FortiProxy Administration Guide

VERSION 1.1.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FORTINET PRIVACY POLICY

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdocs@fortinet.com

July 30, 2019

FortiProxy 1.1.0 Administration Guide

45-110-492050-20190730

TABLE OF CONTENTS

Change log

Date	Change Description
December 14, 2018	Initial document release for FortiProxy 1.1.0
January 3, 2019	Added the “Link health monitor” section.
July 8, 2019	Updated the “WAN optimization profiles” section.
July 30, 2019	Added the “Automatic backup to an FTP or TFTP server” appendix.

Introduction

The FortiProxy unit provides a secure web gateway, which protects against web attacks with URL filtering, visibility and control of encrypted web traffic through SSL and SSH inspection, and 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 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.

About this document

This document contains the following sections:

Concepts

This chapter describes the following:

Transparent and NAT/Route modes

A FortiProxy unit can operate in one of two modes: Transparent or NAT/Route mode.

In transparent mode, the FortiProxy unit is installed between the internal network and the router. In this mode, the FortiProxy unit does not make any changes to IP addresses and only applies security scanning to traffic. When a FortiProxy unit is added to a network in transparent mode, no network changes are required, except to provide the FortiProxy unit with a management IP address. The transparent mode is used primarily when there is a need to increase network protection but changing the configuration of the network itself is impractical.

In NAT/Route mode, a FortiProxy unit is installed as a gateway or router between two networks. In most cases, it is used between a private network and the Internet. This allows the FortiProxy unit to hide the IP addresses of the private network using network address translation (NAT).

Web proxy

Web proxy covers both transparent proxy and explicit proxy.

This section covers the following topics:

Web proxy concepts

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

- 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.

NOTE: These configurations apply to only the Security Profiles proxy-based processes and not the flow-based processes.

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
- RTMP/RPMPT

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" on page 13.

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.

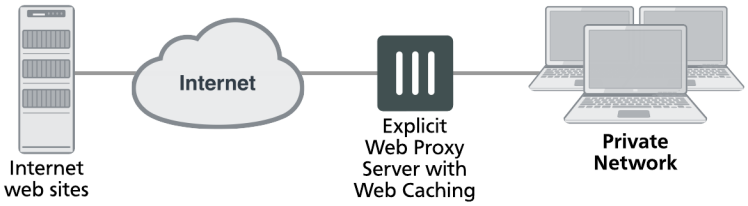
Explicit web proxy topologies

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.

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 13.

WAN optimization topologies

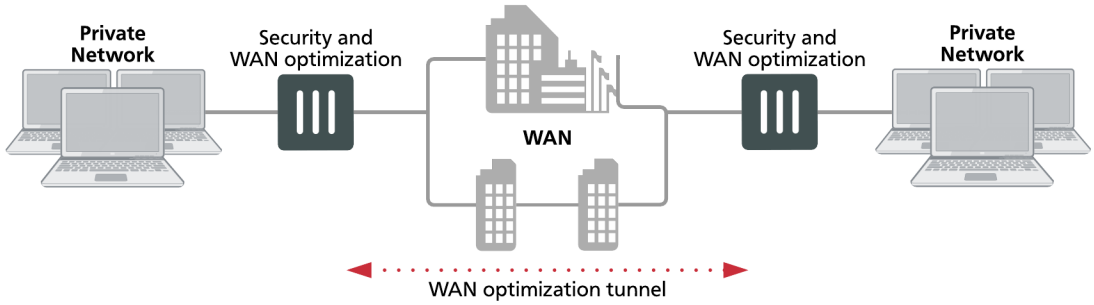
The WAN optimization topologies are described in the following sections:

- 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.

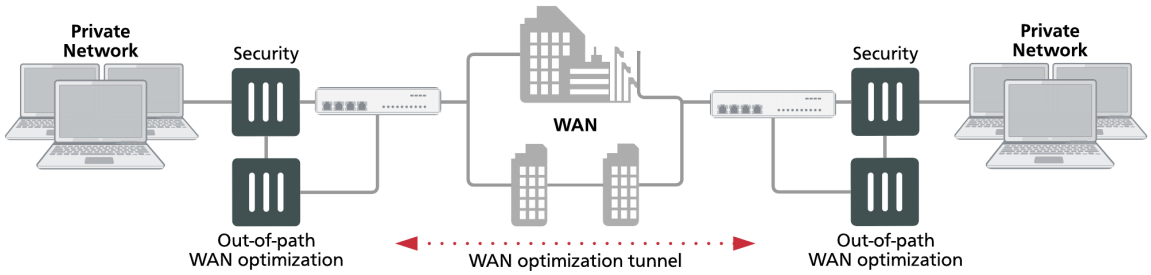
The WAN optimization configuration is the same for FortiProxy units deployed as security devices and for single-purpose WAN optimization FortiProxy units. The only differences would result from the different network topologies.

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.

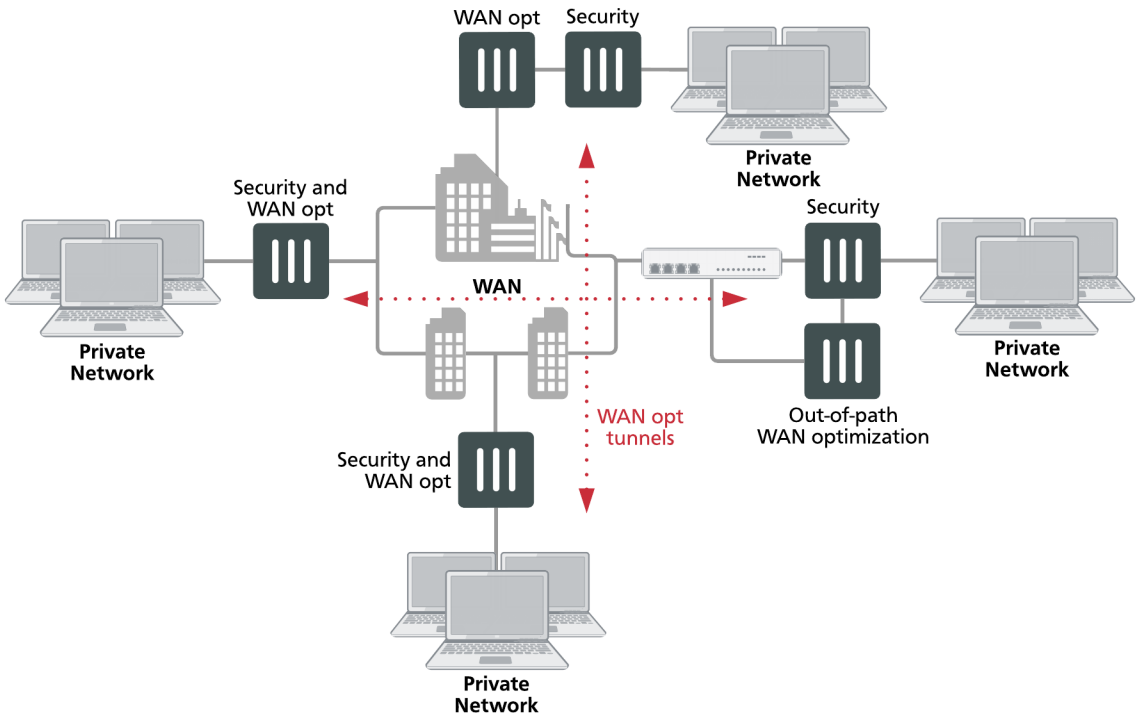
The out-of-path FortiProxy units can operate in NAT/Route or transparent mode.

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

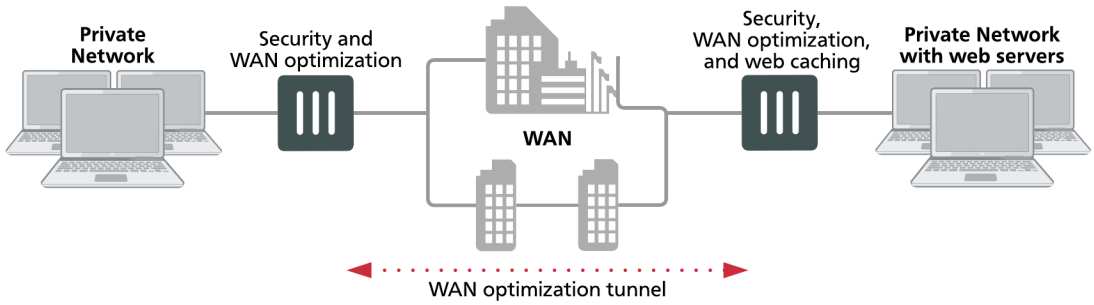


You can also configure WAN optimization between FortiProxy units with different roles on the WAN. FortiProxy units configured as security devices and for WAN optimization can perform WAN optimization as if they are single-purpose FortiProxy units just configured for WAN optimization.

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 "WAN optimization" on page 19 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:

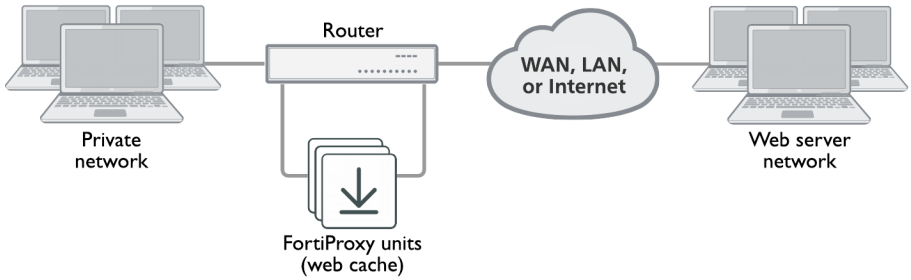
```
config wanopt cache-service
   set collaboration enable
   set acceptable-peers src-peer
   set device-id "peer-id"
   config src-peer
      edit "fch-1"
         set ip xxx.xxx.xxx.xxx
      next
   end
```

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.

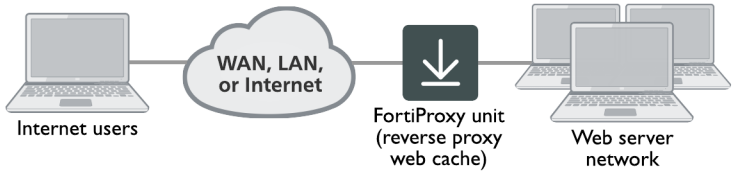
Most commonly the topology uses a router to route HTTP and HTTPS traffic to be cached to one or more FortiProxy units. Traffic that should not be cached bypasses the FortiProxy units. This is a scalable topology that allows you to add more FortiProxy units if usage increases.

Web-caching topology with web traffic routed to FortiProxy units



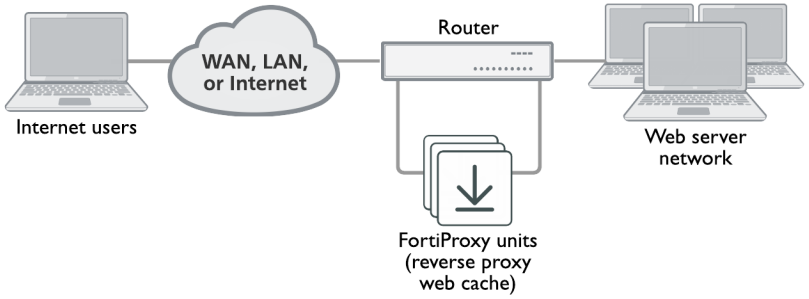
You can also configure reverse proxy web caching. In this configuration, users on the Internet browse to a web server installed behind a FortiProxy unit. The FortiProxy unit intercepts the web traffic (HTTP and HTTPS) and caches pages from the web server. Reverse proxy web caching on the FortiProxy unit 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.

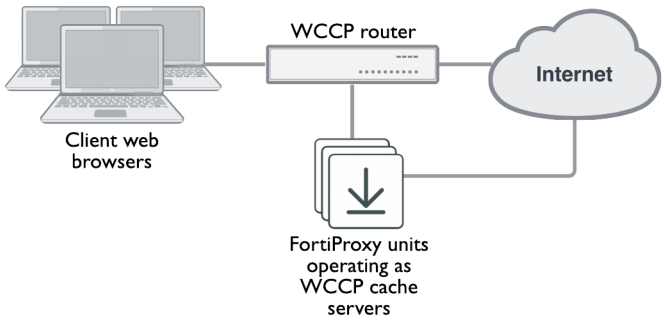
WCCP

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.

Content Analysis Service

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.

Please contact your Fortinet Account Manager should you require a trial of this service. You can purchase this service from https://support.fortinet.com/.

For configuration information, see "Content Analysis" on page 222.

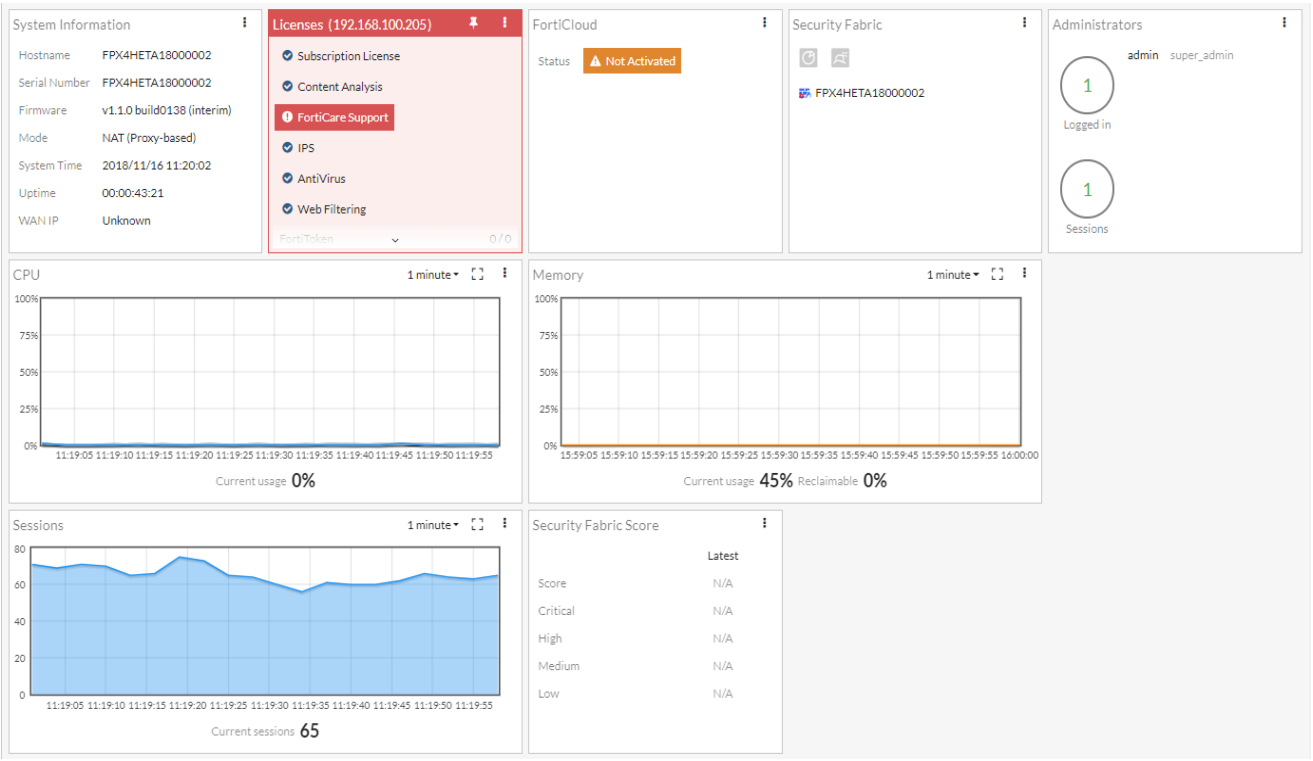
Dashboard

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* > *Main*.

Your browser must support JavaScript to view the dashboard.



The following widgets are displayed:

- System Information
- Licenses
- FortiCloud
- Security Fabric
- Administrators
- CPU
- Memory

- Sessions
- Security Fabric Score

You can add the following FortiView widgets to the dashboard:

- Sources
- Destinations
- Applications
- Cloud Applications
- Web Sites
- Threats
- System Events
- Policies
- Interfaces

This section describes the following:

Managing widgets

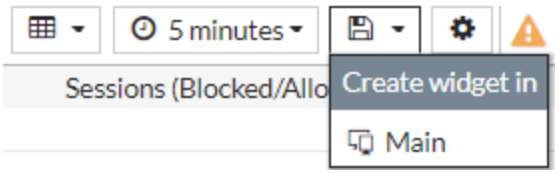
To rearrange widgets on the dashboard, drag the widgets by their title bars.

All widgets have the following two title bar options:

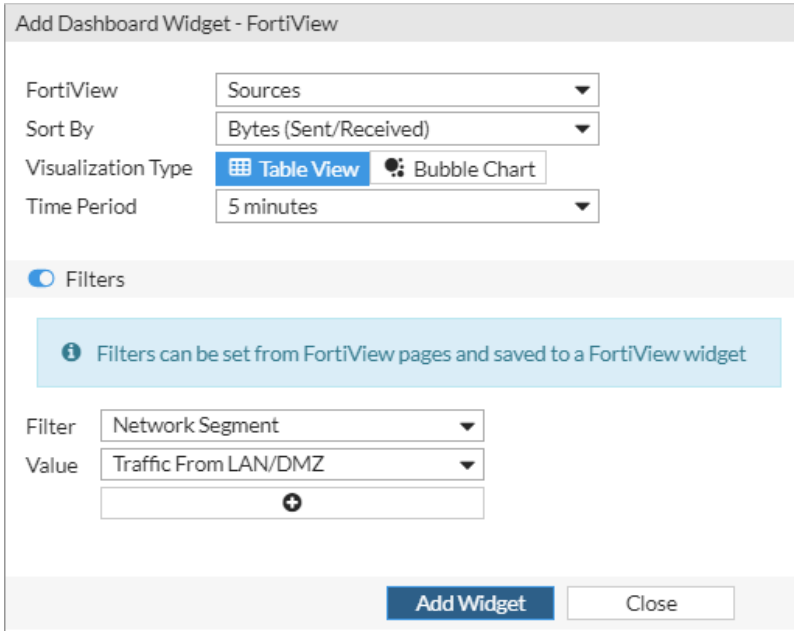
Resize	Select the size of the widget.
Remove	Remove the widget from the dashboard.

To add a FortiView widget to a dashboard:

1. Go to *FortiView* menu and select *Sources*, *Destinations*, *Applications*, *Cloud Applications, Web Sites*, *Threats*, *System Events*, *Policies*, or *Interfaces*.
2. From the toolbar, select *Create widget in* > *Main*.

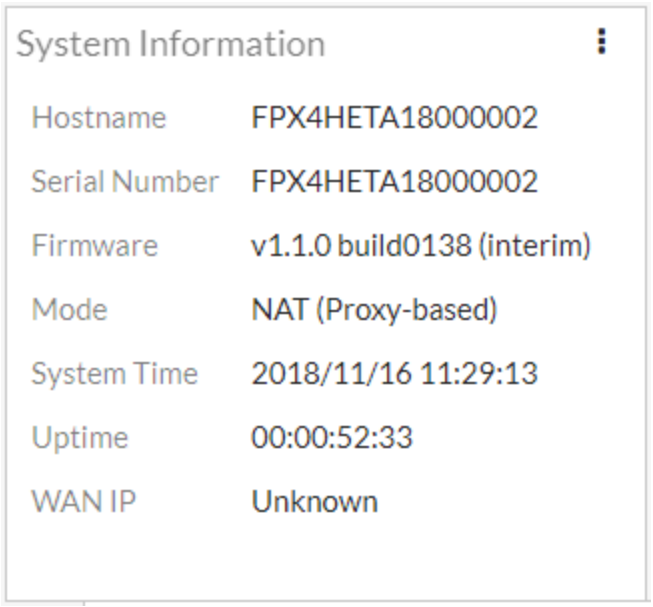


The *Add Dashboard Widget - FortiView* window opens.



3. Select which FortiView widget you want to add.
4. Select the field to sort by.
5. If there is more than one visualization type, select *Table View* or *Bubble Chart*.
6. Select the time period to display.
7. If you want the data filtered, enable *Filters*, select the filter and value. You can select multiple filter-and-value pairs.
8. Select *Add Widget*.
   The settings page opens.
9. Make any changes needed.
10. Select *Close*.
    The new widget is displayed in the main dashboard.

System Information widget



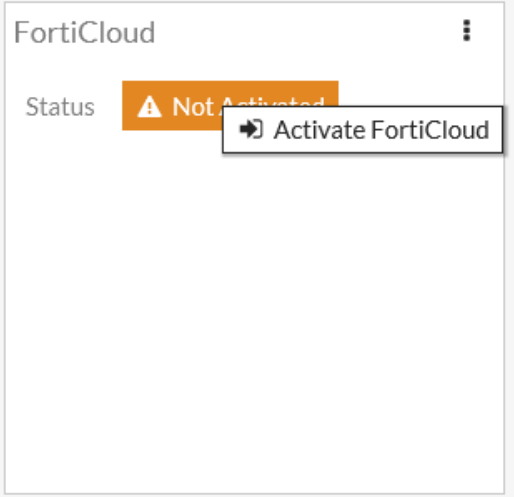
The *System Information* widget displays general system information, such as the FortiProxy unit serial number, firmware version, host name, and system time. Clicking on the widget provides you links to two other pages:

- 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 *admin* > *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 (Proxy-based) mode or transparent mode.

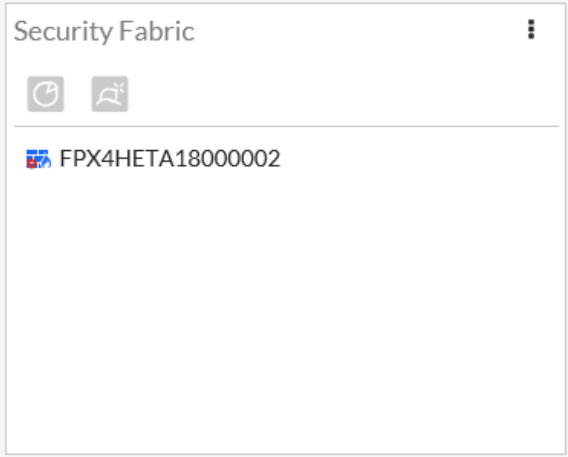
System Time	The current date and time according to the FortiProxy unit's internal clock.
Uptime	The time in days, hours, and minutes since the FortiProxy unit was started.
WAN IP	The WAN IP address and location. Additionally, if the WAN IP is blacklisted in the FortiGuard server, there is a notification in the notification area, located in the upper right-hand corner of the Dashboard. Clicking on the notification opens the WAN IP Blacklisted slider with the relevant blacklist information.

FortiCloud widget



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

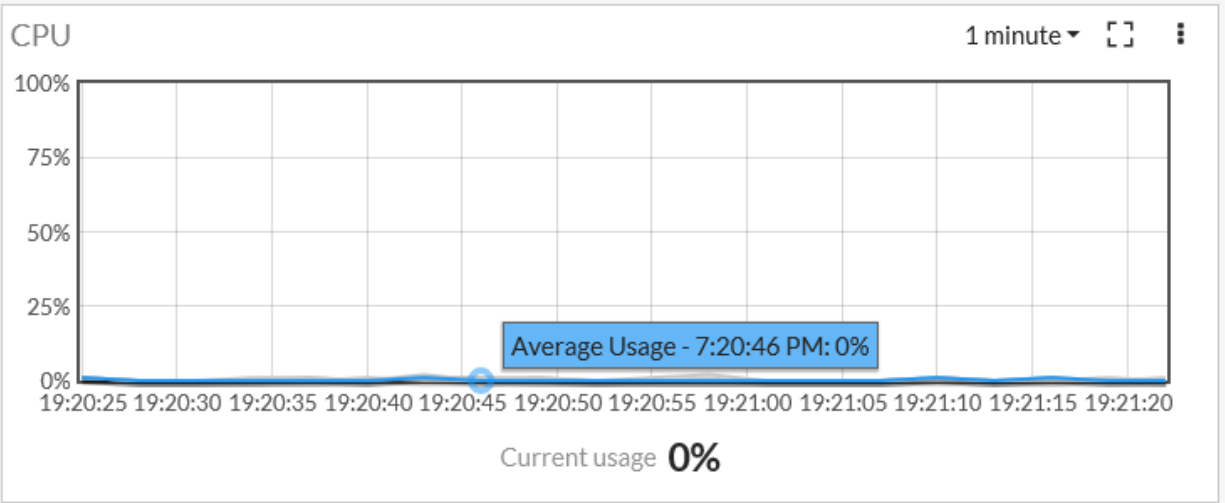
Security Fabric widget



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.

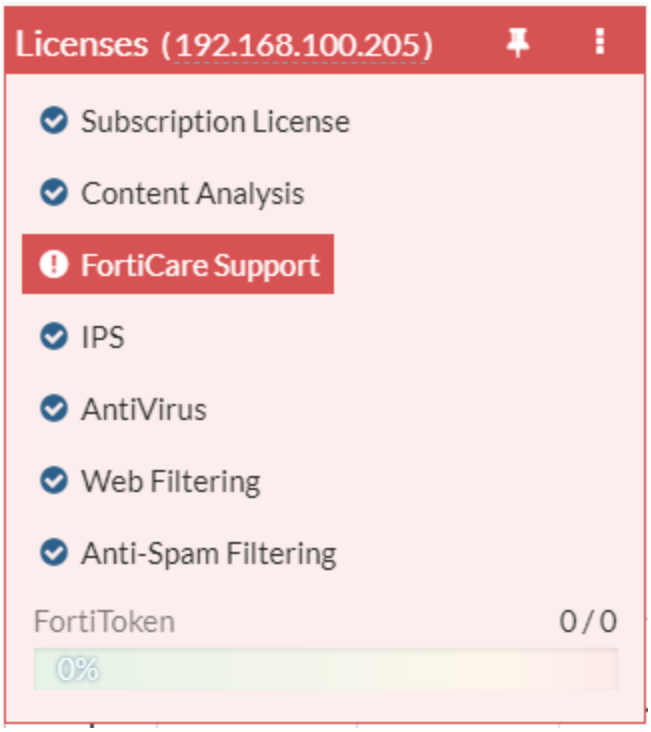
Click on an icon for a link to configure the settings for that component.

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. Click on the graph for a link to see the per-core CPU usage for different time frames. Hovering over any point on the graph displays the average CPU usage along with a time stamp. Click the dashed-line box icon to maximize the widget size.

Licenses widget

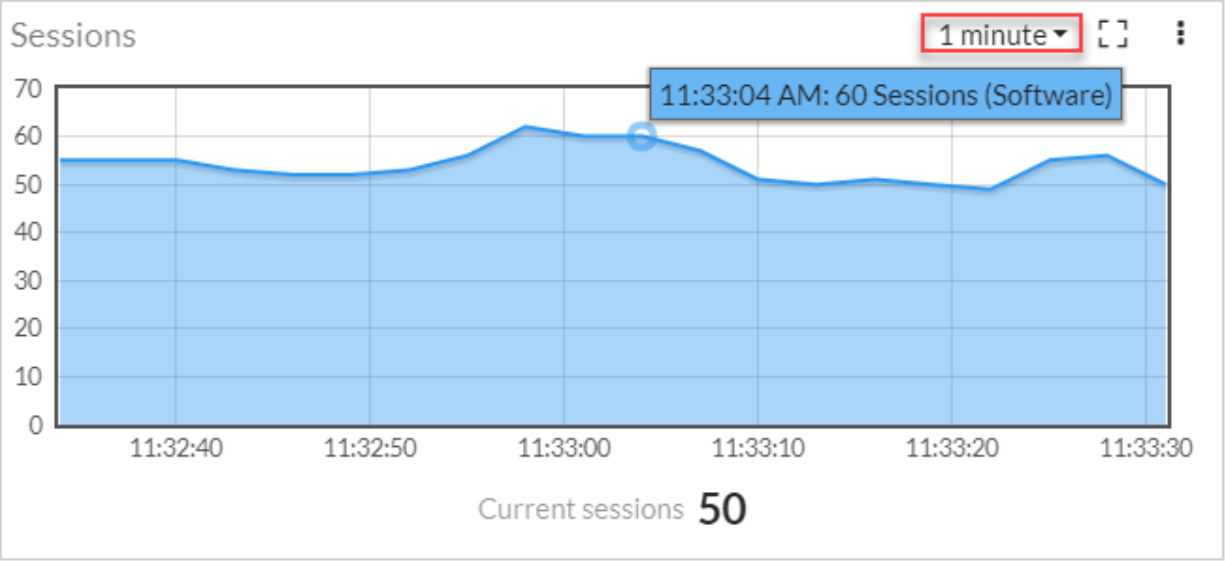


The *Licenses* widget displays the statuses of your licenses and FortiGuard subscriptions. It also allows you to update your device's registration status and FortiGuard definitions.

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

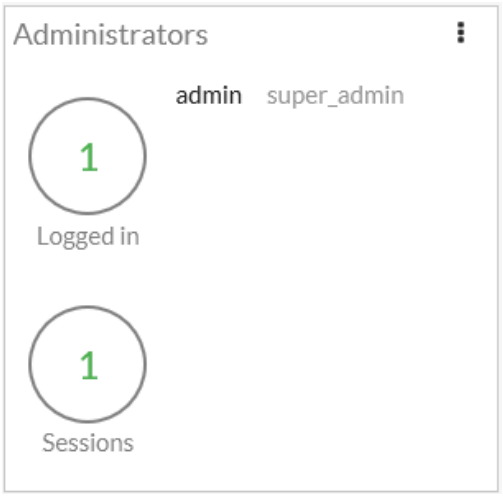
Go to *System* > *FortiGuard* to register for FortiCare Support, upgrade databases, and view details. See "FortiGuard" on page 104.

Sessions widget



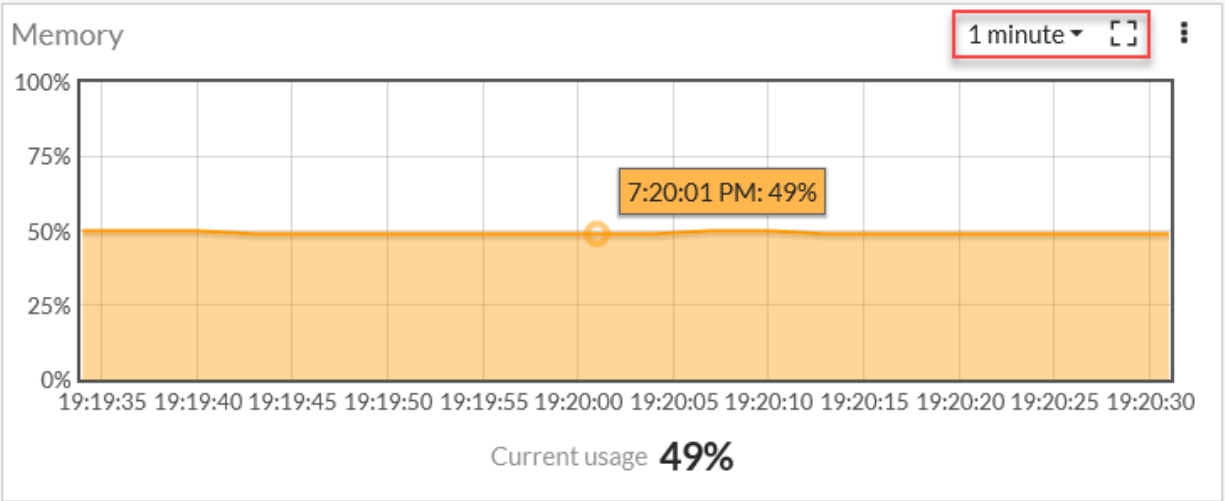
The number of active sessions is displayed for different time frames. Select the time frame from the drop-down list at the top of the widget. Hovering over any point on the graph displays how many sessions are active at that time. Click the dashed-line box icon to maximize the widget size.

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.

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. Click the dashed-line box icon to maximize the widget size.

Security Fabric Score widget

The Security Fabric Score is based on how many checks your network passes and fails, as well as the severity level of these checks. The score will be positive or negative, and a higher score represents a more secure network.

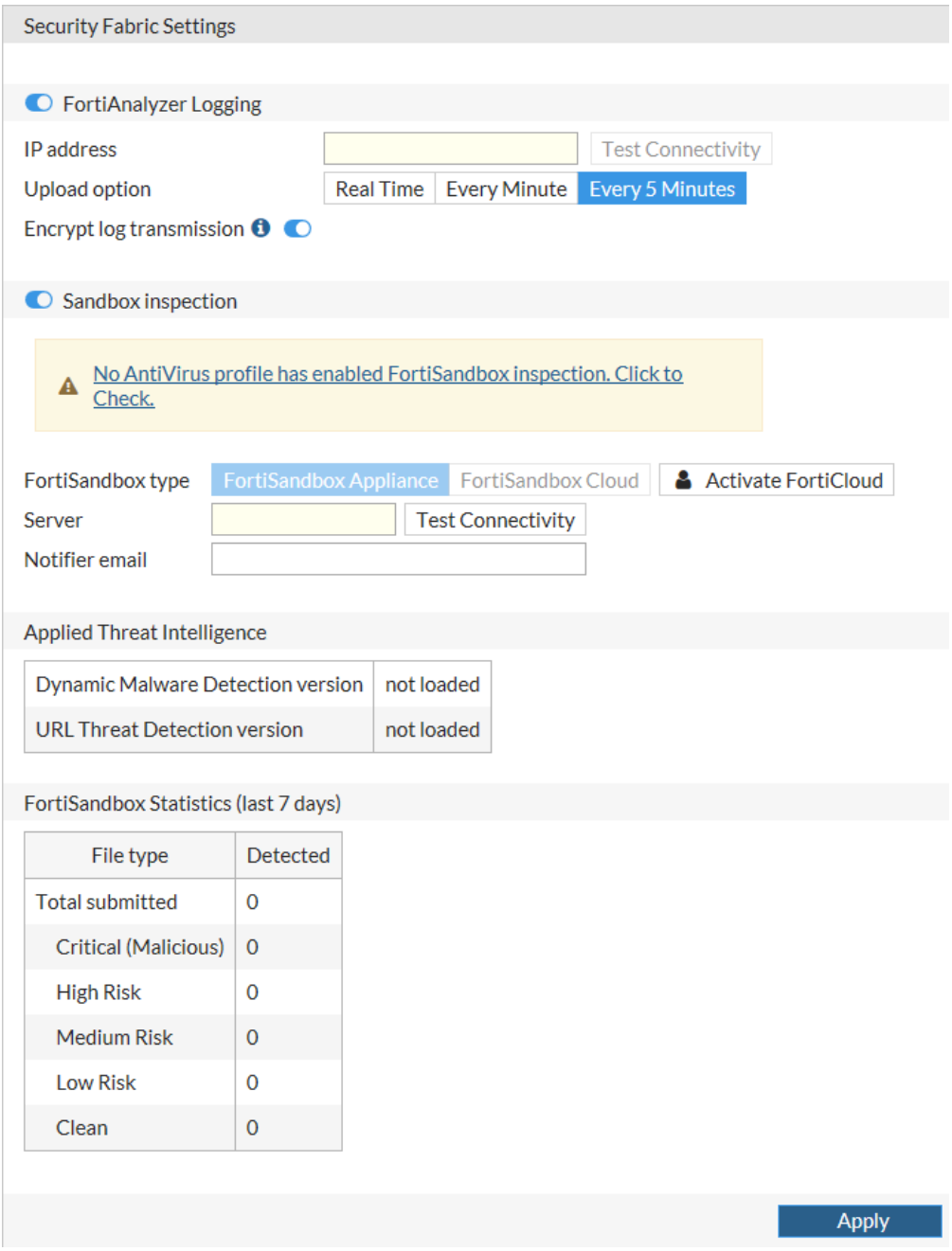
Security Fabric

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.

To configure the Security Fabric, go to *Security Fabric* > *Settings*.



The following options are available:

FortiAnalyzer Logging	Enable to allow the Security Fabric to show logs for the entire Security Fabric.

IP address	Enter the IP address of the FortiAnalyzer unit that you want the Security Fabric to send logs to. Select *Test Connectivity* to test if the FortiAnalyzer can be contacted. If the FortiAnalyzer functionality has not been enabled on the FortiManager, you will receive an error.
Upload option	Select how often you want the FortiProxy unit to send logs to the FortiAnalyzer unit: *Real Time*, *Every Minute*, or *Every 5 Minutes*. The default is *Every 5 Minutes*.
Encrypt log transmission	Enable if you want log transmissions encrypted. The log transmissions are encrypted using SSL.
Sandbox Inspection	Enable to have the FortiProxy unit send suspicious files to FortiSandbox for inspection and analysis. When a FortiProxy unit sends files for sandbox inspection, the FortiSandbox uses virtual machines (VMs) running different operating systems to test the file and to determine if it is malicious. FortiSandbox can process multiple files simultaneously since the FortiSandbox has a VM pool. The time to process a file depends on hardware and the number of sandbox VMs used to scan the file. It can take 60 seconds to five minutes to process a file. To use sandbox inspection, you need an antivirus profile with FortiSandbox inspection enabled.
FortiSandbox type	Select *FortiSandbox Appliance* or *FortiSandbox Cloud*. FortiSandbox is available as a physical or virtual appliance (FortiSandbox Appliance) or as a cloud advanced threat protection service (FortiSandbox Cloud). If you want to use FortiSandbox Cloud, you need an active FortiCloud account. If you do not have an active FortiCloud account, select *Activate FortiCloud*.
Server	Enter the IP address of the FortiSandbox server. Select *Test Connectivity* to test if the server can be contacted.
Notifier email	Enter an email address for FortiSandbox notifications.
Applied Threat Intelligence	Reports if Dynamic Malware Detection and URL Threat Detection are loaded and, if loaded, which version.

FortiSandbox Statistics (last 7 days)	The last 7 days of FortiSandbox statistics. When a FortiProxy unit uses sandbox inspection, files are sent to the FortiSandbox. Then the FortiSandbox uses virtual machines (VMs) running different operating systems to test the file, to determine if it is malicious. If the file exhibits risky behavior or is found to contain a virus, a new signature can be added to both the local FortiProxy malware database and the FortiGuard AntiVirus signature database.
Apply	Select to save your changes.

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 chapter covers the following topics:

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
Sources	• Disk logging enabled • Historical FortiView enabled • Traffic logging enabled in a policy
Destinations	• Disk logging enabled • Historical FortiView enabled • Traffic logging enabled in a policy
Applications	• Disk logging enabled • Historical FortiView enabled • Traffic logging enabled in a policy • Application Control profile added to a policy

FortiView Console	Dependencies
Cloud Applications	• Disk logging enabled • Historical FortiView enabled • Full SSL inspection enabled for all protocols in a SSL/SSH Inspection profile • Application Control profile and Full SSL Inspection profile added to the same policy
Web Sites	• Disk logging enabled • Historical FortiView enabled • FortiGuard categories enabled in a Web Filter profile • Traffic logging enabled in a policy • Web Filter profile added to a policy
Threats	• Disk logging enabled • Historical FortiView enabled • Threat weight detection enabled • Traffic logging enabled in a policy
System Events	• Disk logging enabled • Historical FortiView enabled • *Event Logging* and *System activity event* enabled in *Log Settings*
Policies	• Disk logging enabled • Historical FortiView enabled • Traffic logging enabled in a policy
Interfaces	• Disk logging enabled • Historical FortiView enabled • Traffic logging enabled in a policy
All Sessions	• Disk logging enabled • Traffic logging enabled in a policy

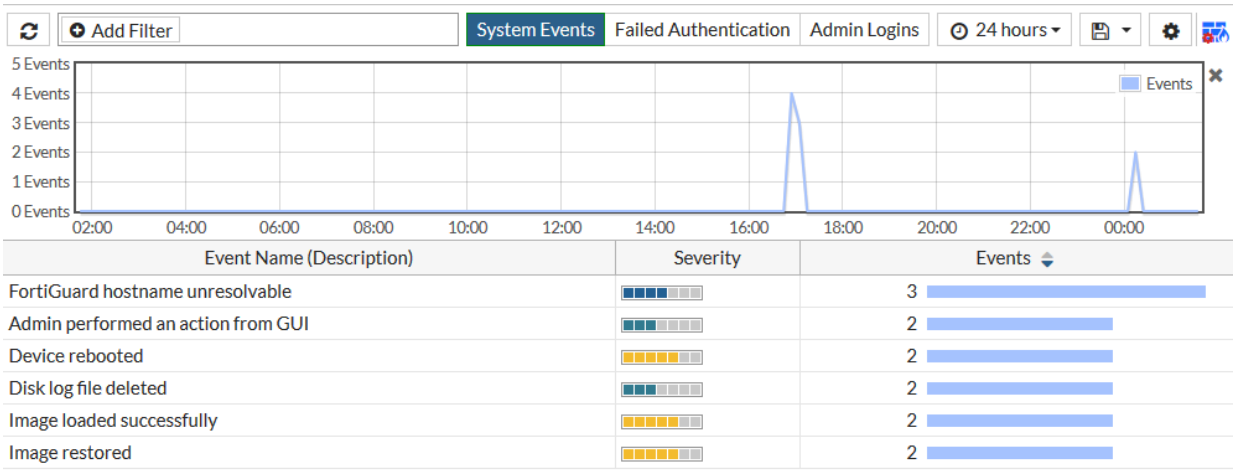
To enable disk logging and historical FortiView:

1. Go to *Log* > *Log Settings*.
2. Under *Local Log*, enable *Disk* and *Enable Historical FortiView*.
3. Select *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*, *24 hours*, or *more*)
- Dashboard widget drop-down menu
- *Settings* button
- Information icon

FortiView consoles

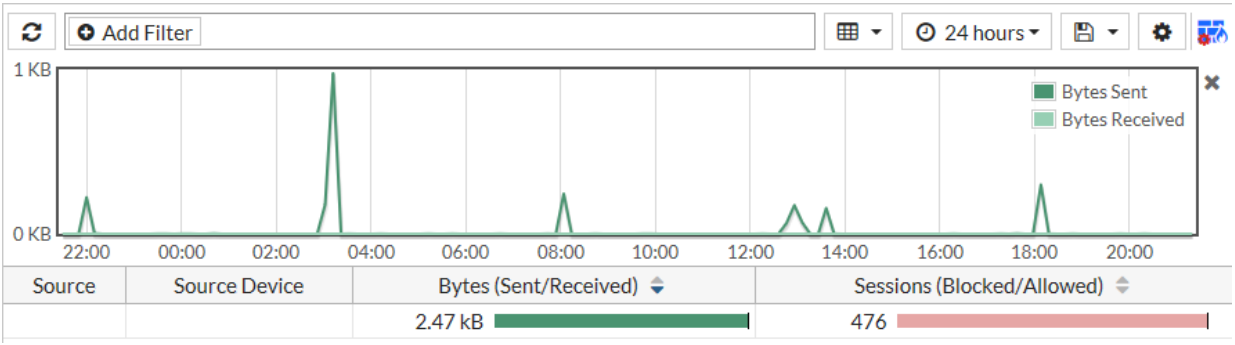
This section briefly describes the consoles available in FortiView:

- "Sources console" on page 43 displays detailed information on the sources of traffic passing through the FortiProxy unit, and the section covers how you can investigate an unusual spike in traffic to determine which user is responsible.
- "Destinations console" on page 43 displays detailed information on user destination-accessing through the use of drill-down functionality.
- "Applications console" on page 44 displays Applications used on the network that have been recognized by Application Control, and this section shows how you can view what sort of applications individual employees are using.
- "Cloud Applications console" on page 44 displays Web/Cloud Applications used on the network, and this section shows how you can drill down to access detailed data on cloud application usage, for example, YouTube.
- "Web Sites console" on page 45 displays web sites visited as part of network traffic that have been recognized by Web Filtering, and this section shows how you can investigate instances of proxy avoidance, which is the act of circumventing blocks using proxies.
- "Threats console" on page 45 monitors threats to the network, both in terms of their Threat Score and Threat Level.

- "System Events console" on page 46 displays security events detected by FortiProxy, providing a name and description for the events, an assessment of the event's severity level, and the number of instances the events were detected.
- "Threat Map console" on page 46 provides a geographical display of threats, in real time, from international sources as they arrive at your FortiProxy unit.
- "Policies console" on page 46 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.
- "Interfaces console" on page 47 displays the number of interfaces connected to your network, how many sessions there are in each interface, and what sort of traffic is occurring.
- "All Sessions console" on page 47 displays complete information on all FortiProxy sessions, with the ability to filter sessions by port number and application type.
- "User console" on page 48 displays information about all users and user groups who have logged in.
- "Quarantine console" on page 48 lists IP addresses and interfaces blocked by NAC quarantine.
- "WAN Opt. Peer console" on page 49 displays information about the WAN optimization peers.
- "WAN Optimization console" on page 49 displays a LAN and WAN traffic summary, as well as how many bytes are saved with WAN optimization.
- "Caching and Optimization console" on page 49 displays information about the web caching and request optimization.

Sources console

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

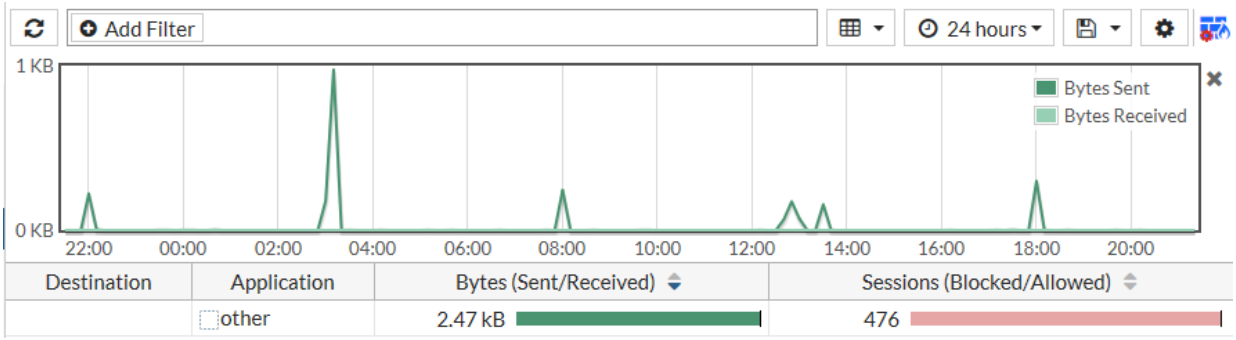


This console can be filtered by Country, Destination Device, Destination Interface, Device Type, Policy, Policy Type, Security Action, Source, Source Device, and Source Interface.

Specific devices and time periods can be selected and drilled down for deep inspection.

Destinations console

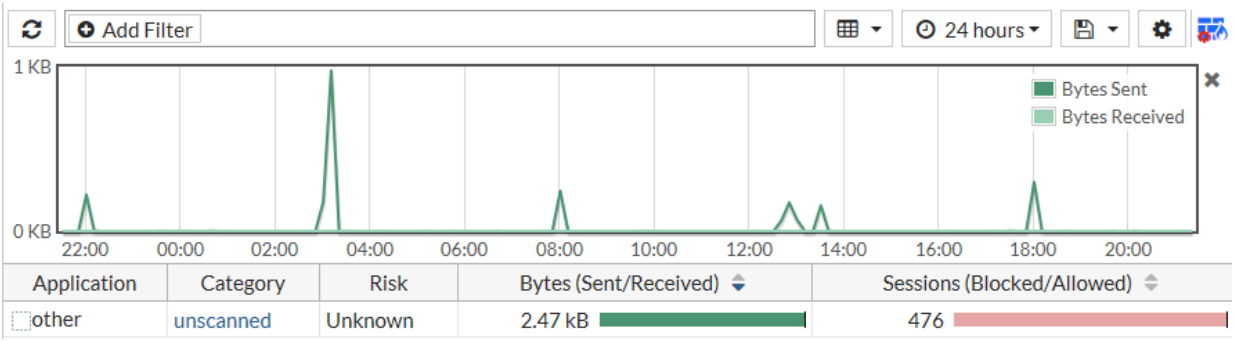
The *Destinations* console provides information about the destination IP addresses of traffic on your FortiProxy unit, as well as the application used. You can drill down the displayed information, and also select the device and time period, and apply search filters.



This console can be filtered by Country, Destination Device, Destination Interface, Destination IP, Policy, Policy Type, Security Action, Source Device, and Source Interface.

Applications console

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



This console can be filtered by Application, Country, Destination Interface, Policy, Policy Type, Security Action, and Source Interface.

Specific devices and time periods can be selected and drilled down for deep inspection.

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

Cloud Applications console

The 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 was able to view the login event.

This console can be filtered by Cloud User.

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.

Web Sites console

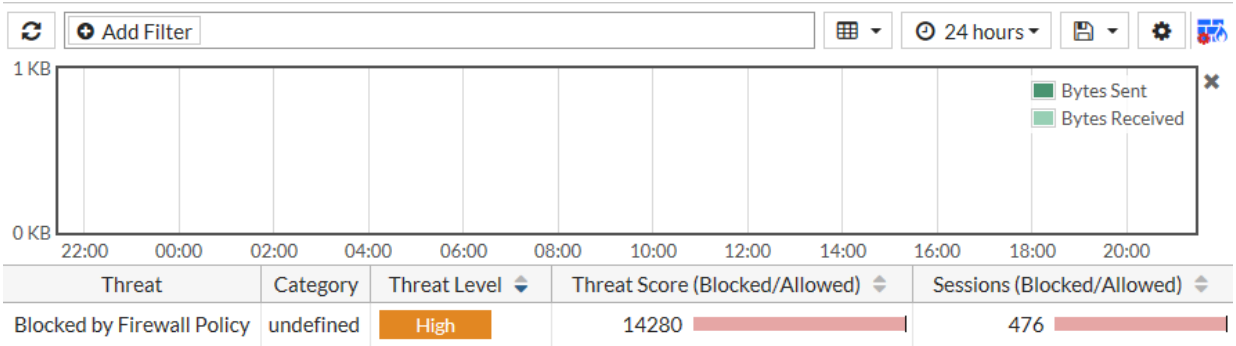
The *Web Sites* console lists the top allowed and top blocked web sites. You can view information by domain or by FortiGuard categories by using the options in the top right corner. Each FortiGuard category can be selected to see a description of the category and several example sites, with content loaded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

This console can be filtered by Destination Interface, Domain, Policy, Policy Type, Security Action, and Source Interface.

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

Threats console

The *Threats* console lists the top users involved in incidents, as well as information on the top threats to your network.



The following incidents are considered threats:

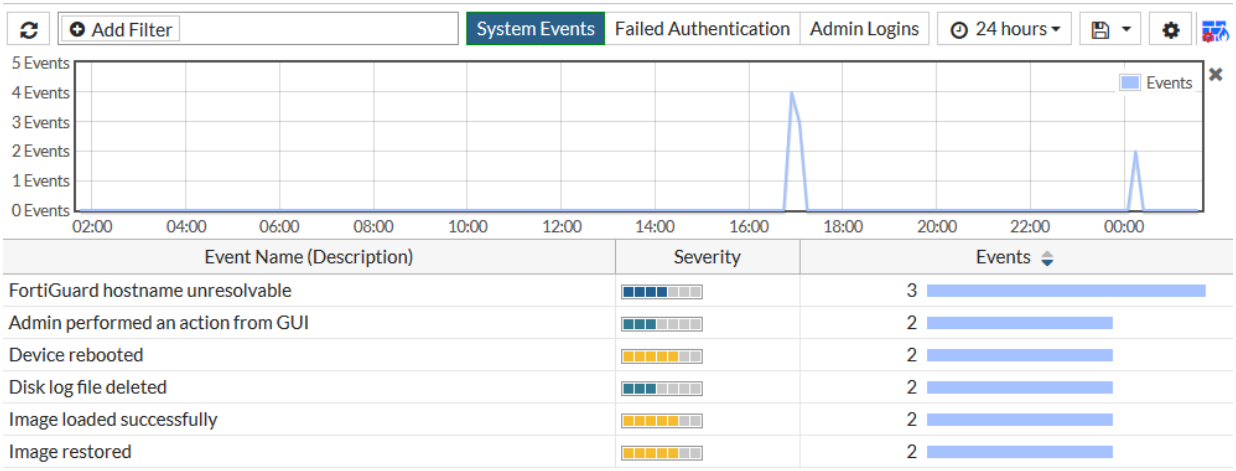
- Risk applications detected by application control
- Intrusion incidents detected by IPS
- Malicious web sites detected by web filtering
- Malware/botnets detected by antivirus

This console can be filtered by Country, Destination Interface, Policy, Result, Security Action, Source Interface, Threat, and Threat Type.

For information to appear in the *Threats* console, Threat Weight Tracking must be enabled.

System Events console

The *System Events* console lists security events detected by the FortiProxy unit, providing a name and description for the events, an assessment of the event's severity level (*Alert*, *Critical*, *Emergency*, *Error*, or *Warning*), and the number of instances the events were detected.



This console can be filtered by Event Name and Severity.

