
FortiClient EMS using an Incoming Webhook."
        set status disable
        set trigger "Incoming Webhook Call"
        config actions
            edit 1
                set action "Quarantine FortiClient EMS Endpoint"
            next
        end
    next
end
```

Reboot

```
config system automation-action
    edit "Default Email"
        set description "Default automation action configuration for sending an email with
basic information on the log event."
        set action-type email
        set email-subject "%%log.logdesc%%"
    next
end
```

```
config system automation-trigger
    edit "Reboot"
        set description "Default automation trigger configuration for when a FortiProxy is
rebooted."
        set event-type reboot
    next
end
```

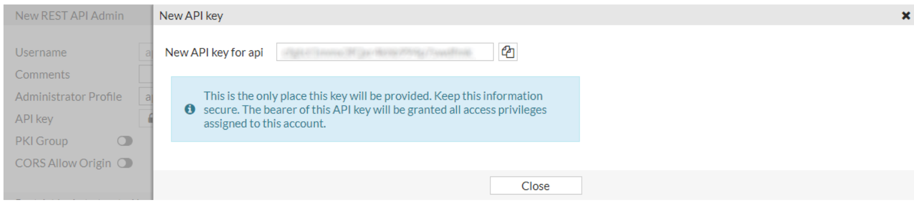
```
config system automation-stitch
    edit "Reboot"
        set description "Default automation stitch to send an email when a FortiProxy is
rebooted."
        set status disable
        set trigger "Reboot"
        config actions
            edit 1
                set action "Default Email"
            next
        end
    next
end
```

Incoming Webhook Quarantine stitch

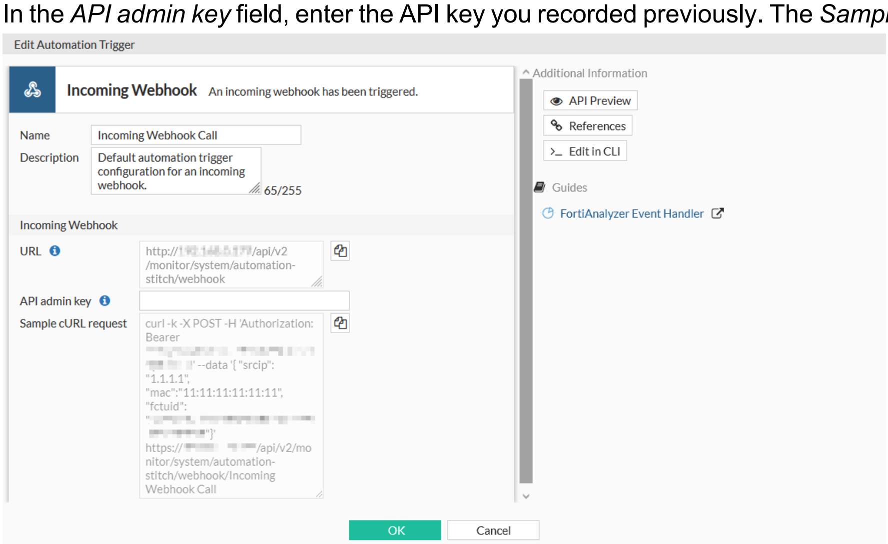
The Incoming Webhook Quarantine stitch for API calls to the FortiProxy accepts multiple parameters (MAC address and FortiClient UUID) from an Incoming Webhook trigger, which enacts either the Access Layer Quarantine action (MAC address) or the FortiClient Quarantine action (FortiClient UUID). This is a default automation stitch included in FortiOS.

To trigger the Incoming Webhook Quarantine stitch in the GUI:

1. Create a new API user:
   a. Go to *System > Administrators*.
   b. Click *Create New > REST API Admin*.
   c. Configure the *New REST API Admin* settings, and copy the API key to the clipboard.



2. Enable the stitch:
   a. Go to *Security Fabric > Automation* and select the *Stitch* tab.
   b. Under *Incoming Webhook*, right-click *Incoming Webhook Quarantine*, and select *Select Status > Enable*.
3. Get the sample cURL request:
   a. Go to the *Trigger* tab.
   b. Under *Incoming Webhook*, right-click *Incoming Webhook Call*, and select *Edit*.
   c. In the *API admin key* field, enter the API key you recorded previously. The *Sample cURL request* field updates.



   d. Copy the *Sample cURL request* to the clipboard.
   e. Click *OK*.
4. Execute the request:
   a. Edit the sample cURL request you just copied.
   b. Add parameters to the `data` field (`"mac"` and `"fctuid"`), and then execute the request.

```
root@pc:~# curl -k -X POST -H 'Authorization: Bearer
cfgtct1mmx3fQxr4khb994p7swdfmk' --data '{ "mac":"0c:0a:00:0c:ce:b0", "fctuid":
"0000BB0B0ABD0D00B0D0A0B0E0F0B00B"}'
https://172.16.116.226/api/v2/monitor/system/automation-
stitch/webhook/Incoming%20Webhook%20Quarantine
{
   "http_method":"POST",
   "status":"success",
   "http_status":200,
```

```
  "serial":"FGT00E0Q00000000",
  "version":"v6.4.0",
  "build":1545
```

Encode spaces in the automation stitch name with `%20`. For example, `Incoming%20Webhook%20Quarantine`

Once the automation stitch is triggered, the MAC address is quarantined by the FortiProxy, and an event log is created. The FortiClient UUID is quarantined on the EMS server side.

To trigger the Incoming Webhook Quarantine stitch in the CLI:

1. Create a new API user and note the API key:

   ```
   config system api-user
   ```

2. Enable the automation stitch:

   ```
   config system api-user
       edit "api"
           set api-key ************
           set accprofile "api_profile"
           set vdom "root"
           config trusthost
               edit 1
                   set ipv4-trusthost 10.6.30.0 200.200.200.0
               next
           end
       next
   end
   ```

3. Edit the cURL request to include parameters in the `data` field (`"mac"` and `"fctuid"`), then execute the request:

   ```
   root@pc56:~# curl -k -X POST -H 'Authorization: Bearer
   cfgtct1mmx0fQxr4khb000p70wdfmk' --data '{ "mac":"0c:0a:00:0c:ce:b0", "fctuid":
   "3000BB0B0ABD0D00B0D0A0B0E0F0B00B"}'
   https://100.10.100.200/api/v2/monitor/system/automation-
   stitch/webhook/Incoming%20Webhook%20Quarantine
   {
     "http_method":"POST",
     "status":"success",
     "http_status":200,
     "serial":"FGT80E0Q00000000",
     "version":"v6.4.0",
     "build":1545
   ```

Encode spaces in the automation stitch name with `%20`. For example, `Incoming%20Webhook%20Quarantine`.

Once the automation stitch is triggered, the MAC address is quarantined by the FortiProxy, and an event log is created. The FortiClient UUID is quarantined on the EMS server side.

Sample log

```
date=2020-02-14 time=15:37:48 logid="0100046600" type="event" subtype="system"
level="notice" vd="root" eventtime=1581723468644200712 tz="-0800" logdesc="Automation
stitch triggered" stitch="Incoming Webhook Quarantine" trigger="Incoming Webhook
Quarantine" stitchaction="Compromised Host Quarantine_quarantine,Compromised Host
Quarantine_quarantine-forticlient" from="log" msg="stitch:Incoming Webhook Quarantine is
triggered."
```

Triggers

The following table outlines the available triggers.

Category	Trigger	Description
Security Fabric		
	Compromised Host	An indicator of compromise (IoC) is detected on a host endpoint. The threat level must be selected and can be *Medium* or *High*. If *Medium* is selected, both medium and high level threats are included. Additional actions are available only for *Compromised Host* triggers: • Access Layer Quarantine • FortiClient Quarantine • VMware NSX Security Tag • IP Ban
	Security Rating Summary	A summary is available for a recently run Security Rating report. Options include: • Security Posture • Fabric Coverage • Optimization • Any
	FortiAnalyzer Event Handler	The specified FortiAnalyzer event handler has occurred.
	Fabric Connector Event	An event has occurred on a specific Fabric connector.
System		
	Reboot	A FortiProxy is rebooting.
	HA Failover	An HA failover has occurred.
	Conserve Mode	A FortiProxy entered conserve mode due to low memory. See Execute a CLI script based on CPU and memory thresholds on page 562 for an example.
	Configuration Change	An administrator's session that changed a FortiProxy's configuration has ended.
	License Expiry	A FortiGuard license is expiring. The license type must be selected. Options include:

Category	Trigger	Description
		• FortiCare Support • FortiGuard Web Filter • FortiGuard AntiSpam • FortiGuard AntiVirus • FortiGuard IPS • FortiGuard Management Service • FortiGate Cloud • Any
	AV & IPS DB Update	The antivirus and IPS database has been updated.
	High CPU	A FortiProxy has high CPU usage. See Execute a CLI script based on CPU and memory thresholds on page 562 for an example.
Miscellaneous		
	FortiProxy Event Log	A specified FortiProxy event log ID has occurred. Multiple event log IDs can be selected, and log field filters can be applied. See FortiProxy event log trigger on page 534 for an example.
	Incoming Webhook	An incoming webhook has been triggered.
	Schedule	A scheduled monthly, weekly, daily, or hourly trigger. Set to occur on a specific minute of an specific hour on a specific day.

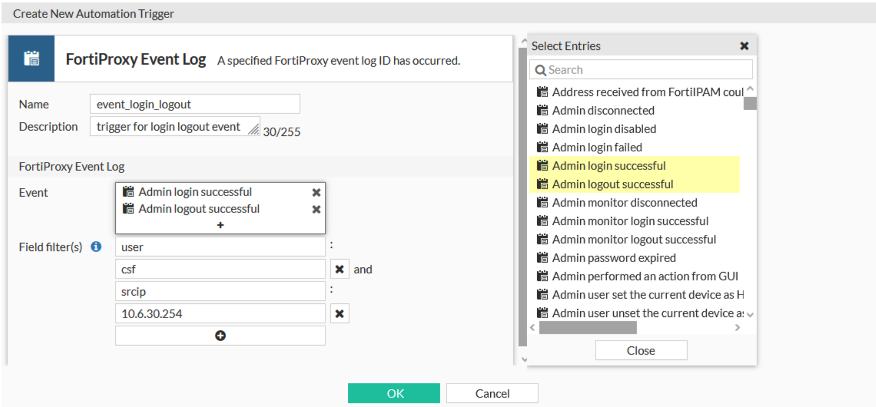
FortiProxy event log trigger

You can configure a FortiProxy event log trigger for when a specific event log ID occurs. You can select multiple event log IDs, and apply log field filters.

To configure a FortiProxy event log trigger in the GUI:

1. Go to *Security Fabric* > *Automation*, select the *Trigger* tab, and click *Create New*.
2. In the *Miscellaneous* section, click *FortiProxy Event Log*.
3. Enter a name and description.
4. In the *Event* field, click the + to select multiple event log IDs.

   The *Event* options correspond to the *Message Meaning* listed in the Log Message Reference. Hover over an entry to view the tooltip that includes the event ID and log name. In this example, the *Admin login successful* event in the GUI corresponds to log ID *32001*, which is *LOG_ID_ADMIN_LOGIN_SUCC*.
5. In the *Field filter(s)* field, click the + to add multiple field filters. The configured filters much match in order for the stitch to be triggered.



6. Click *OK*.

To configure a FortiProxy event log trigger in the CLI:

```
config system automation-trigger
    edit "event_login_logout"
        set description "trigger for login logout event"
        set event-type event-log
        set logid 32001 32003
        config fields
            edit 1
                set name "user"
                set value "csf"
            next
            edit 2
                set name "srcip"
                set value "10.6.30.254"
            next
        end
    next
end
```

Actions

The following table outlines the available actions. Multiple actions can be added to an automation stitch. Actions can be reorganized in the *Edit Automation Stitch* page by dragging and dropping the actions in the diagram.

Category	Action	Description
Security Response		
	Access Layer Quarantine	This option is only available for Compromised Host triggers. Quarantine the MAC address on access layer devices (FortiSwitch and FortiAP).
	FortiClient Quarantine	This option is only available for Compromised Host triggers. Use FortiClient EMS to block all traffic from the source addresses that are flagged as compromised hosts.

Category	Action	Description
		Quarantined devices are flagged on the Security Fabric topology views.
	FortiNAC Quarantine	This option is only available for Compromised Host and Incoming Webhook triggers. Use FortiNAC to quarantine a client PC and disable its MAC address.
	VMware NSX Security Tag	This option is only available for Compromised Host triggers. If an endpoint instance in a VMware NSX environment is compromised, the configured security tag is assigned to the compromised endpoint. See VMware NSX security tag action on page 537 and VMware NSX-T security tag action on page 541 for details.
	IP Ban	This option is only available for Compromised Host triggers. Ban the IP address specified in the automation trigger event.
Notifications		
	Email	Send a custom email message to the selected recipients. At least one recipient and an email subject must be specified. The email body can use parameters from logs or previous action results. Wrapping the parameter with %% will replace the expression with the JSON value for the parameter, for example: *%%results.source%%* is the source property from the previous action. Replacement messages can be enabled in the email body to create branded email alerts. See Replacement messages for email alerts on page 545 for details.
	FortiExplorer Notification	Send push notifications to FortiExplorer. The FortiProxy must be registered to FortiCare on the mobile app that will receive the notification.
	Slack Notification	Send a notification to a Slack channel. See Slack Notification action on page 548 for details.
	Microsoft Teams Notification	Send a notification to channels in Microsoft Teams. See Microsoft Teams Notification action on page 551 for details.
Cloud Compute		
	AWS Lambda	AWS Lambda functions can be called when an automation stitch is triggered. See AWS Lambda action on page 554 for details.
	Azure Function	Azure functions can be called when an automation stitch is triggered. See Azure Function action on page 556 for details.
	Google Cloud Function	Google Cloud functions can be called when an automation stitch is triggered. See Google Cloud Function action on page 557 for details.

Category	Action	Description
	AliCloud Function	AliCloud functions can be called when an automation stitch is triggered. See AliCloud Function action on page 559 for details.
General		
	CLI Script	Run one or more CLI scripts. See CLI script action on page 560 for details, and Execute a CLI script based on CPU and memory thresholds on page 562 for an example.
	Webhook	Send an HTTP request using a REST callback. See Webhook action on page 568 for details, and Slack integration webhook on page 572 and Microsoft Teams integration webhook on page 574 for examples.
	Alert	Generate a FortiProxy dashboard alert. This option is only available in the CLI.
	Disable SSID	Disable the SSID interface. This option is only available in the CLI.

VMware NSX security tag action

If an endpoint instance in a VMware NSX environment is compromised, this action will assign the configured security tag to the compromised endpoint.

This action is only available when the automation trigger is set to compromised host.

To set up the NSX quarantine action, you need to:

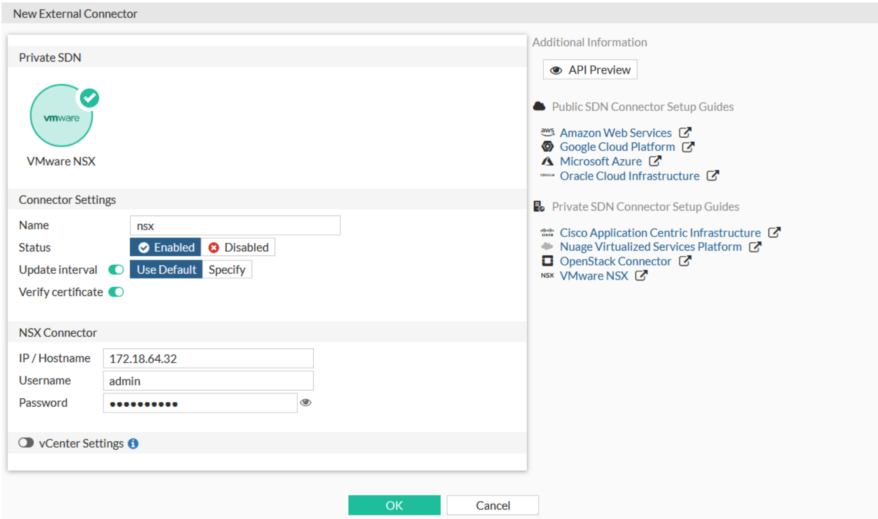
1. Configure a VMware NSX SDN connector
2. Configure an NSX security tag automation stitch
3. Configure FortiAnalyzer logging

Configure a VMware NSX SDN connector

The FortiPRoxy retrieves security tags from the VMware NSX server through the connector.

To configure a VMware NSX SDN connector in the GUI:

1. Go to *Security Fabric* > *External Connectors* and click *Create New*.
2. Select *VMware NSX*.
3. Configure the settings as needed.



4. Click *OK*.

To configure a VMware NSX SDN connector in the CLI:

```
config system sdn-connector
    edit "nsx"
        set type nsx
        set server "172.18.64.32"
        set username "admin"
        set password xxxxxxxxxxxx
    next
end
```

Configure an NSX security tag automation stitch

Security tags are retrieved from the VMware NSX server through the NSX SDN connector.

To configure an automation stitch with an NSX security tag in the GUI:

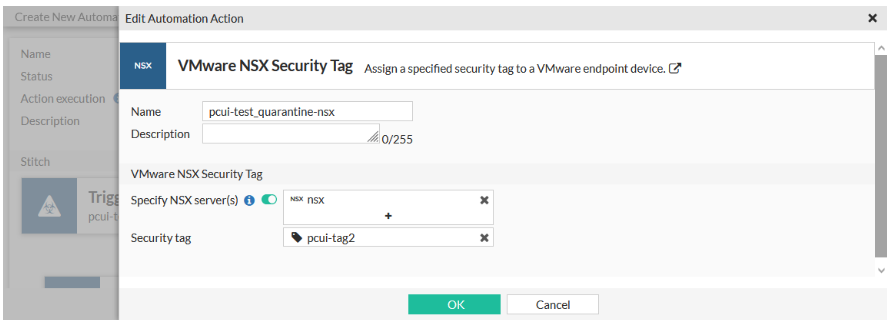
1. Go to *Security Fabric > Automation*, select the *Stitch* tab, and click *Create New*.
2. Enter the stitch name (*pcui-test*).
3. Configure the trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *Compromised Host*.
   c. Enter the following:

Name	pcui-test
Threat level threshold	High

   d. Click *OK*.
   e. Select the trigger from the list and click *Apply*.
4. Configure the VMware NSX Security Tag action:

a. Click *Add Action*.
b. Click *Create* and select *VMware NSX Security Tag*.
c. Enter the following:

Name	pcui-test_quarantine-nsx
Specify NSX server(s)	Enable and select the SDN connector
Security tag	Select an existing tag, or create a new one



d. Click *OK*.
e. Select the action in the list and click *Apply*.

5. Click *OK*.

To configure an automation stitch with an NSX security tag in the CLI:

1. Create an automation trigger:

```
config system automation-trigger
    edit "pcui-test"
        set ioc-level high
    next
end
```

2. Create an automation action:

```
config system automation-action
    edit "pcui-test_quarantine-nsx"
        set action-type quarantine-nsx
        set security-tag "pcui-tag2"
        set sdn-connector "nsx"
    next
end
```

3. Create the automation stitch:

```
config system automation-stitch
    edit "pcui-test"
        set trigger "pcui-test"
        config actions
            edit 1
                set action "pcui-test_quarantine-nsx"
                set required enable
            next
        end
```

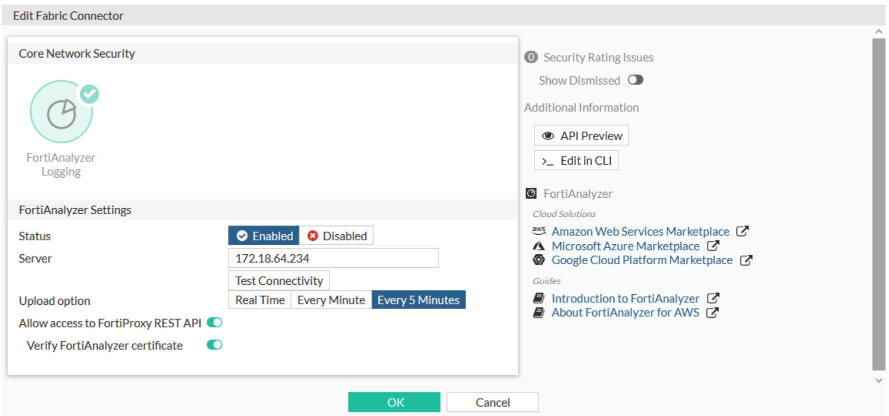
```
        next
    end
```

Configure FortiAnalyzer logging

The FortiAnalyzer is used to send endpoint compromise notification to the FortiProxy.

To configure FortiAnalyzer logging in the GUI:

1. Go to *Security Fabric > Fabric Connectors* and double-click the *FortiAnalyzer Logging* card.
2. Ensure the *Status* is *Enabled*, and configure the settings as needed.



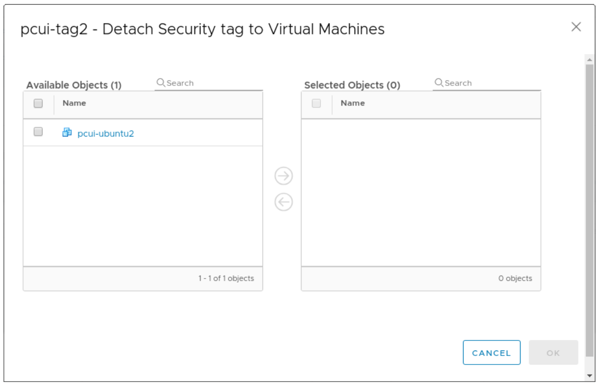
3. Click *OK*.

To configure FortiAnalyzer logging in the CLI:

