# FortiWeb™ Web Application Security

Version 4.0.2
Administration Guide

FORTINET®

***FortiWeb™ Web Application Security Administration Guide***

Version 4.0.2

Revision 2

7 April 2010



**Trademarks**

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate®, FortiGate Unified Threat Management System, FortiGuard®, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, Fortinet®, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

**Regulatory compliance**

FCC Class A Part 15 CSA/CUS

**CAUTION:** Risk of explosion if battery is replaced by incorrect type.
Dispose of used batteries according to instructions.

# Contents

# Introduction

Welcome and thank you for selecting Fortinet products for your network protection.

FortiWeb units are designed specifically to protect web servers.

Traditional firewalls and unified threat management (UTM) devices often understand the HTTP protocol, but do not understand simple object access protocol (SOAP) and other XML protocols and document types encapsulated within HTTP (RFC 2616). Because they lack in-depth inspection and analysis, traditional firewalls often cannot route connections based upon XML content. Worse still, attackers can bypass traditional firewall protection and cause problems for web servers that host HTML or XML-based services.

High performance is also important because XML and SOAP parsing requires relatively high amounts of CPU and memory resources. Traditional firewalls may be devoted to other business critical security functions, unable to meet performance requirements while also performing thorough scanning of XML and other HTTP document requests.

FortiWeb units are designed specifically to meet these needs.

In addition to providing application content-based routing and in-depth protection for many HTTP/HTTPS- and XML-specific attacks, FortiWeb units contain specialized hardware to accelerate SSL processing, and can thereby enhance both the security and the performance of connections to your web servers.

This section introduces you to FortiWeb units and the following topics:



## Registering your Fortinet product

Before you begin, take a moment to register your Fortinet product at the Fortinet Technical Support web site, https://support.fortinet.com.

Many Fortinet customer services, such as firmware updates, technical support, and FortiGuard Antivirus and other FortiGuard services, require product registration.

For more information, see the Fortinet Knowledge Base article Registration Frequently Asked Questions.

## Customer service & technical support

Fortinet Technical Support provides services designed to make sure that you can install your Fortinet products quickly, configure them easily, and operate them reliably in your network.

To learn about the technical support services that Fortinet provides, visit the Fortinet Technical Support web site at https://support.fortinet.com.

You can dramatically improve the time that it takes to resolve your technical support ticket by providing your configuration file, a network diagram, and other specific information. For a list of required information, see the Fortinet Knowledge Base article Technical Support Requirements.

# Training

Fortinet Training Services provides classes that orient you quickly to your new equipment, and certifications to verify your knowledge level. Fortinet provides a variety of training programs to serve the needs of our customers and partners world-wide.

To learn about the training services that Fortinet provides, visit the Fortinet Training Services web site at http://campus.training.fortinet.com, or email them at training@fortinet.com.

# Documentation

The Fortinet Technical Documentation web site, http://docs.fortinet.com, provides the most up-to-date versions of Fortinet publications, as well as additional technical documentation such as technical notes.

In addition to the Fortinet Technical Documentation web site, you can find Fortinet technical documentation on the Fortinet Tools and Documentation CD, and on the Fortinet Knowledge Base.

## Fortinet Tools and Documentation CD

Many Fortinet publications are available on the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For current versions of Fortinet documentation, visit the Fortinet Technical Documentation web site, http://docs.fortinet.com.

## Fortinet Knowledge Base

The Fortinet Knowledge Base provides additional Fortinet technical documentation, such as troubleshooting and how-to-articles, examples, FAQs, technical notes, and more. Visit the Fortinet Knowledge Base at http://kb.fortinet.com.

## Comments on Fortinet technical documentation

Please send information about any errors or omissions in this technical document to techdoc@fortinet.com.

# Scope

This document describes how to use the web-based manager of the FortiWeb unit. It assumes you have already successfully installed the FortiWeb unit by following the instructions in the *FortiWeb Installation Guide*.

At this stage:

- You have administrative access to the web-based manager and/or CLI.
- The FortiWeb unit is integrated into your network.

- The operation mode has been configured.
- The system time, DNS settings, administrator password, and network interfaces have been configured.
- Firmware updates have been completed.
- Basic policies have been configured.

Once that basic installation is complete, you can use this document. This document explains how to use the web-based manager to:

- maintain the FortiWeb unit, including backups
- reconfigure basic items that were configured during installation
- configure advanced features, such as customized protection profiles, logging, and reporting

This document does ***not*** cover commands for the command line interface (CLI). For information on the CLI, see the *FortiWeb CLI Reference*.

# Conventions

Fortinet technical documentation uses the conventions described below.

## IP addresses

To avoid publication of public IP addresses that belong to Fortinet or any other organization, the IP addresses used in Fortinet technical documentation are fictional and follow the documentation guidelines specific to Fortinet. The addresses used are from the private IP address ranges defined in RFC 1918: Address Allocation for Private Internets, available at http://ietf.org/rfc/rfc1918.txt?number-1918.

## Cautions, Notes, & Tips

Fortinet technical documentation uses the following guidance and styles for cautions, notes and tips.

**Caution:** Warns you about commands or procedures that could have unexpected or undesirable results including loss of data or damage to equipment.

**Note:** Presents useful information, usually focused on an alternative, optional method, such as a shortcut, to perform a step.

**Tip:** Highlights useful additional information, often tailored to your workplace activity.

## Typographical conventions

Fortinet documentation uses the following typographical conventions:

**Table 1: Typographical conventions in Fortinet technical documentation**

| Convention | Example |
|---|---|
| **Button, menu, text box, field, or check box label** | From *Minimum log level*, select *Notification*. |
| **CLI input** | `config system dns`<br>`  set primary <address_ipv4>`<br>`end` |
| **CLI output** | `FGT-602803030703 # get system settings`<br>`comments  : (null)`<br>`opmode  : nat` |
| **Emphasis** | HTTP connections are ***not*** secure and can be intercepted by a third party. |
| **File content** | `<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD>`<br>`<BODY><H4>You must authenticate to use this service.</H4>` |
| **Hyperlink** | Visit the Fortinet Technical Support web site, https://support.fortinet.com. |
| **Keyboard entry** | Type a name for the remote VPN peer or client, such as `Central_Office_1`. |
| **Navigation** | Go to *VPN* > *IPSEC* > *Auto Key (IKE)*. |
| **Publication** | For details, see the *FortiGate Administration Guide*. |

## Command syntax conventions

The command line interface (CLI) requires that you use valid syntax, and conform to expected input constraints. It will reject invalid commands.

Brackets, braces, and pipes are used to denote valid permutations of the syntax. Constraint notations, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable value input.

**Table 2: Command syntax notation**

| Convention | Description |
|---|---|
| **Square brackets** `[ ]` | A non-required word or series of words. For example:<br>`[verbose {1 \| 2 \| 3}]`<br>indicates that you may either omit or type both the `verbose` word and its accompanying option, such as:<br>`verbose 3` |

**Table 2: Command syntax notation**

| | |
|---|---|
| **Angle brackets** < > | A word constrained by data type.<br>To define acceptable input, the angled brackets contain a descriptive name followed by an underscore ( _ ) and suffix that indicates the valid data type. For example:<br>`<retries_int>`<br>indicates that you should enter a number of retries, such as `5`.<br>Data types include:<br>• `<xxx_name>`: A name referring to another part of the configuration, such as `policy_A`.<br>• `<xxx_index>`: An index number referring to another part of the configuration, such as `0` for the first static route.<br>• `<xxx_pattern>`: A regular expression or word with wild cards that matches possible variations, such as `*@example.com` to match all email addresses ending in `@example.com`.<br>• `<xxx_fqdn>`: A fully qualified domain name (FQDN), such as `mail.example.com`.<br>• `<xxx_email>`: An email address, such as `admin@mail.example.com`.<br>• `<xxx_url>`: A uniform resource locator (URL) and its associated protocol and host name prefix, which together form a uniform resource identifier (URI), such as `http://www.fortinet.com/`.<br>• `<xxx_ipv4>`: An IPv4 address, such as `192.168.1.99`.<br>• `<xxx_v4mask>`: A dotted decimal IPv4 netmask, such as `255.255.255.0`.<br>• `<xxx_ipv4mask>`: A dotted decimal IPv4 address and netmask separated by a space, such as `192.168.1.99 255.255.255.0`.<br>• `<xxx_ipv4/mask>`: A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as such as `192.168.1.99/24`.<br>• `<xxx_ipv6>`: A colon( `:` )-delimited hexadecimal IPv6 address, such as `3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234`.<br>• `<xxx_v6mask>`: An IPv6 netmask, such as `/96`.<br>• `<xxx_ipv6mask>`: An IPv6 address and netmask separated by a space.<br>• `<xxx_str>`: A string of characters that is ***not*** another data type, such as `P@ssw0rd`. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences. See the *FortiWeb CLI Reference*.<br>• `<xxx_int>`: An integer number that is ***not*** another data type, such as `15` for the number of minutes. |
| **Curly braces** { } | A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces.<br>You must enter at least one of the options, unless the set of options is surrounded by square brackets [ ]. |

**Table 2: Command syntax notation**

| | |
|---|---|
| **Options delimited by vertical bars** \| | Mutually exclusive options. For example:<br>`{enable \| disable}`<br>indicates that you must enter either `enable` or `disable`, but must not enter both. |
| **Options delimited by spaces** | Non-mutually exclusive options. For example:<br>`{http https ping snmp ssh telnet}`<br>indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as:<br>`ping https ssh`<br>**Note:** To change the options, you must re-type the entire list. For example, to add `snmp` to the previous example, you would type:<br>`ping https snmp ssh`<br>If the option adds to or subtracts from the existing list of options, instead of replacing it, or if the list is comma-delimited, the exception will be noted. |

# Characteristics of XML threats

XML messages can be relatively large: many megabytes and thousands of packets. Unstructured matching of elements in those messages is complex and CPU- and memory-intensive. Because of the complexity of XML content, it is often not practical to develop signatures for XML-specific attacks on a traditional firewall or UTM. This leads to “zero day” vulnerabilities before attacks can be characterized and signatures developed.

FortiWeb units understand the XML protocol, and only allows XML operations that you specifically allow. Table 3 lists several XML-related threats and describes how FortiWeb units protect against them.

**Table 3: XML-related threats**

| Attack Technique | Description | Protection | FortiWeb Solution |
|---|---|---|---|
| Schema Poisoning | Manipulating the XML Schema to alter processing information | Protect against schema poisoning by relying on trusted WSDL documents and XML Schema's | Schema Poisoning option in protection profile prevents external schemas references to be used |
| XML Parameter Tampering | Injection of malicious scripts or content into request parameters | Validation of parameter values to ensure they are consistent with WSDL and XML Schema specifications | Schema Validation in protection profile |
| Inadvertent XML DoS | Poorly encoded SOAP messages causing the application to fail | Content inspection ensures SOAP messages are constructed properly according to WSDL, XML Schema and intrusion prevention rules | Schema Validation and WSDL verification and intrusion prevention rule in protection profile. |
| WSDL Scanning | Scanning the WSDL interface can reveal sensitive information about invocation patterns, underlying technology and associated vulnerabilities | Web services cloaking hides the web services true location from consumers | WSDL scanning option and ability to filter services from WSDL on a per IP / Time basis |
| Oversized Payload | Sending oversized messages to create an XDoS attack | Inspect the payload and enforce element, document, and other maximum payload thresholds | XML documents are checked with schema and intrusion prevention rule |
| Recursive Payload | Sending mass amounts of nested data to create an XDoS attack against the XML parser | Content inspection ensures SOAP messages are constructed properly according to WSDL, XML Schema, and other security specifications | Intrusion prevention definition |
| SQL Injection | SQL Injection allows commands to be executed directly against the database for unauthorized disclosure and modification of data | Rely on dirty word searches, restrictive context-sensitive filtering and data validation techniques | XML Profile option to filter SQL transactions from XML documents |
| External Entity Attack | An attack on an application that parses XML input from un-trusted sources (DTD internal subset) | Suppress external URI references to protect against malicious data sources and instructions; rely on well-known and certified URIs | Similar to Schema Poisoning |

# Characteristics of HTTP threats

Web applications are increasingly being targeted by exploits such as SQL Injection and Cross-Site Scripting attacks. These attacks aim to compromise the target web server, either to steal information or to post malicious files on a trusted site to further exploit visitors to the site. The types of attacks that web servers are vulnerable to are numerous and varied. FortiWeb units offer several options for preventing web-related attacks. Table 4 lists several Web-related threats and describes how FortiWeb units protect against them.

**Table 4: Web-related threats**

| Attack Technique | Description | Protection | FortiWeb Solution |
|---|---|---|---|
| Cross-site request forgery (CSRF) | A script causes a browser to access a web site on which the browser has already been authenticated, giving a third party access to a user's session on that site. | Enforce web application business logic to prevent random access to URLs | Page Access rules |
| Cross-site scripting (XSS) | Attackers cause a browser to execute a client-side script, allowing them to bypass security. | Content filtering, cookie security, disable client-side scripts | XSS signature scanning in Server Protection Rules |
| SQL injection | SQL Injection allows commands to be executed directly against the database for unauthorized disclosure and modification of data | Rely on dirty word searches, restrictive context-sensitive filtering and data validation techniques | Parameter Validation rules, Hidden Fields Protection features, and SQL Injection signature scanning |
| Attacks via Flash AMF binary protocol | Attackers attempt XSS, SQL injection or other common exploits through a flash client | Actively scan Flash Action Message Format binary data for known exploits | AMF3 Protocol scanning for known exploits |
| Information Leakage | A web server reveals details (such as its OS, server software and installed modules) in responses or error messages. An attacker can leverage this information to craft exploits for a specific system or configuration. | Configure server software to minimize information leakage. | Information disclosure detection in Server Protection Rules can alert when leakage happens, or block it altogether. URL re-writing can hide underlying implementation details. |
| Credit card theft | Attackers use exploits to obtain users' credit card information from a secure server. | Detect and block credit card disclosure | Credit card detection in Server Protection Rules can detect and block disclosure of credit card numbers on web pages |
| SYN Flood DoS Attack | An attacker sends multiple SYN messages to a host without responding to an ACK reply, leaving connections half open and consuming resources on the server. This may cause the server to ignore SYN messages from legitimate users and reduce service. | Detect increased SYN activity, close half open connections before resources are exhausted | Configurable threshold to detect a flood of SYN messages. |
| Brute force login attack | An attacker attempts to gain authorization by repeatedly trying ID and password combinations until one works. | Require strong passwords for users, and throttle login attempts | Brute Force Login policies can throttle the number of login attempts per standalone or shared IP for specific resources. |

**Table 4: Web-related threats**

| Attack Technique | Description | Protection | FortiWeb Solution |
|---|---|---|---|
| Bad robots | Misbehaving web crawlers ignore the robots.txt file, and consume server resources and bandwidth on a site | Ban bad robots by source IP or User Agent field | Robot Control can throttle requests per IP, and block robots identified by the User Agent field. |
| HTTP protocol attack | Attackers use specially crafted HTTP requests to target web server vulnerabilities (such as a buffer overflow) to execute malicious code | Limit the length of HTTP protocol fields | HTTP Protocol Parameter policies enforce configurable limits on the length of HTTP headers, bodies, and parameters |

# What's new

The list below contains features which have changed since the previous release, FortiWeb v4.0.1. For upgrade information, see the Release Notes available with the firmware, and "Installing firmware" on page 279.

- **Disable redirection reason in the URL** – You can now choose whether or not to include the reason for the redirection as a parameter in the URL. This option can prevent redirect loops. For details, see "Redirect URL With Reason" on page 219.
- **Packet payloads for traffic logs** – You can now specify whether traffic logs retain the decoded packet payload for all client requests. For details, see "Enabling logging and alerts" on page 253.
- **Redirect option for information disclosure** - In addition to *Alert* and *Alert & Erase*, there is a new *Redirect* option for information disclosure in the server protection rules. For details, see "Information Disclosure" on page 166.

# About the web-based manager

This chapter describes aspects that are general to use of the web-based manager, a graphical user interface (GUI) that you can use to access the FortiWeb unit from within a current web browser.

This section includes the following topics:



## System requirements

The management computer that you use to access the web-based manager must have:

- a compatible web browser, such as Microsoft Internet Explorer 6.0 or greater, or Mozilla Firefox 3.0 or greater
- Adobe Flash Player 10 or greater plug-in

To minimize scrolling, the computer's screen should have a resolution that is a minimum of 1280 x 1024 pixels.

## URL for access

The web-based manager can be accessed by URL using the network interfaces' enabled administrative access protocols and IP addresses.

By default, the URL when accessing the web-based manager through port1 is https://192.168.1.99/.

If the network interfaces have been configured such as during the installation instructions in the *FortiWeb Install Guide*, the URL and/or permitted administrative access protocols (in this case, HTTPS) may no longer be in their default state. In that case, for the URL, use either a DNS-resolvable domain name for the FortiWeb unit, or the IP address that you configured for the network interface to which you are connected.

For example, you might have configured port2 with the IP address 10.0.0.1 and enabled HTTPS. You might have also configured a private DNS server on your network to resolve fortiweb.example.com to 10.0.0.1. In this case, to access the web-based manager through port2, you could enter either `https://fortiweb.example.com/` or `https://10.0.0.1/`.

For information on enabling administrative access protocols and configuring IP addresses, see "Configuring the network interfaces" on page 34.

**Note:** If the URL is correct and you still cannot access the web-based manager, you may also need to configure from which hosts the FortiWeb unit will accept login attempts for your administrator account (that is, trusted hosts), and/or static routes. For details, see "Configuring administrator accounts" on page 53 and "Configuring static routes" on page 81.

# Settings

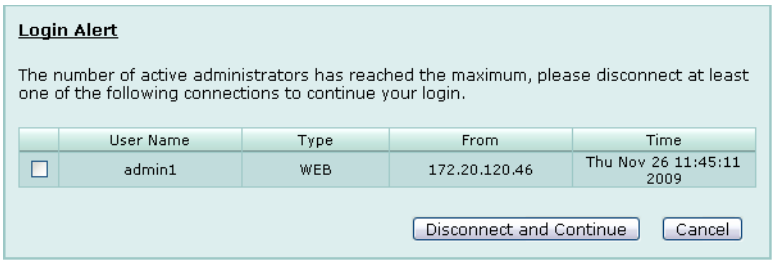
Some settings for the web-based manager apply regardless of which administrator account you use to log in. Global settings include the idle timeout, TCP port number on which the web-based manager listens for connection attempts, the network interface(s) on which it listens, the language of its display, and whether or not more than one administrator can be logged in at any given time.

For details, see “Configuring the web-based manager’s global settings” on page 60 and “Configuring the network interfaces” on page 34.

## Single administrator mode

If single administrator mode is enabled, when you log in to the web-based manager, you may be required to disconnect other administrator accounts’ sessions before you can continue.

**Figure 1: Single administrator mode disconnection prompt**




For details, see “Enable Single admin User login” on page 61.

# Language support & regular expressions

Characters such as ñ, é, symbols, and ideographs are sometimes acceptable input. Support varies by the nature of the item being configured.

For example, the host name must not contain special characters, and so the web-based manager and CLI will not accept most symbols and non-ASCII encoded characters as input when configuring the host name. This means that languages other than English often are not supported. However, some configuration items, such as names and comments, may be able to use the language of your choice.

To use other languages in those cases, you must use an encoding that supports it.

Input is stored using Unicode UTF-8 encoding, but is not normalized from other encodings into UTF-8 before it is stored. If your input method encodes some characters differently than in UTF-8, your configured items may not display or operate as expected.

***Regular expressions are especially impacted. Matching uses the UTF-8 character values. If you enter a regular expression using another encoding, or if an HTTP client sends a request in an encoding other than UTF-8, matches may not be what you expect.***

For example, with Shift-JIS, backslashes ( \ ) could be inadvertently interpreted as yen symbols ( ¥ ) and vice versa. A regular expression intended to match HTTP requests containing money values with a yen symbol therefore may not work it if the symbol is entered using the wrong encoding.

For best results, you should:

- use UTF-8 encoding, or
- use only the characters whose numerically encoded values are the same in UTF-8, such as the US-ASCII characters that are also encoded using the same values in ISO 8859-1, Windows code page 1252, Shift-JIS and other encodings, or
- for regular expressions that must match HTTP requests, use the same encoding as your HTTP clients

**Note:** HTTP clients may send requests in encodings other than UTF-8. Encodings usually vary by the client's operating system or input language. If you cannot predict the client's encoding, you may only be able to match any parts of the request that are in English, because regardless of the encoding, the values for English characters tend to be encoded identically. For example, English words may be legible regardless of interpreting a web page as either ISO 8859-1 or as GB2312, whereas simplified Chinese characters might only be legible if the page is interpreted as GB2312.

In order to configure your FortiWeb unit using other encodings, you may need to switch language settings on your management computer, including for your web browser or Telnet/SSH client. For instructions on how to configure your management computer's operating system language, locale, or input method, see its documentation.

**Note:** If you choose to configure parts of the FortiWeb unit using non-ASCII characters, verify that all systems interacting with the FortiWeb unit also support the same encodings. You should also use the same encoding throughout the configuration if possible in order to avoid needing to switch the language settings of your web browser or Telnet/SSH client while you work.

Similarly to input, your web browser or CLI client should usually interpret display output as encoded using UTF-8. If it does not, your configured items may not display correctly in the web-based manager or CLI. Exceptions include items such as regular expressions that you may have configured using other encodings in order to match the encoding of HTTP requests that the FortiWeb unit receives.

For information on configuring the display language of the web-based manager, see "Configuring the web-based manager's global settings" on page 60.

# System

This section describes the *System* menu, which displays the current status and configures basic features of the FortiWeb unit.

This topic includes:

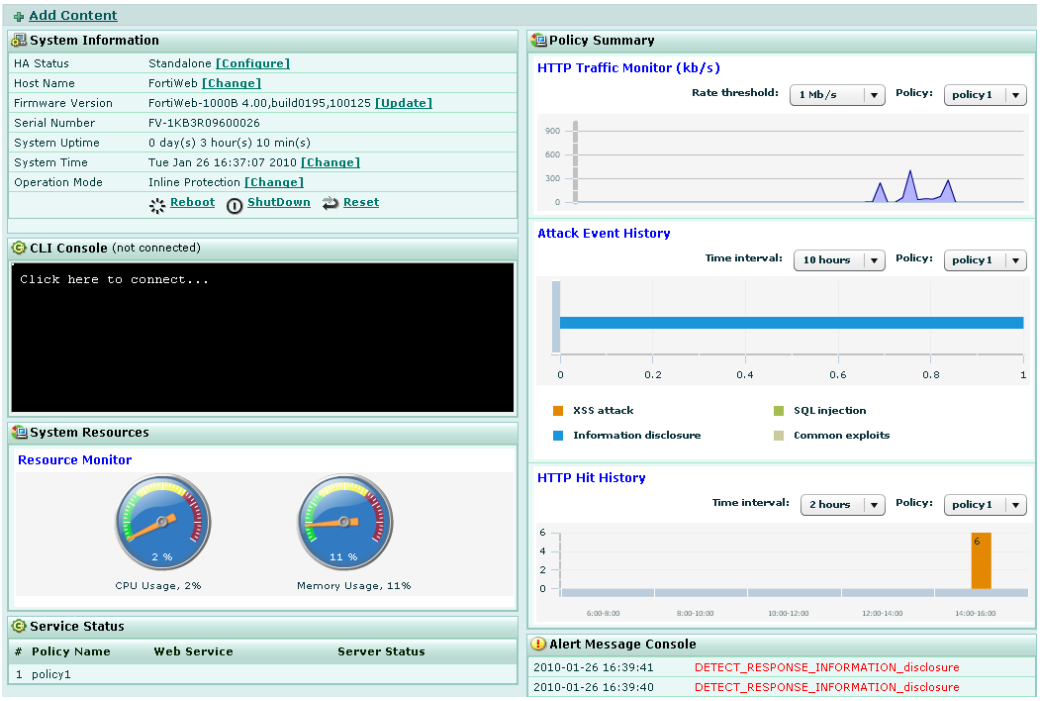


## Viewing the system statuses

*System* > *Status* > *Status* displays first after you log in to the web-based manager. It contains a dashboard with widgets that each indicate performance level or other statuses.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *System Configuration* category. For details, see "About permissions" on page 58.

**Figure 2: Viewing the dashboard**



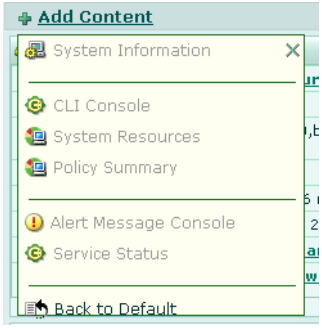

By default, widgets appear which display the serial number and current system status of the FortiWeb unit, including uptime, system resource usage, alert messages, host name, firmware version, system time, and status of connected web servers. The dashboard also contains a CLI widget that enables you to use the command line through the web-based manager.