Threat Map console

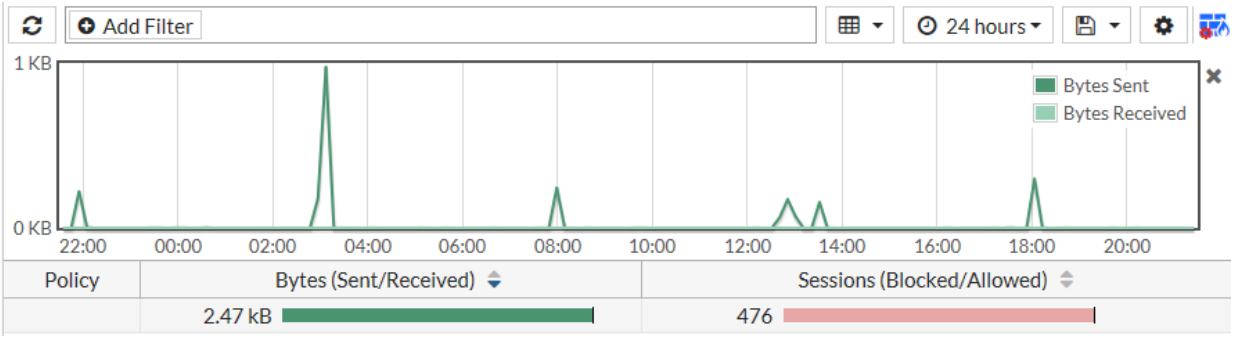
The *Threat Map* console displays network activity by geographic region. Threats from various international destinations will be shown, but only those arriving at your destination, as depicted by the FortiProxy. You can place your cursor over the FortiProxy's location to display the device name, IP address,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

A visual lists of threats is shown at the bottom, displaying the location, severity, and nature of the attacks. The color gradient of the darts on the map indicate the traffic risk, where red indicates the more critical risk.

Unlike other FortiView consoles, this console has no filtering options; however, you can click on any country to drill down into greater (filtered) detail.

Policies console

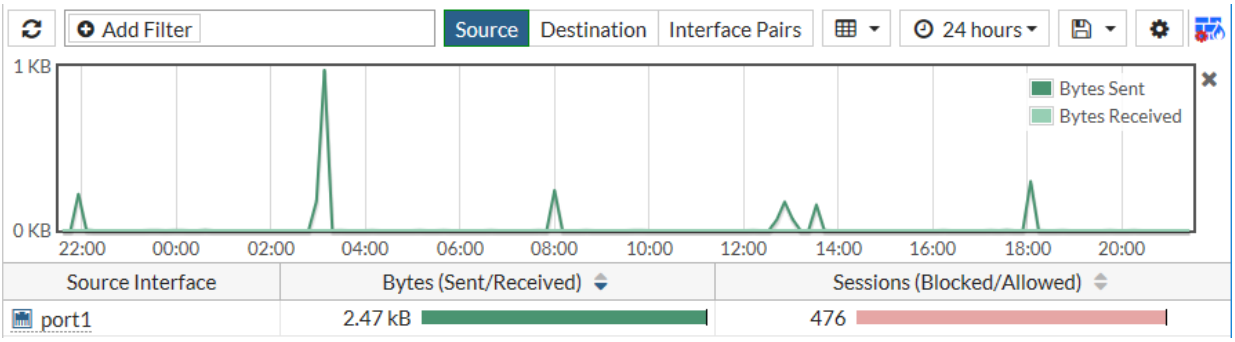
The *Policies* console shows what policies are in affect on your network, what their source and destination interfaces are, how many sessions are in each policy, and what sort of traffic is occurring, represented in bytes sent and received.



This console can be filtered by Country, Destination Device, Destination Interface, Destination IP, Policy, Policy Type, Source, Source Device, and Source Interface.

Interfaces console

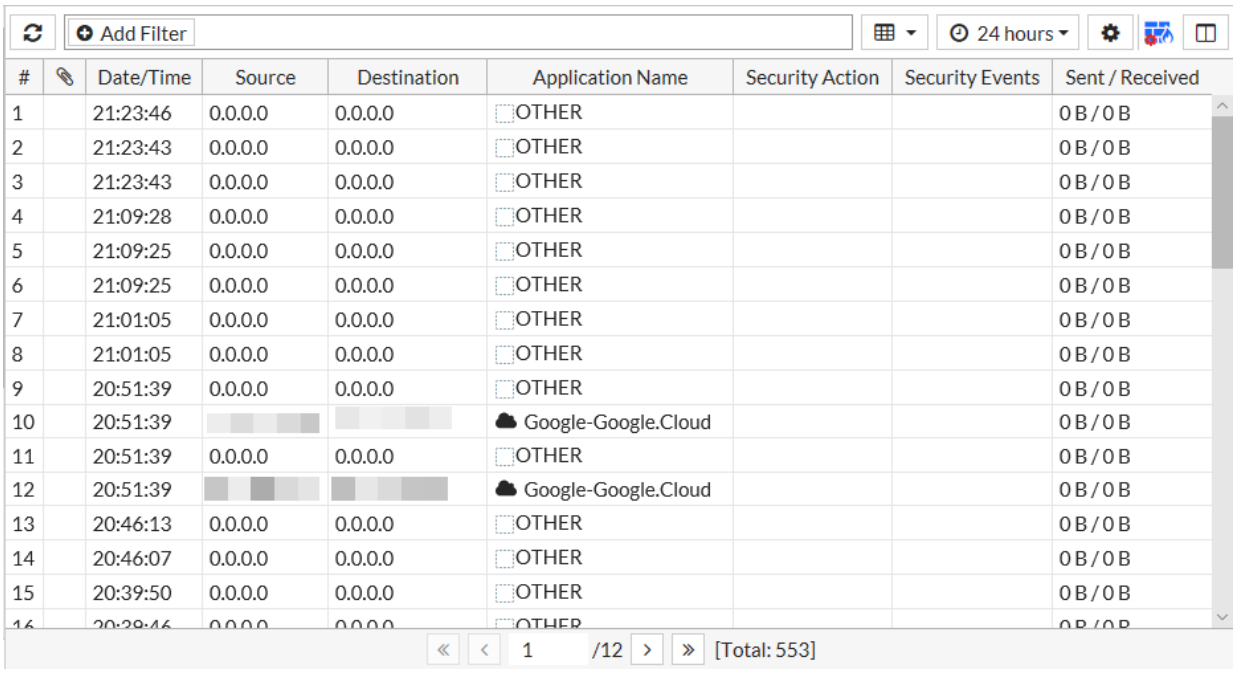
The Interfaces console lists the total number of interfaces connected to your network, how many sessions there are in each interface, and what sort of traffic is occurring, represented in both bytes sent and received, and the total bandwidth used.



This console can be filtered by Country, Destination Interface, Destination IP, Policy, Policy Type, Source, and Source Interface.

All Sessions console

The *All Sessions* console provides information about all FortiProxy traffic. This console can be filtered by AP, Application, Country, Destination Device, Destination Interface, Destination IP, Destination Port, Device Type, FortiProxy, Policy, Policy Type, Security Action, Source, Source Device, Source Interface, Source Port, Source SSID, and Threat.



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.

A number of 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.

User console

The *User* console allows you to check which users and users groups are logged in, how long they were logged in for, which IP address was used, how much traffic each generated, which method was used, and how long until the session times out.

You can also select a user or user group and then select *Deauthenticate* to force the user or user group to log in again.

Quarantine console

The *Quarantine* console shows all IP addresses and interfaces blocked by NAC quarantine. The list also shows all IP addresses, authenticated users, senders, and interfaces blocked by data leak prevention (DLP). The system administrator can selectively release users or interfaces from quarantine or configure quarantine to expire after a selected time period.

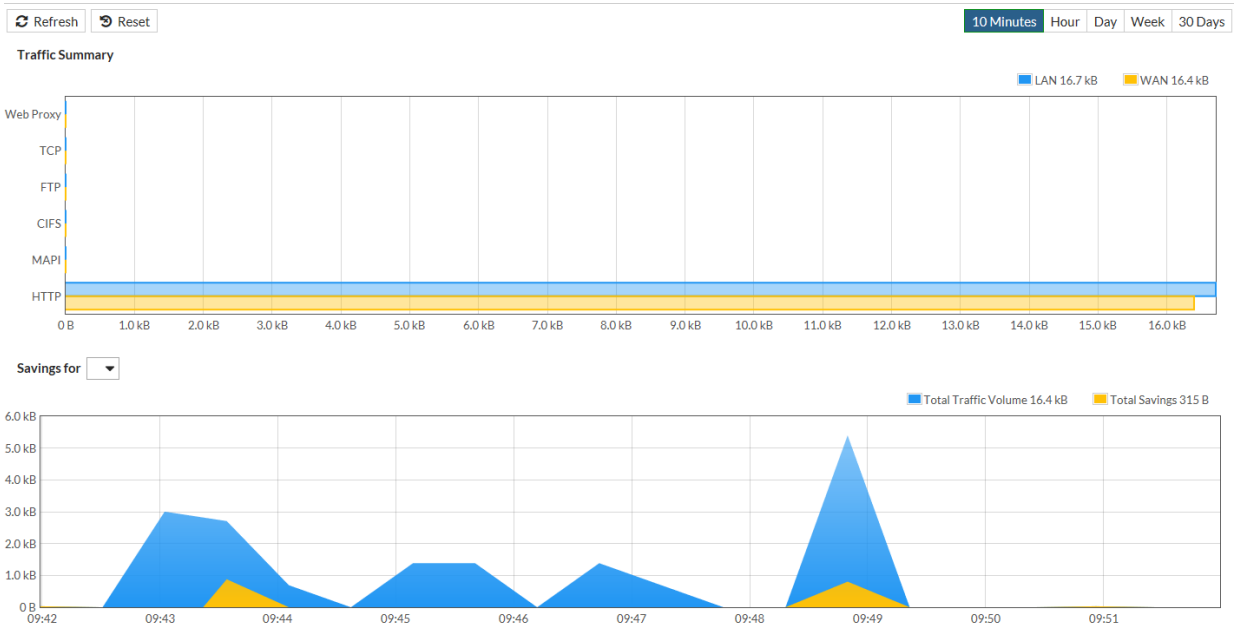
All sessions started by users or IP addresses on the user quarantine list are blocked until the user or IP address is removed from the list. All sessions to an interface on the list are blocked until the interface is removed from the list.

WAN Opt. Peer console

The *WAN Opt. Peer* console allows you to see a list of available WAN optimization peers and how much traffic reduction each peer is responsible for.

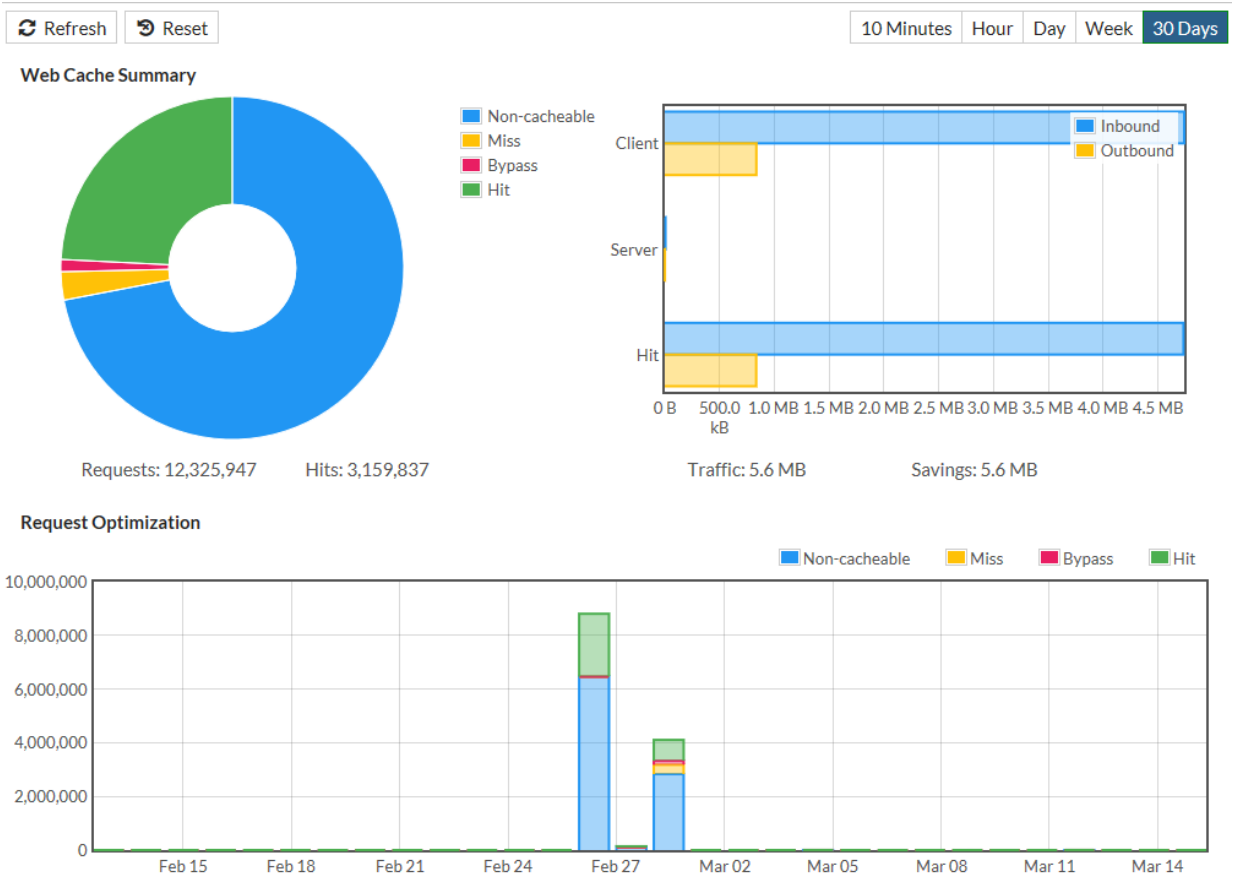
WAN Optimization console

The *WAN Optimization* console allows you to see a summary of LAN and WAN traffic. A second graph show how many bytes have been saved by WAN optimization. You can select the time period to display.



Caching and Optimization console

The *Caching and Optimization* console allows you to see how much traffic is being cached and how much request optimization is being performed. You can select the time period to display.


Refresh
Reset
10 Minutes
Hour
Day
Week
30 Days
Web Cache Summary
Non-cacheable
Miss
Bypass
Hit
Client
Server
Hit
Inbound
Outbound
0 B
500.0 kB
1.0 MB
1.5 MB
2.0 MB
2.5 MB
3.0 MB
3.5 MB
4.0 MB
4.5 MB
Requests: 12,325,947
Hits: 3,159,837
Traffic: 5.6 MB
Savings: 5.6 MB
Request Optimization
Non-cacheable
Miss
Bypass
Hit
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
0
Feb 15
Feb 18
Feb 21
Feb 24
Feb 27
Mar 02
Mar 05
Mar 08
Mar 11
Mar 14

Network

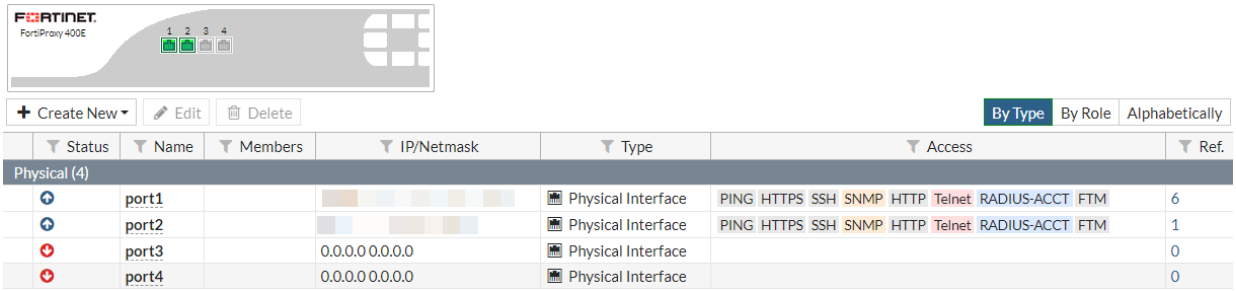
The Network menu allows you to configure the unit to operate on the network. This menu provides features for configuring and viewing basic network settings, such as the unit's interfaces, Domain Name System (DNS) options, and routing table.

This section describes the following:

Interfaces

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.



Right-click on any column heading to select which columns are displayed 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 new interface. See "Create or edit an interface" on page 54.
Edit	Modifies settings within the interface. When you select *Edit*, you are automatically redirected to the *Edit Interface* page. See "Create or edit an interface" on page 54.

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*.
Sorting	Select *By Type*, *By Role*, or *Alphabetically* to change how the rows are displayed on the interface list.
Status	The administrative status for the interface. If the administrative status is a blue arrow, the interface is up and can accept network traffic. If the administrative status is a red arrow, the interface is administratively down and cannot accept traffic. To change the administrative status of an interface, select the *Edit* icon to edit the interface and change the *Interface State* 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.
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.
Type	The type of the interface, such as *Physical Interface*.
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.
DHCP Server	The IPv4 address of the DHCP server.
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 Server	The IPv6 address of the DHCP server.
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 IPs	Displays the secondary IPv4 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.

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:

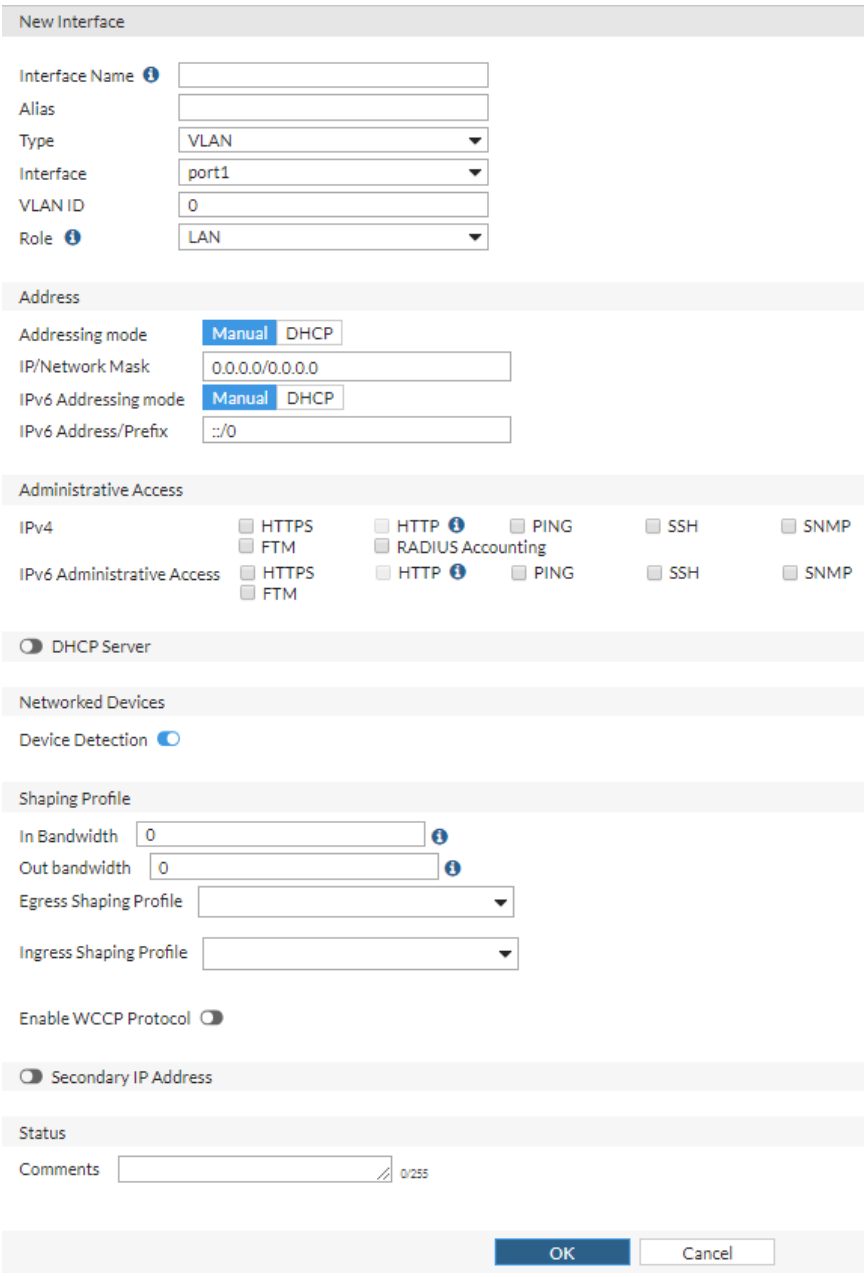
```
config system link-monitor
   edit <link_monitor_name>
      set srcintf <interface_name>
      set server <server_IP_address>
      set protocol {ping | tcp-echo | udp-echo | http | twamp}
      set gateway-ip <gateway_IPv4_address>
      set source-ip <IPv4_address>
      set interval <seconds>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

CLI option	Description
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`.

Create or edit an interface

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



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 select *OK*:

Interface 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*.
Interface	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 except when you add a new VLAN interface.
Interface Members	Select the ports to be included in the interface if the *Type* is *802.3ad Aggregate*.
VLAN ID	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	Select *LAN*, *WAN*, *DMZ*, or *Undefined*. The options displayed on the rest of the page change depending on the role selected.
Estimated Bandwidth	Enter your estimate of the number of Kbps upstream and the number of Kbps downstream needed. This option is displayed only if *Role* is set to *WAN*.
Addressing mode **IPv6 Addressing mode**	Select the addressing mode for the interface: • Select *Manual* and add an IP 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.
IP/Network Mask	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 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*.
Administrative Access **IPv6 Administrative Access**	Select the types of administrative access permitted for IPv4 and IPv6 connections to this 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.
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.
DHCP Server	Enable to add a DHCP server.
Address Range	If you enable the DHCP server, select *Create New* to specify the starting IP address and the ending IP address of the address range.
Netmask	If you enable the DHCP server, enter the netmask of the addresses that the DHCP server assigns.
Default Gateway	If you enable the DHCP server, select *Same as Interface IP* or select *Specify* and enter the IP address of the default gateway that the DHCP server assigns to DHCP clients.
DNS Server	If you enable the DHCP server, select *Same as System DNS*, *Same as Interface IP*, or select *Specify* and enter the IP address of the DNS server.

Mode	Select the type of DHCP server the FortiProxy unit will be. By default, it is a *server*. Select *Relay* if needed. If you select *Relay*, enter the IP address for the DHCP server.
NTP Server	To synchronize the system time and date for the DHCP server, select *Local*, *Same as System NTP*, or *Specify*. If you select *Specify*, enter the IP address for the NTP server.
Time Zone	Select the time zone for the DHCP server, either *Same as System* or *Specify*. If you select *Specify*, select the time zone.
Next Bootstrap Server	Enter the IP address of the next bootstrap server.
Additional DHCP Options	Select *Create New* to create new DHCP options.
MAC Reservation + Access Control	Select *Create New* to match an IP address from the DHCP server to a specific client or device using its MAC address. In a typical situation, an IP address is assigned ad hoc to a client, and that assignment times out after a specific time of inactivity from the client, known as the lease time. To ensure a client or device always has the same IP address (there is no lease time), use IP reservation.
Type	Select this to use the DHCP in *Regular* or *IPsec* mode.
Device Detection	Enable or disable whether the FortiProxy unit can monitor your networks and gather information about the devices operating on those networks.
In Bandwidth	Enter the bandwidth limit for incoming traffic. The range is 0-16,776,000 kbps. Enter 0 for unlimited bandwidth.
Out bandwidth	Enter the bandwidth limit for outgoing traffic. The range is 0-16,776,000 kbps.
Egress Shaping Profile	Select a traffic shaper for outgoing traffic. To create a traffic shaper, see "Create or edit a traffic shaper" on page 143.
Ingress Shaping Profile	Select a traffic shaper for incoming traffic. To create a traffic shaper, see "Create or edit a traffic shaper" on page 143.
Scan Outgoing Connections to Botnet Sites	Select *Disable* or *Block* to protect from botnet and command-and-control traffic. This option is available only if *Role* is *WAN*, *DMZ*, or *Undefined*.
Enable Explicit Web Proxy	Select this to enable explicit web proxying on this interface.

Enable Explicit FTP Proxy	Select this to enable 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.
Secondary IP Address	Add additional IPv4 addresses to this interface. See "Create or edit an interface" on page 59.
Comments	Enter a description up to 255 characters to describe the interface.

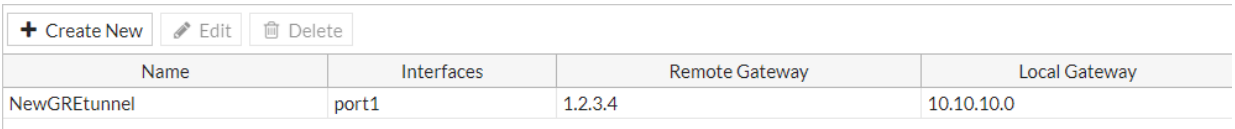
To add secondary IP addresses:

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. Select *OK*.
   The new IP address is added to the table.

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.



Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

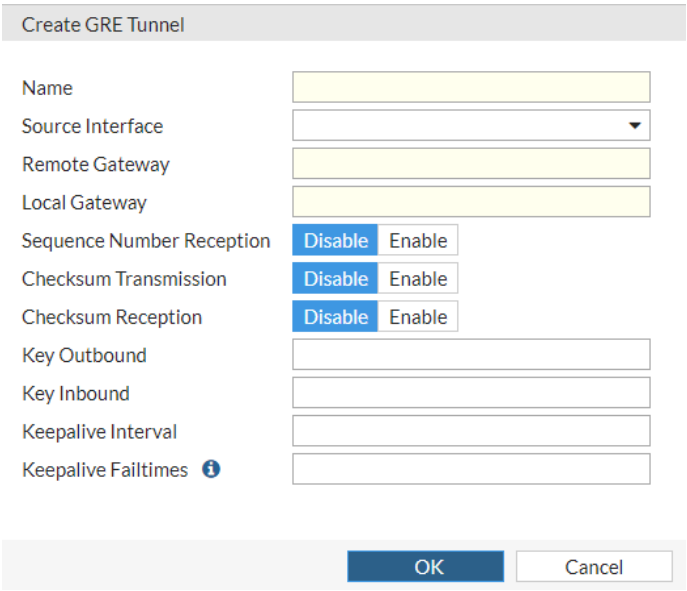
The following options are available:

Create New	Select to create a new GRE tunnel. See "Create or edit a GRE tunnel" on page 60.

Edit	Modifies settings for the selected GRE tunnel. When you select *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.

Create or edit a GRE tunnel

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



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

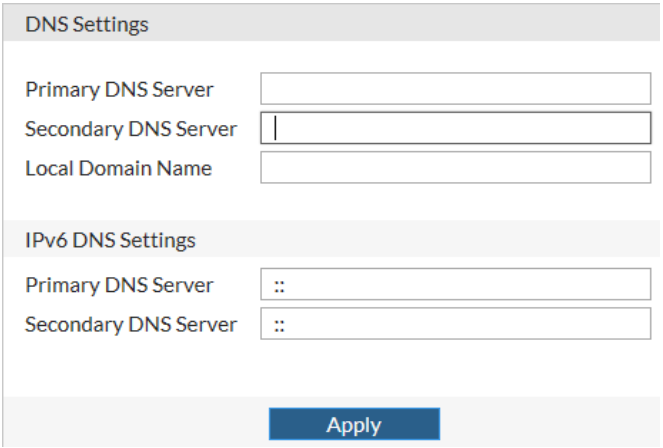
Configure the following settings in the Create GRE Tunnel page or Edit GRE Tunnel page and then select *OK*:

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.

DNS settings

Several FortiProxy functions use DNS, including alert email. You can specify the IP addresses of the DNS servers to which your unit connects. 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*:

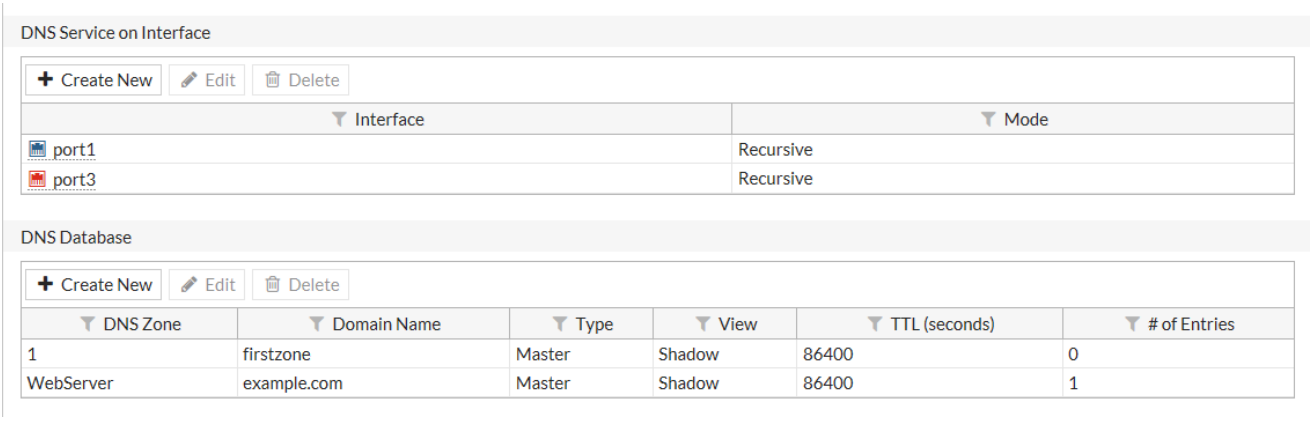
Primary DNS Server	Enter the primary DNS server IPv4 or IPv6 address.
Secondary DNS Server	Enter the secondary DNS server IPv4 or IPv6 address.
Local Domain Name	Enter the domain name to append to addresses with no domain portion when performing DNS lookups.

DNS service

You can also create local DNS servers for your network. Depending on your requirements, you can manually maintain your entries (master DNS server) or use it as a jumping point, where the server refers to an outside source (slave DNS server). A local master 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 (master or slave). 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*.



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

- "Create or edit a DNS service" on page 62
- "Create or edit a DNS zone" on page 63

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. Select *OK*.
   The new DNS service is added to the table.

To add a DNS service on a specific interface:

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

Create or edit a DNS zone

You can create a master or a slave DNS zone.

To create a master DNS zone:

1. Go to *Network* > *DNS Service* and, under *DNS Database*, select *Create New*.
2. Select *Master* 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 master DNS server.
7. Enter the contact 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 or disable *Authoritative*.
10. Select or create a DNS entry. See "Create or edit a DNS entry" on page 63.
11. Select *OK* to save your new DNS zone.
    The new DNS zone is added to the table.

To create a slave DNS zone:

1. Go to *Network* > *DNS Service* and, under *DNS Database*, select *Create New*.
2. Select *Slave* 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 master DNS zone.
7. Enable or disable *Authoritative*.
8. Select *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. Select *OK* to save your changes.

Create or edit a DNS entry

You can create or edit a DNS entry.

To create a DNS entry:

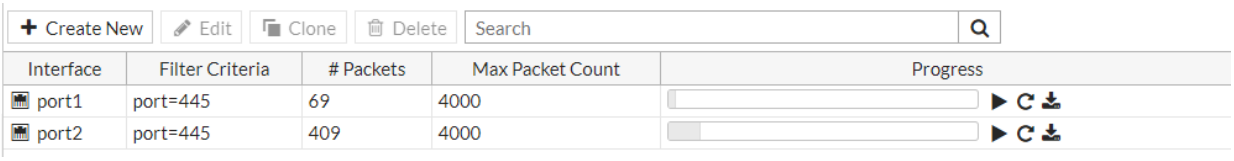
1. Go to *Network* > *DNS Service* and, under *DNS Database*, select a DNS zone and then select *Edit*.
2. In the Edit DNS Zone page, select *Create New*.
   The New DNS Entry page opens.
3. Select the type of DNS entry, one of *Address (A)*, *Name Server (NS)*, *Canonical Name (CNAME)*, *Mail Exchange (MX)*, *IPv6 Address (AAAA)*, *IPv4 Pointer (PTR)*, or *IPv6 Pointer (PTR)*.
4. Enter the host name for the DNS entry.
5. Enter the IP address for the DNS entry.
6. 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.
7. Enable or disable the status to make the DNS entry active or inactive.
8. Select *OK* to save your new DNS entry.
   The new DNS entry is added to the table.
9. Select *OK* to save your changes to the DNS zone.

To edit a DNS zone:

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



Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

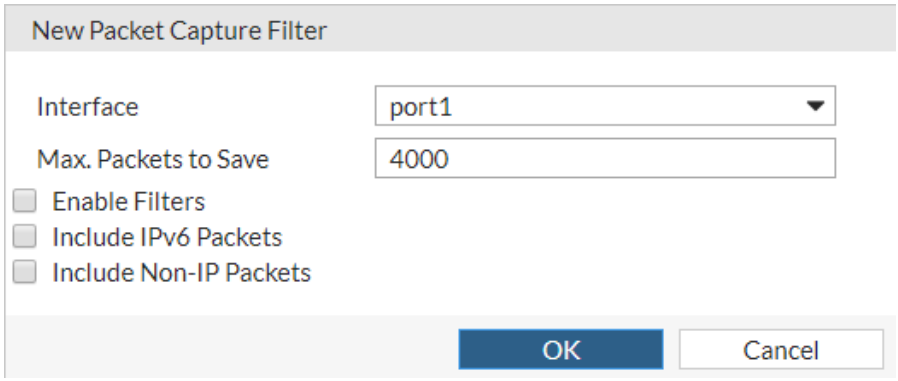
The following options are available:

Create New	Creates a new packet capture filter. See "Create or edit a packet capture filter" on page 66.
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.
Interface	The interface or port number that the filter will examine.
Filter Criteria	The hosts, ports, VLANs, or protocols being examined.
# Packets	The number of packets captured.
Max Packet Count	The maximum number of packets to collect.
Progress	Whether the filter 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.

To create a new packet capture filter:

1. Select *Create New*.



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

Interface	Select an interface.
Max. Packets to Save	Enter how many packets to collect.
Enable Filters	If you enable this option, you can create a filter using multiple host names, ports, VLAN identifiers, and protocols. Use commas to separate items. Use a hyphen to specify a range.

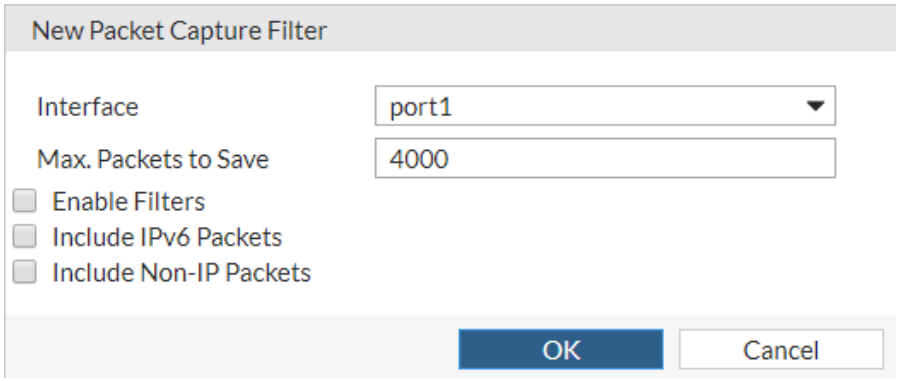
Include IPv6 Packets	Select this option if you want to collect IPv6 packets, as well as IPv4 packets.
Include Non-IP Packets	Select this option if you want to include packets from non-IP protocols.

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 select *OK*:

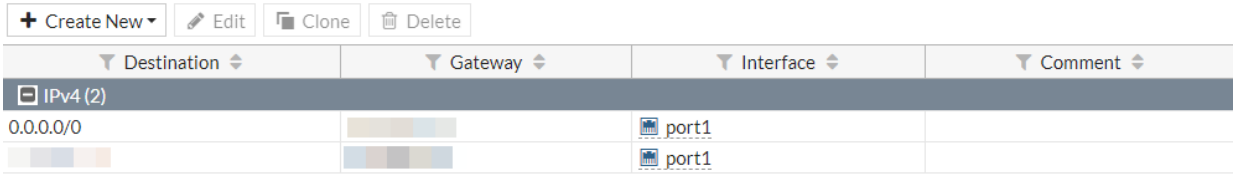
Interface	Select an interface.
Max. Packets to Save	Enter how many packets to collect.
Enable Filters	If you enable this option, you can create a filter using multiple host names, ports, VLAN identifiers, and protocols. Use commas to separate items. Use a hyphen to specify a range.
Include IPv6 Packets	Select this option if you want to collect IPv6 packets, as well as IPv4 packets.
Include Non-IP Packets	Select this option if you want to include packets from non-IP protocols.

To edit a packet capture filter:

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

Static routing

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



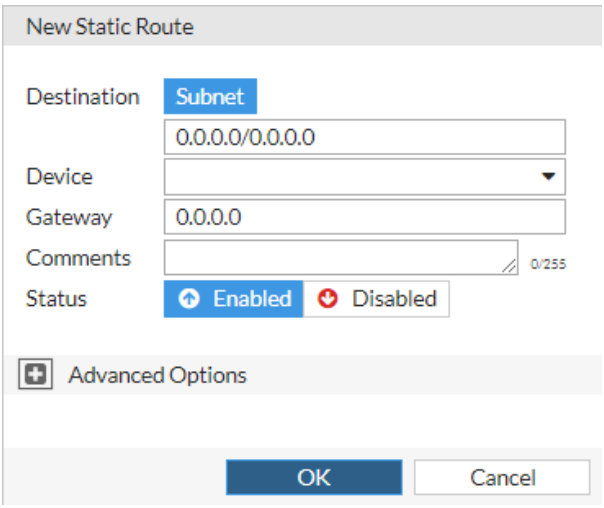
Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

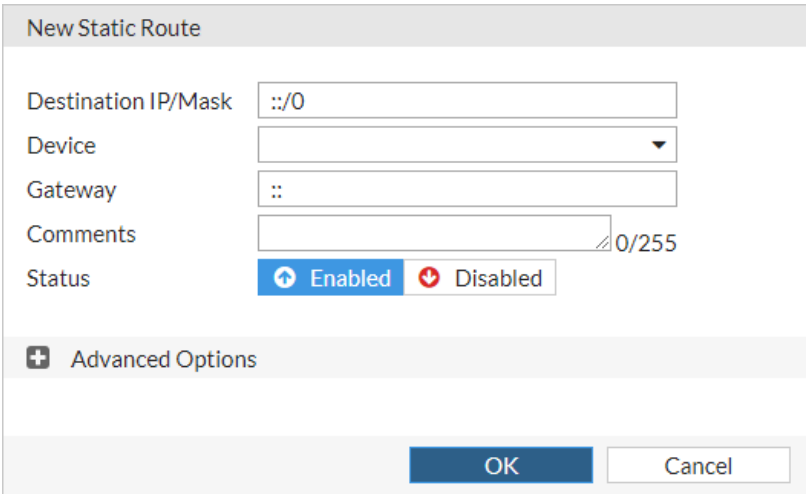
The following options are available:

Create New	Creates a new IPv4 or IPv6 static route. See "Create or edit a static route" on page 67.
Edit	Modifies settings within the static route. See "Create or edit a static route" on page 67.
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*.
Destination	The destination IP addresses and network masks of packets that the FortiProxy unit intercepts.
Gateway	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.
Comment	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 new static route.





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

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

Destination or Destination IP/Mask	Enter the IP address and netmask of the new static route. To use the default route, set the IP address and netmask to 0.0.0.0/0.0.0.0.
Device	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.

Gateway	Enter the gateway IP address for those packets that you intend the unit to intercept.
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	Select 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.

System

The System menu provides submenus for four areas: system administration, system configuration, and certificates.

System administration covers the following topics:

- "Administrators" on page 70
- "Administrative profiles" on page 74
- "Firmware" on page 77
- "Settings" on page 78

System configuration covers the following topics:

- "High availability (HA)" on page 81
- "SNMP" on page 83
- "Replacement messages" on page 93
- "FortiGuard" on page 104
- "WCCP settings" on page 109
- "Advanced" on page 116
- "Feature visibility" on page 120

"Certificates" on page 123 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.

Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

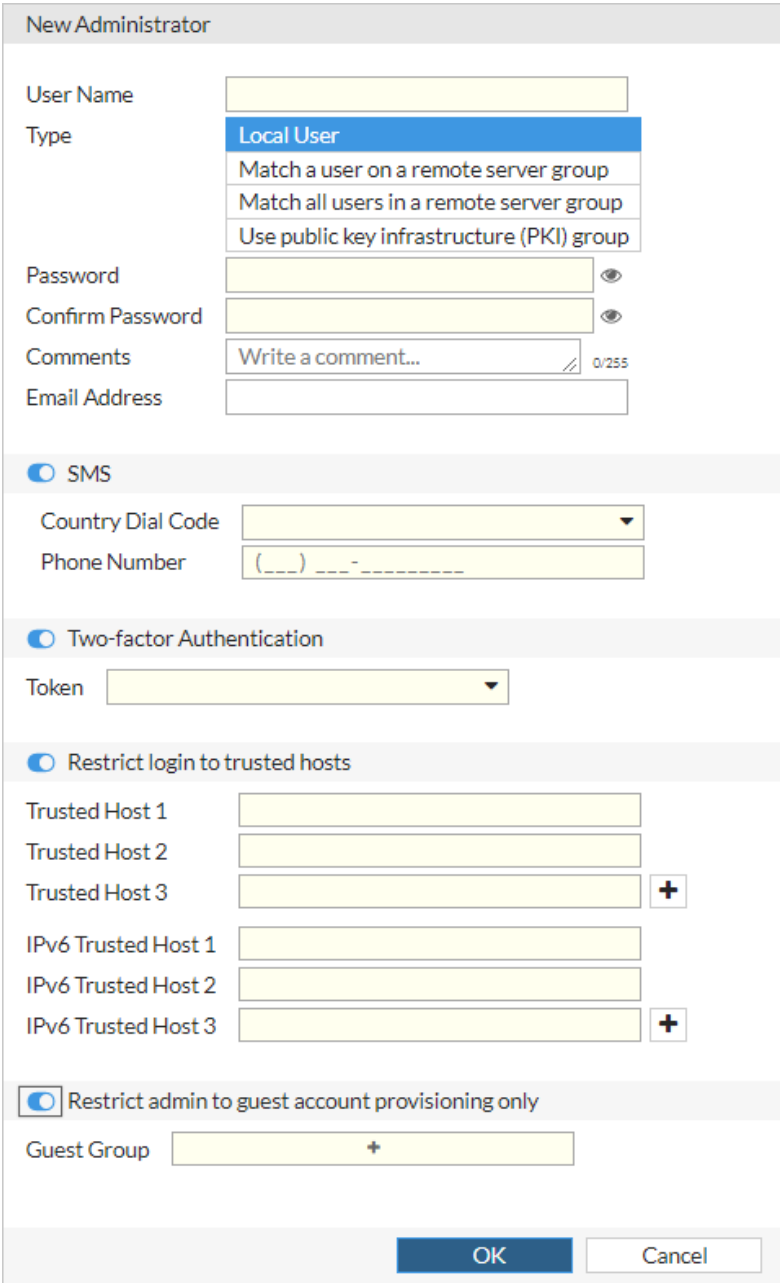
You need to use the default `admin` account, an account with the super_admin admin profile, or an administrator with read-write access control to add new administrator accounts and control their permission levels. If you log in with an administrator account that does not have the super_admin admin profile, 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 72.
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 72.
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 select *Edit* to open the Edit Administrator page.

Configure the following settings in the New Administrator page or Edit Administrator page and then select *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.
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. These addresses all default to 0.0.0.0/0 or 0.0.0.0/0.0.0.0.
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.

Administrative 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.

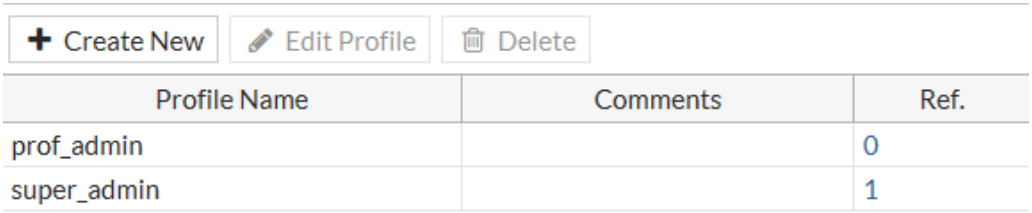
The admin profile has a similar effect on administrator access to CLI commands. You can access `get` and `show` commands with *Read Only* access, but access to `config` commands requires *Read-Write* access.

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 a new admin profile.

To view administrator profiles, go to *System* > *Admin Profiles*.



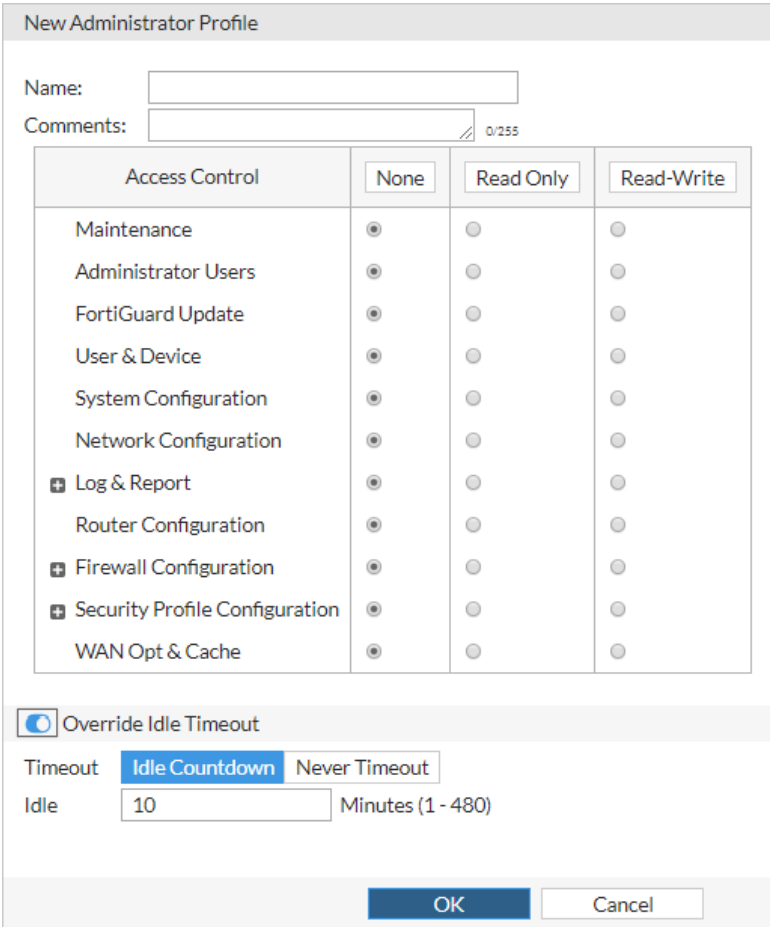
Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Creates an administrator profile. See "Create or edit an administrator profile" on page 76.
Edit Profile	Modifies the selected administrator profile. When you select *Edit Profile*, the Edit Administrator Profile page opens. See "Create or edit an administrator profile" on page 76. **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 select *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 select *OK*.

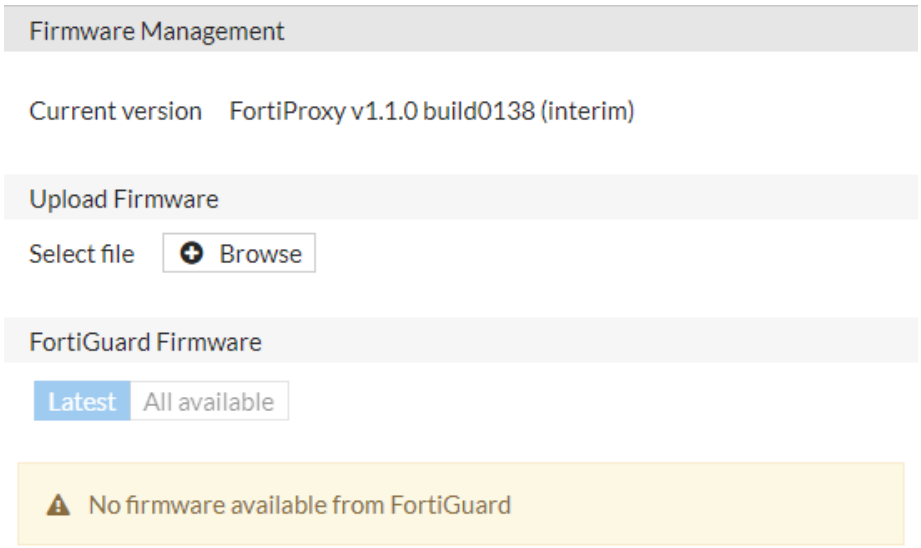
NOTE: You cannot edit the super_admin profile.

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 • 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.



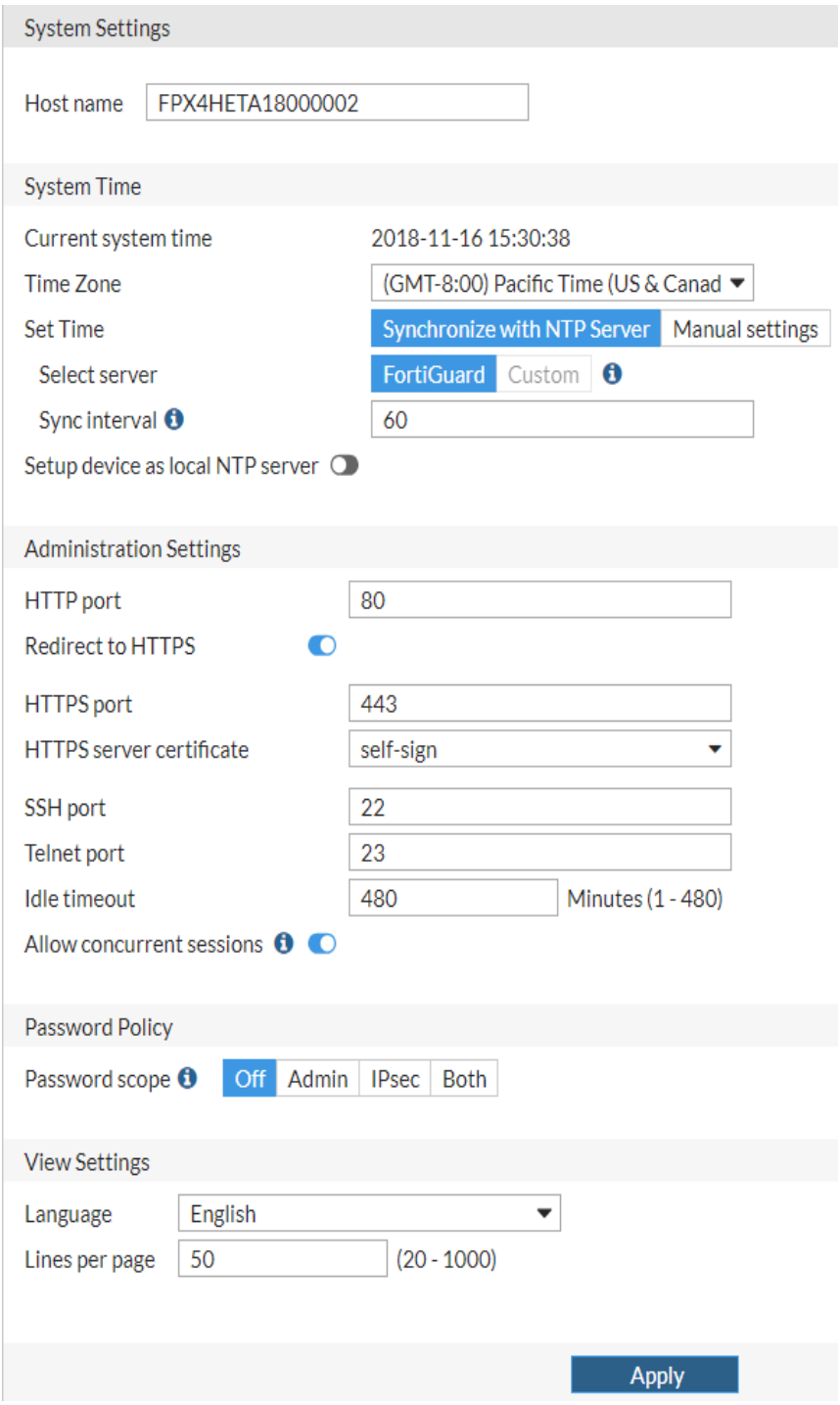
To upload a new firmware image from your computer:

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 admin settings to configure general settings for web administration access, password policies, idle timeout settings, and display settings.

Go to *System* > *Settings* to configure administrator 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	
Current system time	The current time. By default, FortiProxy has the daylight savings time configuration enabled. The system time must be manually adjusted after daylight saving time ends.
Time Zone	Select the time zone of your FortiProxy unit.
Set Time	Select *Synchronize with NTP Server* or *Manual settings*.
Select server	If you select *Synchronize with NTP Server*, you can either use the default FortiGuard server or specify a custom server using the CLI.
Sync interval	If you select *Synchronize with NTP Server*, enter how often the FortiProxy time is synchronized with the NTP server. The value range is 1-1,440 minutes.
Date	If you select *Manual settings*, enter the date.
Hour	If you select *Manual settings*, enter the hour in 24-hour format.
Minute	If you select *Manual settings*, enter the number of minutes.
Second	If you select *Manual settings*, enter the number of seconds.
Minute	If you select *Manual settings*, enter the number of minutes.
Setup device as local NTP server	Enable to identify a specific interface for this self-originating traffic. After you enable this option, select + in the Listen on Interfaces field and select one or more interfaces.
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.
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.
Lines per page	Number of lines per page to display in table lists. The range is from 20 to 1000; the default is 50.

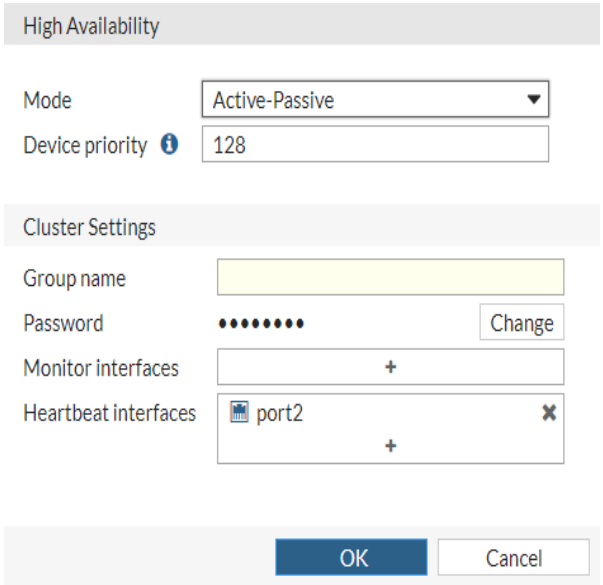
High availability (HA)

FortiProxyHA 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. To configure HA and cluster settings or to view the cluster member list, select *System* > *HA*.



Configure the following settings and then select *OK*:

Mode	Enter the mode. Select *Standalone*, *Config-Sync*, or *Active-Passive* from the drop-down menu. If you select *Standalone*, no other options are displayed.
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 master) 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.
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 Interface	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.

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
```

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 87 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.