```
config log fortianalyzer setting
    set status enable
    set server "172.18.64.234"
    set serial "FL-8HFT000000000"
    set upload-option realtime
    set reliable enable
end
```

When an endpoint instance is compromised

When an endpoint instance, such as *pcui-ubuntu2*, in the VMware NSX environment is compromised, the automation stitch is triggered. The FortiProxy then assigns the configured security tag, *pcui-tag2* in this example, to the compromised NSX endpoint instance.



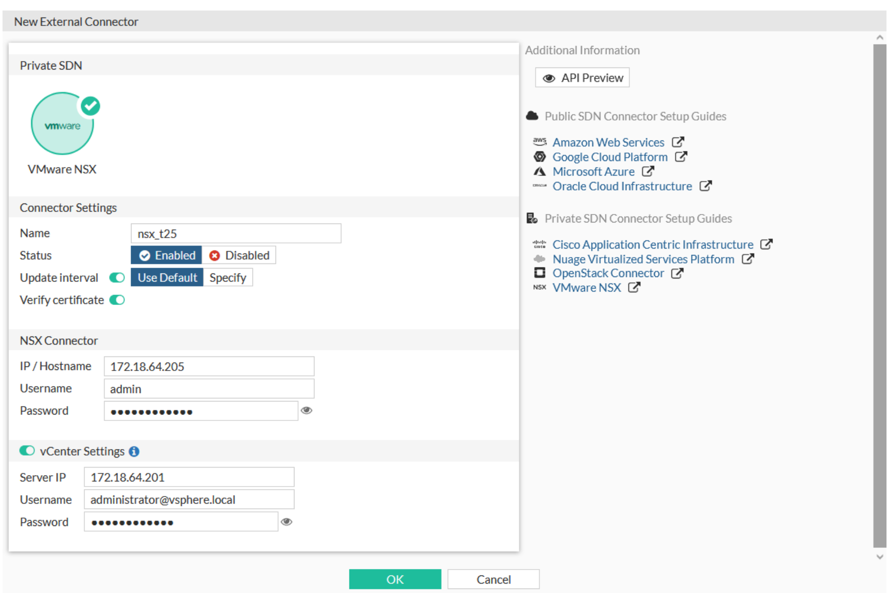
VMware NSX-T security tag action

VMware NSX SDN connectors' vCenter server and credentials can be configured so the FortiProxy resolves NSX-T VMs. The FortiProxy uses the VMWare NSX Security Tag automation action to assign a tag to the VM through an automation stitch.

The FortiProxy is notified of a compromised host on the NSX-T network by an incoming webhook or other means, such as FortiGuard IOC. An automation stitch can be configured to process this trigger and action it by assigning a VMware NSX security tag on the VM instance.

To configure an automation stitch to assign a security tag to NSX-T VMs in the GUI:

1. Configure the NSX SDN connector:
   a. Go to *Security Fabric > External Connectors* and click *Create New*.
   b. Select *VMware NSX*.
   c. Configure the connector settings.
   d. Enable *vCenter Settings* and configure as needed.

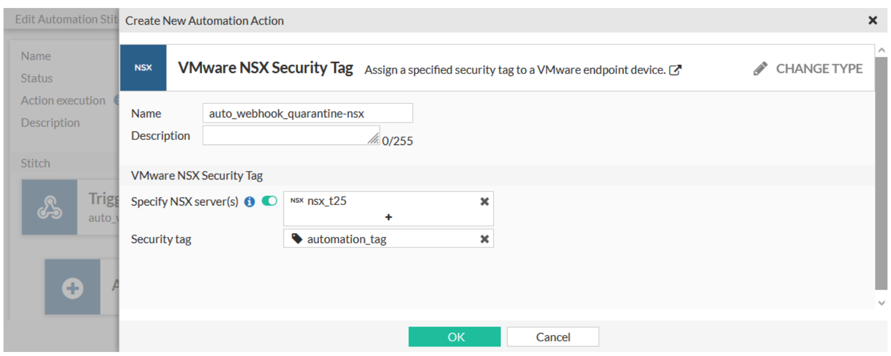


   e. Click *OK*.
2. Configure the automation stitch trigger:

a. Go to *Security Fabric > Automation*, select the *Stitch* tab, and click *Create New*.
b. Enter the stitch name (*auto_webhook*).
c. Click *Add Trigger*.
d. Click *Create* and select *Incoming Webhook*.
e. Enter a name (*auto_webhook*).
f. Click *OK* to close the *Incoming Webhook URL* prompt.
g. Select the trigger in the list and click *Apply*.

3. Configure the automation stitch action:
   a. Click *Add Action*.
   b. Click *Create* and select *VMware NSX Security Tag*.
   c. Enter the following:

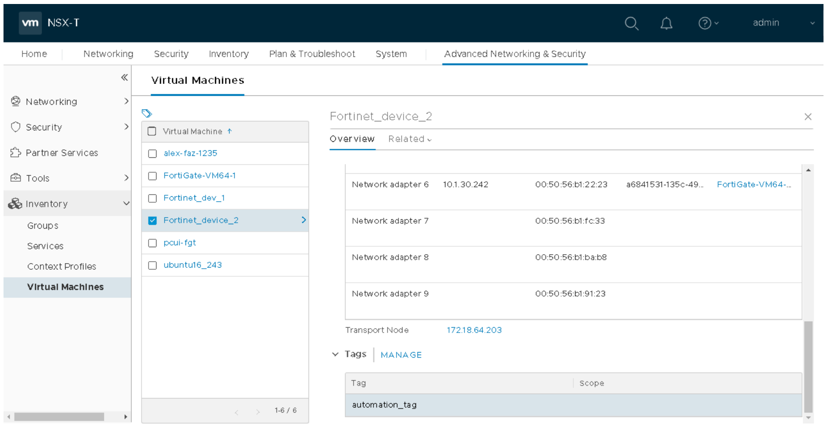
Name	auto_webhook_quarantine-nsx
Specify NSX server(s)	Enable and select the SDN connector
Security tag	Select an existing tag, or create a new one



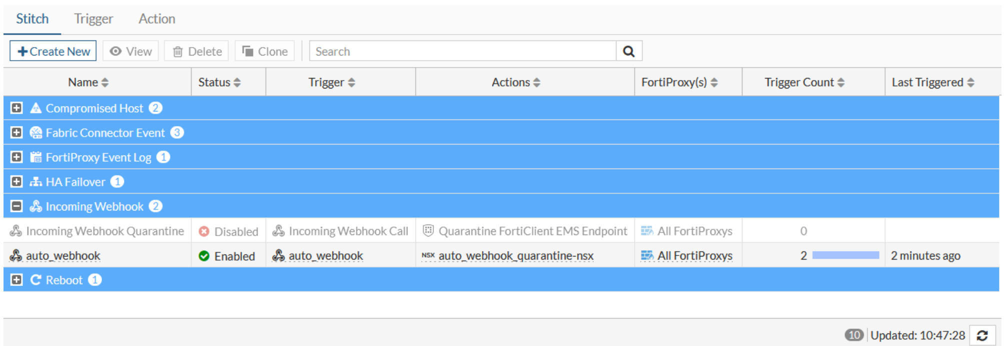
   d. Click *OK*.
   e. Select the action in the list and click *Apply*.
4. Click *OK*.
5. In NSX-T, create a cURL request to trigger the automation stitch on the FortiProxy:

```
root@pc56:/home# curl -k -X POST -H 'Authorization: Bearer
3fdxNG08mgNg0fh4NQ51g1NQ1QHcxx' --data '{ "srcip": "10.1.30.242"}'
https://172.16.116.230/api/v2/monitor/system/automation-stitch/webhook/auto_webhook
{
  "http_method":"POST",
  "status":"success",
  "http_status":200,
  "serial":"FGVM08TM20000000",
  "version":"v6.4.0",
  "build":1608
}
```

The automation stitch is triggered and the configured tag is added to the NSX-T VM.



On the FortiProxy, the *Security Fabric > Automation* page shows the last trigger time.



To configure an automation stitch to assign a security tag to NSX-T VMs in the CLI:

1. Configure the NSX SDN connector:

```
config system sdn-connector
    edit "nsx_t25"
        set type nsx
        set server "172.18.64.205"
        set username "admin"
        set password xxxxxxxxxxxx
        set vcenter-server "172.18.64.201"
        set vcenter-username "administrator@vsphere.local"
        set vcenter-password xxxxxxxxxxxx
    next
end
```

2. Configure the automation stitch:

```
config system automation-trigger
    edit "auto_webhook"
        set trigger-type event-based
        set event-type incoming-webhook
    next
end
```

```
config system automation-action
    edit "auto_webhook_quarantine-nsx"
        set action-type quarantine-nsx
```

```
        set security-tag "automation_tag"
        set sdn-connector "nsx_t25"
    next
end
```

```
config system automation-stitch
    edit "auto_webhook"
        set trigger "auto_webhook"
        config actions
            edit 1
                set action "auto_webhook_quarantine-nsx"
                set required enable
            next
        end
    next
end
```

3. In NSX-T, create a cURL request to trigger the automation stitch on the FortiProxy:

```
root@pc56:/home# curl -k -X POST -H 'Authorization: Bearer
3fdxNG08mgNg0fh4NQ51g1NQ1QHcxx' --data '{ "srcip": "10.1.30.242"}'
https://172.16.116.230/api/v2/monitor/system/automation-stitch/webhook/auto_webhook
{
  "http_method":"POST",
  "status":"success",
  "http_status":200,
  "serial":"FGVM08TM20000000",
  "version":"v6.4.0",
  "build":1608
}
```

To verify the automation stitch is triggered and the action is executed:

```
# diagnose test application autod 2

csf: enabled root:yes
version:1586883541 sync time:Tue Apr 14 11:04:05 2022

total stitches activated: 1

stitch: auto_webhook
        destinations: all
        trigger: auto_webhook
                type:incoming webhook

                field ids:
                        (id:15)service=auto_webhook

        local hit: 2 relayed to: 0 relayed from: 0
        actions:
                auto_webhook_quarantine-nsx type:quarantine-nsx interval:0
                        delay:0 required:yes
                        security tag:automation_tag
                        sdn connector:
        nsx_t25;
```

Replacement messages for email alerts

Automation stitches with an Email action can leverage the formatting options provided by replacement messages to create branded email alerts.

You can enable a replacement message and edit the message body or select a customized replacement message group when you configure the automation action. When the automation stitch is triggered, the FortiProxy will send the email with the defined replacement message.

In this example, a Security Rating report triggers an Email notification action. The email uses a customized replacement message group.

To configure the replacement message group in the GUI:

1. Go to *System > Replacement Message Groups* and click *Create New*.
2. Enter the following:

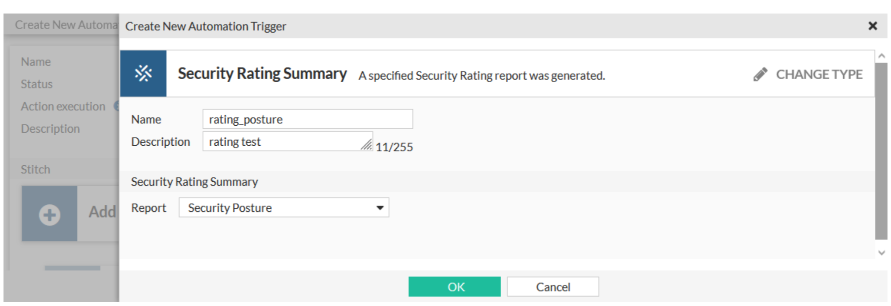
Name	group-sec1
Group Type	Security

3. Click *OK*.
4. Select the group in the list and click *Edit*.
5. Select *Automation Alert Email* and click *Edit*.
6. Edit the HTML code as needed, then click *Save*.

To configure the email action in the GUI:

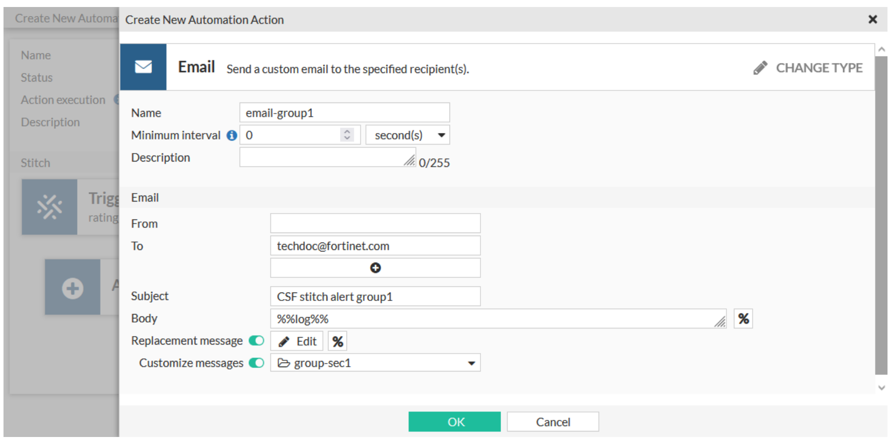
1. Go to *Security Fabric > Automation*, select the *Stitch* tab, and click *Create New*.
2. Enter the stitch name.
3. Configure the trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *Security Rating Summary*.
   c. Enter the following:

Name	rating_posture
Description	rating test
Report	Security Posture



   d. Click *OK*.
   e. Select the trigger in the list and click *Apply*.
4. Configure the Email notification action:
   a. Click *Add Action*.
   b. Click *Create* and select *Email*.
   c. Enter the following:

Name	email-group1
To	Enter an email address
Subject	CSF stitch alert group1
Replacement message	Enable
Customize messages	Enable and select group-sec1 from the dropdown



   d. Click *OK*.
   e. Select the action in the list and click *Apply*.
5. Click *OK*.
6. Right-click the automation stitch, and click *Test Automation Stitch*.

   After the Security Rating report is finished, the automation is triggered, and the email is delivered with the customized replacement message in the email body.

To configure the replacement message group in the CLI:

```
config system replacemsg-group
    edit "group-sec1"
        set comment ""
        set group-type utm
        config automation
            edit "automation-email"
                set buffer "...<h1> Security Fabric Automation rating trigger </h1>..."
                ...
            next
        end
    next
end
```

To configure the email action in the CLI:

1. Configure the automation trigger:

```
config system automation-trigger
    edit "rating_posture"
        set description "rating test"
        set event-type security-rating-summary
    next
end
```

2. Configure the automation action:

```
config system automation-action
    edit "email-group1"
        set action-type email
        set email-to "admin@fortinet.com"
        set email-subject "CSF stitch alert group1"
        set replacement-message enable
        set replacemsg-group "group-sec1"
    next
end
```

3. Configure the automation stitch:

```
config system automation-stitch
    edit "auto_rating"
        set trigger "rating_posture"
        config actions
            edit 1
                set action "email-group1"
                set required enable
            next
        end
    next
end
```

4. To view the automation stitch information after it is triggered:

```
# diagnose test application autod 3
stitch: auto_rating
        local hit: 1 relayed to: 0 relayed from: 0
        last trigger:Tue Sep 13 11:25:01 2022
        last relay:
        actions:
                email-group1:
                        done: 1 relayed to: 0 relayed from: 0
                        last trigger:Tue Sep 13 11:25:01 2022
                        last relay:

logid2stitch mapping:
id:52000  local hit: 1 relayed hits: 0
        auto_rating
```

Slack Notification action

To configure an automation stitch with a Slack Notification action, you first need to configure an incoming webhook in Slack. Then you can enter the webhook URL when you configure the Slack Notification action.

This example uses a Security Rating Summary trigger in the automation stitch with two Slack Notification actions with different notification messages. One message is a custom message, and the other is for the Security Rating Summary log with a 90 second delay.

To create an Incoming Webhook in Slack:

1. Go to the Slack website, and create a workspace.
2. Create a Slack application for the workspace.
3. Add an Incoming Webhook to a channel in the workspace (see Sending messages using Incoming Webhooks for more details).
4. Activate the Incoming Webhook, and copy the *Webhook URL* to the clipboard.

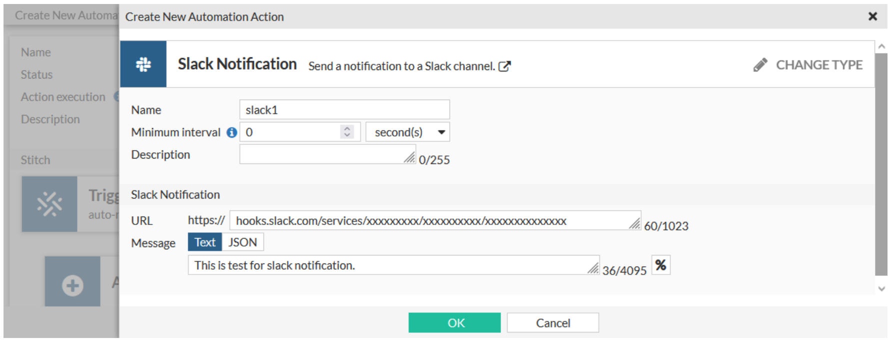
To configure an automation stitch with Slack Notification actions in the GUI:

1. Go to *Security Fabric > Automation*, select the *Stitch* tab, and click *Create New*.
2. Enter the stitch name.
3. Configure the Security Rating Summary trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *Security Rating Summary*.
   c.

Name	auto-rating
Report	Security Posture

   Enter the following:
   d. Click *OK*.
   e. Select the trigger in the list and click *Apply*.
4. Configure the first Slack Notification action:
   a. Click *Add Action*.
   b. Click *Create* and select *Slack Notification*.
   c. Enter the following:

Name	slack1
URL	Paste the webhook URL from the clipboard
Message	Text
Message text	This is test for slack notification.

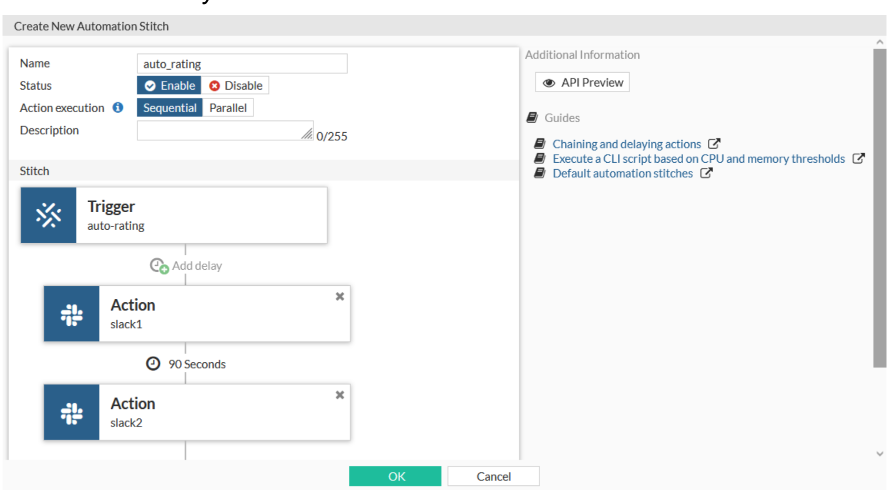


d. Click *OK*.
e. Select the action in the list and click *Apply*.

5. Configure the second Slack Notification action:
   a. Click *Add Action*.
   b. Click *Create* and select *Slack Notification*.
   c. Enter the following:

Name	slack2
URL	Paste the webhook URL from the clipboard
Message	Text
Message text	%%log%%

   d. Click *OK*.
   e. Select the action in the list and click *Apply*.
   f. Click the *Add delay* located between both actions. Enter *90* and click *OK*.



6. Click *OK*.
7. Trigger the automation stitch:
   a. Right-click the automation stitch and select *Test Automation Stitch*.
      After the Security Rating report is finished, the automation is triggered and an event log is created by the FortiProxy. The two notifications are sent to the Slack channel.

To configure an automation stitch with Slack Notification actions in the CLI:

1. Configure the automation trigger:

```
config system automation-trigger
    edit "auto-rating"
        set event-type security-rating-summary
    next
end
```

2. Configure the automation actions:

```
config system automation-action
    edit "slack1"
        set action-type slack-notification
        set message "This is test for slack notification."
        set uri "hooks.slack.com/services/xxxxxxxxx/xxxxxxxxx/xxxxxxxxxxxxxxxxxxxxxxxx"
    next
    edit "slack2"
        set action-type slack-notification
        set uri "hooks.slack.com/services/xxxxxxxxx/xxxxxxxxx/xxxxxxxxxxxxxxxxxxxxxxxx"
    next
end
```

3. Configure the automation stitch:

```
config system automation-stitch
    edit "auto_rating"
        set trigger "auto-rating"
        config actions
            edit 1
                set action "slack1"
                set required enable
            next
            edit 2
                set action "slack2"
                set delay 90
                set required enable
            next
        end
    next
end
```

4. Verify that the automation action was triggered:

```
# diagnose test application autod 3
stitch: auto-rating
    local hit: 1 relayed to: 0 relayed from: 0
    last trigger:Tue Sep 13 11:34:56 2022
    last relay:
    actions:
        slack1:
            done: 1 relayed to: 0 relayed from: 0
            last trigger:Tue Sep 13 11:34:56 2022
            last relay:
        slack2:
            done: 1 relayed to: 0 relayed from: 0
```

```
last trigger:Tue Sep 13 11:34:56 2022
last relay:
```

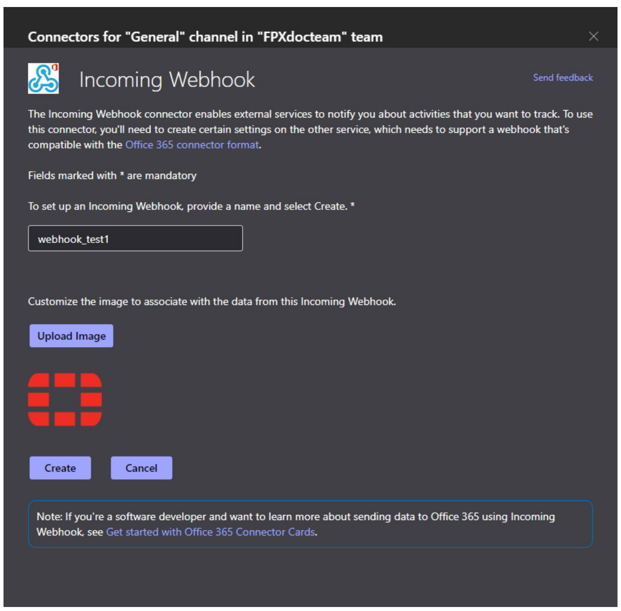
Microsoft Teams Notification action

Microsoft Teams Notification actions can be configured to send notifications to channels in Microsoft Teams. To trigger the notifications, you need to add an Incoming Webhook connector to a channel in Microsoft Teams, then you can configure the automation stitch with the webhook URL.

In the following example, you will configure an automation stitch with a Security Rating Summary trigger and two Microsoft Teams Notification actions with different notification messages. One message is for the Security Rating Summary log, and the other is a custom message with a ten second delay.

To add the Incoming Webhook connector in a Microsoft Teams channel:

1. In Microsoft Teams, click the *...* (*More options*) beside the channel name, and select *Connectors*.
2. Find *Incoming Webhook* and click *Configure*.
3. Enter a name for the webhook, upload an image for the webhook, and click *Create*.



4. Copy the webhook to the clipboard and save it.
5. Click *Done*.

To configure an automation stitch with Microsoft Teams Notification actions in the GUI:

1. Go to *Security Fabric > Automation*, select the *Stitch* tab, and click *Create New*.
2. Enter the stitch name.
3. Configure the Security Rating Summary trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *Security Rating Summary*.
   c. Enter a name, and for *Report*, select *Security Posture*.

d. Click *OK*.

e. Select the trigger in the list and click *Apply*.

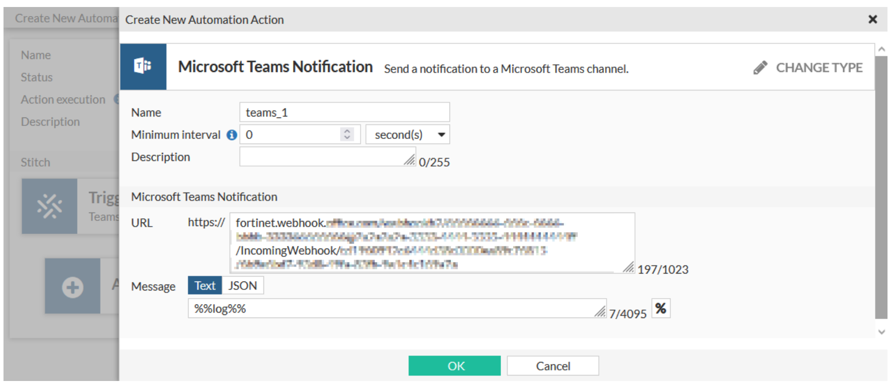
4. Configure the first Microsoft Teams Notification action:

a. Click *Add Action*.

b. Click *Create* and select *Microsoft Teams Notification*.

c. Enter the following:

Name	teams_1
URL	Paste the webhook URI from the clipboard
Message	Text
Message text	%%log%%



d. Click *OK*.

e. Select the action in the list and click *Apply*.

5. Configure the second Microsoft Teams Notification action:

a. Click *Add Action*.

b. Click *Create* and select *Microsoft Teams Notification*.

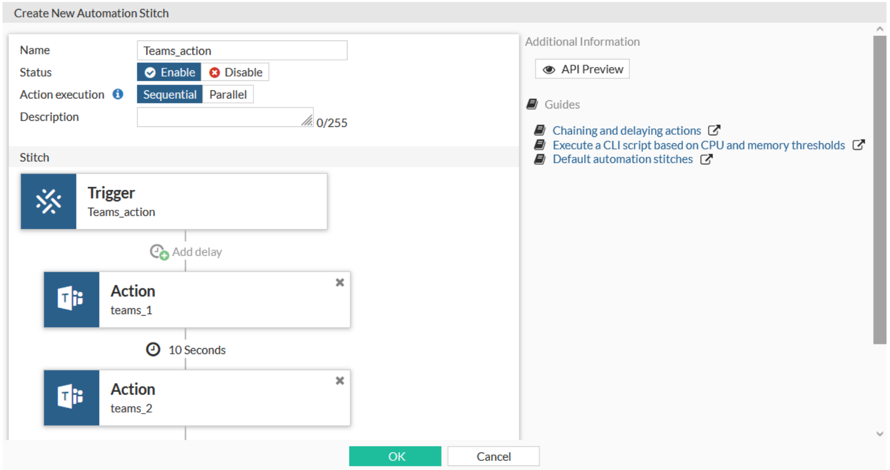
c. Enter the following:

Name	teams_2
URL	Paste the webhook URI from the clipboard
Message	Text
Message text	This is for test.

d. Click *OK*.

e. Select the action in the list and click *Apply*.

f. Click the *Add delay* located between both actions. Enter *10* and click *OK*.



6. Click *OK*.
7. Trigger the automation stitch:
   a. Right-click the automation stitch and select *Test Automation Stitch*.

      After the Security Rating report is finished, the automation is triggered and an event log is created by the FortiProxy. The two notifications are sent to the Microsoft Teams channel.

To configure an automation stitch with Microsoft Teams Notification actions in the CLI:

1. Configure the automation trigger:

```
config system automation-trigger
    edit "Teams_action"
        set event-type security-rating-summary
    next
end
```

2. Configure the automation actions:

```
config system automation-action
    edit "teams_1"
        set action-type microsoft-teams-notification
        set uri "outlook.office.com/webhook/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx@xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/IncomingWebhook/xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx"
    next
    edit "teams_2"
        set action-type microsoft-teams-notification
        set message "This is for test."
        set uri "outlook.office.com/webhook/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx@xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/IncomingWebhook/xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx"
    next
end
```

3. Configure the automation stitch:

```
config system automation-stitch
    edit "Teams_action"
        set trigger "Teams_action"
        config actions
            edit 1
                set action "teams_1"
                set required enable
            next
            edit 2
                set action "teams_2"
                set delay 10
                set required enable
            next
        end
    next
end
```

4. Verify that the automation action was triggered:

```
# diagnose test application autod 3
stitch: Teams_action

        local hit: 2 relayed to: 0 relayed from: 0
        last trigger:Tue Sep 13 12:09:12 2022
        last relay:
        actions:
                teams_1:
                        done: 2 relayed to: 0 relayed from: 0
                        last trigger:Tue Sep 13 12:09:12 2022
                        last relay:
                teams_2:
                        done: 2 relayed to: 0 relayed from: 0
                        last trigger:Tue Sep 13 12:09:12 2022
                        last relay:
         logid2stitch mapping:
         id:52000  local hit: 22 relayed hits: 0
         Teams_action
```

AWS Lambda action

AWS Lambda functions can be called when an automation stitch is triggered. This example uses a Security Rating Summary trigger in the automation stitch.

To configure an AWS Lambda function automation stitch in the GUI:

1. Go to *Security Fabric > Automation*, select the *Stitch* tab, and click *Create New*.
2. Enter the stitch name.
3. Configure the trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *Security Rating Summary*.
   c. Enter the following:

Name	auto-aws
Report	Security Posture

d. Click *OK*.
e. Select the trigger in the list and click *Apply*.

4. Configure the AWS Lambda function action:
   a. Click *Add Action*.
   b. Click *Create* and select *AWS Lambda*.
   c. Enter the following:

Name	aws-action-1
URL	Enter the request API URI
API key	Enter the API key
HTTP header	header2 : header2_value

   d. Click *OK*.
   e. Select the action in the list and click *Apply*.
5. Click *OK*.

To configure an AWS Lambda function automation stitch in the CLI:

1. Create the automation trigger:

```
config system automation-trigger
    edit "auto-aws"
        set event-type security-rating-summary
    next
end
```

2. Create the automation action:

```
config system automation-action
    edit "aws-action-1"
        set action-type aws-lambda
        set aws-api-key *************
        set uri "0100000000.execute-api.us-east-2.amazonaws.com/default/xxxxx-
autobatoon-XXX-lambdaXXX"
        config http-headers
            edit 1
                set key "header2"
                set value "header2_value"
            next
        end
    next
end
```

3. Create the automation stitch:

```
config system automation-stitch
    edit "auto-aws"
        set trigger "auto-aws"
        config actions
```

```
            edit 1
                set action "aws-action-1"
                set required enable
            next
        end
    next
end
```

When the automation stitch is triggered, the *Security Fabric* > *Automation* page shows the stitch trigger time. In AWS, the log shows that the function was called, executed, and finished.

Azure Function action

Azure functions can be called when an automation stitch is triggered. This example uses a Security Rating Summary trigger in the automation stitch.

To configure an Azure function automation stitch in the GUI:

1. Go to *Security Fabric* > *Automation*, select the Stitch tab, and click *Create New*.
2. Enter the stitch name.
3. Configure the trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *Security Rating Summary*.
   c. Enter the following:

Name	auto-azure
Report	Security Posture

   d. Click *OK*.
   e. Select the trigger in the list and click *Apply*.
4. Configure the Azure Function action:
   a. Click *Add Action*.
   b. Click *Create* and select *Azure Function*.
   c. Enter the following:

Name	azure_function
URL	Enter the request API URI
Authorization	Function
API key	Enter the API key
HTTP header	header1 : value1

   d. Click *OK*.
   e. Select the action in the list and click *Apply*.
5. Click *OK*.

To configure an Azure function automation stitch in the CLI:

1. Create an automation trigger:

```
config system automation-trigger
    edit "auto-azure"
        set event-type security-rating-summary
    next
end
```

2. Create an automation action:

```
config system automation-action
    edit "azure_function"
        set action-type azure-function
        set azure-function-authorization function
        set azure-api-key **********
        set uri "xxxxx00-no-delete-xxxx.azurewebsites.net/api/headersResponse"
        config http-headers
            edit 1
                set key "header1"
                set value "value1"
            next
        end
    next
end
```

3. Create the automation stitch:

```
config system automation-stitch
    edit "auto-azure"
        set trigger "auto-azure"
        config actions
            edit 1
                set action "azure_function"
                set required enable
            next
        end
    next
end
```

When the automation stitch is triggered, the *Security Fabric > Automation* page shows the stitch trigger time. In Azure, the function log shows that the function was called, executed, and finished.

Google Cloud Function action

Google Cloud functions can be called when an automation stitch is triggered. This example uses a Security Rating Summary trigger in the automation stitch.

To configure a Google Cloud function automation stitch in the GUI:

1. Go to *Security Fabric > Automation* and click *Create New*.
2. Enter the stitch name.
3. Configure the trigger:

  a. Click *Add Trigger*.
  b. Click *Create* and select *Security Rating Summary*.
  c. Enter the following:

Name	auto-google1
Report	Security Posture

  d. Click *OK*.
  e. Select the trigger in the list and click *Apply*.
4. Configure the Google Cloud Function action:
  a. Click *Add Action*.
  b. Click *Create* and select *Google Cloud Function*.
  c. Enter the following:

Name	google-echo
URL	Enter the request API URI
HTTP header	echo-header : echo-value

  d. Click *OK*.
  e. Select the action in the list and click *Apply*.
5. Click *OK*.

To configure a Google Cloud function automation stitch in the CLI:

1. Create an automation trigger:

```
config system automation-trigger
    edit "auto-google1"
        set event-type security-rating-summary
    next
end
```

2. Create an automation action:

```
config system automation-action
    edit "google-echo"
        set action-type google-cloud-function
        set uri "us-central1-xxx-xxxxxxx-000-000000.cloudfunctions.net/xxxx-echo"
        config http-headers
            edit 1
                set key "echo-header"
                set value "echo-value"
            next
        end
    next
end
```

3. Create the automation stitch:

```
config system automation-stitch
    edit "auto-google1"
        set trigger "auto-google1"
```

```
            config actions
                edit 1
                    set action "google-echo"
                    set required enable
                next
            end
        next
    end
```

When the automation stitch is triggered, the *Security Fabric > Automation* page shows the stitch trigger time. In Google Cloud, go to *Logs* to see the function log showing that the configured function was called, executed, and finished.

AliCloud Function action

AliCloud functions can be called when an automation stitch is triggered. This example uses a Security Rating Summary trigger in the automation stitch.

To configure an AliCloud function automation stitch in the GUI:

1. Go to *Security Fabric > Automation* and click *Create New*.
2. Enter the stitch name.
3. Configure the trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *Security Rating Summary*.
   c. Enter the following:

Name	auto-ali
Report	Security Posture

   d. Click *OK*.
   e. Select the trigger in the list and click *Apply*.
4. Configure the AliCloud Function action:
   a. Click *Add Action*.
   b. Click *Create* and select *AliCloud Function*.
   c. Enter the following:

Name	Ali-Action-1
URL	Enter the request API URI
Authorization	Function
AccessKey ID	Enter the access key ID
AccessKey Secret	Enter the access key secret

   d. Click *OK*.
   e. Select the action in the list and click *Apply*.
5. Click *OK*.

To configure an AliCloud function automation stitch in the CLI:

1. Create an automation trigger:

```
config system automation-trigger
    edit "auto-ali"
        set event-type security-rating-summary
    next
end
```

2. Create an automation action:

```
config system automation-action
    edit "Ali-Action-1"
        set action-type alicloud-function
        set alicloud-function-authorization function
        set alicloud-access-key-id "XXXXXxXXXXxxxxxx"
        set alicloud-access-key-secret xxxxxx
        set uri "0000000000000000.us-east-1.fc.aliyuncs.com/2099-99-99/proxy/test-
function/echoBodyAuth/"
    next
end
```

3. Create the automation stitch:

```
config system automation-stitch
    edit "auto-ali"
        set trigger "auto-ali"
        config actions
            edit 1
                set action "Ali-Action-1"
                set required enable
            next
        end
    next
end
```

When the automation stitch is triggered, the *Security Fabric > Automation* page shows the stitch trigger time. In AliCloud, the function log shows that the function was called, executed, and finished.

CLI script action

CLI scripts can run when an automation stitch is triggered. The scripts can be entered manually, uploaded as a file, or recorded in the CLI console. The output of the script can be sent as an email action.

The maximum size of the CLI script action output is 16K characters.

In this example, the script sets the idle timeout value to 479 minutes, and sends an email with the script output.

To configure a stitch with a CLI script action in the GUI:

1. Go to *Security Fabric > Automation*, select the *Stitch* tab, and click *Create New*.
2. Enter the stitch name (*auto-cli-1*).

3. Configure the trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *Security Rating Summary*.
   c. Enter the following:

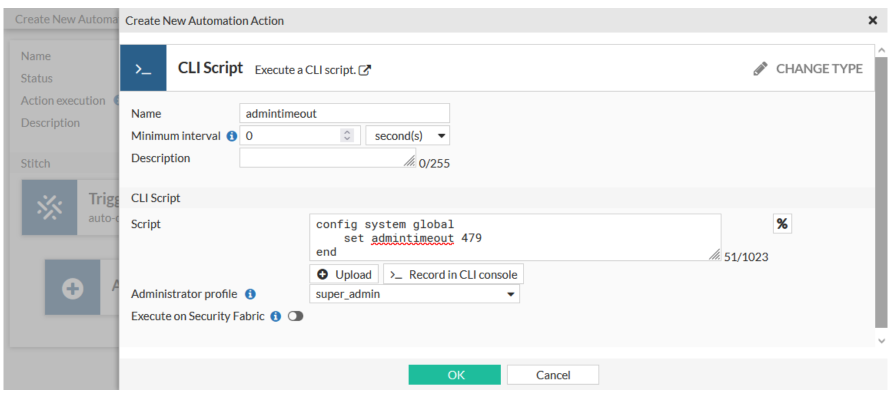
Name	auto-cli-1
Report	Security Posture

   d. Click *OK*.
   e. Select the trigger in the list and click *Apply*.
4. Configure the CLI Script action:
   a. Click *Add Action*.
   b. Click *Create* and select *CLI Script*.
   c. Enter the following:

Name	admintimeout

Script	`config system global`
	`    set admintimeout 479`
	`end`
	
	Alternatively, click *Upload* to upload a file, or click >_*Record in CLI console* and enter the CLI commands.

Administrator profile	Select a profile



   d. Click *OK*.
   e. Select the action in the list and click *Apply*.
5. Configure the Email notification action:
   a. Click *Add Action*.
   b. Click *Create* and select *Email*.
   c. Enter the following:

Name	auto-cli-1_email
To	Enter an email address
Subject	CSF stitch alert
Body	%%results%%

   d. Click *OK*.
   e. Select the action in the list and click *Apply*.
6. Click *OK*.

To configure a stitch with a CLI script action in the CLI:

1. Create the automation trigger:

```
config system automation-trigger
    edit "auto-cli-1"
        set event-type security-rating-summary
    next
end
```

2. Create the automation actions:

```
config system automation-action
    edit "admintimeout"
        set action-type cli-script
        set script "config system global
            set admintimeout 479
            end"
        set accprofile "super_admin"
    next
    edit "auto-cli-1_email"
        set action-type email
        set email-to "admin@fortinet.com"
        set email-subject "CSF stitch alert"
        set message "%%results%%"
    next
end
```

3. Create the automation stitch:

```
config system automation-stitch
    edit "auto-cli-1"
        set trigger "auto-cli-1"
        config actions
            edit 1
                set action "admintimeout"
                set required enable
            next
            edit 2
                set action "auto-cli-1_email"
                set required enable
            next
        end
    next
end
```

Execute a CLI script based on CPU and memory thresholds

Automation stitches can be created to run a CLI script and send an email message when CPU or memory usage exceeds specified thresholds.

In this example, two automation stitches are created that run a CLI script to collect debug information, and then email the results of the script to a specified email address when the CPU usage threshold is exceeded, or memory usage causes the FortiProxy to enter conserve mode.

The maximum size of the CLI script action output is 16K characters.

To define CPU and memory usage thresholds:

```
config system global
    set cpu-use-threshold <percent>
    set memory-use-threshold-extreme <percent>
    set memory-use-threshold-green <percent>
    set memory-use-threshold-red <percent>
end
```

Where:

`cpu-use-threshold`	Threshold at which CPU usage is reported, in percent of total possible CPU utilization (default = 90).
`memory-use-threshold-extreme`	Threshold at which memory usage is considered extreme, and new sessions are dropped, in percent of total RAM (default = 95).
`memory-use-threshold-green`	Threshold at which memory usage forces the FortiProxy to exit conserve mode, in percent of total RAM (default = 82).
`memory-use-threshold-red`	Threshold at which memory usage forces the FortiProxy to enter conserve mode, in percent of total RAM (default = 88).

Configuring the automation stitches

High CPU usage stitch

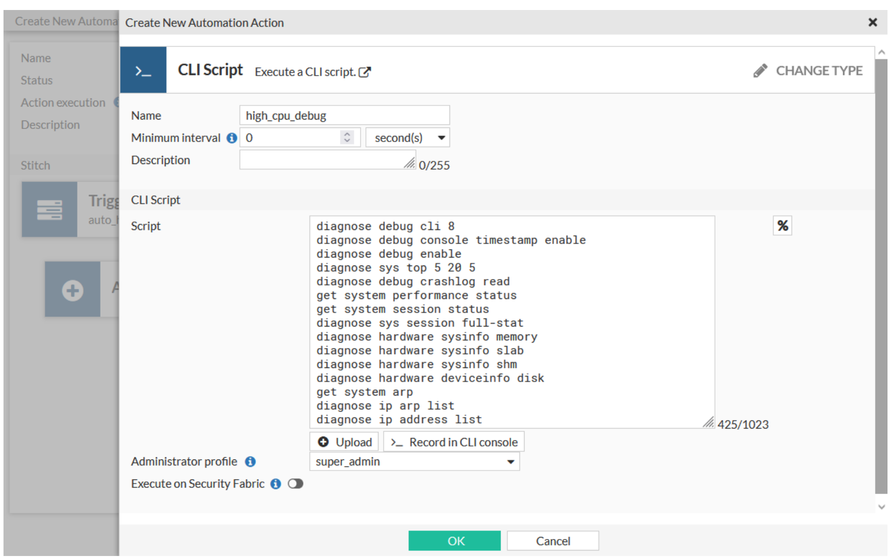
To create an automation stitch for high CPU usage in the GUI:

1. Go to *Security Fabric > Automation*, select the *Stitch* tab, and click *Create New*.
2. Enter the stitch name (*auto_high_cpu*).
3. Configure the trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *High CPU*.
   c. Enter the name, *auto_high_cpu*.
   d. Click *OK*.
   e. Select the trigger in the list and click *Apply*.
4. Configure the CLI Script action:
   a. Click *Add Action*.
   b. Click *Create* and select *CLI Script*.
   c. Enter the following:

Name	high_cpu_debug

Script	`diagnose debug cli 8`
	`diagnose debug console timestamp enable`
	`diagnose debug enable`
	`diagnose sys top 5 20 5`
	`diagnose debug crashlog read`
	`get system performance status`
	`get system session status`
	`diagnose sys session full-stat`
	`diagnose firewall iprope state`
	`diagnose sys flash list`
	`diagnose hardware sysinfo memory`
	`diagnose hardware sysinfo slab`
	`diagnose hardware sysinfo shm`
	`diagnose hardware deviceinfo disk`
	`get system arp`
	`diagnose ip arp list`
	`diagnose ip address list`
	`get router info routing-table all`
	`get router info kernel`

Administrator profile	Select a profile



  d. Click *OK*.
  e. Select the action in the list and click *Apply*.
5. Configure the Email notification action:
  a. Click *Add Action*.
  b. Click *Create* and select *Email*.
  c. Enter the following:

Name	auto_high_cpu_email

To	Enter an email address
Subject	CSF stitch alert: high_cpu
Body	%%results%%

   d. Click *OK*.
   e. Select the action in the list and click *Apply*.
6. Click *OK*.

To create an automation stitch for high CPU usage in the CLI:

1. Create the automation trigger:

```
config system automation-trigger
    edit "auto_high_cpu"
        set event-type high-cpu
    next
end
```

2. Create the automation actions:

```
config system automation-action
    edit "high_cpu_debug"
        set action-type cli-script
        set script "diagnose debug cli 8
diagnose debug console timestamp enable
diagnose debug enable
diagnose sys top 5 20 5
diagnose debug crashlog read
get system performance status
get system session status
diagnose sys session full-stat
diagnose hardware sysinfo memory
diagnose hardware sysinfo slab
diagnose hardware sysinfo shm
diagnose hardware deviceinfo disk
get system arp
diagnose ip arp list
diagnose ip address list"
        set accprofile "super_admin"
    next
    edit "auto_high_cpu_email"
        set action-type email
        set email-to "person@fortinet.com"
        set email-subject "CSF stitch alert: high_cpu"
        set message "%%results%%"
    next
end
```

3. Create the automation stitch:

```
config system automation-stitch
    edit "auto_high_cpu"
        set trigger "auto_high_cpu"
        config actions
            edit 1
```

```
                set action "high_cpu_debug"
                set required enable
            next
            edit 2
                set action "auto_high_cpu_email"
                set required enable
            next
        end
    next
end
```

High memory usage stitch

To create an automation stitch for high memory usage in the GUI:

1. Go to *Security Fabric > Automation* and click *Create New*.
2. Enter the stitch name (*auto_high_memory*).
3. Configure the trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *Conserve Mode*.
   c. Enter the name, *auto_high_memory*.
   d. Click *OK*.
   e. Select the trigger in the list and click *Apply*.
4. Configure the CLI Script action:
   a. Click *Add Action*.
   b. Click *Create* and select *CLI Script*.
   c. Enter the following:

Name	high_memory_debug

Script	`diagnose debug cli 8`
	`diagnose debug console timestamp enable`
	`diagnose debug enable`
	`diagnose sys top 5 20 5`
	`diagnose debug crashlog read`
	`get system performance status`
	`get system session status`
	`diagnose sys session full-stat`
	`diagnose hardware sysinfo memory`
	`diagnose hardware sysinfo slab`
	`diagnose hardware sysinfo shm`
	`diagnose hardware deviceinfo disk`
	`get system arp`
	`diagnose ip arp list`
	`diagnose ip address list`

Administrator profile	Select a profile

   d. Click *OK*.
   e. Select the action in the list and click *Apply*.

5. Configure the Email notification action:
   a. Click *Add Action*.
   b. Click *Create* and select *Email*.
   c. Enter the following:

Name	auto_high_memory_email
To	Enter an email address
Subject	CSF stitch alert: high_memory
Body	%%results%%

   d. Click *OK*.
   e. Select the action in the list and click *Apply*.
6. Click *OK*.

To create an automation stitch for high memory usage in the CLI:

1. Create the automation trigger:

```
config system automation-trigger
    edit "auto_high_memory"
        set event-type low-memory
    next
end
```

2. Create the automation actions:

```
config system automation-action
    edit "high_memory_debug"
        set action-type cli-script
        set script "diagnose debug cli 8
diagnose debug console timestamp enable
diagnose debug enable
diagnose sys top 5 20 5
diagnose debug crashlog read
get system performance status
get system session status
diagnose sys session full-stat
diagnose hardware sysinfo memory
diagnose hardware sysinfo slab
diagnose hardware sysinfo shm
diagnose hardware deviceinfo disk
get system arp
diagnose ip arp list
diagnose ip address list"
        set accprofile "super_admin"
    next
    edit "auto_high_memory_email"
        set action-type email
        set email-to "person@fortinet.com"
        set email-subject "CSF stitch alert: high_memory"
        set message "%%results%%"
    next
end
```

3. Create the automation stitch:

```
config system automation-stitch
    edit "auto_high_memory"
        set trigger "auto_high_memory"
        config actions
            edit 1
                set action "high_memory_debug"
                set required enable
            next
            edit 2
                set action "auto_high_memory_email"
                set required enable
            next
        end
    next
end
```

Results

When the FortiProxy enters conserve mode due to the `memory-use-threshold-red` being exceeded, the GUI displays a notice, and the *auto_high_memory* automation stitch is triggered. This causes the CLI script to run and the script results are emailed to the specified address.

Here is sample text from the email message:

```
CSF stitch alert: high_memory
noreply@notification.fortinet.net
Thu 11/21/2019 11:06 AM
John Doe
FPX[FPXM16TM11111111] Automation Stitch:auto_high_memory is triggered.
########## script name: autod.47 ##########
========== #1, 2019-11-21 11:07:24 ==========
FPXM16TM11111111 $  diag deb cli 8
Debug messages will be on for 25 minutes.
FPXM16TM11111111 $  diag deb console timestamp enable
FPXM16TM11111111 $  diag deb enable
FPXM16TM11111111 $  diag deb crashlog read
1: 2019-08-08 11:35:25 the killed daemon is /bin/dhcpcd: status=0x0
2: 2019-08-08 17:52:47 the killed daemon is /bin/pyfcgid: status=0x0
3: 2019-08-23 11:32:31 from=license status=INVALID
4: 2019-08-23 11:32:32 from=license status=INVALID
5: 2019-11-21 09:53:31 from=license status=VALID
...
```

Webhook action

The webhook automation stitch action makes HTTP and HTTPS requests to a specified server, with custom headers, bodies, ports, and methods. It can be used to leverage the ubiquity of HTML requests and APIs to integrate with other tools.

The URI and HTTP body can use parameters from logs or previous action results. Wrapping the parameter with %% will replace the expression with the JSON value for the parameter, for example: *%%results.source%%* is the source property from the previous action.

In this example, a specific log message (failed administrator log in attempt) triggers the FortiProxy to send the contents of the log to a server. The server responds with a generic reply. This example assumes that the server is already configured and able to communicate with the FortiProxy.

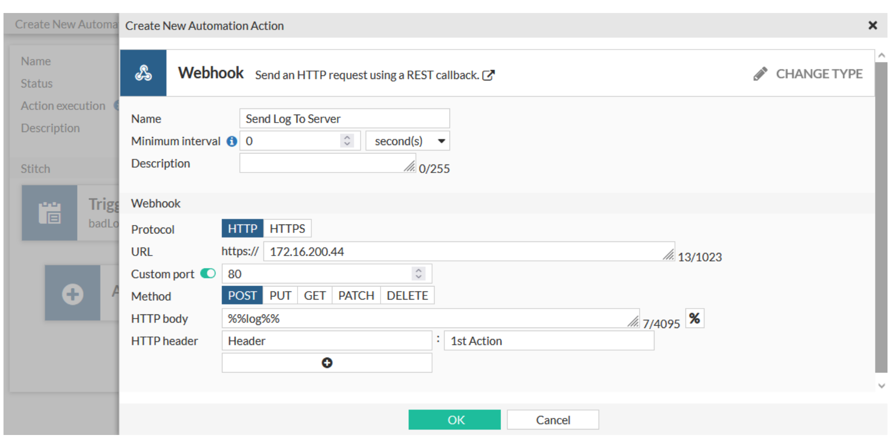
To configure the webhook automation stitch in the GUI:

1. Go to *Security Fabric > Automation* and click *Create New*.
2. Enter the stitch name (*badLogin*).
3. Configure the trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *FortiProxy Event Log*.
   c. Enter the following:

Name	badLogin
Event	Admin login failed

   d. Click *OK*.
   e. Select the trigger in the list and click *Apply*.
4. Configure the automation stitch action:
   a. Click *Add Action*.
   b. Click *Create* and select *Webhook*.
   c. Enter the following:

Name	Send Log To Server
Protocol	HTTP
URL	172.16.200.44
Custom port	Enable and enter 80
Method	POST
HTTP body	%%log%%
HTTP header	Header : 1st Action



   d. Click *OK*.
   e. Select the action in the list and click *Apply*.
5. Click *OK*.

To configure the webhook automation stitch in the CLI:

1. Create an automation trigger:

```
config system automation-trigger
    edit "badLogin"
        set event-type event-log
        set logid 32002
    next
end
```

2. Create the automation action:

```
config system automation-action
    edit "Send Log To Server"
        set action-type webhook
        set uri "172.16.200.44"
        set http-body "%%log%%"
        set port 80
        config http-headers
            edit 1
                set key "Header"
                set value "1st Action"
            next
        end
    next
end
```

3. Create the automation stitch:

```
config system automation-stitch
    edit "badLogin"
        set trigger "badLogin"
        config actions
            edit 1
                set action "Send Log To Server"
                set required enable
            next
        end
    next
end
```

To test the automation stitch:

1. Attempt to log in to the FortiProxy with an incorrect username or password.
2. On the server, check the log to see that its contents were sent by the FortiProxy.
   The body content is replaced with the log from the trigger.
3. On the FortiProxy, go to *Log & Report > Events* and select *System Events* to confirm that the stitch was activated.
4. Go to *Security Fabric > Automation* to see the last time that the stitch was triggered.

Diagnose commands

To enable log dumping:

```
# diagnose test application autod 1
autod dumped total:1 logs, num of logids:1
autod log dumping is enabled

vdom:root(0) logid:32002 len:408 log:
date=2019-05-30 time=17:41:03 logid="0100032002" type="event" subtype="system" level="alert"
vd="root" eventtime=1559263263858888451 tz="-0700" logdesc="Admin login failed" sn="0"
user="admin" ui="http(10.6.30.254)" method="http" srcip=10.6.30.254 dstip=10.6.30.5
action="login" status="failed" reason="passwd_invalid" msg="Administrator admin login failed
from http(10.6.30.254) because of invalid password"
autod log dumping is disabled

autod logs dumping summary:
        logid:32002 count:1

autod dumped total:1 logs, num of logids:1
```

To show the automation settings:

```
# diagnose test application autod 2
csf: enabled   root:yes
total stitches activated: 2

stitch: badLogin
       destinations: all
       trigger: badLogin

       local hit: 6 relayed to: 6 relayed from: 6
       actions:
               Send Log To Server type:webhook interval:0
                       delay:0 required:no
                       proto:0 method:0 port:80
                       uri: 172.16.200.44
                       http body: %%log%%
                       headers:
                       0. Header:1st Action
```

To show the automation statistics:

```
# diagnose test application autod 3

stitch: badLogin

       local hit: 1 relayed to: 1 relayed from: 1
       last trigger:Tue Sep 13 13:25:09 2022
       last relay:Tue Sep 13 13:25:09 2022

       actions:
               Send Log To Server:
                       done: 1 relayed to: 1 relayed from: 1
                       last trigger:Tue Sep 13 13:25:09 2022
```

```
                         last relay:Tue Sep 13 13:25:09 2022

logid2stitch mapping:
id:32002  local hit: 3 relayed to: 3 relayed from: 3
       badLogin

action run cfg&stats:
total:55 cur:0 done:55 drop:0
       email:
               flags:10
               stats: total:4 cur:0 done:4 drop:0
       fortiexplorer-notification:
               flags:1
               stats: total:0 cur:0 done:0 drop:0
       alert:
               flags:0
               stats: total:0 cur:0 done:0 drop:0
       disable-ssid:
               flags:7
               stats: total:0 cur:0 done:0 drop:0
       quarantine:
               flags:7
               stats: total:0 cur:0 done:0 drop:0
       quarantine-forticlient:
               flags:4
               stats: total:0 cur:0 done:0 drop:0
       quarantine-nsx:
               flags:4
               stats: total:0 cur:0 done:0 drop:0
       ban-ip:
               flags:7
               stats: total:0 cur:0 done:0 drop:0
       aws-lambda:
               flags:11
               stats: total:21 cur:0 done:21 drop:0
       webhook:
               flags:11
               stats: total:6 cur:0 done:6 drop:0
       cli-script:
               flags:10
               stats: total:4 cur:0 done:4 drop:0
       azure-function:
               flags:11
               stats: total:0 cur:0 done:0 drop:0
       google-cloud-function:
               flags:11
               stats: total:0 cur:0 done:0 drop:0
       alicloud-function:
               flags:11
               stats: total:20 cur:0 done:20 drop:0
```

Slack integration webhook

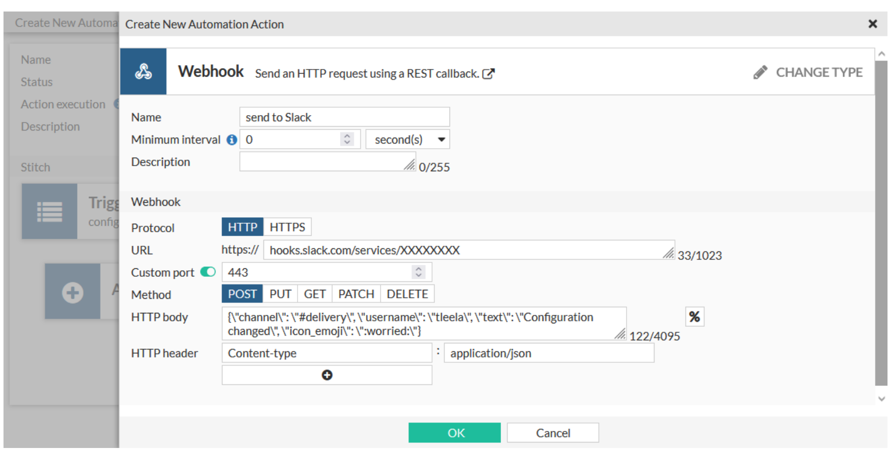
A webhook can be created to post messages and notifications to Slack.

In this example, a configuration change triggers the FortiProxy to post a message to Slack.

To create a webhook automation stitch for Slack integration in the GUI:

1. Create an incoming webhook in Slack. See Sending messages using Incoming Webhooks for more information.
2. Go to *Security Fabric > Automation*, select the *Stitch* tab, and click *Create New*.
3. Enter the stitch name.
4. Configure the trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *Configuration Change*.
   c. Enter a name (*config change*).
   d. Click *OK*.
   e. Select the trigger in the list and click *Apply*.
5. Configure the action:
   a. Click *Add Action*.
   b. Click *Create* and select *Webhook*.
   c. Enter the following:

Name	send to Slack
Protocol	HTTPS
URL	Enter the incoming webhook URL created in Slack
Custom port	Enable and enter 443
Method	POST
HTTP body	{\"channel\": \"#delivery\", \"username\": \"tleela\", \"text\": \"Configuration changed\", \"icon_emoji\": \":worried:\"}
HTTP header	Content-type : application/json



   d. Click *OK*.
   e. Select the action in the list and click *Apply*.
6. Click *OK*.

To create a webhook automation stitch for Slack integration in the CLI:

1. Create an incoming webhook in Slack. See Sending messages using Incoming Webhooks for more information.
2. Create the automation trigger:

```
config system automation-trigger
    edit "config change"
        set event-type config-change
    next
end
```

3. Create the automation action:

```
config system automation-action
    edit "send to Slack"
        set action-type webhook
        set protocol https
        set uri "hooks.slack.com/services/XXXXXXXX"
        set http-body "{\"channel\": \"#delivery\", \"username\": \"tleela\", \"text\":
\"Configuration changed\", \"icon_emoji\": \":worried:\"}"
        set port 443
        config http-headers
            edit 1
                set key "Content-type"
                set value "application/json"
            next
        end
    next
end
```

4. Create the automation stitch:

```
config system automation-stitch
    edit "Slack"
        set trigger "config change"
        config actions
            edit 1
                set action "send to Slack"
                set required enable
            next
        end
    next
end
```

Microsoft Teams integration webhook

A webhook can be created to post messages and notifications to Microsoft Teams.

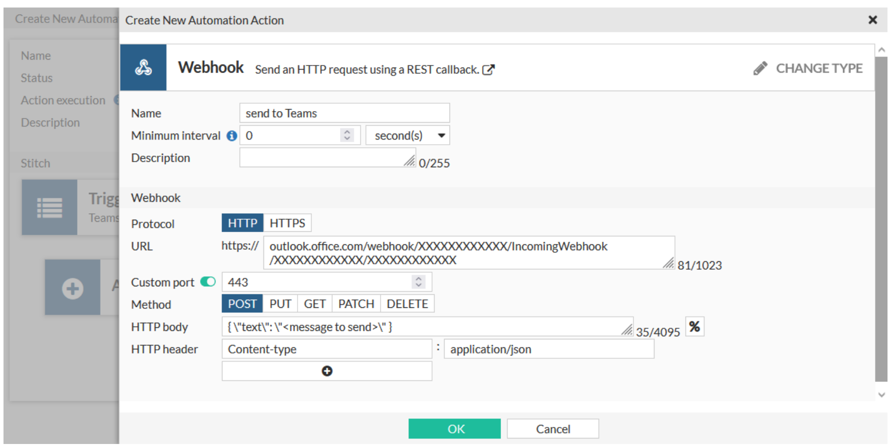
In this example, a configuration change triggers the FortiProxy to post a message to Teams.

To create a webhook automation stitch for Teams integration in the GUI:

1. Create an incoming webhook in Teams. See Create an incoming webhook for information.
2. Go to *Security Fabric* > *Automation* and click *Create New*.
3. Enter the stitch name.

4. Configure the trigger:
   a. Click *Add Trigger*.
   b. Click *Create* and select *Configuration Change*.
   c. Enter a name (*Teams*).
   d. Click *OK*.
   e. Select the trigger in the list and click *Apply*.
5. Configure the action:
   a. Click *Add Action*.
   b. Click *Create* and select *Webhook*.
   c. Enter the following:

Name	send to Teams
Protocol	HTTPS
URL	Enter the incoming webhook URL created in Teams
Custom port	Enable and enter 443
Method	POST
HTTP body	{ \"text\": \"<message to send>\" }
HTTP header	Content-type : application/json



   d. Click *OK*.
   e. Select the action in the list and click *Apply*.
6. Click *OK*.

To create a webhook automation stitch for Teams integration in the CLI:

1. Create an incoming webhook in Teams. See Create an incoming webhook for information.
2. Create the automation trigger:

```
config system automation-trigger
    edit "Teams"
        set event-type config-change
    next
end
```

3. Create the automation action:

```
config system automation-action
    edit "send to Teams"
        set action-type webhook
        set protocol https
        set uri
"outlook.office.com/webhook/XXXXXXXXXXXX/IncomingWebhook/XXXXXXXXXXXX/XXXXXXXXXXXX"
        set http-body "{ \"text\": \"<message to send>\" }"
        set port 443
        config http-headers
            edit 1
                set key "Content-type"
                set value "application/json"
            next
        end
    next
end
```

4. Create the automation stitch:

```
config system automation-stitch
    edit "Teams"
        set trigger "Teams"
        config actions
            edit 1
                set action "send to Teams"
                set required enable
            next
        end
    next
end
```

For information about more advanced messages that can be configured and sent to the Teams incoming webhook, see Sending messages to connectors and webhooks.

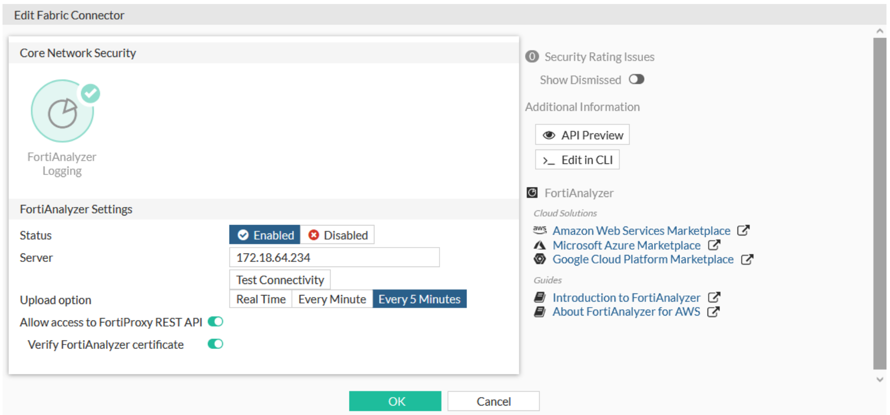
Fabric Connectors

Fabric connectors provide integration with Fortinet products to automate the process of managing dynamic security updates without manual intervention.

Creating a Security Fabric Group

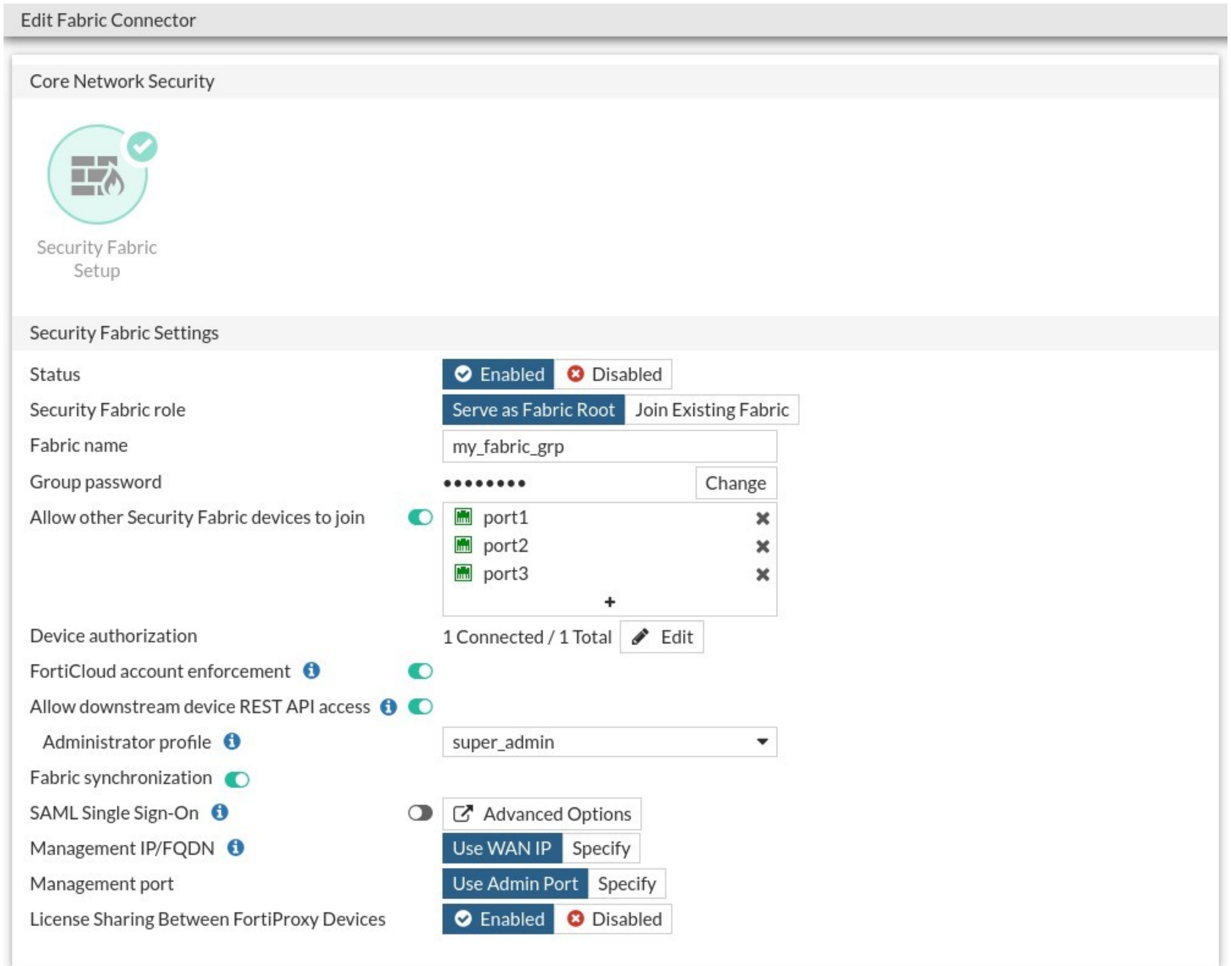
To create a Security Fabric group in the GUI:

1. Configure FortiAnalyzer logging:
   a. Go to *Security Fabric > Fabric Connectors* and double-click the *FortiAnalyzer Logging* card.
   b. Ensure the *Status* is *Enabled*, and configure the settings as needed.



   c. Click *OK*.

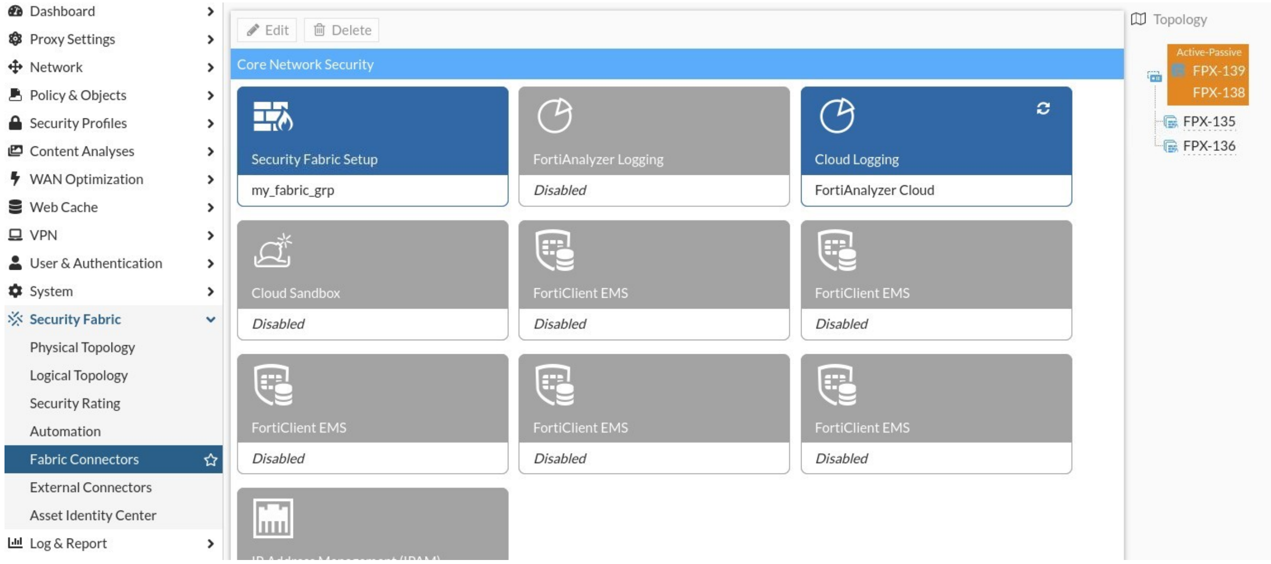
2. Configure the Security Fabric group root:
   a. Go to *Security Fabric > Fabric Connectors* and double-click the *Security Fabric Setup* card.



   b. Change *Status* to *Enabled*.
   c. In *Security Fabric role*, select *Serve as Fabric Root* to configure a Security Fabric root.
   d. In the *Fabric name* and *Group password* fields, specify the group name and password, which are required for other devices to join the group.
   e. Enable *Allow other Security Fabric devices to join*.
   f. Add members to the trusted list by clicking *Edit* next to *Device authorization* and clicking *Create New* in the *Device Authorization* panel. Fill in the license serial number of the member and specify a name. The license serial number can be retrieved by running the `get system status` command in the member device.
   g. Configure other options as needed, such as *License Sharing Between FortiProxy Devices* which specifies whether to allow the root to share licenses with other devices within the group.
   h. Click *OK*.
3. **(Optional)** Add additional members to the group by editing the root you just configured and repeat step f. Alternatively, you can add additional members by configuring a new *Security Fabric Setup* card:
   a. Go to *Security Fabric > Fabric Connectors* and double-click the *Security Fabric Setup* card.
   b. Change *Status* to *Enabled*.
   c. In *Security Fabric role*, select *Join Existing Fabric* to configure a Security Fabric member.
   d. Fill in the root device address in *Upstream FortiProxy IP/FQDN*.
   e. In the *Group password* field, enter the password you set in the root.

f. Configure other options as needed, such as *License Sharing Between FortiProxy Devices* which specifies whether to allow the device to share licenses with other devices within the group.

4. Verify the fabric group status using the fabric group topology in right-side menu on the *Security Fabric >> Fabric Connectors* page.



To create a Security Fabric group in the CLI:

1. Configure FortiAnalyzer logging:

```
config log fortianalyzer setting
    set status enable
    set server "172.18.64.234"
    set serial "FL-8HFT000000000"
    set upload-option realtime
    set reliable enable
end
```

Refer to the config log fortianalyzer setting topic in the CLI guide for more details about each option and a full list of available options.

2. Configure the security fabric group root:

```
config system csf
   set status enable
   set group-name <string>
   set downstream-access enable
   set license-sharing enable
   config trusted-list
      edit <MEMBER_DEVICE_NAME>
         set serial <LICENSE_SERIAL_OF_MEMBER_DEVICE>
         set guaranteed-seats <integer>
      next
      edit <MEMBER_DEVICE_2_NAME>
         set serial <LICENSE_SERIAL_OF_MEMBER_DEVICE_2>
         set guaranteed-seats <integer>
   next ...
end
```

When adding devices to the trusted list, you can retrieve the license serial number by running the `get system status` command in the member device.

Refer to the config system csf topic in the CLI guide for more details about each option and a full list of available options.

3. **(Optional)** Apply the following configuration to each trusted member device you defined in step 2:
```
config system csf
    set status enable
    set upstream <IP_OF_FABRIC_ROOT>
    set group-name <FABRIC_GROUP_NAME>
    set group-password <FABRIC_GROUP_PASSWORD>
    set configuration-sync local
    set license-sharing enable
end
```
When license sharing is enabled, setting `configuration-sync` to `local` disables configuration synchronization with a management device, which is recommended for license sharing.

Refer to the config system csf topic in the CLI guide for more details about each option and a full list of available options.

4. Verify the fabric group status:
   - To check connected member devices to the root, run `diag system csf downstream`. All connected devices will be listed, regardless of the authorization status.
   - To check the root device status, run `diag system csf upstream`. The connection status should be `Authorized`. If the connection status is `Authorization Rejected`, check if the member device is added to the trusted list of the root device.
   - To check the fabric group setting, run `get system csf`. The following is an example of the results from a root device:
```
status : enable
upstream :
upstream-port : 8013
group-name : my_fabric_grp
group-password : *
accept-auth-by-cert : enable
log-unification : enable
authorization-request-type: serial
fabric-workers : 2
downstream-access : enable
license-sharing : enable
downstream-accprofile: super_admin
configuration-sync : local
fabric-object-unification: local
trusted-list:
== [ 1 ]
name: 1 serial: FPX*************
ha-members:
fabric-connector:
forticloud-account-enforcement: enable
```

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

FortiClient EMS with Fabric authorization and silent approval capabilities is 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 Connectors

You can use external connectors to connect your FortiProxy unit to public and private cloud solutions. By using an external connector, you can ensure that changes to cloud environment attributes are automatically updated in the Security Fabric. You can use external connector address objects to create policies that provide dynamic access control based on cloud environment attribute changes. There is no need to manually reconfigure addresses and policies whenever changes to the cloud environment occur.

There are four steps to creating and using an external connector:

1. Gather the required information. The required information depends on which public or private cloud solution SDN connector you are configuring.
2. Create the external connector.
3. Create an external connector address.
4. Add the address to a firewall policy.

The following provides general instructions for creating an external connector and using the dynamic address object in a firewall policy.

To create an SDN connector in the GUI:

1. Go to *Security Fabric > External Connectors*.
2. Click *Create New*.
3. Click the desired public or private cloud.
4. Enter the *Name*, *Status*, and *Update interval* for the connector.
5. Enter the previously collected information for the connector as needed.
6. Click *OK*.

To create an SDN connector in the CLI:

```
config system sdn-connector
    edit <name>
        set status {enable | disable}
        set type {connector type}
        ...
        set update-interval <integer>
    next
end
```

The available CLI commands vary depending on the selected SDN connector type.

External threat feeds

Threat feeds dynamically import an external block list from an HTTP server in the form of a plain text file, or from a STIX/TAXII server. Block lists can be used to enforce special security requirements, such as long term policies to always block access to certain websites, or short term requirements to block access to known compromised locations. The lists are dynamically imported, so that any changes are immediately imported by FortiProxy.

FortiProxy can also download external threat feeds as a downstream-proxy in an isolated environment, where the upstream-proxy only has internet access. All SWG functions, including SSL deep-inspection, are performed by the downstream proxy. FDS updates and management is done on the FortiManager.

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 <name>
        set status {enable | disable}
        set type {category | address | domain | malware | url}
```

```
        set category <integer>
        set username <string>
        set password <string>
        set comments <string>
        set resource <uri>
        set user-agent <string>
        set refresh-rate <integer>
        set source-ip <ip_address>
        set interface-select-method {auto | sdwan | specify}
        set interface <interface>
        set proxy <proxy_server>
        set proxy-port <port>
        set proxy-username <username>
        set proxy-password <password>
        set server-identity-check {none | basic | full}
    next
end
```

`status {enable | disable}`	Enable/disable the user resource.
`type {category | address | domain | malware | url}`	User resource type: • `category`: FortiGuard category • `address`: Firewall IP address • `domain`: Domain name • `malware`: Malware hash • `url`: URL List
`category <integer>`	User resource category. This option is only available when `type` is `category` or `domain`.
`username <string>`	HTTP basic authentication user name.
`password <string>`	HTTP basic authentication password.
`comments <string>`	Comments.
`*resource <uri>`	URI of the external resource. Leading and tail strings are automatically removed.
`user-agent <string>`	HTTP User-Agent header (default = 'curl/7.58.0').
`*refresh-rate <integer>`	Time interval to refresh external resource, in minutes (1 - 43200, default = 5).
`source-ip <ip_address>`	Source IPv4 address used to communicate with server.
`interface-select-method {auto | sdwan | specify}`	Specify how to select outgoing interface to reach server: • `auto`: Set the outgoing interface automatically • `sdwan`: Set the outgoing interface by SD-WAN or policy routing rules • `specify`: Set the outgoing interface manually
`interface <interface>`	Specify outgoing interface to reach server. This option is only available when `interface-select-method` is `specify`.
`proxy <proxy_server>`	Proxy server host (IP or domain name).
`proxy-port <port>`	Port number that the proxy server expects to receive HTTP sessions on (1 - 65535, default = 8080).

`proxy-username <username>`	HTTP proxy basic authentication user name.
`proxy-password <password>`	HTTP proxy basic authentication password.
`server-identity-check {none | basic | full}`	Certificate verification option: • `none`: No certificate verification (default). • `basic`: Check server certificate only. • `full`: Check server certificate and domain match server certificate.

Malware hashes

The malware hash threat feed connector supports a list of file hashes that can be used as part of virus outbreak prevention. The FortiProxy unit can retrieve an external malware hash list from a remote server and poll the hash list every *n* minutes for updates. The external malware hash list can include MD5, SHA1, and SHA256 hashes.