The dashboard is customizable. You can select which widgets to display, where they are located on the tab, and whether they are minimized or maximized.

To move a widget, position your mouse cursor on the widget's title bar, then click and drag the widget to its new location.

To display any of the widgets not currently shown on the *Status* tab, click *Add Content*. Any widgets currently already displayed on the *Status* tab will be greyed out in the *Add Content* menu, as you can only have one of each display on the *Status* tab.

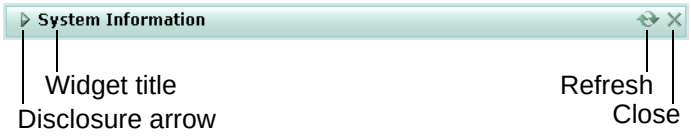
**Figure 3: Adding a widget**




To display the default set of widgets on the *Status* tab, select *Back to Default*.

To see the available options for a widget, position your mouse cursor over the icons in the widget's title bar. Options vary slightly from widget to widget, but always include options to close or minimize/maximize the widget.

**Table 5: A minimized widget**




| *Name of the GUI item* | *Description* |
|---|---|
| **Widget Title** | The name of the widget. |
| **Disclosure arrow** | Click to maximize or minimize the widget.<br>This arrow replaces the widget's icon when you place your mouse cursor over the title bar. |
| **Edit** | Click to change settings for the widget.<br>This option appears only on the *CLI Console* widget. |
| **Refresh** | Click to update the displayed information.<br>This option does not appear on the *CLI Console* widget. |
| **Close** | Click to close the widget on the dashboard. You will be prompted to confirm the action. To show the widget again, click *Add Content* near the top of the tab. |

The available dashboard widgets are:

- System Information widget
- CLI Console widget
- System Resources widget
- Alert Message Console widget
- Service Status widget
- Policy Summary widget

## System Information widget

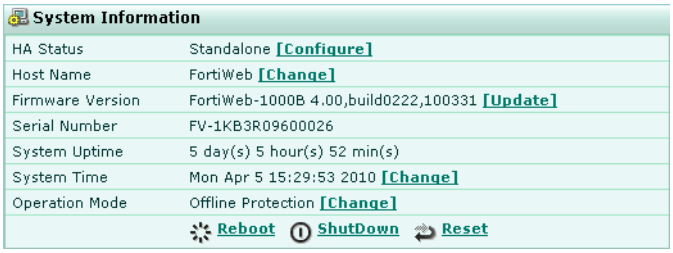
The *System Information* widget displays the serial number and basic system statuses such as the firmware version, system time, up time, and host name, and high availability (HA) status.

In addition to displaying basic system information, the *System Information* widget enables you to configure some basic attributes such as the host name, operation mode, and high availability (HA) mode, and to change the firmware.

FortiWeb administrators whose access profiles permit *Write* access to items in the *System Configuration* category can change the system time, host name, firmware, and operation mode, and high availability (HA) mode.

To view the *System Information* widget, go to *System* > *Status* > *Status*.

**Table 6:** *System Information* **widget**




| *Name of the GUI item* | *Description* |
|---|---|
| **HA Status** | The status of high availability (HA) for this unit, either:<br>• **Standalone**: The FortiWeb unit is not operating in HA mode.<br>• **Active-Passive**: The FortiWeb unit is operating in HA mode.<br>Click *Configure* to configure the HA status for this unit. See "Configuring high availability (HA)" on page 42. |
| **Host Name** | The host name of the FortiWeb unit.<br>Click *Change* to change the host name. See "Changing the FortiWeb unit's host name" on page 29. |
| **Firmware Version** | The version of the firmware currently installed on the FortiWeb unit.<br>Click *Update* to install firmware. See "Installing firmware" on page 279. |
| **Serial Number** | The serial number of the FortiWeb unit. The serial number is specific to the FortiWeb unit's hardware and does not change with firmware upgrades. Use this number when registering the hardware with Fortinet Technical Support. |
| **System Uptime** | The time in days, hours, and minutes since the FortiWeb unit was started. |
| **System Time** | The current date and time according to the FortiWeb unit's internal clock.<br>Click *Change* to change the time or configure the FortiWeb unit to get the time from an NTP server. See "Configuring the time & date" on page 75. |
| **Operation Mode** | The operation mode of the FortiWeb unit, either:<br>• **Inline Protection**: Reverse proxy traffic destined for a virtual server's network interface and IP address, forwarding it to a physical server, and apply the first applicable policy. The FortiWeb unit logs, blocks, or modifies traffic according to the matching policy and its protection profile.<br>• **Offline Protection**: Pass through traffic received on the virtual server's network interface (regardless of the IP address) to the physical servers, and apply the first applicable policy. The FortiWeb unit logs or blocks traffic according to the matching policy and its protection profile, but does ***not*** otherwise modify it. (It does not, for example, apply SSL or load balance connections.)<br>**Caution:** Unlike in inline protection mode, actions other than *Alert* cannot be guaranteed to be successful in offline protection mode. The FortiWeb unit will attempt to block traffic that violates the policy by mimicking the client or server and requesting to reset the connection. However, the client or server may receive the reset request after it receives the other traffic due to possible differences in routing paths.<br>• **Transparent**: Proxy traffic destined for a physical server's IP address, and apply the first applicable policy. Traffic is received on a network port that belongs to a Layer 2 bridge, and no changes to the IP address scheme of the network are required. It does not apply SSL or load balance connections.<br>Click *Configure* to switch the operation mode.<br>**Caution:** Back up the configuration before changing the operation mode. Policies that are inapplicable to the operation mode you choose will be deleted. For instructions on backing up the configuration, see "Backing up the configuration & installing firmware" on page 74. |
| **Reboot** | Click to halt and restart the operating system of the FortiWeb unit. |

| | |
|---|---|
| **ShutDown** | Click to halt the operating system of the FortiWeb unit, preparing its hardware to be powered off. |
| **Reset** | Click to revert the configuration of the FortiWeb unit to the default values for its currently installed firmware version.<br>**Caution:** Back up the configuration before resetting the configuration of your FortiWeb unit. This operation cannot be undone. For instructions on backing up the configuration, see "Backing up the configuration & installing firmware" on page 74. |

## Changing the FortiWeb unit's host name

The host name of the FortiWeb unit is used in several places.

- It appears in the *System Information* widget on the *Status* tab. For more information about the *System Information* widget, see "System Information widget" on page 27.
- It is used in the command prompt of the CLI.
- It is used as the SNMP system name. For information about SNMP, see "Configuring the SNMP agent" on page 47.

The *System Information* widget and the `get system status` CLI command will display the full host name. However, if the host name is longer than 16 characters, the CLI and other places display the host name in a truncated form ending with a tilde ( ~ ) to indicate that additional characters exist, but are not displayed.

For example, if the host name is FortiWeb1234567890, the CLI prompt would be `FortiWeb123456789~#`.

Administrators whose access profiles permit *Write* access to items in the *System Configuration* category can change the host name.

**Note:** You can also configure the local domain name of the FortiWeb unit. For details, see "Configuring the DNS settings" on page 42.

### To change the host name of the FortiWeb unit

1. Go to *System* > *Status* > *Status*.
2. In the *System Information* widget, in the *Host Name* row, click *Change*.
3. In the *New Name* field, type a new host name.

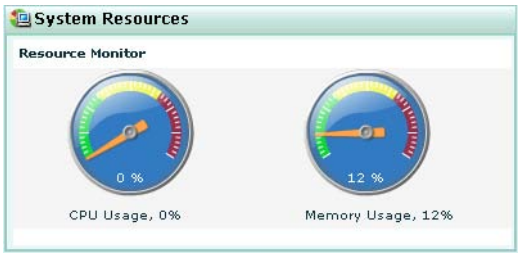
   The host name may be up to 35 characters in length. It may include US-ASCII letters, numbers, hyphens, and underscores. Spaces and special characters are not allowed.
4. Click *OK*.

## System Resources widget

The *System Resources* widget displays the CPU and memory usage.

To view the *System Resources* widget, go to *System* > *Status* > *Status*.

**Table 7:** *System Resources* **widget**



| Name of the GUI item | Description |
|---|---|
| **CPU Usage** | The current CPU usage displayed as a dial gauge and as a percentage.<br>The web-based manager displays CPU usage for core processes only. CPU usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded. |
| **Memory Usage** | The current memory (RAM) usage displayed as a dial gauge and as a percentage.<br>The web-based manager displays memory usage for core processes only. Memory usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded. |

## CLI Console widget

The *CLI Console* widget enables you to enter command lines through the web-based manager, without making a separate Telnet, SSH, or local console connection to access the CLI.

**Note:** The *CLI Console* widget requires that your web browser support JavaScript.

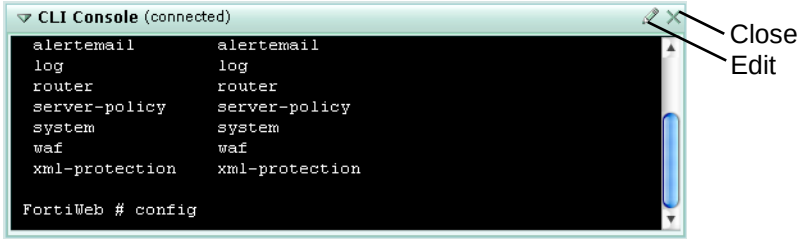
To use the console, first click within the console area. Doing so will automatically log you in using the same administrator account you used to access the web-based manager. You can then enter commands by typing them. Alternatively, you can copy and paste commands from or into the *CLI Console*.

**Note:** The prompt, by default the model number such as `FortiWeb-1000B #`, contains the host name of the FortiWeb unit. To change the host name, see "Changing the FortiWeb unit's host name" on page 29.

For information on available commands, see the *FortiWeb CLI Reference*.

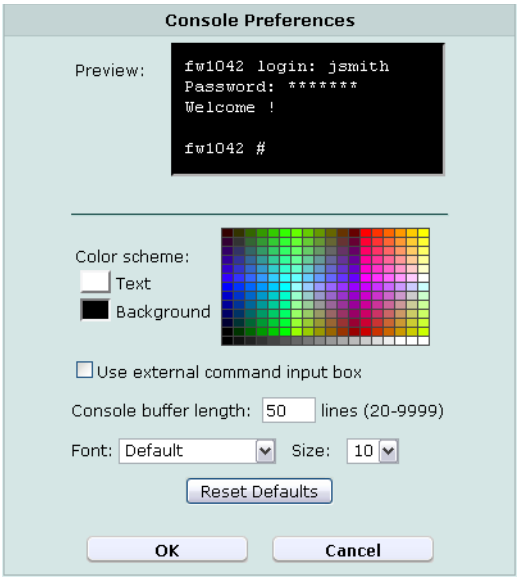
To use the *CLI Console* widget, go to *System* > *Status* > *Status*.

**Table 8:** *CLI Console* **widget**




| Name of the GUI item | Description |
|---|---|
| **Close** | Click to hide the widget. It will no longer be displayed on the dashboard unless you add it again by clicking *Add Content*. |
| **Edit** | Click to open the *Console Preferences* pop-up window, where you can change the buffer length, input method, and the appearance of the console by defining fonts and colors for the text and background. |

**Table 9:** *Console Preferences* **window**




| *Name of the GUI item* | *Description* |
|---|---|
| **Preview** | A preview of your changes to the *CLI Console* widget's appearance. |
| **Text** | Click the current color swatch to the left of this label, then click a color from the color palette to the right to change the color of the text in the *CLI Console*. |
| **Background** | Click the current color swatch to the left of this label, then click a color from the color palette to the right to change the color of the background in the *CLI Console*. |
| **Use external command input box** | Enable to display a command input field below the normal console emulation area. When this option is enabled, you can enter commands by typing them into either the console emulation area or the external command input field. |
| **Console buffer length** | Enter the number of lines the console buffer keeps in memory. The valid range is from 20 to 9999. |
| **Font** | Select a font from the list to change the display font of the *CLI Console*. |
| **Size** | Select the size in points of the font. The default size is 10 points. |

## Alert Message Console widget

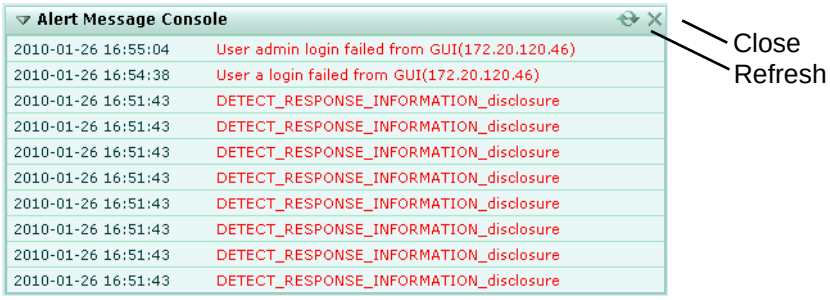
The *Alert Message Console* widget displays log-based alert messages.

Alert messages help you track system events on your FortiWeb unit such as firmware changes, and network events such as detected attacks. Each message shows the date and time that the event occurred.

**Tip:** Alert messages can also be delivered by email, Syslog, or SNMP. For more information, see "Enabling logging and alerts" on page 253, "Configuring logging to a Syslog server or FortiAnalyzer unit" on page 259, "Configuring the SNMP agent" on page 47, and "Configuring and testing alerts" on page 260.

To view the *Alert Message Console* widget, go to *System* > *Status* > *Status*.

**Figure 4:** *Alert Message Console* **widget**

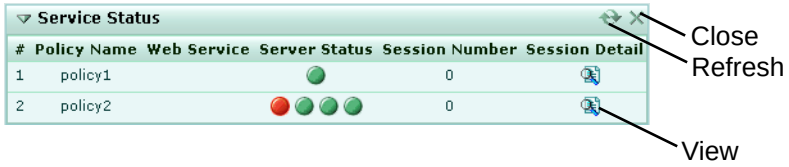



## Service Status widget

The *Service Status* widget lists policies that you have configured, the connectivity status of servers associated with the policy, and the number of sessions currently governed by the policy.

To view the *Service Status* widget, go to *System* > *Status* > *Status*.

**Table 10:** *Service Status* **widget**

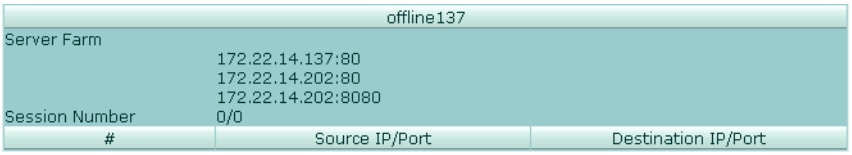



| *Name of the GUI item* | *Description* |
|---|---|
| # | The index number of the policy. |
| **Policy Name** | The name of the policy.<br>For information on policies, see "Configuring policies" on page 91. |
| **Web Service** | If the policy applies an XML protection profile, and you have enabled *WSDL Verify* in the XML protection profile, this column indicates which web services are permitted by the policy according to the selected web services group.<br>For more information, see "WSDL Verify" on page 147. |
| **Service Status** | The connectivity status with each physical server in a server farm.<br>There may be multiple icons in this column.To determine which physical server is associated with an icon, hover your mouse cursor over the icon. The name of the physical server then appears in a tool tip.<br>• **Green icon**: The server health check is currently detecting that the physical server is responsive to connections.<br>• **Flashing yellow-to-red icon**: The server health check is currently detecting that the physical server is ***not*** responsive to connections. The method that the FortiWeb unit will use to reroute connections to an available server varies by your configuration of *Deployment Mode*.<br>For information on server health checks, see "Configuring server health checks" on page 109.<br>**Note:** For a single server, there is no associated server health check, and therefore no icon in this column. To make server health checks for a single server, instead of configuring the policy with a *Deployment Mode* of *Single Server*, create a server farm and add that physical server as the sole member, then select that server farm in the policy. |
| **Session Number** | The total number of sessions currently being governed by the policy. |

| | |
|---|---|
| **Session Detail** | Click the *View* icon to display a detail table containing:<br>• the IP address and port number used by the policy to forward traffic to each physical server<br>• the total number of sessions currently governed by the policy<br>• the source and destination IP address and TCP port number of each session currently governed by the policy |
| **Close** | Click to hide the widget. It will no longer be displayed on the dashboard unless you add it again by clicking *Add Content*. |
| **Refresh** | Click to refresh the information displayed on the widget. |

Clicking the *View* icon in the *Session Detail*column displays a table of session details.

**Figure 5: Service Status widget: Session Detail**




## Policy Summary widget

The *Policy Summary* widget displays three graphs:

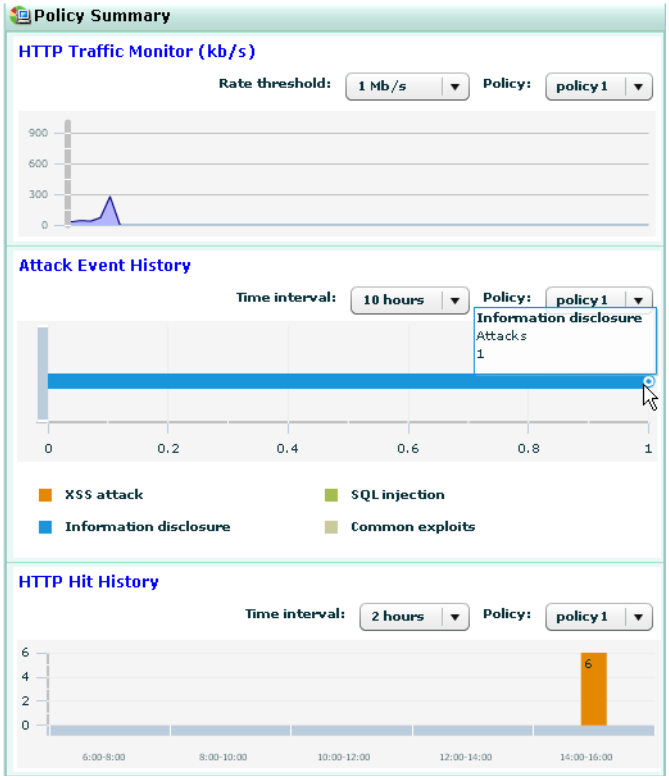
- **HTTP Traffic Monitor**: Displays the traffic volume throughput during each time period.
- **Attack Event History**: Displays the number of each type of common exploit, SQL injection, cross-site scripting (XSS), or information disclosure attacks that were prevented.
- **HTTP Hit History**: Displays the total number of requests.

For each graph, you can select which policy's statistics to view, and the size of the interval (*Rate threshold* or *Time interval*) represented by each unit on the graph.

By positioning your cursor over a point in the graph, you can display information for that point in time, such as (for *HTTP Traffic Monitor*) the traffic volume at that point in time.

To view the *Policy Summary* widget, go to *System* > *Status* > *Status*.

**Figure 6:** *Policy Summary* **widget**




# Configuring the network interfaces

*System* > *Network* > *Interface* displays a list of the FortiWeb unit's network interfaces associated with the physical ports, as well as VLAN subinterfaces (see "About VLANs" on page 39).

You ***must*** configure at least one of the FortiWeb unit's network interfaces for you to be able to connect to the CLI and web-based manager, which require an IP address.

**Note:** If the FortiWeb unit is operating in transparent mode and you will therefore instead configure a bridge, do ***not*** configure any physical network interfaces other than port1. For details, see "Configuring bridges" on page 39.

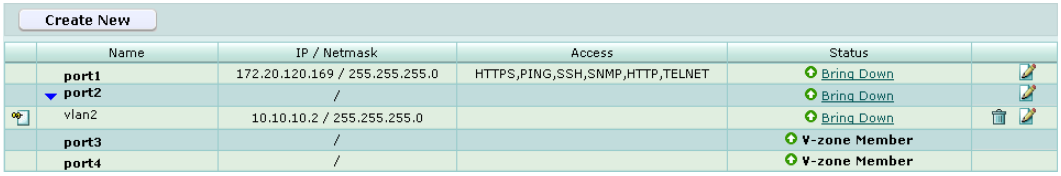
Depending on your network topology and other considerations, to enable the FortiWeb unit to connect to your network and to the web servers it protects, you may need to configure one or more of the FortiWeb unit's other network interfaces. You can configure each network interface separately, with its own IP address, netmask, and accepted administrative access protocols.

**Caution:** Enable administrative access only on network interfaces connected to trusted private networks or directly to your management computer. If possible, enable only secure administrative access protocols such as HTTPS or SSH. Failure to restrict administrative access could compromise the security of your FortiWeb unit.

**Note:** You can restrict which IP addresses are permitted to log in as a FortiWeb administrator through the network interfaces. For details, see "Configuring administrator accounts" on page 53.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have *Read* permission to items in the *Network Configuration* category. For details, see "About permissions" on page 58.

**Table 11:** *Interface* **tab**



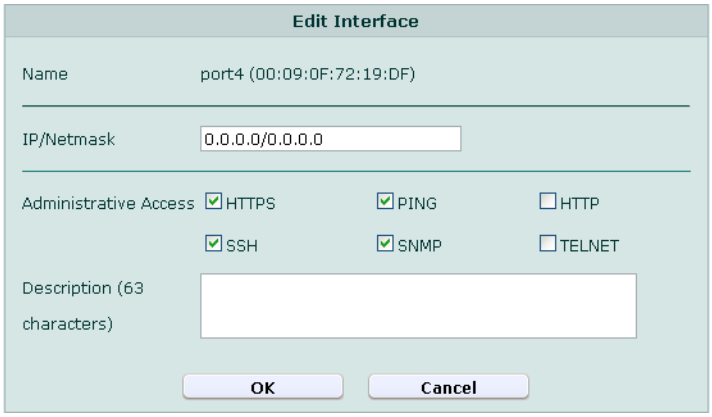

| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to create a VLAN subinterface. For details, see "About VLANs" on page 39 and "To add a VLAN subinterface" on page 37. |
| (No column heading.) | The description for the network interface or VLAN subinterface. To view the description, hover your cursor over the icon. |
| **Name** | The name of the network interface, usually directly associated with one physical link as indicated by its name, such as *port1*. |
| **IP/Netmask** | The IP address and netmask of the network interface, separated by a slash ( / ). |
| **Access** | The administrative access services that are enabled on the network interface, such as HTTPS for the web-based manager. |
| **Status** | Indicates the "up" (available) or "down" (unavailable) administrative status of the network interface.<br>• **Green up arrow**: The network interface is up and permitted to receive or transmit traffic. To disable the network interface, click *Bring Down*.<br>• **Red down arrow**: The network interface is down and not permitted to receive or transmit traffic. To enable the network interface, click *Bring Up*. |
| (No column heading.) | Click *Edit* to view or modify the settings of the network interface or VLAN subinterface.<br>Click *Delete* to remove a VLAN subinterface. This icon does not appear for network interfaces associated with a physical port, which cannot be removed. |

### To edit a network interface

1 Go to *System* > *Network* > *Interface*.

2 In the row corresponding to a network interface, click *Edit*.

3 Configure the following:




| *Name of the GUI item* | *Description* |
|---|---|
| **Name** | The name (such as *port2*) and media access control (MAC) address of this network interface. |
| **IP/Netmask** | Type the IP address/subnet mask. The IP address must be on the same subnet as the network to which the interface connects. Two network interfaces cannot have IP addresses on the same subnet. |
| **Administrative Access** | Enable the types of administrative access that you want to permit on this interface. |
| **HTTPS** | Enable to allow secure HTTPS connections to the web-based manager through this network interface.<br>For information on configuring the port number on which the FortiWeb listens for these connections, see "Configuring the web-based manager's global settings" on page 60. |
| **PING** | Enable to allow ICMP ping responses from this network interface. |
| **HTTP** | Enable to allow HTTP connections to the web-based manager through this network interface.<br>For information on configuring the port number on which the FortiWeb listens for these connections, see "Configuring the web-based manager's global settings" on page 60.<br>**Caution:** HTTP connections are ***not*** secure, and can be intercepted by a third party. If possible, enable this option only for network interfaces connected to a trusted private network, or directly to your management computer. Failure to restrict administrative access through this protocol could compromise the security of your FortiWeb unit. |
| **SSH** | Enable to allow SSH connections to the CLI through this network interface. |
| **SNMP** | Enable to allow SNMP connections to this network interface.<br>**Note:** This setting only configures which network interface will ***receive*** SNMP queries. To configure which network interface will ***send*** traffic, see "Configuring the SNMP agent" on page 47. |
| **TELNET** | Enable to allow Telnet connections to the CLI through this network interface.<br>**Caution:** Telnet connections are ***not*** secure, and can be intercepted by a third party. If possible, enable this option only for network interfaces connected to a trusted private network, or directly to your management computer. Failure to restrict administrative access through this protocol could compromise the security of your FortiWeb unit. |
| **Description** | Type a comment. The comment may be up to 63 characters long. This field is optional. |

4 Click *OK*.

If you were connected to the web-based manager through this network interface, you are now disconnected from it.