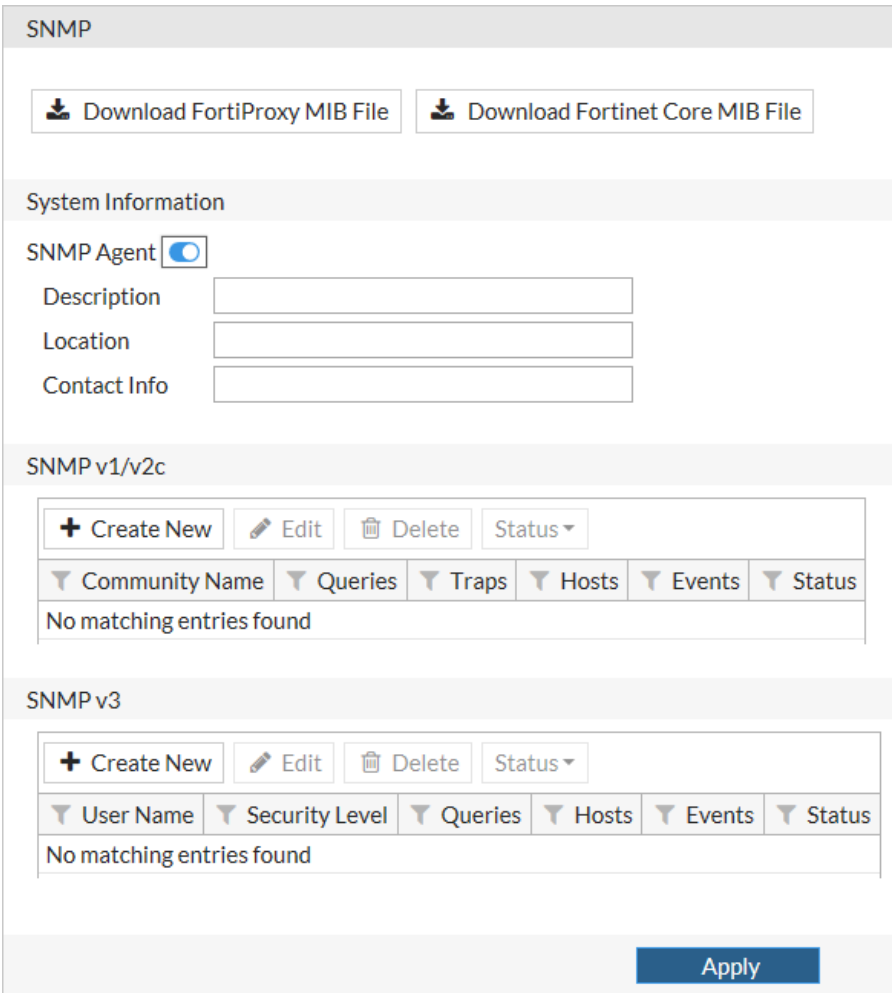
Before a remote SNMP manager can connect to the FortiProxy agent, you must configure one or more FortiProxy interfaces to accept SNMP connections. Interfaces are configured in *Network* > *Interfaces*. See "Interfaces" on page 51.

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*.



Configure the following settings and select *Apply*:

Download FortiProxy MIB File	Download the FortiProxy MIB file. See "Fortinet MIBs" on page 87.
Download Fortinet Core MIB File	Download the Fortinet MIB file. See "Fortinet MIBs" on page 87.
SNMP Agent	Enable the FortiProxy SNMP agent. See "SNMP agent" on page 88.
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 89.
Edit	Modifies settings within an SNMP community. When you select *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 92.
Edit	Modifies settings within the SNMP v3 user. When you select *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 83.

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 or RFC	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. Select *Apply* to save your changes.

To configure the SNMP agent with the CLI:

Enter the following CLI commands:

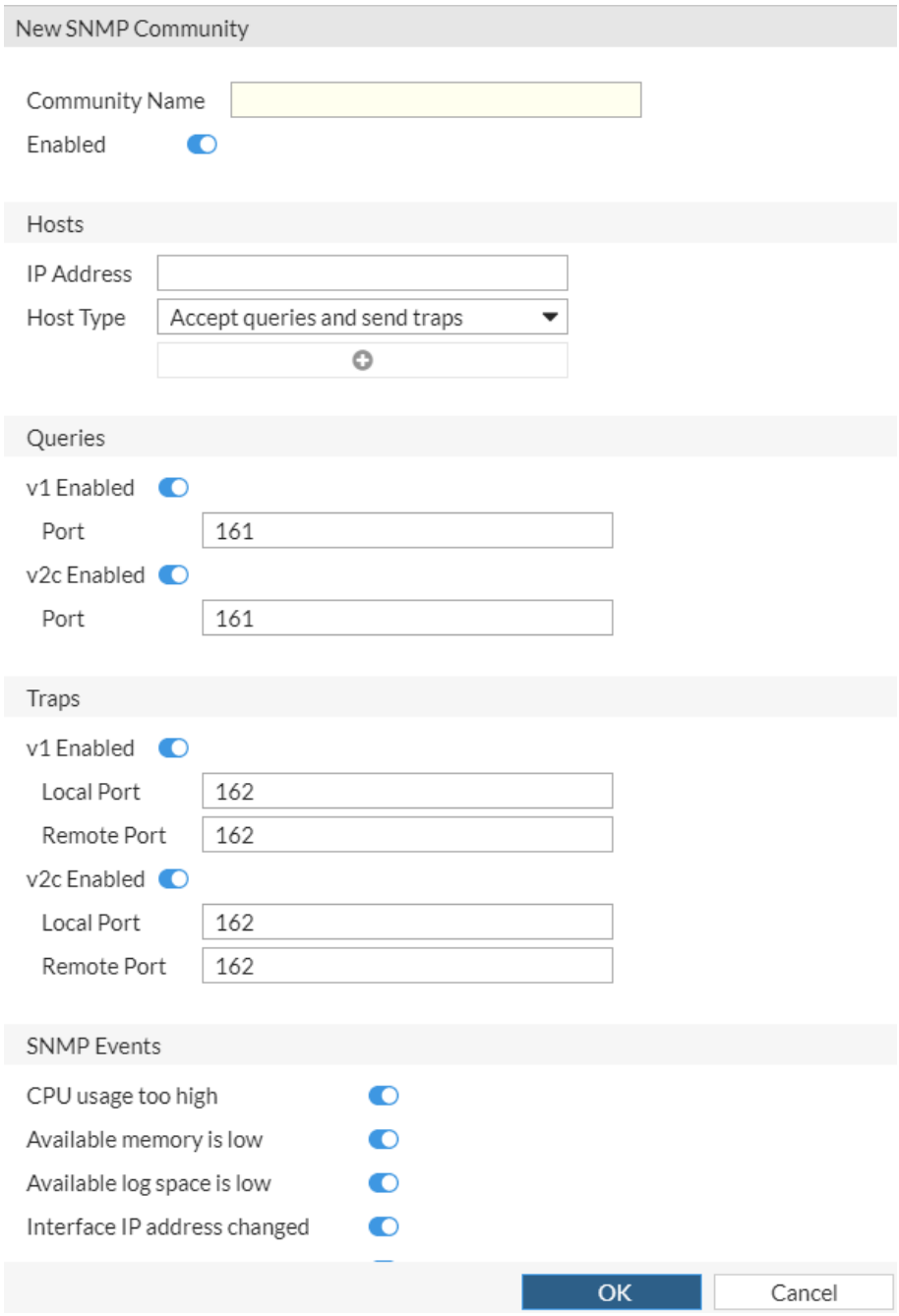
```
config system snmp sysinfo
   set status enable
   set contact-info <contact_information>
   set description <description_of_FortiProxy>
   set location <FortiProxy_location>
end
```

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.



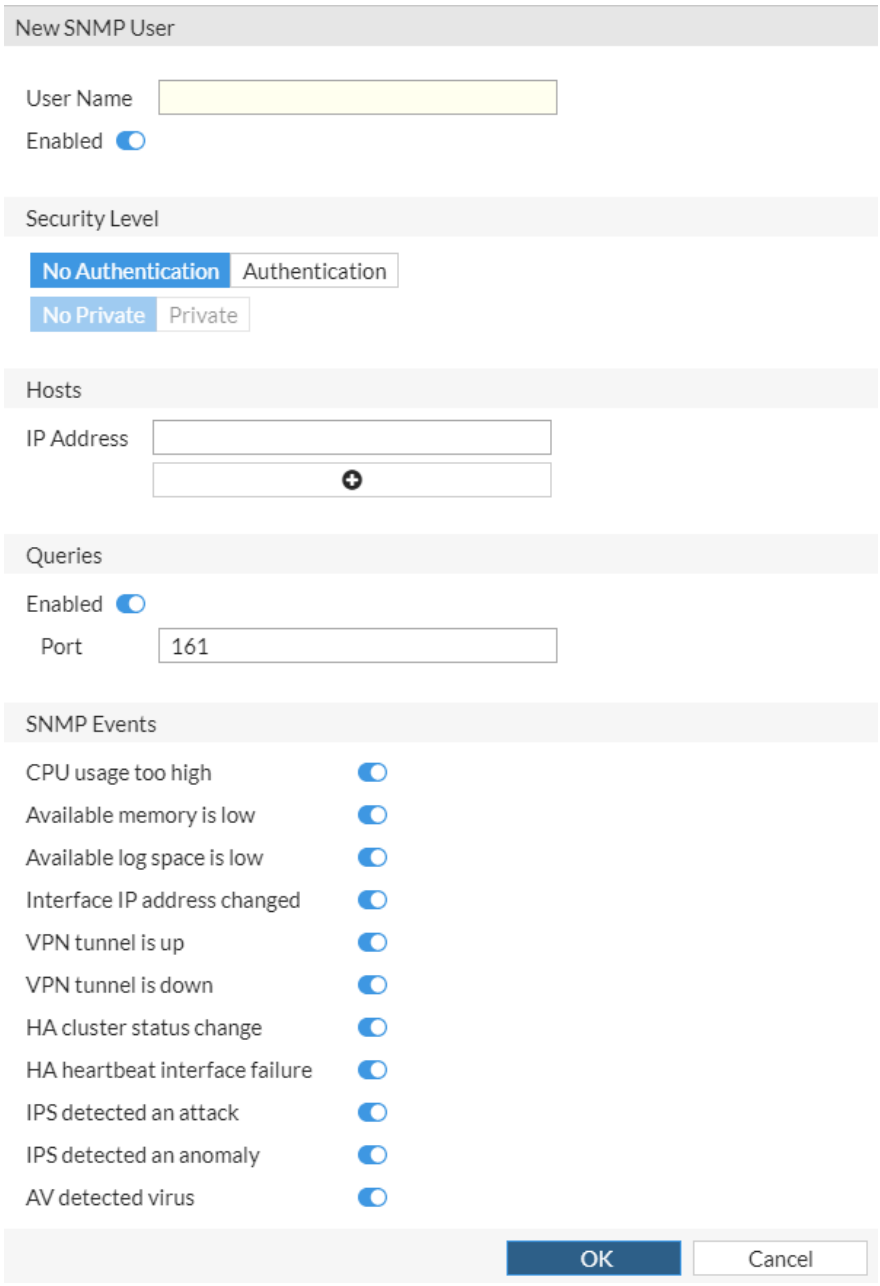
Configure the following settings in the New SNMP Community page or Edit SNMP Community page and select *OK*:

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.



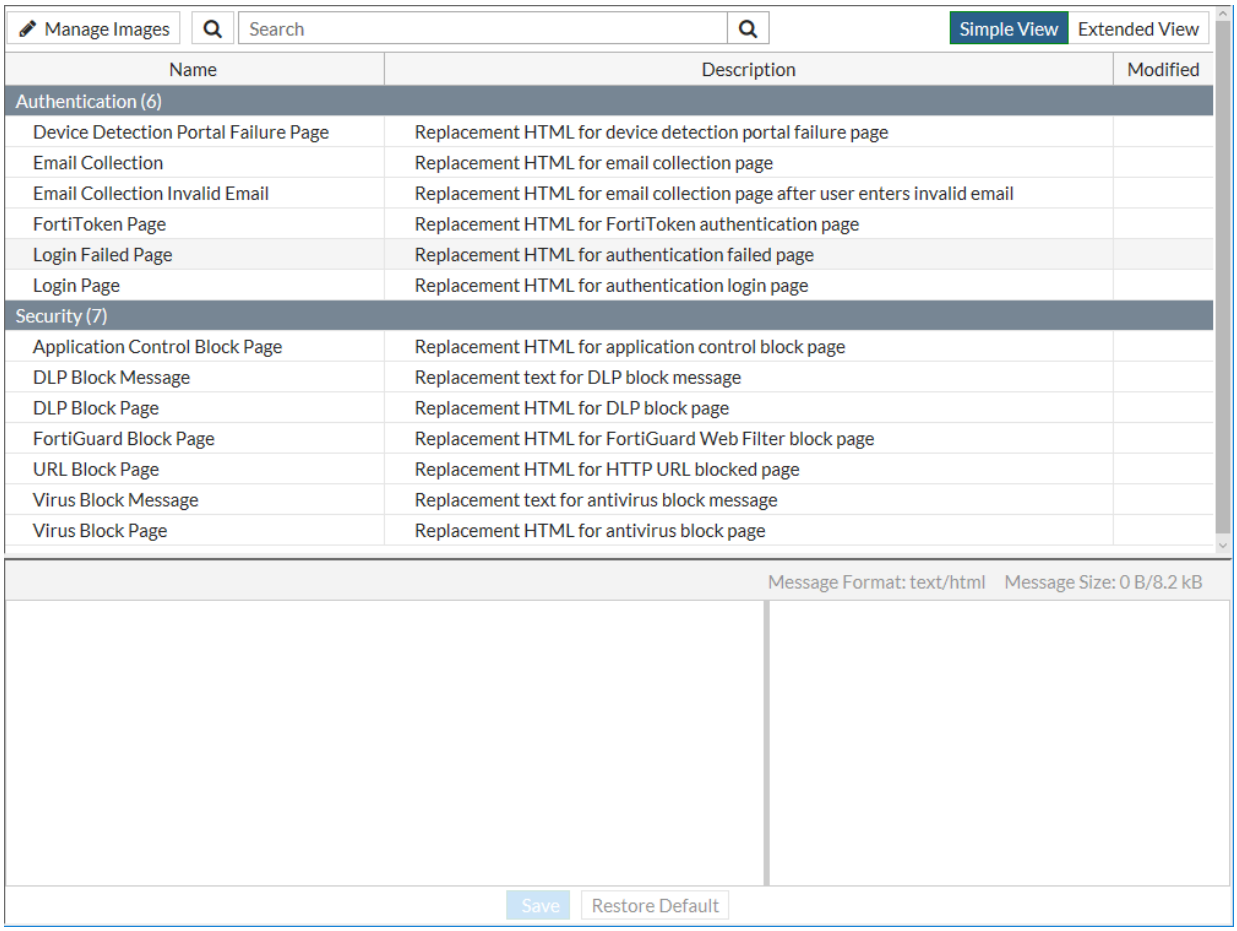
Configure the following settings in the New SNMP User page or Edit SNMP User page and select *OK*:

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 N*o 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 the plus sign 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.



The following options are available:

Manage Images	Select to view the available images and their respective tags.
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 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 the 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 printout.

Category	Messages	Description
Authentication (continued)	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.
	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
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.

Category	Messages	Description
HTTP	Archive Block Message	Replacement HTML for HTTP archive block message.
	Block Message	Replacement HTML for HTTP file block 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.
	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
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 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.

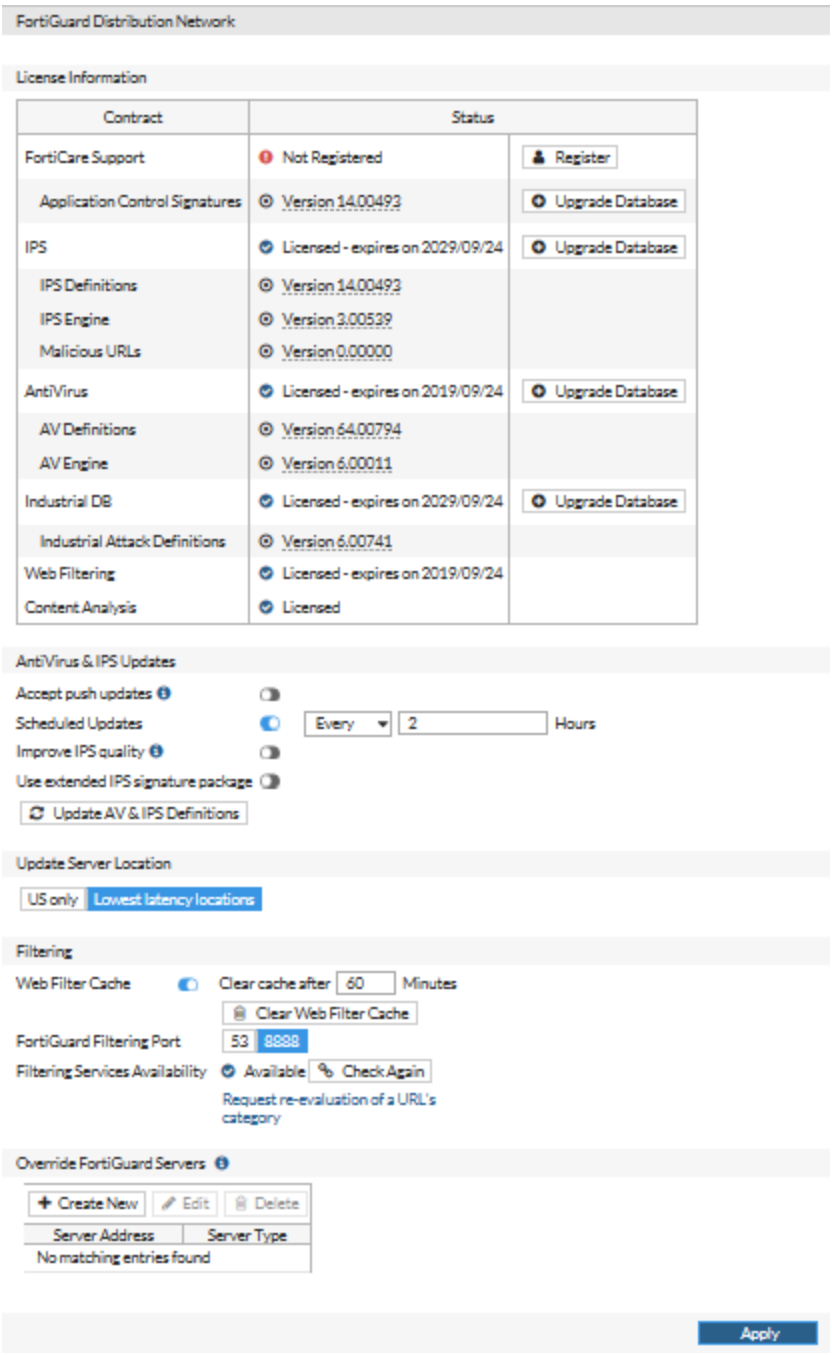
Category	Messages	Description
Spam	ASE Block Message	Replacement text for emails blocked due to detection by Advanced Antispam Engine (ASE).
	Banned Word Block Message	Replacement text for emails blocked due to prohibited content (banned words) in message.
	DNSBL Block Message	Replacement text for emails 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.
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.
Traffic Quota	Traffic Quota Limit Exceeded Page	Replacement HTML for traffic quota limit exceeded block page.

Category	Messages	Description
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.

FortiGuard

The *FortiGuard Distribution Network* page provides information and configuration settings for FortiGuard subscription services. For more information about FortiGuard services, see the FortiGuard Center web page.

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*. 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.
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.
Anti-Spam Cache	Enable the antispam cache and then enter the number of minutes to store the antispam cache.
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 select *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 select *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*.

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 chapter 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 select *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 select *OK* to save your changes.
4. Go to *System* > *Settings*.
5. Select *Enable* for the *WCCP Cache Engine* and then select *Apply* to save your changes.
6. Go to *System* > *WCCP Settings* and select *Create New*.
7. 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.

8. Select *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
   vdom-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 vdom-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 vdom-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 vdom-root: num=0, usable=0
diag debug application wccpd -1
Sample output:
wccp_on_recv()-98: vdom-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
```

Advanced

The Advanced page offers configuration for features that will interest more experienced users.

Email service

To configure a custom email server in the GUI:

1. Go to *System* > *Advanced*.
2. Move the Use Custom Email Server slider to enable it.
3. Enter the name of the SMTP server.
   NOTE: The SMTP server must be a server that does not support SSL/TLS connections.

4. Enter the port the SMTP server will use.
5. Enter an email address for replies.
6. If you want to use authentication, move the Authentication slider to enable it, enter a user name, and enter the corresponding password.
7. Select *None*, *SMTPS*, or *STARTTLS* for the security mode.

To configure a custom email server in the CLI:

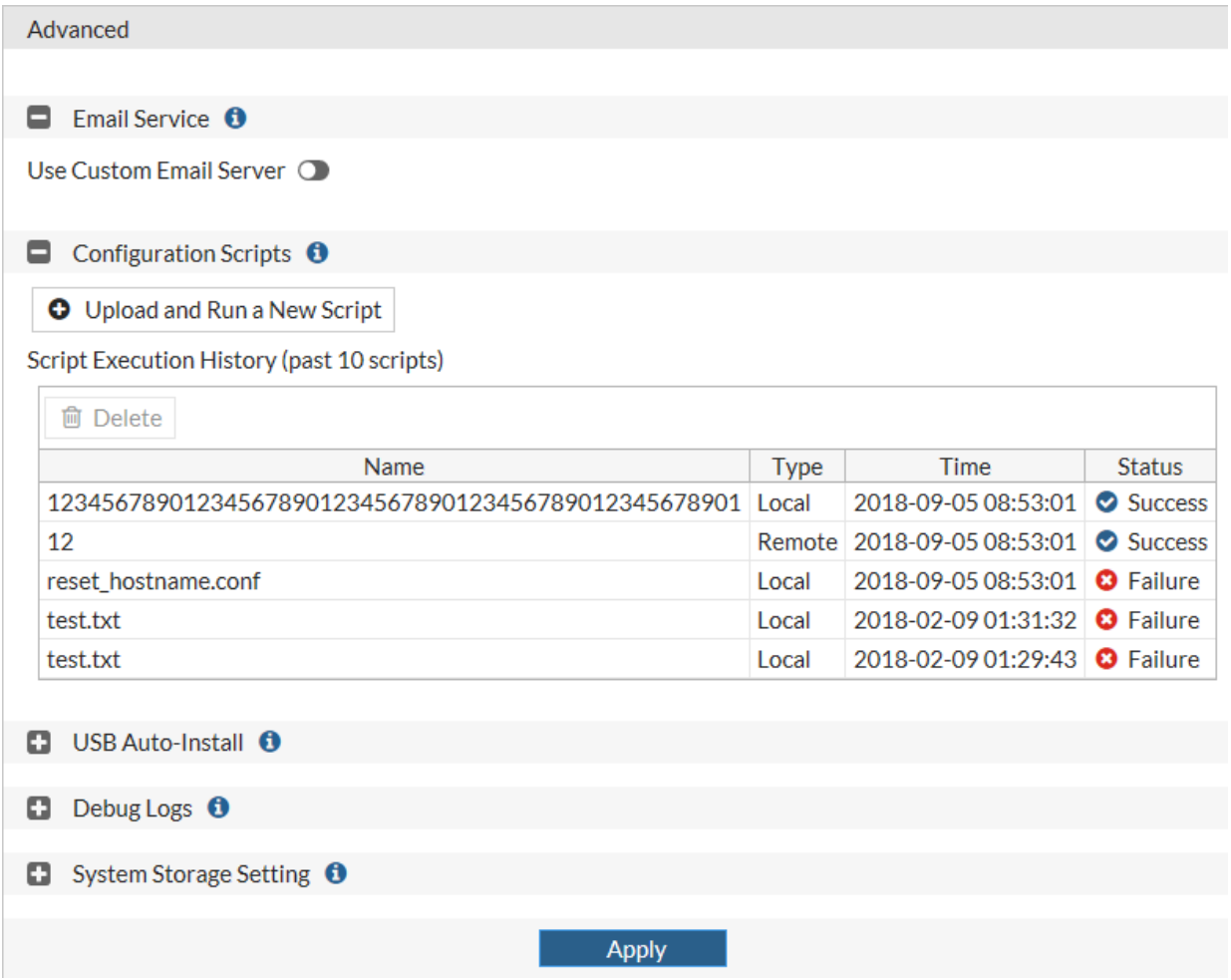
```
config system email-server
   set type                        --Configure a custom email server.
   set reply-to                    --Enter the default reply to email address.
   set server <IP or hostname>     --Enter the name or address of the SMTP email server.
   set port                        --Set the SMTP server port.
   set source-ip                   --Set the SMTP server source IP.
   set source-ip6                  --Set the SMTP server source IP.
   set authenticate                --Enable or disable authentication.
   set validate-server             --Enable or disable the validation of the server certificate.
   set security                    --Set connection security.
   next
end
```

Configuration scripts

Scripts are text files containing CLI command sequences. Scripts can be used to deploy identical configurations to many devices. For example, if all of your devices use identical security policies, you can enter the commands required to create the security policies in a script, and then deploy the script to all the devices which should use those same settings.

Use a text editor such as Notepad or other application that creates simple text files. Enter the commands in sequence, with each line as one command.

After you have created a script file, you can then upload it through *System* > *Advanced*. When a script is uploaded, it is automatically executed.



Commands that require the FortiProxy unit to reboot when entered in the command line will also force a reboot if included in a script.

To execute a configuration script:

1. Go to *System* > *Advanced*.
2. Select *Upload and Run a New Script* and then locate the script file.
3. Select *Open*.

If the FortiProxy unit is not configured for remote management, or if it is configured to use a FortiManager unit, uploaded scripts are discarded after execution. Save script files to your management PC if you want to execute them again later.

If the FortiProxy unit is configured to use the FortiGuard Analysis and Management Service, the script file is saved to the remote server for later reuse. You can view the script or run it from the FortiGuard Analysis and Management Service portal web site.

USB auto-install

This feature allows the FortiProxy unit to automatically install a file from a USB drive after the FortiProxy unit is restarted.

- Move the Detect Configuration slider to enable it if you want the FortiProxy unit to install a configuration file from a USB drive after the FortiProxy unit is restarted.
- Move the Detect Firmware slider to enable it if you want the FortiProxy unit to install a firmware image from a USB drive after the FortiProxy unit is restarted.

Debug logs

Customer Support might request a copy of your debug logs for troubleshooting.

To download the debug logs:

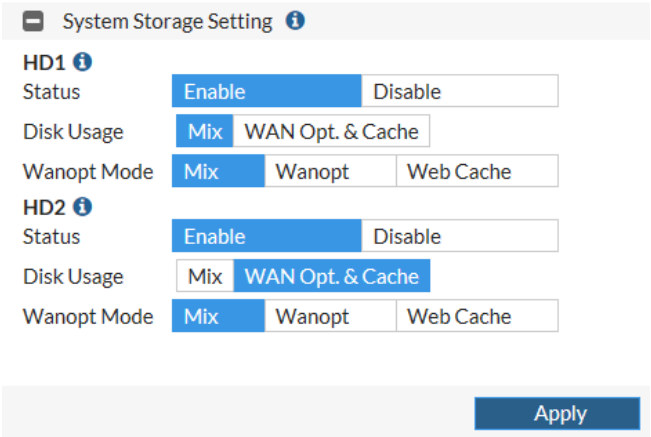
1. Go to *System* > *Advanced*.
2. Select Download Debug Logs in the Debug Logs section.

System storage setting

Go to *System* > *Advanced* to view the disk information. The *System Storage Setting* area shows information about the storage space for different features for each hard disk and allows you to edit quota and storage settings. You can use this section for WAN optimization and logging. Hover over the label for the hard disk to see the partition size, disk size, how much is used, and how much is free.

When possible, performance can be improved by logging to a disk that is not used for caching. Go to *Log* > *Log Settings* to change the settings for logging and archiving. See "Log settings" on page 335.

NOTE: If you want to use WAN optimization, go to *System* > *Feature Visibility* and enable *WAN Opt. & Cache*.



Configure the following settings and select *Apply*:

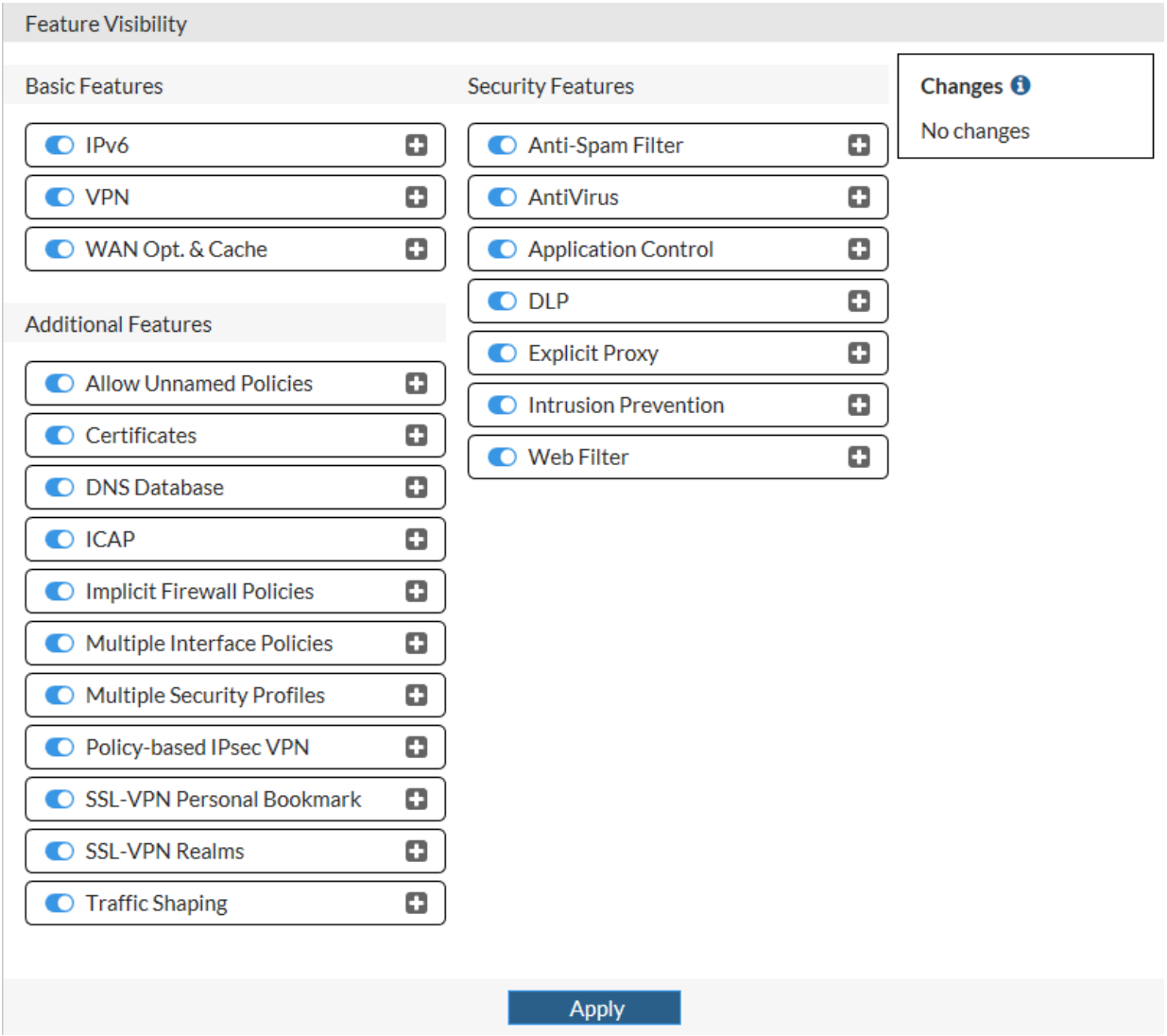
Status	Enable or disable the hard disk drive.
Disk Usage	Select whether the disk is used for *WAN Opt. & Cache* or *Mix*. Select *Mix* if you want to allow logging on the hard disk, as well as WAN optimization and web caching. WAN optimization requires significant memory resources and generates a high amount of I/O on disk. If possible, avoid other disk-intensive features such as heavy traffic logging on the same disk as the one configured for WAN optimization.

Wanopt Mode	Select *Wanopt* if you want the hard disk used just for WAN optimization, select *Web Cache* if you want the hard disk used just for web caching, or select *Mix* if you want the hard disk used for both WAN optimization and web caching.

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.
WAN Opt. & Cache	Controls the visibility of the *WAN Opt. & Cache* menu. Enables WAN optimization and web caching to reduce the amount of bandwidth used by traffic on your WAN.
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.
DNS Database	Allows you to set up the FortiProxy unit as the DNS server for your network. You can add local DNS entries to the DNS database and forward other DNS lookups to external DNS servers, manage the DNS database from *Network* > *DNS*, and optionally set up DNS filter profiles (*Security Profiles* > *DNS Filter*) and add them to a DNS server on a FortiProxy interface.
ICAP	Controls the visibility of the *Security Profiles* > *ICAP* menu. 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.
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.
Local Reports	Controls whether you cna view PDF security reports in the GUI.
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* > *IPv4 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 Realms* 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.
Explicit Proxy	Controls the visibility of the *Enable Explicit Web Proxy* and *Enable Explicit FTP Proxy* options on the *Edit Interface* page. Allows you to enable HTTP, HTTPS, or FTP proxies for your network, which can be added to interfaces. You can create security policies to control access to the proxy and apply UTM and other features to proxy traffic. Users on the network must configure their browsers to use the proxy.
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

There are three types of certificates that FortiProxy units use:

- Local certificates—Local certificates are issued for a specific server or web site. Generally they are very specific and often for an internal enterprise network.
- CA certificates—External CA certificates are similar to local certificates, except they 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. External CA certificates can be deleted, downloaded, and their details can be viewed, in the same way as local certificates.
- Remote certificates—These remote certificates are public certificates without private keys. They can be deleted, imported, and downloaded, and their details can be viewed in the same way as local certificates.

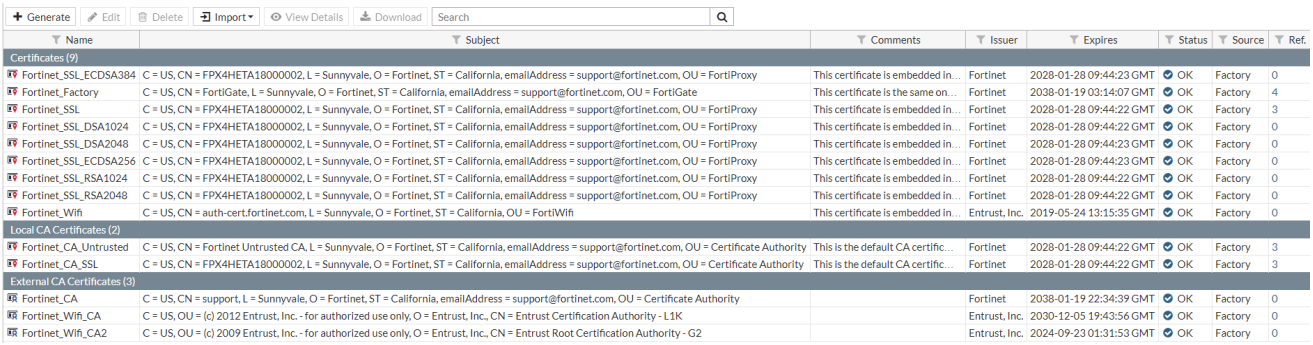
The FortiProxy unit generates a certificate request based on the information you entered to identify the FortiProxy unit. After you generate a certificate request, you can download the request to a computer that has management access to the FortiProxy unit and then forward the request to a CA.

The certificate window also enables you to export certificates for authentication, importing, and viewing.

This section describes the following:

Certificate list

To see a list of certificates that have been imported, go to *System* > *Certificates*.



Name	Subject	Comments	Issuer	Expires	Status	Source	Ref.
Certificates (9)							
Fortinet_SSL_ECDSA384	C = US, CN = FPX4HETA18000002, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiProxy	This certificate is embedded in...	Fortinet	2028-01-28 09:44:23 GMT	OK	Factory	0
Fortinet_Factory	C = US, CN = FortiGate, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate	This certificate is the same on...	Fortinet	2038-01-19 03:14:07 GMT	OK	Factory	4
Fortinet_SSL	C = US, CN = FPX4HETA18000002, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiProxy	This certificate is embedded in...	Fortinet	2028-01-28 09:44:22 GMT	OK	Factory	3
Fortinet_SSL_DSA1024	C = US, CN = FPX4HETA18000002, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiProxy	This certificate is embedded in...	Fortinet	2028-01-28 09:44:22 GMT	OK	Factory	0
Fortinet_SSL_DSA2048	C = US, CN = FPX4HETA18000002, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiProxy	This certificate is embedded in...	Fortinet	2028-01-28 09:44:23 GMT	OK	Factory	0
Fortinet_SSL_ECDSA256	C = US, CN = FPX4HETA18000002, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiProxy	This certificate is embedded in...	Fortinet	2028-01-28 09:44:23 GMT	OK	Factory	0
Fortinet_SSL_RSA1024	C = US, CN = FPX4HETA18000002, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiProxy	This certificate is embedded in...	Fortinet	2028-01-28 09:44:22 GMT	OK	Factory	0
Fortinet_SSL_RSA2048	C = US, CN = FPX4HETA18000002, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiProxy	This certificate is embedded in...	Fortinet	2028-01-28 09:44:22 GMT	OK	Factory	0
Fortinet_Wifi	C = US, CN = auth-cert.fortinet.com, L = Sunnyvale, O = Fortinet, ST = California, OU = FortiWifi	This certificate is embedded in...	Entrust, Inc.	2019-05-24 13:15:35 GMT	OK	Factory	0
Local CA Certificates (2)							
Fortinet_CA_Untrusted	C = US, CN = Fortinet Untrusted CA, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority	This is the default CA certific...	Fortinet	2028-01-28 09:44:22 GMT	OK	Factory	3
Fortinet_CA_SSL	C = US, CN = FPX4HETA18000002, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority	This is the default CA certific...	Fortinet	2028-01-28 09:44:22 GMT	OK	Factory	3
External CA Certificates (3)							
Fortinet_CA	C = US, CN = support, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority		Fortinet	2038-01-19 22:34:39 GMT	OK	Factory	0
Fortinet_Wifi_CA	C = US, OU = (c) 2012 Entrust, Inc. - for authorized use only, O = Entrust, Inc., CN = Entrust Certification Authority - L1K		Entrust, Inc.	2030-12-05 19:43:56 GMT	OK	Factory	0
Fortinet_Wifi_CA2	C = US, OU = (c) 2009 Entrust, Inc. - for authorized use only, O = Entrust, Inc., CN = Entrust Root Certification Authority - G2		Entrust, Inc.	2024-09-23 01:31:53 GMT	OK	Factory	0

Right-click on any column heading to select which columns are displayed 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:

Generate	Generate a CSR. See "Certificate Signing Requests" on page 125.
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. Select *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*.

Import	Import a certificate. Select any of the options in the drop-down list: • *Local Certificate* • *CA Certificate* • *Remote Certificate* • *CRL* See "Import a local certificate" on page 128, "Import a CA certificate" on page 128, "Upload a remote certificate" on page 129, and "Import a CRL" on page 129.
View Details	View a certificate. See "View certificate details" on page 129.
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

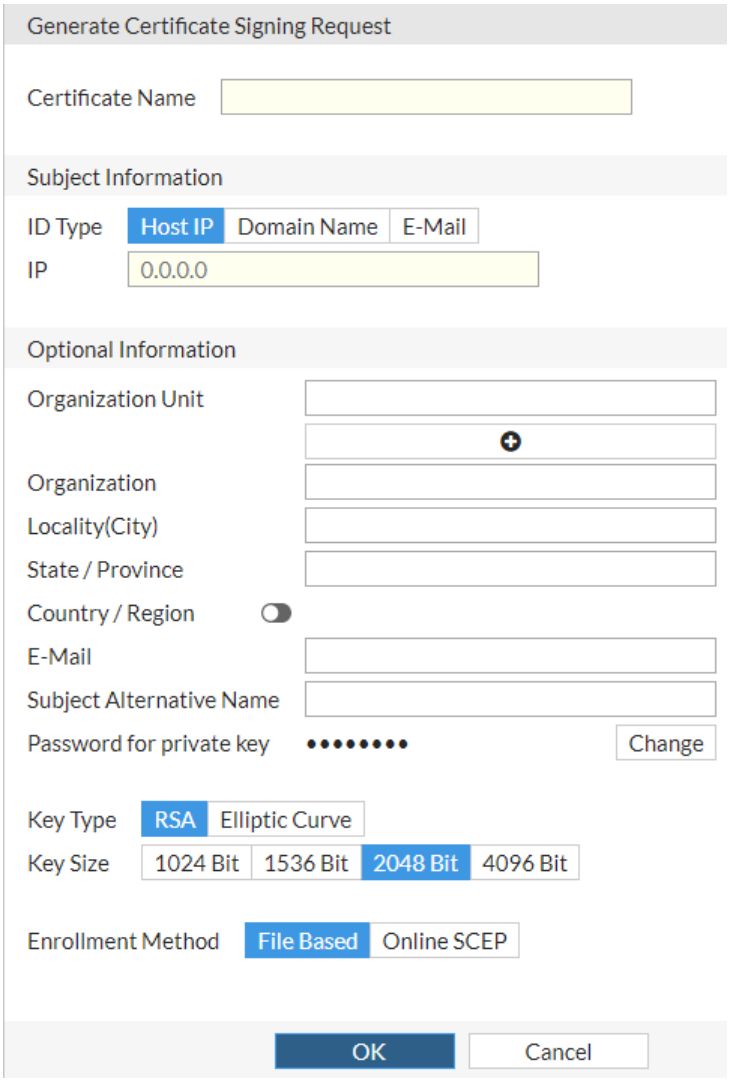
Whether you create certificates locally or obtain them from an external certificate service, you need to generate a Certificate Signing Request (CSR).

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. From the Certificates page, select *Generate*.
   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	Select *Change* to choose a new password for the private key. A password is automatically generated for you, but you can change it.
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. Select *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. From the Certificates page, select *Import* > *Local 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. Select *OK* to import the certificate.

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. Select *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. Select *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. Select *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.

Policy & objects

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

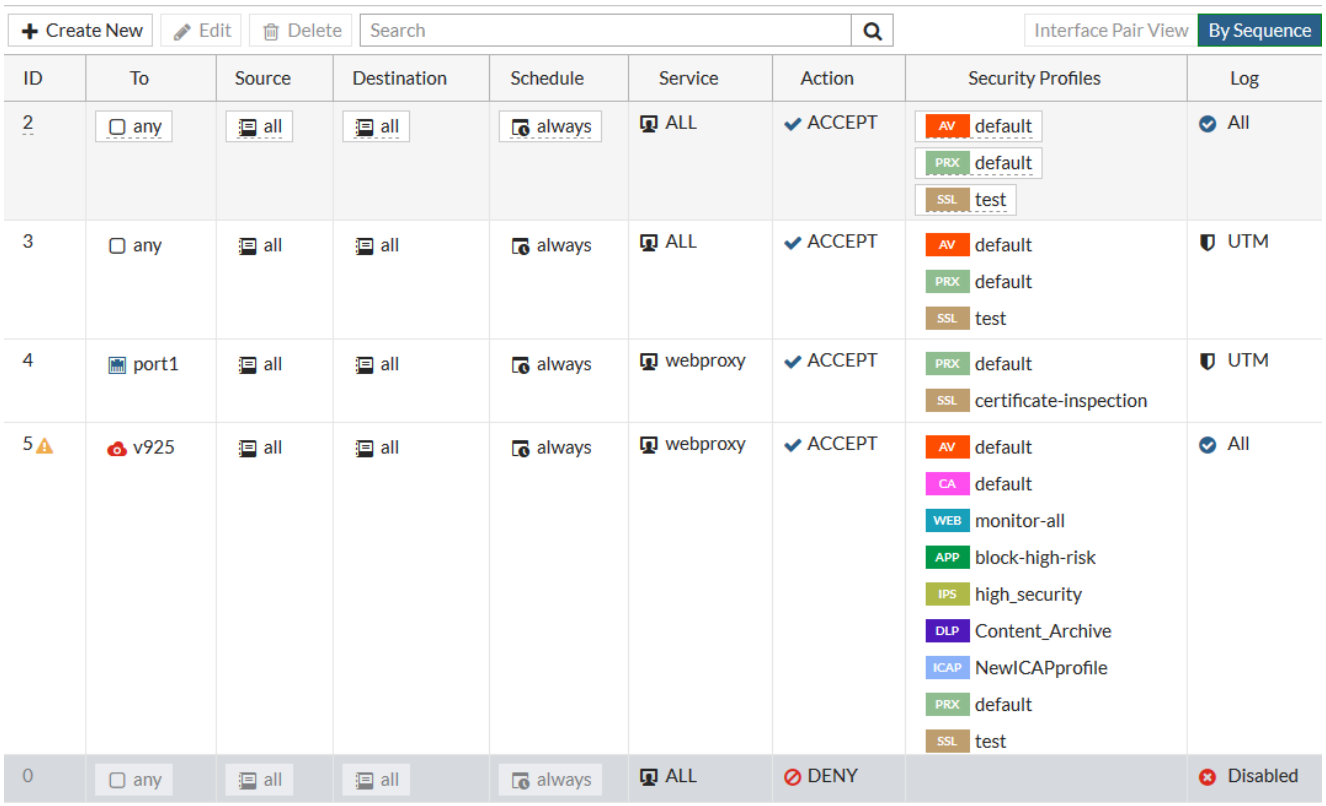
Policy

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*.



Right-click on any column heading to select which columns are displayed 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 136.
Edit	Edit the selected policy. See "Create or edit a policy" on page 136.
Delete	Delete the selected policy.
Search	Enter a search term to search the policy list.

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.
ID	The policy identifier. Policies are numbered in the order they are added to the configuration.
To	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 "Policy" on page 135.
Schedule	The time frame that is applied to the policy. See "Schedules" on page 167.
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 161.
Action	The action to be taken by the policy, such as ACCEPT, DENY, LEARN, or IPsec.
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 187.
Log	The logging level of the policy. Options vary depending on the policy type.
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 189.
Bytes	The number of bytes.
Comments	Comments about the policy (up to 1023 characters).
Content Analysis Profile	The profile used for Content Analysis, if any.

Destination Address	The destination addresses that the policy matches. The destination address can be used as a traffic filter.
DLP	The DLP sensor used by the policy. See "Data leak prevention" on page 215.
Explicit Proxy	The explicit web proxy profile being used, if any.
First Used	When the policy was first used.
From	The incoming interface or interfaces.
Groups	Which groups the policy matches.
Hit Count	Number of results found.
ICAP	The ICAP profile used by the policy. See "ICAP" on page 225.
IPS	Which IPS signatures the policy uses.
Last Used	When the policy was last used.
Proxy Options	The proxy options used by the policy. See "Proxy options" on page 228.
Source Address	The addresses that a policy can receive traffic from. For more information, see "Policy" on page 135.
SSL/SSH Inspection	The SSL/SSH inspection options used by the policy. See "SSL/SSH inspection" on page 232.
Status	Select to enable a policy or clear to disable a policy. A disabled policy is out of service.
Type	The type of policy, such as Explicit Web, Transparent, or SSH Tunnel.
Users	Which users the policy matches.
Web Filter	The web filter profile used by the policy. See "Web filter" on page 191.

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.

To configure which columns are visible and which are hidden, right-click on the header row of the table for a drop-down menu. The drop-down menu is divided into sections. At the top is the Selected Columns section that shows the columns that are currently visible; the next section is the Available Columns section that shows which columns are available to add to the table. To move a column from the Available list to the Selected list, click on the column name. To move a column from the Selected list to the Available list, click on the column name. To

save your changes, go to the bottom of the drop-down menu and select *Apply*. Any additions to the table show up on the right side. Select *Reset All Columns* to return to the default column view. You can also drag column headings to change their order.

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.

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 "Policy" on page 135 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 sequence number 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 sequence number then select *Copy* from the pop-up menu. Right-click in the sequence number cell of the policy 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.

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.

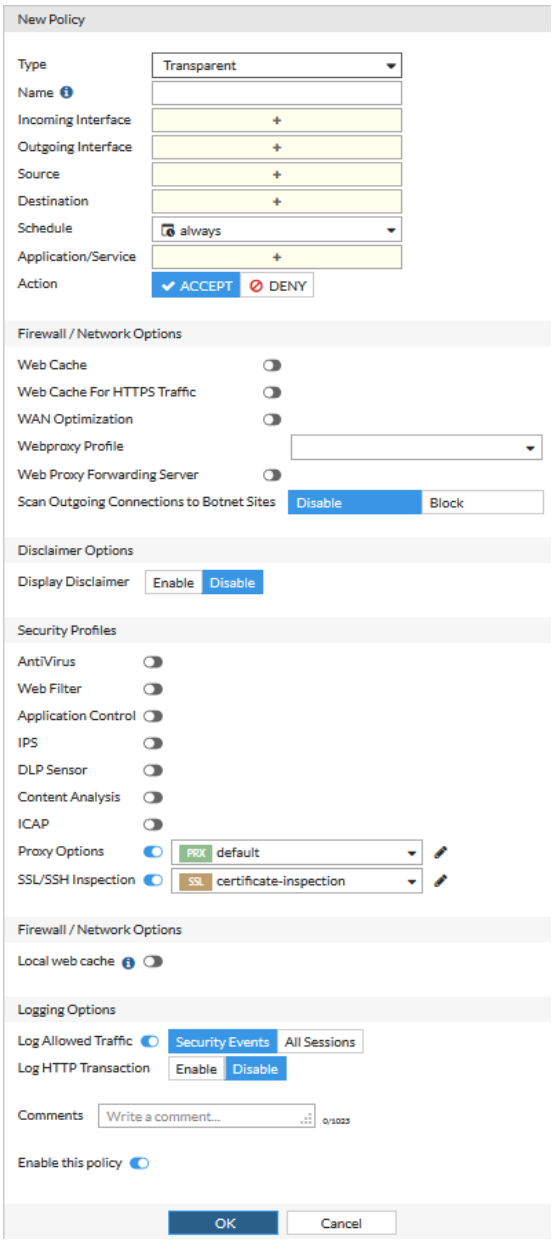
When representing hosts by an IP address range, the range indicates hosts with continuous IP addresses in a subnet, such as `192.168.1.[2-10]`, or `192.168.1.*`, to indicate the complete range of hosts on that subnet. You can also indicate the complete range of hosts on a subnet by entering `192.168.1.[0-255]`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



Policy information can be edited as required in three ways:

- By double-clicking on the sequence number of a policy in the policy list.
- By selecting a policy and then selecting *Edit* from the toolbar
- By right-clicking on the sequence number of the policy and selecting *Edit* from the right-click menu

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

To edit a policy, select the ID number and then select *Edit* (the pencil icon) to open the Edit Policy window.

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

Type	Select the type of policy: *Explicit*, *Transparent*, *FTP*, *SSH Tunnel*, *Wanopt*, or *SSL VPN*. 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 "Explicit proxy" on page 171.
Incoming Interface	If you selected *Transparent* for the policy type, select the field with the "+" next to the field label. Selecting the field will slide out a window 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	Select the field with the "+" next to the field label. Selecting the field will slide out a window 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	Select the field with the "+" next to the field label. 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. The "+" icon next to the Search field is a shortcut for creating a new option based on the tab that is currently selected.
Destination	Select the field with the "+" next to the field label. You can select destination proxy addresses, destination IPv4 addresses, destination IPv6 addresses, and destination Internet services. **NOTE:** You can mix IPv4 and IPv6 addresses.
Schedule	Select a schedule from the drop-down list. Select *Create New* to create a new schedule. For more information, see "Schedules" on page 167.
Application/Service	If you selected *Explicit*, *Transparent*, *SSH Tunnel*, *Wanopt*, or *SSL VPN* for the policy type, select a service or service group that packets must match to trigger this policy. Select *Create New* to create a new service list. See "Services" on page 161. 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 *Web Cache* is enabled.
Web Cache For HTTPS Traffic	Enable or disable web caching for HTTPS traffic.
WAN Optimization	If you selected *Transparent* for the policy type, enable or disable WAN optimization for traffic accepted by the policy. If *WAN Optimization* is enabled, select *Active*, *Passive*, or *Manual*. See "WAN optimization and web caching" on page 316.
Profiles	If you selected *Transparent* for the policy type and enabled *WAN Optimization*, select or create a new profile to use for WAN optimization.
Webproxy Profile	If you selected *Explicit* for the policy type, select a web proxy profile, if one has been configured under *Policy & Objects* > *Web Proxy Profile*. See "Web proxy profile" on page 180.
Web Proxy Forwarding Server	If you selected *Explicit* for the policy type, enable a web proxy forwarding server and then select a server from the drop-down list. See "Forwarding server" on page 174.
Scan Outgoing Connections to Botnet Sites	Select *Disable* or *Block* to protect from botnet and command-and-control traffic.
Force Proxy	If you selected *Transparent* for the policy type, enable or disable whether proxying will be forced.
Display Disclaimer	Select *Enable* to display a disclaimer about Internet content that is not controlled by the network access provider. This option is available only if *Action* is set to *ACCEPT*.
Customize Messages	Enable and then select *Edit Disclaimer Message* if you want to change the content of the disclaimer. This option is available only if *Display Disclaimer* is enabled.
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 new profile from the drop-down list. See "Antivirus" on page 189.
Web Filter	Enable the web filter profile and select or create a new profile from the drop-down list. See "Web filter" on page 191.

Application Control	Enable the Application Control profile and select or create a new profile from the drop-down list.
IPS	Enable the IPS profile and select or create a new profile from the drop-down list.
DLP Sensor	Enable DLP sensors and select or create a new sensor from the drop-down list. See "Data leak prevention" on page 215.
Content Analysis	Enable the Content Analysis profile and select or create a new profile from the drop-down list. See "Content Analysis" on page 222.
ICAP	Enable the ICAP profile and select or create a new profile from the drop-down list. See "ICAP" on page 225.
Proxy Options	Enable the proxy profile and select or create a new profile from the drop-down list. See "Create or edit a proxy option profile" on page 230.
SSL/SSH Inspection	Enable the SSL/SSH inspection profile and select or create a new profile from the drop-down list. See "SSL/SSH inspection" on page 232.
Log Violation Traffic	Enable *Log Violation Traffic* to add violations to the log. This option is available only if *Action* is set to *DENY*.
Log Allowed Traffic	Enable and then select *Security Events* or *All Sessions*. This option is available only if *Action* is set to *ACCEPT*.
Logging Options	This section is available only if *Action* is set to *ACCEPT*.
Log HTTP Transaction	Enable or disable the logging of HTTP transactions.
Comments	Enter a description up to 1,023 characters to describe the policy.
Enable this policy	Enable to use this policy.

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*—for an SSH tunnel.
- *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.

- *SSL VPN*—for an SSL VPN policy. An SSL VPN policy enables clients to authenticate and permits a web-mode connection to the destination network.

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.

Traffic shaping

To control network traffic with traffic shaping, use the following process:

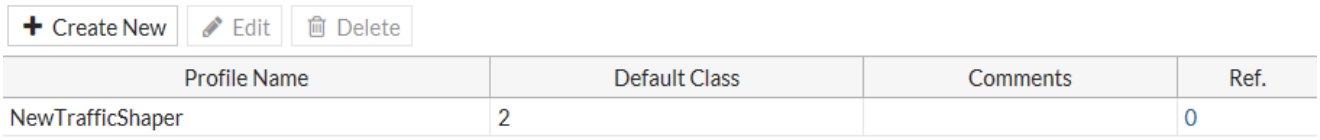
1. Define a traffic shaper to control the maximum and guaranteed throughput.
   See "Traffic shapers" on page 143.

2. Assign the traffic shaper in an interface.
   See "Create or edit an interface" on page 54.You can define separate traffic shapers for incoming and outgoing network traffic.
3. Configure a traffic-shaping policy.
   See "Traffic-shaping policy" on page 146.

Traffic shapers

With a traffic shaper, you can divide the available bandwidth among several classes. Each class specifies how much bandwidth is needed as a percentage of the total bandwidth.

To see a list of available traffic shapers in the GUI, go to *Policies & Objects* > *Traffic Shapers*.



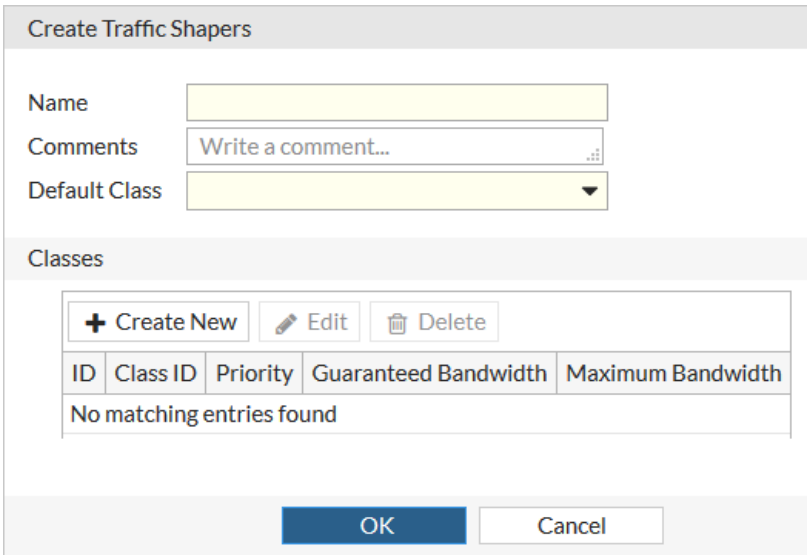
Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Select to open the *Create Traffic Shapers* window. See "Create or edit a traffic shaper" on page 143.
Edit	Edit the selected traffic shaper. See "Create or edit a traffic shaper" on page 143.
Delete	Delete the selected traffic shaper.
Profile Name	The name of the traffic shaper.
Default Class	The class that the traffic shaper will use by default.
Comments	A description of the traffic shaper.
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 traffic shaper

Select *Create New* to open the *Create Traffic Shapers* window. To edit a traffic shaper, select the traffic shaper and then select *Edit*.



Configure the following settings in the *Create Traffic Shapers* window or the *Edit Traffic Shaper* window and then select *OK*:

Name	Enter a name for the new traffic shaper. You cannot change the name after you create the traffic shaper.
Comments	Enter any additional information that might be needed by administrators, as a reminder of the traffic shaper's purpose and scope. This setting is optional.
Default Class	Select the class that the traffic shaper will use by default. The range is 2-31. The default class must be equal to the Class ID for one of the classes in the traffic shaper.
Classes	Classes that can be used in the traffic shaper.
Create New	Select to create a new class. See "Create or edit a class" on page 145.
Edit	Select to modify a class.
Delete	Select to remove a class from the list.
ID	Traffic shaper identifier.
Class ID	Class identifier. The range is 2-31.
Priority	The priority is *top*, *critical*, *high*, *medium*, or *low*.
Guaranteed Bandwidth	The guaranteed bandwidth ensures that a consistent reserved bandwidth is available for a given service or user. Ensure that you set the bandwidth to a value that is significantly less than the bandwidth capacity of the interface. Otherwise, little to no traffic will pass through the interface and potentially cause unwanted latency. Enter the percentage, from 0 to 100.

Maximum Bandwidth	The maximum bandwidth instructs the security policy what the largest percentage of traffic allowed. Enter the percentage, from 1 to 100. The *Maximum Bandwidth* must be equal or greater than the *Guaranteed Bandwidth*.

To create a new traffic shaper and class in the CLI:

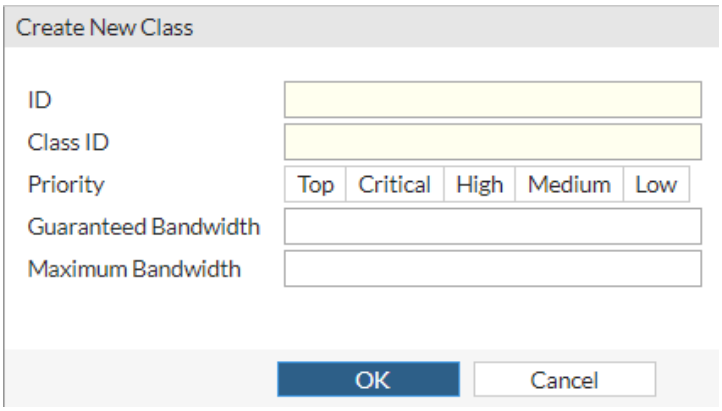
```
config firewall shaping-profile
   edit <traffic_shaper_name>
      config classes
         edit <ID_value>
            set class-id <2-31>
            set priority <top | critical | high | medium | low}
            set guaranteed-bandwidth <0-100 percent>
            set maximum-bandwidth <1-100 percent>
         end
         set default-class <2-31, must be equal to class-id value>
      end
```

For example:

```
config firewall shaping-profile
   edit TrafficShaper1
      config classes
         edit 1
            set class-id 3
            set priority low
            set guaranteed-bandwidth 50
            set maximum-bandwidth 75
         end
         set default-class 3
      end
```

Create or edit a class

From the *Create Traffic Shapers* window or the *Edit Traffic Shapers* window, you can create or edit a class. Select *Create New* to open the *Create New Class* window. To change a class, select the class and then select *Edit*.



Configure the following settings in the *Create New Class* window or the *Edit Class* window and then select *OK*:

ID	Enter the traffic shaper identifier.
Class ID	Enter the class identifier. The range is 2-31.
Priority	Select the priority: *Top*, *Critical*, *High*, *Medium*, or *Low*.
Guaranteed Bandwidth	Enter the percentage, from 0 to 100.
Maximum Bandwidth	Enter the percentage, from 1 to 100. The *Maximum Bandwidth* must be equal or greater than the *Guaranteed Bandwidth*.

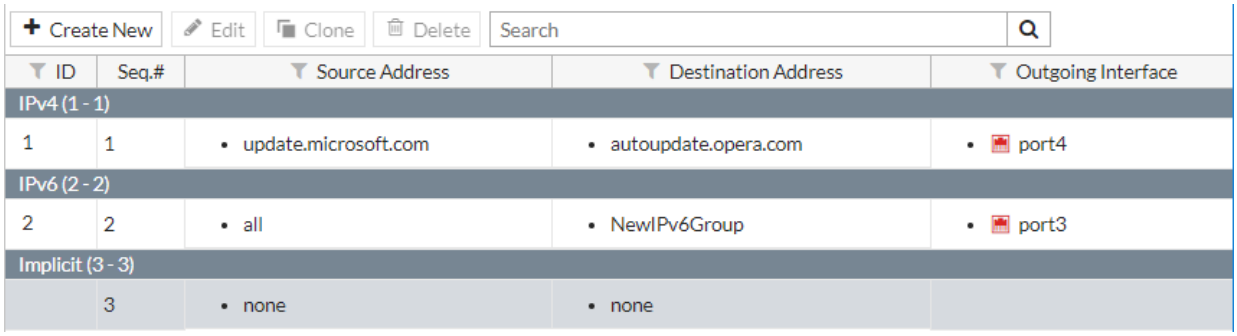
Traffic-shaping policy

A traffic-shaping policy is defined by the following:

- Matching criteria for IPv4 or IPv4 network traffic
- Class ID of a traffic shaper
- Reverse class ID of a traffic shaper

The matching criteria can be any combination of source address, destination addresses, services, and outgoing interfaces. Whenever an outgoing packet matches the criteria in the traffic-shaping policy, the packet is assigned the class ID of the traffic shaper defined in the traffic-shaping policy. Whenever an incoming packet matches the criteria in the traffic shaper, the packet is assigned the reverse class ID of the traffic shaper defined in the traffic-shaping policy. If the incoming or outgoing packet does not match the criteria in any traffic-shaping policy, the packet is assigned the default class ID.

To see the available traffic-shaping policies in the GUI, go to *Policies & Objects* > *Traffic Shaping Policy*.



Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

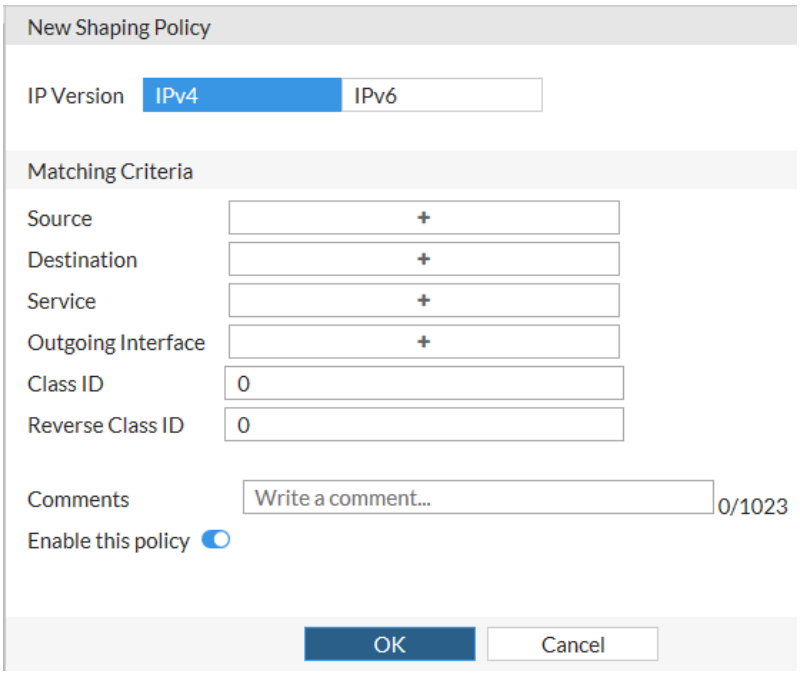
The following options are available:

Create New	Select to open the *New Shaping Policy* window. See "Create or edit a traffic-shaping policy" on page 147.
Edit	Select to edit the selected policy. See "Create or edit a traffic-shaping policy" on page 147.

Clone	Select to copy the selected policy.
Delete	Select to delete the selected policy.
Search	Enter a search term to search the policy list.
ID	The class ID of a traffic shaper.
Seq.#	The policy sequence number.
Source Address	The source address, address group, user, or user group that the policy matches.
Destination Address	The destination address or address group that the policy matches.
Outgoing Interface	Ports, VLANs, *wanopt*, *web-proxy*, or *any*.
Application	The applications allowed by the policy.
Application Category	The application groupings allowed by the policy.
Groups	Groups allowed by the policy.
Service	Services allowed by the policy.
URL Category	URL categories allowed by the policy.
Users	Users allowed by the policy.

Create or edit a traffic-shaping policy

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



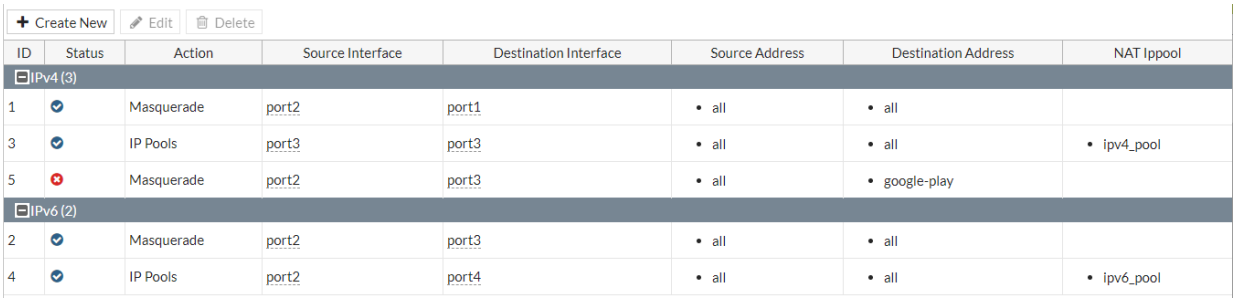
Configure the following settings in the *New Shaping Policy* window or the *Edit Shaping Policy* window and then select *OK*:

IP Version	Select *IPv4* or *IPv6*.
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	Select one or more services that the 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.
Reverse Class ID	The class ID of a traffic shaper for incoming packets.
Comments	Enter any additional information that might be needed by administrators, as a reminder of the policy's purpose and scope. This setting is optional.
Enable this policy	Policies are enabled by default, but, if you want to disable a traffic-shaping policy, disable it here.

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. SNAT is only available when the FortiProxy unit is operating in transparent mode.



+ Create New | Edit | Delete

ID	Status	Action	Source Interface	Destination Interface	Source Address	Destination Address	NAT Ippool
IPv4 (3)							
1	✓	Masquerade	port2	port1	• all	• all	
3	✓	IP Pools	port3	port3	• all	• all	• ipv4_pool
5	✗	Masquerade	port2	port3	• all	• google-play	
IPv6 (2)							
2	✓	Masquerade	port2	port3	• all	• all	
4	✓	IP Pools	port2	port4	• all	• all	• ipv6_pool

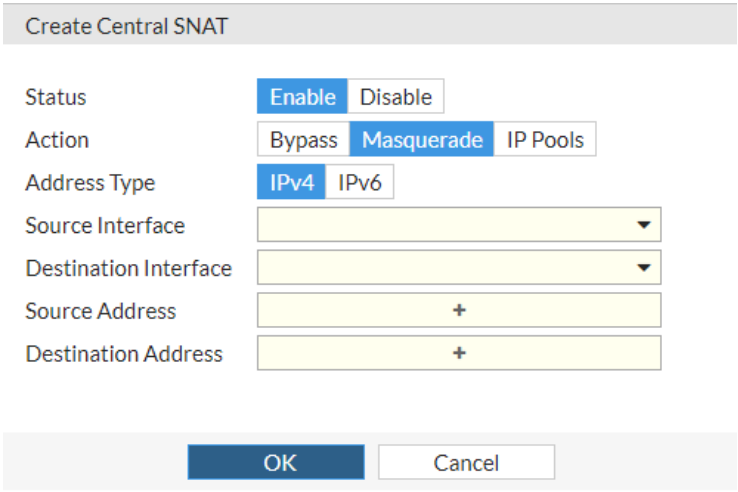
Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

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 150.
Edit	Edit the selected central SNAT policy. See "Create or edit a central SNAT policy" on page 150.
Delete	Delete the selected central SNAT policy.
ID	SNAT identifier.
Status	The status is either *enable* (active) or *disable* (inactive).
Action	The central SNAT action is *Bypass*, *Masquerade*, or *IP Pools*.
Source Interface	The source interface name is either a port or *any*.
Destination Interface	The destination interface name.
Source Address/Source IPv6 Address	The source addresses and address groups.
Destination Address/Destination IPv6 Address	The destination addresses and address groups.
NAT Ippool/IPv6 NAT Ippool	The name of the NAT IP pool.

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 select *Edit*.



Configure the following settings in the *Create Central SNAT* window or the *Edit Central SNAT* window and then select *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.
Address 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**	Select the "+" in the field. A window slides out to 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 154.
Destination Address **Destination IPv6 Address**	Select the "+" in the field. A window slides out to 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 154.

To create a new 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
```

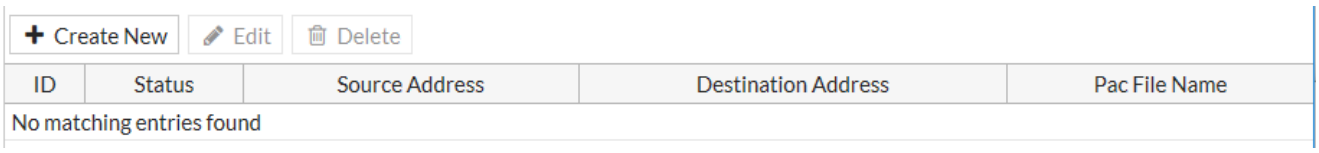
For example, to create an IPv6 central SNAT policy:

```
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*.



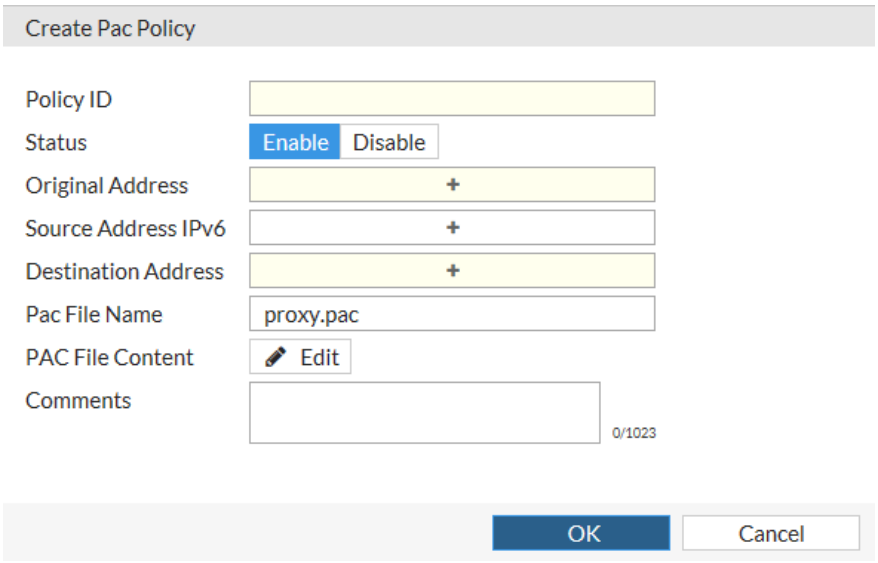
Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Select to open the *Create Pac Policy* window. See "Create or edit a PAC policy" on page 152.
Edit	Edit the selected PAC policy. See "Create or edit a PAC policy" on page 152.
Delete	Delete the selected PAC policy.
ID	The PAC policy identifier.
Status	The status is enabled or disabled.
Source 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.

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 select *Edit*.



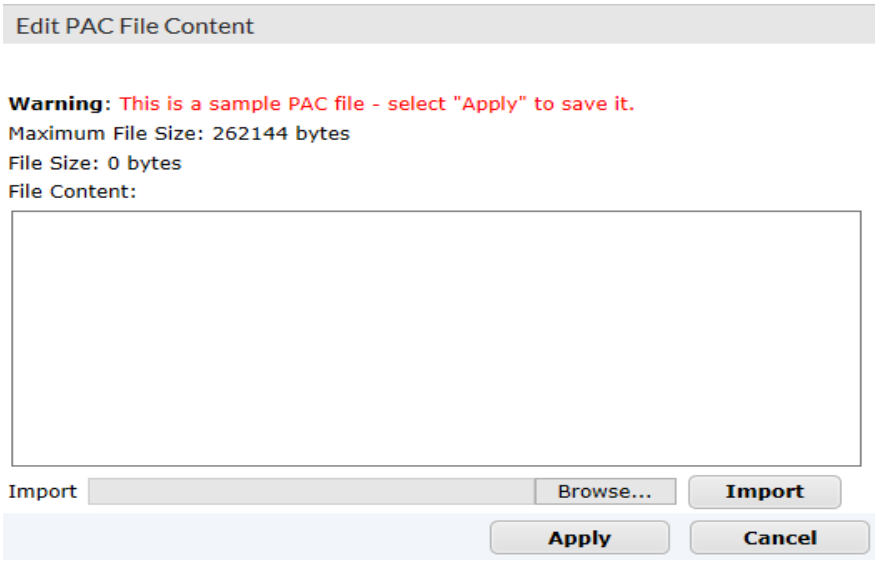
Configure the following settings in the *Create Pac Policy* window or the *Edit Pac Policy* window and then select *OK*:

Policy ID	Enter the PAC policy identifier.

Status	Enable the status to make the policy active.
Source 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.
PAC File Content	Select *Edit* to create or import a PAC file. See "Edit a PAC file" on page 153.
Comments	Enter an optional description of the PAC policy.

Edit a PAC file

In the Create Pac Policy window or Edit Pac Policy window, select *Edit* to open the *Edit Pac File Content* window.

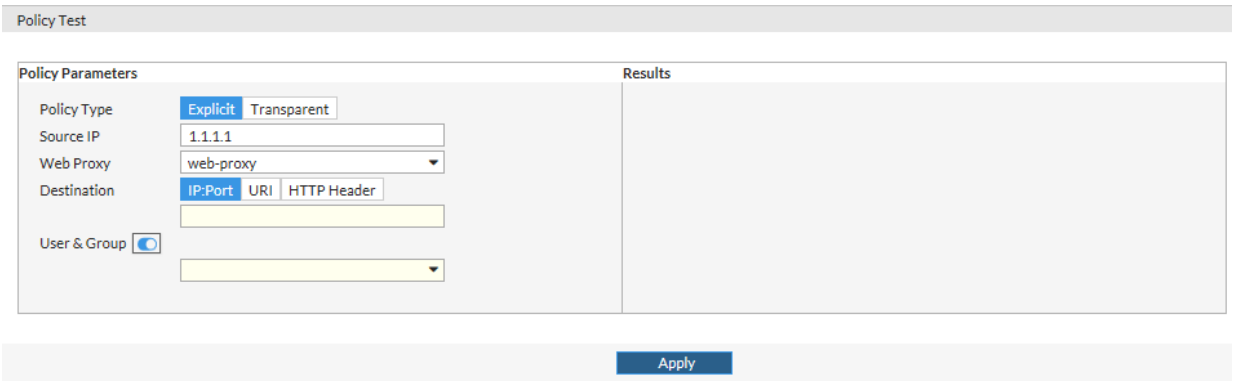


To add content to a PAC file:

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. Select *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 "Web proxy profile" on page 180.
Source IP	If you selected Transparent, enter the source IP address.
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. Select *Apply*.
   The results show the policy configuration if a policy matches the parameters.

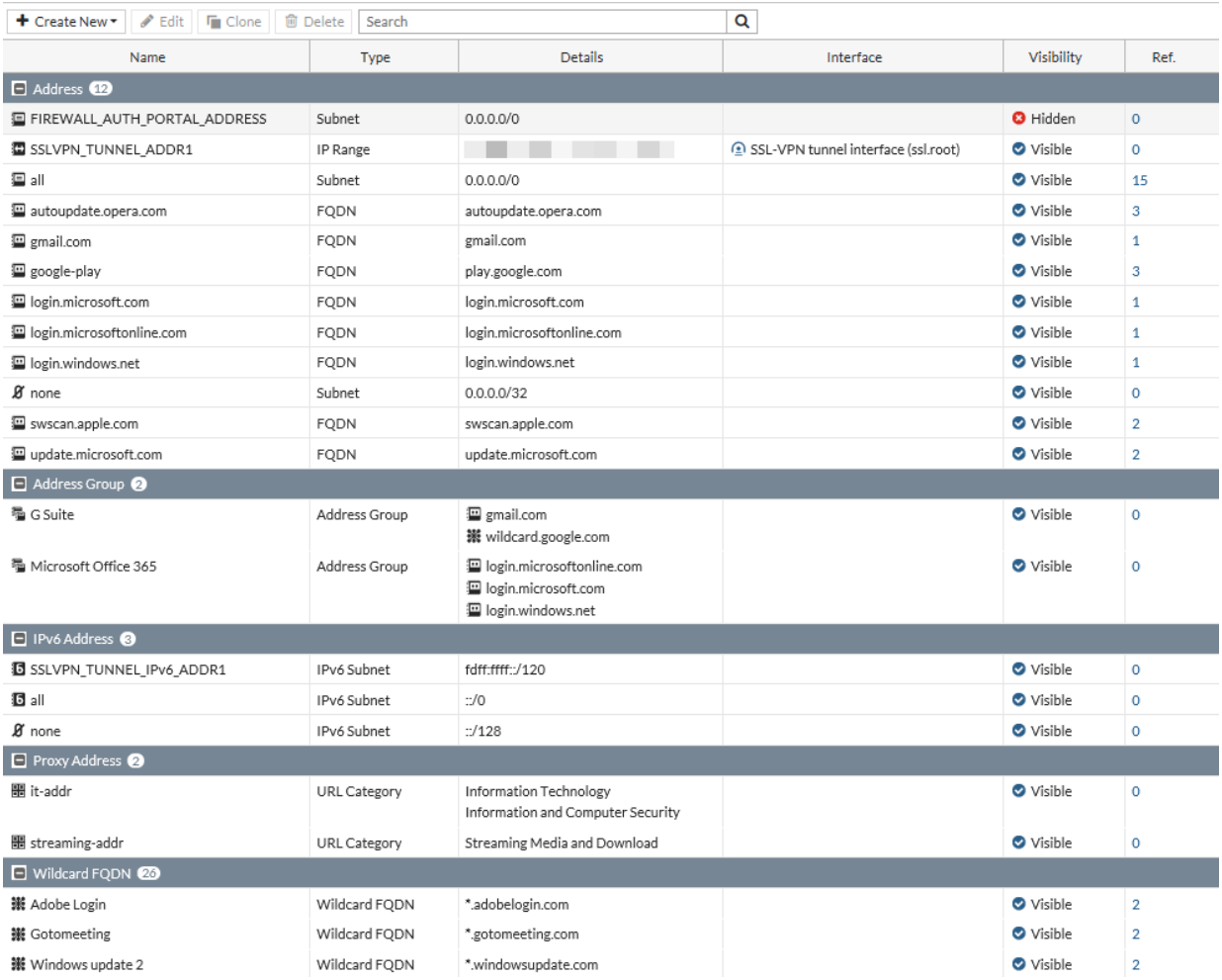
Addresses

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*.



Name	Type	Details	Interface	Visibility	Ref.
Address 12					
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0		Hidden	0
SSLVPN_TUNNEL_ADDR1	IP Range		SSL-VPN tunnel interface (ssl.root)	Visible	0
all	Subnet	0.0.0.0/0		Visible	15
autoupdate.opera.com	FQDN	autoupdate.opera.com		Visible	3
gmail.com	FQDN	gmail.com		Visible	1
google-play	FQDN	play.google.com		Visible	3
login.microsoft.com	FQDN	login.microsoft.com		Visible	1
login.microsoftonline.com	FQDN	login.microsoftonline.com		Visible	1
login.windows.net	FQDN	login.windows.net		Visible	1
none	Subnet	0.0.0.0/32		Visible	0
swscan.apple.com	FQDN	swscan.apple.com		Visible	2
update.microsoft.com	FQDN	update.microsoft.com		Visible	2
Address Group 2					
G Suite	Address Group	gmail.com wildcard.google.com		Visible	0
Microsoft Office 365	Address Group	login.microsoftonline.com login.microsoft.com login.windows.net		Visible	0
IPv6 Address 3					
SSLVPN_TUNNEL_IPv6_ADDR1	IPv6 Subnet	fdff:ffff::/120		Visible	0
all	IPv6 Subnet	::/0		Visible	0
none	IPv6 Subnet	::/128		Visible	0
Proxy Address 2					
it-addr	URL Category	Information Technology Information and Computer Security		Visible	0
streaming-addr	URL Category	Streaming Media and Download		Visible	0
Wildcard FQDN 26					
Adobe Login	Wildcard FQDN	*.adobelogin.com		Visible	2
Gotomeeting	Wildcard FQDN	*.gotomeeting.com		Visible	2
Windows update 2	Wildcard FQDN	*.windowsupdate.com		Visible	2

Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

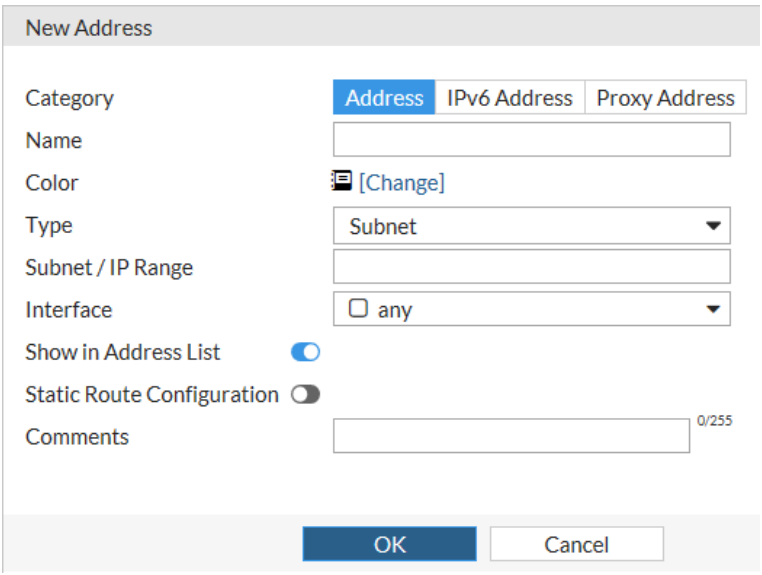
The following options are available:

Create New > Address	Add a new address. See "Create or edit an address" on page 156.

Create New > Address Group	Add a new address group. See "Create or edit an address group" on page 159.
Edit	Edit the selected address. See "Create or edit an address" on page 156.
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.
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)*.
Details	The domain name.
Interface	The interface to which the address is bound.
Visibility	If this setting is enabled, the address will appear in drop-down menus where it is an option.
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.
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 select *Edit*.

Configure the following settings in the *New Address* window or the *Edit Address* window and then select *OK*:

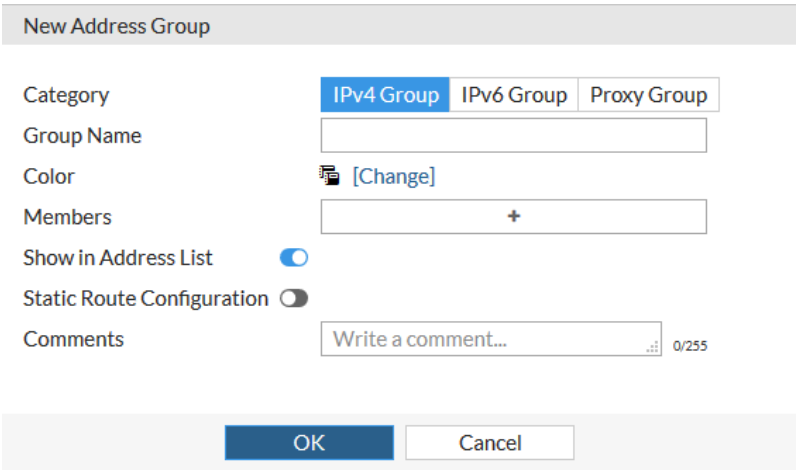
Category	Select *Address*, *IPv6 Address*, or *Proxy Address*.
Name	Enter a name for the IPv4 address, IPv6 address, or proxy address. Addresses must have unique names.
Color	Select *Change* to choose a color for the icon.
Type	If you selected *Address* for the category, select one of the following: *FQDN*, *FQDN Group*, *Geography*, *IP Range*, *Subnet*, *Wildcard FQDN*, *Dynamic SDN address*. If you selected *IPv6 Address* for the category, select *Subnet* or *IP Range*. If you selected *Proxy Address* for the category, select *URL Pattern*, *Host Regex Match*, *URL Category*, *HTTP Method*, *User Agent*, *HTTP Header*, *Advanced (Source)*, or *Advanced (Destination)*.
FQDN	If you selected *FQDN* as the IPv4 address type, enter the fully qualified domain name.
FQDN Group	If you selected *FQDN Group* as the IPv4 address type, enter the FQDN group.
Pattern Start	If you selected *FQDN Group* as the IPv4 address type, enter the beginning of the pattern to match.
Pattern End	If you selected *FQDN Group* as the IPv4 address type, enter the end of the pattern to match.

Cache TTL (seconds)	If you selected *FQDN Group* as the IPv4 address type, enter how many seconds to keep data in the cache.
Country/Region	If you selected *Geography* as the IPv4 address type, select the country or region.
Subnet/IP Range	If you selected *IP Range* or *Subnet* as the IPv4 address type or you selected *IP Range* as the IPv6 address type, enter the IP address, followed by a forward slash (/), and then the subnet mask or enter an IP address range separated by a hyphen. See Web cache policy address formats.
Wildcard FQDN	If you selected *Wildcard FQDN* as the IPv4 address type, enter the FQDN. You can use "?", "*", and "?*" in wildcard FQDN addresses. There are a number of companies that use secondary and even tertiary domain names or FQDNs for their websites. Wildcard FQDN addresses are to ease the administrative overhead in cases where this occurs. Sometimes it is as simple as sites that still use www. as a prefix for their domain name. If you do not know whether or not the www is being used it is simpler to use a wildcard and include all of the possibilities whether it be example.com, www.example.com or even ftp.example.com. Wildcard FQDN addresses do not resolve to a specific set of IP addresses in the same way that a normal FQDN address does. They are intended for use in SSL exemptions and should not be used as source or destination addresses in policies.
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.
IPv6 Address	If you selected *Subnet* as the IPv6 address type, enter the IPv6 address.
Host	If you selected *URL Pattern*, *URL Category*, *HTTP Method*, *User Agent*, *HTTP Header*, *Advanced (Source)*, or *Advanced (Destination)* as the proxy address type, select the host name.
URL Path Regex	If you selected *URL Pattern* or *Advanced (Destination)* as the proxy address type, enter the appropriate string.
Host Regex Pattern	If you selected *Host Regex Match* 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.
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.
Header Group	If you selected Advanced (Source) as the proxy address type, select a header group or create a new header group.
Show in Address List	If the setting is enabled, the address appears in drop-down menus where it is an option.
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* or *Subnet*.
Comments	Optionally, enter a description of the address.

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 select *Edit*.

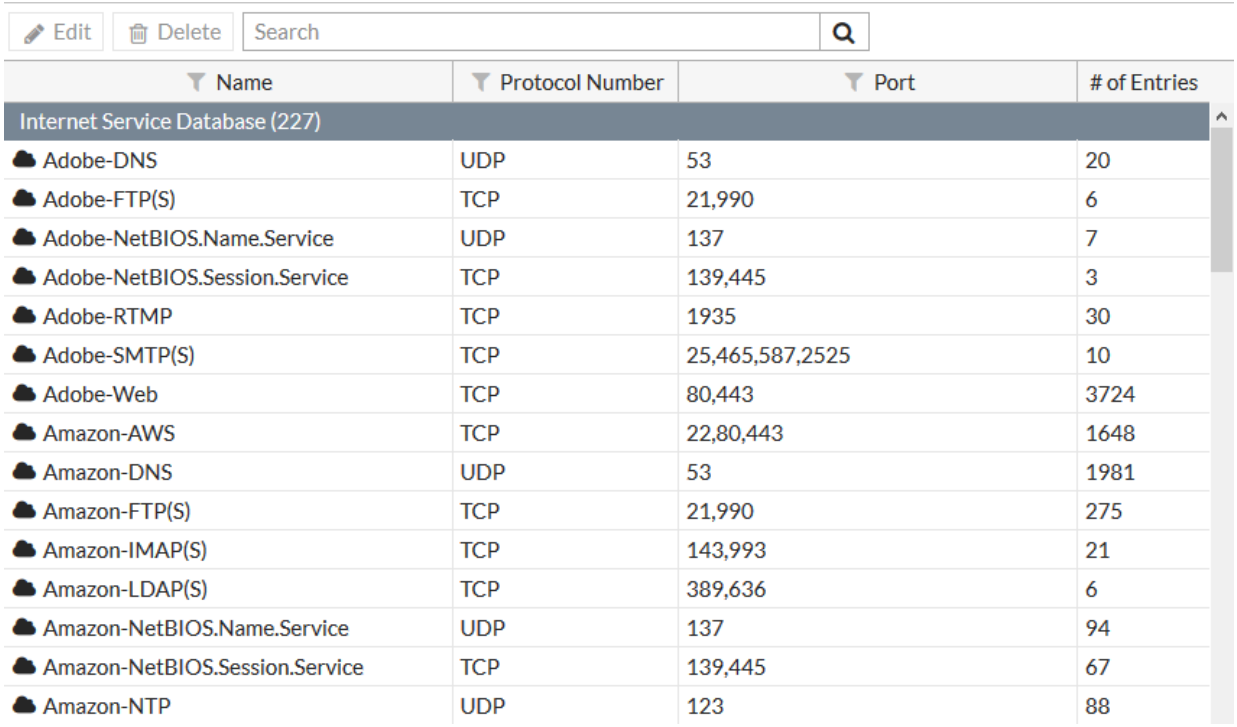
Configure the following settings in the *New Address Group* window or the *Edit Address Group* window and then select *OK*:

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	Select *Source Group* or *Destination Group*. This option is available only if *Category* is *Proxy Group*.
Members	Select the addresses to add to the address group.
Show in Address List	Select to show the address group in the address list.
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.

Internet service database

To view the Fortinet database of cloud-based applications, go to *Policy & Objects* > *Internet Service Database*.



Name	Protocol Number	Port	# of Entries
Internet Service Database (227)			
Adobe-DNS	UDP	53	20
Adobe-FTP(S)	TCP	21,990	6
Adobe-NetBIOS.Name.Service	UDP	137	7
Adobe-NetBIOS.Session.Service	TCP	139,445	3
Adobe-RTMP	TCP	1935	30
Adobe-SMTP(S)	TCP	25,465,587,2525	10
Adobe-Web	TCP	80,443	3724
Amazon-AWS	TCP	22,80,443	1648
Amazon-DNS	UDP	53	1981
Amazon-FTP(S)	TCP	21,990	275
Amazon-IMAP(S)	TCP	143,993	21
Amazon-LDAP(S)	TCP	389,636	6
Amazon-NetBIOS.Name.Service	UDP	137	94
Amazon-NetBIOS.Session.Service	TCP	139,445	67
Amazon-NTP	UDP	123	88

Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

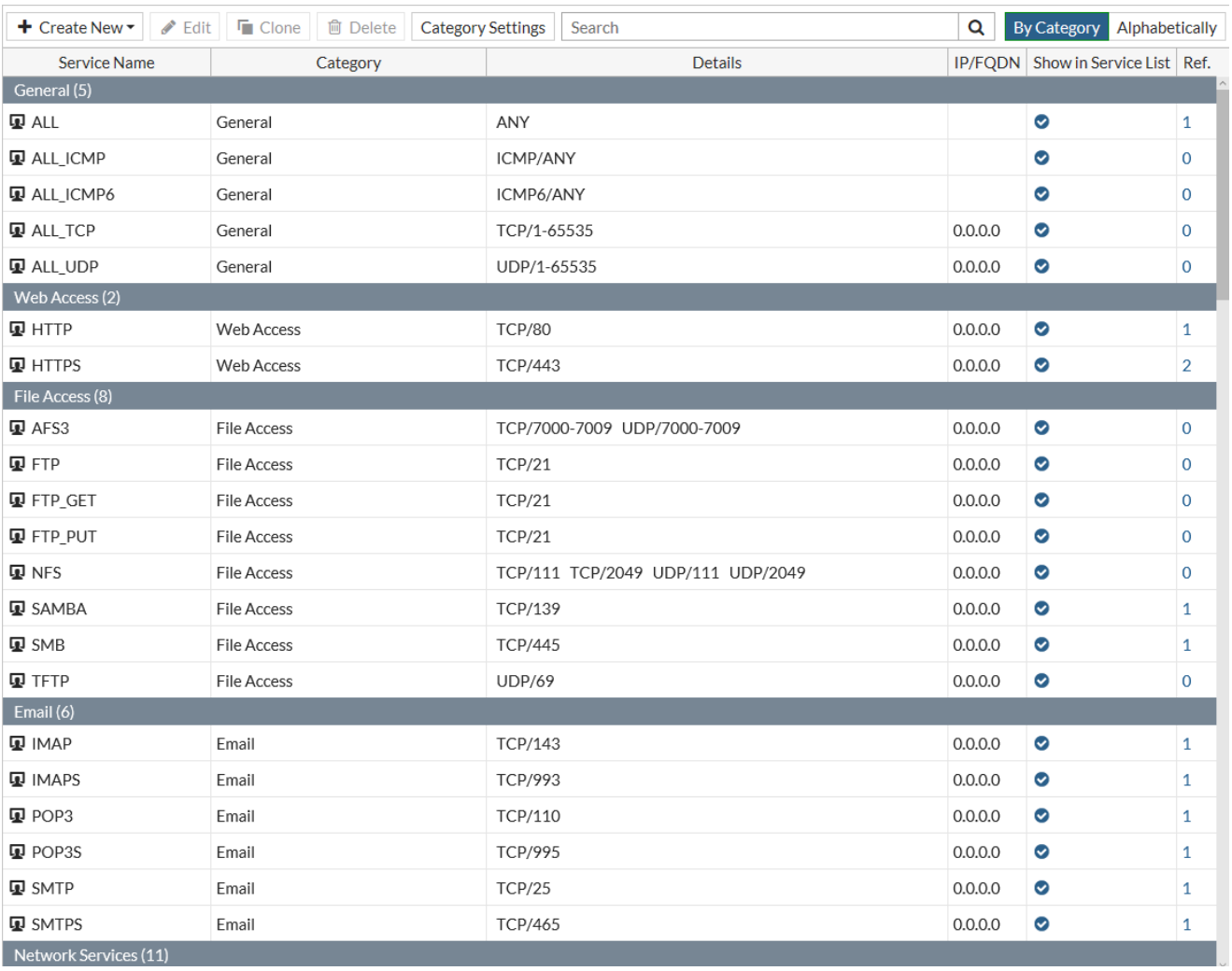
The following options are available:

Edit	Select if you want to enable or disable a database entry.
Delete	Remove a database entry from the list. Most database entries cannot be deleted.
Search	Enter a search term to search the database.
Name	The name of the cloud-based application.
Protocol Number	Which protocols are used.
Port	Which port has been assigned.
# of Entries	The number of entries in the database.

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	Category	Details	IP/FQDN	Show in Service List	Ref.
General (5)					
ALL	General	ANY		✓	1
ALL_ICMP	General	ICMP/ANY		✓	0
ALL_ICMP6	General	ICMP6/ANY		✓	0
ALL_TCP	General	TCP/1-65535	0.0.0.0	✓	0
ALL_UDP	General	UDP/1-65535	0.0.0.0	✓	0
Web Access (2)					
HTTP	Web Access	TCP/80	0.0.0.0	✓	1
HTTPS	Web Access	TCP/443	0.0.0.0	✓	2
File Access (8)					
AFS3	File Access	TCP/7000-7009 UDP/7000-7009	0.0.0.0	✓	0
FTP	File Access	TCP/21	0.0.0.0	✓	0
FTP_GET	File Access	TCP/21	0.0.0.0	✓	0
FTP_PUT	File Access	TCP/21	0.0.0.0	✓	0
NFS	File Access	TCP/111 TCP/2049 UDP/111 UDP/2049	0.0.0.0	✓	0
SAMBA	File Access	TCP/139	0.0.0.0	✓	1
SMB	File Access	TCP/445	0.0.0.0	✓	1
TFTP	File Access	UDP/69	0.0.0.0	✓	0
Email (6)					
IMAP	Email	TCP/143	0.0.0.0	✓	1
IMAPS	Email	TCP/993	0.0.0.0	✓	1
POP3	Email	TCP/110	0.0.0.0	✓	1
POP3S	Email	TCP/995	0.0.0.0	✓	1
SMTP	Email	TCP/25	0.0.0.0	✓	1
SMTPS	Email	TCP/465	0.0.0.0	✓	1
Network Services (11)					

Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

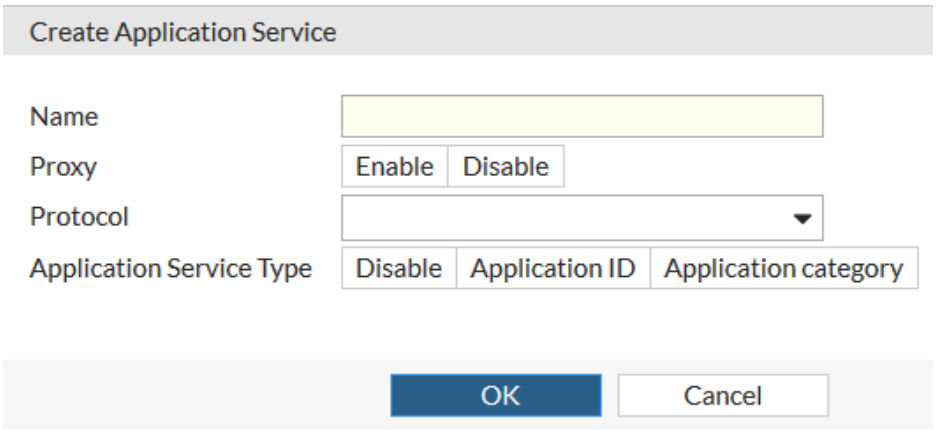
The following options are available:

Create New	Create a new application service, service, service group, or category. See "Create or edit an application service" on page 163, "Create or edit a service" on page 164, "Create or edit a service group" on page 166, and "Create a service category" on page 167.
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.
By Category/Alphabetically	View the list organized by categories or organized alphabetically.
Service Name	The name of the custom service.
Category	Categories include *General*; *Application*; *Web Access*; *File Access*; *Email*; *Network Services*; *Authentication*; *Remote Access*; *Tunneling*; *VoIP*, *Messaging & Other Applications*; *Web Proxy*; *Firewall Group*; and *Uncategorized*.
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.



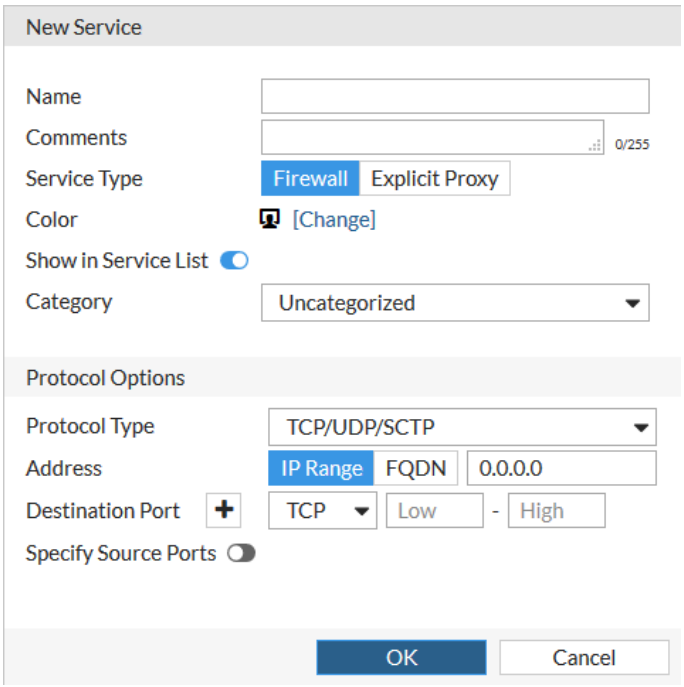
To open the *Edit Application Service* window, select an application service and then select *Edit*.

Configure the following settings in the *Create Application Service* window or *Edit Application Service* window and then select *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 an *Application Service Type* of *Application ID*, select + 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*, select + to open the *Select Entries* window. Select one or more entries and then select *Close*.
TCP PortRange	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 select *Edit*.

Configure the following settings in the *New Service* window or *Edit Service* window and then select *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	Select 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 167.
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. This option is only available if *Protocol Type* is set to *TCP/UDP/SCTP*.
Destination Port	Select *TCP*, *UDP*, or *SCTP* and then enter a range of port numbers. This option is only available if *Protocol Type* is set to *TCP/UDP/SCTP*.
Specify Source Ports	Enable and then enter a range of port numbers. This option is only available if *Protocol Type* is set to *TCP/UDP/SCTP*.
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*.

Create or edit a service group

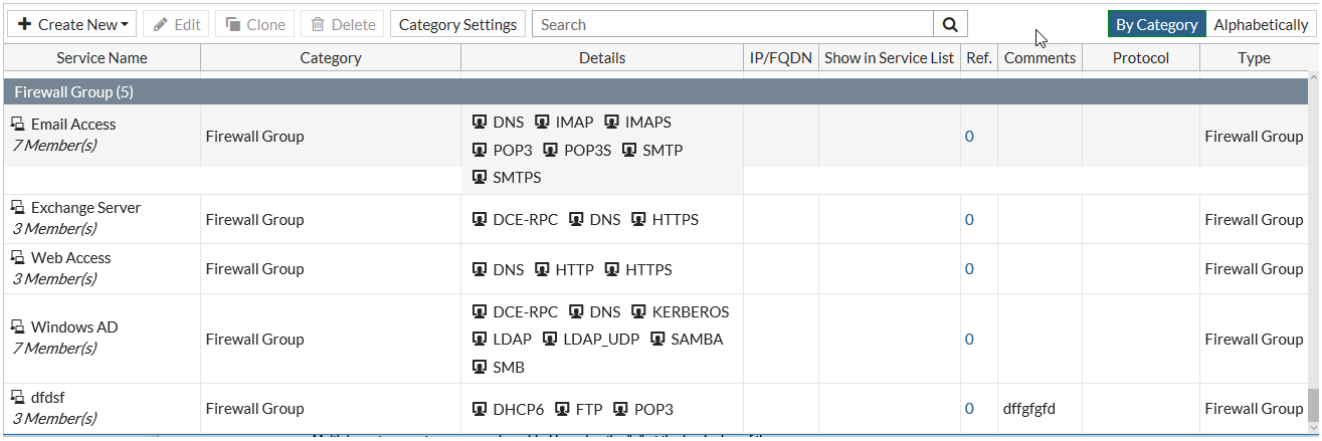
You can organize multiple services into a service group to simplify your policy list. For example, instead of having five identical policies for five different but related services, you can combine the five services into a single service group that is used by a single policy.

Service groups cannot contain other service groups.

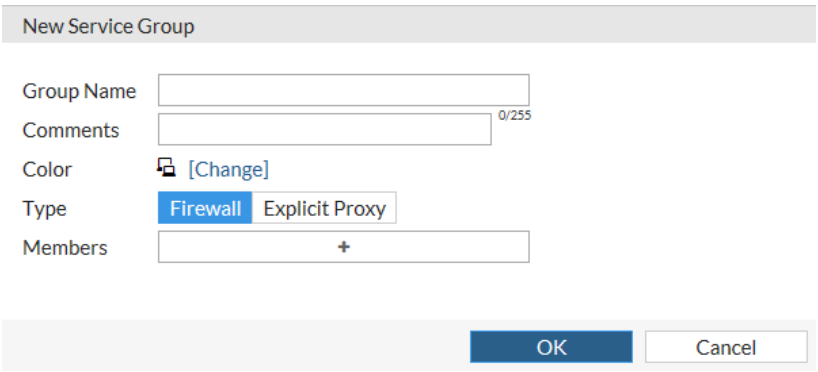
Configure a service group using the following CLI commands:

```
config firewall service group
   edit <name>
      set member              --Address group member.
      set explicit-proxy      --Enable/disable explicit web proxy service group.
      set comment             --Comment.
      set color               --GUI icon color.
   next
end
```

Service groups are listed in the Firewall Groups 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 select *Edit*.

Configure the following settings in the *New Service Group* window or the *Edit Service Group* window and then select *OK*:

Group 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.

Create a service category

1. From *Policy & Objects* > *Services*, select *Create New* > *Category*.
   The *New Service Category* window opens.
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. Select *OK* to create the new service category.

Schedules

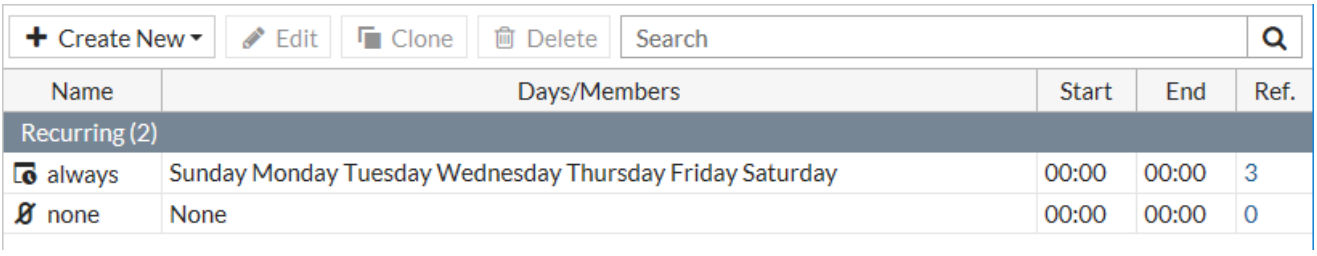
When you add security policies on a FortiProxy unit, those policies are always on, policing the traffic through the device. Schedules control when policies are in effect.

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*.



Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

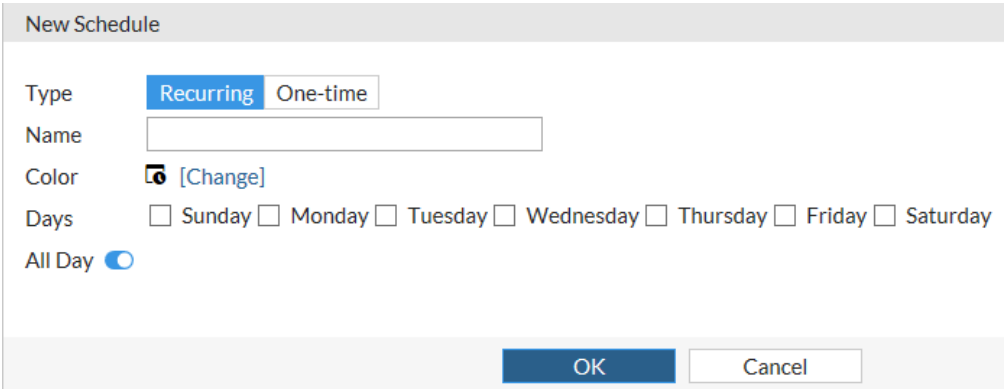
The following options are available:

Create New	Create a schedule or a schedule group. See "Create or edit a schedule" on page 168 or Create or edit a schedule group on page 169.
Edit	Edit the selected schedule or schedule group. See "Create or edit a schedule" on page 168 or Create or edit a schedule group on page 169.
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 select *Edit*.

Configure the following settings in the *New Schedule* window or the *Edit Schedule* window and then select *OK*:

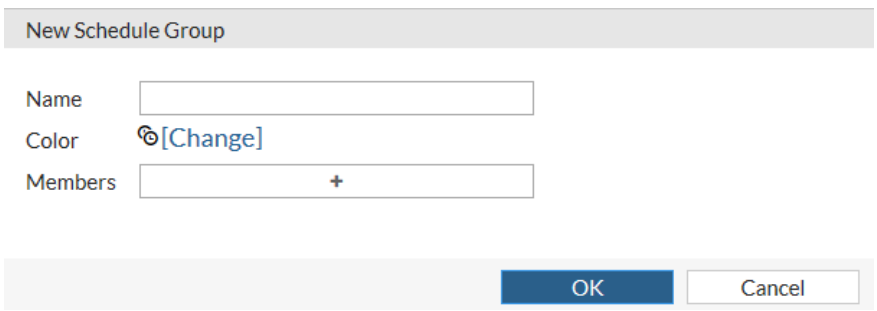
Type	Select *Recurring* or *One-time*.
Name	Enter the name of the schedule.
Color	Select *Change* to choose a color for the icon.
Days	If you selected a recurring schedule, select the days of the week when the schedule will be active.
All Day	If you selected a recurring schedule and the scheduled time 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.

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 select *Edit*.

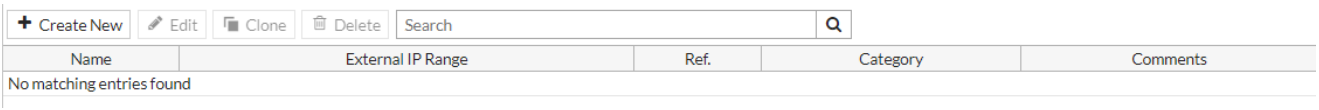
Configure the following settings in the *New Schedule Group* window or the *Edit Schedule Group* window and then select *OK*:

Name	Enter the name of the schedule group.
Color	Select *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.

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*.



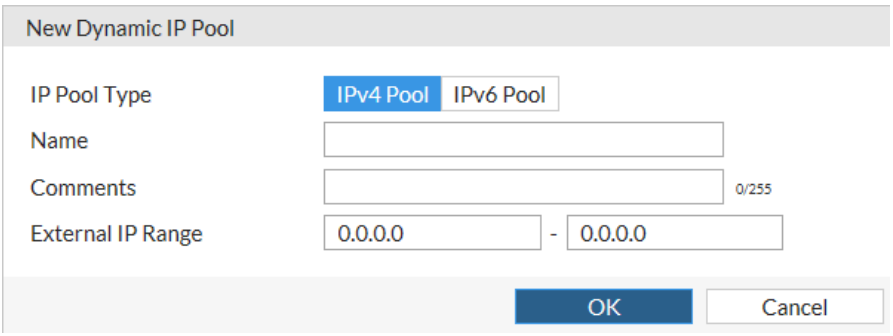
Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a new IP pool. See "Create or edit an IP pool" on page 171.
Edit	Edit the selected IP pool. See "Create or edit an IP pool" on page 171.
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
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.
Category	The type of IP pool, either *IPv4 Pool* or *IPv6 Pool*.
Comments	An optional description of the IP pool.

Create or edit an IP pool

Select *Create New* to open the *New Dynamic IP Pool* window.



To open the *Edit Dynamic IP Pool* window, select an IP pool and then select *Edit*.

Configure the following settings in the *New Dynamic IP Pool* window or *Edit Dynamic IP Pool* window and then select *OK*:

To create a new IP pool:

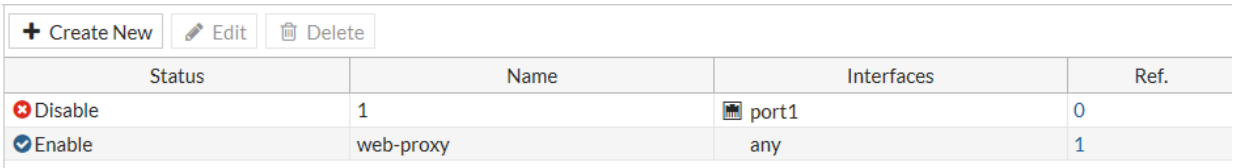
IP Pool Type	Select *IPv4 Pool* if your IP pool contains IPv4 addresses or select *IPv6 Pool* if your IP pool contains IPv6 addresses.
Name	Enter a name for the IP pool in the *Name* field.
Comments	Add an optional description of the IP pool.
External IP Range	Enter the lowest and highest IP addresses in the range. If you only want a single address used, enter the same address in both fields.

Explicit proxy

Use the explicit web proxy 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, go to *Policy & Objects* > *Explicit Proxy*.



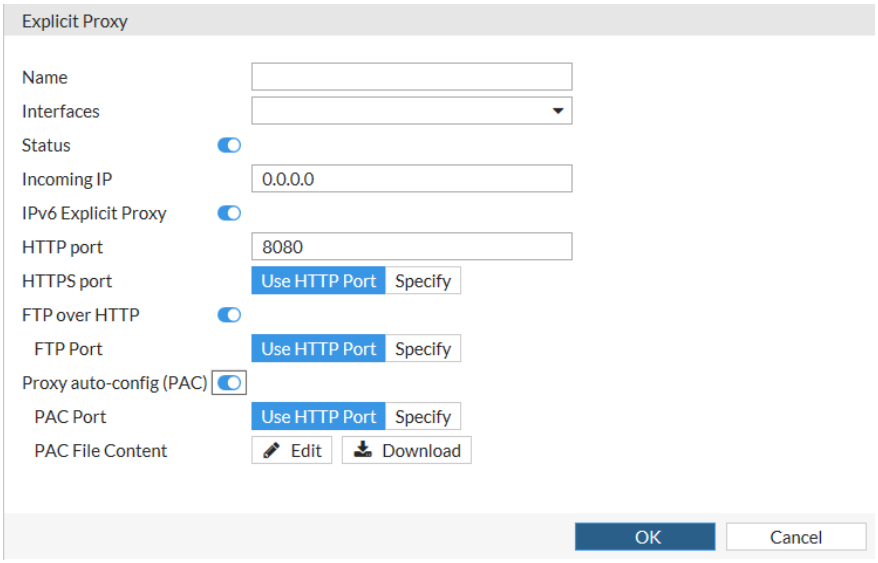
Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a new explicit web proxy. See "Create or edit an explicit web proxy" on page 172.
Edit	Modify settings to an explicit web proxy. See "Create or edit an explicit web proxy" on page 172.
Delete	Remove a proxy from the list.
Status	The status of the explicit web proxy.
Name	The name of the explicit web proxy.
Interfaces	The interface to which the proxy applies.

Create or edit an explicit web proxy

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



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

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

Name	Enter the name of the explicit web proxy.
Interfaces	Select the interface that are being monitored by the explicit web proxy from the drop-down list.
IPv6 Explicit Proxy	Toggle to turn on the explicit web proxy for IPv6 traffic.

HTTP port	Enter the HTTP 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 (default = 8080).
HTTPS port	Select *Use HTTP Port* or select *Specify* and then enter the HTTPS 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.
FTP over HTTP	Toggle to enable FTP over HTTP for the explicit web proxy.
FTP Port	Select *Use HTTP Port* or select *Specify* and then enter the FTP port number that traffic from client web browsers use to connect to the explicit proxy for the specific protocol.
Proxy auto-config (PAC)	Toggle 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 PAC 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.

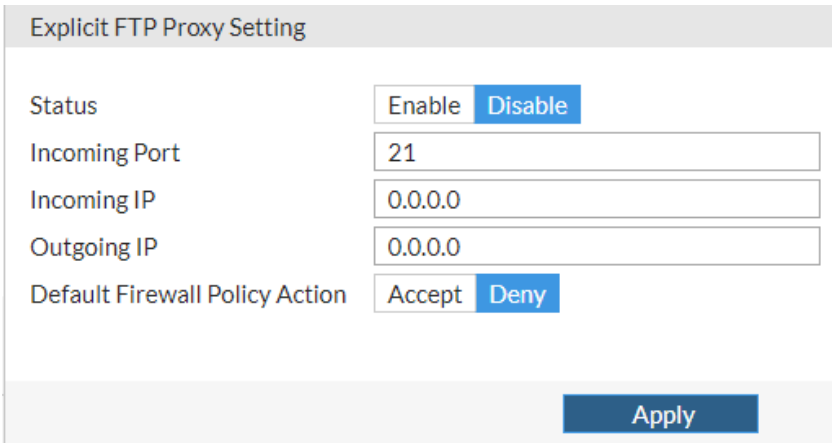
The FTP over HTTP proxy engine supports PORT mode, FTP over HTTP CONNECT, and uploads through PUT (UTM scanning).

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 *Policy & Objects* > *FTP Proxy*.



Configure the following settings and then select *Apply*:

Status	Select *Enable* to make the explicit FTP proxy active.
Incoming Port	Select the incoming port number.
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.

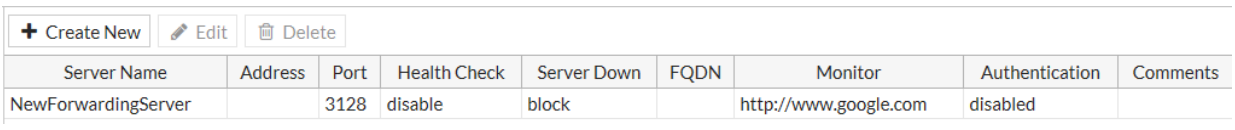
Forwarding server

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 server and specify a different web site to check for each one.

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 *Policy & Objects* > *Forwarding Server*.



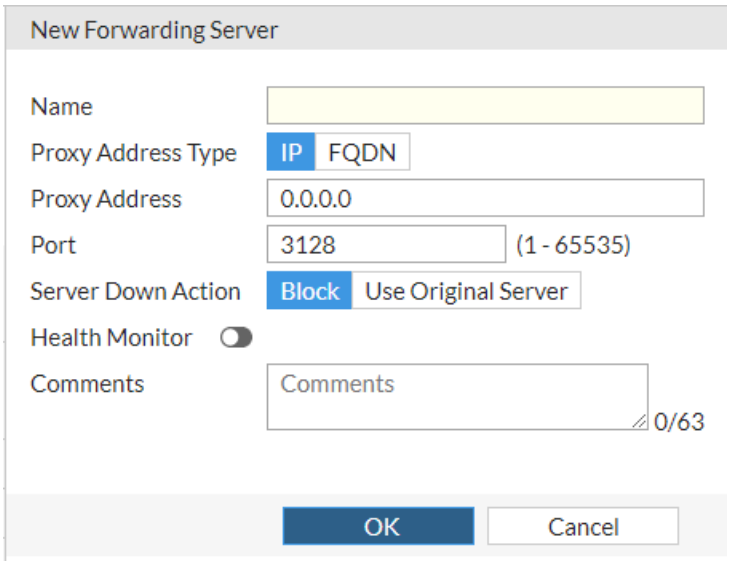
Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a new forwarding server. See "Create or edit a forwarding server" on page 175.
Edit	Edit a forwarding server. See "Create or edit a forwarding server" on page 175.
Delete	Remove a forwarding server from 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 will take when the server is down.
FQDN	The fully qualified domain name of the forwarding server.
Monitor	The URL address of the health check monitoring site.
Authentication	Indicates whether authentication is enabled or disabled for that forwarding server.
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 select *Edit*.

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

Name	Enter the name of the forwarding server.
Proxy Address Type	Select the type of IP address of the forwarding server, either *IP* or *FQDN*.
Proxy Address	If you selected *IP* for the proxy address type, enter the IP address of the forwarding server.
FQDN	If you selected *FQDN* for the proxy address type, enter the fully qualified domain name of the forwarding server.
Port	Enter the port number of the forwarding server.
Server Down Action	Select what action the FortiProxy unit will take if the forwarding server is down, either *Block* or *Use Original Server*.
Health Monitor	Enable or disable health check monitoring.
Health Check Monitor Site	If you enabled *Health Monitor*, enter the URL address of the health check monitoring site.
Comments	Enter an optional description of the forwarding server.

To create a new 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}
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 *Policy & Objects* > *Server URL*.

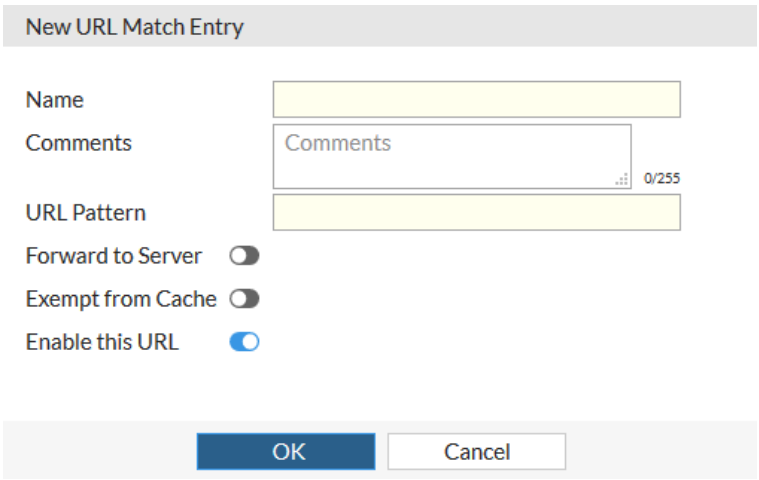
Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a URL match entry. See "Create or edit a URL match entry" on page 177.
Edit	Edit a URL match entry. See "Create or edit a URL match entry" on page 177.
Delete	Remove a URL match entry from the list.
Name	The name for the URL match entry.
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.; the Object Usage window opens and displays the various locations of the referenced object.

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 select *Edit*.

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

Name	Enter a name for the URL match entry.
Comments	Enter an optional description of 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 174.
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.

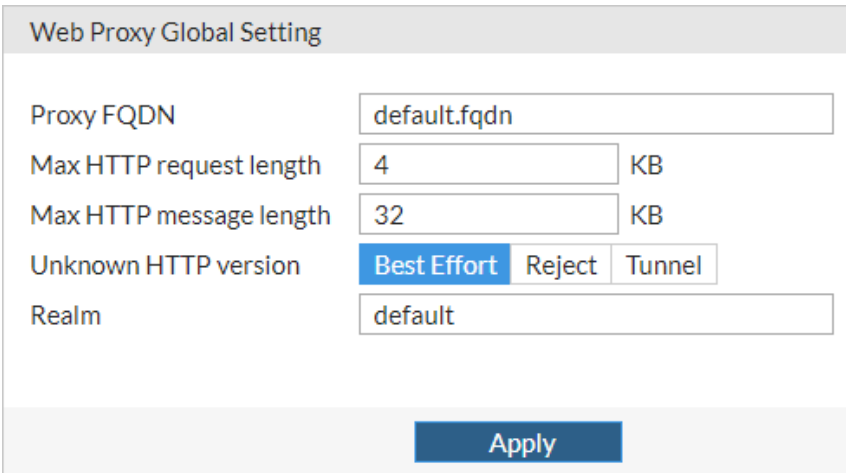
To create a URL match entry in the CLI:

```
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
```

Web proxy global

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

Go to *Policy & Objects* > *Web Proxy Global* to change the global explicit web proxy settings.



Configure the following settings and then select *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 (default = 4 Kb).
Max HTTP message length	The maximum length of an HTTP message that can be cached, in Kb. Larger messages are rejected (default = 32 Kb).
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. *Tunnel* requires user authentication on the HTTP CONNECT request.
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.

Web proxy auto-discovery protocol

The Web Proxy Auto-Discovery Protocol (WPAD) is a method for a browser to automatically discover the proxy configuration file, without any browser configuration, using settings in DNS or DHCP. For more information about this method, refer to the following Internet Engineering Task Force (IETF) draft:

http://tools.ietf.org/html/draft-ietf-wrec-wpad-01

When using DNS, the most widely supported resolution method, an entry is made in the local authoritative zone to map the name `wpad` (such as `wpad.example.com`) to one or more IP addresses. The browser is configured to automatically look in the following locations to find the WPAD configuration, which is in effect a PAC file, as described in "PAC policy" on page 151:

http://wpad.department.branch.example.com/wpad.dat

http://wpad.branch.example.com/wpad.dat

http://wpad.example.com/wpad.dat

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 *Policy & Objects* > *Web Proxy Profile* to change the web proxy profiles.

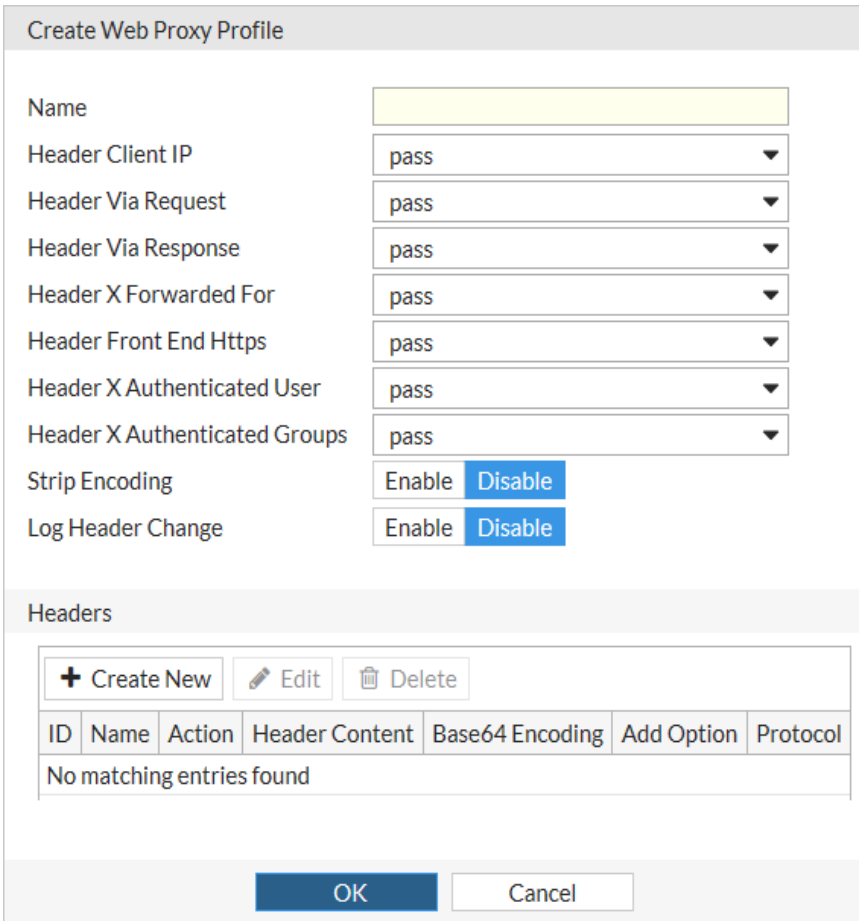
Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a new web proxy profile. See "Create or edit a web proxy profile" on page 180.
Edit	Edit the selected web proxy profile. See "Create or edit a web proxy profile" on page 180.
Delete	Remove the selected web proxy profile.
Name	The name of the web proxy 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.*, 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 *Create Web Proxy Profile* window.



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

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

Name	Enter the name of the new web proxy profile.
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 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.

Strip Encoding	Select whether to strip out unsupported encoding from request headers and correctly block banned words. This is to resolve issues when attempting to successfully block content using Google Chrome.
Log Header Change	Select whether to allow changes to the log header.
Create New	Select to add a new header. See "Create or edit an HTTP header" on page 182.
Edit	Select to change an existing header. See "Create or edit an HTTP header" on page 182.
Delete	Select to remove an existing header.
ID	The identifier for the HTTP forwarded header.
Name	The name 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*.
Header Content	The content of the HTTP header.
Base64 Encoding	Whether base64 encoding is enabled or disabled.
Add Option	How the new header is added: *append*, *new-on-not-found*, or *new*.
Protocol	Whether the new header uses HTTP, HTTPS, or both.

Create or edit an HTTP header

You can change the following HTTP headers:

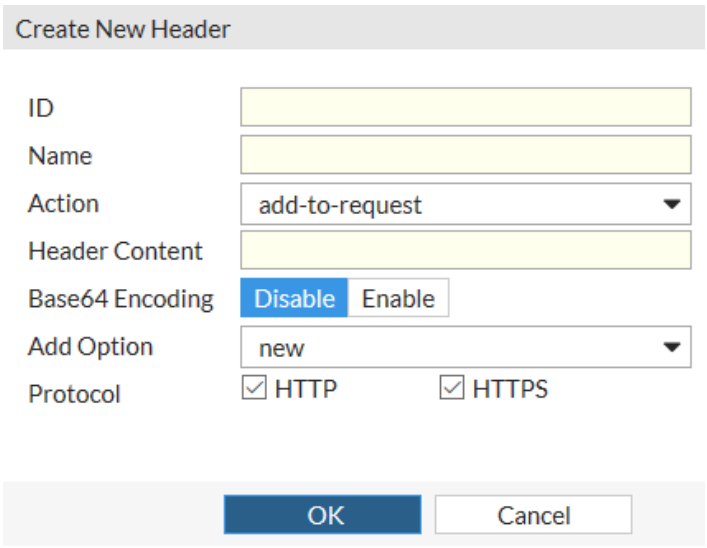
- Client IP
- Header via request
- Header via response
- Header *x* forwarded for
- Header Front End HTTPS
- X Authenticated User
- X Authenticated Groups

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 New Header* window.



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

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

ID	Enter or select an identifier for the HTTP forwarded header.
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.

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

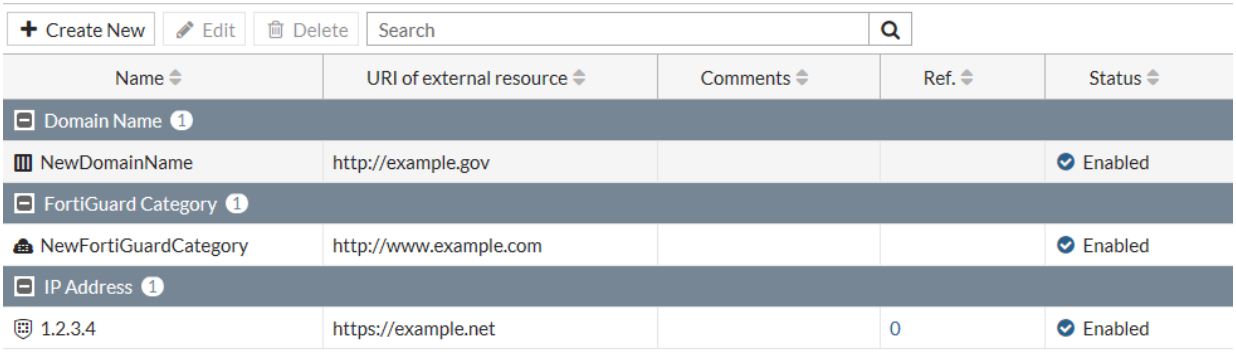
```
config web-proxy profile
   edit <name>
   set header-client-ip {add | pass | remove}
   set header-via-request {add | pass | remove}
   set header-via-response {add | pass | remove}
   set header-x-forwarded-for {add | pass | remove}
      set header-front-end-https {add | pass | remove}
      set 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
```

External resources

The External Resources page lists FortiGuard categories, IP addresses, and domain names that have been added for various FortiProxy features to access.

Go to *Policy & Objects* > *External Resources* to see which external resources have been added.



Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

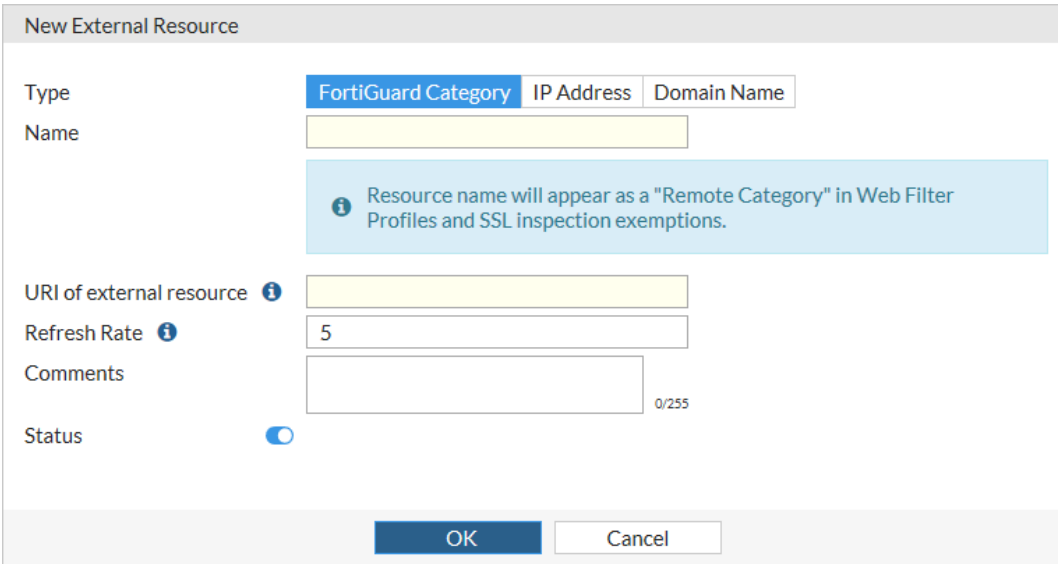
The following options are available:

Create New	Select to create an external resource. See "Create or edit an external resource" on page 185.
Edit	Modifies settings for the selected external resource. When you select *Edit*, the Edit External Resource page opens. See "Create or edit an external resource" on page 185.
Delete	Removes the selected external resource.
Search	Enter a search term to filter the list.
Name	The name of the external resource, which appears under the Domain Name, FortiGuard Category, or IP Address subheading.
URI of external resource	The link to an external resource file.
Comments	An optional description of the external resource.
Ref.	Displays the number of times that the object is referenced. To view the location of the referenced object, select the number in Ref. A window opens and lists the current locations and possible locations of the referenced object.

Status	The status is either *Enabled* or *Disabled*.

Create or edit an external resource

Select *Create New* to open the New External Resource page.



Select an external resource and then select *Edit* to open the Edit External Resource page.

Configure the following settings in the New External Resource page or Edit External Resource page and then select *OK*:

Type	Enter the name to identify the external resource. You cannot edit the name after you create the external resource. There are three types of external resources: • *FortiGuard Category*—When you create a FortiGuard category, the name appears under “Remote Categories” in *Security Profiles* > *Web Filter* and SSL inspection exemptions. • *IP Address*—When you create an IP address, the name appears as an “External Domain Block List” under *Security Profiles* > *DNS Filter* and as a “Source/Destination” in proxy policies. • *Domain Name*—When you create a domain name, the name appears as an “Remote Categories” under *Security Profiles* > *DNS Filter*.
Name	Required. The name of the external resource.

URI of external resource	The link to an external resource file. The size of the file can be 10 MB, or 128,000 lines of text, whichever is most restrictive. • If you selected *FortiGuard Category*, the file should be a plain text file with one URL on each line. • If you selected *IP Address,* the file should be a plain text file with one IP address, IP address range, or subnet on each line. IPv6 addresses are ignored n the DNS filter profile. • If you selected *Domain Name*, the file should be a plain text file with one domain on each line. Simple wildcards are supported.
Refresh Rate	The time interval to refresh the external resource. The range is 1-43,200 minutes.
Comments	Enter an optional description of the external resource.
Status	Enable or disable whether the external resource is active.

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.

This chapter 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.

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.

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.

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.

Content Analysis

Content Analysis is a licensed feature that allows you to detect adult content in real-time. This service is a real time analysis of the content passing through the FortiProxy unit. Unlike other image analysis tools, this one does

not just look for skin tone colors but can detect limbs, body parts, and the position of bodies. Once detected, such content can be optionally blocked or reported.

ICAP

This module 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.

Proxy options

Proxy options includes features you can configure for when your FortiProxy is operating in proxy mode, including protocol port mapping, block oversized files/emails, and other web and email options.

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.

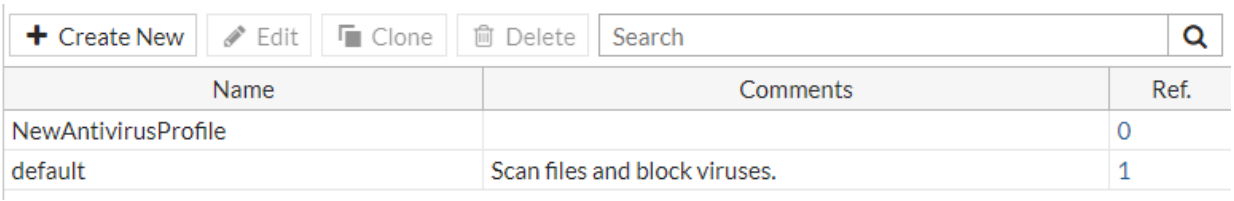
Individual Deep Inspection profiles can be created, depending on the requirements of the policy. Depending on the profile, you can:

- 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

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* and select 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).



Name	Comments	Ref.
NewAntivirusProfile		0
default	Scan files and block viruses.	1

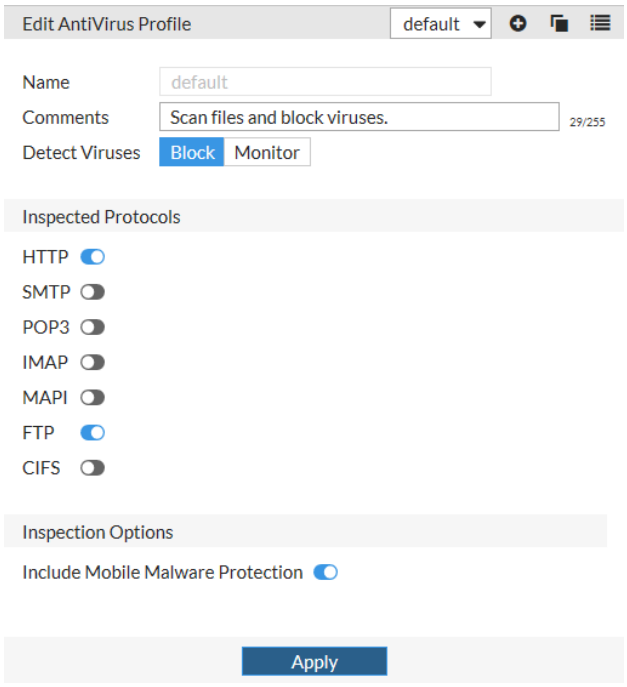
Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a new antivirus profile. See "Create or edit an antivirus profile" on page 190.
Edit	Modify the selected antivirus profile. See "Create or edit an antivirus profile" on page 190.
Clone	Make a copy of the selected antivirus profile.
Delete	Remove the selected antivirus profile.
Search	Enter a search term to find in the antivirus profile 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

To change the default antivirus profile, go to *Security Profiles* > *AntiVirus*. The *Edit AntiVirus Profile* page opens.



To create a new antivirus profile:

1. Go to *Policy & Objects* > *Policy* and select *Create New*.
2. Under *Security Profiles* in the *New Policy* window, enable *AntiVirus*, and select the *Create New* icon (a plus sign) from the drop-down menu.
   The *New AntiVirus Profile* window opens.
3. Configure the following settings:

Name	Enter the name of the antivirus profile.
Comments	Optionally, enter a description of the profile.
Detect Viruses	When a virus is found, select either *Block* to prevent infected files from passing throughout the FortiProxy unit or *Monitor* to allow infected files to pass through the FortiProxy unit but to record instances of infection.
Inspected Protocols	Enable the protocols that you want scanned for viruses.
Include Mobile Malware Protection	Select to protect mobile devices from malware.

4. Select *OK* to create the antivirus profile.

To edit the antivirus profile:

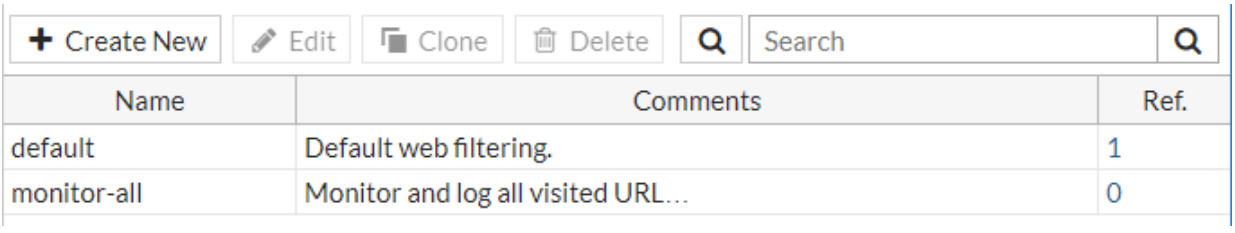
1. Go to *Security Profiles* > *AntiVirus*.
   The *Edit AntiVirus Profile* window opens.
2. Make any necessary changes and then select *Apply* to save your changes.

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* and select 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).



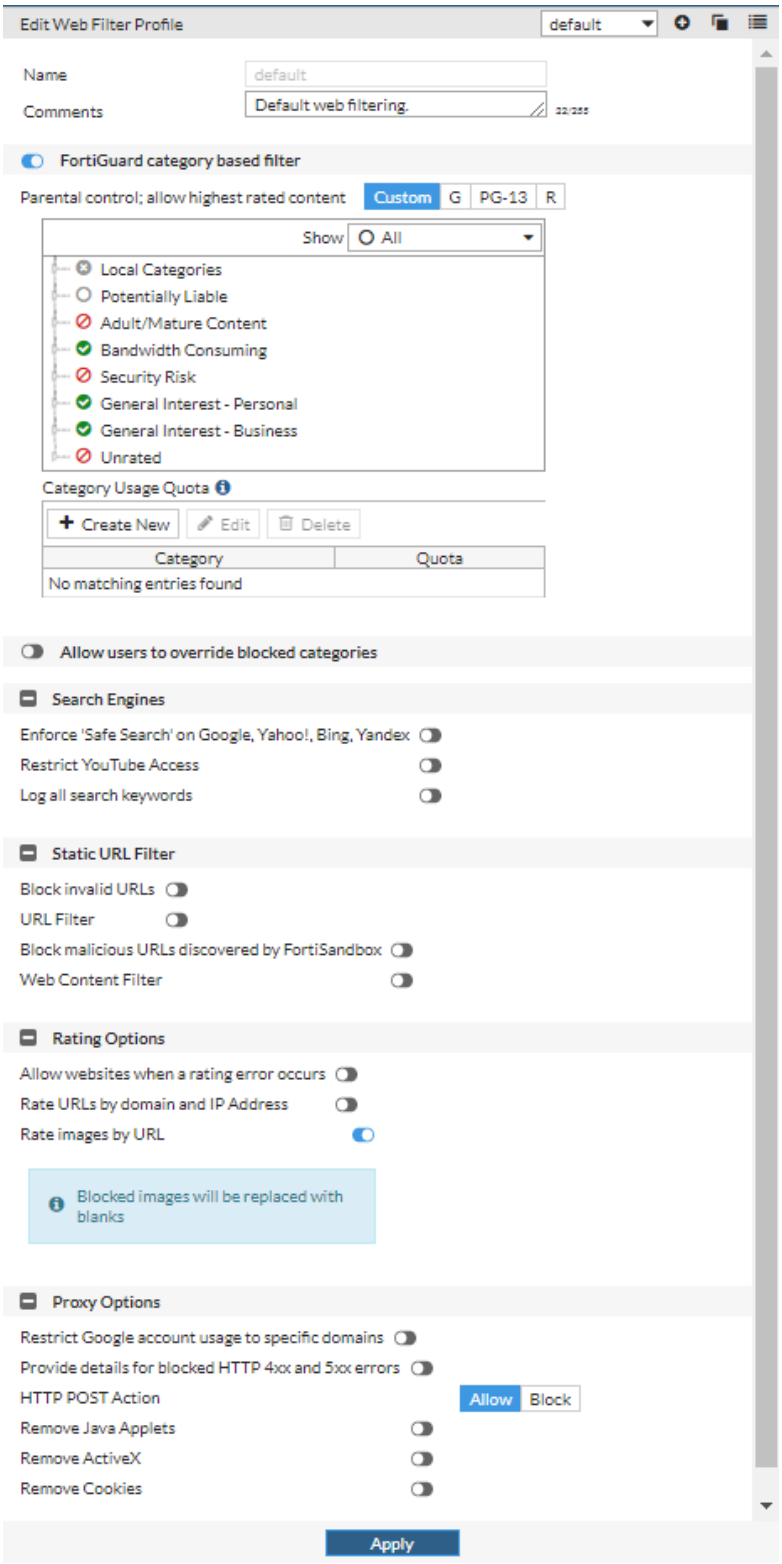
Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a new web filter profile. See "Create or edit a web filter profile" on page 192.
Edit	Modify the selected web filter profile. See "Create or edit a web filter profile" on page 192.
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

To change the default web filter profile, go to *Security Profiles* > *Web Filter*. The *Edit Web Filter Profile* page opens.


Edit Web Filter Profile
default
Name
default
Comments
Default web filtering.
22/255
FortiGuard category based filter
Parental control; allow highest rated content
Custom
G
PG-13
R
Show
All
Local Categories
Potentially Liable
Adult/Mature Content
Bandwidth Consuming
Security Risk
General Interest - Personal
General Interest - Business
Unrated
Category Usage Quota
Create New
Edit
Delete
Category
Quota
No matching entries found
Allow users to override blocked categories
Search Engines
Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex
Restrict YouTube Access
Log all search keywords
Static URL Filter
Block invalid URLs
URL Filter
Block malicious URLs discovered by FortiSandbox
Web Content Filter
Rating Options
Allow websites when a rating error occurs
Rate URLs by domain and IP Address
Rate images by URL
Blocked images will be replaced with blanks
Proxy Options
Restrict Google account usage to specific domains
Provide details for blocked HTTP 4xx and 5xx errors
HTTP POST Action
Allow
Block
Remove Java Applets
Remove ActiveX
Remove Cookies
Apply

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

Name	The name of the web filter profile.
Comments	Optional description of the profile.
FortiGuard category based filter	Enable FortiGuard categories. If the device is not licensed for the FortiGuard web-filtering service, traffic can be blocked by enabling this option.
Parental control; allow highest rated content	Select *Custom*, *G*, *PG-13*, or *R*.
Show	Select which filter to use to display the FortiGuard categories: *All*, *Allow*, *Authenticate*, *Block*, *Monitor*, or *Warning*. You can enter a category to search for.
Category Usage Quota	For categories set to Monitor, Warning, or Authenticate, you can create a category usage quota by selecting *Create New*.
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 can switch to	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 Group*, or *IP* or whether to *Ask*. The user or user group 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*.
Search Engines	

Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex	Enable to use predefined web filter rules to edit web profiles and provide safe search for Google, Bing, and YouTube.
Restrict YouTube Access	Enable and then select the *Strict* or *Moderate* level of restriction for YouTube access.
Log all search keywords	Enable if you want all search keywords logged.
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 196.
Block malicious URLs discovered by FortiSandbox	Enable to block malicious URLs discovered by FortiSandbox.
Web Content Filter	Enable and then create or edit a web content filter to block access to web pages that include the specified patterns. See "Create or edit a web content filter" on page 198.
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.

Rate images by URL	Enable to have the FortiProxy unit retrieve ratings for individual images in addition to web sites. Images in a blocked category are not displayed even if they are part of a site in an allowed category. Blocked images are replaced on the originating web pages with blank placeholders. Rated image file types include GIF, JPEG, PNG, BMP, and TIFF.
Proxy Options	
Restrict Google account usage to specific domains	This feature allow the blocking of access to some Google accounts and services while allowing access to accounts that are included in the domains specified in the exception list.
Provide details for blocked HTTP 4xx and 5xx errors	Enable to have the FortiProxy unit display its own replacement message for 400 and 500-series HTTP errors. If the server error is allowed through, malicious or objectionable sites can use these common error pages to circumvent web filtering.
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 Java Applets	Enable to filter Java applets from web traffic. Web sites using Java applets might not function properly with this filter enabled.
Remove ActiveX	Enable to filter ActiveX scripts from web traffic. Web sites using ActiveX might not function properly with this filter enabled.
Remove Cookies	Enable to filter cookies from web traffic. Web sites using cookies might not function properly with this enabled.

To create a web filter profile:

1. Go to *Security Profiles* > *Web Filter* and select *Create New* (a plus sign in a circle) from the toolbar.
2. Enter the required information and then select *OK* to create the new web filter profile.

To edit a web filter profile:

1. Go to *Security Profiles* > *Web Filter*, select 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) from the toolbar.
2. Select the profile you want to edit and then select *Edit* from the toolbar or double-click on the profile name in the list.
   The *Edit Web Filter Profile* window opens.
3. Edit the information as required and then select *Apply* to save your changes.

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. Enable *URL Filter*.
3. In the *URL Filter* table, select *Create*.
   The *New URL Filter* dialog box opens.
4. 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.
5. Select the type of pattern to match. One of: *Simple*, *Reg. Expression*, or *Wildcard*.
6. 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.
     See"Replacement messages" on page 93.
   - *Allow*: Allow access to any URL that matches the URL pattern.
   - *Monitor*: Monitor traffic to and from URLs matching the URL pattern.
7. Enable or disable the status of the filter to make the filter active or inactive.
8. Select *OK* to save the URL filter.
9. Select *Apply* in the *Edit Web Filter Profile* page to save the changes to the web filter.

To edit a URL filter:

1. Go to *Security Profiles* > *Web Filter* and enable *URL Filter*.
2. In the URL Filter table, double-click on a filter or select the filter and then select *Edit* in the toolbar.
3. Edit the filter settings as required.

4. Select *OK* to save your changes to the URL filter.
5. Select *Apply* in the *Edit Web Filter Profile* page to save the changes to the web filter.

To delete a URL filter or filters:

1. Go to *Security Profiles* > *Web Filter* and enable *URL Filter*.
2. In the URL Filter table, select the filter or filters that need to be deleted and then select *Delete* in the toolbar.
3. Select *OK* in the confirmation dialog box to delete the selected filter or filters.

Create or edit a web content filter

Web content filters can be added, edited, and deleted as required.

To create a new web content filter:

1. Go to *Security Profiles* > *Web Filter*.
2. In the *Static URL Filter* section, enable *Web Content Filter*.
3. Select *Create New*.
4. Select the *Pattern Type*, either *Wildcard* or *Reg. Expression*.
5. Enter the content *Pattern* to match.
6. Select the *Language* from the drop-down menu.
7. Select *Block* or *Exempt*.
8. Enable the *Status*.
9. Select *OK*.

To edit a web content filter:

1. Go to *Security Profiles* > *Web Filter*.
2. In the *Static URL Filter* section, enable *Web Content Filter*.
3. Select the filter you want to edit and then select *Edit* from the toolbar.
   The *Edit Web Content Filter* window opens.
4. Edit the information as required and then select *OK* to apply your changes.

To delete a web content filter or filters:

1. Go to *Security Profiles* > *Web Filter*.
2. In the *Static URL Filter* section, enable *Web Content Filter*.
3. Select the filter or filters that you want to delete.
4. Select *Delete* from the toolbar.
5. Select *OK* in the confirmation dialog box to delete the selected filter or filters.

DNS filter

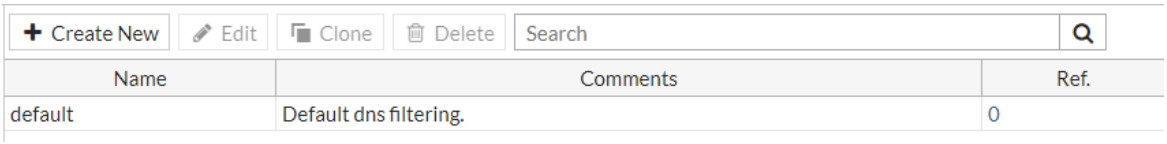
You can configure DNS web filtering to allow, block, or monitor access to web content according to FortiGuard categories. When DNS web filtering is enabled, your FortiProxy unit must use the FortiGuard DNS service for

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 FortiGuard category.

To view available DNS filter profiles, go to *Security Profiles* > *DNS Filter* and select 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).

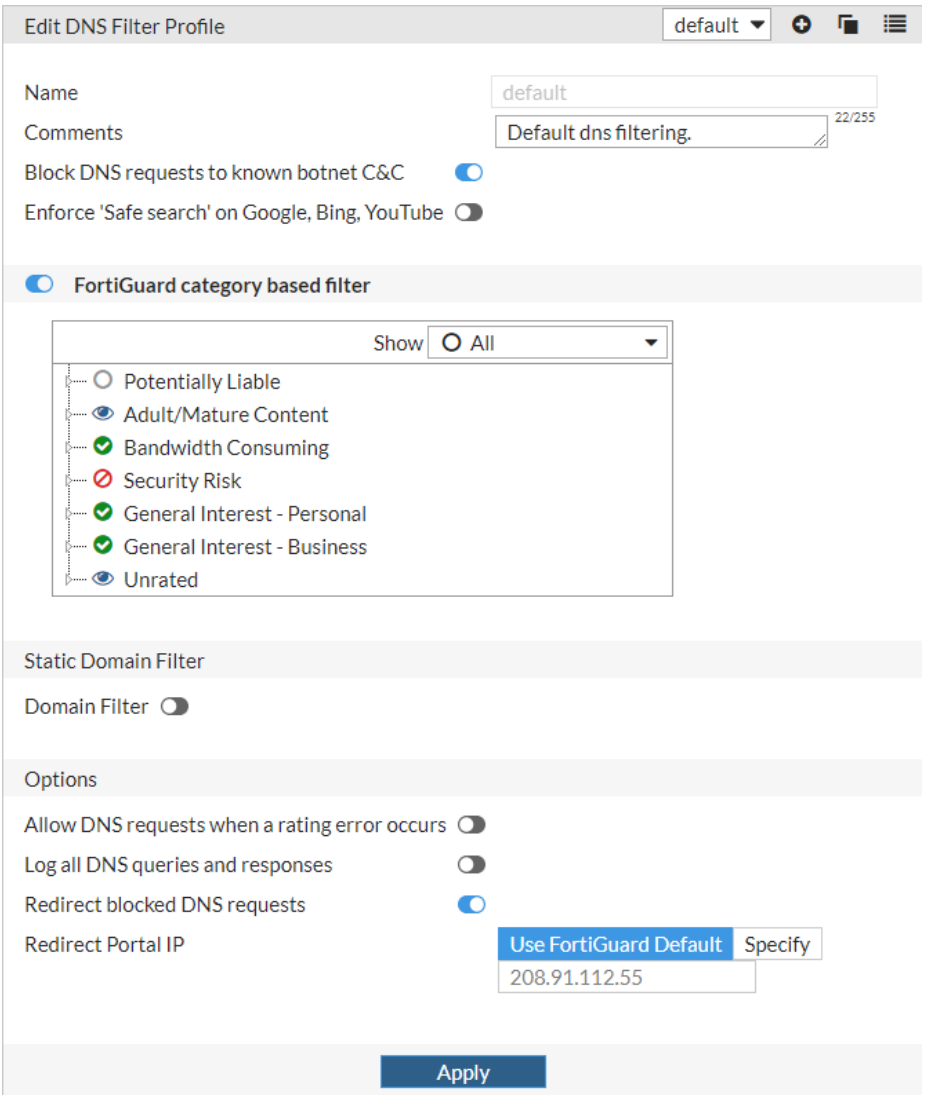


The following options are available:

Create New	Create a DNS filter profile. See "Create or edit a DNS filter profile" on page 199.
Edit	Modify the selected DNS filter profile. See "Create or edit a DNS filter profile" on page 199.
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

To edit the default DNS filter profile, go to *Security Profiles* > *DNS Filter*. The *Edit DNS Filter Profile* page opens.



Configure the following settings and then select *Apply* to apply any changes:

Name	The name of the DNS filter profile.
Comments	Optional description of the profile.
Block DNS requests to known botnet C&C	FortiGuard maintains a database containing a list of known botnet command and control (C&C) addresses. This database is updated dynamically and stored on the FortiProxy unit. This database is covered by FortiGuard web filter licensing, so you must have a FortiGuard web filtering license to use this feature. When you block DNS requests to known botnet C&C addresses, using IPS, DNS lookups are checked against the botnet C&C database. All matching DNS lookups are blocked. Matching uses a reverse prefix match, so all subdomains are also blocked.

Enforce 'Safe search' on Google, Bing, YouTube	Enable to use predefined DNS filter rules to edit DNS profiles and provide safe search for Google, Bing, and YouTube.
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.
Show	In the *Show* drop-down menu, select which filter to use to display the FortiGuard categories: *All*, *Allow*, *Block*, or *Monitor* . You can enter a category to search for.
Static Domain Filter	
Domain Filter	Enable to create or edit domain filters. See "Create or edit a domain filter" on page 202.
Options	
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.
Redirect blocked DNS requests	Enable if you want blocked DNS requests to be redirected.
Redirect Portal IP	Select *Use FortiGuard Default* or *Specify*. If you select *Specify*, enter the IP address. This option is available only if *Redirect blocked DNS requests* is enabled.

To create a new DNS filter profile:

1. Go to *Security Profiles* > *DNS Filter* and select *Create New*.
2. Enter the required information and then select *OK* to create the new DNS filter profile.

To edit a DNS filter profile:

1. Go to *Security Profiles* > *DNS Filter*, select 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) from the toolbar.

2. Select the profile you want to edit and then select *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 *Apply* 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 new domain filter:

1. Go to Security Profiles > DNS Filter and enable *Domain Filter*.
2. In the *Domain Filter* table, select *Create*.
   The *New Domain Filter* dialog box opens.
3. 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.
4. Select the type of pattern to match. One of: *Simple*, *Reg. Expression*, or *Wildcard*.
5. Select the action to take when the pattern is matched:
   - *Block*: Block access to any domains matching the domain pattern and display a replacement message. See "Replacement messages" on page 93.
   - *Allow*: Allow access to any domain that matches the domain pattern.
   - *Monitor*: Monitor traffic to and from domains matching the domain pattern.
6. Enable or disable the status of the filter to make the filter active or inactive.
7. Select *OK* to save the domain filter.
8. Select *Apply* in the *Edit DNS Filter Profile* page to save the DNS filter.

To edit a domain filter:

1. Go to *Security Profiles* > *DNS Filter* and enable *Domain Filter*.
2. In the Domain Filter table, double-click on a filter or select the filter and then select *Edit* in the toolbar.
3. Edit the filter settings as required.
4. Select *OK* to save your changes to the domain filter.
5. Select *Apply* in the *Edit DNS Filter Profile* page to save the changes to the DNS filter.

To delete a domain filter or filters:

1. Go to *Security Profiles* > *DNS Filter* and enable *Domain Filter*.
2. In the Domain Filter table, select the filter or filters that need to be deleted and then select *Delete* in the toolbar.
3. Select *OK* in the confirmation dialog box to delete the selected filter or filters.

Application control

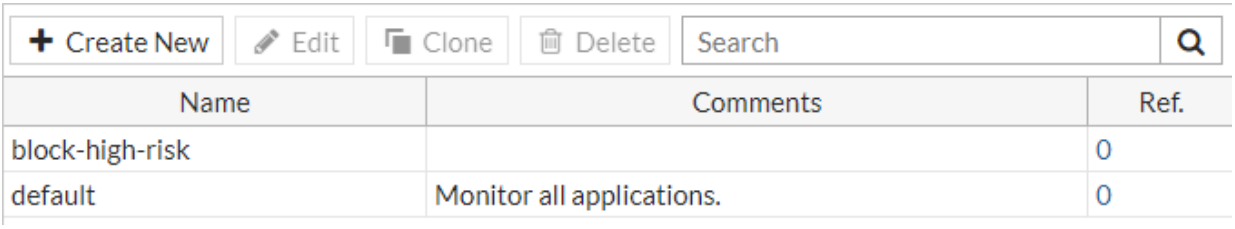
Using the Application Control feature, your FortiProxy unit can detect and take action against network traffic depending on the application generating the traffic. Based on FortiProxy Intrusion Protection protocol decoders, application control is a user-friendly and powerful way to use Intrusion Protection 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* and select 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).



Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

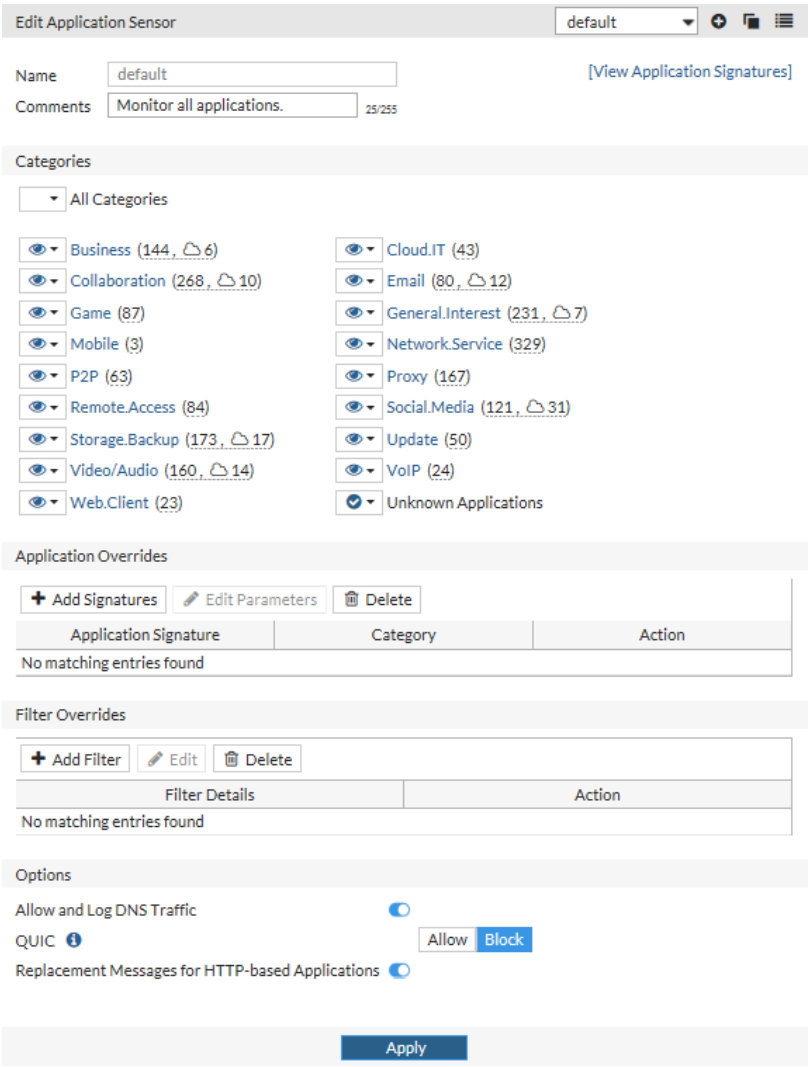
The following options are available:

Create New	Create a new application sensor. See "Create or edit an application sensor" on page 204.
Edit	Modify the selected application sensor. See "Create or edit an application sensor" on page 204.
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 change the default application sensor, go to *Security Profiles* > *Application Control*. The *Edit Application Sensor* page is displayed.



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

Name	The name of the application sensor.
View Application Signatures	Select to see a list of predefined application signatures. To create a new application signature, see "Create or edit an application signature" on page 206.
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 that category.
Application Overrides	Application overrides allow you to choose individual applications. To add signatures for an application override, see "Add or edit a signature" on page 206.
Filter Overrides	Filter overrides allow you to select groups of applications and override the application signature settings for them. To add filters for a filter override, see "Add or edit a filter" on page 206.
Allow and Log DNS Traffic	Enable to allow DNS traffic.
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.

To create a new application sensor:

1. From the application sensor list, select *Create New*.
2. Enter the required information and then select *Apply* to create the application sensor.

To edit an application sensor:

1. From the application sensor list, select the sensor that you need to edit and then select *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 *Apply* to save your changes.

Create or edit an application signature

If you have to detect an application that is not already in the application list, you can create a new application signature:

1. Go to *Security Profiles* > *Application Control*.
2. Select the link in the upper right corner, *[View Application Signatures]*.
3. Select *Create New*.
4. Enter a name (no spaces) for the application signature in the *Name* field.
5. Enter a brief description in the *Comments* field
6. Enter the text for the signature in the *Signature* field. The syntax for signatures is described in "Custom signatures" on page 238.
7. Select *OK*.

You can edit application signatures that you have created. Select the application signature and then select *Edit*.

Add or edit a signature

Signatures for application overrides can be added or edited as required.

To add predefined signatures:

1. Go to *Security Profiles* > *Application Control*.
2. In the *Application Overrides* section, select *Add Signatures*.
3. Use the *Add Filter* search field to narrow down the list of possible signatures by a series of attributes.
4. Select *Use Selected Signatures*.

To edit a predefined signature:

1. Go to *Security Profiles* > *Application Control*.
2. In the *Application Overrides* section, select the signature to edit and then select *Edit Parameters* from the toolbar. **NOTE:** You can only edit signatures that have parameters.
3. Edit the information as required and then select *OK* to apply your changes.

Add or edit a filter

Filters for filter overrides can be added or edited as required.

To create a new filter:

1. Go to *Security Profiles* > *Application Control*.
2. In the *Filter Overrides* section, select *Add Filter*.
3. Use the *Add Filter* search field to narrow down the list of possible signatures by a series of attributes.
4. Select *Use Filters*.

To edit a filter:

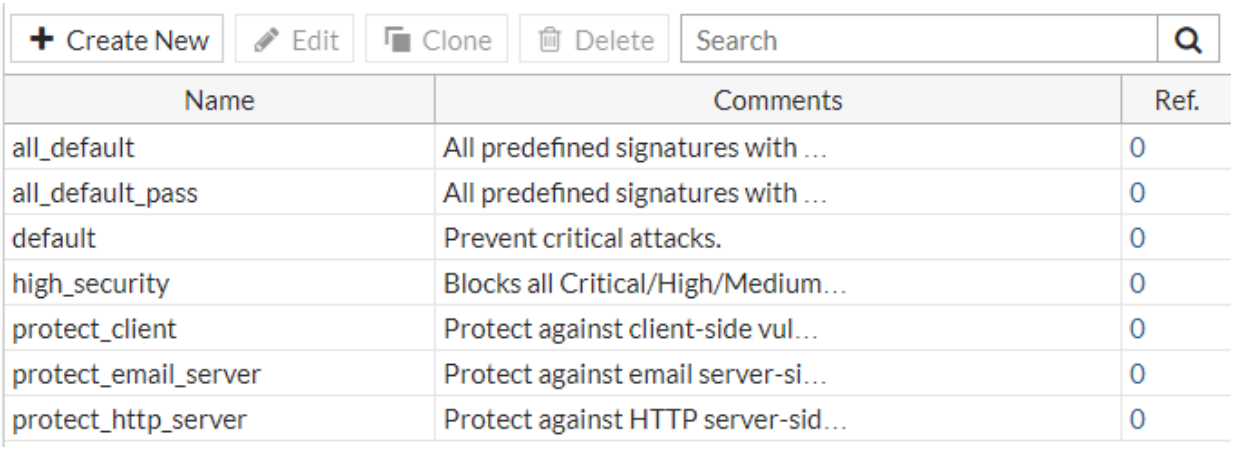
1. Go to *Security Profiles* > *Application Control*.
2. In the *Filter Overrides* section, select the filter you want to edit and then select *Edit* from the toolbar. The *Edit Filter Overrides* window opens.
3. Edit the information as required and then select *Save Filters* to apply your changes.

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* and select 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).



Right-click on any column heading to select which columns are displayed 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 208.
Edit	Modify the selected IPS sensor. See "Create or edit an IPS sensor" on page 208.
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.

IPS sensors can be added, edited, cloned, and deleted as required.

To create a new IPS sensor:

1. From the IPS sensor list, select *Create New*.
2. Enter the name of the new IPS sensor.
3. Optionally, enter a comment. The comment appears in the IPS sensor list.
4. Add individual IPS signatures or use an IPS filter to add multiple signatures to a sensor by specifying the characteristics of the signatures to be added. See "Add or edit an IPS signature" on page 211 and "Add or edit an IPS filter" on page 211.
5. Toggle the *Enable* button in the Rate Based Signatures table that corresponds with the signature that you want enabled.
6. Select *OK* to create the IPS sensor.

To edit an IPS sensor:

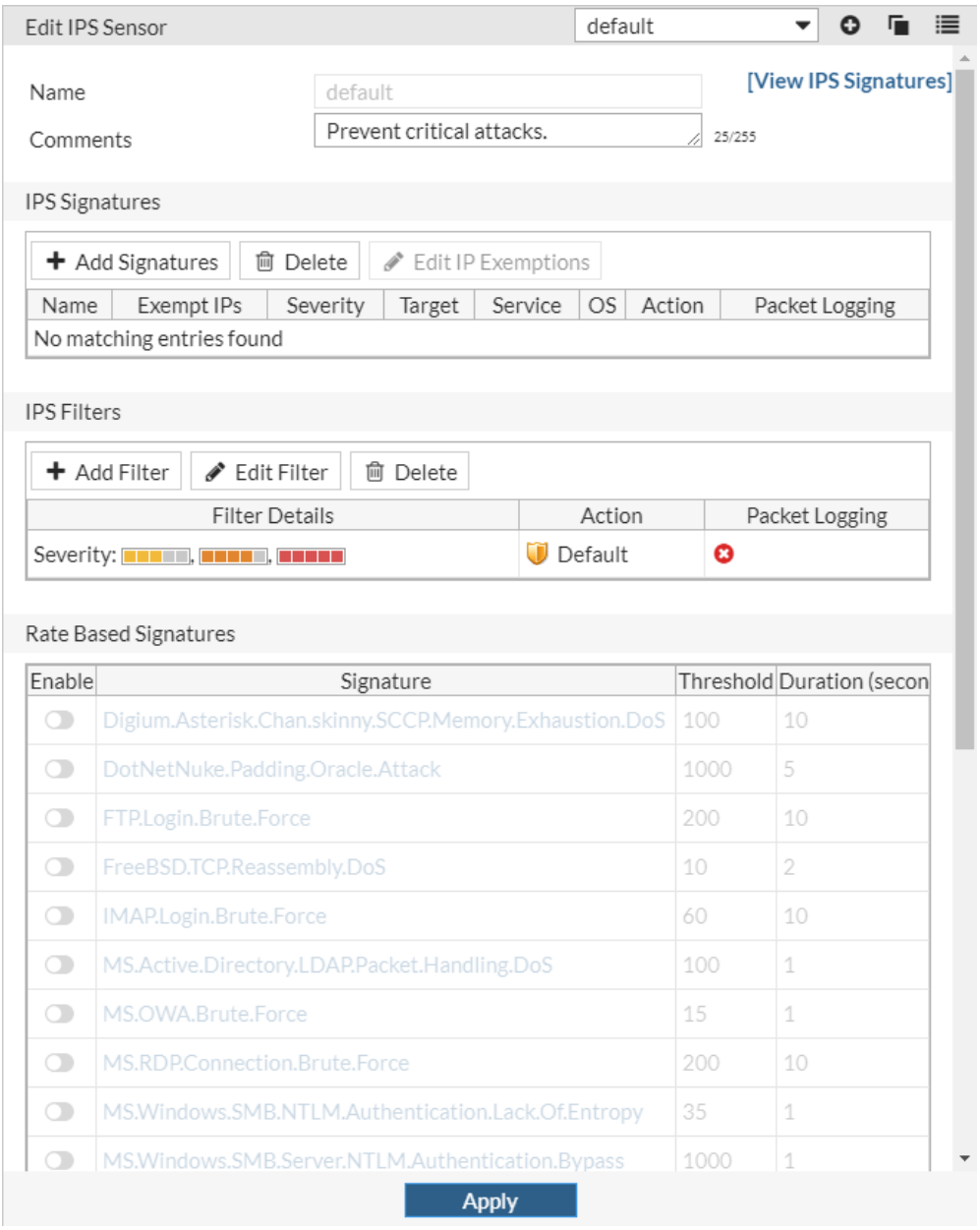
1. From the IPS sensor list, select the sensor that you need to edit and then select *Edit* from the toolbar or double-click on the sensor name in the list.
   The *Edit IPS Sensor* window opens.
2. Edit the information as required and then select *Apply* to save your changes.

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.

This section describes how to configure the Intrusion Prevention settings.

To change the default IPS sensor, go to *Security Profiles* > *Intrusion Prevention*. The *Edit IPS Sensor* page is displayed.



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

Name	The name of the IPS sensor.
View IPS Signatures	Select to see a list of predefined IPS signatures. To create a new IPS signature, see "Create or edit an IPS signature" on page 210.
Comments	Optional description of the IPS sensor.

IPS Signatures	Select from the predefined IPS signatures, edit a predefined IPS signature, or create a new IPS signature. See "Add or edit an IPS signature" on page 211.
IPS Filters	Add or edit an IPS filter. See "Add or edit an IPS filter" on page 211. 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.
Rate Based Signatures	Toggle the *Enable* button in the Rate Based Signatures table that corresponds with the signature that you want enabled. This group is a subset of the signatures that are found in the database that are normally monitored. This group of signatures is for vulnerabilities that are normally only considered a serious threat when the targeted connections come in multiples, a little like DoS attacks.

To create a new IPS sensor:

1. From the IPS sensor list, select *Create New*.
2. Enter the name of the new IPS sensor.
3. Optionally, enter a comment. The comment appears in the IPS sensor list.
4. Add individual IPS signatures or use an IPS filter to add multiple signatures to a sensor by specifying the characteristics of the signatures to be added. See "Add or edit a signature" on page 206 and "Add or edit an IPS filter" on page 211.
5. Toggle the *Enable* button in the Rate Based Signatures table that corresponds with the signature that you want enabled.
6. Select *OK* to create the IPS sensor.

To edit an IPS sensor:

1. From the IPS sensor list, select the sensor that you need to edit and then select *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 *Apply* to save your changes.

Create or edit an IPS signature

You can create an IPS signature.

To create a new IPS signature:

1. Go to *Security Profiles* > *Intrusion Prevention*.
2. Select the link in the upper right corner, *[View IPS Signatures]*.
3. Select *Create New*.
4. Enter a name (no spaces) for the IPS signature in the *Name* field.
5. Enter a brief description in the *Comments* field

6. Enter the text for the signature in the *Signature* field. The syntax for signatures is described in "Custom signatures" on page 238.
7. Select *OK*.

You can also edit IPS signatures that you have created. Select the IPS signature and then select *Edit*.

Add or edit an IPS signature

You can add or edit predefined IPS signatures.

To add a predefined signature:

1. Go to *Security Profiles* > *Intrusion Prevention*.
2. In the *IPS Signatures* section, select *Add Signatures*.
3. Select the predefined signatures to add.
4. Select *Use Selected Signatures*.

To exempt IP addresses from a predefined signature:

1. Go to *Security Profiles* > *Intrusion Prevention*.
2. In the *IPS Signatures* section, select the signature to edit and then select *Edit IP Exemptions* from the toolbar.
3. Select *Create New*.
4. Enter the source IP address, destination IP address, and netmasks,
5. Select *OK* to save the IP addresses.

Add or edit an IPS filter

You can add or edit IPS filters.

To create a new filter:

1. Go to *Security Profiles* > *Intrusion Prevention*.
2. In the *IPS Filters* section, select *Add Filter*.
3. Use the *Add Filter* search field to narrow down the list of possible signatures by a series of attributes.
4. Select *Use Filters*.

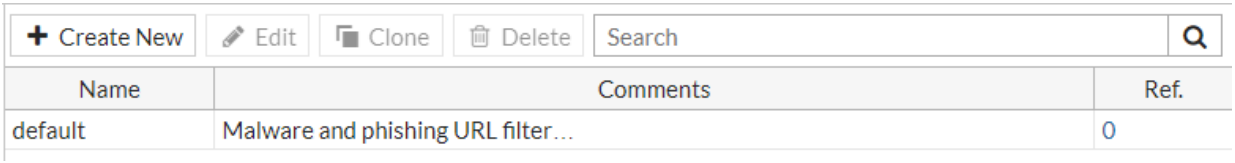
To edit a filter:

1. Go to *Security Profiles* > *Intrusion Prevention*.
2. In the *IPS Filters* section, select the filter you want to edit and then select *Edit Filter* from the toolbar. The *Edit Filter Overrides* window opens.
3. Edit the information as required and then select *Save Filters* to apply your changes.

Antispam

An antispam 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 antispam profiles can be created for different antispam scanning requirements. These profiles can then be applied to firewall policies.

To view the available antispam profiles, go to *Security Profiles* > *Anti-Spam* and select the List icon (the farthest right of the three icons in theupper right of the window; it resembles a page with some lines on it).



Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

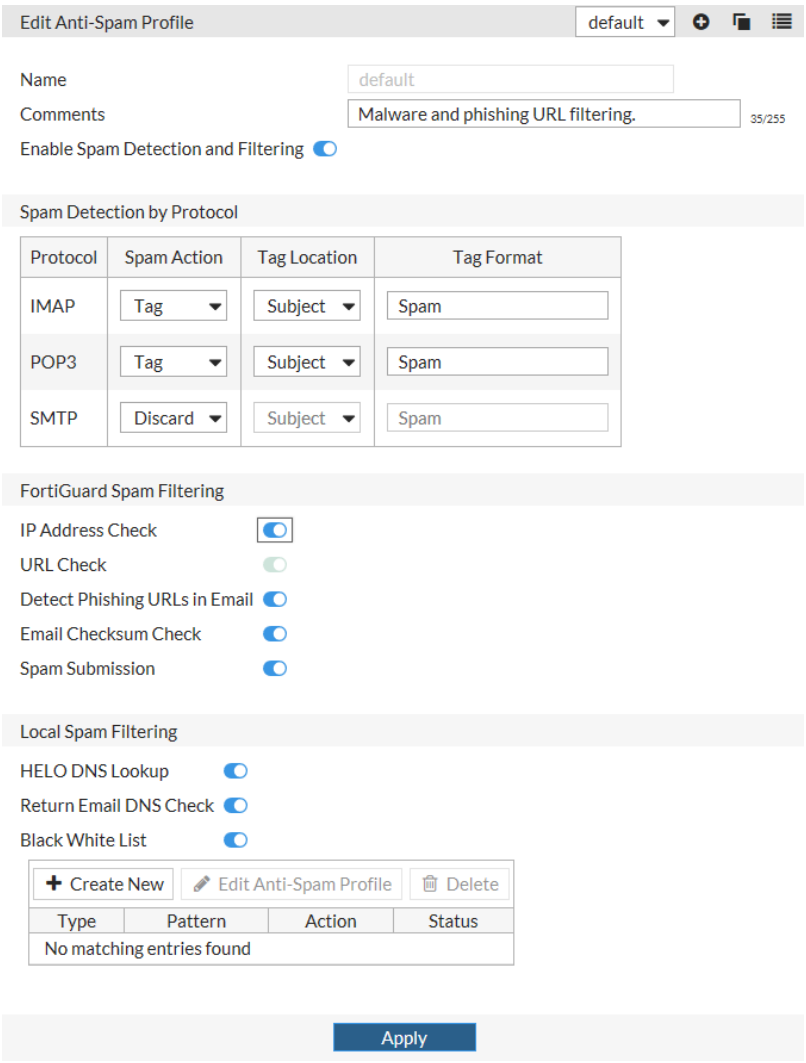
The following options are available:

Create New	Create an antispam profile. See "Create or edit an antispam profile" on page 212.
Edit	Modify the selected antispam profile. See "Create or edit an antispam profile" on page 212.
Clone	Make a copy of the selected antispam profile.
Delete	Remove the selected antispam profile.
Search	Enter a search term to find in the antispam profile list.
Name	The name of the antispam profile.
Comments	An optional description of the antispam 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 antispam profile

An antispam 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 antispam profiles can be created for different antispam scanning requirements. These profiles can then be applied to firewall policies.

To change the default antispam profile, go to *Security Profiles* > *Anti-Spam*. The *Edit Anti-Spam Profile* page opens.



To enable antispam scanning:

1. Go to *Policy & Objects* > *Policy* and either add or select the security policy that accepts the traffic to be scanned for spam. See "Create or edit a policy" on page 136.
2. In the *New Policy* or *Edit Policy* window, under *Security Profiles*, enable *Anti-Spam* and then select an antispam profile from the drop-down list.
3. Select *OK* to save the policy.

To create a new antivirus profile:

1. Go to *Policy & Objects* > *Policy* and select *Create New*.
2. Under *Security Profiles* in the *New Policy* window, enable *Anti-Spam* and select the *Create New* icon (a plus sign) from the drop-down menu.
   The *New Anti-Spam Profile* window opens.
3. Configure the following settings:

Name	Enter the name of the antispam profile.
Comments	Optionally, enter a description of the profile.
Enable Spam Detection and Filtering	Enable this option to configure the antispam profile.
Spam Detection by Protocol	For each protocol, select how the FortiProxy unit deals with detected spam: • *Tag*—When the spam action is set to *Tag*, messages detected as spam are labeled and delivered normally. The text used for the label is set in the Tag Format field and the label is placed in the subject or MIME header, as set with the Tag Location drop-down list. • *Discard*—When the spam action is set to *Discard*, messages detected as spam are deleted. No notification is sent to the sender or recipient. • *Pass*—When the spam action is set to *Pass*, the spam filter is disabled for the related protocol.
IP Address Check	Enable this option if you want the FortiProxy unit to query the FortiGuard Anti-Spam Service to determine if the IP address of the client delivering the email is blacklisted.
URL Check	Enable this option is you want the FortiProxy unit to submit all URLs in the email message body to the FortiGuard service for checking.
Detect Phishing URLs in Email	Enable this option if you want the FortiProxy unit to submit all URL hyperlinks appearing in the email message body to the FortiGuard service for checking.
Email Checksum Check	Enable this option if you want the FortiProxy unit to submit a checksum of each email message to the FortiGuard service for checking.
Spam Submission	Enable this option to add a link to the end of every message marked as spam. You then can select this link to inform the FortiGuard Anti-Spam service when a message is incorrectly marked.
HELO DNS Lookup	Whenever a client opens an SMTP session with a server, the client sends a HELO command with the client domain name. The FortiProxy unit takes the domain name specified by the client in the HELO and does a DNS lookup to determine if the domain exists. If the lookup fails, the FortiProxy unit determines that any messages delivered during the SMTP session are spam. The HELO DNS lookup is available only for SMTP traffic.
Return Email DNS Check	When you enable this option, your FortiProxy unit will take the domain in the reply-to email address and reply-to domain and check the DNS servers to see if there is an A or MX record for the domain. If the domain does not exist, your FortiProxy unit will treat the message as spam.
Black White List	Enable this option to add list items that should be marked as spam, marked as clear (the email is not filtered), or marked as rejected (the email session is dropped). Select *Create New* to add a list item, select the type, enter the pattern, select the action, and then enable the status.

4. Select *OK* to create the antivirus profile.

To edit the antispam profile:

1. Go to *Security Profiles* > *Anti-Spam*.
   The *Edit Anti-Spam Profile* window opens.
2. Edit the information as required and then select *Apply* to save your changes.

Data leak prevention

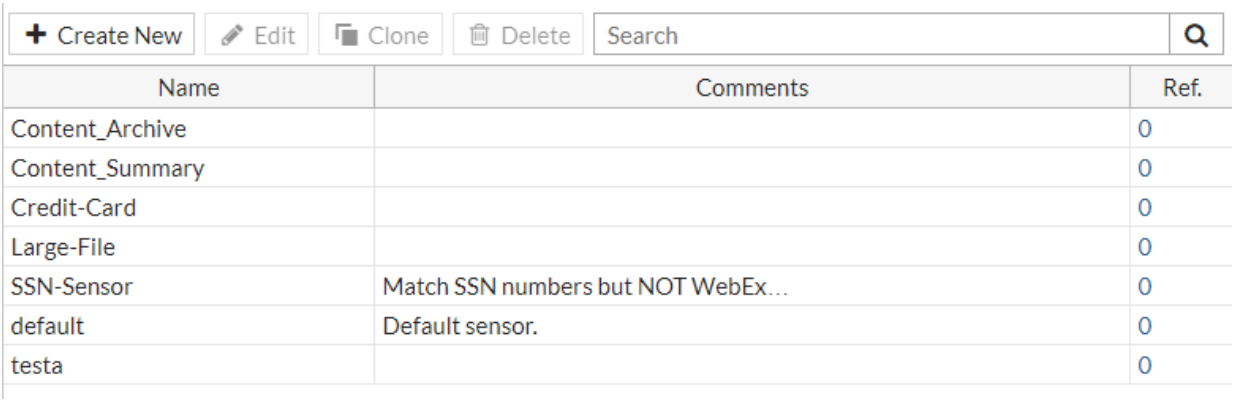
The data leak prevention (DLP) system allows you to prevent sensitive data from leaving your network. After sensitive data patterns are defined, data matching the patterns will either be blocked or logged and then allowed.

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* and select 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).



Name	Comments	Ref.
Content_Archive		0
Content_Summary		0
Credit-Card		0
Large-File		0
SSN-Sensor	Match SSN numbers but NOT WebEx...	0
default	Default sensor.	0
testa		0

The following options are available:

Create New	Create a DLP sensor. See "Create or edit a DLP sensor" on page 217.
Edit	Modify the selected DLP sensor. See "Create or edit a DLP sensor" on page 217.
Clone	Make a copy of a DLP sensor.
Delete	Remove the selected DLP sensor.

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.

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.

Watermark identifier and sensitivity

The watermark 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>
```