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

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

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
```

IP addresses

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 in the GUI:

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*.

To use an external IP list object in the CLI:

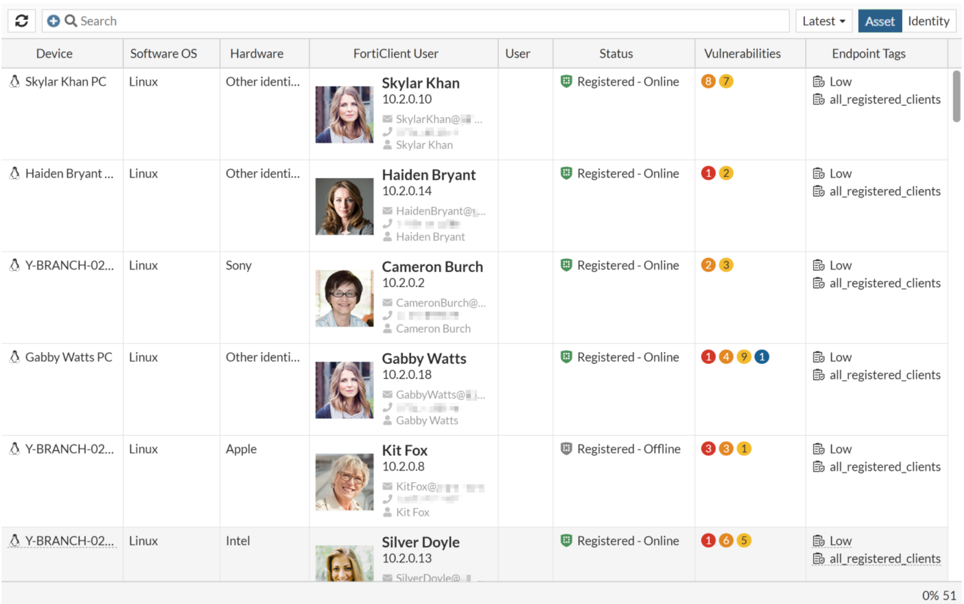
```
config system external-resource
    edit <external_resource_name>
        set type address
        set resource <string>
    next
end
```

Asset Identity Center

The *Asset Identity Center* page unifies information from detected addresses, devices, and users into a single page, while building a data structure to store the user and device information in the backend. *Asset* view groups information by *Device*, while *Identity* view groups information by *User*. Hover over a device or a user in the GUI to perform different actions relevant to the object, such as adding a firewall device address, adding an IP address, banning the IP address, quarantining the host, and more.

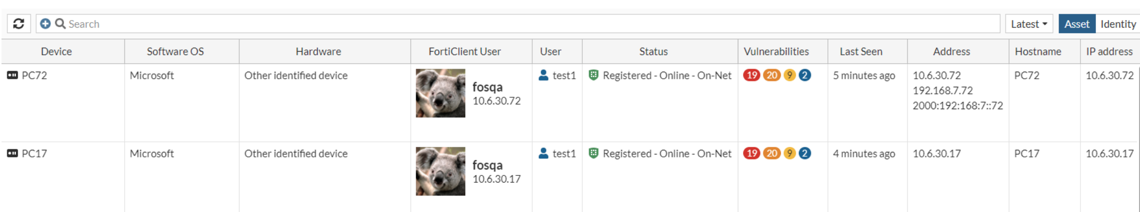
To view the Asset Identity Center page:

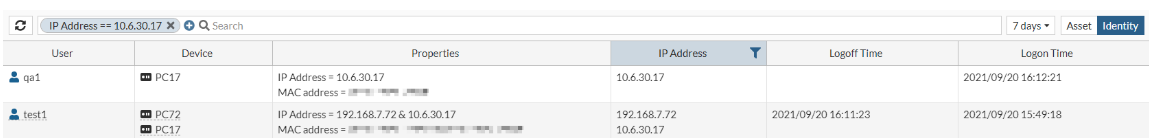
1. Go to *Security Fabric > Asset Identity Center*.
2. Click *Asset* to view information by device. The available columns are *Device*, *Software OS*, *Hardware*, *FortiClient User*, *User*, *Status*, *Vulnerabilities*, *Endpoint Tags*, and *Last Seen*. The optional columns are *Address*, *Firewall Address*, *Hostname*, *IP Address*, and *Server*.



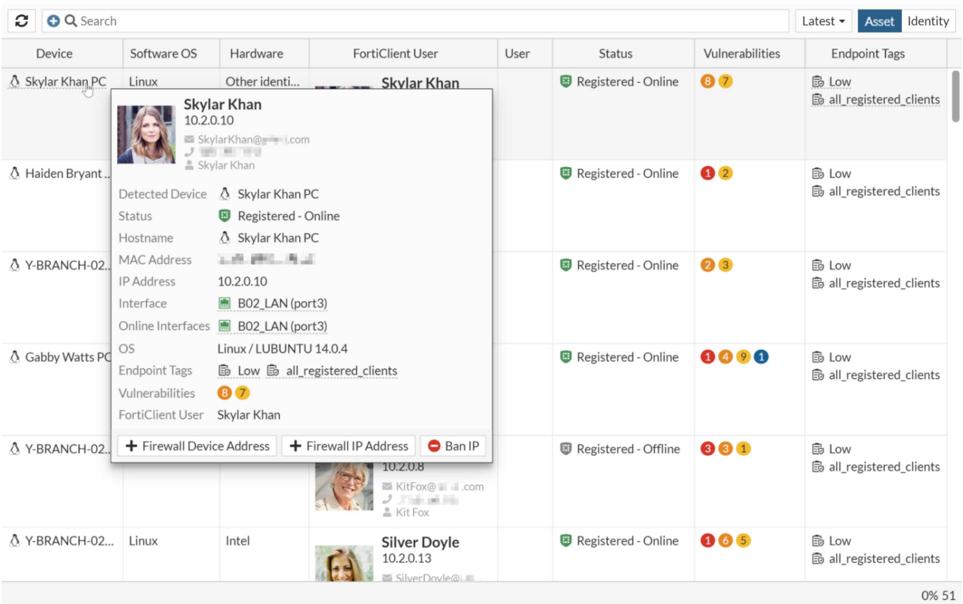
3. Click *Identity* to view information by user. The available columns are *User*, *Device*, and *Properties*. The optional columns are *IP Address*, *Logoff Time*, and *Logon Time*.

Each view has a dropdown option to view the information within different time frames (*Latest*, *1 hour*, *24 hours*, and *7 days*). Vulnerability information is displayed when applicable. The page displays user and device relationships, such as which users are logged in to multiple devices or if multiple users are logged in to single devices.





4. Hover over a device in the list to view the tooltip and possible actions. In this example, the available actions are add firewall device address, add firewall IP address, and ban the IP.



Diagnostics for the unified user device store

The following options are available for `diagnose user-device-store unified <option>`:

Option	Description
`device-memory-query`	Get device records and associated user records from memory.
`device-query`	Get device records and associated user records from memory and disk.
`user-memory-query`	Get user records and associated device records from memory.
`user-query`	Get user records and associated device records from memory and disk.
`re-query`	Retrieve query by `<query-id> <iteration-start> <iteration-count>` (takes 0-3 arguments).
`list`	List unified queries.
`clear`	Delete all unified queries.
`dump`	Dump unified query stats by `<query-id>` (takes 0-1 arguments).
`delete`	Delete unified query by `<query-id>` (takes 0-1 arguments).
`stats`	Get statistics for unified queries.
`debug`	Enable/disable debug logs for unified queries.

Log & Report

The *Log & Report* menu allows you to view and download reports and traffic, event, and security logs. Logging, archiving, and user interface settings can also be configured.

This section describes the following:

- Types of logs on page 590
- Local Reports on page 593
- Log Settings on page 593
- Threat Weight on page 597
- Email Alert Settings on page 598
- Port Exhaustion Alert on page 601

The log messages are a record of all of the traffic that passes through the FortiProxy device, and the actions taken by the device while scanning said traffic.

After a log message is recorded, it is stored in a log file. The log files can be stored on the FortiProxy device itself, on a connected FortiManager or FortiAnalyzer device, or on a FortiCloud server (you must have a FortiCloud subscription before you can configure the FortiProxy device to send logs to a FortiCloud server). The FortiProxy device's system memory or local disk can be configured to store logs.

The HTTP response code returned by the upstream content server has been added to the FortiProxy logs to aid in the debugging of content failures.

Each page of log messages contains the following controls.

Refresh	Select *Refresh* to refresh the log list.
Download Log	Select *Download Log* to download the raw log file to your local computer. The log file can be viewed in any text editor.
Add Filter	When you select the *Add Filter* button, a drop-down list appears with a list of available filtering options. Available options differ based on which log is currently being viewed.
Log Location	The location where the displayed logs are stored.
Details	Details about the selected log message. The information displayed varies depending on the type of log message selected.
Log list	The log messages. The available columns vary depending on the type of log being viewed. Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.
Page navigation	Navigate to different pages of the log list. The total number of log messages are also shown.

Debug logs

Customer Support might request a copy of your debug logs for troubleshooting.

To download the debug logs:

1. Go to *System* > *Advanced*.
2. Select *Download Debug Logs* in the Debug Logs section.

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
```

Filter WAD log messages by process types or IDs

WAD log messages can be filtered by process types or IDs. Multiple process type filters can be configured, but only one process ID filter can be configured.

```
# diagnose wad filter process-type <integer>
# diagnose wad filter process-id <integer>
```

diagnose wad filter process-type <integer>	Select process type to filter by (0 - 17, 0 = disable): • 1 = manager • 2 = dispatcher • 3 = worker • 4 = algo • 5 = informer

	• 6 = user-info • 7 = cache-service-cs • 8 = cache-service-db • 9 = cert-inspection • 10 = YouTube-filter-cache-service • 11 = user-info-history • 12 = debug • 13 = config-notify • 14 = object-cache • 15 = byte-cache • 16 = traffic aggregator • 17 = preload daemon
`diagnose wad filter process-id <integer>`	Select process id to filter by (0 = disable).

To configure multiple filters:

```
# diagnose wad filter process-type 1
# diagnose wad filter process-type 3
# diagnose wad filter process-type 16
# diagnose wad filter process-id 1115
```

To view the configured filters:

```
# diagnose wad filter list
        drop unknown sessions: disabled
        process type:
                manager
                worker
                traffic aggregator
        process id: 1115
```

Types of logs

The *Log & Report* menu allows you to view traffic logs, event logs, and security logs:

Traffic logs	
Forward Traffic	The forward traffic log includes log messages for traffic that passes through the FortiProxy device. It includes both traffic and security log messages so that messages about security events can be viewed alongside messages about the traffic at the time of the event. See also Logging client IP for forward traffic and HTTP transaction on page 60.
HTTP Transaction	HTTP transaction-related traffic log.

		To allow HTTP transaction log to appear here, make sure the *Log HTTP Transaction* option is not disabled when you Create or edit a policy on page 134. See also Logging client IP for forward traffic and HTTP transaction on page 60.
	Correlation Log	Correlation log of forward traffic log(s) and HTTP transaction log(s) that have a common session ID.
	Local Traffic	The local traffic log includes messages for traffic that terminates at the FortiProxy unit, either allowed or denied by a local policy.
	Sniffer Traffic	The sniffer log records all traffic that passes through a particular interface that has been configured to act as a One-Armed Sniffer, so it can be examined separately from the rest of the traffic logs.
	ZTNA Traffic	
Event logs		
	System Events	General system events.
	Router Events	Events relating to layer-3 routing.
	VPN Events	Events relating to VPN.
	User Events	Events relating to users.
	HA Events	Events relating to HA
	Security Rating Events	Events relating to Security Rating.
	WAN Opt. & Cache Events	Events relating to WAN optimization and cache.
	SDN Connector Events	Events relating to Fabric connectors.
	CIFS Events	Events relating to CIFS.

	REST API Events	The REST API events log subtype logs POST, PUT, DELETE, and GET REST API requests. They can be enabled or disabled in the CLI:
		`config log setting`
		`    set rest-api-set {enable | disable}`
		`    set rest-api-get {enable | disable}`
		`end`

Security logs		
	AntiVirus	The antivirus log records when, during the antivirus scanning process, the FortiProxy unit finds a match within the antivirus profile, which includes the presence of a virus or grayware signature.
	Content Analyses	

Web Filter	The web filter log records HTTP log rating errors, including web content blocking actions that the FortiProxy device performs. It also includes how long it takes to scan the HTTP request, the client request host header, the client request host inside of the request line, and the server response code.
SSL	Records detected and blocked malicious SSL connections.
DNS Query	The DNS query log messages include details of each DNS query and response. DNS log messages are recorded for all DNS traffic though the FortiProxy unit and originated by the FortiProxy unit. The detailed DNS log can be used for low-impact security investigation. Most network activity involves DNS activity of some kinds. Analyzing the DNS log can provide a lot of details about the activity on your network without using resource-intensive techniques.
File Filter	Records file filter events.
Data Leak Prevention	The data leak prevention (DLP) log provides valuable information about the sensitive data trying to get through to your network as well as any unwanted data trying to get into your network. The DLP log can record the following traffic types: • email (SMTP, POP3, or IMAP; if SSL content, SMTPS, POP3S, and IMAPS) • HTTP • HTTPS • FTP • NNTP • IM
Application Control	The Application Control log provides detailed information about the traffic that internet applications such as Skype are generating. The Application Control feature controls the flow of traffic from a specific application, and the FortiProxy unit examines this traffic for signatures that the application generates. The log messages that are recorded provide information such as the type of application being used (such as P2P software), and what type of action the FortiProxy unit took. These log messages can also help you to determine the top ten applications that are being used on your network. This feature is called Application Control monitoring and you can view the information from a widget on the Executive Summary page. The Application Control list that is used must have logging enabled within the list, as well as logging enabled within each application entry. Each application entry can also have packet logging enabled. Packet logging for Application Control records the packet when an application type is identified, similar to IPS packet logging. Logging of Application Control activity can only be recorded when an Application Control list is applied to a firewall policy, regardless of whether or not logging is enabled within the Application Control list.

Intrusion Prevention	The Intrusion Prevention log, also referred to as the attack log, records attacks that occurred against your network. Attack logs contain detailed information about whether the FortiProxy unit protected the network using anomaly-based defense settings or signature-based defense settings, as well as what the attack was. The Intrusion Prevention or attack log file is especially useful because the log messages that are recorded contain a link to the FortiGuard Center, where you can find more information about the attack. This is similar to antivirus logs, where a link to the FortiGuard Center is provided as well that informs you of the virus that was detected by the FortiProxy unit. An Intrusion Prevention sensor with log settings enabled must be applied to a firewall policy so that the FortiProxy unit can record the activity.

Local Reports

Reports provide a clear, concise overview of what is happening on your network based on log data and can be customized to serve different purposes.

To create local reports, you need to enable disk logging and local reports in *Log & Report* > *Log Settings*.

Local reports are created from logs stored on the FortiProxy unit's hard drive. These reports, generated by the FortiProxy unit itself, provide a central overview of traffic and security features on the FortiProxy unit. The default report compiles security feature activity from various security-related logs, such as virus and attack logs.

On the *Log & Report* > *Local Reports* page, you can set the frequency and timing of auto-generated reports.

You can select *Generate Now* on the *Local Reports* page to immediately create a report. After generating a report, select it from the list and then select *View*.

Local reports are marked as "Schedule-default" if created automatically or "On-Demand-default" if created by selecting *Generate Now*.

Log Settings

The type and frequency of log messages you intend to save determines the type of log storage to use. For example, if you want to log traffic and content logs, you need to configure the unit to log to a syslog server. The FortiProxy system disk is unable to log traffic and content logs because of their frequency and large file size.

Storing log messages to one or more locations, such as a syslog server, might be a better solution for your logging requirements than the FortiProxy system disk.

This topic contains information about logging to FortiAnalyzer or FortiManager units, a syslog server, and to disk.

To configure log settings, go to *Log* > *Log Settings*.


Log Settings
Local Log
Memory
Disk
Enable Local Reports
Enable Historical FortiView
Disk Usage
Logs older than 7 day(s) are deleted from the disk
Historical Disk Usage
Disk Usage
Remote Logging and Archiving
Send logs to FortiAnalyzer/FortiManager
Send Logs to FortiCloud
Send Logs to Syslog
Log Settings
Event Logging
All
Customize
Local Traffic Log
All
Customize
Log Allowed Traffic
Log Local Out Traffic
Log Denied Unicast Traffic
Log Denied Broadcast Traffic
GUI Preferences
Display Logs From
Memory
Resolve Hostnames
Resolve Unknown Applications
Apply

Configure the following settings:

Memory	Enable to store logs in the unit's memory.
Disk	Enable to store logs on the unit's disk. Enabling disk logging is required to produce data for all FortiView consoles. Logs older than 7 days are deleted from the disk.
Enable Local Reports	Enable to create local reports.
Enable Historical FortiView	Enabling Historical FortiView is required to product data for all FortiView consoles.
Send Logs to FortiAnalyzer/FortiManager	Select to send logs to a FortiAnalyzer or a FortiManager unit. HTTP transaction logs are also sent to a FortiAnalyzer unit to generate additional details in reports.
IP Address	The IP address of the FortiAnalyzer or FortiManager unit. Select *Test Connectivity* to test the connectivity with the device.
Upload option	Select how often to upload log entries: *Real Time*, *Every Minute*, or *Every 5 Minutes*.
Encrypt log transmission	Enable to encrypt logs. Encrypted logs are sent using SSL communication.
Send Logs to FortiCloud	This option is not available.
Send Logs to Syslog	Enable to send logs to a syslog server.
IP Address/FQDN	If you enable *Send Logs to Syslog*, enter the IP address or fully qualified domain name of the syslog server.
Log Settings	
Event Logging	Select *All* or select *Customize* and then select the events to log: *System activity event*, *User activity event*, *Router activity event*, *Explicit web proxy event*, *HA event*, *Compliance Check Event*, and *Security audit event*.
Local Traffic Log	Select *All* or select *Customize* and then select the local traffic to log: *Log Allowed Traffic*, *Log Denied Unicast Traffic*, *Log Local Out Traffic*, and *Log Denied Broadcast Traffic*.
GUI Preferences	
Display Logs From	Select where logs are displayed from: *Memory* or *Disk*.
Resolve Hostnames	Enable to resolve host names using reverse DNS lookup.
Resolve Unknown Applications	Enable to resolve unknown applications using the Internet Service Database.

Memory debugging

Memory on FortiProxy might appear high, even on an unloaded system; however, this level is not usually cause for concern because available memory is used to improve the disk-caching performance and is returned to the system if needed.

To enable debugging of memory status in cases of high memory usage and to confirm that there is no issue, use the following CLI commands to show memory use by each WAD-worker and cache-service memory usages.

CLI syntax

```
diagnose wad memory <ssl | ssh>
```

```
diagnose wad <worker | csvc> memory stats <basic | misc>
```

The TAC report generated by `execute tac report` includes the WAD memory usage statistics.

Local logging and archiving

The FortiProxy system can store log messages on disk. It can store traffic and content logs on the system disk or disks. When the log disk is full, logging to disk can either be suspended, or the oldest logs can be overwritten.

Remote logging to a syslog server

A syslog server is a remote computer running syslog software and is an industry standard for logging. Syslog is used to capture log information provided by network devices. The syslog server is both a convenient and flexible logging device because any computer system, such as Linux, Unix, and Intel-based Windows can run syslog software.

When configuring logging to a syslog server, you need to configure the facility and the log file format, which is either normal or Comma Separated Values (CSV). The CSV format contains commas, whereas the normal format contains spaces. Logs saved in the CSV file format can be viewed in a spreadsheet application, while logs saved in normal format are viewed in a text editor because they are saved as plain text files.

Configuring a facility easily identifies the device that recorded the log file. You can choose from many different facility identifiers, such as daemon or local7.

If you are configuring multiple syslog servers, configuration is available only in the CLI. You can also enable the reliable delivery option for syslog log messages in the CLI.

If you are configuring multiple syslog servers, configuration is available only in the CLI. You can also enable the reliable delivery option for syslog log messages in the CLI.

From the CLI, you can enable reliable delivery of syslog messages using the following commands:

```
config log {syslogd | syslogd2 | syslogd3 |syslogd4} setting
   set status enable
   set reliable enable
end
```

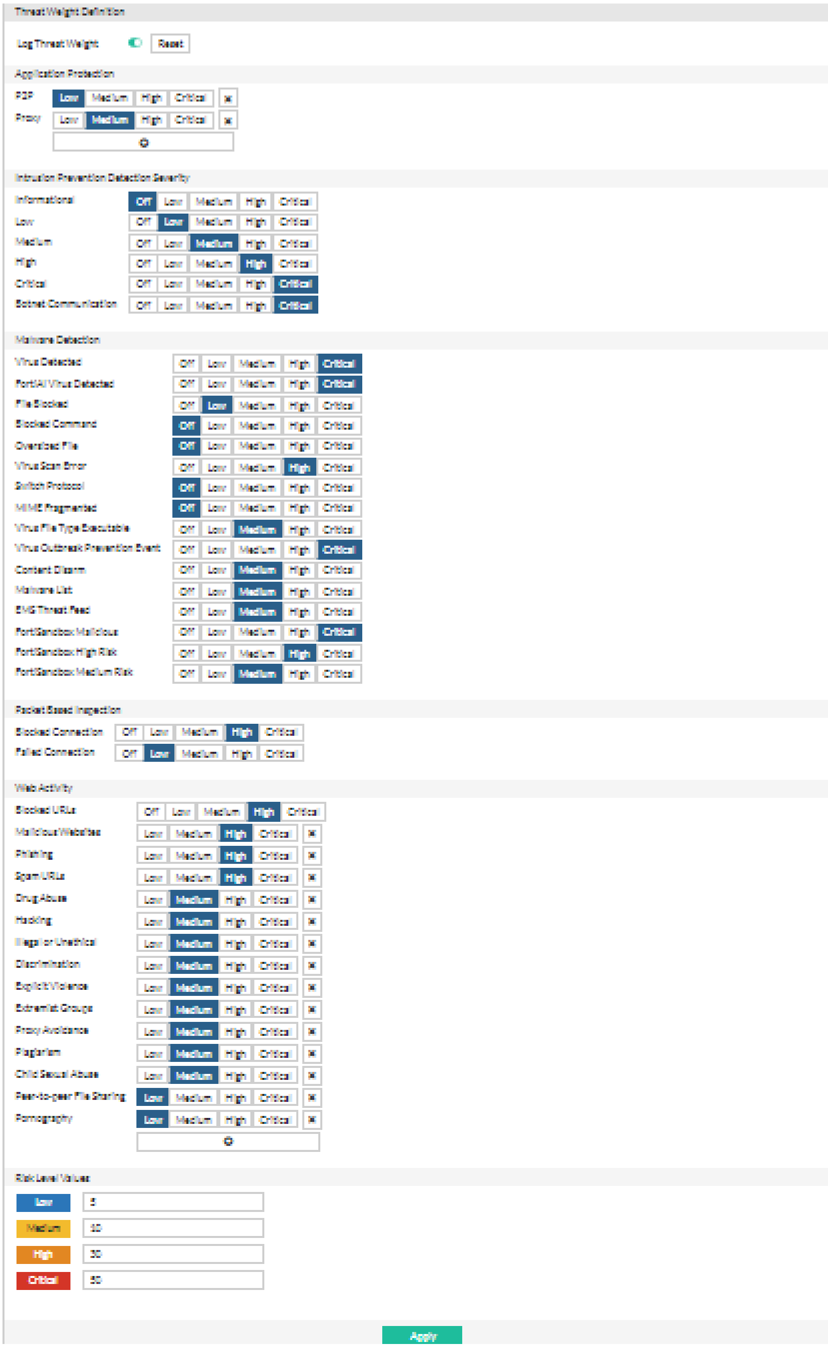
The FortiProxy unit implements the RAW profile of RFC 3195 for reliable delivery of log messages. Reliable syslog protects log information through authentication and data encryption and ensures that the log messages are reliably delivered in the correct order. This feature is disabled by default.

If more than one syslog server is configured, the syslog servers and their settings appear on the Log Settings page. You can configure multiple syslog servers in the CLI using the `config log {syslogd | syslogd2 | syslogd3 | syslogd4} settings` CLI command.

You can specify the source IP address of self-originated traffic when configuring a syslog server; however, this is available only in the CLI.

Threat Weight

Go to *Log & Report* > *Threat Weight* to change the threat weight definition.



Email Alert Settings

Alert email messages provide notification about activities or events logged. These email messages also provide notification about the log severity level, such as a critical or emergency.

You can send alert email messages to up to three email addresses. Alert messages are also logged and can be viewed from the System Events log file.

You can use the alert email feature to monitor logs for log messages, and to send email notification about a specific activity or event logged. For example, if you require notification about administrators logging in and out, you can configure an alert email that is sent whenever an administrator logs in and out. You can also base alert email messages on the severity levels of the logs.

Before configuring alert email, you must configure at least one DNS server if you are configuring with an Fully Qualified Domain Server (FQDN). The FortiProxy unit uses the SMTP server name to connect to the mail server, and must look up this name on your DNS server. You can also specify an IP address.