5 To access the web-based manager again, in your web browser, modify the URL to match the new IP address of the network interface. For example, if you configured the network interface with the IP address 172.16.1.20, you would browse to https://172.16.1.20.

If the new IP address is on a different subnet than the previous IP address, and your computer is directly connected to the FortiWeb unit, you may also need to modify the IP address and subnet of your computer to match the FortiWeb unit's new IP address.

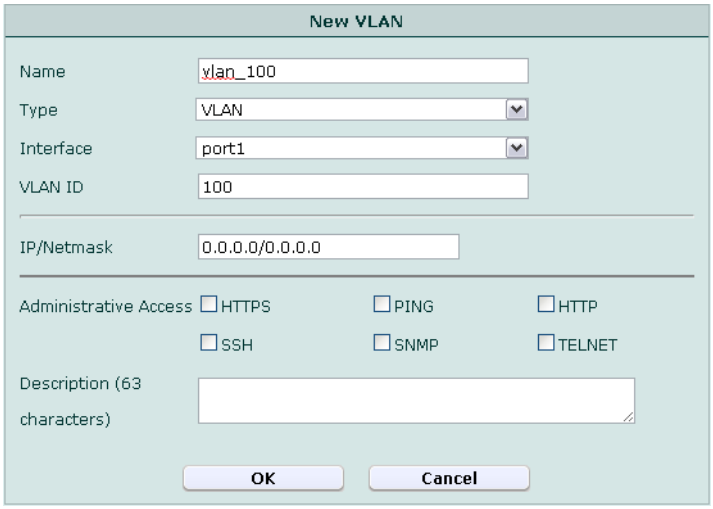
### To add a VLAN subinterface

**Note:** When the FortiWeb unit is operating in transparent mode, VLAN subinterfaces do not support Cisco discovery protocol (CDP). For more information about VLANs, see "About VLANs" on page 39.

1 Go to *System* > *Network* > *Interface*.

2 Click *Create New*.

3 Configure the following:




| *Name of the GUI item* | *Description* |
|---|---|
| **Name** | Type the name (such as `vlan_100`) of this VLAN subinterface.<br>This field cannot be modified if you are editing an existing entry. To modify the name, delete the entry, then recreate it using the new name. |
| **Type** | Indicates whether the interface is directly associated with a physical network port, or is instead a VLAN subinterface.<br>This option is set by the system automatically, and cannot be changed. |
| **Interface** | Select the name of the network interface with which the VLAN subinterface will be associated. |

**VLAN ID**

Type the VLAN IDof packets that belong to this VLAN subinterface.

- If one physical network port (that is, a VLAN trunk) will handle multiple VLANs, create multiple VLAN subinterfaces on that port, one for each VLAN ID that will be received.
- If multiple different physical network ports will handle the same VLANs, on each of the ports, create VLAN subinterfaces that have the same VLAN IDs.

The valid range is between 1 and 4094 and must match the VLAN ID added by the IEEE 802.1q-compliant router or switch connected to the VLAN subinterface.

For more information on VLANs, see "About VLANs" on page 39.

For the maximum number of interfaces, including VLAN subinterfaces, see "Appendix B: Maximum values matrix Appendix B: Maximum values matrix" on page 291.

**Note:** Inter-VLAN routing is not supported if the FortiWeb unit is operating in transparent mode. In that case, you must configure the same VLAN IDs on each physical network port.

**IP/Netmask**

Type the IP address/subnet mask, if any. The IP address must be on the same subnet as the network to which the interface connects. Two network interfaces cannot have IP addresses on the same subnet.

**Administrative Access**

Enable the types of administrative access that you want to permit on this interface.

**HTTPS**

Enable to allow secure HTTPS connections to the web-based manager through this interface.

For information on configuring the port number on which the FortiWeb listens for these connections, see "Configuring the web-based manager's global settings" on page 60.

**PING**

Enable to allow ICMP ping responses from this interface.

**HTTP**

Enable to allow HTTP connections to the web-based manager through this interface.

For information on configuring the port number on which the FortiWeb listens for these connections, see "Configuring the web-based manager's global settings" on page 60.

**Caution:** HTTP connections are ***not*** secure, and can be intercepted by a third party. If possible, enable this option only for network interfaces connected to a trusted private network, or directly to your management computer. Failure to restrict administrative access through this protocol could compromise the security of your FortiWeb unit.

**SSH**

Enable to allow SSH connections to the CLI through this interface.

**SNMP**

Enable to allow SNMP connections to this interface.

**Note:** This setting only configures which network interface will ***receive*** SNMP queries. To configure which network interface will ***send*** traffic, see "Configuring the SNMP agent" on page 47.

**TELNET**

Enable to allow Telnet connections to the CLI through this interface.

**Caution:** Telnet connections are ***not*** secure, and can be intercepted by a third party. If possible, enable this option only for network interfaces connected to a trusted private network, or directly to your management computer. Failure to restrict administrative access through this protocol could compromise the security of your FortiWeb unit.

**Description**

Type a description or other comment. The comment may be up to 63 characters long.

This field is optional.

**4** Click *OK*.

### About VLANs

Similar to local area networks (LANs), IEEE 802.1q virtual LANs (VLANs) can be used to reduce the size of a broadcast domain and thereby reduce the amount of broadcast traffic received by network hosts, improving network performance.

Unlike physical LANs, VLANs do not require you to install separate hardware switches and routers to achieve this effect. Instead, VLAN-compliant switches such as FortiWeb units restrict broadcast traffic based upon whether its VLAN ID matches that of the destination network. As such, VLAN trunks can be used to join physically distant broadcast domains as if they were close.

The VLAN ID is part of the tag that is inserted into each Ethernet frame in order to identify traffic for a specific VLAN. VLAN header addition is handled automatically by FortiWeb units, and does not require that you adjust the maximum transmission unit (MTU). Depending on whether the device receiving a packet operates at Layer 2 or Layer 3 of the network, this tag may be added, removed, or rewritten before forwarding to other nodes on the network.

For example, a Layer 2 switch or FortiWeb unit operating in transparent mode would typically add or remove a tag when forwarding traffic among members of the VLAN, but would ***not*** route tagged traffic to a different VLAN ID. In contrast, a FortiWeb unit operating in inline protection mode, inspecting the traffic to make routing decisions based upon higher-level layers/protocols, might route traffic between different VLAN IDs (also known as inter-VLAN routing) if indicated by its policy, such as if it has been configured to do WSDL-based routing.

## Configuring bridges

*System* > *Network* > *V-zone* displays a list of network ports that are configured as bridges.

Bridges allow network connections to travel through the FortiWeb unit's physical network ports ***without*** explicitly connecting to one of its IP addresses.

Bridges are used when the FortiWeb unit is operating in transparent mode and you want to be able to deploy it between incoming connections and the web server it is protecting, ***without*** changing your IP address scheme or performing routing or network address translation (NAT). In that case, do ***not*** assign IP addresses to the ports that you will connect to either the web server or to the overall network. Instead, group the two physical network ports by adding their associated network interfaces to a bridge.

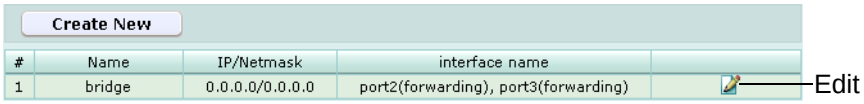
Bridges on the FortiWeb unit support IEEE 802.1d spanning tree protocol (STP) and therefore do not require that you manually test the bridged network for Layer 2 loops, and are capable of electing a root switch and designing on their own a tree that uses the minimum cost path to the root switch, although you may prefer to do so manually for design and performance reasons.

**Note:** If you prefer to disable STP, see the `config system bridge` command in the *FortiWeb CLI Reference*.

True bridges typically have no IP address of their own. They use only media access control (MAC) addresses to describe the location of physical ports within the scope of their network and do network switching at Layer 2 of the OSI model. However, if you require the ability to use an IP address to use ICMP ECHO requests (ping) to test connectivity with the physical ports comprising the bridge, you can assign an IP address to the bridge and thereby create a virtual network interface that will respond.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have *Read* permission to items in the *Network Configuration* category. For details, see "About permissions" on page 58.

**Table 12:** *Bridge* **tab**



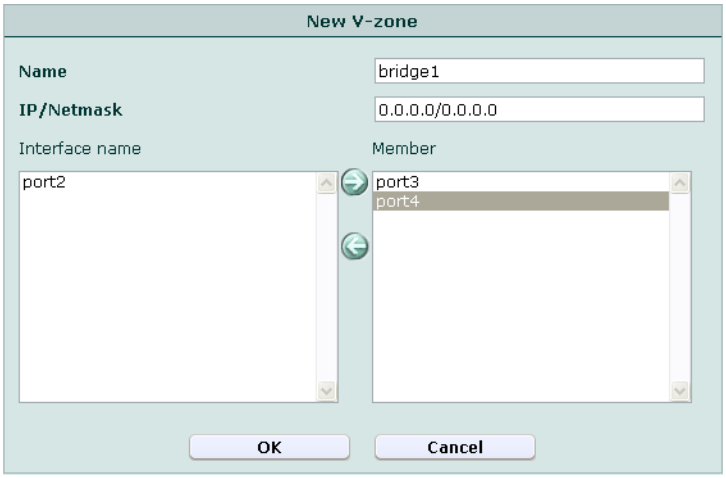

| *Name of the GUI item* | *Description* |
|---|---|
| **Name** | The name of the bridge. |
| **interface name** | The name and current status (in parentheses) of each network port that belongs to the bridge, such as *port4(forwarding)*. Possible states include:<br>• **listening**: The port is up and, using the spanning tree protocol (STP), has determined that it will participate in forwarding frames. It is receiving bridge protocol data units (BPDUs) that tell it about its distance from the root switch, but it is not yet transmitting BPDUs about itself or forwarding frames, and is not yet learning.<br>• **learning**: The port is building a database of media access control (MAC) addresses of the network nodes that are connected on the Ethernet network in order to discover which links in the tree are functional. It continues to receive BPDUs, but now is also transmitting BPDUs to allow the spanning tree to learn about its existence in preparation for forwarding. The time required to learn the spanning tree varies by the size of the network, but can be many seconds.<br>• **forwarding**: Learning is sufficient for the port to be capable of forwarding frames. It continues to receive and forward BPDUs and update its database of MAC addresses, and therefore may leave this state if STP detects a topology change that requires this port to, for example, block instead of forward frames in order to maintain a valid, non-looping tree. This is the usual state during normal operation.<br>• **disabled**: The port has been automatically disabled. Its network cable may be disconnected or the link is otherwise broken. The cause must be corrected before the port can function in the bridge.<br>• **blocked**: The port has been automatically disabled in order to prevent a Layer 2 loop in the spanning tree, because its link is redundant with another part of the tree. It is on standby and could be automatically enabled again in failover scenarios, if the redundant part of the tree fails. If you do not want this port to be disabled, you must remove the redundant part of the tree that causes this port to be blocked. |
| (No column heading.) | Click *Edit* to view or modify the settings of the bridge. For details, see "Configuring the network interfaces" on page 34. |

### To configure a bridge

1 Go to *System* > *Network* > *V-zone*.

2 Click *Create New*, or, in the row corresponding to an existing bridge, click *Edit*.

3 Configure the following:




| *Name of the GUI item* | *Description* |
|---|---|
| **Name** | Type the name of the bridge. |
| **IP/Netmask** | To create a true bridge without its own IP address, enter `0.0.0.0/0.0.0.0`.<br>To create a virtual network interface that can respond to ICMP ECHO (ping) requests, enter an IP address/subnet mask for the virtual network interface. |
| **Interface name** | A list of network interfaces that currently have no IP address of their own, nor are members of another bridge, and therefore could be members of this bridge.<br>To add a pair of network interfaces to the bridge, select their names, then click the right arrow.<br>**Note:** In transparent mode, port1 is configured with an IP address to allow CLI and web-based manager connections, and thus cannot be included in a bridge. |
| **Member** | A list of network interfaces that belong to this bridge. |

4 Click *OK*.

In the *interface name* column, each network interface's status is in parentheses next to the name of the port, such as *port4(forwarding)*. Depending on the status, each port in the bridge may or may not be immediately functional. For detail see, see "interface name" on page 40.

5 Connect one of the physical ports in the bridge to your protected servers, and the other port to your overall network.

## Configuring fail-open

*System* > *Network* > *Fail-open* enables you to configure fail-to-wire behavior in the event that the FortiWeb unit is shut down, rebooted, or unexpectedly loses power.

**Note:** Fail-open is supported only when the FortiWeb unit is operating in transparent mode, and only for models with a CP7 processor, such as the FortiWeb-3000C.

While powered off, if configured to fail open, the FortiWeb unit allows connections to pass through unfiltered.

This may be useful if you are required by contract to provide uninterrupted connectivity, or if you consider connectivity interruption to be a greater risk than being open to attack during the power interruption.

Select either:

- *Poweroff-bypass*: Behave as a wire when powered off, allowing connections to pass through, bypassing policy and profile filtering.
- *Poweroff-keep*: Interrupt connectivity when powered off.

# Configuring the DNS settings

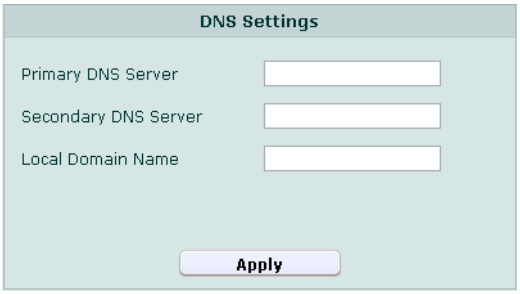
*System* > *Network* > *DNS* enables you to configure the FortiWeb unit with its local domain name, and the IP addresses of the domain name system (DNS) servers that the FortiWeb unit will query to resolve domain names such as www.example.com into IP addresses.

FortiWeb units require connectivity to DNS servers for DNS lookups. Your Internet service provider (ISP) may supply IP addresses of DNS servers, or you may want to use the IP addresses of your own DNS servers.

**Note:** For improved performance, use DNS servers on your local network.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *System Configuration* category. For details, see "About permissions" on page 58.

**Table 13:** *DNS* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Primary DNS Server** | Type the IP address of the primary DNS server. |
| **Secondary DNS Server** | Type the IP address of the secondary DNS server. |
| **Local Domain Name** | Type the name of the local domain to which the FortiWeb unit belongs, if any.<br>This field is optional. It will not appear in the `Host:` field of HTTP headers for client connections to protected web servers. |

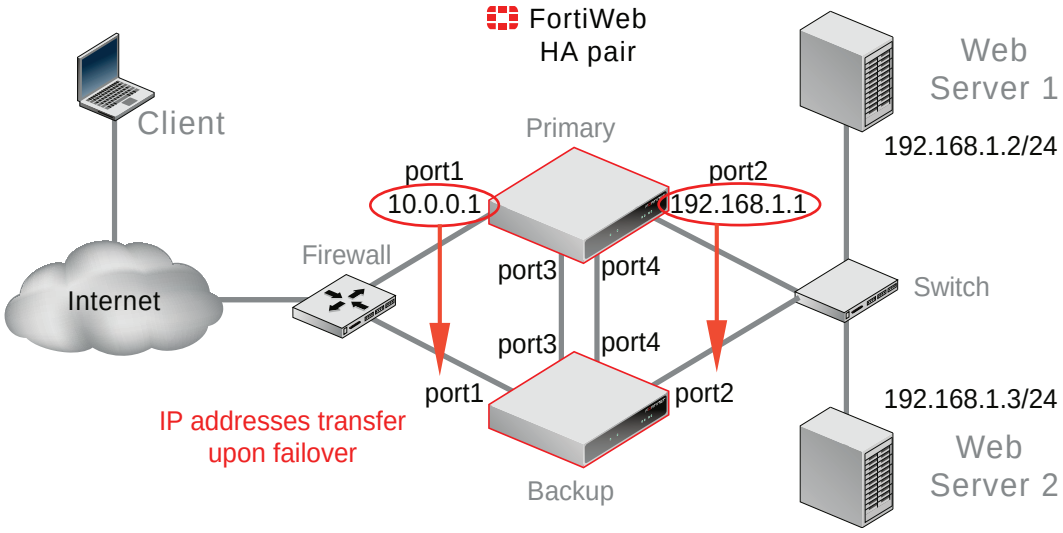
# Configuring high availability (HA)

*System* > *Config* > *HA-Config* enables you to configure a FortiWeb unit to operate as one of two units in an active-passive high availability (HA) pair.

**Note:** HA is not supported in offline protection mode. If you have an HA group configured in inline protection mode and then switch to an unsupported mode, the primary unit will be automatically reconfigured as a standalone unit. Because standalone units do not synchronize with another FortiWeb, you must then manually disable HA on the backup unit by connecting to its local console. For more information on using the local console, see the *FortiWeb CLI Reference*.

FortiWeb units that are joined as an HA pair enhance availability. If the primary unit fails, the backup unit (sometimes called a hot standby) automatically assumes the role of the primary unit. Failure is assumed after the primary unit is unresponsive to the heartbeat for the configured amount of time (*Detection interval* x *Heartbeat lost threshold*). After failure is determined, the amount of time that it takes the backup unit to assume the role of the primary unit also varies by your network's responsiveness to changeover notification and by your configuration (*ARP packet numbers* x *ARP packet interval*).

**Figure 7: HA topology and failover**

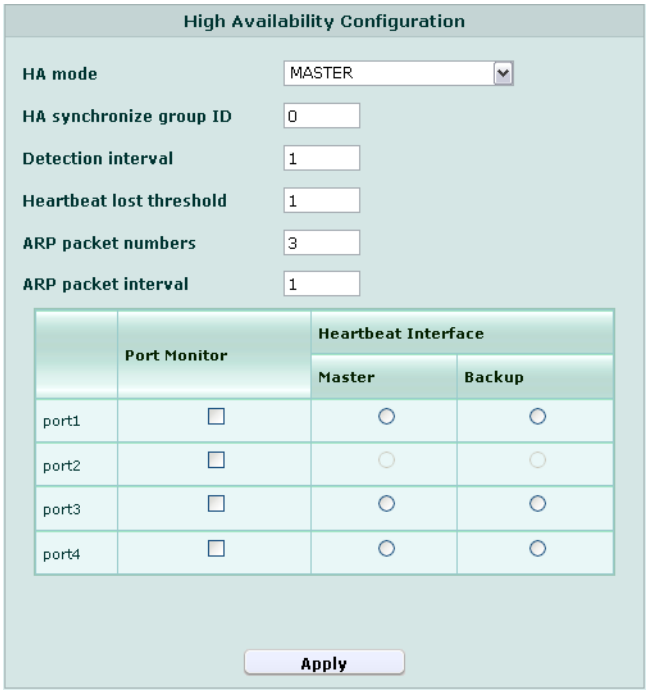



Before configuring HA, verify that your FortiWeb units meet HA pair requirements:

- Two FortiWeb units
- Identical hardware platforms
- Identical firmware versions
- Two physical network ports connected (for best results, directly, using a cross-over Ethernet cable) to the same ports on the other FortiWeb unit in order to carry HA heartbeat and synchronization traffic between members of the HA pair
- A redundant network topology: if the primary unit fails, physical network cabling and routes must be able to redirect traffic to the secondary (backup) unit

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *System Configuration* category. For details, see "About permissions" on page 58.

**Table 14:** *HA-Config* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **HA mode** | Select one of the following:<br>• **MASTER**: Operate as the primary unit in an HA pair. The FortiWeb unit will form an HA pair with another FortiWeb unit whose *HA synchronize group ID* matches, and which is connected to its *Heartbeat Interface*.<br>• **SLAVE**: Operate as the backup unit in an HA pair. The FortiWeb unit will form an HA pair with another FortiWeb unit whose *HA synchronize group ID* matches, and which is connected to its *Heartbeat Interface*. The backup unit will not scan web traffic ***unless*** it detects through the heartbeat interface that the primary unit has failed, at which time it will automatically assume the role of the primary unit by broadcasting ARP packets to notify the network of the changeover, and begin scanning web traffic in its place. It will ***not*** revert to its configured role if it detects that the primary unit is once again available. Instead, a second failover must occur in order to cause the HA pair to revert to their configured roles. Or you can manually switch over their roles.<br>• **STANDALONE**: Do not operate as a member of an HA pair. Instead, operate as a single, independent FortiWeb unit.<br>The default value is *STANDALONE*. |
| **HA synchronize group ID** | Enter a number that identifies the HA pair. ***Both members of the HA pair must have the same group ID.*** If you have more than one HA pair on the same network, each HA pair must have a different group ID.<br>Changing the group ID changes the cluster's virtual MAC address.<br>The default value is 0. The valid range is 0 to 63. |

**Detection interval**

Enter the number of 100-millisecond intervals between each heartbeat packet that the FortiWeb unit sends to the other member of the HA pair. This is also the amount of time that a FortiWeb unit waits before expecting to receive a heartbeat packet from the other unit.

This part of the configuration is synchronized between the primary and backup units.

The default value is 1 (that is, 100 milliseconds). The valid range is 1 to 20 (that is, between 100 and 2,000 milliseconds).

**Note:** Although this setting is synchronized between the primary unit and backup unit, you should initially configure both with the same *Detection interval* to prevent inadvertent failovers from occurring before the initial synchronization.

**Heartbeat lost threshold**

Enter the number of heartbeat intervals that one of the HA units retries the heartbeat and waits to receive HA heartbeat packets from the other HA unit before assuming that the other unit has failed.

This part of the configuration is synchronized between the primary and backup units.

Normally, you do not need to change this setting. Exceptions include:

- Increase the failure detection threshold if the cluster detects a failure when none has actually occurred. For example, during peak traffic times, if the primary unit is very busy, it might not respond to heartbeat packets in time, and the backup unit may assume that the primary unit has failed.
- Reduce the failure detection threshold or detection interval if administrators and HTTP clients have to wait too long before being able to connect through the new primary unit, resulting in noticeable down time.

The default value is 1. The valid range is from 1 to 60.

**Note:** Although this setting is synchronized between the primary unit and backup unit, you should initially configure both with the same *Heartbeat lost threshold* to prevent inadvertent failovers from occurring before the initial synchronization.

**ARP packet numbers**

Enter the number of times that a FortiWeb unit will broadcast address resolution protocol (ARP) packets when it becomes a primary unit in order to notify the network that a new physical port has become associated with the HA cluster's IP address and virtual MAC. This is sometimes called "using gratuitous ARP packets to train the network," and can occur when the cluster is starting up, or during a failover. Also configure *ARP packet interval*.

Normally, you do not need to change this setting. Exceptions include:

- Increase the number of times the primary unit sends gratuitous ARP packets if your cluster takes a long time to fail over or to train the network. Sending more gratuitous ARP packets may help the failover to happen faster.
- Decrease the number of times the primary unit sends gratuitous ARP packets if your cluster has a large number of VLAN interfaces and virtual domains. Because gratuitous ARP packets are broadcast, sending gratuitous ARP packets may generate a large amount of network traffic. As long as the cluster still fails over successfully, you could reduce the number of times gratuitous ARP packets are sent to reduce the amount of traffic produced by a failover.

The default value is 3. The valid range is 1 to 16.

**ARP packet interval**

Enter the number of seconds to wait between each time that the FortiWeb unit broadcasts ARP packets.

Normally, you do not need to change this setting. Exceptions include:

- Decrease the interval if your cluster takes a long time to fail over or to train the network. Sending ARP packets more frequently may help the failover to happen faster.
- Increase the interval if your cluster has a large number of VLAN interfaces and virtual domains. Because gratuitous ARP packets are broadcast, sending gratuitous ARP packets may generate a large amount of network traffic. As long as the cluster still fails over successfully, you could increase the interval between gratuitous ARP packets are sent to reduce the rate of traffic produced by a failover.