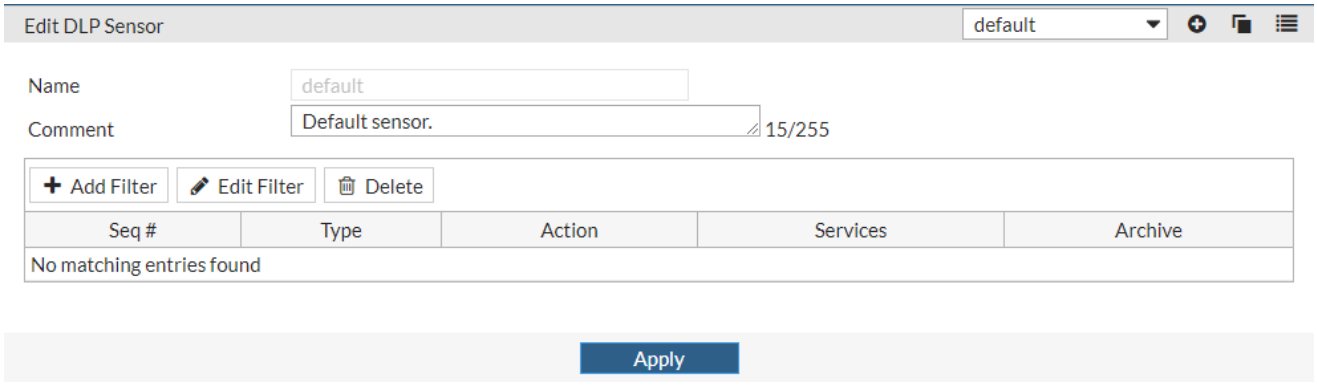
```
watermark_linux_amd64 <options> -d <directory> -i <identifier> -l <sensitivity level>
```

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
```

Create or edit a DLP sensor

To configure the default DLP sensor, go to *Security Profiles* > *Data Leak Prevention*.



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

drop-down list	Select a DLP sensor to view or edit.
Create New icon	Create a new sensor.
Clone icon	Make a copy of a DLP sensor.
List icon	Display a list of DLP sensors. See "Data leak prevention" on page 215.
Name	The name of the sensor.
Comment	An optional description of the sensor.
Add Filter	Add a new filter. See "Create or edit a DLP filter" on page 219.
Edit Filter	Edit the selected filter. See "Create or edit a DLP filter" on page 219.
Delete	Delete the selected filter or filters.
Seq #	The filter sequence number.
Type	The filter type is either *Messages* or *Files*.

Action	The action to take when a match is found: *Allow*, *Log Only*, *Block*, or *Quarantine IP Address*.
Services	Types of services that are filtered.
Archive	Whether archiving is enabled or disabled. See DLP archiving.

To create a DLP sensor:

1. Go to *Security Profiles* > *Data Leak Prevention* and select the *Create New* icon (a plus sign within a circle). 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 *Comment* field.
3. Add filters to the sensor. See "Create or edit a DLP filter" on page 219.
4. Select *OK* to create the new sensor.

To edit a DLP sensor:

1. Go to *Security Profiles* > *Data Leak Prevention*.
2. Select the *List* icon (the farthest right of the three icons in the upper right of the window, resembling a page with some lines on it), select the sensor you want to edit from the list, and then select *Edit*. The *Edit DLP Sensor* window opens.
3. Edit the sensor name and comments as required.
4. Edit, create new, or delete sensor filters as required. See "Create or edit a DLP filter" on page 219.
5. Select *Apply* 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
   end
```

Create or edit a DLP filter

Each DLP sensor must have one or more filters configured within it. Filters can examine traffic for the following:

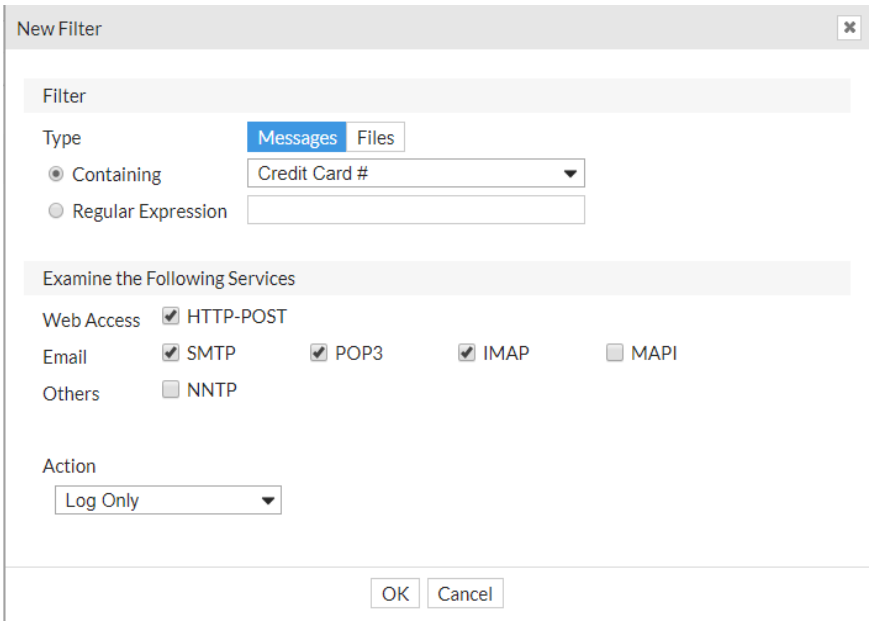
- Known files using DLP fingerprints
- Files of a particular name or type
- Files larger than a specified size
- Data matching a specified regular expression
- Traffic matching an advanced or compound rule

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. Edit the sensor to filter either messages or specific file types.
3. Select the DLP sensor in a security policy.

Select *Add Filter* to open the New Filter window.



To open the Edit Filter window, select a filter and then select *Edit Filter*.

Configure the following settings in the New Filter window or the Edit Filter window and then select *OK*.

Filter	
Type	Select *Messages* or *Files* to filter for specific messages or based on file attributes, respectively.
Containing	Select and then select *Credit Card #* or *SSN* from the drop-down list.
File size over	Select and then enter the maximum file size allowed, in KB. This option is only available when filtering files.
Specify File Types	Select and then select *File Types* and *File Name Patterns* from the drop-down menus provided. See File types. This option is only available when filtering files.
Regular Expression	Select and then enter the pattern that network traffic is examined for. See "Create or edit a DLP filter" on page 221
Encrypted	Select to cause encrypted files to trigger the filter. This option is only available when filtering files.
Examine the Following Services	Select the services whose traffic the filter will examine. This allows resources to be optimized by only examining relevant traffic. The available services are: • *HTTP-POST* and *HTTP-GET* • *SMTP*, *POP3*, *IMAP*, and *MAPI* • *FTP* and *NNTP*

Action	Select an action to take if the filter is triggered from the drop-down list. 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 93.
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).

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 "Appendix A - Perl regular expressions" on page 342. 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)	Encoded Data (binhex)	Packer (aspack)
Archive (arj)	Encoded Data (mime)	Packer (fsg)
Archive (bzip)	Encoded Data (uue)	Packer (petite)
Archive (bzip2)	Executable (elf)	Packer (upx)
Archive (cab)	Executable (exe)	PalmOS Application (prc)
Archive (gzip)	GIF Image (gif)	PDF (pdf)
Archive (lzh)	HTML Application (hta)	PNG Image (png)
Archive (rar)	HTML File (html)	Real Media Streaming (rm)
Archive (tar)	Ignored File Type (ignored)	Symbian Installer System File (sis)
Archive (xz)	Java Application Descriptor (jad)	TIFF Image (tiff)
Archive (zip)	Java Class File (class)	Torrent (torrent)
Audio (avi)	Java Compiled Bytecode (cod)	Unknown File Type (unknown)
Audio (mp3)	JavaScript File (javascript)	Video (mov)
Audio (wav)	JPEG Image (jpeg)	Video (mpeg)
Audio (wma)	Microsoft Active Mime Object (activemime)	Windows Help File (hlp)
Batch File (bat)	Microsoft Office (msoffice)	Windows Installer Package (msi)
BMP Image (bmp)	Microsoft Office (msofficex)	
Common Console Document (msc)		
Encoded Data (base64)		

Content Analysis

Content Analysis is a licensed feature that allows you to detect adult content in real-time. This service is a real-time analysis of the content passing through the FortiProxy unit. Unlike other image analysis tools, this one does not just look for skin tone colors but can detect limbs, body parts, and the position of bodies. After adult content is detected, such content can be optionally blocked or reported.

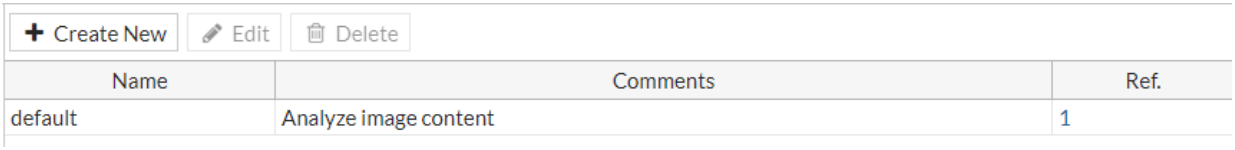
In general, the procedure is similar to the HTTP antivirus scanning procedure.

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 *Security Profiles* > *Content Analysis*.



Right-click on any column heading to select which columns are displayed 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 a Content Analysis profile" on page 223.
Edit	Modify the selected Content Analysis profile. See "Create or edit a Content Analysis profile" on page 223.
Delete	Remove the selected Content Analysis profile.
Name	The name of the Content Analysis profile.
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

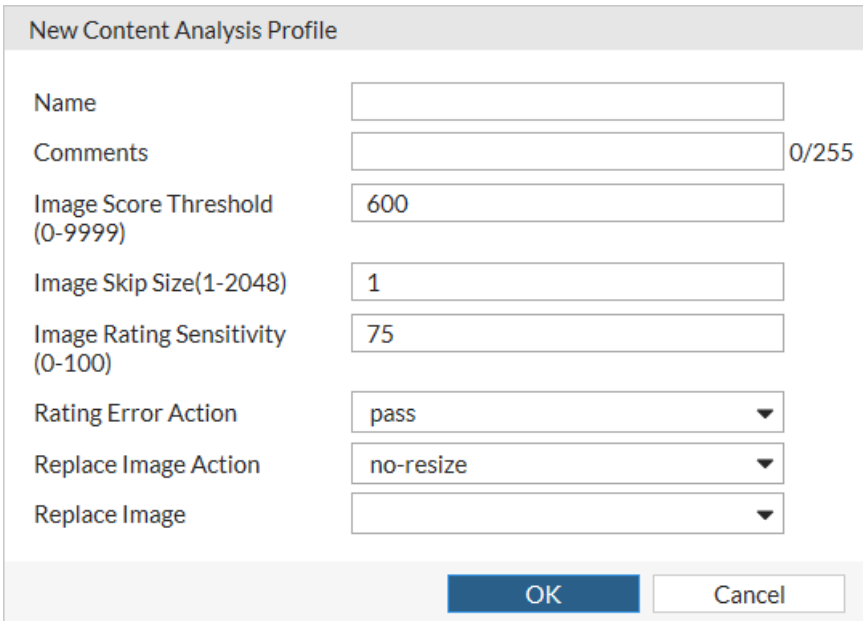
You can use the following debug commands to validate the service licensing and image cache:

`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 a Content Analysis profile

Select *Create New* to open the New Content Analysis Profile window.



To open the Edit Content Analysis Profile window, select a Content Analysis profile and then select *Edit*.

Configure the following settings in the New Content Analysis Profile window or Edit Content Analysis Profile window and then select *OK*:

Name	Enter a name for this profile.
Comments	Optional description of the profile.
Image Score Threshold (0-9999)	Enter a value between 0 and 9,999. 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 the *Image Score Threshold* setting, the *Rating Error Action* is taken. The default value is 600.
Image Skip Size (1-2048)	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.
Image Rating Sensitivity (0-100)	This value determines the strictness of the *Image Score Threshold*. The higher the sensitivity, the more strict it is on the threshold. If you make it too strict, it will block legitimate images. The default value is 75.

Rating Error Action	Set to either *pass* or *block* the image when it exceeds the rating threshold. The default is *pass*.
Replace Image Action	If you choose to display a replacement image by selecting *Yes* for the Replace Image setting, you can set the *Replace Image Action* value to re-size the replacement image to match the original (*resize*) or leave the replacement image at its default size (*no-resize*).
Replace Image	Select whether or not to display a replacement image. To specify the replacement image, go to *System* > *Replacement Messages* and select *Manage Images*. NOTE: The file type must be `.jpg`.

ICAP

FortiProxy supports ICAP. ICAP is a light-weight response/request protocol that allows the FortiProxy unit to offload HTTP and HTTPS traffic to external servers for different kinds of processing.

You can offload HTTP responses or HTTP requests (or both) to the same or different ICAP servers.

ICAP does not appear by default in the GUI. You must enable it in *System* > *Feature Visibility* to display ICAP in the GUI. See "Feature visibility" on page 120.

The ICAP menu allows you to view and configure ICAP profiles and ICAP servers, which can then be applied 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 *Security Profiles* > *ICAP*.

Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

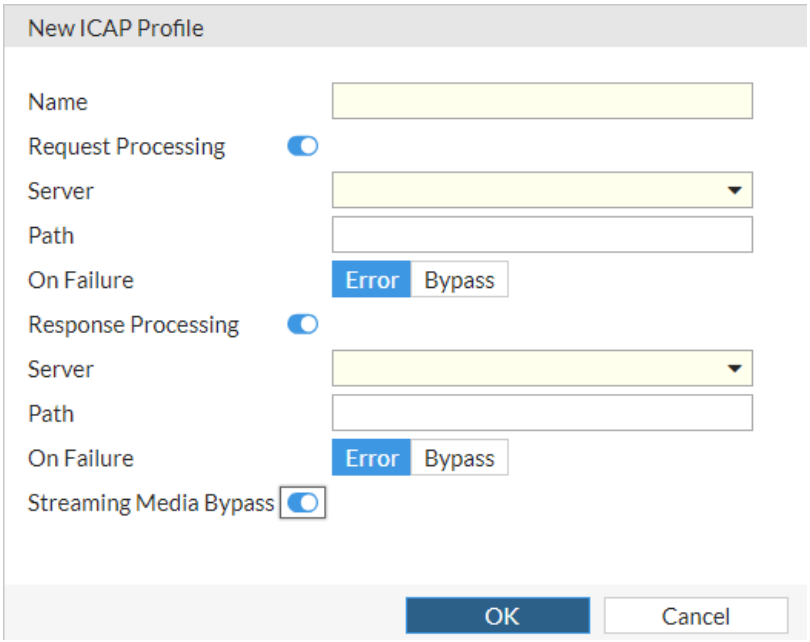
The following options are available:

Create New	Create a new ICAP profile. See "Create or edit an ICAP profile" on page 226.

Edit	Edit an ICAP profile. See "Create or edit an ICAP profile" on page 226.
Delete	Delete a profile or profiles.
Name	The name of the ICAP 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 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 select *Edit*.

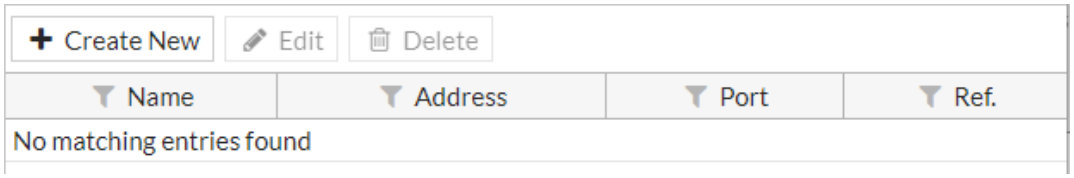
Configure the following settings in the New ICAP Profile window or Edit ICAP Profile window and then select *OK*:

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. If you enable request processing, select a server from the drop-down menu, specify the path on the server to the processing component, and then select the behavior on failure, either *Error* or *Bypass*.

Response Processing	Enable or disable request processing. If you enable request processing, select a server from the drop-down menu, specify the path on the server to the processing component, and then select the behavior on failure, either *Error* or *Bypass*.
Streaming Media Bypass	Enable to allow streaming media to ignore offloading to the ICAP server.

ICAP servers

To view the ICAP server list, go to *Security Profiles* > *ICAP Servers*.



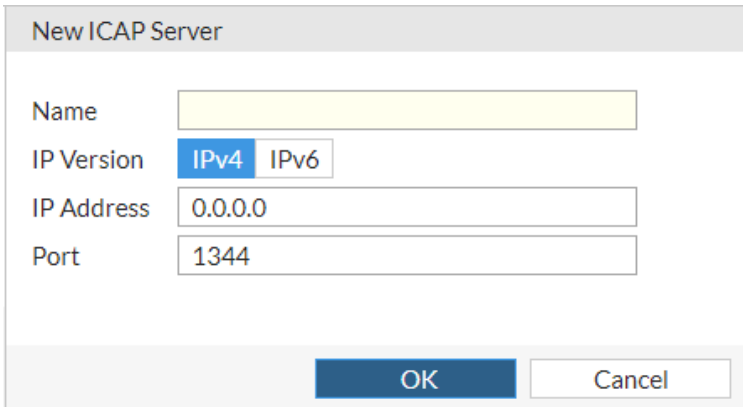
Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a new ICAP server. See "Create or edit an ICAP server" on page 227.
Edit	Edit an ICAP server. See "Create or edit an ICAP server" on page 227.
Delete	Delete an ICAP server or servers.
Name	The name of the ICAP server.
Address	The IP address of the ICAP server.
Port	The port number that the ICAP server is using.
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 server

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



To open the Edit ICAP Server window, select a server and then select *Edit*.

Configure the following settings in the New ICAP Server window or Edit ICAP Server window and then select *OK*:

Name	Enter a name for the ICAP server. After you create an ICAP server, you cannot change the name.
IP Version	Select *IPv4* or *IPv6*.
IP Address/IPv6 Address	Enter the IPv4 or IPv6 address for the ICAP server.
Port	Enter the TCP port number used by the ICAP server, from 1 to 65,535. The default is 1344.

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:

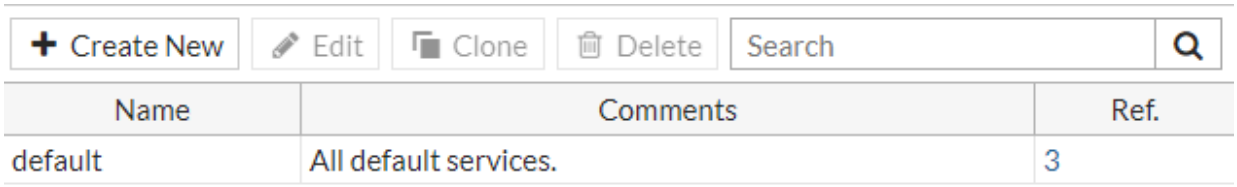
- HTTP
- SMTP
- POP3
- IMAP
- FTP
- MAPI
- DNS

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 *Security Profiles* > *Proxy Options* and select 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).



Right-click on any column heading to select which columns are displayed 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 new proxy option profile. See "Create or edit a proxy option profile" on page 230.
Edit	Modify the selected proxy option profile. See "Create or edit a proxy option profile" on page 230.
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.
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.

To create a new proxy option profile:

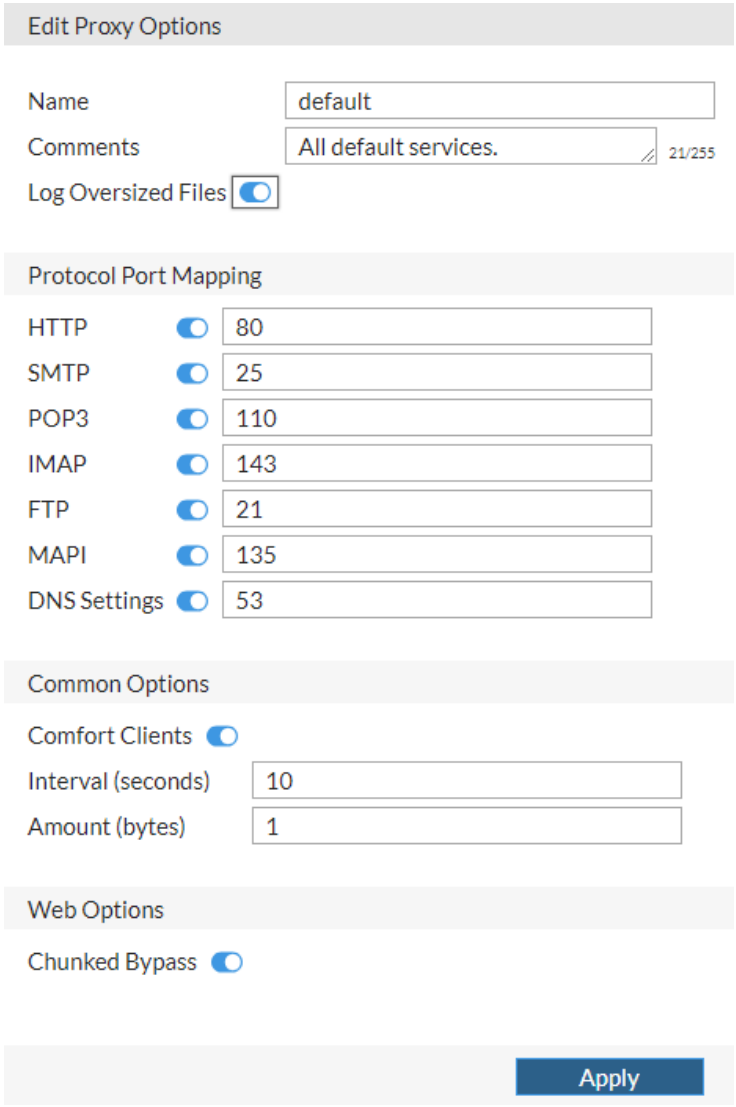
1. Go to *Security Profiles* > *Proxy Options*.
2. Select *Create New* (a plus sign in a circle).
3. Enter the required information and then select *OK* to create the new web filter profile.

To edit a proxy option profile:

1. Go to *Security Profiles* > *Proxy Options*.
2. From the *Edit Proxy Options* page, select the profile you need to edit from the profile drop-down list.
3. Edit the information as required and then select *Apply* to save your changes.

Create or edit a proxy option profile

To configure the default proxy option profile, go to *Security Profiles* > *Proxy Options*. The *Edit Proxy Options* page is displayed.



Configure the following settings and then select *Apply* 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.
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.
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.

To create a new proxy option profile:

1. Go to *Security Profiles* > *Proxy Options*.
2. Select *Create New* (a plus sign in a circle).
3. Enter the required information and then select *OK* to create the new web filter profile.

To edit a proxy option profile:

1. Go to *Security Profiles* > *Proxy Options*.
2. From the *Edit Proxy Options* page, select the profile you need to edit from the profile drop-down list.
3. Edit the information as required and then select *Apply* to save your changes.

SSL/SSH inspection

Individual deep inspection security profiles can be created depending on the requirements of the policy. Depending on the inspection profile selected, you can:

- Configure which Certificate Authority (CA) certificate will be used to decrypt the Secure Sockets Layer (SSL) encrypted traffic.
- Configure whether a specific SSL protocol will be inspected, blocked or bypassed.
- Configure which ports will be associated with which SSL protocols for the purpose of inspection.
- Configure which websites or website categories will be exempt from SSL inspection.
- Identify how to treat invalid, unsupported or untrusted SSL certificates.
- Determine which inspection method will be applied to Secure Shell (SSH)/SSL traffic.

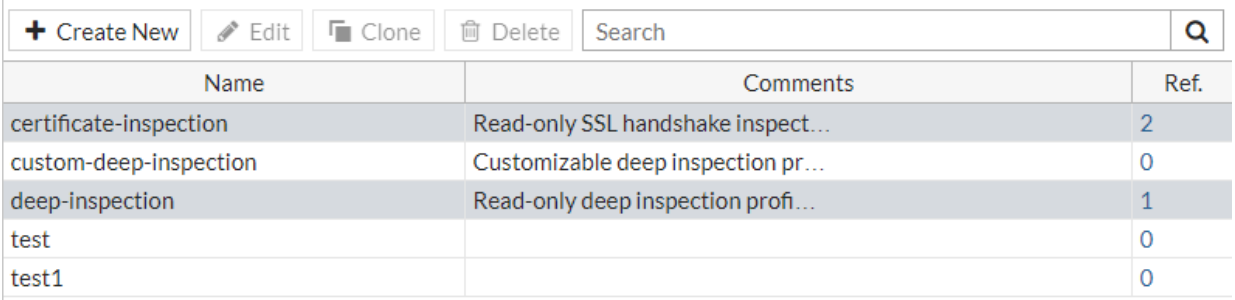
SSL inspection

Secure Sockets Layer (SSL) content scanning and inspection allows you to apply antivirus scanning, web filtering, FortiGuard Web Filtering, and email filtering to encrypted traffic. To perform SSL content scanning and inspection, the FortiProxy unit does the following:

- Intercepts and decrypts HTTPS, IMAPS, POP3S, SMTPS, and FTPS sessions between clients and servers (FortiProxy SSL acceleration speeds up decryption)
- Applies content inspection to decrypted content, including:
  - HTTPS, IMAPS, POP3S, and SMTPS Antivirus, DLP, and DLP archiving
  - HTTPS web filtering and FortiGuard web filtering
  - IMAPS, POP3S, and SMTPS email filtering
- Encrypts the sessions and forwards them to their destinations.