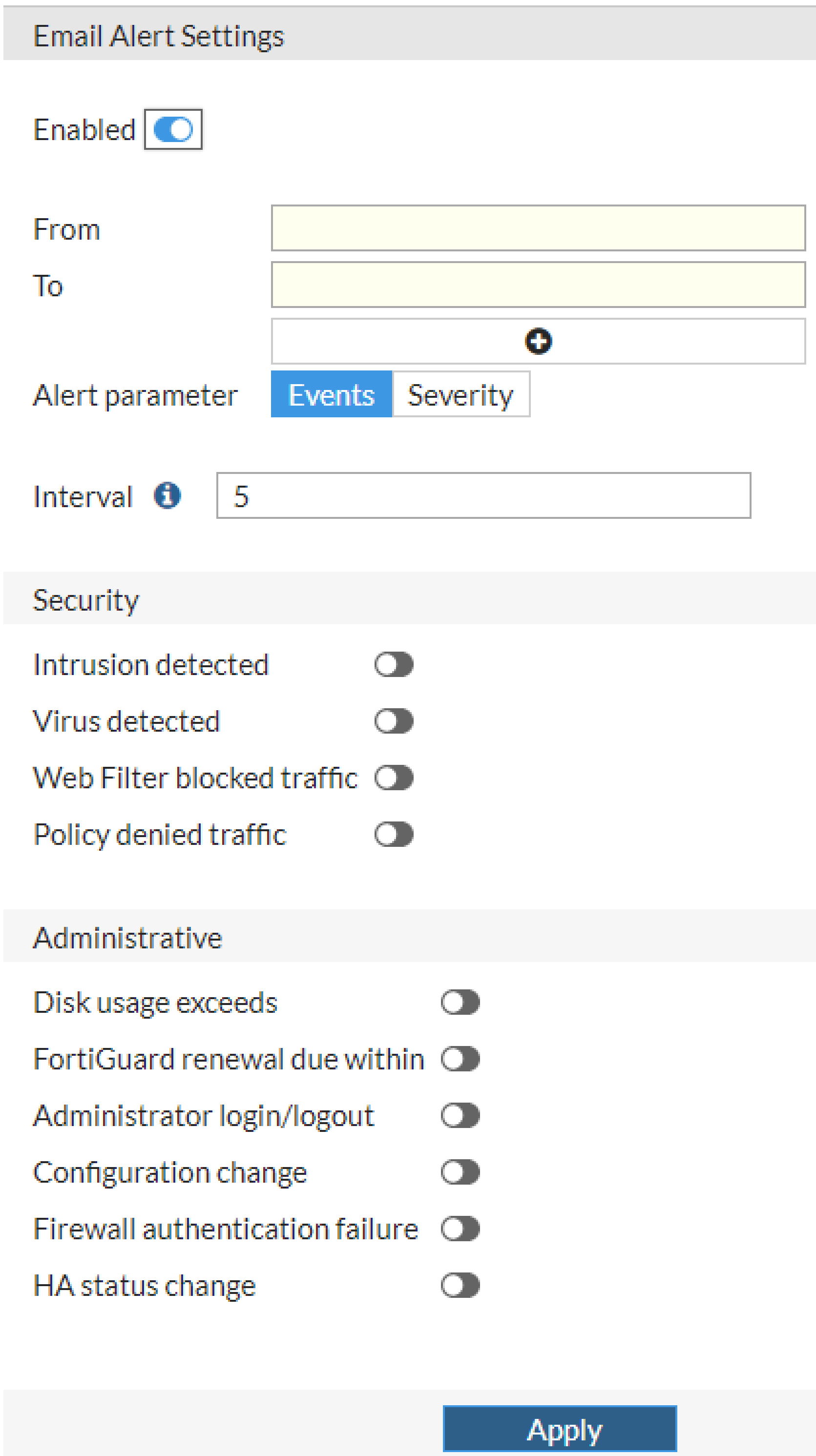
> The default minimum log severity level is Alert. If the FortiProxy unit collects more than one log message before an interval is reached, the FortiProxy unit combines the messages and sends out one alert email.

How to configure email notifications

The following procedure explains how to configure an alert email notification for IPsec tunnel errors, firewall authentication failure, configuration changes and FortiGuard license expiry.

1. In *System* > *Advanced*, under *Email Service*, enable *Use Custom Email Server* and configure the SMTP server.

   The SMTP server settings allow the FortiProxy unit to know exactly where the email will be sent from, as well as who to send it to. The SMTP server must be a server that does not support SSL/TLS connections; if the SMTP server does, the alert email configuration will not work. The FortiProxy unit does not currently support SSL/TLS connections for SMTP servers.
2. In *Log* > *Email Alert Settings*, toggle *Enabled*, configure the email alert settings as described in the table, and select *Apply* to save your changes.



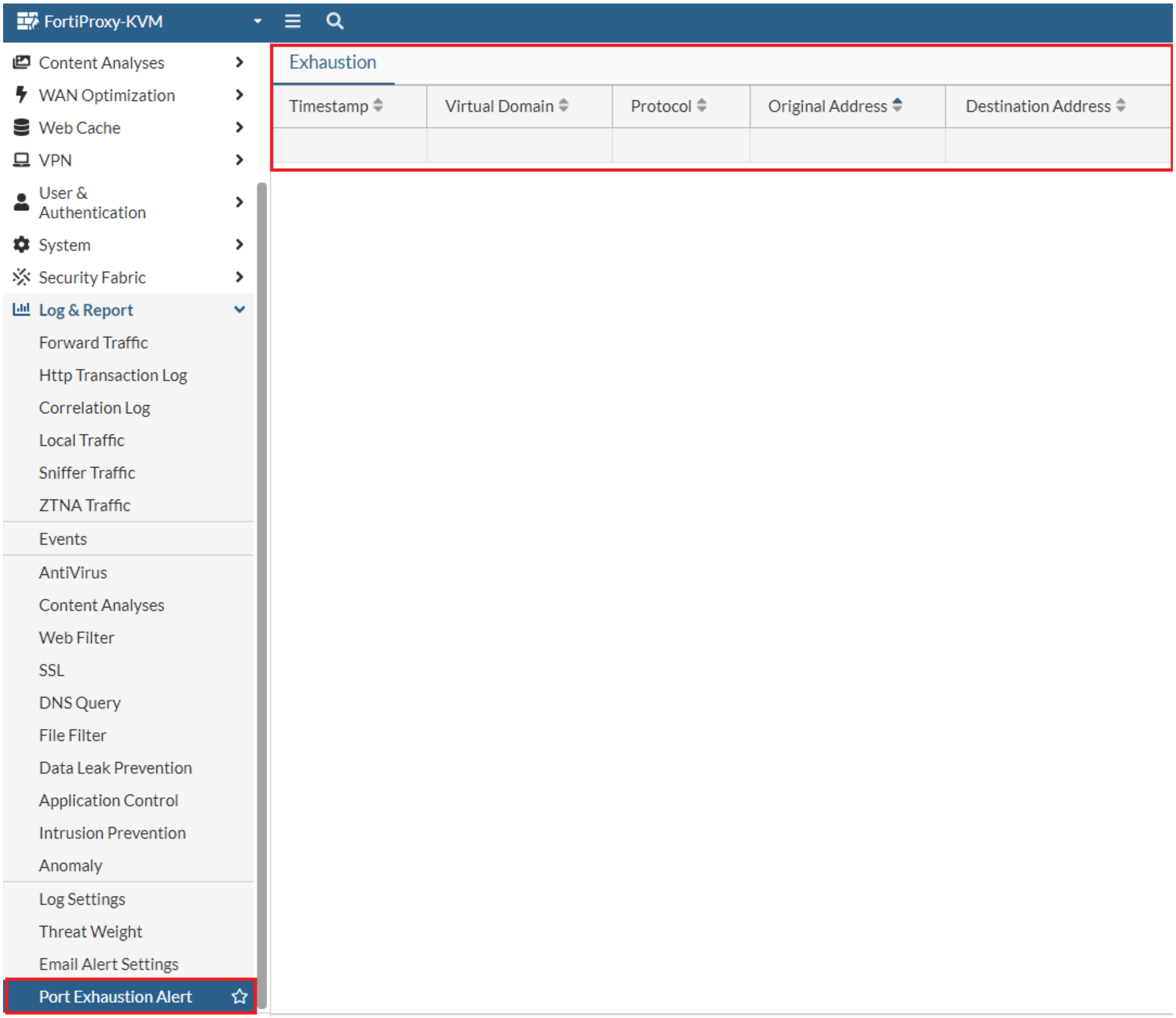
Configure the following settings:

From	Enter the source email address.
To	Enter up to three target email addresses.

Alert parameter	If you select *Events*, enter the number of minutes in *Interval* and enable the events that will cause email alerts to be sent. If you select *Severity*, select the event priority level for email alerts to be sent in the *Minimum level* drop-down list. The priority level indicates the immediacy and the possible repercussions of the event. There are eight priority levels from *Debug* (lowest priority) to *Emergency* (highest priority). The default priority level is *Alert*.
Interval	Select the number of minutes between email alerts, from 1 to 99,999 minutes. The default is 5 minutes.
Intrusion detected	Enable to send an email alert when an intrusion is detected.
Virus detected	Enable to send an email alert when a virus is detected.
Web Filter blocked traffic	Enable to send an email alert when a web filter blocked traffic.
Policy denied traffic	Enable to send an email alert when a policy denied traffic.
Disk usage exceeds	Enable and enter a percentage to send an email alert when the disk usage exceeds the specified level. The default is 75%.
FortiGuard renewal due within	Enable and enter the number of days to send an email alert before FortiGuard must be renewed.
Administrator login/logout	Enable to send an email alert when an administrator logs in or out of the FortiProxy unit.
Configuration change	Enable to send an email alert when the FortiProxy configuration has been changed.
Firewall authentication failure	Enable to send an email when traffic fails authentication.
HA status change	Enable to send an email when there is a change in the HA status.

Port Exhaustion Alert

The *Port Exhaustion Alert* tab displays port exhaustion events with timestamp, virtual domain, protocol, and address information of the exhaustion. When a port exhaustion occurs, an alert appears next to *Log & Report* and *Port Exhaustion Alert* until the event expires.



You can also use the following logs to learn about source port usage:

- High source port usage—This log is recorded when more than half of the available source ports on an IP is in use during the last few consecutive attempts of the FortiProxy to get a source port.
- Source port exhaustion—This log is recorded when no available source port can be found for a source IP.

Appendices

Perl regular expressions

The following table lists and describes some examples of Perl regular expressions.

Expression	Matches
abc	"abc" (the exact character sequence but anywhere in the string).
^abc	"abc" at the beginning of the string.
abc$	"abc" at the end of the string.
a|b	Either "a" or "b".
^abc|abc$	The string "abc" at the beginning or at the end of the string.
ab{2,4}c	"a" followed by two, three, or four "b"s followed by a "c".
ab{2,}c	"a" followed by at least two "b"s followed by a "c".
ab*c	"a" followed by any number (zero or more) of "b"s followed by a "c".
ab+c	"a" followed by one or more "b"s followed by a "c".
ab?c	"a" followed by an optional "b" followed by a "c"; that is, either "abc" or "ac".
a.c	"a" followed by any single character (not newline) followed by a "c".
a\.c	"a.c" exactly.
[abc]	Any one of "a", "b", and "c".
[Aa]bc	Either of "Abc" and "abc".
[abc]+	Any (nonempty) string of "a"s, "b"s and "c"s (such as "a", "abba", "acbabcacaa").
[^abc]+	Any (nonempty) string that does not contain any of "a", "b", and "c" (such as "defg").
\d\d	Any two decimal digits, such as 42; same as \d{2}.
/i	Makes the pattern case insensitive. For example, /bad language/i blocks any instance of "bad language" regardless of case.
\w+	A "word": A nonempty sequence of alphanumeric characters and low lines (underscores), such as "foo", "12bar8", and "foo_1".
100\s*mk	The strings "100" and "mk" optionally separated by any amount of white space (spaces, tabs, and newlines).
abc\b	"abc" when followed by a word boundary (for example, in "abc!" but not in "abcd").
perl\B	"perl" when not followed by a word boundary (for example, in "perlert" but not in "perl stuff").
\x	Tells the regular expression parser to ignore white space that is neither preceded by a backslash character nor within a character class. Use this to break up a regular expression into slightly more readable parts.

Expression	Matches
/x	Used to add regular expressions within other text. If the first character in a pattern is forward slash “/”, the “/” is treated as the delimiter. The pattern must contain a second “/”. The pattern between the “/” is taken as a regular expression, and anything after the second “/” is parsed as a list of regular expression options (“i”,“x”, and so on). An error occurs if the second “/” is missing. In regular expressions, the leading and trailing space is treated as part of the regular expression.

Block common spam phrases

Block common phrases found in spam messages with the following expressions:

```
/try it for free/i
/student loans/i
/you’re already approved/i
/special[\+\-\*=<>\.\,;!\?%&~#§@\^°\$£€\{\}()\[\]\|\\_1]offer/i
```

Block purposely misspelled words

Random characters are often inserted between the letters of a word to bypass spam-blocking software. The following expressions can help to block those messages:

```
/^.*v.*i.*a.*g.*r.*o.*$/i
/cr[eéèêë][\+\-\*=<>\.\,;!\?%&§@\^°\$£€\{\}()\[\]\|\\_01]dit/i
```

Block any word in a phrase

Use the following expression to block any word in a phrase:

```
/block|any|word/
```

Preload cache content and web crawler

You can configure FortiProxy to pre-load cache content based on manually defined URL patterns with scheduled crawling function. This feature is useful for schools and hotels where popular content, such as video, can be predicted ahead of schedule, downloaded outside of peak hours, and viewed by customers using the cache.

The following `execute preload` CLI commands list and describe configurable preload caching and web crawler options.

execute preload list

Use this command to show currently active URLs and their run schedules:

```
execute preload list
```

For example:

```
URL's scheduled for preload:
http://google.com
    Depth: 0, runs every 1 minutes, next run at Dec 23 16:49
http://google.ca
    Depth: 5, runs every 2 minutes, next run at Dec 23 16:52
https://news.cnn.com
    Depth: 1, runs every 5 minutes, next run at Dec 23 18:47
```

execute preload show-log

Use this command to display all the completed operations and their status.

execute preload url

Use this command to schedule a crawl, preload, refresh, or pin request for a given URL:

```
execute preload url <url> <depth> <at_time> <repeat_after> <repetitions> <user-agent>
<password>
```

- **<url>:** URL to preload.
- **<depth>:** Depth of preload.
- **<at_time>:** In the format of HHH:MM. HHH is hours from present (between 0-672), and MM is minutes from present (between 0-59). The default is set to 0:00.
- **<repeat_after>:** HHH:MM. Set HHH between 0-168 and MM between 0-59. The default is set to 168:59 (max).
- **<repetitions>:** End after this many repetitions (between 1-365). The default is set to 1.
- **<user-agent>:** Specify client type (free text) to identify as a user agent. The default is set to "Wget/1.17 (linux-gnu)".
- **<user>:** Specify user name.
- **<password>:** Password for the user (asked for in a separate prompt).

execute preload url-delete

Use this command to delete a scheduled crawl, preload, refresh, or pin request for a given URL:

```
execute preload url-delete <url>
```

Use the following command, for example, to delete all operations for `http://www.fortinet.com`:

```
execute preload url-delete http://www.fortinet.com/
```

To view a list of pending crawls, see execute preload list on page 606.

Examples

The following command would fetch `http://www.fortinet.com` and do the following:

- preload cache immediately:

  ```
  execute preload url http://www.fortinet.com/
  ```

- crawl it to depth two immediately:

  ```
  execute preload url http://www.fortinet.com/ 2
  ```

- crawl it to depth two after ten minutes:

  ```
  execute preload url http://www.fortinet.com/ 2 00:10
  ```

- crawl it to depth two after ten minutes and after 24 hours 30 times (that is,fetch the URL in ten minutes and every day for 30 days):

  ```
  execute preload url http://www.fortinet.com/ 2 00:10 24:00 30
  ```

- crawl with the user agent “Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0”:

  ```
  execute preload url http://www.fortinet.com/ 0 00:00 00:01 1 "Mozilla/5.0 (Macintosh;
  Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0"
  ```

Automatic backup to an FTP or TFTP server

You can schedule automatic FortiProxy backups to an FTP or TFTP server.

Manual backups to a remote FTP or TFTP using IPv4

To manually back up the full FortiProxy configuration to a remote FTP server:

```
execute backup full-config ftp <configuration_file_name> <FTP_server_IPv4_address> <user_
name> <password>
```

To manually back up the full FortiProxy configuration to a remote TFTP server:

```
execute backup full-config tftp <configuration_file_name> <TFTP_server_IPv4_address>
<password>
```

Specifying a password is optional for backing up to a TFTP server.

Manual backups to a remote FTP or TFTP using IPv6

IPv6 addresses are 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
```

Scheduled automatic backups with an auto script

Use an auto script to schedule a FortiProxy backup and to define how many times to repeat the backup. The auto script overrides the existing configuration file with the same name. Auto script does not support keeping all of the hourly configuration files. When using the `%%PASSWD%%` variable in the script, the variable is replaced by the `password` setting and encrypted.

The following example shows how to automate the hourly backup of the FortiProxy configuration to an FTP server.

FTP server: `10.1.5.241`

FTP user: `ftp_user`

FTP user password: `ftppassword`

Name of the configuration file: `FPX1_autoScript.conf`

```
config system auto-script
    edit "hourly_config_backup"
        set interval 3600
        set repeat 0
        set start auto
        set script "execute backup full-config ftp FPX1_autoScript.conf 10.1.5.241 ftp_user
%%PASSWD%%"
        set password ftppassword
    next
end
```

If the FTP auto script was executed successfully, the following is the result:

```
FPX1 $  execute auto-script status
========== #1, 2019-07-29 09:00:01 ==========
FPX1 $  execute backup full-config ftp FPX1_autoScript.conf 10.1.5.241 ftp_user ftppassword

Connect to ftp server 10.1.5.241 ...
Please wait...
Send config file to ftp server OK.

========== #2, 2019-07-29 10:00:01 ==========
FPX1 $  execute backup full-config ftp FPX1_autoScript.conf 10.1.5.241 ftp_user ftppassword

Connect to ftp server 10.1.5.241 ...
Please wait...
Send config file to ftp server OK.
```

The following example shows to automate the hourly backup of the FortiProxy configuration to a TFTP server:

```
config system auto-script
    edit "hourly_config_backup"
        set interval 3600
        set repeat 0
        set start auto
        set script "execute backup full-config tftp FPX1_autoScript.conf 10.1.5.241"
    next
end
```

The following is the full syntax of the auto-script CLI commands:

```
config system auto-script
    edit <name>
        set name <string>
        set interval <integer>
        set repeat <integer>
        set start {manual | auto}
        set script <string>
        set password <string>
        set output-size <integer>
        set timeout <integer>
```

```
    next
end
```

`name <string>`	Auto script name. The size is 35 characters.
`interval <integer>`	Repeat interval, in seconds (0 - 31557600, default = 0).
`repeat <integer>`	Number of times to repeat this script (0 - 65535, 0 = infinite, default = 1).
`start {manual | auto}`	Script starting mode. • `manual`: Starting manually (default). • `auto`: Starting automatically.
`script <string>`	List of FortiProxy CLI commands to repeat. The maximum size is 1023 characters.
`password <string>`	Script password to replace %%PASSWD%% tag in the script. Use cases include replacing a password tag for SFTP/FTP server password.
`output-size <integer>`	Number of megabytes to limit script output to (10 - 1024, default = 10).
`timeout <integer>`	Maximum running time for this script, in seconds (0 - 300, 0 = no timeout, default = 0).

Manual backups with SCP

You can use the secure copy protocol (SCP) to perform manual backups of the FortiProxy configuration.

1. To enable SCP, run the following commands:

   ```
   config system global
       set admin-scp enable
   end
   ```

2. Enable the SSH administrative access on the interface handling the SCP services.
3. Use any Linux client to download the FortiProxy configuration file using the following command:

   ```
   $ scp admin@<FortiProxy_IP>:sys_config <location>
   ```

The following example is run using Lubuntu 19.04. This backup runs one time from the Linux client.

```
$ scp admin@10.1.5.252:sys_config ~/config/"FPX.autobackup.$(date +%Y%m%d_%H%M%S).conf"
```

The example downloads the configuration file and saves it to the `~/config` folder with a file name of `FPX.autobackup.$(date +%Y%m%d_%H%M%S).conf`.

Using `$(date +%Y%m%d_%H%M%S)` ensures that each configuration file has a unique file name, for example, `FPX.autobackup.20190729_110001.conf`.

Scheduled automatic backups with SCP

To perform an hourly automatic backup, you need to run the SCP command as a cron job.

For example, you can use a bash script to run hourly backups with all the configuration files saved in the `~/config` folder.

NOTE: Remember to change the IP address to your own FortiProxy IP address before adding the following command to a cron job. If the `~/config` folder does not already exist, you need to create it before running the cron job.