The default value is 1. The valid range is from 1 to 20.

| | |
|---|---|
| **Port Monitor** | Enable to monitor for link failure the network interfaces that correlate directly to a physical port.<br>Port monitoring (also called interface monitoring) monitors physical network ports to verify that they are functioning properly and connected to their networks. If the physical port fails or becomes disconnected, a failover will occur.<br>**Note:** To prevent unintentional failover, do not configure port monitoring ***until*** you have configured HA on both members of the HA pair, and connected the physical ports that will be monitored to the network. |
| **Heartbeat Interface** | Select which network interfaces that the primary unit (*Master*) and backup unit (*Backup*) will use to send HA heartbeat signals between each other.<br>Both units' heartbeat traffic must ***not*** travel through the same network interface. Connect two of the network interfaces to the same network interfaces on the other member of the HA pair, and separate the heartbeat traffic of the primary unit from the backup unit: one on each network interface.<br>The heartbeat network interfaces should be connected directly to each other, and not attached to your overall network.<br>**Note:** Network interfaces currently used by virtual servers or bridges cannot be selected as heartbeat interfaces. |

## About the heartbeat and synchronization

To keep the configurations concurrent so the backup unit will be ready in case of failover, HA pairs synchronize their configuration every 30 seconds. Synchronization includes WSDL files, certificates, and Schema files. (HTTP sessions, state data related to protection profile features, and log messages, however, are ***not*** synchronized. Upon failover, sessions must be re-formed with the new primary unit.)

Only the FortiWeb unit that is currently acting as the primary unit, however, ***uses*** the configured IP addresses for its network interfaces. The backup unit will ***only*** use the configured IP addresses if a failover occurs, and it therefore must assume the role of the primary unit.

**Note:** Because backup units lack IP addresses, while acting as a backup unit, a FortiWeb unit will only be accessible by local console. For more information on using the local console's CLI, see the *FortiWeb CLI Reference*.

Heartbeat and synchronization traffic occur over the network interfaces that you have configured in *Heartbeat Interface*, using multicast UDP on port numbers 5055 (heartbeat) and 5056 (synchronization). The multicast IP address 224.0.0.1 is hard-coded, and cannot be configured.

Failover is triggered by any interruption to either the heartbeat ***or*** a port monitored network interface whose length of time exceeds your configured limits (*Detection interval* x *Heartbeat lost threshold*). While the primary unit is unresponsive, the backup unit:

1. Notifies the network that the IP addresses are now associated with its virtual MAC addresses.
2. Performs the role of the primary unit.

When the primary unit resumes responsiveness to the heartbeat, both the backup unit and the primary unit will ***not*** revert to their configured HA roles. Instead, a second failover must occur in order to cause the HA pair to revert to their configured roles. Or you can manually switch over their roles.

Because log messages are not synchronized, after a failover, you may notice that there is a gap in the primary unit's log files that corresponds to the period of its down time. These log files, during which the backup unit was acting as the primary unit, are stored on the backup unit.

# Configuring the SNMP agent

*System* > *Config* > *SNMP v1/v2c* enables you to configure the FortiWeb unit's simple network management protocol (SNMP) agent to allow queries for system information and/or to send traps (alarms or event messages) to the computer that you designate as its SNMP manager. In this way you can use an SNMP manager to monitor the FortiWeb unit.

Before you can use SNMP, you must activate the FortiWeb unit's SNMP agent and add it as a member of at least one community. You must also enable SNMP access on the network interface through which the SNMP manager will connect. (See "Configuring the network interfaces" on page 34.)

On the SNMP manager, you must also verify that the SNMP manager is a member of the community to which the FortiWeb unit belongs, and compile the necessary Fortinet-proprietary management information blocks (MIBs) and Fortinet-supported standard MIBs. For information on MIBs, see "Appendix C: SNMP MIB support" on page 293.

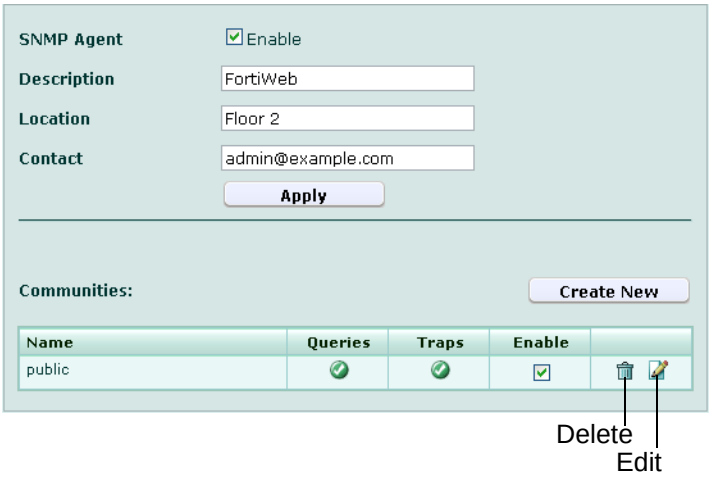
**Caution:** Failure to configure the SNMP manager as a host in a community to which the FortiWeb unit belongs, or to supply it with required MIBs, will cause the SNMP monitor to be unable to query or receive traps from the FortiWeb unit.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *System Configuration* category. For details, see "About permissions" on page 58.

### To configure the SNMP agent

1 Go to *System* > *Config* > *SNMP v1/v2c*.

2 Configure the following and click *OK*.




| *Name of the GUI item* | *Description* |
|---|---|
| **SNMP Agent** | Enable to activate the SNMP agent, enabling the FortiWeb unit to send traps and/or receive queries for the communities in which you have enabled queries and/or traps.<br>For more information on communities, see "Configuring an SNMP community" on page 48. |
| **Description** | Enter a comment about the FortiWeb unit. The description can be up to 35 characters long, and can contain only letters (a-z, A-Z), numbers, hyphens ( - ) and underscores ( _ ). |

| | | |
|---|---|---|
| **Location** | | Enter the physical location of the FortiWeb unit. The location can be up to 35 characters long, and can contain only letters (a-z, A-Z), numbers, hyphens ( - ) and underscores ( _ ). |
| **Contact** | | Enter the contact information for the administrator or other person responsible for this FortiWeb unit, such as a phone number or name. The contact information can be up to 35 characters long, and can contain only letters (a-z, A-Z), numbers, hyphens ( - ) and underscores ( _ ). |
| **Apply** | | Click to save changes made to the description, location, and contact information. |
| **Create New** | | Click *Create New* to add a new SNMP community. You can add up to 3 communities. You must add at least one community for SNMP to be functional.<br>For more information, see "Configuring an SNMP community" on page 48. |
| **Communities** | | The list of SNMP communities to which the FortiWeb unit belongs. |
| | **Name** | The name of the SNMP community. |
| | **Queries** | Whether or not the SNMP manager of the community is permitted to query the FortiWeb unit. |
| | **Traps** | Whether or not the FortiWeb unit will send traps to the SNMP manager of the community. |
| | **Enable** | Enable to activate the SNMP community. |
| | (No column heading.) | Click *Delete* to remove an SNMP community.<br>Click *Edit* to view or modify an SNMP community. For more information, see "Configuring an SNMP community" on page 48. |

## Configuring an SNMP community

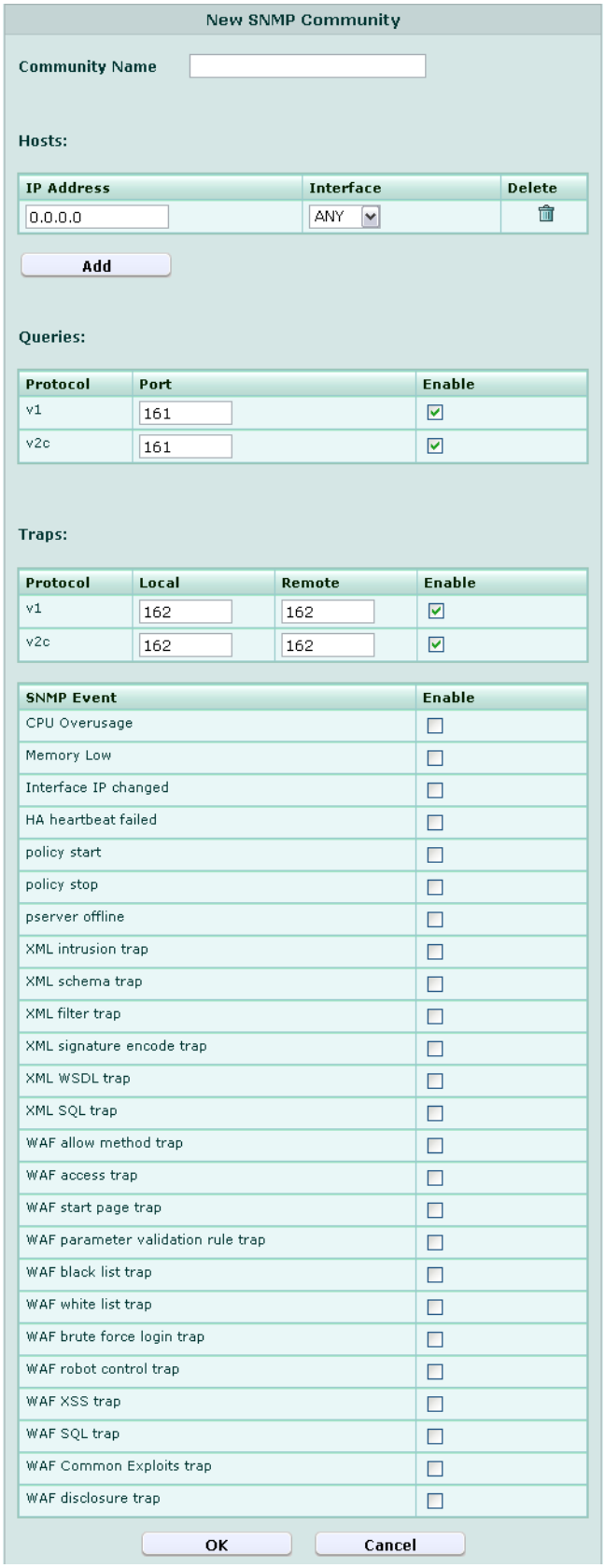
An SNMP community is a grouping of equipment for network administration purposes. You must configure your FortiWeb unit to belong to at least one SNMP community so that community's SNMP managers can query the FortiWeb unit's system information and/or receive SNMP traps from the FortiWeb unit.

You can add up to three SNMP communities. Each community can have a different configuration for queries and traps, and the set of events which trigger a trap. You can also add the IP addresses of up to eight SNMP managers to each community, which designate the destination of traps and which IP addresses are permitted to query the FortiWeb unit.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *System Configuration* category. For details, see "About permissions" on page 58.

### To add an SNMP community to the FortiWeb unit's SNMP agent

1. Go to *System* > *Config* > *SNMP v1/v2c*.
2. Click *Create New*.
3. Configure the following, then click *OK*:


New SNMP Community
Community Name
Hosts:
IP Address
Interface
Delete
0.0.0.0
ANY
Add
Queries:
Protocol
Port
Enable
v1
161
v2c
161
Traps:
Protocol
Local
Remote
Enable
v1
162
162
v2c
162
162
SNMP Event
Enable
CPU Overusage
Memory Low
Interface IP changed
HA heartbeat failed
policy start
policy stop
pserver offline
XML intrusion trap
XML schema trap
XML filter trap
XML signature encode trap
XML WSDL trap
XML SQL trap
WAF allow method trap
WAF access trap
WAF start page trap
WAF parameter validation rule trap
WAF black list trap
WAF white list trap
WAF brute force login trap
WAF robot control trap
WAF XSS trap
WAF SQL trap
WAF Common Exploits trap
WAF disclosure trap
OK
Cancel

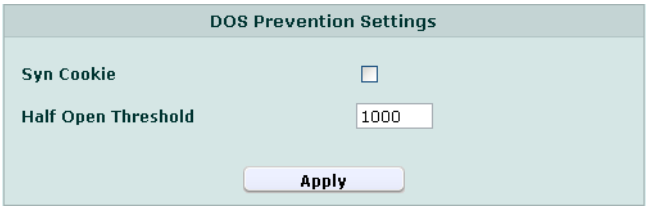
| *Name of the GUI item* | *Description* |
|---|---|
| **Community Name** | Enter the name of the SNMP community to which the FortiWeb unit and at least one SNMP manager belongs.<br>The FortiWeb unit will not respond to SNMP managers whose query packets do not contain a matching community name. Similarly, trap packets from the FortiWeb unit will include community name, and an SNMP manager may not accept the trap if its community name does not match. |
| **Hosts** | |
| **IP Address** | Enter the IP address of the SNMP manager that, if traps and/or queries are enabled in this community:<br>• will receive traps from the FortiWeb unit<br>• will be permitted to query the FortiWeb unit<br>SNMP managers have read-only access.<br>To allow any IP address using this SNMP community name to query the FortiWeb unit, enter `0.0.0.0`.<br>**Note:** Entering `0.0.0.0` effectively disables traps if there are no other host IP entries, because there is no specific destination for trap packets. If you do not want to disable traps, you must add at least one other entry that specifies the IP address of an SNMP manager. |
| **Interface** | Select either *ANY* or the name of the network interface from which the FortiWeb unit will send traps and reply to queries.<br>**Note:** You must select a specific network interface if the SNMP manager is not on the same subnet as the FortiWeb unit. This can occur if the SNMP manager is on the Internet or behind a router.<br>**Note:** This option only configures which network interface will ***send*** SNMP traffic. To configure which network interface will ***receive*** queries, see "Configuring the network interfaces" on page 34. |
| **Delete** | Click to remove an SNMP manager from the SNMP community configuration. |
| **Add** | Click to add an SNMP manager entry. You can add up to eight SNMP managers to each community. |
| **Queries** | Enter the port number (161 by default) on which the FortiWeb unit listens for SNMP queries from the SNMP managers in this community, then enable queries for either or both SNMP v1 and SNMP v2c. |
| **Traps** | Enter the port number (162 by default) that will be the source (*Local*) port number and destination (*Remote*) port number for trap packets sent to SNMP managers in this community, then enable traps for either or both SNMP v1 and SNMP v2c. |
| **SNMP Event** | Enable the types of SNMP traps that you want the FortiWeb unit to send to the SNMP managers in this community.<br>While most trap events are described by their names, the following events occur when a threshold has been exceeded:<br>• **CPU Overusage**: CPU usage has exceeded 80%.<br>• **Memory Low**: Memory (RAM) usage has exceeded 80%.<br>For more information on supported traps and queries, see "Appendix C: SNMP MIB support" on page 293. |

# Configuring DoS protection

*DOS Protection* > *SYN Flood* > *SYN Flood* enables you to configure protection from TCP SYN flood-style denial of service (DoS) attacks. Protection will be applied to connections matching any policy.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *System Configuration* category. For details, see "About permissions" on page 58.

**Table 15:** *SYN Flood* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Syn Cookie** | Enable to detect TCP SYN flood attacks. Also configure *Half Open Threshold.* |
| **Half Open Threshold** | Enter the maximum number of TCP SYN packets, including retransmission, that may be sent per second to a destination address. If this threshold is exceeded, the FortiWeb unit detects a DoS attack, and will ignore additional traffic from that source address. |

# Configuring the operation mode

*System* > *Config* > *Operation* enables you to configure the operation mode of the FortiWeb unit.

FortiWeb units can operate in one of the following modes:

- **Inline Protection:** Reverse proxy traffic destined for a virtual server's network interface and IP address, forwarding it to a physical server, and apply the first applicable policy. The FortiWeb unit logs, blocks, or modifies traffic according to the matching policy and its protection profile.
- **Offline Protection:** Pass through traffic received on the virtual server's network interface (regardless of the IP address) to the physical servers, and apply the first applicable policy. The FortiWeb unit logs or blocks traffic according to the matching policy and its protection profile, but does ***not*** otherwise modify it. (It does not, for example, apply SSL or load balance connections.)

**Caution:** Unlike in inline protection mode, actions other than *Alert* cannot be guaranteed to be successful in offline protection mode. The FortiWeb unit will attempt to block traffic that violates the policy by mimicking the client or server and requesting to reset the connection. However, the client or server may receive the reset request after it receives the other traffic due to possible differences in routing paths.

- **Transparent**: Proxy traffic destined for a physical server's IP address, and apply the first applicable policy. Traffic is received on a network port that belongs to a Layer 2 bridge, and no changes to the IP address scheme of the network are required.

The default operation mode is inline protection mode.

You will usually set the operation mode once, during installation. Exceptions include if you install the FortiWeb unit in offline protection mode for evaluation purposes, before deciding to switch to inline protection mode and actively begin filtering traffic.

**Table 16: Supported features in different operation modes**

| Feature | Inline | Offline | Transparent | |
|---|---|---|---|---|
| | | | HTTP | HTTPS |
| **Auto Learn** | Yes | Yes | Yes | Yes |
| **XML Protection** | Yes | No | No | No |
| **Parameter Validation** | Yes | Yes | Yes | Yes |
| **Page Access Rule** | Yes | No | Yes | No |
| **Server Protection Rules** | Yes | Yes | Yes | Yes |
| **Start Pages** | Yes | No | Yes | No |
| **Black List Rules** | Yes | Yes | Yes | Yes |
| **White List Rules** | Yes | Yes | Yes | Yes |
| **IP List** | Yes | No | Yes | Yes |
| **Brute Force Login** | Yes | No | Yes | Yes |
| **Robot Control** | Yes | No | Yes | Yes |
| **Allow Method** | Yes | Yes | Yes | Yes |
| **Hidden Field** | Yes | Yes | Yes | Yes |
| **URL Rewriting** | Yes | No | Yes | No |
| **HTTP Protocol Constraints** | Yes | Yes | Yes | Yes |
| **Authentication Policy** | Yes | No | Yes | No |
| **HTTP Conversion** | Yes | No | Yes | No |
| **Cookie Poisoning** | Yes | No | Yes | No |
| **SSLv2 Support** | Yes | No | N/A | No |
| **X-Forwarded-For** | Yes | No | Yes | No |
| **Information Disclosure** | Yes | Yes (alert only) | Yes | Yes (alert only) |
| **Session Management** | Yes | Yes | Yes | Yes |
| **AMF3 Support** | Yes | Yes | Yes | Yes |
| **Custom Packet Log Filter** | Yes | Yes | Yes | Yes |
| **Client Certificate Verify** | Yes | No | No | No |
| **Web Anti-Defacement** | Yes | Yes | Yes | Yes |
| **Web Vulnerability Scan** | Yes | Yes | Yes | Yes |

**Caution:** Back up your configuration before changing the operation mode. Choose your operation mode carefully. If you switch the operation mode later, you may need to re-cable your network topology to suit the operation mode, reconfigure routes, reconfigure policies, reconfigure network interfaces and virtual servers on the FortiWeb unit, and enable or disable SSL on your web servers. The FortiWeb unit will automatically delete policies that are not applicable to its new application mode. For details on policies, see “Configuring policies” on page 91. For details on backups, see “Backing up the configuration & installing firmware” on page 74.

**Note:** The physical topology must match the operation mode. For details, see the *FortiWeb Install Guide*.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *System Configuration* category. For details, see "About permissions" on page 58.

**To configure the operation mode**

1 Go to *System* > *Config* > *Operation*.

Alternatively, go to *System* > *Status* > *Status*. Then, in the *System Information* widget, in the *Operation Mode* row, click *Change*.

**Figure 8: Configuring the operation mode**

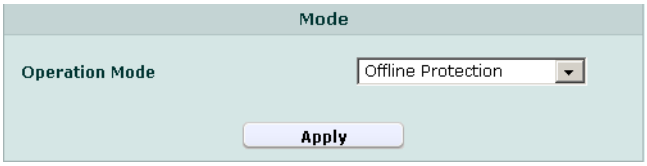
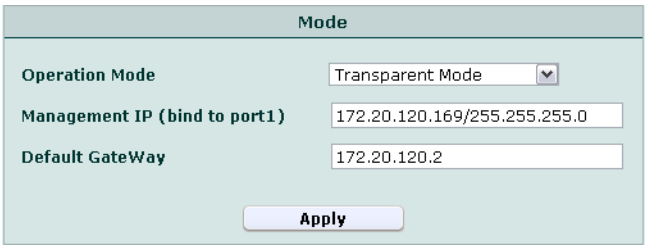



**Figure 9: Configuring the operation mode (transparent mode)**




2 From *Operation Mode*, select *Inline Protection*, *Offline Protection*, or *Transparent Mode*.

If you are changing to transparent mode, also enter the gateway and the IP address of port1 (*Management IP*).

3 Click *Apply*.

If you have not yet adjusted the physical topology to suit the new operation mode, see the *FortiWeb Install Guide*. You may also need to reconfigure IP addresses, static routes, bridges, and virtual servers, and on your web servers, enable or disable SSL.

# Configuring administrator accounts

*System* > *Admin* > *Administrators* displays a list of FortiWeb administrator accounts.

In its factory default configuration, a FortiWeb unit has one administrator account, named `admin`. The `admin` administrator has permissions that grant full access to the FortiWeb configuration and firmware. After connecting to the web-based manager or the CLI using the `admin` administrator account, you can configure additional administrator accounts with various levels of access to different parts of the FortiWeb configuration.

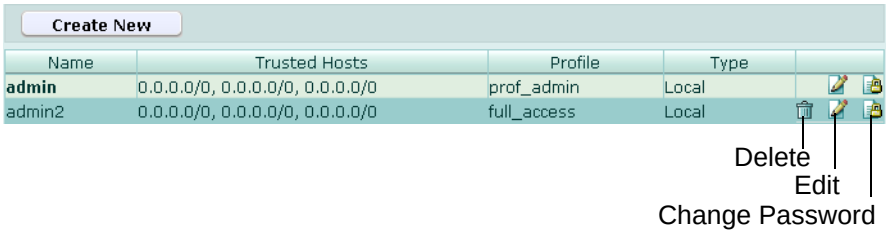
Administrators may be able to access the web-based manager and/or the CLI through the network, depending on administrator account's trusted hosts, and the administrative access protocols enabled for each of the FortiWeb unit's network interfaces. For details, see "Configuring the network interfaces" on page 34 and "About trusted hosts" on page 56.

To determine which administrators are currently logged in, use the CLI command `get system logged-users`. For details, see the *FortiWeb CLI Reference*.

**Tip:** To prevent multiple administrators from logging in simultaneously, which could allow them to inadvertently overwrite each other's changes, enable *Enable Single admin User login*. For details, see "Configuring the web-based manager's global settings" on page 60.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have *Read* permission to items in the *Admin Users* category. For details, see "About permissions" on page 58.

**Table 17:** *Administrators* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add an administrator account. |
| **Name** | The name of the administrator account. |
| **Trusted Hosts** | The IP addresses and netmasks of hosts from which the administrator is permitted to log in. |
| **Profile** | The access profile assigned to the administrator account. Access profiles determine which parts of the configuration that an administrator has permission to access. For more information on access profiles, see "Configuring access profiles" on page 56. |
| **Type** | The type of authentication for this administrator.<br>This version currently supports only authentication using a locally stored password. |
| (No column heading.) | Click *Delete* to remove the administrator account. You cannot delete the `admin` administrator account.<br>Click *Edit* to view or modify the administrator account.<br>Click *Change Password* to change the password for the administrator account. |

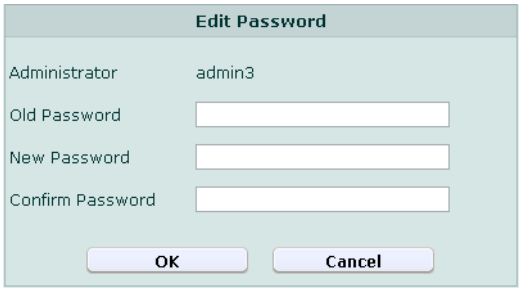
### To change an administrator account's password

1 If an administrator forgot their password or if you need to change an administrator account's password and you do not know its current password, log in as the `admin` administrator. Otherwise, you may log in with any administrator account whose access profile permits *Read* and *Write* access to items in the *Admin Users* category.

If you have forgotten the password of the `admin` administrator, you can restore the firmware to reset the FortiWeb unit to its default state, including the default administrator account and password. For details, see "Restoring firmware" on page 285.

2 Go to *System* > *Admin* > *Administrators*.

3 In the row corresponding to the administrator account, click *Change Password*.




4 In the *Old Password* field, enter the current password for the account.

This field appears only if you are not logged in as the `admin` administrator, or if you are changing the password of the `admin` administrator account.

5 In the *New Password* and *Confirm Password* fields, enter the new password.

6 Click *OK*.

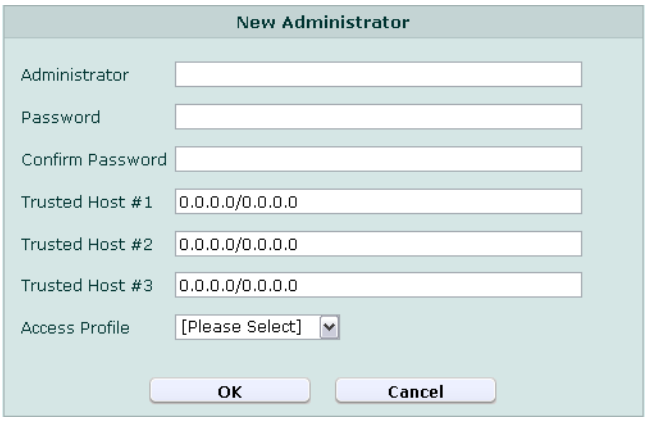
If you are changing the password for the `admin` administrator account, the FortiWeb unit logs you out. To continue using the web-based manager, you must log in again. The new password takes effect the next time that administrator account logs in.