SSL/SSH inspection profile

To view the available SSL/SSH inspection profiles, go to *Security Profiles* > *SSL/SSH Inspection* and then select 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).



Right-click on any column heading to select which columns are displayed 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 SSL/SSH inspection profile. See "Create or edit an SSL/SSH inspection profile" on page 233.
Edit	Modify the selected SSL/SSH inspection profile. See "Create or edit an SSL/SSH inspection profile" on page 233.
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.
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.

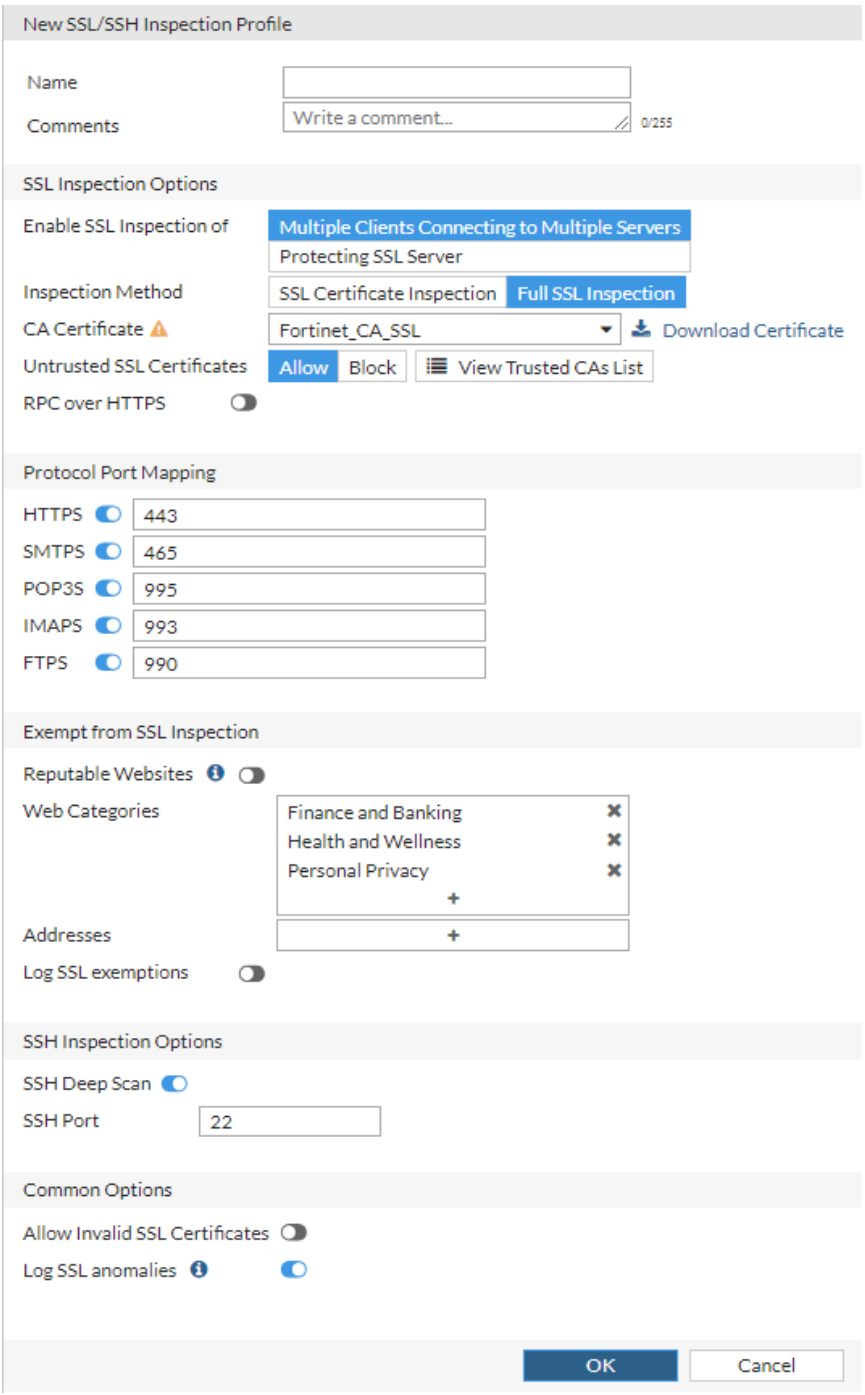
Create or edit an SSL/SSH inspection profile

To configure an SSL/SSH inspection profile, go to *Security Profiles* > *SSL/SSH Inspection*. The *Edit SSL/SSH Inspection Profile* opens. Your FortiProxy unit has two preconfigured SSL/SSH inspection profiles that cannot be edited: certificate-inspection and deep-inspection.

You can create a new profile, modify the custom-deep-inspection profile, or clone and then edit certificate-inspection or deep-inspection profile. The links for the actions are located in the upper right hand corner of the window.

- To view a list of the existing profiles, select 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).
- To clone an existing profile, select the Clone icon (one page behind another), second from the right.
- To create a new profile, select the Create New icon ("+ "symbol), third from the right.
- To view or edit an existing profile, choose it from the drop-down menu field.

To create an SSL/SSH inspection profile, go to *Security Profiles* > *SSL/SSH Inspection* and then select the *Create New* icon (a plus sign).



Configure the following settings and then select *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.

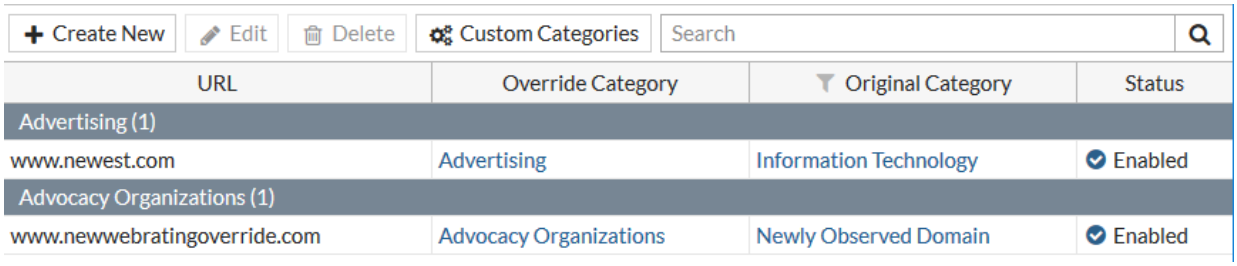
SSL Inspection Options	
Enable SSL Inspection of	• *Multiple Clients Connecting to Multiple Servers*—Select this option for generic policies where the destination is unknown. The *Exempt from SSL Inspection* and *Common Options* options are only available with this option enabled. • *Protecting SSL Server*—Select this option when setting up a profile customized for a specific SSL server with a specific certificate.
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.
Untrusted SSL Certificates	Select *Allow* or *Block* for untrusted SSL certificates. You can also select *View Trusted CAs List* to see which SSL certificates are trusted.
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. Enable a protocol. 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* and *Health and Wellness* have been added because they are most likely to require a specific certificate. Add web categories to be exempt from SSL inspection.
Addresses	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.
Allow Invalid SSL Certificates	Enable this option to allow traffic with invalid certificate.
Log SSL anomalies	Enable this option to record traffic sessions containing untrusted or expired certificates.

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*.



Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

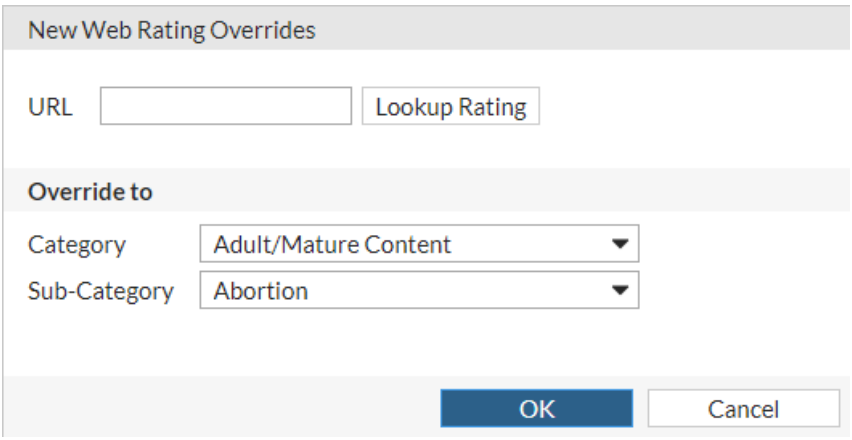
The following options are available:

Create New	Create a web rating override. See "Create or edit a web rating override" on page 237.
Edit	Modify the selected web rating override. See "Create or edit a web rating override" on page 237.
Delete	Remove the selected web rating override.
Custom Categories	Select to create a custom category for groups of URLs. See "Create or edit a custom category" on page 237.
Search	Enter a search term to find in the web rating override list.
URL	The URL of a web site.

Override Category	The new category for the web site.
Original Category	The category that the web site originally belonged to.
Status	Whether the override is enabled or disabled.

Create or edit a web rating override

Select *Create New* to open the *New Web Rating Overrides* window.



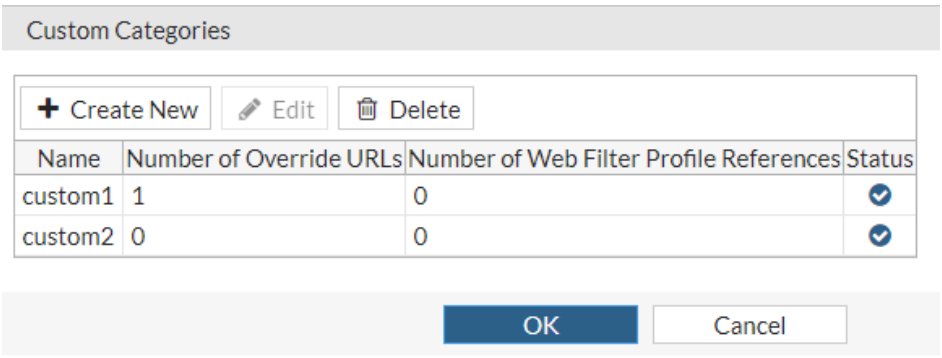
To open the *Edit Web Rating Overrides* window, select a web rating override from the list and then select *Edit*.

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

URL	The URL of a web site.
Lookup Rating	Select this button to find the FortiGuard rating if it exists for the URL you entered.
Category	The new category for the web site.
Sub-Category	A more narrowly defined option within the category that you selected for the web site.

Create or edit a custom category

Select *Custom Categories* to open the *Custom Categories* window.



To create a new category for a group of web sites:

1. Go to *Security Profiles* > *Web Rating Overrides*.
2. Select *Custom Categories*.
   The *Custom Categories* window opens.
3. Select *Create New*.
4. Enter the name of the custom category.
5. Select *OK*.
   To use the new category, select the *Custom Categories* category in the *New Web Rating Overrides* window or the *Edit Web Rating Overrides* 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 select *Edit*.

Custom 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 signatures, go to *Security Profiles* > *Custom Signatures*.

To create a custom IPS signature, see "Create or edit an IPS signature" on page 210.

To create a custom application signature, see "Create or edit an application signature" on page 206.

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 239.

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.

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. If you are using VDOMs, custom signatures appear only in the VDOM in which you create them. You can use the same attack ID for signatures in different VDOMs.

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. If you are using VDOMs, custom signatures appear only in the VDOM in which you create them. You can use the same rule name for signatures in different VDOMs. 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 "Custom signature keywords" on page 244 and "Custom signature keywords" on page 243 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 "Custom signature keywords" on page 243 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.

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.

FortiOS 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 FortiGate unit on the office private network.

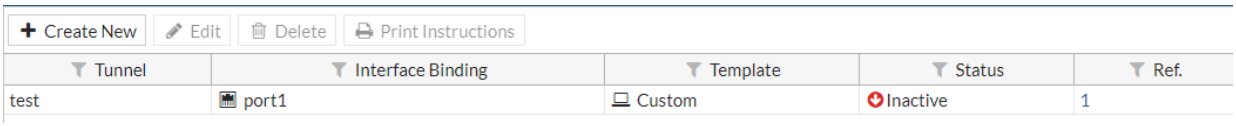
Encapsulation makes this possible. IPsec packets pass from one end of the tunnel to the other and contain data packets that are exchanged between the local user and the remote private network. Encryption of the data packets ensures that any third-party who intercepts the IPsec packets can not access 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

For more information on third-party VPN software, refer to the Fortinet Knowledge Base for more information.

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. By default, the tunnel list indicates the name of the tunnel, its interface binding, the tunnel template used, and the tunnel status. If you right-click on the table header row, you can include columns for comments, IKE version, mode (aggressive vs main), phase 2 proposals, and reference number. The tunnel list page also includes the option to create a new tunnel, as well as the options to edit or delete a highlighted tunnel.



Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

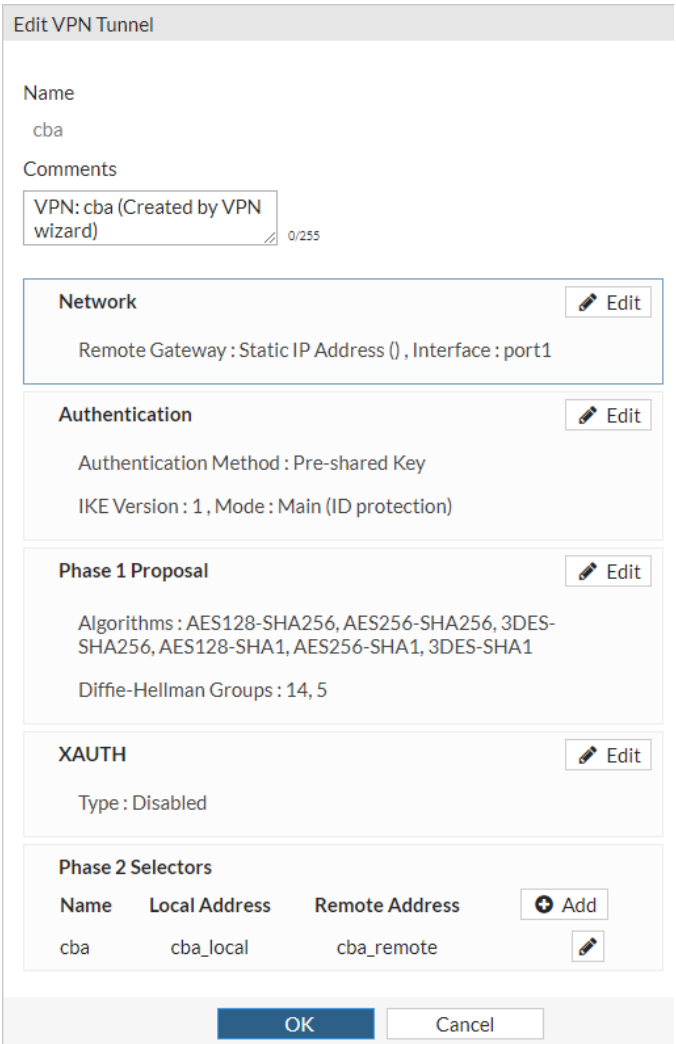
The following options are available:

Create New	Run the IPsec Wizard and create an IPSec tunnel. See "IPsec wizard" on page 263.
Edit	Edit an IPsec tunnel. See "Edit an IPsec tunnel" on page 255.
Delete	Delete the selected IPsec tunnel.
Print Instructions	Select this option to print instructions for creating an IPsec tunnel.
Tunnel	The name of the IPsec tunnel.
Interface Binding	Select the name of the interface through which remote peers connect to the FortiGate unit that is managed by the FortiProxy unit.
Template	The template is *Site to Site*, *Remote Access*, or *Custom*: • *Site to Site*—Static tunnel between a FortiGate unit managed by a FortiProxy unit and a remote FortiGate unit or a static tunnel between a FortiGate unit managed by a FortiProxy unit and a remote Cisco firewall. • *Remote Access*—On-demand tunnel for users using the FortiClient software or Cisco IPsec client, for iPhone/iPad users using the native iOS IPsec client, or for Android users using the native L2TP/IPsec client. • *Custom*—No template. See "Create a custom VPN tunnel" on page 259.
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.

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 select *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, select *OK*.

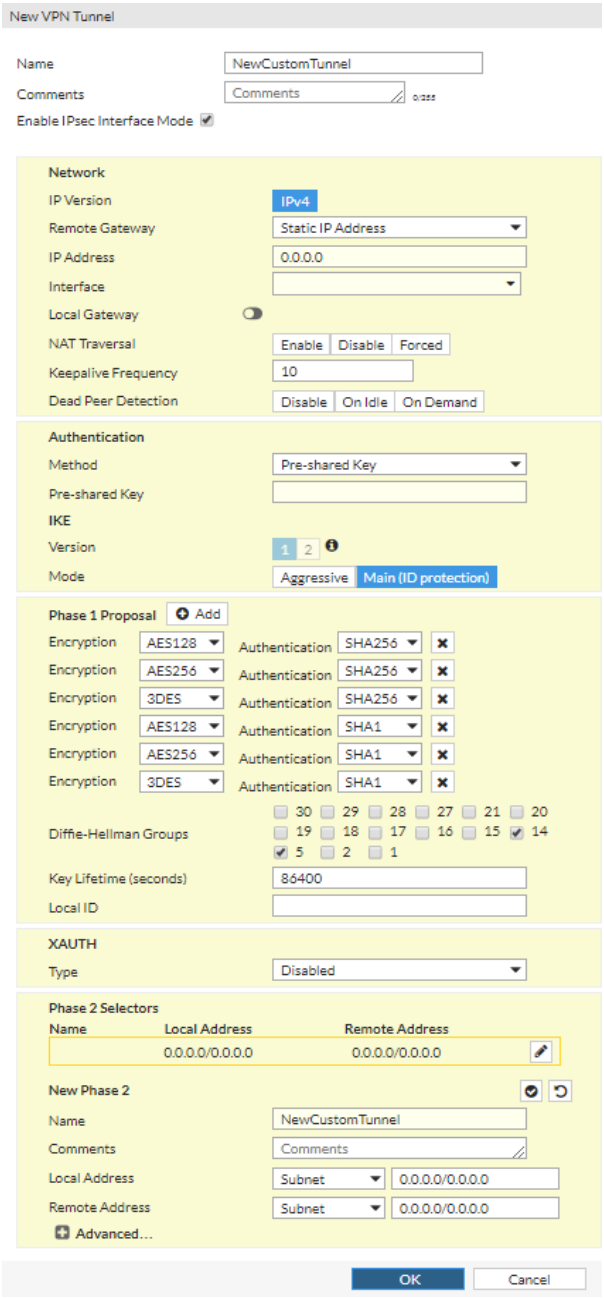
Name	The name of the IPsec tunnel cannot be changed.
Comments	An optional description of the IPsec tunnel.
Network	Select *Edit* to make changes.
IP Version	This option is set to *IPv4*.
Remote Gateway	This option is set to *Static IP Address* for a remote peer that has a static IP address.
IP Address	Enter the IP address of the remote peer.
Interface	Select the name of the interface through which remote peers connect to the FortiGate unit that is managed by 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 FortiGate unit that is managed by a FortiProxy unit. and the VPN peer or client. The local FortiGate 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 FortiGate 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.
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 FortiGate unit managed by a FortiProxy unit will use to authenticate itself to the remote peer or dialup 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 FortiGate unit managed by a 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 *Edit* to make changes. 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.
XAUTH	Select *Edit* to make changes.

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.
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 *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.

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.



Configure the following settings and then select *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 FortiGate unit that is managed by 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 FortiGate unit that is managed by a FortiProxy unit. and the VPN peer or client. The local FortiGate 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 FortiGate 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 FortiGate unit managed by a FortiProxy unit will use to authenticate itself to the remote peer or dialup 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 FortiGate unit managed by a 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 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*, *Remote Access*, or *Custom*: • *Site to Site*—Static tunnel between a FortiGate unit managed by a FortiProxy unit and a remote FortiGate unit or a static tunnel between a FortiGate unit managed by a FortiProxy unit and a remote Cisco firewall. • *Remote Access*—On-demand tunnel for users using the FortiClient software or Cisco IPsec client, for iPhone/iPad users using the native iOS IPsec client, or for Android users using the native L2TP/IPsec client. • *Custom*—No template. See "Create a custom VPN tunnel" on page 259.
Remote Device type	If you selected *Site to Site*, select *FortiGate* or *Cisco*. If you selected *Remote Access*, select *FortiClient VPN for OSX, Windows, and Android*; *iOS Native*; *Android Native*; *Windows Native*; or *Cisco Client*.
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*.

4. 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*.
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 FortiGate unit managed by a FortiProxy unit will use to authenticate itself to the remote peer or dialup 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 FortiGate unit managed by a FortiProxy unit will use to authenticate itself.
User Group	If you selected *Remote Access* for the template type, select a user group from the drop-down list.

6. Configure the policy and routing settings:

Local Interface	Select the name of the interface through which remote peers or dialup clients connect to the FortiGate unit managed by a 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.

Local Address	If you selected *Remote Access* for the template type, select + and then select one of more local addresses.
Client Address Range	If you selected *Remote Access* for the template type, enter address range for the client.
Subnet Mask	If you selected *Remote Access* for the template type, enter a subnet mask.
DNS Server	If you selected *Remote Access* for the template type, select *Use System DNS* or *Specify*. If you select Specify, enter the IP address of the DNS server.
Enable IPv4 Split Tunnel	If you selected *Remote Access* for the template type, enable or disable this option. Enabled by default, this option enables the FortiClient user to use the VPN to access internal resources while other Internet access is not sent over the VPN, alleviating potential traffic bottlenecks in the VPN connection. Disable this option to have all traffic sent through the VPN tunnel.
Allow Endpoint Registration	If you selected *Remote Access* for the template type, enable or disable this option. When selected, the FortiGate unit managed by a FortiProxy unit requests a registration key from FortiClient before a connection can be established.

8. If you selected *Site to Site* for the template type, select *Create*. If you selected *Remote Access* for the template type, select *Next*.
9. If you selected *Remote Access* for the template type, configure the client options and then select *Create*:

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.
Auto Connect	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.
Always Up (Keep Alive)	When enabled, if the user selects this option, the FortiClient connection will not shut down. When not selected, during periods of inactivity, FortiClient will attempt to stay connected every three minutes for a maximum of 10 minutes.

11. Select *Add Another* to start at the beginning of the IPsec Wizard or select *Show Tunnel List* to see the available IPsec tunnels.

IPsec tunnel templates

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 Templates* to see a list and descriptions of these templates:

- Dialup - FortiClient (Windows, Mac OS, Android)
- Site to Site - FortiProxy
- Dialup- FortiProxy

- Dialup - iOS (Native)
- Dialup - Android (Native L2TP/IPsec)
- Dialup - Windows (Native L2TP/IPsec)
- Dialup - Cisco IPsec Client
- Site to Site - Cisco
- Dialup - Cisco Firewall

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 FortiGate unit managed by a 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.

Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

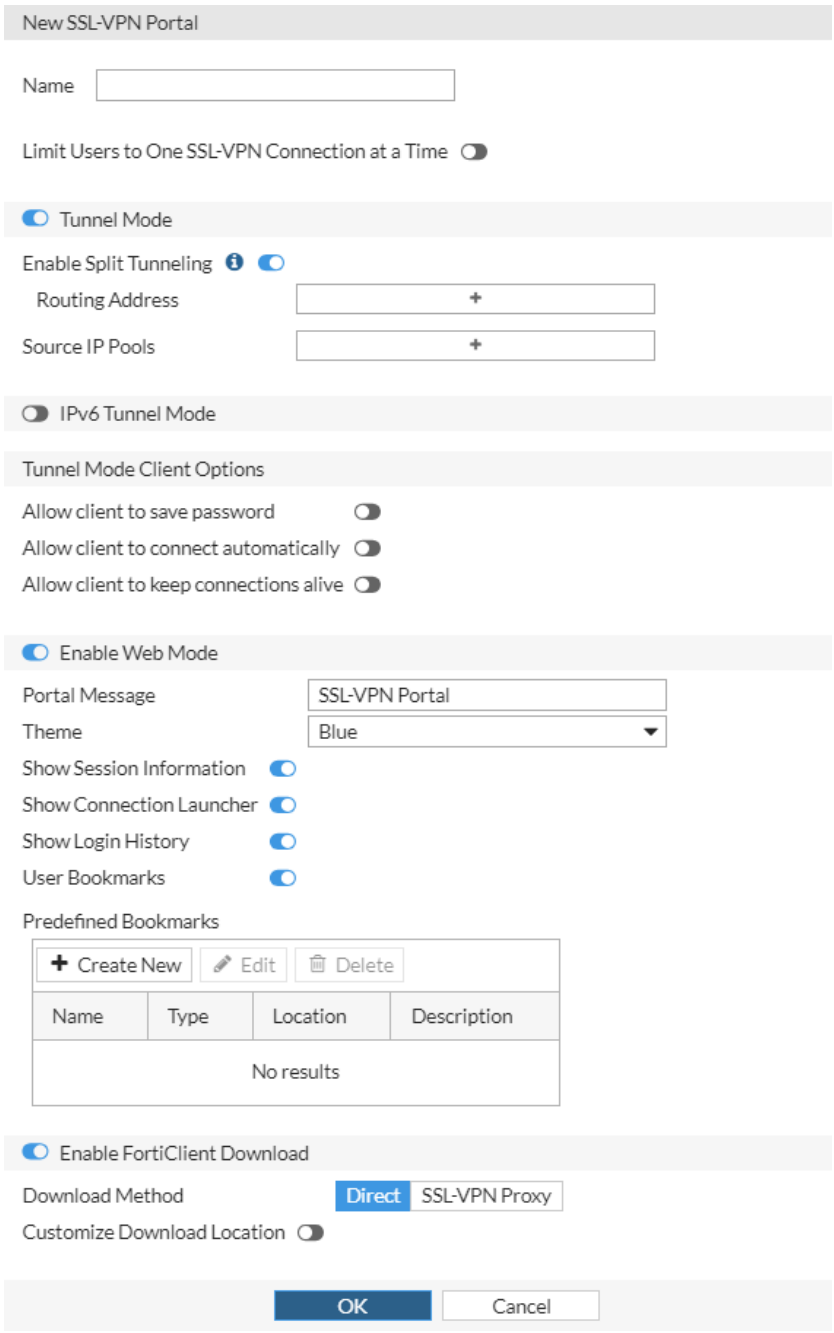
The following options are available:

Create New	Create an SSL-VPN portal. See "Create or edit an SSL-VPN portal" on page 267.
Edit	Edit an SSL-VPN portal. See "Create or edit an SSL-VPN portal" on page 267.
Delete	Delete an SSL-VPN portal.
Name	The name for the portal.
Tunnel Mode	Whether this portal is using tunnel mode.
IPv6 Tunnel Mode	Whether this portal is using IPv6 tunnel mode.
Web Mode	Whether this portal is using web-only 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 select *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 select *OK*:

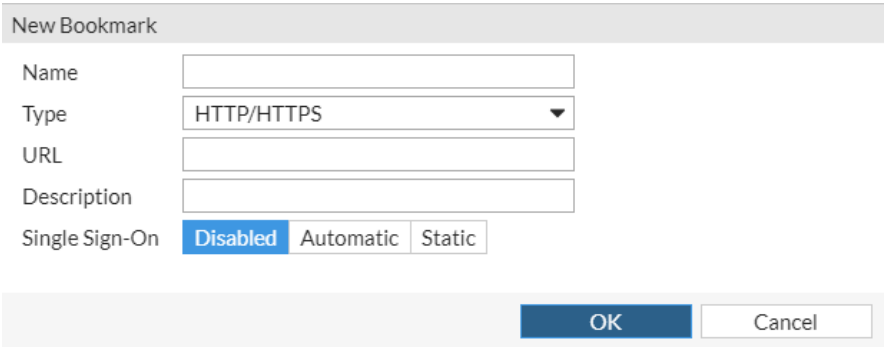
Name	The name for the portal. After you create the SSL-VPN portal, the name cannot be changed.
Limit Users to One SSL-VPN Connection at a Time	You can set the SSL VPN tunnel such that each user can only log into the tunnel one time concurrently per user per login. That is, after logging into the portal, they cannot go to another system and log in with the same credentials again. This option is disabled by default.
Tunnel Mode	Move the slider to determine how tunnel-mode clients are assigned IPv4 addresses.
Enable Split Tunneling	Select this option so that the VPN carries only the traffic for the networks behind the FortiGate unit managed by the FortiProxy unit. The user's other traffic follows its normal route.
Routing Address	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 this option so that the VPN carries only the traffic for the networks behind the FortiGate unit managed by the FortiProxy unit. The user's other traffic follows its normal route.
IPv6 Routing Address	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).
Enable Web Mode	Move the slider to enable 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.
Create New	Create a bookmark. See "Create or edit a bookmark" on page 269.
Edit	Edit a selected bookmark. See "Create or edit a bookmark" on page 269.
Delete	Delete a selected bookmark.
Enable FortiClient Download	Move this slider 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	Move this slider to change the download location.
Windows	Move this slider to specify the Windows download location.
Mac	Move this slider to specify the Mac download location.

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.



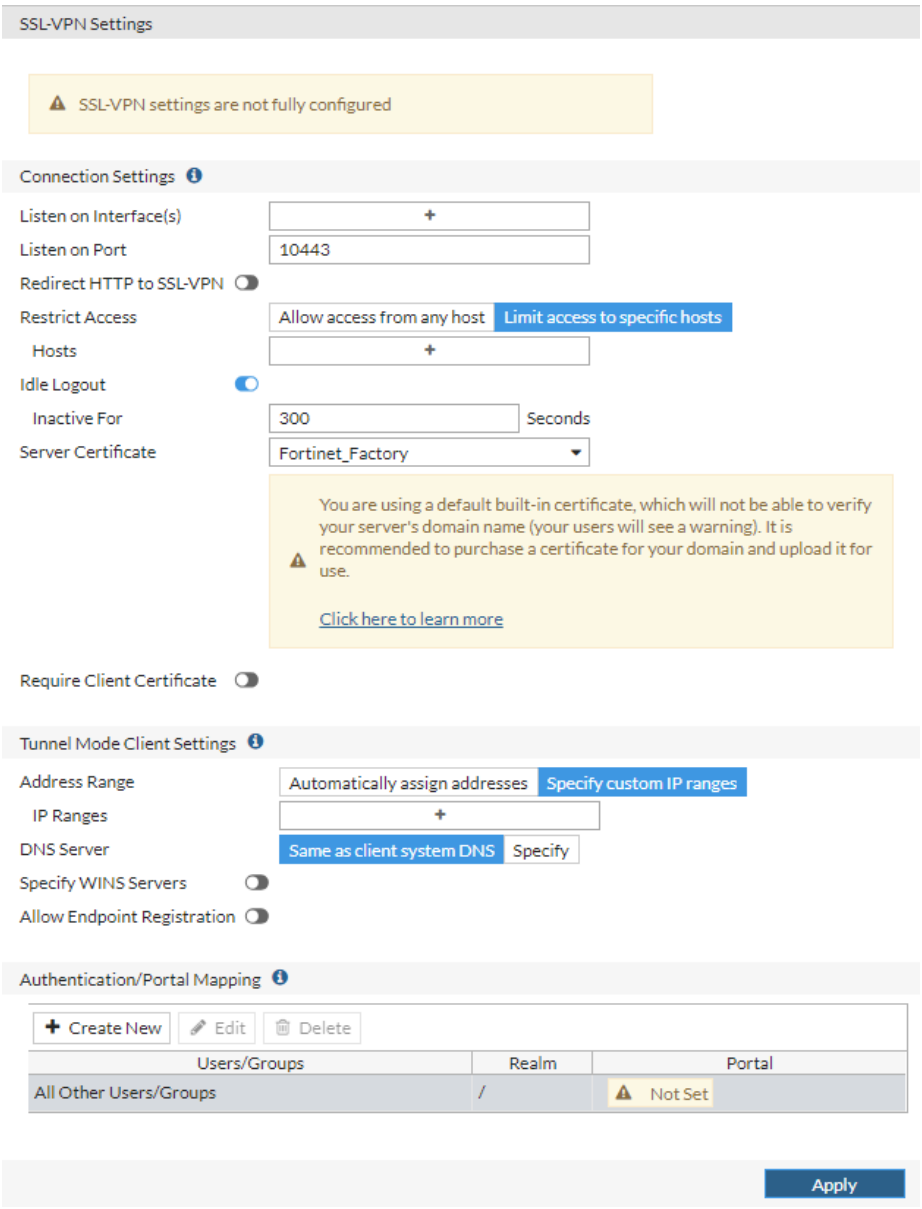
Select bookmark from the list and then select *Edit* to open the *Edit Bookmark* page.

Configure the following settings in the *New Bookmark* page or *Edit Bookmark* page and then select *OK*:

Name	Enter a name for the bookmark.
Type	Select the type of link from the drop-down list. *Telnet*, *VNC*, and *RDP* require a browser plugin. *FTP* replaces the bookmarks page with an HTML file-browser.
URL	Enter the IP address source.
Description	Enter a brief description of the link.
Single Sign-On	Select *Automatic* or *Static* if you want to use Single Sign-On (SSO) for any links that require authentication. When including a link using SSO, be sure to use the entire URL. For example, `http://10.10.1.0/login`, rather than just the IP address.
SSO Credentials	If you selected *Automatic* or *Static* for SSO, select whether you want to use the same credentials as the *SSL-VPN Login* or *Alternative* credentials.
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.
SSO Form Data	Enter the SSO form data. Select *Add* for additional rows.

SSL-VPN settings

To configure the basic SSL-VPN settings for encryption and login options, go to *VPN* > *SSL-VPN Settings*.



Configure the following settings and then select *Apply:*

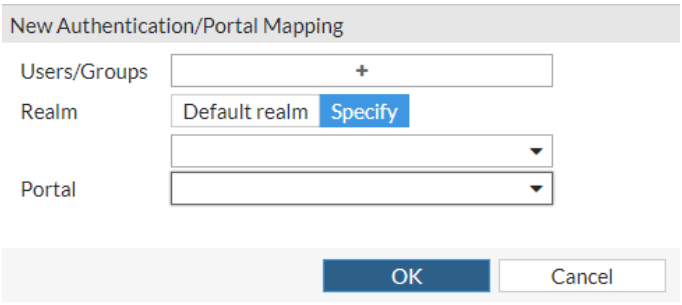
Listen on Interface(s)	Select + to choose one or more interfaces that the FortiProxy unit will use to listen for SSL-VPN tunnel requests. This is generally your external interface.
Listen on Port	Enter the port number for HTTPS access.
Redirect HTTP to SSL-VPN	Move the slider to redirect the admin HTTP 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	Move the slider 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_CA_SSLProxy), the FortiGate unit offers its built-in certificate from Fortinet to remote clients when they connect. A warning appears that recommends you purchase a certificate for your domain and upload it for use.
Require Client Certificate	Select to use group certificates for authenticating remote clients. When the remote client initiates a connection, the FortiGate 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.

Allow Endpoint Registration	Move the slider so that FortiClient registers with the FortiProxy unit when connecting.
Create New	Creates an authentication/portal mapping. See "Create or edit an authentication/portal mapping" on page 273.
Edit	Modifies the selected authentication/portal mapping. See "Create or edit an authentication/portal mapping" on page 273.
Delete	Removes the selected authentication/portal mapping.

Create or edit an authentication/portal mapping

Select *Create New* to open the New Authentication/Portal Mapping page.



Configure the following settings and then select *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 267.

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. Select *Apply*.

To view the list of personal bookmarks, go to *VPN* > *SSL-VPN Personal Bookmarks*.

Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

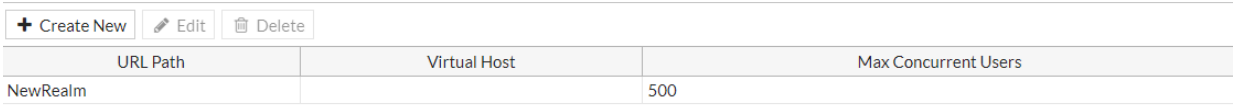
The following options are available:

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.
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*.



Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

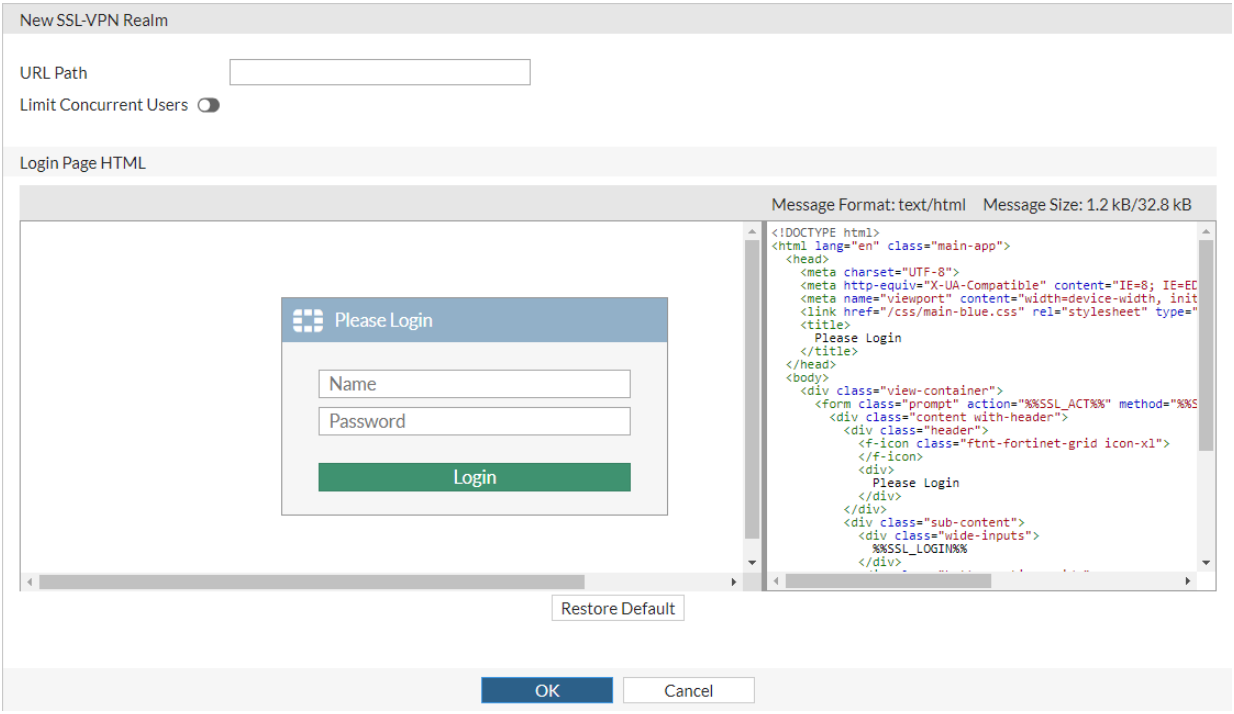
The following options are available:

Create New	Create an SSL-VPN realm. See "Create or edit an SSL-VPN realm" on page 275.
Edit	Modify the selected SSL-VPN realm. See "Create or edit an SSL-VPN realm" on page 275.
Delete	Delete the selected SSL-VPN realm.

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.

Create or edit an SSL-VPN realm

Select *Create New* to open the New SSL-VPN Realm page.



Select an SSL-VPN realm and then select *Edit* to open the Edit SSL-VPN Realm page.

Configure the following settings in the New SSL-VPN Realm page or Edit SSL-VPN Realm page and then select *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.
Login Page HTML	Enter replacement HTML for SSL-VPN login page.
Restore Default	Select this option to undo your changes.

To configure SSL-VPN realms using the GUI:

1. Go to *System* > *Feature Visibility* and move the slider for *SSL-VPN Realms* to make the feature visible.
2. 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.
3. Configure the settings and select *OK*.
4. 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 group(s) and the associated realm.

User & device

The *User & Device* 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:

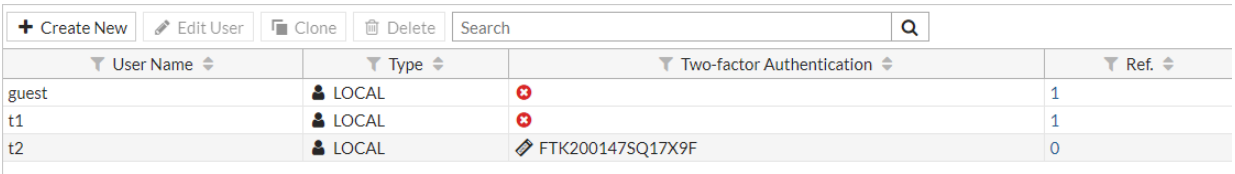
User definition

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 & Device* > *User Definition* and select *Create New* to create new users with the *Users/Groups Creation Wizard*.

To configure users, go to *User & Device* > *User Definition*.



Right-click on any column heading to select which columns are displayed 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 new user. You can also use the wizard to create new groups. See "Create a user" on page 278.
Edit User	Edit a user. See "Edit a user" on page 280.
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 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 282.
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 294.

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 282.
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 297
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 282.
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 a new LDAP server and then select *Next*. To create a new LDAP server, select the *Create New* icon in the drop-down menu, enter the required information, and then select *OK*. For information on LDAP servers, see "Create or edit an LDAP server" on page 291.
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 FSSO agent, go to *User & Device* > *Single Sign-On* and select *Create New*; see "Create or edit a single sign-on server" on page 287 for details.
   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. Select *OK* in the confirmation dialog box.

To create an AD group:

```
config user adgrp
   edit <AD_group_name>
      set server-name <FSSO_agent_name>
   end
```

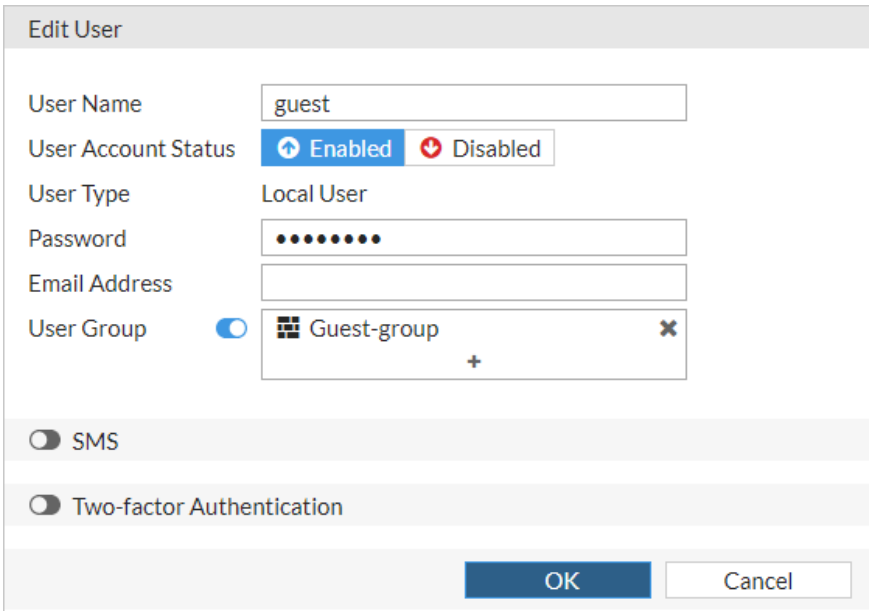
For example:

```
config user adgrp
   edit adgroup1
      set server-name NewFSSOserver
   end
```

Edit a user

To edit a user:

1. Select the user you want to edit and then select *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. Select *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

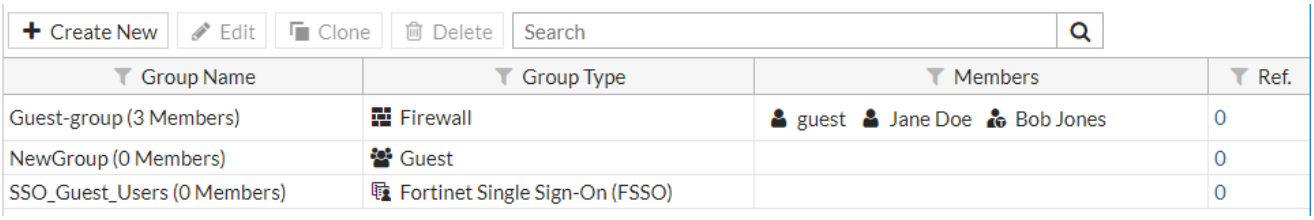
There are four types of user groups:

- 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 & Device* > *User Groups*.



Right-click on any column heading to select which columns are displayed 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:

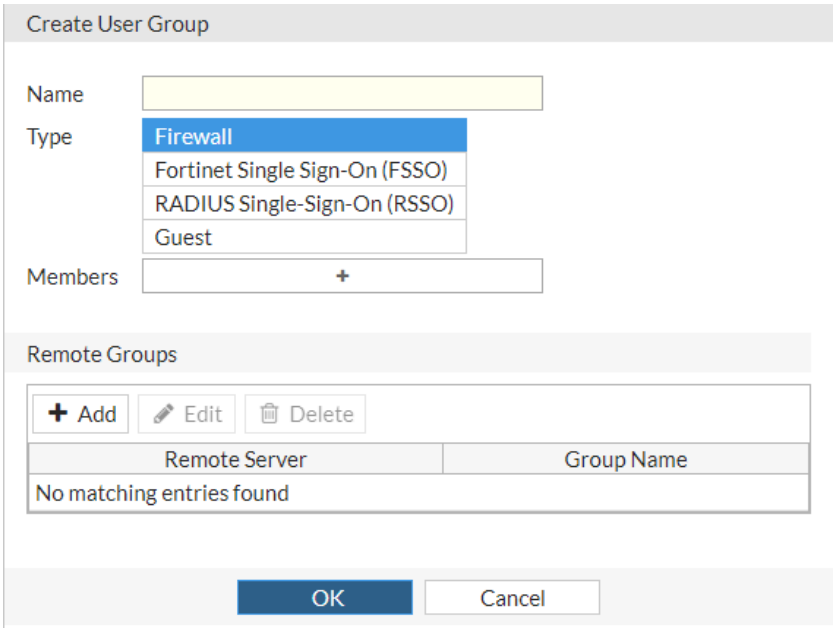
Create New	Create a new user group. See "Create or edit a user group" on page 282.
Edit	Edit a user group. See "Create or edit a user group" on page 282.
Clone	Make a copy of a user group.
Delete	Delete a group or groups.
Search	Enter a search term to search the user group list.
Group Name	The name of 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 new 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.
Members	If you selected a Firewall user group, select users to add to the group from the drop-down list.

Remote groups	If you selected a Firewall user group, add remote authentication servers to the group. Select *Add* and then select the server from the drop-down menu. If required, select a group for the server.
Fortinet Single Sign-On (FSSO)	This type of group can be selected in any security policy that requires FSSO authentication.
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. Select *OK* to create the new user group.

To edit a user group:

1. Select the group you want to edit and then select *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 select *OK* to apply your changes.

Guest management

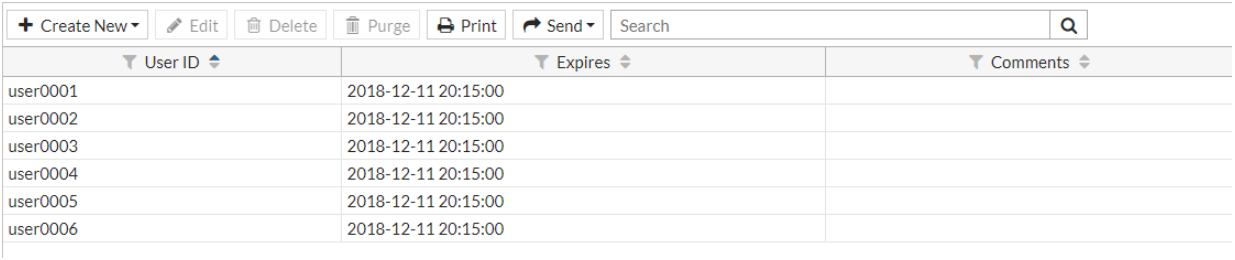
Visitors to your premises might need user accounts on your network for the duration of their stay. If you are hosting a large event such as a conference, you might need to create many such temporary accounts. The FortiProxy Guest Management feature is designed for this purpose.

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 & Device* > *Guest Management*.



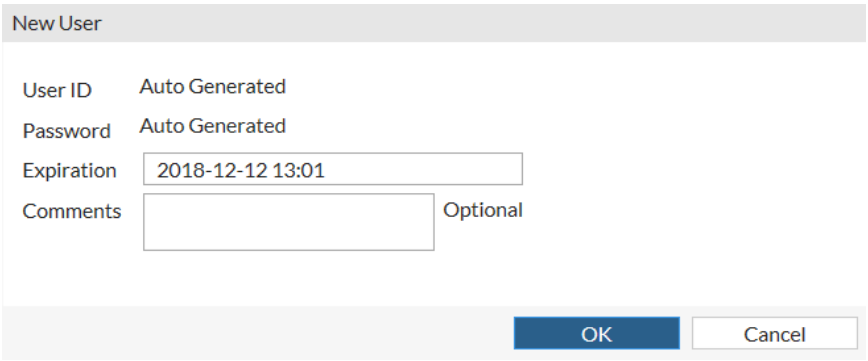
Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New > User	Create a guest user account. See "Create or edit a guest user account" on page 285.
Create New > Multiple Users	Create more than one guest user account at the same time. See "Create multiple guest user accounts" on page 286.
Edit	Modify a guest user account. See "Create or edit a guest user account" on page 285.
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.



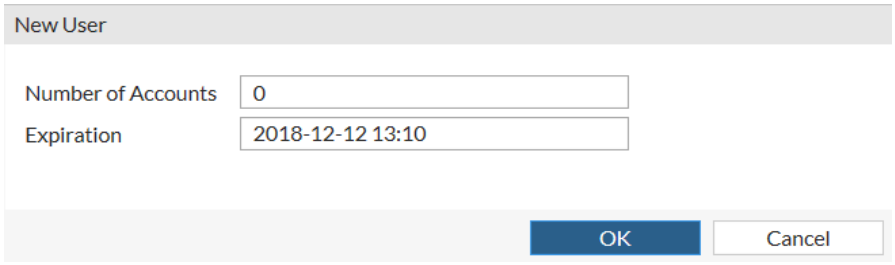
Select a guest user account and then select *Edit* to open the *Edit User* page.

Configure the following settings in the *New User* page or *Edit User* page and then select *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 select *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.

Single sign-on

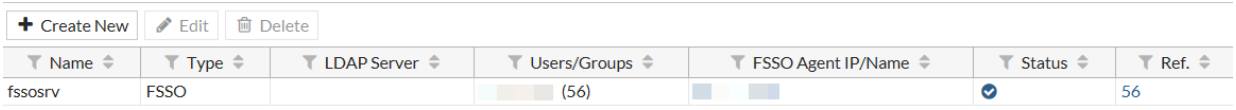
Fortinet units use security policies to control access to resources based on user groups configured in the policies. Each Fortinet user group is associated with one or more Directory Service user groups. When a user logs in to the Windows or Novell domain, an FSSO agent sends the user's IP address, and the names of the Directory Service user groups that the user belongs to, to the FortiProxy unit.

The FSSO agent has two components that must be installed on your network:

- The domain controller agent must be installed on every domain controller to monitor user logins and send information about them to the collector agent.
- The collector agent must be installed on at least one domain controller to send the information received from the domain controller agents to the Fortinet unit. Alternately, a FortiAuthenticator server can take the place of the collector agent in an FSSO polling mode configuration.

The unit uses this information to maintain a copy of the domain controller user group database. Because the domain controller authenticates users, the unit does not perform authentication. It recognizes group members by their IP address. You must install the FSSO agent on the network and configure the unit to retrieve information from the Directory Service server.

To manage single sign-on (SSO) servers, go to *User & Device* > *Single Sign-On*.



Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

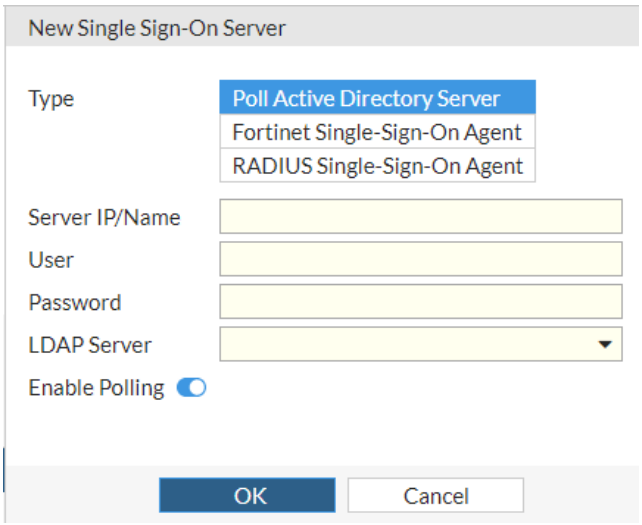
The following options are available:

Create New	Create an FSSO server. See "Create or edit a single sign-on server" on page 287.
Edit	Modify an FSSO server. See "Create or edit a single sign-on server" on page 287.
Delete	Remove an FSSO server or servers.
Name	The name of the FSSO server.
Type	An icon representing the type of server. Hover your cursor over the icon to view the type.
LDAP Server	The LDAP server associated with the FSSO server.
Users/Groups	The users and groups associated with the server.
FSSO Agent IP/Name	The IP address or name of the FSSO agent.
Status	The status of the FSSO 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 single sign-on server

To create a new SSO server:

1. In the single sign-on server list, select *Create New* from the toolbar.
   The *New Single Sign-On Server* page opens.



2. Select the type of server that will be created in the *Type* area. One of: *Poll Active Directory Server*, *Fortinet Single Sign-On Agent*, or *RADIUS Single Sign-On Agent*.

Only one RADIUS single sign-on agent can be created on the FortiProxy device.

3. Enter the following information, depending on the type selected:

Poll Active Directory Server	
Server IP/Name	If you selected *Poll Active Directory Server*, enter the server name or IP address.
User	If you selected *Poll Active Directory Server*, enter the user name.
Password	If you selected *Poll Active Directory Server*, enter the password for the user.
LDAP Server	If you selected *Poll Active Directory Server*, select an LDAP server from the drop-down list to access the Directory Service. To add an LDAP server, see "Create or edit an LDAP server" on page 291.
Enable Polling	If you selected *Poll Active Directory Server*, select this option to enable polling.
Users/Groups	If you selected *Poll Active Directory Server* and selected an LDAP server, view or edit the users, groups, and organizational units associated with the server.
Fortinet Single-Sign-On Agent	
Name	If you selected *Fortinet Single-Sign-On Agent*, enter a name for the agent.

Primary FSSO Agent	If you selected *Fortinet Single-Sign-On Agent*, enter the server IP address or name for the primary agent. Then enter the password in the *Password* field. Select + to add up to four more FSSO agents. Enter the IP address or name of the Directory Service server where the collector agent is installed. The maximum number of characters is 63. Then enter the password for the collector agent. This is required only if you configured your FSSO agent collector agent to require authenticated access.
Collector Agent AD access mode	If you selected *Fortinet Single-Sign-On Agent*, select *Standard* or *Advanced* for the Collector agent AD access mode. The Collector agent has two ways to access Active Directory user information. The main difference between Standard and Advanced mode is the naming convention used when referring to user name information. Standard mode uses the regular Windows convention: Domain\Username. Advanced mode uses LDAP convention: CN=User, OU=Name, DC=Domain. If there is no special requirement to use LDAP—best practices suggest you set up FSSO in Standard mode. This mode is easier to set up and is usually easier to maintain and troubleshoot. Standard and advanced modes have the same level of functionality with the following exceptions: • Users have to create Group filters on the Collector agent. This differs from Advanced mode where Group filters are configured from the FortiProxy unit. Fortinet strongly encourages users to create filters from CA. • Advanced mode supports nested or inherited groups. This means that a user can be a member of multiple monitored groups. Standard mode does not support nested groups so a user must be a direct member of the group being monitored.
Users/Groups	If you selected *Fortinet Single-Sign-On Agent*, select Apply & Refresh to update the Collector agent group filters and then select *View* to see the Collector agent group filters. This option is only available if you selected the *Standard* mode.
LDAP Server	If you selected *Fortinet Single-Sign-On Agent*, select an LDAP server from the drop-down list to access the Directory Service. After you select an LDAP server, you can view or edit the users, groups, and organizational units associated with the server. This option is available only if you selected the *Advanced* mode.
RADIUS Single-Sign-On Agent	
Name	If you selected *RADIUS Single Sign-On Agent*, enter the name of the RADIUS single-sign-on agent.

Use RADIUS Shared Secret	If you selected *RADIUS Single Sign-On Agent*, enable *Use RADIUS Shared Secret* to use the RADIUS shared secret and then enter the shared secret in the field.
Send RADIUS Responses	If you selected *RADIUS Single Sign-On Agent*, enable *Send RADIUS Responses* to send RADIUS responses.

4. Select *OK* to create the new single sign-on server.

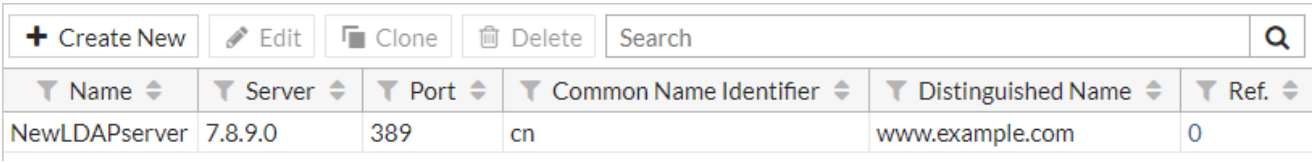
To edit an SSO server:

1. Select the server you want to edit and then select *Edit* from the toolbar or double-click on the address group. The *Edit Single Sign-On Server* window opens.
2. Edit the server information as required and select *OK* to apply your changes.

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 & Device* > *LDAP Servers*.



Right-click on any column heading to select which columns are displayed 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:

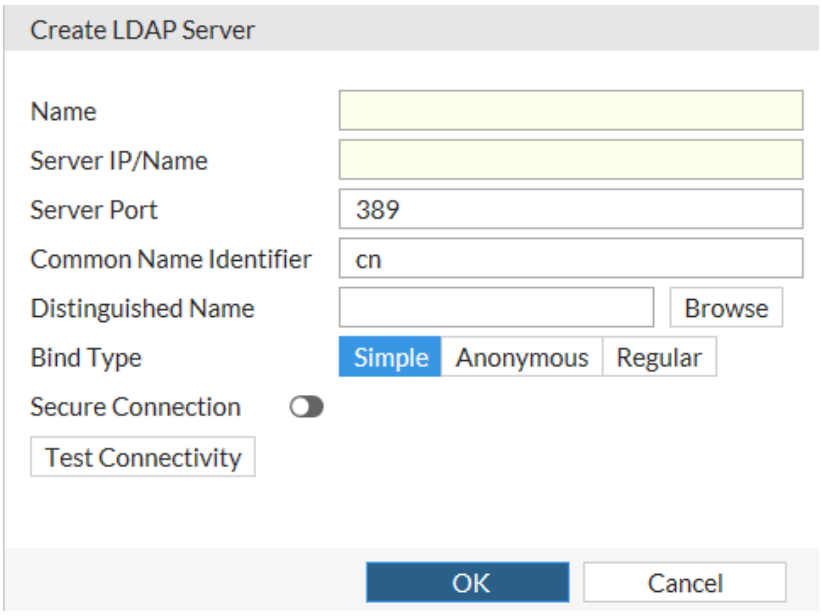
Create New	Create an LDAP server. See "Create or edit an LDAP server" on page 291.
Edit	Modify an LDAP server. See "Create or edit an LDAP server" on page 291.
Clone	Make a copy of an LDAP server.
Delete	Remove a server or servers.
Search	Enter a search term to find in the LDAP server list.
Name	The 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. Select *OK* to create the new LDAP server.

To edit an LDAP server:

1. Select the LDAP server you want to edit and then select *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 select *OK* to apply your changes.

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

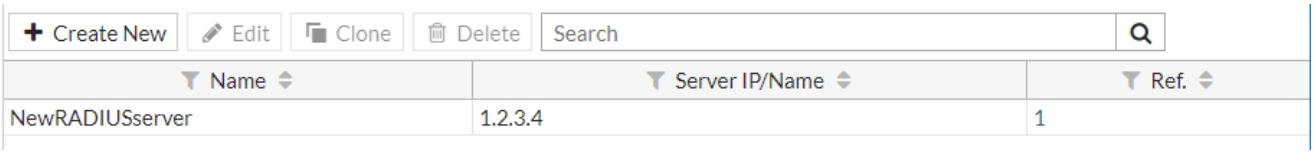
RADIUS servers are currently defined by RFC 2865 (RADIUS) and RFC 2866 (Accounting). They listen on either UDP ports 1812 (authentication) and 1813 (accounting) or ports 1645 (authentication) and 1646 (accounting) requests. RADIUS servers exist for all major operating systems.

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 & Device* > *RADIUS Servers*.



Right-click on any column heading to select which columns are displayed 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:

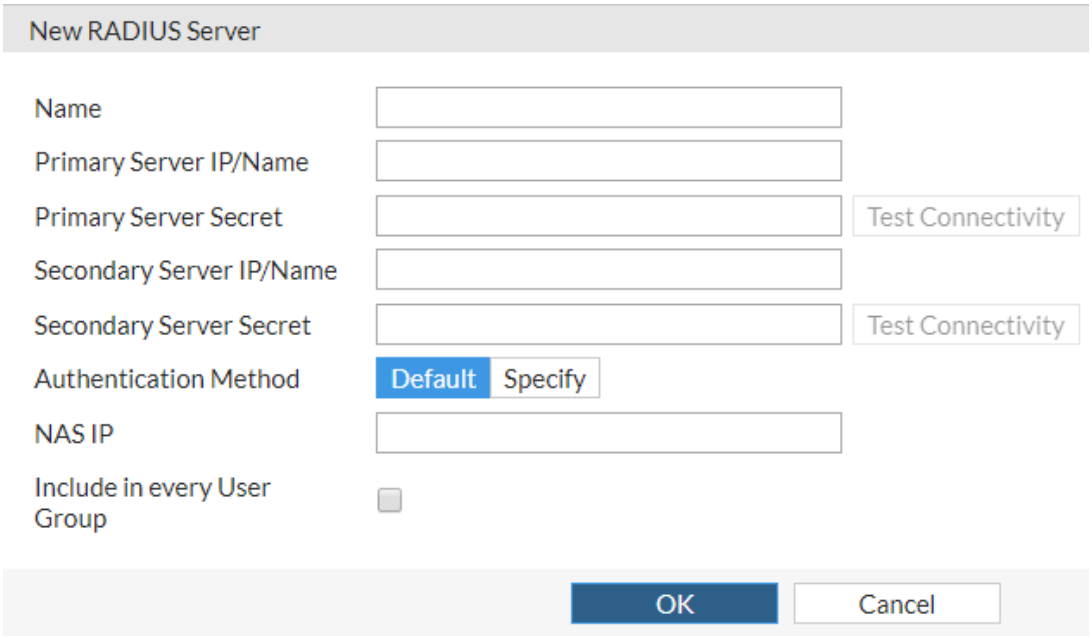
Create New	Create a RADIUS server. See "Create or edit a RADIUS server" on page 294.
Edit	Modify a RADIUS server. See "Create or edit a RADIUS server" on page 294.
Clone	Make a copy of a RADIUS server.
Delete	Remove a server or servers.
Search	Enter a search term to find in the RADIUS server list.

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. Select *OK* to create the new RADIUS server.

To edit a RADIUS server:

1. Select the RADIUS server you want to edit and then select *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 select *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.

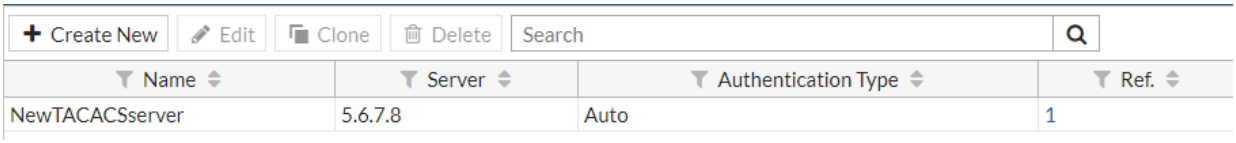
TACACS+ offers fully encrypted packet bodies and supports both IP and AppleTalk protocols. TACACS+ uses TCP port 49, which is seen as more reliable than RADIUS's UDP.

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
```

Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

To manage TACACS+ servers, go to *User & Device* > *TACACS+ Servers*.



Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

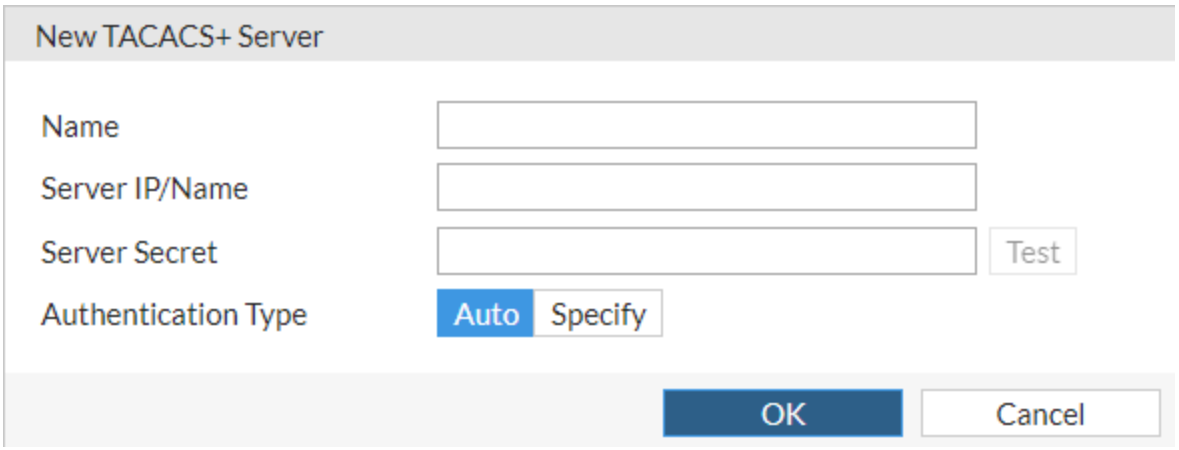
The following options are available:

Create New	Create a TACACS+ server. See "Create or edit a TACACS server" on page 297.
Edit	Modify a TACACS+ server. See "Create or edit a TACACS server" on page 297.
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. Select *OK* to create the new TACACS+ server.

To edit a TACACS+ server:

1. Select the TACACS+ server you want to edit and then select *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 select *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 & Device* > *Kerberos*.

Right-click on any column heading to select which columns are displayed 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:

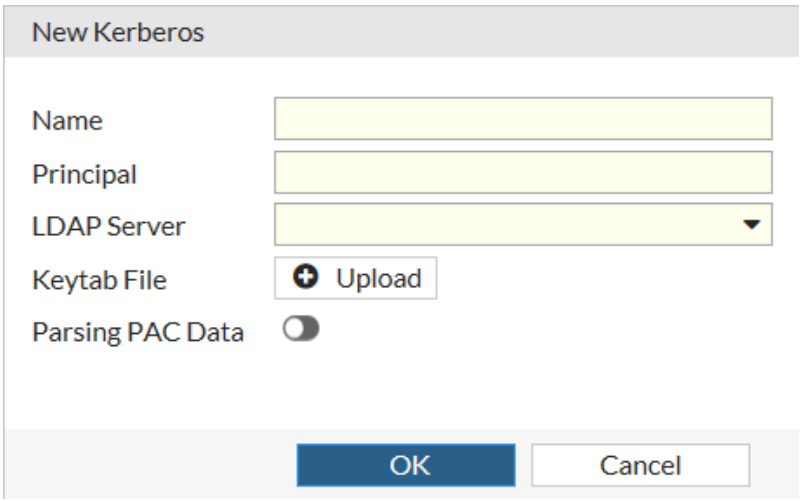
Create New	Create a Kerberos authentication service. See "Create or edit a Kerberos authentication service" on page 299.
Edit	Modify a Kerberos authentication service. See "Create or edit a Kerberos authentication service" on page 299.
Delete	Remove a Kerberos authentication service or services.

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* 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 File	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.
Parsing PAC Data	Move the slider if you want to use proxy auto-config (PAC).

3. Select *OK* to create the new Kerberos authentication service.

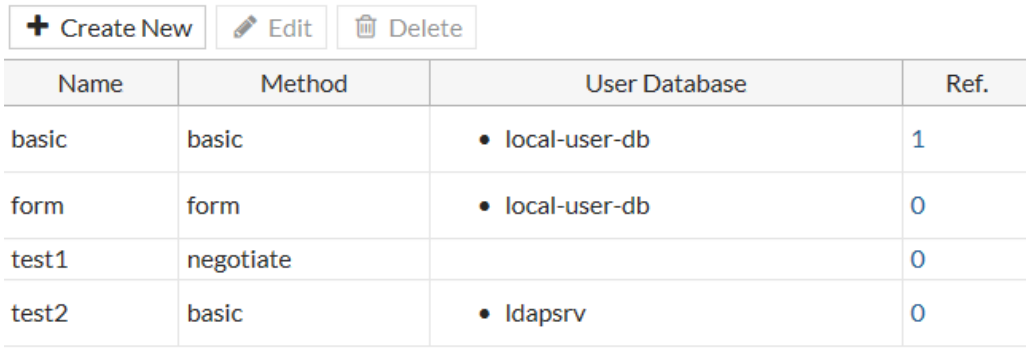
To edit the Kerberos authentication service:

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

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 schemes, go to *User & Device* > *Scheme*.



Right-click on any column heading to select which columns are displayed 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:

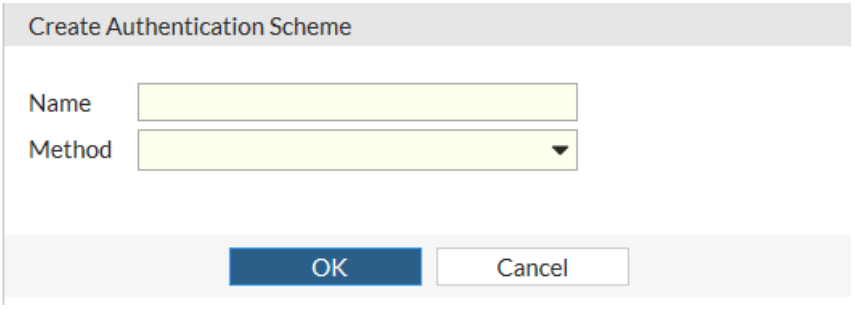
Create New	Create a new authentication scheme. See "Create or edit an authentication scheme" on page 301.
Edit	Edit an authentication scheme. See "Create or edit an authentication scheme" on page 301
Delete	Delete an authentication scheme or schemes.
Name	The name of the authentication scheme.
Method	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 or *local*.

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 scheme

To create an authentication scheme:

1. In the authentication scheme list, select *Create New* from the toolbar.
   The *Create Authentication Scheme* window opens.



2. Configure the following:

Name	Enter the name of the authentication scheme.
Method	Select the authentication method: *NTLM*, *Basic*, *Digest*, *Form-based*, *Negotiate*, *SAML*, *SSH Public Key*, or *Fortinet Single Sign-On (FSSO)*. For agentless NTML authentication, see "Agentless NTLM support" on page 302.

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

To edit an authentication scheme:

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

To create an authentication scheme in the CLI:

```
config authentication scheme
   edit <name>
      set method {basic|digest|ntlm|form|negotiate|fsso|rsso|saml|ssh-publickey}
      set fsso-guest {enable | disable}
      set user-database {name | local}
   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 302.
- `form`—Form-based HTTP authentication.
- `negotiate`—Negotiate authentication.
- `fsso`—FSSO authentication.
- `rsso`—RADIUS Single Sign-On authentication.
- `saml`—SAML-IDP authentication (requires external FortiAuthenticator).
- `publickey`—Public-key-based SSH authentication.

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> - default = 445
      set domain-name <dns-name>
      set ldap-server <name>
   next
end
```

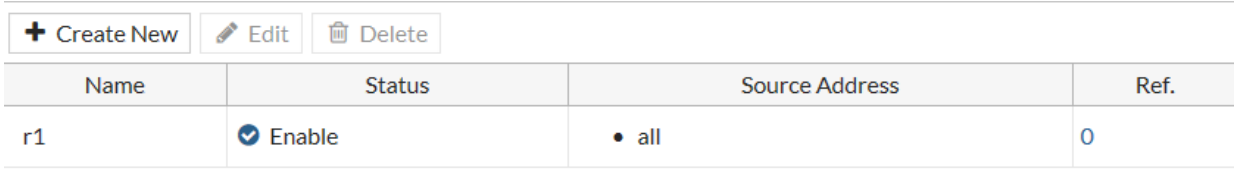
Authentication rule

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`.

To manage authentication rules, go to *User & Device* > *Authentication Rule*.



Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

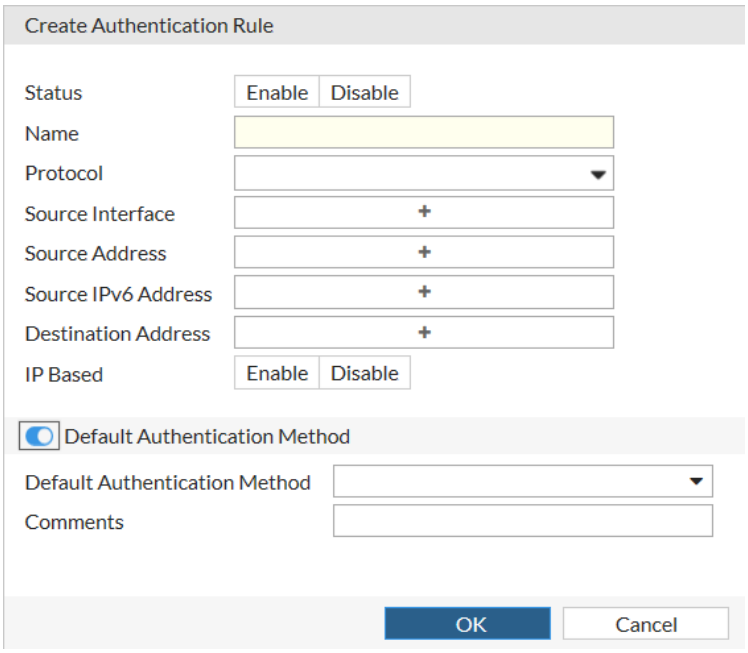
The following options are available:

Create New	Create an authentication rule. See "Create or edit an authentication rule" on page 303.
Edit	Modify an authentication rule. See "Create or edit an authentication rule" on page 303.
Delete	Remove an authentication rule or rules.
Name	The name of the authentication rule.
Status	Whether the rule is enabled or disabled.
Source Address	The source address.
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* from the toolbar.
   The *Create Authentication Rule* window opens.


Create Authentication Rule
Status
Enable
Disable
Name
Protocol
Source Interface
Source Address
Source IPv6 Address
Destination Address
IP Based
Enable
Disable
Default Authentication Method
Default Authentication Method
Comments
OK
Cancel

2. Configure the following:

Status	Select *Enable* or *Disable* to control whether the authentication rule is used or ignored.
Name	The name of the authentication rule.
Protocol	Select which protocol is matched for the rule.
Source Interface	Select *any* or the incoming interfaces.
Source Address	Select the source IPv4 addresses, address groups, *all*, or *none*. Required for web-proxy authentication.
Source Address IPv6	Select the source IPv6 address or addresses, *all*, or *none*. Required for web-proxy authentication.
Destination Address	Select the destination IPv4 addresses, address groups, *all*, or *none*. Required for web-proxy authentication.
IP Based	Select *Enable* if you want to use IP-based authentication.
Default Authentication Method	If you want to select which authentication scheme is the default, move the slider and then select the authentication scheme. To create an authentication scheme, see "Create or edit an authentication scheme" on page 301.
Single Sign-On Method	If you selected Enable for IP-based authentication, move the slider if you want to use a single sign-on method and then select which authentication scheme to use for single sign-on. To create an authentication scheme, see "Create or edit an authentication scheme" on page 301.
Comments	Enter an optional description of the rule.

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

To edit an authentication rule:

1. Select the authentication rule you want to edit and then select *Edit* from the toolbar or double-click on the rule in the rule table.
   The *Edit Authentication Rule* window opens.
2. Edit the rule information as required and select *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 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 comments <string>
    next
end
```

- `status`—Enable/disable auth rule status.
- `protocol`—Set protocols to be matched.
- `srcintf`—Incoming (ingress) interface.
- `srcaddr`/`srcaddr6`—Source address name. [srcaddr or srcaddr6 (web proxy only) must be set].
- `dstaddress`—Destination address name.
- `ip-based`—Enable/disable IP-based authentication.
- `active-auth-method`—Active authentication method.
- `sso-auth-method`—SSO authentication method (require ip-based enabled)
- `comments`—Comment.

Proxy authentication setting

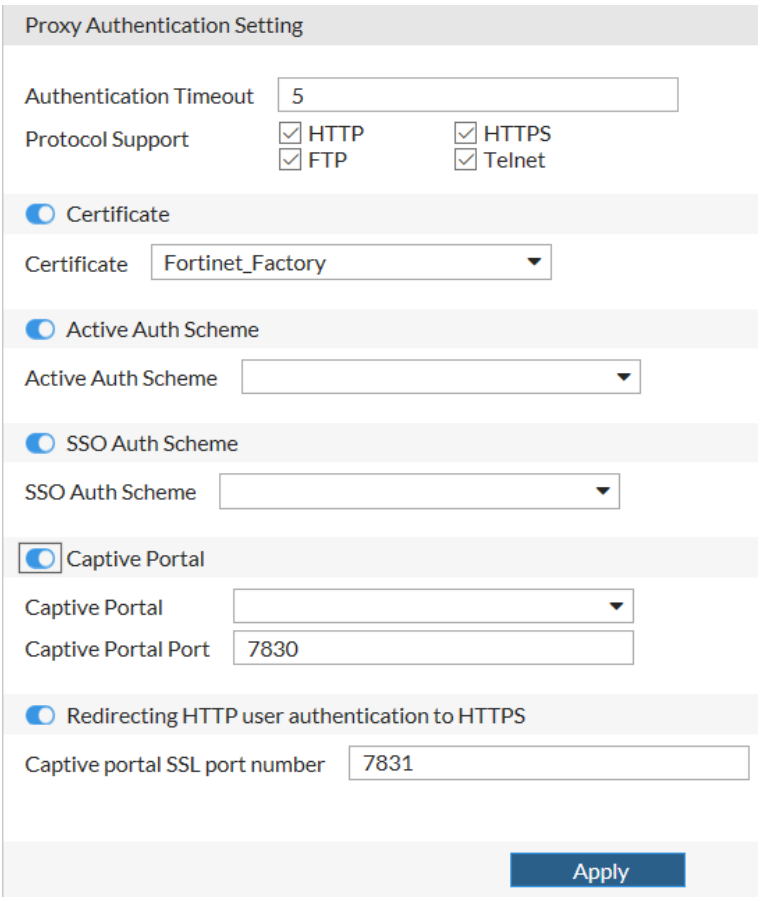
This submenu provides settings for configuring authentication timeout, protocol support, authentication certificates, authentication schemes, and captive portals. When user authentication is enabled within a security policy, the authentication challenge is normally issued for any of the four protocols (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 *User & Device* > *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 301.
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. To create an authentication scheme, see "Create or edit an authentication scheme" on page 301.
Captive Portal	If you want use a captive portal to authenticate web users, enable *Captive Portal* and then select which web page to use and enter the port number.
Redirecting HTTP user authentication to HTTPS	Move the slider if you want HTTPS user authentication used instead of HTTP user authentication and then enter the captive portal SSL port number.

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.

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 313.

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 315.

To view a list of available FortiTokens, go to *User & Device* > *FortiTokens*.

Right-click on any column heading to select which columns are displayed 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 311.
Edit	Modify a FortiToken that was added to your FortiProxy unit. See "Add or edit a FortiToken " on page 311.
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 313.
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	Updates the data displayed.
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 311
2. "Activate a FortiToken on the FortiProxy unit" on page 313
3. "Associate FortiTokens with accounts" on page 313

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).

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 & Device* > *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. Select *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 & Device* > *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. Select *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 & Device* > *FortiTokens*.
2. Select a FortiToken from the list.

3. Select *Edit*.
4. Change the comments and serial number as needed.
5. Select *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 & Device* > *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 & Device* > *User Definition*, select the user account, and then select *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. Select *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 select *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. Select *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.

WAN optimization and web caching

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.

You can add WAN optimization to improve traffic performance and efficiency as it crosses the WAN.

This chapter describes the following:

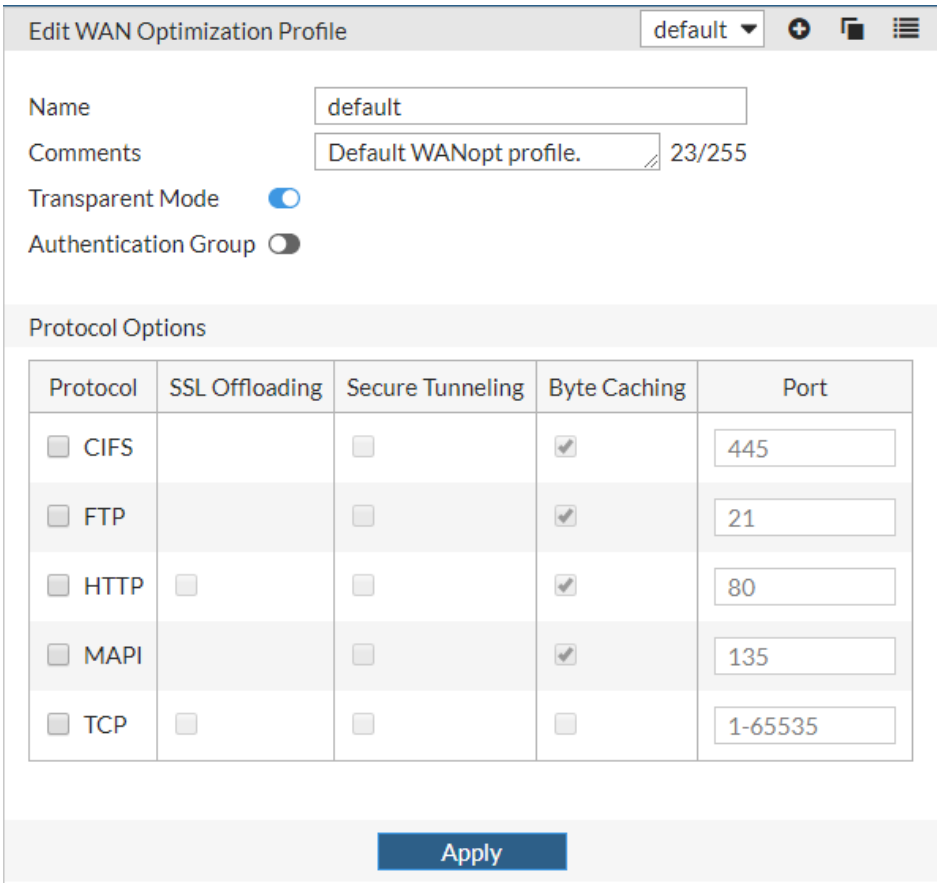
WAN optimization profiles

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.

To configure WAN optimization profiles, go to *WAN Opt. & Cache* > *Profiles*. The *Edit WAN Optimization Profile* page is displayed.



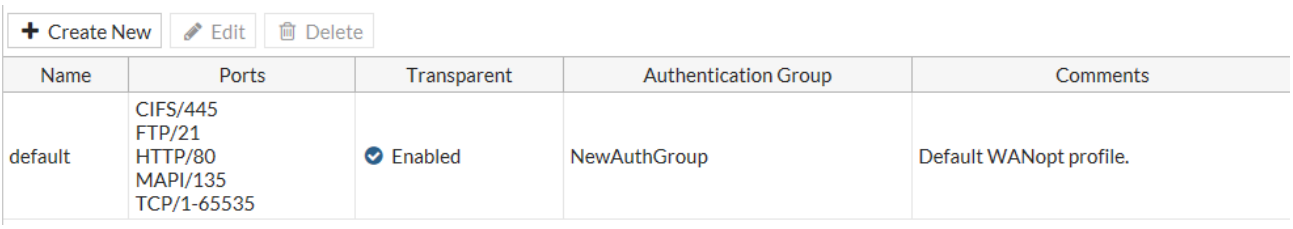
Configure the following settings and then select *Apply* to save your changes:

drop-down list	Select a profile to edit from the drop-down list. See "WAN optimization profiles" on page 319.
Create New icon	Create a new WAN optimization profile. See "WAN optimization profiles" on page 319.
Clone icon	Clone the current profile. See "WAN optimization profiles" on page 320.
List icon	View the WAN optimization profile list. See "WAN optimization profiles" on page 318.
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" on page 18.

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 "WAN optimization peers" on page 322.
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.
Port	Specify the port number for the protocol. The following are the default values: • CIFS: 445 • FTP: 21 • HTTP: 80 • MAPI: 135 • TCP: 1 - 65535

Profile list

You can view the WAN optimization profile list by 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.



Right-click on any column heading to select which columns are displayed 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 new WAN optimization profile. See "WAN optimization profiles" on page 319.
Edit	Modify the profile. See "WAN optimization profiles" on page 319.
Delete	Remove the profile. See "WAN optimization profiles" on page 320.
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" on page 18.
Authentication Group	The authentication group used by the profile, if any. See "WAN optimization peers" on page 321.
Comments	Optional description of the WAN optimization profile.

You can add, edit, and delete WAN optimization profiles.

To create a new 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 select *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 select *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 select *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. Select *Delete* from the toolbar.
3. Select *OK* in the confirmation dialog box to delete the selected profile or profiles.

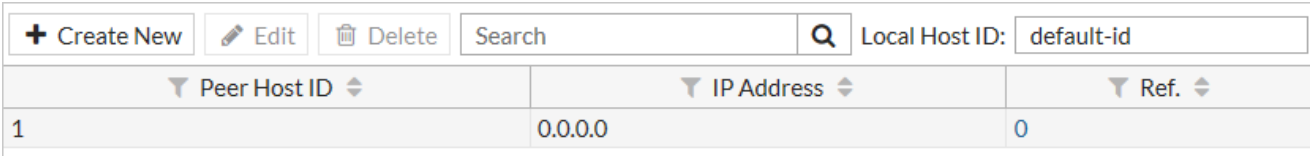
WAN optimization peers

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.

Peers

Go to *WAN Opt. & Cache* > *Peers* to view the WAN optimization peer list.



Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

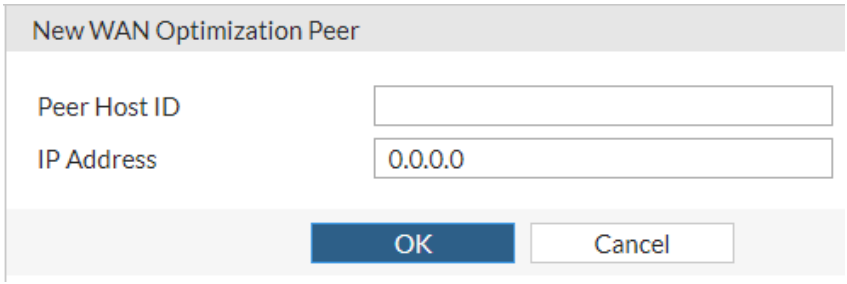
The following options are available:

Create New	Create a new WAN optimization peer. See "WAN optimization peers" on page 321.
Edit	Edit a WAN optimization peer. See "WAN optimization peers" on page 321.
Delete	Delete a WAN optimization peer or peers. See "WAN optimization peers" on page 321.

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.

To create a new 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. Select *OK* to create the new peer.

To edit a WAN optimization peer:

1. Select the peer that you want to edit and then select *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 select *OK* to apply your changes.

To delete a WAN optimization peer or peers:

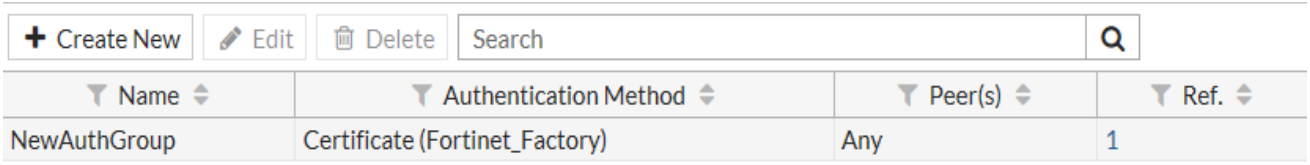
1. Select the peer or peers that you want to delete.
2. Select *Delete* from the toolbar.
3. Select *OK* in the confirmation dialog box to delete the selected peer or peers.

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 Opt. & Cache* > *Authentication Groups* to manage the authentication groups.



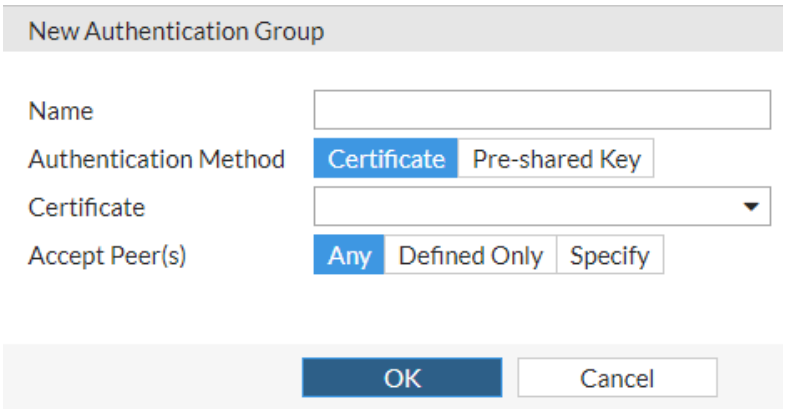
Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Create a new authentication group. See "WAN optimization peers" on page 322.
Edit	Edit an authentication group. See "WAN optimization peers" on page 324.
Delete	Delete an authentication group or groups. See "WAN optimization peers" on page 324.
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.

To create a new authentication group:

1. Select *Create New* from the toolbar.
   The *New Authentication Group* window opens.



2. 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.
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 new peer; see "WAN optimization peers" on page 321.

3. Select *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 "WAN optimization profiles" on page 319.

To edit an authentication group:

1. Select the group you want to edit and then select *Edit* from the toolbar or double-click on the group in the authentication group list.
   The *Edit Authentication Group* window opens.
2. Edit the group information as required and select *OK* to apply your changes.

To delete an authentication group or groups:

1. Select the group or groups that you want to delete.
2. Select *Delete* from the toolbar.
3. Select *OK* in the confirmation dialog box to delete the selected group or groups.

Cache

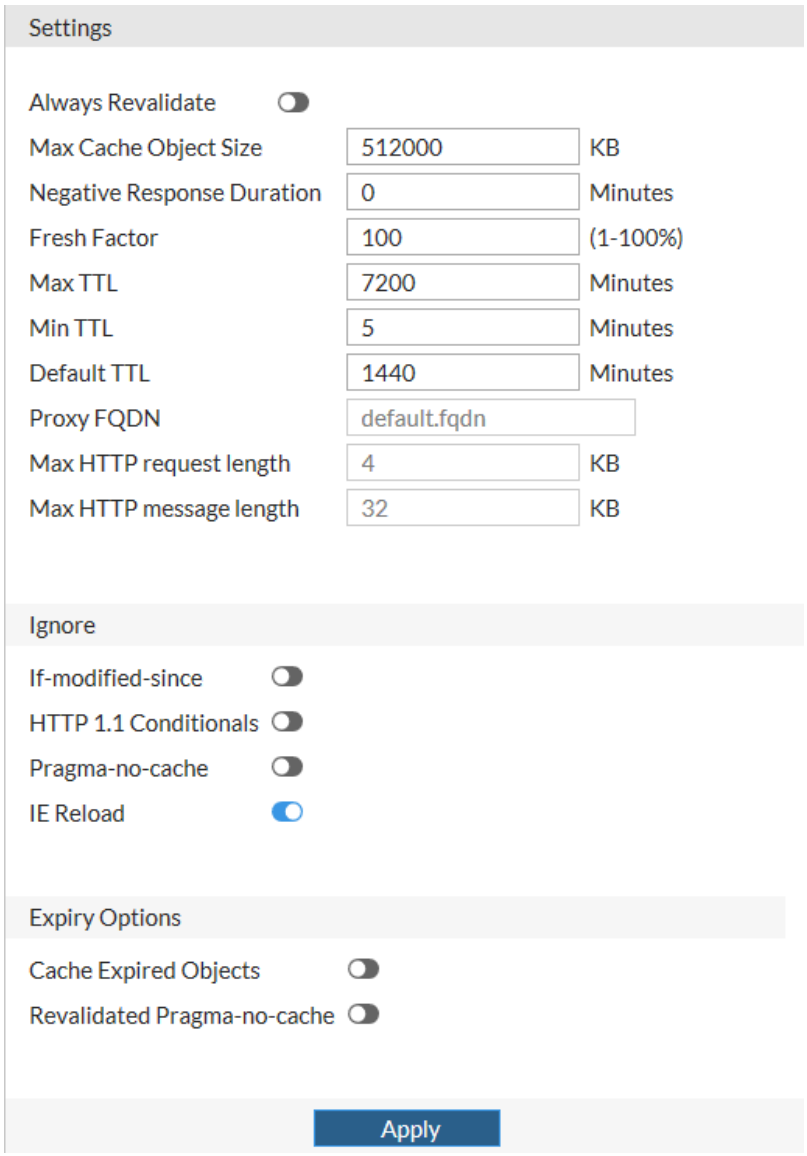
You can optimize web cache settings to improve performance and exempt specific URL patterns from caching and/or forward them to a web proxy server.

This chapters covers the following topics:

Settings

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 *WAN Opt. & 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.

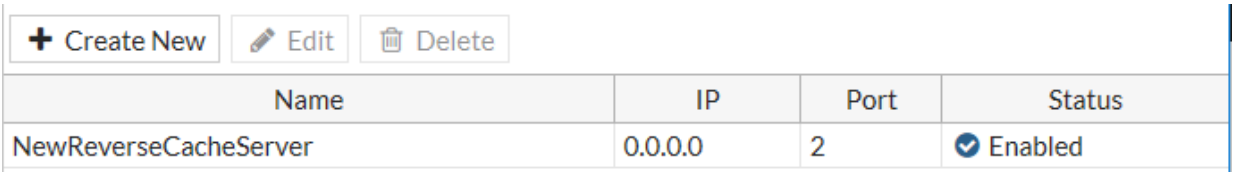
Negative Response Duration	The amount of time, in minutes, that the FortiProxy unit caches error responses from web servers (default is 0 minutes). The content server might send a client error code (4xx HTTP response) or a server error code (5xx HTTP response) as a response to some requests. If the web 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.

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" on page 23.

To see the list of reverse cache servers, go to *WAN Opt. & Cache* > *Reverse Cache Server*.



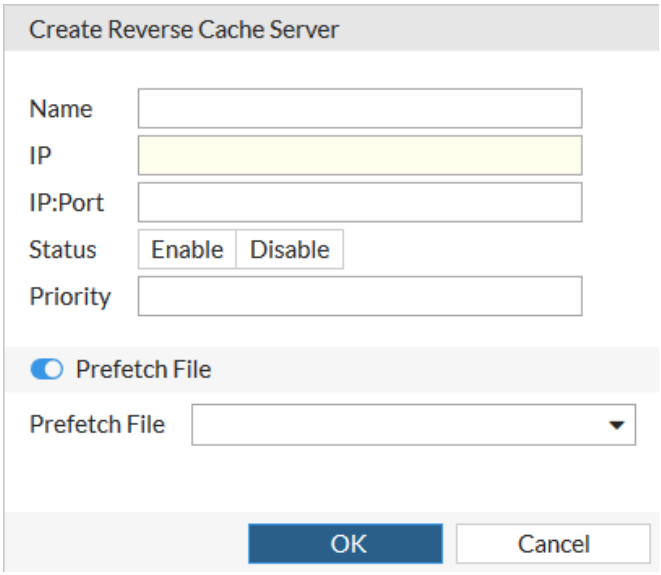
Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Add a new reverse cache server. See "Cache" on page 328.
Edit	Edit the selected reverse cache server. See "Cache" on page 329.
Delete	Delete the selected reverse cache server. See "Cache" on page 329.
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*.

To create a new reverse cache server:

1. Go to *WAN Opt. & 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:Port	Enter the IP address of the reverse cache server and the port number that it 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, enable the slider and select the file or select + to open the *Create Reverse Cache Prefetch* window. To create a prefetch file, see "Cache" on page 328.

3. Select *OK* to create the new reverse cache server.

To edit a reverse cache server:

1. Select the server you want to edit and then select *Edit* from the toolbar or double-click on the server in the table. The *Edit Reverse Cache Server* window opens.
2. Edit the information as required and then select *OK* to apply your changes.

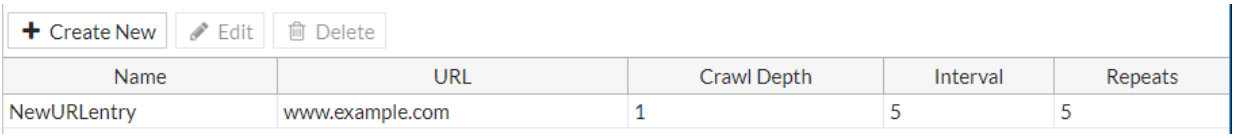
To delete a reverse cache server or servers:

1. Select the server or servers that you want to delete.
2. Select *Delete* from the toolbar.
3. Select *OK* in the confirmation dialog box to delete the selected server or servers.

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 *WAN Opt. & Cache* > *Prefetch URLs*.



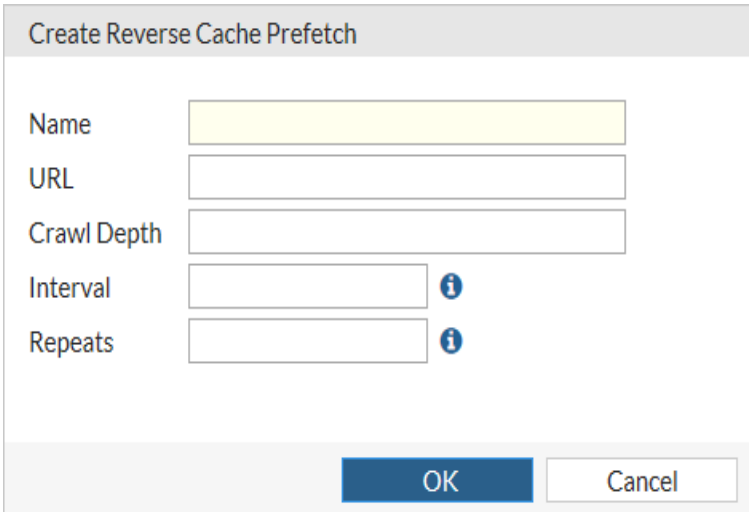
Right-click on any column heading to select which columns are displayed or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available:

Create New	Add a new prefetch file. See "Cache" on page 328.
Edit	Edit the selected prefetch file. See "Cache" on page 330.
Delete	Delete the selected prefetch file. See "Cache" on page 330.
Name	The name of the 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 0-365.

To create a prefetch file:

1. Go to *WAN Opt. & Cache* > *Prefetch URLs* 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 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.
Interval	Enter how often, in seconds, to preload the URLs.
Repeats	Enter how many times to preload the URLs. The value range is 0-365.

3. Select *OK* to create the new prefetch file.

To edit a prefetch file:

1. Select the file that you want to edit and then select *Edit* from the toolbar or double-click on the file in the table.
   The *Edit Reverse Cache Prefetch* window opens.
2. Edit the information as required, then select *OK* to apply your changes.

To delete a prefetch file or files:

1. Select the file or files that you want to delete.
2. Select *Delete* from the toolbar.
3. Select *OK* in the confirmation dialog box to delete the selected file or files.

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 cachable percent of total requests
- **03:** Top entries by cache hit percent of total requests
- **04:** Top entries by cache hit percent of cachable requests
- **05:** Top entries by bandwidth saved with cache hits

Each generated report shows the appropriate domain traffic within the last hour.

Log

The *Log* menu provides an interface for viewing and downloading traffic, event, and security logs. Logging, archiving, and user interface settings can also be configured. See "Log settings" on page 335.

This chapter describes the following:

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.

The following logs are available:

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.
HTTP Transaction	HTTP transaction-related traffic log.
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.
Event logs	
System Events	Log for system-related events.
VPN Events	Log for VPN-related events.
User Events	Log for user-related events.

HA Events	Log for HA-related events.
WAN Opt. & Cache Events	Log for WAN optimization and caching events.
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 flow or proxy-based resource-intensive techniques.
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.
Web Filter	The web filter log records HTTP log rating errors, including web content blocking actions that the FortiProxy device performs.
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.
Anomaly	Protocol anomaly attacks involve malformed or corrupt packets that typically fall outside of protocol specifications. These packets are not seen on a production network. Protocol anomaly attacks exploit poor programming practices when decoding packets, and are typically used to maliciously impair system performance or elevate privileges.
Anti-Spam	The FortiGuard Antispam Service uses both a sender IP reputation database and a spam signature database, along with sophisticated spam filtering tools on Fortinet appliances and agents, to detect and block a wide range of spam messages. Updates to the IP reputation and spam signature databases are provided continuously by the FDN.
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

Log messages can be viewed from the *Log* menu in the FortiProxy GUI.

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.

Log 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 visible columns can be customized by right-clicking on a column header and selecting which columns are displayed. The available columns vary depending on the type of log being viewed.
Page navigation	Navigate to different pages of the log list. The total number of log messages are also shown.

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*.

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 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.

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.

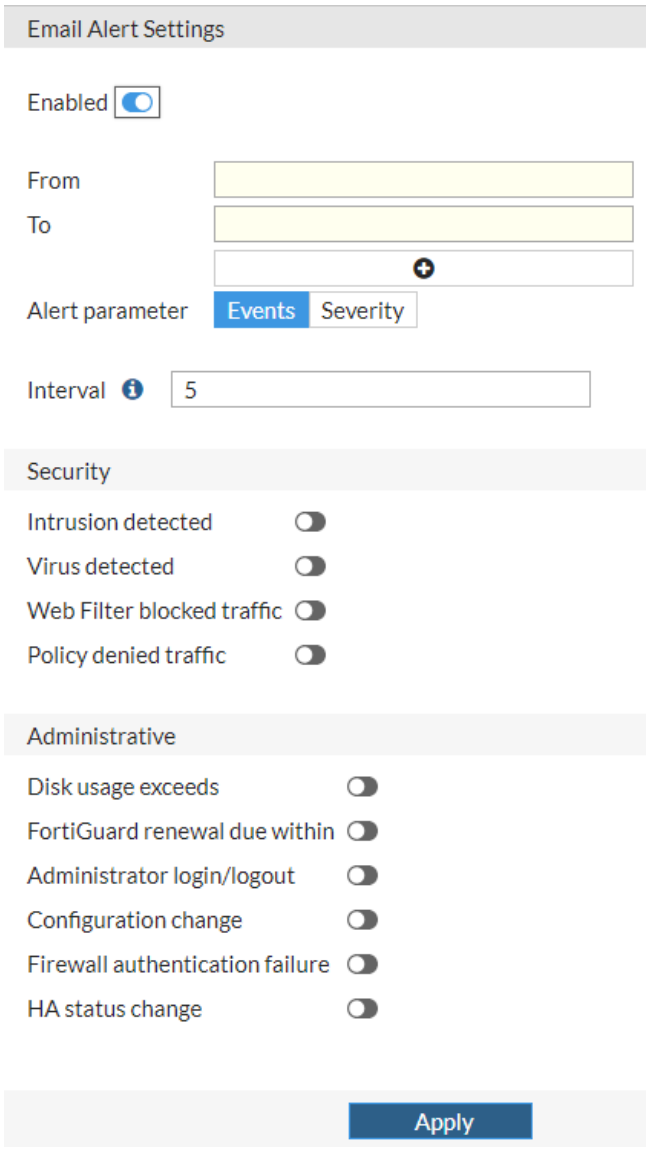
Before configuring alert email, you must configure at least one DNS server if you are configuring with an Fully Qualified Domain Server (FQDN). The FortiProxy unit uses the SMTP server name to connect to the mail server, and must look up this name on your DNS server. You can also specify an IP address.

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.

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.

Appendix A - 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”.

Expression	Matches
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.
/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/
```

Appendix B - 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 "Appendix B - Preload cache content and web crawler" on page 344.

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"
  ```

Appendix C - 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

To manually back up the full FortiProxy configuration to a remote FTP server:

```
execute backup full-config ftp <configuration_file_name> <FTP_server_IP_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_IP _address>
    <password>
```

Specifying a password is optional for backing up to a TFTP server.

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.

NOTE: The auto script overrides the existing configuration file with the same name. Auto script does *not* support keeping all of the hourly configuration files.

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
          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
Please wait...

Connect to ftp server 10.1.5.241 ...
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
Please wait...

Connect to ftp server 10.1.5.241 ...
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>
   # Configure auto script.
      set name <string> Auto script name. The size is 35 characters.
      set interval <integer> Repeat interval in seconds. The range is 0-31557600.
      set repeat <integer> Number of times to repeat this script (0 = infinite). The range
          is 0-65535.
      set start {manual | auto} Script starting mode.
         manual Starting manually.
         auto Starting automatically.
      set script <string> List of FortiProxy CLI commands to repeat. The size is 255
          characters.
      set output-size <integer> Number of megabytes to limit script output to. The range
          is 10-1024. The default is 10.
   next
end
```

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$
```