```
#!bin/bash

# This command will pull a copy of the FortiProxy (10.1.5.252) using SCP on port 10104
# and save the config to the ~/config folder with the file-naming convention of
# FPX.autobackup.$(date +%Y%m%d_%H%M%S).conf

scp -P 10104 admin@10.1.5.252:sys_config ~/config/"FPX.autobackup.$(date
     +%Y%m%d_%H%M%S).conf"
```

Save the bash script file to `~/auto_backup/hourly_backup.sh`.

Add execution permission to the bash script file:

```
$ sudo chmod +x ~/auto_backup/hourly_backup.sh
```

Run the `ls -l` command on the Linux client:

```
lubuntu@lubuntu-pc:~/auto_backup$ ls -l
total 4
-rwxr-xr-x 1 lubuntu lubuntu 106 Jul 29 14:41 hourly_backup.sh
lubuntu@lubuntu-pc:~/auto_backup$
```

To add the bash script to the cron table file, use the following command:

```
$ sudo crontab -e

# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task.
#
# To define the time, you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and time zones.
#
# Output of the cron table jobs (including errors) is sent through
# email to the user the cron tab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m. every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information, see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
@hourly ~/auto_backup/hourly_backup.sh <==== Add this to the file and save it.
```

You can change the `@hourly` to `@monthly` or `@weekly` or `@daily`.

To verify that the backups were run correctly, look at the contents of the `~/config` folder:

```
lubuntu@lubuntu-pc:~/config$ ls -l
total 784
-rw------- 1 lubuntu lubuntu 197872 Jul 29 11:00 FPX.autobackup.20190729_110001.conf
```

```
-rw------- 1 lubuntu lubuntu 197872 Jul 29 12:00 FPX.autobackup.20190729_120001.conf
-rw------- 1 lubuntu lubuntu 197872 Jul 29 13:00 FPX.autobackup.20190729_130001.conf
-rw------- 1 lubuntu lubuntu 197872 Jul 29 14:00 FPX.autobackup.20190729_140001.conf
lubuntu@lubuntu-pc:~/config$
```

Custom signature keywords

- information
- session
- content
- IP header
- TCP header
- UDP header
- ICMP
- other

Information keywords

attack_id

Syntax: `--attack_id <id_int>;`

Description:

Use this optional value to identify the signature. It cannot be the same value as any other custom rules. If an attack ID is not specified, the FortiProxy automatically assigns an attack ID to the signature.

An attack ID you assign must be between 1000 and 9999.

Example: `--attack_id 1234;`

name

Syntax: `--name <name_str>;`

Description:

Enter the name of the rule. A rule name must be unique. The name you assign must be a string greater than 0 and less than 64 characters in length.

Example: `--name "Buffer_Overflow";`

Session keywords

flow

Syntax: `--flow {from_client[,reversed] | from_server[,reversed] | bi_direction };`

Description:

Specify the traffic direction and state to be inspected. They can be used for all IP traffic.

Example: `--src_port 41523; --flow bi_direction;`

The signature checks traffic to and from port 41523.

If you enable “quarantine attacker”, the optional reversed keyword allows you to change the side of the connection to be quarantined when the signature is detected.

For example, a custom signature written to detect a brute-force log in attack is triggered when “Login Failed” is detected from_server more than 10 times in 5 seconds. If the attacker is quarantined, it is the server that is quarantined in this instance. Adding reversed corrects this problem and quarantines the actual attacker.

service

Syntax: `--service {HTTP | TELNET | FTP | DNS | SMTP | POP3 | IMAP | SNMP | RADIUS | LDAP | MSSQL | RPC | SIP | H323 | NBSS | DCERPC | SSH | SSL};`

Description:

Specify the protocol type to be inspected. This keyword allows you to specify the traffic type by protocol rather than by port. If the decoder has the capability to identify the protocol on any port, the signature can be used to detect the attack no matter what port the service is running on. Currently, HTTP, SIP, SSL, and SSH protocols can be identified on any port based on the content.

app_cat

Syntax: `--app_cat <category_int>;`

Description:

Specify the category of the application signature. Signatures with this keyword are considered as application rules. These signatures will appear under Application Control instead of IPS configuration. To display a complete list of application signature categories, enter the following CLI commands:

```
config application list
   edit default
      config entries
         edit 1
            set category ?
```

weight

Syntax: `--weight <weight_int>;`

Description:

Specify the weight to be assigned to the signature. This keyword allows a signature with the higher weight to have priority over a signature with a lower weight. This is useful to prioritize between custom and stock signatures and also between different custom signatures.

The weight must be between 0 an 255. Most of the signatures in the Application Control signature database have weights of 10; botnet signatures are set to 250. A range of 20 to 50 is recommended for custom signatures.

Content keywords

byte_extract

Syntax: `byte_extract:<bytes_to_extract>, <offset>, <name> \ [, relative][, multiplier <multiplier value>][, <endian>]\ [, string][, hex][, dec][, oct][, align <align value>][, dce];`

Description:

Use the `byte_extract` option to write rules against length-encoded protocols. This reads some of the bytes from the packet payload and saves it to a variable.

byte_jump

Syntax: `--byte_jump <bytes_to_convert>, <offset>[, multiplier][, relative] [, big] [, little] [, string] [, hex] [, dec] [, oct] [, align];`

Description:

Use the `byte_jump` option to extract a number of bytes from a packet, convert them to their numeric representation, and jump the match reference up that many bytes (for further pattern matching or byte testing). This keyword allows relative pattern matches to take into account numerical values found in network data. The available keyword options include:

- `<bytes_to_convert>`: The number of bytes to examine from the packet.
- `<offset>`: The number of bytes into the payload to start processing.
- `[multiplier]`: multiplier is optional. It must be a numerical value when present. The converted value multiplied by the number is the result to be skipped.
- `relative`: Use an offset relative to last pattern match.
- `big`: Process the data as big endian (default).
- `little`: Process the data as little endian.
- `string`: The data is a string in the packet.
- `hex`: The converted string data is represented in hexadecimal notation.
- `dec`: The converted string data is represented in decimal notation.
- `oct`: The converted string data is represented in octal notation.
- `align`: Round up the number of converted bytes to the next 32-bit boundary.

byte_test

Syntax: `--byte_test <bytes_to_convert>, <operator>, <value>, <offset>[multiplier][, relative] [, big] [, little] [, string] [, hex] [, dec] [, oct];`

Description:

Use the `byte_test` keyword to compare a byte field against a specific value (with operator). This keyword is capable of testing binary values or converting representative byte strings to their binary equivalent and testing them. The available keyword options include:

- `<bytes_to_convert>`: The number of bytes to compare.
- `<operator>`: The operation to perform when comparing the value (<,>,=,!,&).
- `<value>`: The value to compare the converted value against.
- `<offset>`: The number of bytes into the payload to start processing.
- `[multiplier]`: multiplier is optional. It must be a numerical value when present. The converted value multiplied by the number is the result to be skipped.
- `relative`: Use an offset relative to last pattern match.
- `big`: Process the data as big endian (default).
- `little`: Process the data as little endian.
- `string`: The data is a string in the packet.
- `hex`: The converted string data is represented in hexadecimal notation.
- `dec`: The converted string data is represented in decimal notation.
- `oct`: The converted string data is represented in octal notation.

depth

Syntax: `--depth <depth_int>;`

Description:

Use the depth keyword to search for the contents within the specified number of bytes after the starting point defined by the offset keyword. If no offset is specified, the offset is assumed to be equal to 0.

If the value of the depth keyword is smaller than the length of the value of the content keyword, this signature will never be matched.

The depth must be between 0 and 65535.

distance

Syntax: `--distance <dist_int>;`

Description:

Use the distance keyword to search for the contents within the specified number of bytes relative to the end of the previously matched contents. If the within keyword is not specified, continue looking for a match until the end of the payload.

The distance must be between 0 and 65535.

content

Syntax: `--content [!]"<content_str>";`

Description:

Deprecated. See pattern on page 622 and context on page 618 keywords. Use the content keyword to search for the content string in the packet payload. The content string must be enclosed in double quotes.

To have the FortiProxy unit search for a packet that does not contain the specified context string, add an exclamation mark (!) before the content string.

Multiple content items can be specified in one rule. The value can contain mixed text and binary data. The binary data is generally enclosed within the pipe (|) character.

The double quote ("), pipe sign(|) and colon(:) characters must be escaped using a back slash if specified in a content string.

If the value of the content keyword is greater than the length of the value of the depth keyword, this signature will never be matched.

context

Syntax: `--context {uri | header | body | host};`

Description:

Specify the protocol field to look for the pattern. If context is not specified for a pattern, the FortiProxy unit searches for the pattern anywhere in the packet buffer. The available context variables are:

- `uri`: Search for the pattern in the HTTP URI line.
- `header`: Search for the pattern in HTTP header lines or SMTP/POP3/SMTP control messages.
- `body`: Search for the pattern in HTTP body or SMTP/POP3/SMTP email body.
- `host`: Search for the pattern in HTTP HOST line.

no_case

Syntax: `--no_case;`

Description:

Use the no-case keyword to force the FortiProxy unit to perform a case-insensitive pattern match.

offset

Syntax: `--offset <offset_int>;`

Description:

Use the offset keyword to look for the contents after the specified number of bytes into the payload. The specified number of bytes is an absolute value in the payload. Follow the offset keyword with the depth keyword to stop looking for a match after a specified number of bytes. If no depth is specified, the FortiProxy unit continues looking for a match until the end of the payload.

The offset must be between 0 and 65535.

pattern

Syntax: `--pattern [!]"<pattern_str>";`

Description:

The FortiProxy unit will search for the specified pattern. A pattern keyword normally is followed by a context keyword to define where to look for the pattern in the packet. If a context keyword is not present, the FortiProxy unit looks for the pattern anywhere in the packet buffer. To have the FortiProxy search for a packet that does not contain the specified URI, add an exclamation mark (!) before the URI.

Example: `--pattern "/level/" --pattern "|E8 D9FF FFFF|/bin/sh" --pattern !"|20|RTSP/"`

pcre

Syntax: `--pcre [!]"/<regex>/[ismxAEGRUB]";`

Description:

Similarly to the pattern keyword, use the pcre keyword to specify a pattern using Perl-compatible regular expressions (PCRE). A pcre keyword can be followed by a context keyword to define where to look for the pattern in the packet. If no context keyword is present, the FortiProxy unit looks for the pattern anywhere in the packet buffer.

For more information about PCRE syntax, go to http://www.pcre.org.

The switches include:

- `i`: Case insensitive.
- `s`: Include newlines in the dot metacharacter.
- `m`: By default, the string is treated as one big line of characters. ^ and $ match at the beginning and ending of the string. When m is set, ^ and $ match immediately following or immediately before any newline in the buffer, as well as the very start and very end of the buffer.
- `x`: White space data characters in the pattern are ignored except when escaped or inside a character class.
- `A`: The pattern must match only at the start of the buffer (same as ^).
- `E`: Set $ to match only at the end of the subject string. Without E, $ also matches immediately before the final character if it is a newline (but not before any other newlines).
- `G`: Invert the “greediness” of the quantifiers so that they are not greedy by default, but become greedy if followed by ?.
- `R`: Match relative to the end of the last pattern match. (Similar to distance:0;).
- `U`: Deprecated, see the context on page 618 keyword. Match the decoded URI buffers.

uri

Syntax: `--uri [!]"<uri_str>";`

Description:

Deprecated. See pattern and context keywords. Use the uri keyword to search for the URI in the packet payload. The URI must be enclosed in double quotes ("). To have the FortiProxy unit search for a packet that does not contain the specified URI, add an exclamation mark (!) before the URI. Multiple content items can be specified in one rule. The value can contain mixed text and binary data. The binary data is generally enclosed within the pipe (|) character. The double quote ("), pipe sign (|) and colon (:) characters must be escaped using a back slash (\) if specified in a URI string.

within

Syntax: `--within <within_int>;`

Description:

Use this together with the distance keyword to search for the contents within the specified number of bytes of the payload.

The within value must be between 0 and 65535.

IP header keywords

dst_addr

Syntax: `--dst_addr [!]<ipv4>;`

Description:

Use the dst addr keyword to search for the destination IP address. To have the FortiProxy unit search for a packet that does not contain the specified address, add an exclamation mark (!) before the IP address. You can define up to 28 IP addresses or CIDR blocks. Enclose the comma separated list in square brackets.

Example: `dst_addr [172.20.0.0/16, 10.1.0.0/16,192.168.0.0/16]`

ip_dscp

Syntax: `--ip_dscp`

Description:

Use the ip_dscp keyword to check the IP DSCP field for the specified value.

ip_id

Syntax: `--ip_id <field_int>;`

Description:

Check the IP ID field for the specified value.

ip_option

Syntax: `--ip_option {rr | eol | nop | ts | sec | lsrr | ssrr | satid | any};`

Description:

Use the ip_option keyword to check various IP option settings.

The available options include:

- `rr`: Check if IP RR (record route) option is present.
- `eol`: Check if IP EOL (end of list) option is present.
- `nop`: Check if IP NOP (no op) option is present.
- `ts`: Check if IP TS (time stamp) option is present.
- `sec`: Check if IP SEC (IP security) option is present.
- `lsrr`: Check if IP LSRR (loose source routing) option is present.
- `ssrr`: Check if IP SSRR (strict source routing) option is present.
- `satid`: Check if IP SATID (stream identifier) option is present.
- `any`: Check if IP any option is present.

ip_tos

Syntax: `--ip_tos <field_int>;`

Description:

Check the IP TOS field for the specified value.

ip_ttl

Syntax: `--ip_ttl [< | >] <ttl_int>;`

Description:

Check the IP time-to-live value against the specified value. Optionally, you can check for an IP time-to-live greater-than (>) or less-than (<) the specified value with the appropriate symbol.

protocol

Syntax: `--protocol {<protocol_int> | tcp | udp | icmp};`

Description:

Check the IP protocol header.

Example: `--protocol tcp;`

src_addr

Syntax: `--src_addr [!]<ipv4>;`

Description:

Use the src_addr keyword to search for the source IP address. To have the FortiProxy unit search for a packet that does not contain the specified address, add an exclamation mark (!) before the IP address. You can define up to 28 IP addresses or CIDR blocks. Enclose the comma separated list in square brackets.

Example: `src_addr 192.168.13.0/24`

TCP header keywords

ack

Syntax: --ack <ack_int>;

Description:

Check for the specified TCP acknowledge number.

dst_port

Syntax: --dst_port [!]{<port_int> | :<port_int> | <port_int>: | <port_int>:<port_int>};

Description:

Use the dst_port keyword to specify the destination port number.

You can specify a single port or port range:

- <port_int> is a single port.
- :<port_int> includes the specified port and all lower numbered ports.
- <port_int>: includes the specified port and all higher numbered ports.
- <port_int>:<port_int> includes the two specified ports and all ports in between.

seq

Syntax: --seq [operator,]<number>[,relative];

Description:

Check for the specified TCP sequence number.

- operator includes =,<,>,!.
- relative indicates it is relative to the initial sequence number of the TCP session.

src_port

Syntax: --src_port [!]{<port_int> | :<port_int> | <port_int>: | <port_int>:<port_int>};

Description:

Use the src_port keyword to specify the source port number. You can specify a single port or port range:

- <port_int> is a single port.
- :<port_int> includes the specified port and all lower numbered ports.
- <port_int>: includes the specified port and all higher numbered ports.
- <port_int>:<port_int> includes the two specified ports and all ports in between.

tcp_flags

Syntax: --tcp_flags <SAFRUP120>[!|*|+] [,<SAFRUP120>];

Description:

Specify the TCP flags to match in a packet.

- S: Match the SYN flag.
- A: Match the ACK flag.
- F: Match the FIN flag.
- R: Match the RST flag.
- U: Match the URG flag.
- P: Match the PSH flag.
- 1: Match Reserved bit 1.
- 2: Match Reserved bit 2.
- 0: Match No TCP flags set.
- !: Match if the specified bits are not set.
- *: Match if any of the specified bits are set.
- +: Match on the specified bits, plus any others.

The first part if the value (<SAFRUP120>) defines the bits that must be present for a successful match.

Example:

--tcp_flags AP only matches the case where both A and P bits are set.

The second part ([,<SAFRUP120>]) is optional, and defines the additional bits that can be present for a match.

For example tcp_flags S,12 matches the following combinations of flags: S, S and 1, S and 2, S and 1 and 2. The modifiers !, * and + cannot be used in the second part.

window_size

Syntax: --window_size [!]<window_int>;

Description:

Check for the specified TCP window size. You can specify the window size as a hexadecimal or decimal integer. A hexadecimal value must be preceded by 0x. To have the FortiProxy search for the absence of the specified window size, add an exclamation mark (!) before the window size.

UDP header keywords

dst_port

Syntax: `--dst_port [!]{<port_int> | :<port_int> | <port_int>: | <port_int>:<port_int>};`

Description:

Specify the destination port number. You can specify a single port or port range:

- `<port_int>` is a single port.
- `:<port_int>` includes the specified port and all lower numbered ports.
- `<port_int>:` includes the specified port and all higher numbered ports.
- `<port_int>:<port_int>` includes the two specified ports and all ports in between.

src_port

Syntax: `--src_port [!]{<port_int> | :<port_int> | <port_int>: | <port_int>:<port_int>};`

Description:

Specify the destination port number. You can specify a single port or port range:

- `<port_int>` is a single port.
- `:<port_int>` includes the specified port and all lower numbered ports.
- `<port_int>:` includes the specified port and all higher numbered ports.
- `<port_int>:<port_int>` includes the two specified ports and all ports in between.

ICMP keywords

icmp_code

Syntax: --icmp_code <code_int>;

Description:

Specify the ICMP code to match.

icmp_id

Syntax: --icmp_id <id_int>;

Description:

Check for the specified ICMP ID value.

icmp_seq

Syntax: --icmp_seq <seq_int>;

Description:

Check for the specified ICMP sequence value.

icmp_type

Syntax: --icmp_type <type_int>;

Description:

Specify the ICMP type to match.

Other keywords

data_size

Syntax: --data_size {<size_int> | <<size_int> | ><size_int>;

Description:

Test the packet payload size. With data_size specified, packet reassembly is turned off automatically. So a signature with data_size and only_stream values set is wrong.

- <size_int> is a particular packet size.
- <<size_int> is a packet smaller than the specified size.
- ><size_int> is a packet larger than the specified size.

Examples:

- --data_size 300;
- --data_size <300;
- --data_size >300;

data_at

Syntax: `--data_at <offset_int>[, relative];`

Description:

Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.

dump-all-html

Syntax: `--dump-all-html`

Description:

Dump all HTML files for benchmarking via iSniff. When there is no file type specified, all HTML files are dumped.

rate

Syntax: `--rate <matches_int>,<time_int>;`

Description:

Instead of generating log entries every time the signature is detected, use this keyword to generate a log entry only if the signature is detected a specified number of times within a specified time period.

- `<matches_int>` is the number of times a signature must be detected.
- `<time_int>` is the length of time in which the signature must be detected, in seconds.

For example, if a custom signature detects a pattern, a log entry will be created every time the signature is detected. If `--rate 100,10;` is added to the signature, a log entry will be created if the signature is detected 100 times in the previous 10 seconds. Use this command with `--track` to further limit log entries to when the specified number of detections occur within a certain time period involving the same source or destination address rather than all addresses.

rpc_num

Syntax: `--rpc_num <app_int>[, <ver_int> | *][, <proc_int> | *>];`

Description:

Check for RPC application, version, and procedure numbers in SUNRPC CALL requests. The * wild card can be used for version and procedure numbers.

same_ip

Syntax: `--same_ip;`

Description:

Check that the source and the destination have the same IP addresses.

track

Syntax: `--track {SRC_IP |DST_IP |DHCP_CLIENT |DNS_DOMAIN}[,block_int];`

Description:

When used with `--rate`, this keyword narrows the custom signature rate totals to individual addresses.

- `SRC_IP`: tracks the packet's source IP.
- `DST_IP`: tracks the packet's destination IP.
- `DHCP_CLIENT`: tracks the DHCP client's MAC address.
- `DNS_DOMAIN`: counts the number of any specific domain name.
- `block_int` has the FortiProxy unit block connections for the specified number of seconds, from the client or to the server, depending on which is specified.

For example, if `--rate 100,10` is added to the signature, a log entry will be created if the signature is detected 100 times in the previous 10 seconds. The FortiProxy unit maintains a single total, regardless of source and destination address.

If the same custom signature also includes `--track` client; matches are totaled separately for each source address. A log entry is added when the signature is detected 100 times in 10 seconds within traffic from the same source address.

The `--track` keyword can also be used without `--rate`. If an integer is specified, the client or server will be blocked for the specified number of seconds every time the signature is detected.

www.fortinet.com