### To configure an administrator account

1 Go to *System* > *Admin* > *Administrators*.

2 Click *Create New* to add an administrator account, or click the *Edit* icon to change an existing administrator account.

3 Configure the following and click *OK*:




| *Name of the GUI item* | *Description* |
|---|---|
| **Administrator** | Enter the name of the administrator account, such as `admin1`. |
| **Password** | Enter a password for the administrator account. For improved security, the password should be at least 6 characters long, be sufficiently complex, and be changed regularly. |
| **Confirm Password** | Re-enter the password to confirm its spelling. |

| | |
|---|---|
| **Trusted Host #1**<br>**Trusted Host #2**<br>**Trusted Host #3** | Enter the IP address and netmask from which the administrator is allowed to log in to the FortiWeb unit. You can specify up to three trusted hosts.<br>To allow login attempts from any IP address, enter `0.0.0.0/0.0.0.0`. If you allow login from any IP address, consider choosing a longer and more complex password, and limiting administrative access to secure protocols to minimize the security risk. For information on administrative access protocols, see "Configuring the network interfaces" on page 34.<br>For improved security, restrict all three trusted host addresses to the IP addresses of computers from which only this administrator will log in. For more information, see "About trusted hosts" on page 56. |
| **Access Profile** | Select either an existing access profile that indicates the permissions for this administrator account, or select *Create New* to create a new access profile in a pop-up window, without leaving the current page. For more information on access profiles, see "Configuring access profiles" on page 56.<br>You can select *prof_admin*, a special access profile used by the `admin` administrator account. However, selecting this access profile will not confer all of the same permissions as the `admin` administrator. For example, you would still not be able to reset lost administrator passwords. |

## About trusted hosts

Configuring the trusted hosts of your administrator accounts increases the security of your FortiWeb unit by further restricting administrative access. In addition to knowing the password, an administrator must connect only from the subnet or subnets you specify. You can even restrict an administrator to a single IP address if you enter only one trusted host IP address in each of the three trusted host fields, each with a netmask of 255.255.255.255.

When you configure trusted hosts for all administrator accounts, the FortiWeb unit does not respond to administrative access attempts from any other hosts. This provides the greatest degree of security. If you leave even one administrator account unrestricted, the FortiWeb unit accepts administrative access attempts for that account on any interface that has administrative access enabled, potentially exposing the unit to attempts to gain unauthorized access.

Trusted host definitions apply both to the web-based manager, and to the CLI when accessed through Telnet or SSH. Local console access to the CLI is not affected by trusted hosts, as local console access does not occur through the network.

## Configuring access profiles

*System* > *Admin* > *Access Profile* displays the list of administrator access profiles.

Access profiles determine which parts of the configuration an administrator has permission to access, and whether she or he is permitted to view (*Read*), modify (*Write*), or both.

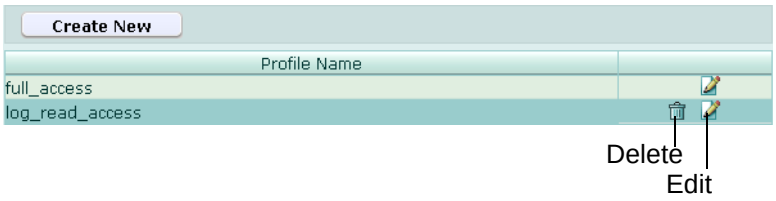
When an administrator has only read access to a feature, the administrator can access the web-based manager tab for that feature, and can use the `get` and `show` CLI command for that feature, but cannot make changes to the configuration. There are no *Create* or *Apply* buttons, or `config` CLI commands, and lists display only the *View* icon instead of icons for *Edit*, *Delete* or other modification commands. Write access is required for modification of any kind.

The `prof_admin` access profile, a special access profile assigned to the `admin` administrator account and required by it, does not appear in the list of access profiles. It exists by default and cannot be changed or deleted. If you create other administrator accounts, you may want create other access profiles with different degrees and areas of access.

For example, for an administrator whose only role is to audit the log messages, you might make an access profile named `log_access_only`.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have *Read* and *Write* permission to items in the *Admin Users* category. For details, see "About permissions" on page 58.

**Table 18:** *Access Profile* **tab**



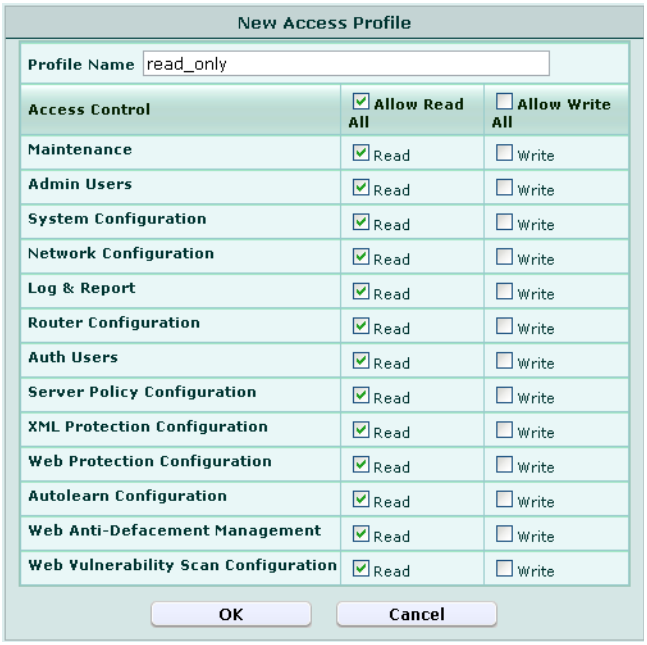

| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a new access profile. |
| **Profile Name** | The name of the access profile. |
| (No column heading.) | Click *Delete* to remove the access profile.<br>This option does not appear if this access profile is currently assigned to an administrator account.<br>Click *Edit* to modify the access profile. |

### To configure an access profile

1 Go to *System* > *Admin* > *Access Profile*.

2 Click *Create New* to add an access profile, or click *Edit* to modify an existing profile.

3 Configure the following and click *OK*:



| Name of the GUI item | Description |
|---|---|
| **Profile Name** | Enter the name of the access profile. |
| **Access Control** (*Maintenance*, *Admin Users*, etc.) | For each row associated with an area of the configuration, mark either or both the *Read* and/or *Write* check boxes to grant that type of permission.<br>Unlike the other rows, whose scope is an area of the configuration, the *Maintenance* row does not affect the configuration. Instead, it indicates whether the administrator can do special system operations such as changing the firmware. |
| **Allow Read All** | Click to mark the *Read* check box in all *Access Control* categories. |
| **Allow Write All** | Click to mark the *Write* check box in all *Access Control* categories. |

## About permissions

Depending on the account that you use to log in to the FortiWeb unit, you may not have complete access to all CLI commands or areas of the web-based manager.

Access profiles control which commands and areas an administrator account can access.

Access profiles assign either read, write, or no access to each area of the FortiWeb software. To view configurations, you must have read access. To make changes, you must have write access. For more information on configuring an access profile that administrator accounts can use, see “Configuring access profiles” on page 56.

**Table 19: Areas of control in access profiles**

| **Access control area name** | | **Grants access to** |
|---|---|---|
| **In the web-based manager** | **In the CLI** | (For each `config` command, there is an equivalent `get`/`show` command, unless otherwise noted. `config` access requires write permission. `get`/`show` access requires read permission.) |
| *Admin Users* | `admingrp` | *System* > *Admin* ***except*** *Settings* tab |
| | | `config system admin`<br>`config system accprofile` |
| *Auth Users* | `authusergrp` | *User* |
| | | `config user ...` |
| *Autolearn Configuration* | `learngrp` | *Auto Learn* and *Web Protection* > *Web Protection Profile* > *Auto Learning Profile*<br>**Note:** Because generating an auto-learning profile also generates its required components, this area also confers *Write* permission to those components in the *Web Protection Configuration* area. |
| | | `config waf web-protection-profile autolearning-profile`<br>**Note:** Because generating an auto-learning profile also generates its required components, this area also confers *Write* permission to those components in the `wafgrp` area. |
| *Log & Report* | `loggrp` | *Log&Report* |
| | | `config alertemail ...`<br>`config log ...`<br>`config system alertemail` |

**Table 19: Areas of control in access profiles**

| | | |
|---|---|---|
| *Maintenance* | `mntgrp` | *System* > *Maintenance* ***except*** *System Time* tab |
| | | `diagnose sys ...`<br>`execute backup ...`<br>`execute factoryreset`<br>`execute reboot`<br>`execute restore`<br>`execute shutdown` |
| *Network Configuration* | `netgrp` | *System* > *Network* > *Interface*<br>*System* > *Network* > *Bridge* |
| | | `config system interface`<br>`config system bridge` |
| *Router Configuration* | `routegrp` | *Router* |
| | | `config router ...` |
| *System Configuration* | `sysgrp` | *System* ***except*** *Network* > *Interface*, *Admin* > *Administrators*, *Admin* > *Access Profile*, *Maintenance* > *Backup & Restore*, and *Maintenance* > *Update Signature* tabs |
| | | `config system` ***`except`*** `accprofile, admin, interface, and alertemail`<br>`diagnose ip ...`<br>`diagnose sniffer ...`<br>`execute date ...`<br>`execute ping ...`<br>`execute ping-options ...`<br>`execute traceroute ...`<br>`execute time ...`<br>`get system` ***`except`*** `accprofile, admin, interface, and alertemail`<br>`get router all` |
| *Server Policy Configuration* | `traroutegrp` | *Server Policy* |
| | | `config server-policy` |
| *Web Anti-Defacement Management* | `wadgrp` | *Web Anti-Defacement* |
| | | `config wad website` |
| *Web Protection Configuration* | `wafgrp` | *Web Protection* ***except*** *Web Protection Profile* > *Auto Learning Profile* |
| | | `config waf` ***`except`*** `web-protection-profile autolearning-profile` |
| *Web Vulnerability Scan Configuration* | `wvsgrp` | *Web Vulnerability Scan* |
| | | N/A |
| *XML Protection Configuration* | `xmlgrp` | *XML Protection* |
| | | `config xml-protection` |

Unlike other administrator accounts, the administrator account named `admin` exists by default and cannot be deleted. The `admin` administrator account is similar to a root administrator account. This administrator account always has full permission to view and change all FortiWeb configuration options, including viewing and changing ***all*** other administrator accounts. Its name and permissions cannot be changed. It is the only administrator account that can reset another administrator's password without being required to enter that administrator's existing password.

**Caution:** Set a strong password for the `admin` administrator account, and change the password regularly. By default, this administrator account has no password. Failure to maintain the password of the `admin` administrator account could compromise the security of your FortiWeb unit.

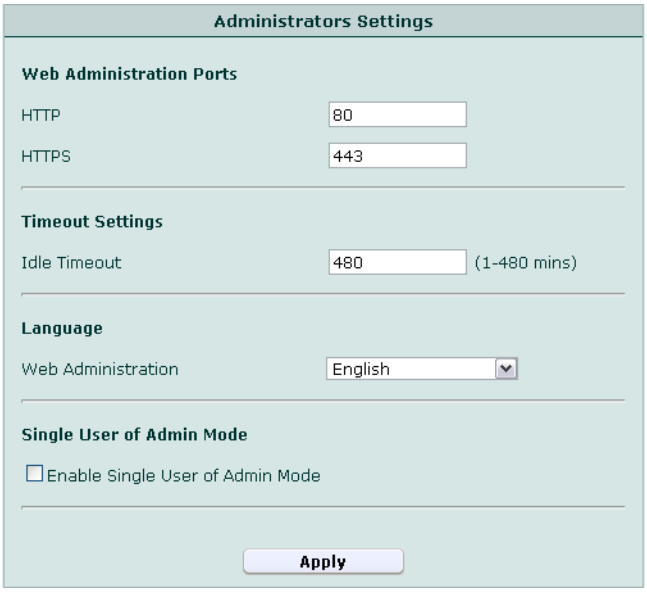
For complete access to all commands, you must log in with the administrator account named `admin`.

# Configuring the web-based manager's global settings

*System* > *Admin* > *Settings* enables you to view and configure settings for the web-based manager that apply regardless of which administrator account you use to log in.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *System Configuration* category. For details, see "About permissions" on page 58.

**Table 20:** *Settings* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Web Administration Ports** | |
| **HTTP** | Enter the TCP port number on which the FortiWeb unit will listen for HTTP administrative access. The default is 80.<br>This setting has an effect only if HTTP is enabled as an administrative access protocol on at least one network interface. For details, see "Configuring the network interfaces" on page 34. |
| **HTTPS** | Enter the TCP port number on which the FortiWeb unit will listen for HTTPS administrative access. The default is 443.<br>This setting has an effect only if HTTPS is enabled as an administrative access protocol on at least one network interface. For details, see "Configuring the network interfaces" on page 34. |
| **Timeout Settings** | |

| | |
|---|---|
| **Idle Timeout** | Enter the number of minutes that a web-based manager connection can be idle before the administrator must log in again. The maximum is 480 minutes (8 hours). To improve security, keep the idle timeout at the default value of 5 minutes. |
| **Language** | |
| **Web Administration** | Select which language to use when displaying the web-based manager.<br>The display's web pages will use UTF-8 encoding, regardless of which language you choose. UTF-8 supports multiple languages, and allows all of them to be displayed correctly, even when multiple languages are used on the same web page.<br>For example, your organization could have web sites in both English and simplified Chinese. Your FortiWeb administrators prefer to work in the English version of the web-based manager. They could use the web-based manager in English while writing rules to match content in both English and simplified Chinese ***without*** changing this setting. Both the rules and the web-based manager will display correctly, as long as all rules were input using UTF-8.<br>Usually, your text input method or your management computer's operating system should match the display, and also use UTF-8. If they do not, you may not be able to correctly display both your input and the web-based manager at the same time.<br>For example, your web browser's or operating system's default encoding for simplified Chinese input may be GB2312. However, you ***usually*** should switch it to be UTF-8 when using the web-based manager, ***unless*** you are writing regular expressions that must match HTTP client's requests, and those requests use GB2312 encoding.<br>For more information on language support in the web-based manager and CLI, see "Language support & regular expressions" on page 22.<br>**Note:** This setting does ***not*** affect the display of the CLI. |
| **Enable Single admin User login** | |
| **Enable Single admin User login** | Enable to allow only one administrator account to be logged in at any given time. If a second administrator attempts to begin a session when another administrator is already logged in, after the second administrator logs in but before they can access the web-based manager, they must either cancel their new session or disconnect the other currently logged-in administrator.<br>This option may be useful to prevent administrators from inadvertently overwriting each other's changes.<br>When multiple administrators simultaneously modify the same part of the configuration, they each edit a copy of the current, saved state of the configuration item. As each administrator makes changes, FortiWeb does ***not*** update the other administrators' working copies. Each administrator may therefore make conflicting changes without being aware of the other. The FortiWeb unit will only use whichever administrator's configuration is saved last.<br>If only one administrator may be logged in at a time, however, this problem cannot occur.<br>Disable to allow multiple administrators to be logged in. In this case, administrators should communicate with each other to avoid overwriting each other's changes. |

# Managing certificates

The *Certificates* submenu enables you to generate, import, revoke, and manage other aspects of certificates used by the FortiWeb unit.

This topic includes:

- Managing local and server certificates

- Managing OCSP server certificates
- Managing CA certificates
- Managing the certificate revocation list
- Configuring certificate verification rules

## Managing local and server certificates

*System* > *Certificates* > *Local* displays the list of server certificates that are stored locally, on the FortiWeb unit.

FortiWeb units require these certificates to present when clients request secure connections, including when:

- administrators connect to the web-based manager (HTTPS connections only)
- web clients use SSL or TLS to connect to a virtual server, if you have enabled SSL offloading in the policy (HTTPS connections and inline protection mode only)

FortiWeb units also require certificates in order to decrypt and scan HTTPS connections travelling through it if operating in offline protection or transparent mode.

Which certificate will be used, and how, depends on the purpose.

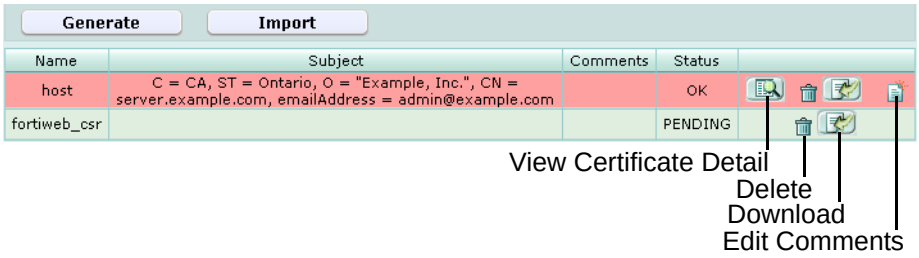
- **For connections to the web-based manager**, the FortiWeb unit presents its default certificate.

**Note:** The FortiWeb unit's default certificate does not appear in the list of local certificates. It is used only for connections to the web-based manager and cannot be removed.

- **For SSL offloading or SSL decryption**, upload certificates that do ***not*** belong to the FortiWeb unit, but instead belong to the protected servers. Then, select which one the FortiWeb unit will use when configuring the SSL option in a policy or server farm. For details, see "Uploading a certificate" on page 66.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have *Read* and *Write* permission to items in the *System Configuration* category. For details, see "About permissions" on page 58.

**Table 21:** *Local* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Generate** | Click to generate a certificate signing request. For details, see "Generating a certificate signing request" on page 63. |
| **Import** | Click to upload a certificate. For details, see "Uploading a certificate" on page 66. |
| **Name** | The name of the certificate. |

| | |
|---|---|
| **Subject** | The distinguished name (DN) located in the `Subject` field of the certificate.<br>If the row contains a certificate request which has not yet been signed, this field is empty. |
| **Comments** | The description of the certificate, if any. Click *Edit Comments* to add or modify the comment associated with the certificate or certificate signing request. |
| **Status** | The status of the local certificate.<br>• **OK**: Indicates that the certificate was successfully imported. To use the certificate, select it in a policy or server farm.<br>• **PENDING**: Indicates that the certificate request has been generated, but must be downloaded, signed, and imported before it can be used as a local certificate. |
| (No column heading.) | Click *View Certificate Detail* to view the certificate's subject, range of dates within which the certificate is valid, version number, serial number, and extensions.<br>Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a policy or server farm.<br>Click *Download* to download the entry in certificate (.cer) or certificate signing request (.csr) file format.<br>Click *Edit Comments* to add or modify the comment associated with the certificate. |

## Generating a certificate signing request

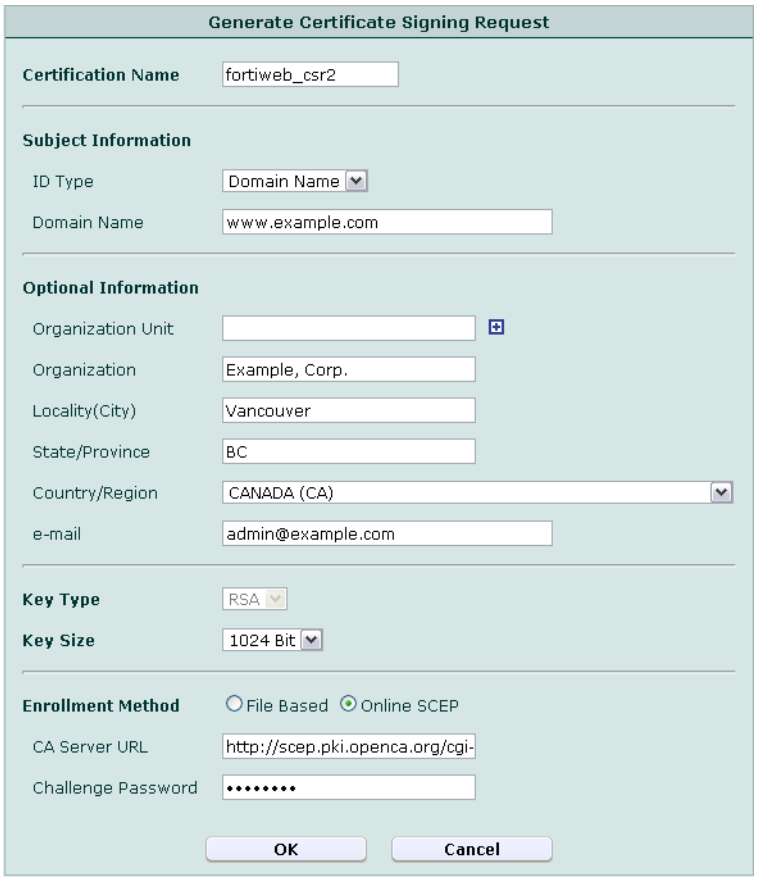
You can generate a certificate request file, based on the information you enter to identify the FortiWeb unit. Certificate request files can then be submitted for verification and signing by a certificate authority (CA).

### To generate a certificate request

1 Go to *System* > *Certificates* > *Local*.

2 Click *Generate*.

**3** Configure the following:




| *Name of the GUI item* | *Description* |
|---|---|
| **Certification name** | Enter a unique name for the certificate request, such as `fwlocal`. |
| **Subject Information** | Information that the certificate is required to contain in order to uniquely identify the FortiWeb unit. |

| | | |
|---|---|---|
| | **ID Type** | Select which type of identifier will be used in the certificate to identify the FortiWeb unit:<br>• **Host IP**<br>• **Domain Name**<br>• **E-Mail**<br>Which type you should select varies by whether or not your FortiWeb unit has a static IP address, a fully-qualified domain name (FQDN), and by the primary intended use of the certificate.<br>For example, if your FortiWeb unit has both a static IP address and a domain name, but you will primarily use the local certificate for HTTPS connections to the web-based manager by the domain name of the FortiWeb unit, you might prefer to generate a certificate based upon the domain name of the FortiWeb unit, rather than its IP address.<br>• *Host IP* requires that the FortiWeb unit have a static, public IP address. It may be preferable if clients will be accessing the FortiWeb unit primarily by its IP address.<br>• *Domain Name* requires that the FortiWeb unit have a fully-qualified domain name (FQDN). It may be preferable if clients will be accessing the FortiWeb unit primarily by its domain name.<br>• *E-Mail* does not require either a static IP address or a domain name. It may be preferable if the FortiWeb unit does not have a domain name or public IP address. |
| | **IP** | Enter the static IP address of the FortiWeb unit.<br>This option appears only if *ID Type* is *Host IP*. |
| | **Domain Name** | Type the fully-qualified domain name (FQDN) of the FortiWeb unit.<br>The domain name must resolve to the static IP address of the FortiWeb unit or protected server. For more information, see "Configuring the network interfaces" on page 34.<br>This option appears only if *ID Type* is *Domain Name*. |
| | **e-mail** | Type the email address of the owner of the FortiWeb unit.<br>This option appears only if *ID Type* is *E-Mail*. |
| **Optional Information** | | Information that you may include in the certificate, but which is not required. |
| | **Organization Unit** | Type the name of your organizational unit, such as the name of your department. (Optional.)<br>To enter more than one organizational unit name, click the + icon, and enter each organizational unit separately in each field. |
| | **Organization** | Type the legal name of your organization. (Optional.) |
| | **Locality(City)** | Type the name of the city or town where the FortiWeb unit is located. (Optional.) |
| | **State/Province** | Type the name of the state or province where the FortiWeb unit is located. (Optional.) |
| | **Country** | Select the name of the country where the FortiWeb unit is located. (Optional.) |
| | **e-mail** | Type an email address that may be used for contact purposes. (Optional.) |
| **Key Type** | | The type of algorithm used to generate the key.<br>This option cannot be changed, but appears in order to indicate that only RSA is currently supported. |

| | |
|---|---|
| **Key Size** | Select a security key size of *512 Bit*, *1024 Bit*, *1536 Bit* or *2048 Bit*. Larger keys are slower to generate, but provide better security. |
| **Enrollment Method** | Select either:<br>• *File Based*: You must manually download and submit the resulting certificate request file to a certificate authority (CA) for signing. Once signed, upload the local certificate.<br>• *Online SCEP*: The FortiWeb unit will automatically use HTTP to submit the request to the simple certificate enrollment protocol (SCEP) server of a CA, which will validate and sign the certificate. Enter the *CA Server URL* and the *Challenge Password*. |

4 Click *OK*.

The certificate is generated. If you selected file-based enrollment, you must now download and manually submit the resulting CSR to a CA. For details, see "Downloading a certificate signing request" on page 66.

## Downloading a certificate signing request

After you have generated a certificate request, you can download the request file to your management computer in order to submit the request file to a certificate authority (CA) for signing.

**To download and submit a certificate request**

1 Go to *System* > *Certificates* > *Local*.

2 Click the row that corresponds to the certificate request in order to select it.

3 Click *Download*, then select *Download*.

Your web browser downloads the certificate request (.csr) file.

4 Submit the certificate request to your CA.

- Using the web browser on the management computer, browse to the web site for your CA.
- Follow your CA's instructions to place a Base64-encoded PKCS #10 certificate request, uploading your certificate request.
- Follow your CA's instructions to download their root certificate and Certificate Revocation List (CRL), and then install the root certificate and CRL.

5 When you receive the signed certificate from the CA, install the certificate on the FortiWeb unit. For more information, see "Uploading a certificate" on page 66.

## Uploading a certificate

You can upload Base64-encoded server-type X.509 certificates or PKCS #12 RSA-encrypted certificates and keys to the FortiWeb unit.

**Note:** DSA-encrypted certificates are not supported if the FortiWeb unit is operating in offline protection mode or transparent mode.

If a local certificate is signed by an intermediate certificate authority (CA) rather than a root CA, before clients will trust the local certificate, you must demonstrate a link with trusted root CAs, thereby proving that the local certificate is genuine. You can demonstrate this chain of trust either by:

- installing each intermediate CA's certificate in the client's list of trusted CAs
- including a signing chain in the local certificate

To include a signing chain, before importing the local certificate to the FortiWeb unit, first open the local certificate file in a plain text editor, append the certificate of each intermediate CA in order from the intermediate CA who signed the local certificate to the intermediate CA whose certificate was signed directly by a trusted root CA, then save the certificate. For example, a local certificate which includes a signing chain might use the following structure:

```
-----BEGIN CERTIFICATE-----
<FortiWeb unit's local server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<certificate of intermediate CA 1, who signed the FortiWeb
   certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<certificate of intermediate CA 2, who signed the certificate of
   intermediate CA 1 and whose certificate was signed by a
   trusted root CA>
-----END CERTIFICATE-----
```

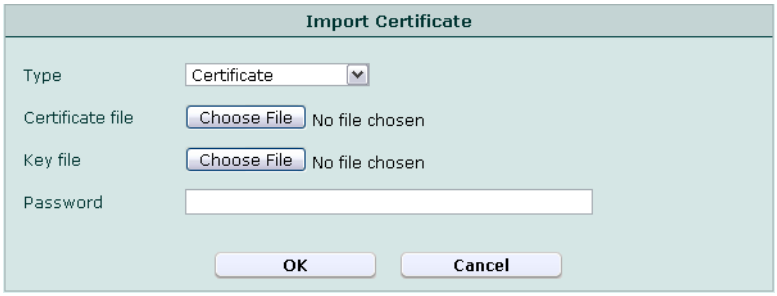
**Note:** The total file size of all certificates, Schema, keys, WSDL, and any other uploaded files may not exceed 12 MB.

### To upload a certificate

1 Go to *System* > *Certificates* > *Local*.

2 Click *Load New*.

3 Configure the following:




| *Name of the GUI item* | *Description* |
|---|---|
| **Name** | Enter the name of the certificate. |
| **Type** | Select which type of certificate file you will upload, either *Certificate* (an unencrypted X.509 certificate) or *PKCS12 Certificate* (a PKCS #12 encrypted certificate with key). |
| **Certificate file** | Click *Choose File* to locate the X.509 certificate file that you want to upload.<br>This option is available only if *Type* is *Certificate*. |
| **Key file** | Click *Choose File* to locate the key file that you want to upload with the certificate.<br>This option is available only if *Type* is *Certificate*. |
| **Certificate With Key File** | Click *Choose File* to locate the PKCS #12 certificate-with-key file that you want to upload.<br>This option is available only if *Type* is *PKCS12 Certificate*. |

| | |
|---|---|
| **Password** | Enter the password that was used to encrypt the file, enabling the FortiWeb unit to decrypt and install the certificate. |
| **Comments** | Enter a description for the certificate. |

4 Click *OK*.

To use a certificate, you must select it in a policy or server farm. For details, see "Configuring policies" on page 91 or "Grouping physical servers into server farms" on page 106.

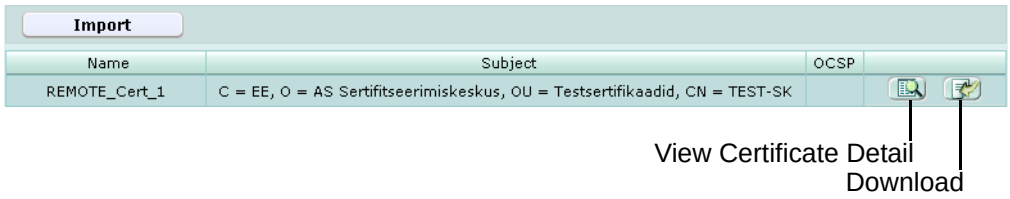
## Managing OCSP server certificates

*System* > *Certificates* > *Remote* displays and imports the certificates of the online certificate status protocol (OCSP) or HTTP CRL servers of your certificate authority (CA).

OCSP enables you to revoke or validate certificates by query, rather than by importing certificate revocation lists (CRL). For information about importing CRLs, see "Managing the certificate revocation list" on page 72.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have *Read* and *Write* permission to items in the *System Configuration* category. For details, see "About permissions" on page 58.

**Table 22:** *Remote* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Import** | Click to import an OCSP server certificate. |
| **Name** | The name of the OCSP server certificate. |
| **Subject** | The distinguished name (DN) located in the `Subject` field of the certificate. |
| **OCSP** | The URL of the OCSP server. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a certificate verification configuration.<br>Click *View Certificate Detail* to view the certificate's subject, range of dates within which the certificate is valid, version number, serial number, and extensions.<br>Click *Download* to download the entry in certificate (.cer) file format. |

## Managing CA certificates

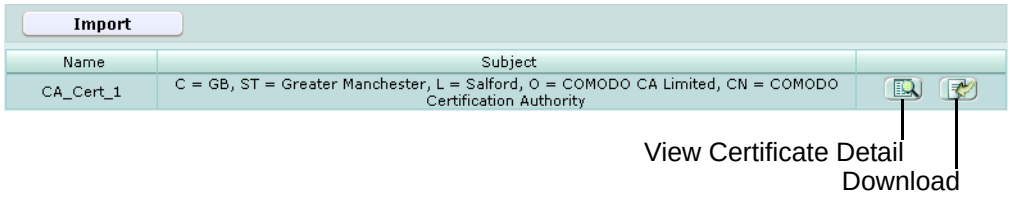
*System* > *Certificates* > *CA* displays and enables you to import certificates for certificate authorities (CA).

Certificate authorities validate and sign other certificates in order to indicate to third parties that those other certificates may be trusted to be authentic.

CA certificates are required by connections that use SSL or transport layer security (TLS).CA certificates are not used directly, but instead must first be grouped in order to be selected in a certificate verification rule. For details, see "Grouping CA certificates" on page 69.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have *Read* and *Write* permission to items in the *System Configuration* category. For details, see "About permissions" on page 58.

**Table 23:** *CA* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Import** | Click to import a CA certificate, then select whether you want to upload it (*Local PC*), or provide the URL of a certificate on a simple certificate enrollment protocol server (*SCEP*). |
| **Name** | The name of the CA certificate. |
| **Subject** | The distinguished name (DN) located in the `Subject` field of the certificate. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a certificate verification configuration.<br>Click *View Certificate Detail* to view the certificate's subject, range of dates within which the certificate is valid, version number, serial number, and extensions.<br>Click *Download* to download the entry in certificate (.cer) file format. |

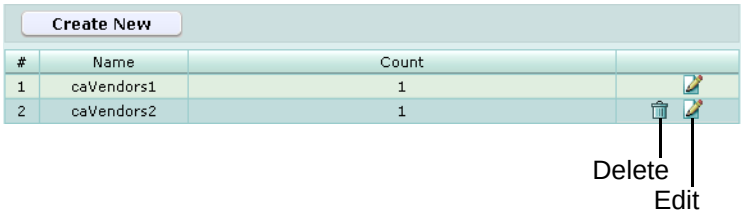
## Grouping CA certificates

*System* > *Certificates* > *CA Group* enables you to group certificate authorities (CA).

CAs must belong to a group in order to be selected in a certificate verification rule. For details, see "Configuring certificate verification rules" on page 73.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have *Read* and *Write* permission to items in the *System Configuration* category. For details, see "About permissions" on page 58.

**Table 24:** *CA Group* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| # | The index number of the entry in the list. |
| **Name** | The name of the certificate authority (CA) group. |

| | |
|---|---|
| **Count** | The number of certificate authorities in the group. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a certificate verification configuration.<br>Click *Edit* to modify the entry. |

**To add a CA group**

Before you can create a CA group, you must upload at least one of the certificate authority (CA) certificates that you want to add to the group. For details, see "Managing CA certificates" on page 68.

1. Go to *System* > *Certificates* > *CA Group*.
2. In *Name*, type a name for the certificate authority group.
3. Click *OK*.
4. Click *Create New*.
5. In *ID*, enter the index number of the host entry within the group, or keep the field's default value of `auto` to let the FortiWeb unit automatically assign the next available index number.
6. In *CA*, select the name of a certificate authority's certificate that you have previously uploaded and want to add to the group.
7. Click *OK*.
8. Repeat the previous 3 steps for each CA that you want to add to the group.

To apply a CA group, select it in a certificate verification rule. For details, see "Configuring certificate verification rules" on page 73.

## Managing certificates for intermediate CAs

*System* > *Certificates* > *Intermediate CA* enables you to upload certificates belonging to intermediate (non-root) certificate authorities (CA).

If a server certificate is signed by an intermediate certificate authority (CA) rather than a root CA, before the client will trust the server's certificate, you must demonstrate a link with trusted root CAs, thereby proving that the server's certificate is genuine. Otherwise, the server certificate may cause the client or browser to display certificate warnings.

You can demonstrate this chain of trust either by:

- installing each intermediate CA's certificate in the client's list of trusted CAs
- including a signing chain in the server's certificate
- configuring the FortiWeb unit to also provide the certificates of intermediate CAs when it presents the server certificate

To include a signing chain, first open the server's certificate file in a plain text editor, append the certificate of each intermediate CA in order from the intermediate CA who signed the server's certificate to the intermediate CA whose certificate was signed directly by a trusted root CA, then save the certificate. For example, a server's certificate which includes a signing chain might use the following structure:

```
-----BEGIN CERTIFICATE-----
<server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<certificate of intermediate CA 1, who signed the server
   certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
```

```
<certificate of intermediate CA 2, who signed the certificate of
   intermediate CA 1 and whose certificate was signed by a
   trusted root CA>
-----END CERTIFICATE-----
```

**Note:** The total file size of all certificates, Schema, keys, WSDL, and any other uploaded files may not exceed 12 MB.

To configure the FortiWeb unit to provide the certificates of intermediate CAs when it presents the server certificate

1 Install the certificates of the intermediate CAs on the FortiWeb unit.

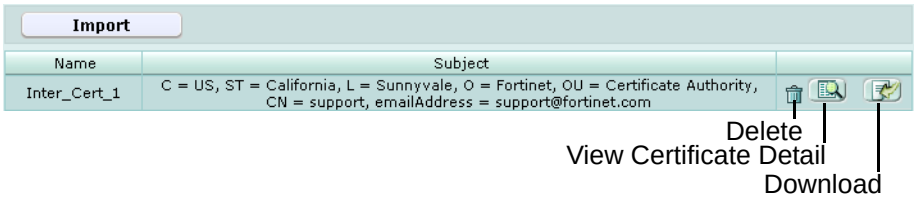
2 Group them to match the signing chain (see "Grouping certificates for intermediate CAs" on page 71).

3 Select that group along with the server certificate in the policy ("Configuring policies" on page 91).

The FortiWeb unit will present both the server's certificate and those of the intermediate CAs when establishing a secure connection with the client.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have *Read* and *Write* permission to items in the *System Configuration* category. For details, see "About permissions" on page 58.

**Table 25:** *Intermediate CA* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Import** | Click to import an intermediate CA certificate, then select whether you want to upload it (*Local PC*), or provide the URL of a certificate on a simple certificate enrollment protocol server (*SCEP*). |
| **Name** | The name of the CA certificate. |
| **Subject** | The distinguished name (DN) located in the `Subject` field of the certificate. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in an intermediate CA certificate group.<br>Click *View Certificate Detail* to view the certificate's subject, range of dates within which the certificate is valid, version number, serial number, and extensions.<br>Click *Download* to download the entry in certificate (.cer) file format. |

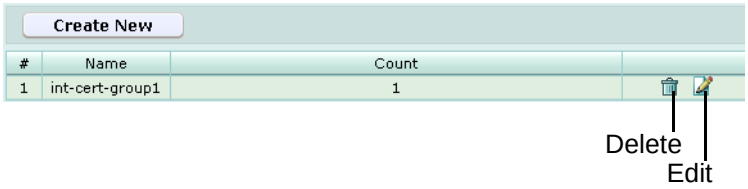
## Grouping certificates for intermediate CAs

*System* > *Certificates* > *Intermediate CA Group* enables you to group certificates of intermediate (non-root) certificate authorities (CA).

Intermediate CA certificates must belong to a group in order to be selected in a policy. For details, see "Managing certificates for intermediate CAs" on page 70.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have *Read* and *Write* permission to items in the *System Configuration* category. For details, see "About permissions" on page 58.

**Table 26:** *Intermediate CA Group* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| # | The index number of the entry in the list. |
| **Name** | The name of the intermediate certificate authority (CA) certificate group. |
| **Count** | The number of intermediate CA certificates in the group. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a policy.<br>Click *Edit* to modify the entry. |

**To add an intermediate CA group**

Before you can create an intermediate CA certificate group, you must upload at least one of the intermediate certificate authority (CA) certificates that you want to add to the group. For details, see "Managing certificates for intermediate CAs" on page 70.

1. Go to *System* > *Certificates* > *Intermediate CA Group*.
2. In *Name*, type a name for the intermediate CA certificate group.
3. Click *OK*.
4. Click *Create New*.
5. In *ID*, enter the index number of the host entry within the group, or keep the field's default value of `auto` to let the FortiWeb unit automatically assign the next available index number.
6. In *CA*, select the name of an intermediate CA's certificate that you have previously uploaded and want to add to the group.
7. Click *OK*.
8. Repeat the previous 3 steps for each intermediate CA certificate that you want to add to the group.

   To apply an intermediate CA certificate group, select it in a policy with a server certificate. For details, see "Configuring policies" on page 91.

## Managing the certificate revocation list

*System* > *Certificates* > *CRL* displays and enables you to import certificate revocation lists.

To ensure that your FortiWeb unit validates only certificates that have not been revoked, you should periodically upload a current certificate revocation list, which may be provided by certificate authorities (CA). Alternatively, you can use HTTP or online certificate status protocol (OCSP) to query for certificate statuses. For more information, see "Managing OCSP server certificates" on page 68.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have *Read* and *Write* permission to items in the *System Configuration* category. For details, see "About permissions" on page 58.

**Table 27:** *CRL* **tab**

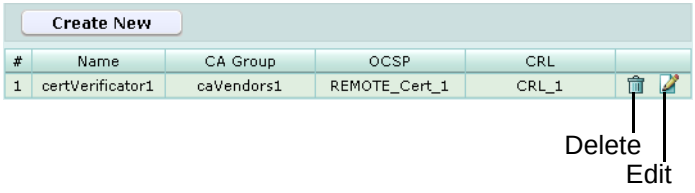

| *Name of the GUI item* | *Description* |
|---|---|
| **Import** | Click to import a certificate revocation list. |
| **Name** | The name of the certificate revocation list. |
| **Subject** | The distinguished name (DN) located in the `Subject` field of the certificate revocation list. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a certificate verification configuration.<br>Click *Edit* to update the CRL by connecting to the URL of new CRL on either a simple certificate enrollment protocol (SCEP) or plain HTTP server.<br>Click *View Certificate Detail* to view the certificate's subject, range of dates within which the certificate is valid, version number, serial number, and extensions.<br>Click *Download* to download the entry in certificate revocation list (.crl) file format. |

## Configuring certificate verification rules

*System* > *Certificates* > *Certificate Verify* enables you to configure how the FortiWeb unit will verify certificates presented by HTTP clients.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have *Read* and *Write* permission to items in the *System Configuration* category. For details, see "About permissions" on page 58.

**Table 28:** *Certificate Verify* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **#** | The index number of the entry in the list. |
| **Name** | The name of the certificate revocation list. |
| **CA Group** | The name of the certificate authority (CA) group selected in the entry. |
| **OCSP** | The name of the remote certificate selected to use with online certificate status protocol (OCSP) by this entry. |

| | |
|---|---|
| **CRL** | The name of the certificate revocation list selected in the entry. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a policy.<br>Click *Edit* to modify the entry. |

### To add a certificate verification rule

1 Go to *System* > *Certificates* > *Certificate Verify*.

2 Click *Create New*.

3 In *Name*, type a name for the certificate verification rule.

4 From *CA Group*, select the name of a CA group, if any, that you want to use to authenticate client certificates.

5 From *OCSP*, select the name of an OCSP or HTTP (remote) server certificate, if any, that you want to use to verify the revocation status of client certificates.

6 From *CRL*, select the name of a certificate revocation list, if any, to use to verify the revocation status of client certificates.

7 Click *OK*.

To apply a certificate verification rule, select it in a policy. For details, see "Configuring policies" on page 91.

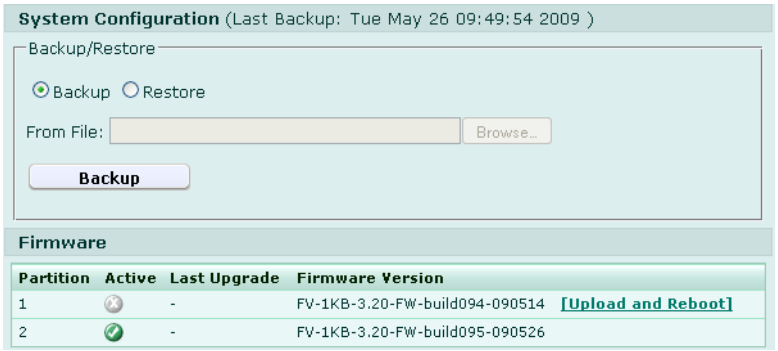
# Backing up the configuration & installing firmware

*System* > *Maintenance* > *Backup & Restore* enables you to download a backup copy of the configuration, or to upload and apply a configuration file. It also enables you to install FortiWeb firmware.

**Note:** Firmware can be installed in multiple ways, and can be tested before installing it. For additional information, see "Installing firmware" on page 279.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Maintenance* category. For details, see "About permissions" on page 58.

**Table 29:** *Backup & Restore* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **System Configuration** | |

| | |
|---|---|
| **Last Backup** | The date and time of the last backup.<br>If the configuration has not yet been backed up, or you have restored the firmware and therefore the time of any preceding backup is not known, this field contains a hyphen ( - ). |
| **Backup**<br>or<br>**Restore**<br>(radio button) | Select whether to back up or restore a configuration. |
| **From File** | Click the *Browse* button to locate the configuration file that you want to restore.<br>This field is available only if you have selected the *Restore* radio button above this field. |
| **Backup**<br>or<br>**Restore**<br>(button) | Click to back up the configuration to a file, or restore the configuration from a file.<br>If you are restoring a configuration file, your web browser uploads the file and the FortiWeb unit restarts with the new configuration. Time required varies by the size of the file and the speed of your network connection. After the FortiWeb unit has restarted, to continue using the web-based manager, you must log in again.<br>The name of this button varies by whether you selected the *Backup* or *Restore* radio button. |
| **Firmware** | |
| **Partition** | The index number of the partition. A partition can contain one version of the firmware and the system configuration. One partition is active and the others are backups. |
| **Active** | Indicates which partition the FortiWeb unit is currently configured to use.<br>• **Green check mark:** The partition contains the configuration and firmware that the FortiWeb unit will use when starting or rebooting.<br>• **Grey X mark:** The partition contains a backup configuration and firmware, which is not currently being used. |
| **Last Upgrade** | The date and time of the last update to this partition. |
| **Firmware Version** | The version and build number of the FortiWeb firmware. On backup partitions, you can click *Upload and Reboot* to replace the firmware on a partition and make the partition active. For more information on changing firmware, see "Installing firmware" on page 279.<br>**Caution:** Back up the FortiWeb configuration before changing firmware. Policies inapplicable to the current operation mode will be deleted when upgrading to FortiWeb v3.3.0 or greater firmware. Failure to make backups can result in loss of configuration for features that change between firmware versions. |

# Configuring the time & date

*System* > *Maintenance* > *System Time* enables you to configure the FortiWeb unit's system time.

You can either manually set the FortiWeb system time or configure the FortiWeb unit to automatically keep its system time correct by synchronizing with a Network Time Protocol (NTP) server.

**Note:** For many features to work, including scheduling, logging, and SSL-dependent features, the FortiWeb system time must be accurate.

**Note:** FortiWeb units support daylight savings time (DST), including recent changes in the USA, Canada and Western Australia.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *System Configuration* category. For details, see "About permissions" on page 58.

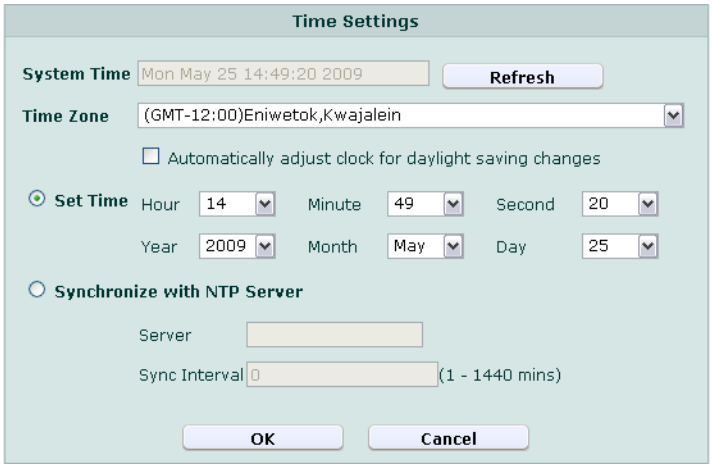
### To configure the date and time

1 Go to *System* > *Maintenance* > *System Time*.

Alternatively, go to *System* > *Status* > *Status*. In the *System Information* widget, in the *System Time* row, click *Change*.

2 From *Time Zone*, select the time zone in which the FortiWeb unit is located.

3 Configure the following to either manually configure the system time, or automatically synchronize the FortiWeb unit's clock with an NTP server:




| *Name of the GUI item* | *Description* |
|---|---|
| **System Time** | The date and time according to the FortiWeb unit's clock at the time that this tab was loaded, or when you last clicked the *Refresh* button. |
| **Refresh** | Click to update the *System Time* field with the current time according to the FortiWeb unit's clock. |
| **Time Zone** | Select the time zone in which the FortiWeb unit is located. |
| **Automatically adjust clock for daylight saving changes** | Enable to automatically adjust the clock of the FortiWeb unit when its time zone changes between daylight savings time (DST) and standard time. |
| **Set Time** | Select this option to manually set the date and time of the FortiWeb unit's clock, then select the *Hour*, *Minute*, *Second*, *Year*, *Month* and *Day* fields before you click *OK*. |
| **Synchronize with NTP Server** | Select this option to automatically synchronize the date and time of the FortiWeb unit's clock with an NTP server, then configure the *Server* and *Sync Interval* fields before you click *OK*. |

| | |
|---|---|
| **Server** | Enter the IP address or domain name of an NTP server. To find an NTP server that you can use, go to http://www.ntp.org. |
| **Sync Interval** | Enter how often in minutes the FortiWeb unit should synchronize its time with the NTP server. For example, entering 1440 causes the FortiWeb unit to synchronize its time once a day. |

**4** Click *OK*.

# Uploading signature updates

*System* > *Maintenance* > *Update Signature* enables you to update the predefined robots, data types, suspicious URLS, and attack signatures that your FortiWeb unit uses to detect attacks such as:

- cross-site scripting (XSS)
- SQL injection
- common exploits

Updating signatures ensures that your FortiWeb unit can detect recently discovered variations of these attacks.

After restoring the firmware of the FortiWeb unit, you should upload the most currently available attack signatures. Restoring firmware installs the attack signatures that were current at the time that the firmware image file was made, which may no longer be up-to-date.

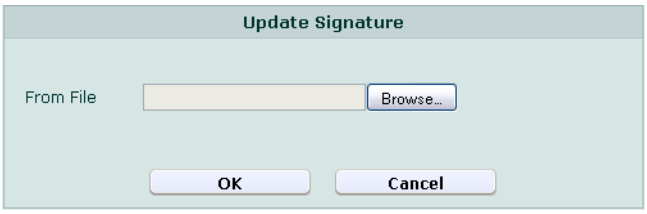
**Tip:** Alternatively, you can schedule automatic updates. For details, see "Scheduling signature updates" on page 78.

Before you can download signature update files to your management computer, you must first register your FortiWeb unit with the Fortinet Technical Support web site, https://support.fortinet.com/, and obtain a valid support contract. Signature update files will then be available for download when you log in to the Fortinet Technical Support web site.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Maintenance* category. For details, see "About permissions" on page 58.

**Note:** After updating its attack signatures from a signature update file, the FortiWeb unit will restart itself. When the restart is complete, to continue using the web-based manager, log in again.

**Figure 10:** *Update Signature* **tab**



# Scheduling signature updates

**Note:** This feature is for future use, pending support by the FortiGuard Distribution Network (FDN). It is not currently supported at the time of this release.

*System* > *Maintenance* > *Auto Update* enables you to configure how the FortiWeb unit will retrieve predefined robots, data types, suspicious URLS, and attack signature updates that your FortiWeb unit uses to detect attacks such as:

- cross-site scripting (XSS)
- SQL injection
- common exploits

**Tip:** Alternatively, you can manually upload update packages. For details, see "Uploading signature updates" on page 77.

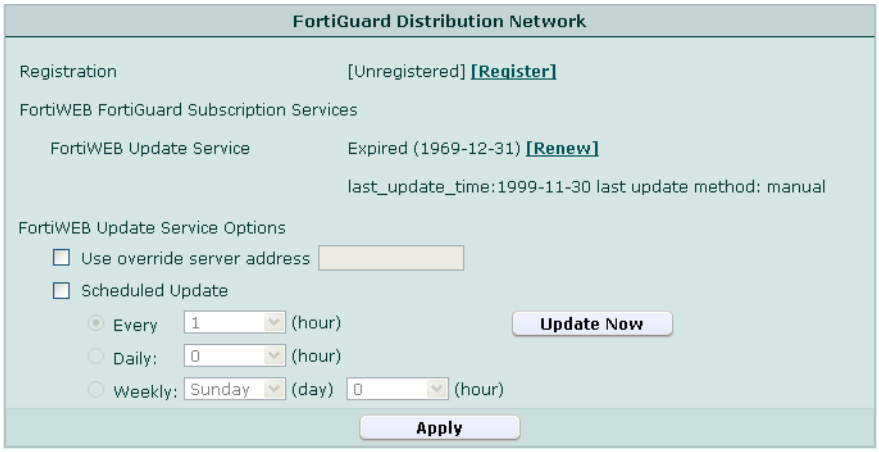
FortiWeb units receive updates from the FortiGuard Distribution Network (FDN). The FDN is a world-wide network of FortiGuard Distribution Servers (FDS). Unless you override the setting with a specific FDS address, FortiWeb units connect to the FDN by connecting to the FDS nearest to the FortiWeb unit by its configured time zone.

**Note:** If required, the FortiWeb unit can be configured to connect through a web proxy. For details, see the *FortiWeb CLI Reference*.

In addition to manual update requests, FortiWeb units support an automatic update mechanism: scheduled updates, by which the FortiWeb unit periodically polls the FDN to determine if there are any available updates.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Maintenance* category. For details, see "About permissions" on page 58.

**Table 30:** *Auto Update* **tab**



| | |
|---|---|
| **Registration** | The registration status of the FortiWeb unit with the FortiGuard Distribution Network (FDN). If it is unregistered, you must click *Register* and complete the form on the Fortinet Technical Support web site in order for the FortiWeb unit to be able to retrieve updates. |
| **FortiWEB Update Service** | The current update license status, as well as the date, time, and method of the previous update attempt. |
| **Renew** | If the FortiWeb unit's attack signature update license has expired, click *Renew* to purchase a new license. |
| **Use override server address** | Enable to override the default FortiGuard Distribution Server (FDS) to which the FortiWeb unit connects for updates, then enter the IP address of the override public or private FDS. |
| **Scheduled Update** | Enable to perform updates according to a schedule, then select one of the following as the frequency of update requests.<br>• **Every**: Select to request to update once every 1 to 23 hours, then select the number of hours between each update request.<br>• **Daily**: Select to request to update once a day, then select the hour of the day to check for updates.<br>• **Weekly**: Select to request to update once a week, then select the day of the week, the hour, and the minute of the day to check for updates.<br>If you select *00* minutes, the update request occurs at a randomly determined time within the selected hour.<br>When the FortiWeb unit requests an update at the scheduled time, results appear in *FortiWEB Update Service*. If event logging is enabled, and the FortiWeb unit cannot successfully connect, it will record a log with the message `update failed, failed to connect any fds servers!` |
| **Apply** | Click to save configuration changes on this tab. |
| **Update Now** | Click to manually initiate an update request.<br>Results will appear in *FortiWEB Update Service*. Time required varies by the availability of updates, size of the updates, and speed of the FortiWeb unit's network connection. If event logging is enabled, and the FortiWeb unit cannot successfully connect, it will record a log with the message `update failed, failed to connect any fds servers!` |

# Router

This section describes the *Router* menu.

Static routes direct traffic exiting the FortiWeb unit — you can specify through which network interface a packet will leave, and the IP address of a next-hop router that is reachable from that network interface. The router is aware of which IP addresses are reachable through various network pathways, and can forward those packets along pathways capable of reaching the packets' ultimate destinations.

A default route is a special type of static route. A default route matches all packets, and defines a gateway router that can receive and route packets if no other, more specific static route is defined for the packet's destination IP address.

This section includes the following topic:



## Configuring static routes

*Router* > *Static* > *Static Route* displays the list of static routes, including the default route.

You should configure at least one static route, a default route, that points to your gateway. However, you may configure multiple static routes if you have multiple gateway routers, each of which should receive packets destined for a different subset of IP addresses.

For example, if a web server is directly attached to one of the network interfaces, but all other destinations, such as connecting clients, are located on distant networks such as the Internet, you might need to add only one route: a default route for the gateway router through which the FortiWeb unit connects to the Internet.

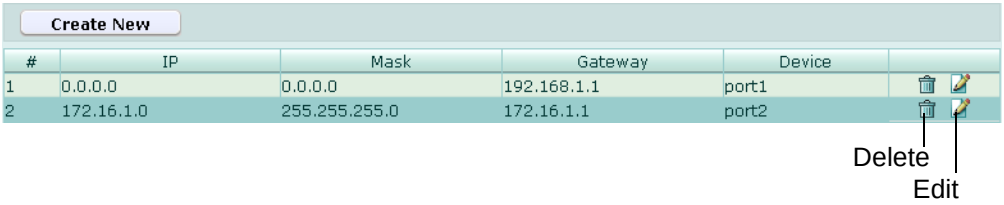
To determine which route a packet will be subject to, the FortiWeb unit examines the packet's destination IP address and compares it to those of the static routes. If more than one route matches the packet, the FortiWeb unit will apply the route with the smallest index number. For this reason, you should give more specific routes a smaller index number than the default route.

When you add a static route through the web-based manager, the FortiWeb unit evaluates the route to determine if it represents a different route compared to any other route already present in the list of static routes. If no route having the same destination exists in the list of static routes, the FortiWeb unit adds the static route, using the next unassigned route index number.

**Note:** By default, the FortiWeb unit will forward only HTTP/HTTPS traffic to your protected physical servers. (That is, IP-based forwarding is disabled.) For information on enabling forwarding of other protocols such as FTP, see the `config router setting` command in the *FortiWeb CLI Reference*.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Router Configuration* category. For details, see "About permissions" on page 58.

**Table 31:** *Static Route* **tab**



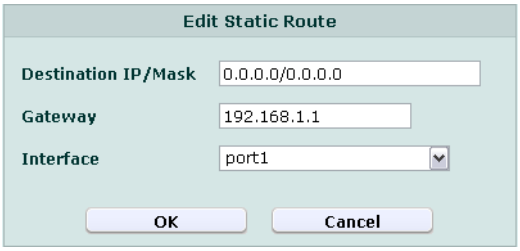

| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a static route. |
| **#** | The index number of the entry in the list. |
| **IP** | The destination IP addresses of packets subject to the static route.<br>`0.0.0.0` indicates that the route matches all destination IP addresses. |
| **Mask** | The network mask associated with the IP address.<br>`0.0.0.0` indicates that the route matches all subnet masks. |
| **Gateway** | The IP address of the next-hop router to which packets subject to the static route will be forwarded. |
| **Device** | The name of the network interface through which packets subject to the static route will egress. |
| (No column heading.) | Click *Delete* to remove an entry.<br>Click *Edit* to modify an entry. |

### To configure a static route

1 Go to *Router* > *Static* > *Static Route*.

2 Click *Create New*.

3 Configure the following, then click *OK*:




| *Name of the GUI item* | *Description* |
|---|---|
| **Destination IP/Mask** | Type the destination IP address and network mask of packets that will be subject to this static route, separated by a slash ( / ).<br>The value `0.0.0.0/0.0.0.0` is reserved for the default route, which matches all packets. |
| **Gateway** | Type the IP address of the next-hop router to which the FortiWeb unit will forward packets subject to this static route. This router must know how to route packets to the destination IP addresses that you have specified in *Destination IP/Mask*. For an Internet connection, the next hop routing gateway routes traffic to the Internet. |
| **Interface** | Select the name of the network interface through which the packets subject to the static route will egress towards the next-hop router. |

# User

This section describes the *User* menu.

The FortiWeb unit authenticates HTTP requests, using local users, LDAP queries, and NTLM queries. You can also create user groups for each user type or even a combination of the three user types for easy management of user authentication.

This section includes the following topic:

- Configuring local users
- Configuring LDAP user queries
- Configuring NTLM user queries
- Grouping users

## Configuring local users

*User* > *Local User* > *Local User* displays the list of locally defined user accounts.

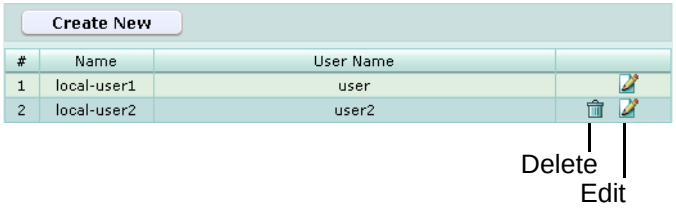
Local user accounts are used by the HTTP authentication feature to authorize HTTP requests. For details, see "Configuring HTTP authentication" on page 207.

Local user accounts are activated indirectly, by selecting them in a user group that is selected within an authentication rule, which is in turn selected within an authentication policy, which is ultimately selected within an inline protection profile. For details, see "Grouping users" on page 88.

**Note:** User passwords are not encrypted when downloading a FortiWeb configuration backup file. If you configure local user accounts, be sure to store configuration backup files in a safe location.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Auth Users* category. For details, see "About permissions" on page 58.

**Table 32:** *Local User* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a user. |
| # | The index number of the entry in the list. |
| **Name** | The name of the entry. |

| | |
|---|---|
| **User Name** | The user name that the client must provide when authenticating. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a user group.<br>Click *Edit* to modify the entry. |

### To configure a local user

1 Go to *User* > *Local User* > *Local User*.

2 Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.

3 In *Name*, type the name of the local user entry.

This field cannot be modified if you are editing an existing entry. To modify the name, delete the entry, then recreate it using the new name.

4 Configure the following:


| *Name of the GUI item* | *Description* |
|---|---|
| **User Name** | Type the user name that the client must provide when authenticating. |
| **Password** | Type the password for the local user account. The maximum length is 63 characters. |

5 Click *OK*.

To apply the local user account, select it in a user group. For details, see “Grouping users” on page 88.

# Configuring LDAP user queries

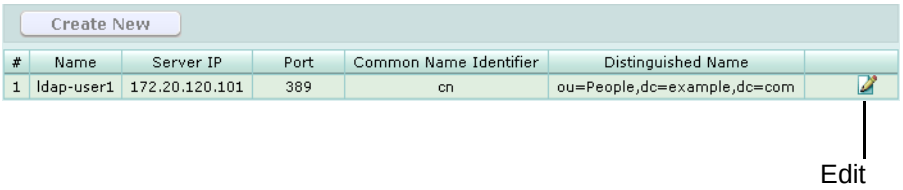
*User* > *LDAP User* > *LDAP User* displays the list of LDAP queries that can be used to authenticate users.

LDAP user queries are used by the HTTP authentication feature to authorize HTTP requests. For details, see “Configuring HTTP authentication” on page 207.

LDAP user accounts are activated indirectly, by selecting them in a user group that is selected within an authentication rule, which is in turn selected within an authentication policy, which is ultimately selected within an inline protection profile. For details, see “Grouping users” on page 88.

To be able to access this part of the web-based manager, in your administrator account’s access profile, you must have both *Read* and *Write* permission to items in the *Auth Users* category. For details, see “About permissions” on page 58.

**Table 33:** *LDAP User* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add an LDAP user account query.<br>Only one LDAP user query can exist at any given time. If a query is already configured, this button is greyed out. |
| # | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Server IP** | The IP address of the LDAP server that will be queried to authenticate users. |
| **Port** | The TCP port number on which the LDAP server listens for queries. |
| **Common Name Identifier** | The common name (CN) attribute, often `cn`, whose value is the user name. |
| **Distinguished Name** | The distinguished name (DN) that, when prefixed with the common name, forms the full path in the directory to user account object. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a user group.<br>Click *Edit* to modify the entry. |

### To configure the LDAP user query

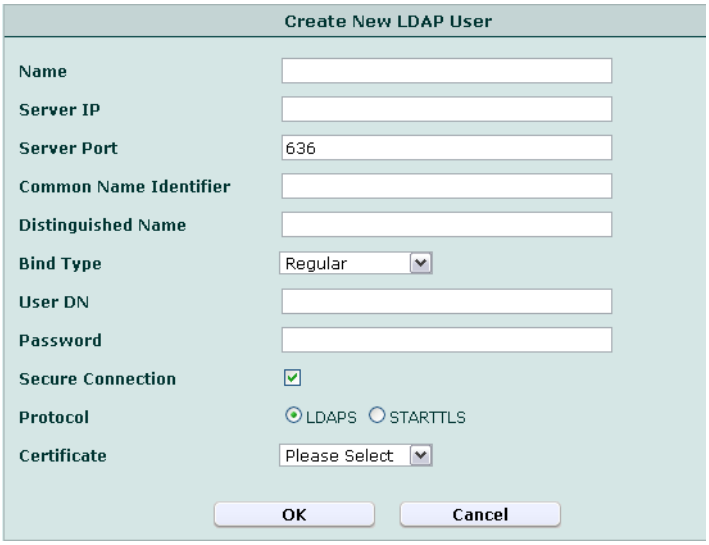
Before configuring the query, if you will configure a secure connection, you must upload the certificate of the CA that signed the LDAP server's certificate. For details, see "Managing CA certificates" on page 68.

1. Go to *User* > *LDAP User* > *LDAP User*.
2. Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.

   Only one LDAP user query can exist at any given time. If a query is already configured, the *Create New* button is greyed out.
3. In *Name*, type the name of the LDAP user query entry.

   This field cannot be modified if you are editing an existing entry. To modify the name, delete the entry, then recreate it using the new name.

**4** Configure the following:




| *Name of the GUI item* | *Description* |
|---|---|
| **Server IP** | Type the IP address of the LDAP server. |
| **Server Port** | Type the port number where the LDAP server listens.<br>The default port number varies by your selection in *Secure Connection*: port 389 is typically used for non-secure connections or for STARTTLS-secured connections, and port 636 is typically used for SSL-secured (LDAPS) connections. |
| **Common Name Identifier** | Type the identifier, often `cn`, for the common name (CN) attribute whose value is the user name.<br>Identifiers may vary by your LDAP directory's schema. |
| **Distinguished Name** | Type the distinguished name (DN) that, when prefixed with the common name, forms the full path in the directory to user account objects. |
| **Bind Type** | Select one of the following LDAP query binding styles:<br>• **Simple**: Bind using the client-supplied password and a bind DN assembled from the *Common Name Identifier*, *Distinguished Name*, and the client-supplied user name.<br>• **Regular**: Bind using a bind DN and password that you configure in *User DN* and *Password*.<br>• **Anonymous**: Do not provide a bind DN or password. Instead, perform the query without authenticating. Select this option only if the LDAP directory supports anonymous queries. |
| **User DN** | Type the bind DN, such as `cn=FortiWebA,dc=example,dc=com`, of an LDAP user account with permissions to query the *Distinguished Name*.<br>This field may be optional if your LDAP server does not require the FortiWeb unit to authenticate when performing queries, and does not appear if *Bind Type* is *Anonymous* or *Simple*. |
| **Password** | Type the password of the *User DN*.<br>This field may be optional if your LDAP server does not require the FortiWeb unit to authenticate when performing queries, and does not appear if *Bind Type* is *Anonymous* or *Simple*. |
| **Secure Connection** | Enable to connect to the LDAP server(s) using an encrypted connection, then select the style of the encryption in *Protocol*. |

| | |
|---|---|
| **Protocol** | Select whether the LDAP query will be secured using LDAPS or STARTTLS. You may need to reconfigure *Server Port* to correspond to the change in protocol.<br>This option appears only if *Secure Connection* is enabled. |
| **Certificate** | Select which certificate authority (CA) certificate to use in order to validate the LDAP server's certificate. This must be the same one that signed the LDAP server's certificate.<br>This option appears only if *Secure Connection* is enabled. |

5 Click *OK*.

To apply the LDAP user query, select it in a user group. For details, see "Grouping users" on page 88.

# Configuring NTLM user queries

*User* > *NTLM User* > *NTLM User* displays the list of NT LAN Manager (NTLM) user account queries.

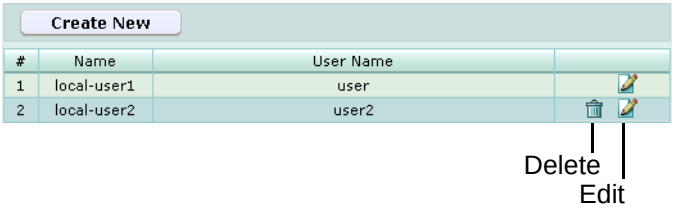
NTLM queries can be made to a Microsoft Windows or Active Directory server that has been configured for NTLM authentication. Both NTLM v1 and NTLM v2 versions of the protocol are supported.

NTLM user queries are used by the HTTP authentication feature to authorize HTTP requests. For more information, see "Configuring HTTP authentication" on page 207.

NTLM user account queries are used indirectly, by selecting them in a user group that is selected within an authentication rule, which is in turn selected within an authentication policy, which is ultimately selected within an inline protection profile. For details, see "Grouping users" on page 88.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Auth Users* category. For details, see "About permissions" on page 58.

**Table 34:** *NTLM User* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add an NTLM user account query. |
| **#** | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Server IP** | The IP address of the NTLM server that will be queried. |
| **Port** | The TCP port number on which the NTLM server listens for queries. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a user group.<br>Click *Edit* to modify the entry. |

**To configure an NTLM user query**

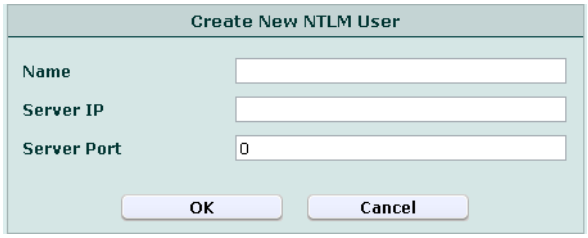
1 Go to *User* > *NTLM User* > *NTLM User*.

2 Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.

3 In *Name*, type the name of the NTLM user entry.

This field cannot be modified if you are editing an existing entry. To modify the name, delete the entry, then recreate it using the new name.

4 Configure the following:




| *Name of the GUI item* | *Description* |
|---|---|
| **Server IP** | Type the IP address of the NTLM server that will be queried. |
| **Port** | Type the TCP port number on which the NTLM server listens for queries. |

5 Click *OK*.

To apply the NTLM user account query, select it in a user group. For details, see “Grouping users” on page 88.

# Grouping users

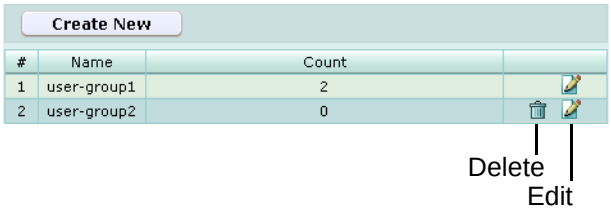
*User* > *User Group* > *User Group* displays the list of user groups.

User groups are used by the HTTP authentication feature to authorize HTTP requests, and can include a mixture of local user accounts, LDAP user queries, amd NTLM user queries.

User groups are used indirectly, by selecting them in within an authentication rule, which is in turn selected within an authentication policy, which is ultimately selected within an inline protection profile. For details, see “Configuring authentication rules” on page 208.

To be able to access this part of the web-based manager, in your administrator account’s access profile, you must have both *Read* and *Write* permission to items in the *Auth Users* category. For details, see “About permissions” on page 58.

**Table 35:** *User Group* **tab**



| Name of the GUI item | Description |
|---|---|
| **Create New** | Click to add an NTLM user account query. |
| # | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Count** | The number of individual user accounts and/or user queries contained in the entry. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in an authentication rule.<br>Click *Edit* to modify the entry. |

### To configure a user group

Before you can configure a user group, you must first configure any local user accounts or user queries that you want to include. For details, see "Configuring local users" on page 83, "Configuring LDAP user queries" on page 84, and "Configuring NTLM user queries" on page 87.

1 Go to *User* > *User Group* > *User Group*.

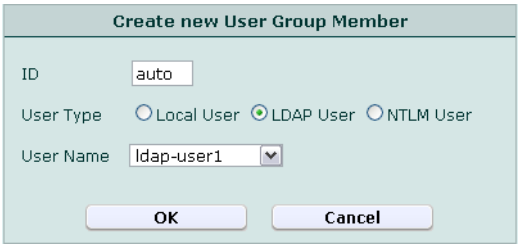
2 Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.

3 In *Name*, type the name of the user group.

This field cannot be modified if you are editing an existing entry. To modify the name, delete the entry, then recreate it using the new name.

4 Click *OK*.

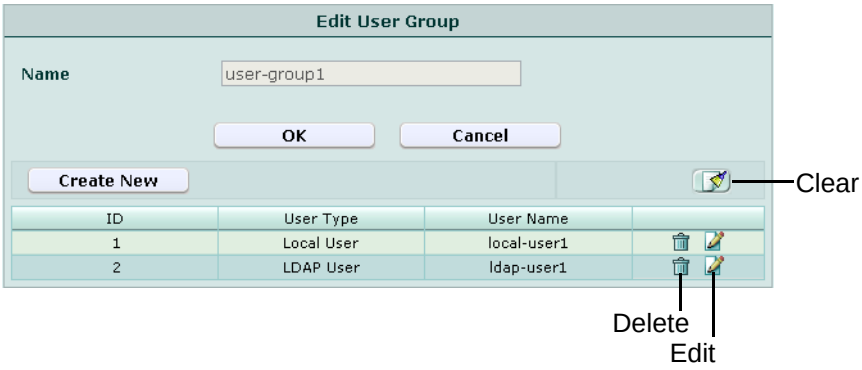
5 Click *Create New*, then configure the following:




| Name of the GUI item | Description |
|---|---|
| **ID** | Type the index number of the individual rule within the group of users, or keep the field's default value of `auto` to let the FortiWeb unit automatically assign the next available index number. |
| **User Type** | Select which type of user or user query that you want to add to the group, either *Local User*, *LDAP User*, or *NTLM User*.<br>**Note:** For best results, only select a user type that is supported by the *Auth Type* you plan to use in the authentication rule. You can mix all user types in the group. However, if the authentication rule's *Auth Type* does not support a given user type, all user accounts of that type will be ignored, effectively disabling them. |
| **User Name** | Select the name of a local user account, LDAP user query, or NTLM user query. Available options vary by your selection in *User Type*. |

6 Repeat the previous step for each individual rule that you want to add to the group of users.

7 If you need to modify an individual rule, click its *Edit* icon. To remove an individual user or user query from the group of users, click its *Delete* icon. To remove all individual users or user queries from the group of users, click the *Clear* icon.




8 Click *OK*.

To apply the user group, select it in an authentication rule. For details, see “Configuring authentication rules” on page 208.

# Server Policy

This section describes the *Server Policy* menu, which defines policies, HTTP servers and their port numbers, virtual or real web hosts on those servers, and certificates.

This section includes the following topics:



## Configuring policies

*Server Policy* > *Policy* > *Policy* displays the list of policies.

Policies:

- determine which connections will be allowed or blocked
- apply a profile that specifies how it will process the connections that it allows
- route traffic to specific destination physical servers (if supported in the operation mode)
- use an auto-learning profile to gather additional information about your HTTP traffic for use as guidance when modifying the policy or profiles

When determining which policy to apply to a connection, FortiWeb units will consider the operation mode:

- **Inline Protection:** Apply the policy whose virtual server and service match the connection.
- **Offline Protection:** Apply the policy whose network interface in the virtual server matches the connection. Do not consider the service, or the IP address of the virtual server.
- **Transparent:** Apply the policy whose bridge matches the connection. Do not considerthe IP address of the bridge.

The FortiWeb unit will apply only one policy to each connection. If an HTTP connection does not match any of the policies, the FortiWeb unit will block the connection.

Policies are not used while they are disabled, as indicated by “Status” on page 94.

Policy behavior varies by the operation mode.

**Table 36: Policy behavior by operation mode**

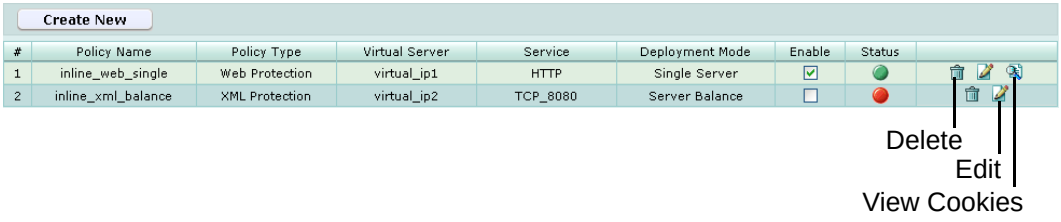
| | Inline Protection | Offline Protection | Transparent |
|---|---|---|---|
| **Matches by** | • Service<br>• Virtual server | • Virtual server's network interface, but ***not*** its IP address | • Service<br>• Bridge, but ***not*** its IP address |
| **Violations** | Blocked or modified, according to profile | Attempts to block by mimicking the client or server and requesting to reset the connection; does ***not*** modify otherwise | Blocked or modified, according to profile |
| **Profile support** | • Inline protection profiles<br>• Auto-learning profiles<br>• XML protection profiles | • Offline protection profiles<br>• Auto-learning profiles | • Inline protection profiles<br>• Auto-learning profiles |
| **SSL** | Certificate used to offload SSL from the servers to the FortiWeb; can optionally re-encrypt before forwarding to the destination server | Certificate used to decrypt and scan only; does ***not*** act as an SSL origin or terminator | Certificate to decrypt and scan only; does ***not*** act as an SSL origin or terminator |
| **Forwarding** | • Forwards to a single physical server or member of a server farm using the port number on which it listens; similar to a network address translation (NAT) policy on a general-purpose firewall<br>• Can load balance or route connections to a specific server based upon XML content | Lets the traffic pass through to a member of a server farm, but does ***not*** load balance | Forwards to a member of a server farm (but allowing to pass through, ***without*** actively redistributing connections) using the port number on which it listens |

**Note:** When you switch the operation mode, policies will be deleted from the configuration file if they are not applicable in the current operation mode.

Policies can be configured to detect URL-embedded attacks that are obfuscated using recursive URL encoding (that is, multiple levels' worth of URL encoding). For more information, see the *FortiWeb CLI Reference*.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have *Read* permission to items in the *Server Policy Configuration* category. For details, see "About permissions" on page 58.

**Table 37:** *Policy* **tab**



| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a policy. |
| # | The index number of the entry in the list.<br>On FortiWeb units, the index number of a policy indicates its alphabetical order only. It does not indicate order of evaluation for matches with connections. Instead, the FortiWeb unit will apply the one policy that matches the connection, if any exists. |
| **Policy Name** | The name of the entry. |
| **Policy Type** | Indicates whether the policy applies a web protection profile (either inline or offline protection profile) or an XML protection profile. |
| **Virtual Server**<br>or<br>**V-zone** | The virtual server or bridge for which the policy will either apply a protection profile and route traffic to one or more physical servers, or use an offline protection profile. |
| **Service** | The service that defines the TCP port number on which the virtual server receives traffic. |
| **Deployment Mode** | The method of distribution that the FortiWeb unit will use when forwarding connections accepted by this policy.<br>• **Single Server**: Forward connections to a single physical server.<br>• **Server Balance**: Use a load balancing algorithm when distributing connections amongst the physical servers in a server farm. If a physical server is unresponsive to the server health check, the FortiWeb unit forwards subsequent connections to another physical server in the server farm.<br>• **Content Routing**: Use content routing rules defined as XPath expressions in the server farm configuration when distributing connections amongst the physical servers in a server farm. If a physical server is unresponsive to the server health check, or if a request does not match the XPath expression, the FortiWeb unit forwards connections to the first physical server in the server farm.<br>• **WSDL Content Routing**: Use WSDL content routing rules defined in the server farm configuration when distributing connections amongst the physical servers in a server farm. If a physical server is unresponsive to the server health check, or if a request does not match the WSDL content routing rules, the FortiWeb unit forwards connections to the first physical server in the server farm.<br>• **Offline Protection**: Allow connections to pass through the FortiWeb unit, but instead of applying an inline protection profile, apply an offline protection profile.<br>• **Transparent Servers**: Allow connections to pass through the FortiWeb unit, and apply a protection profile.<br>You can use the *Service Status* widget to determine whether or not a physical server is currently responding to the server health check. For details, see “Service Status widget” on page 32. |
| **Enable** | Mark this check box to allow the policy to be used when evaluating traffic for a matching policy.<br>For details, see “Enabling or disabling a policy” on page 101.<br>**Note:** You can use SNMP traps to notify you of changes to the policy’s status. For details, see “Configuring an SNMP community” on page 48. |

| | |
|---|---|
| **Status** | Indicates whether or not a policy will be used when evaluating traffic for a matching policy.<br>• **Green icon**: The policy will be used when evaluating traffic for a matching policy.<br>• **Flashing yellow-to-red icon**: The policy will ***not*** be used when evaluating traffic for a matching policy.<br>To be used, a policy's *Enable* must be marked. |
| (No column heading.) | Click *View Cookies* to display cookies that have been observed in reply traffic from the server if handled by this policy.<br>This icon appears only after cookies have been observed in the `Set-Cookie:` HTTP header, and does ***not*** appear for cookies that may have been set using client-side JavaScript.<br>Based upon whether or not the contents of the cookies are sensitive, such as if they are used for state tracking or database input, you may want to enable *Cookie Poison* in the policy's inline protection profile. For details, see "Cookie Poison" on page 214.<br>Click *Edit* to modify the entry. For details, see "Configuring policies" on page 91.<br>Click *Delete* to remove the entry. Policies may be automatically deleted if you switch the *Operation Mode* and the policy's type is not supported by the new mode.<br>**Caution:** Deleting a policy also removes any auto-learning data it has gathered using an auto-learning profile. To retain this data, instead either deselect the auto-learning profile in the policy, or disable the policy. For details, see "Enabling or disabling a policy" on page 101. |

### To add a policy

Before you can configure a policy, you must first configure a virtual server, a physical server or server farm, and an inline or offline protection profile. To restrict traffic based upon which hosts you want to protect, you must also configure a group of protected host names. If you want the FortiWeb unit to gather auto-learning data, you must first generate or configure an auto-learning profile and its required components. If you want to use the FortiWeb unit to apply SSL to connections instead of using physical servers, or if it must decrypt SSL connections in order to log them in offline protection mode or transparent mode, you must also import a server certificate. Finally, if you want the FortiWeb unit to verify the certificate provided by an HTTP client to authenticate themselves, you must also define a certificate verification rule and possibly also an intermediate CA certificate group. For details, see:

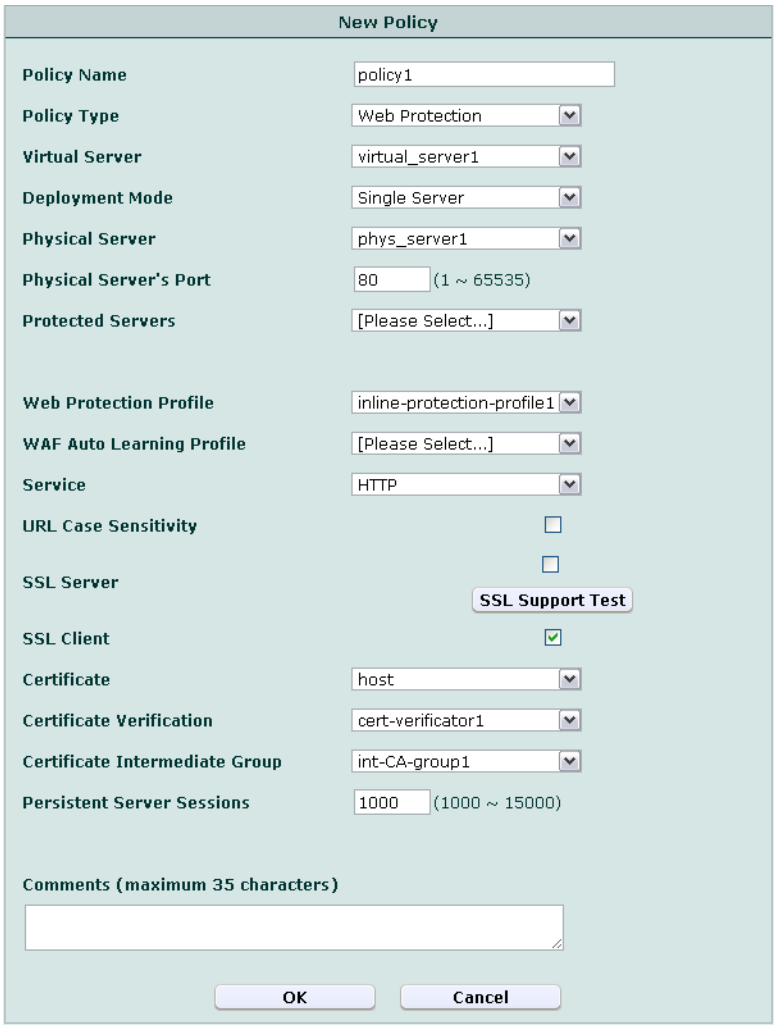
- "Configuring protected hosts" on page 113
- "Configuring virtual servers" on page 101
- "Configuring physical servers" on page 103
- "Grouping physical servers into server farms" on page 106
- "Configuring XML protection profiles" on page 144 (inline protection mode), "Configuring inline web protection profiles" on page 213 (inline protection mode or transparent mode), or "Configuring offline protection profiles" on page 219 (offline protection mode)
- "Configuring auto-learning profiles" on page 223 or "Generating an auto-learning profile and its components" on page 227
- "Uploading a certificate" on page 66
- "Configuring certificate verification rules" on page 73
- "Grouping certificates for intermediate CAs" on page 71

1 Go to *Server Policy* > *Policy* > *Policy*.

2 Click *Create New*.

**3** Configure the following, then click *OK*:

**Note:** Available options vary by the *Operation Mode* of the FortiWeb unit.




| *Name of the GUI item* | *Description* |
|---|---|
| **Policy Name** | Type a name for the policy. |
| **Policy Type** | Select whether you will apply an XML protection profile or a web protection profile, then select the name of the protection profile from *XML Protection Profile* or *Web Protection Profile*.<br>Depending on the types of profiles that the current operation mode supports, not all policy types may be available. For details, see Table 36 on page 92. |

| | |
|---|---|
| **Virtual Server**<br>or<br>**V-zone** | Select the name of a virtual server or bridge.<br>The name and use of this option varies by operating mode:<br>• **Inline Protection**: Indicate the IP address and network interface of incoming traffic that will be routed and to which the policy will apply a profile.<br>• **Offline Protection**: Indicate the network interface of incoming traffic that the policy to which it will attempt to apply a profile. The IP address of the virtual server will be ignored.<br>• **Transparent**: Indicate the bridge of incoming traffic to which the policy will apply a profile.<br>Alternatively, you can select *Create New* to add a virtual server in a pop-up window, without leaving the current page. For details, see "Configuring virtual servers" on page 101 or "Configuring bridges" on page 39. |
| **Deployment Mode** | Select the method of distribution that the FortiWeb unit will use when forwarding connections accepted by this policy.<br>• **Single Server**: Forward connections to a single physical server. Also configure *Physical Server*, and *Physical Server's Port*. This option is available only if the FortiWeb unit is operating in inline protection mode.<br>• **Server Balance**: Use a load balancing algorithm when distributing connections amongst the physical servers in a server farm. If a physical server is unresponsive to the server health check, the FortiWeb unit forwards subsequent connections to another physical server in the server farm. Also configure *Load Balancing Algorithm*, *Persistence Timeout*, *Server Health Check*, and *Server Farm*. This option is available only if the FortiWeb unit is operating in inline protection mode.<br>• **Content Routing**: Use content routing rules defined as XPath expressions in the server farm configuration when distributing connections amongst the physical servers in a server farm. If a physical server is unresponsive to the server health check, or if a request does not match the XPath expression, the FortiWeb unit forwards connections to the first physical server in the server farm. Also configure *Server Health Check* and *Server Farm*. This option is available only if the FortiWeb unit is operating in inline protection mode and *Policy Type* is *XML Protection*.<br>• **WSDL Content Routing**: Use WSDL content routing rules defined in the server farm configuration when distributing connections amongst the physical servers in a server farm. If a physical server is unresponsive to the server health check, or if a request does not match the WSDL content routing rules, the FortiWeb unit forwards connections to the first physical server in the server farm. Also configure *Server Health Check* and *Server Farm*. This option is available only if the FortiWeb unit is operating in inline protection mode and *Policy Type* is *XML Protection*.<br>• **Offline Protection**: Allow connections to pass through the FortiWeb unit, and apply an offline protection profile. Also configure *Server Health Check* and *Server Farm*. This option is available only if the FortiWeb unit is operating in offline protection mode.<br>• **Transparent Servers**: Allow connections to pass through the FortiWeb unit, and apply a protection profile. Also configure *Server Farm*. This option is available only if the FortiWeb unit is operating in transparent mode.<br>Depending on the types of topologies that the current operation mode supports, not all deployment modes may be available. For details, see Table 36 on page 92. |
| **Physical Server** | Select the physical server to which to forward connections, or select *Create New* to configure a new physical server in a pop-up window, without leaving the current page. For details, see "Configuring physical servers" on page 103.<br>This option appears only if *Deployment Mode* is *Single Server*. |
| **Physical Server's Port** | Enter the TCP port number on which the physical server listens for web or web services connections, depending on whether you have selected a web protection profile or an XML protection profile, respectively.<br>This option appears only if *Deployment Mode* is *Single Server*. |

**Load Balancing Algorithm**

Select the load balancing algorithm to use when distributing new connections amongst physical servers in the server farm.

- **Round Robin**: Distributes new connections to the next physical server in the server farm, regardless of weight, response time, traffic load, or number of existing connections. Unresponsive servers are avoided.
- **Weighted Round Robin**: Distributes new connections using the round robin method, except that physical servers with a higher weight value will receive a larger percentage of connections.
- **Least Connection**: Distributes new connections to the physical server with the fewest number of existing, fully-formed connections.
- **HTTP session based Round Robin**: Distributes new connections, if they are not associated with an existing HTTP session, to the next physical server in the server farm, regardless of weight, response time, traffic load, or number of existing connections. Unresponsive servers are avoided. Session management is enabled automatically when you enable this feature, and it therefore does not require that you enable *Session Management* in the web protection profile. This option is available only if *Policy Type* is *Web Protection*.

This option appears only if *Deployment Mode* is *Server Balance*.

**Persistence Timeout**

Enter the timeout for inactive TCP sessions.

This option appears only if *Deployment Mode* is *Server Balance* or *Transparent Servers*.

**Server Health Check**

Select the server health check to use when determining responsiveness of physical servers in the server farm, or select *Create New* to add a server health check in a pop-up window, without leaving the current page. For details, see “Configuring server health checks” on page 109.

This option appears only if *Deployment Mode* is *Server Balance*, *Content Routing*, or *WSDL Content Routing*.

**Note:** If a physical server is unresponsive, wait until the server becomes responsive again before disabling its server health check. Server health checks record the up or down status of the server. If you deactivate the server health check while the server is unresponsive, the server health check will be unable to update the recorded status, and FortiWeb unit will continue to regard the physical server as if it were unresponsive. You can determine the physical server’s connectivity status using the *Service Status* widget or an SNMP trap. For details, see “Service Status widget” on page 32 or “Configuring an SNMP community” on page 48.

**Server Farm**

Select the server farm whose physical servers will receive the connections. For details, see “Grouping physical servers into server farms” on page 106.

This option appears only if *Deployment Mode* is *Server Balance*, *Content Routing*, *WSDL Content Routing*, *Offline Protection*, or *Transparent Servers*.

**Note:** If *Deployment Mode* is *Offline Protection* or *Transparent Servers*, you must select a server farm, even though the FortiWeb unit will be allowing connections to pass through instead of actively distributing connections. Therefore if you want to govern connections for only a single physical server, rather than a group of servers, you must configure a server farm with that single physical server as its only member in order to select it in the policy.

**Protected Servers**

Select a protected hosts group to allow or reject connections based upon whether the `Host:` field in the HTTP header is empty or does or does not match the protected hosts group. For details, see “Configuring protected hosts” on page 113.

If you do not select a protected hosts group, connections will be accepted or blocked based upon other criteria in the policy or protection profile, but regardless of the `Host:` field in the HTTP header.

Attack log messages and *Alert Message Console* messages contain `DETECT_ALLOW_HOST_FAILED` when this feature does not detect an allowed protected host name.

**Note:** Unlike HTTP 1.1, HTTP 1.0 does ***not*** require the `Host:` field. The FortiWeb unit will not block HTTP 1.0 requests for lacking this field, regardless of whether or not you have selected a protected hosts group.

| | |
|---|---|
| **XML Protection Profile**<br>or<br>**Web Protection Profile** | Select the profile to apply to the connections accepted by this policy, or select *Create New* to add a new profile in a pop-up window, without leaving the current page. For details, see "Configuring XML protection profiles" on page 144, "Configuring inline web protection profiles" on page 213 or "Configuring offline protection profiles" on page 219.<br>The name of this drop-down list varies by your selection in *Policy Type*.<br>**Note:** Depending on the profile types that the current operation mode supports, not all profiles may be available. For details, see Table 36 on page 92.<br>• XML protection profiles require inline protection mode.<br>• Offline protection profiles require offline protection mode.<br>• Inline protection profiles require either inline protection mode or transparent mode.<br>**Note:** Whitelisted clients are exempt from being blocked by the protection profile. For details, see "Whitelisting client IP addresses" on page 180.<br>**Note:** Protection profiles are ***not*** applied if `noparse` is set to `enable`. For details, see the *FortiWeb CLI Reference*. |
| **WAF Auto Learning Profile** | Select the auto-learning profile, if any, to use in order to discover attacks, URLs, and parameters in your web servers' HTTP sessions, or select *Create New* to add a new auto-learning profile in a pop-up window, without leaving the current page. For details, see "Configuring auto-learning profiles" on page 223.<br>Data gathered using an auto-learning profile can be viewed in an auto-learning report, and can be used to generate profiles. For details, see "Auto Learn" on page 227. |
| **Service** | Select the custom or predefined service that defines the TCP port number on which the virtual server or bridge receives traffic, or select *Create New* to add a virtual server in a pop-up window, without leaving the current page. For details, see "Configuring custom services" on page 111.<br>This option appears only if *Deployment Mode* is ***not*** *Offline Protection*.<br>**Note:** This option ***only*** defines the port number. It does ***not*** specify SSL/TLS. For example, it is possible to configure a web server to listen on the well-known port number for HTTP (port 80), yet use SSL (HTTPS). To specify SSL/TLS, see *SSL Client*. |
| **URL Case Sensitivity** | Enable to differentiate uniform resource locators (URLs) according to upper case and lower case letters for features that act upon the URLs in the headers of HTTP requests, such as start page rules, black list rules, white list rules, and page access rules.<br>For example, when this option is enabled, an HTTP request involving `http://www.`***`E`***`xample.com/` would ***not*** match profile features that specify `http://www.`***`e`***`xample.com` (difference highlighted in bold). |
| **SSL Server** | Enable to use SSL to encrypt connections from the FortiWeb unit to protected web servers.<br>Disable to pass traffic to protected web servers in clear text.<br>To test whether the web server supports SSL connections, click *SSL Support Test*.<br>This option appears only in inline protection mode. (The FortiWeb unit cannot act as an SSL terminator or initiator in offline protection mode or transparent mode.)<br>**Note:** Enable ***only*** if the protected host supports SSL. |

| | |
|---|---|
| **SSL Client** | Enable if connections from HTTP clients to the FortiWeb unit or protected hosts use SSL. Also configure *Certificate*.<br>FortiWeb units contain specialized hardware to accelerate SSL processing. Offloading SSL processing may improve the performance of secure HTTP (HTTPS) connections.<br>SSL 3.0, TLS 1.0, and TLS 1.1 are supported.<br>The FortiWeb unit handles SSL negotiations and encryption and decryption, instead of the physical server(s), also known as offloading. Connections between the client and the FortiWeb unit will be encrypted. Connections between the FortiWeb unit and each web server will be clear text or encrypted, depending on *SSL Server*.<br>This option appears only if the FortiWeb unit is operating in inline protection mode.<br>**Note:** If the FortiWeb unit is operating in offline protection mode or transparent mode, you must enable *SSL* in the server farm instead.<br>**Caution:** You ***must*** enable either this option or *SSL*, if the connection uses SSL. Failure to enable an SSL option and provide a certificate for HTTPS connections will result in the FortiWeb unit being unable to decrypt connections, and therefore unable to scan HTML or XML content. |
| **Certificate** | Select which server certificate the FortiWeb unit will use when encrypting or decrypting SSL-secured connections, or select *Create New* to upload a new certificate in a pop-up window, without leaving the current page. For more information, see "Uploading a certificate" on page 66.<br>This option appears only if *SSL Client* is enabled. |

**Certificate Verification**

Select the name of a certificate verificator, if any, to use when an HTTP client presents their personal certificate. (If you do not select one, the client is not required to present a personal certificate.)

If the client presents an invalid certificate, the FortiWeb unit will not allow the connection.

To be valid, a client certificate must:

- Not be expired
- Not be revoked by either certificate revocation list (CRL) or, if enabled, online certificate status protocol (OCSP) (see "Configuring certificate verification rules" on page 73)
- Be signed by a certificate authority (CA) whose certificate you have imported into the FortiWeb unit (see "Managing CA certificates" on page 68); if the certificate has been signed by a chain of intermediate CAs, those certificates must be included in an intermediate CA group (see *Certificate Intermediate Group*)
- Contain a `CA` field whose value matches the CA certificate
- Contain an `Issuer` field whose value matches the `Subject` field in the CA certificate

Personal certificates, sometimes also called user certificates, establish the identity of the person connecting to the web site.

You can require that clients present a certificate alternatively or in addition to HTTP authentication. For more information, see "Configuring HTTP authentication" on page 207.

This option appears only if *SSL Client* is enabled, and only applies if the FortiWeb unit is operating in inline protection mode. SSL 3.0 or TLS 1.0 is required.

**Note:** If the connection fails when you have selected a certificate verificator, verify that the certificate meets the web browser's requirements. Web browsers may have their own certificate validation requirements in addition to FortiWeb requirements. For example, personal certificates for client authentication may be required to either:

- not be restricted in usage/purpose by the CA, or
- contain a `Key Usage` field that contains `Digital Signature` or have a `ExtendedKeyUsage` or `EnhancedKeyUsage` field whose value contains `Client Authentication`

If the certificate does ***not*** satisfy browser requirements, although it may be installed in the browser, when the FortiWeb unit requests the client's certificate, the browser may not present a certificate selection dialog to the user, or the dialog may not contain that certificate. In that case, verification will fail.

For browser requirements, see your web browser's documentation.

**Certificate Intermediate Group**

Select the name of a group of intermediate certificate authority (CA) certificates, if any, that will be presented to clients in order for them to validate the server certificate's CA signature.

This can prevent clients from getting certificate warnings when the server certificate configured in *Certificate* has been signed by an intermediate CA, rather than directly by a root CA or other CA currently trusted by the client.

Alternatively, you can include the entire signing chain in the server certificate itself before uploading it to the FortiWeb unit, thereby completing the chain of trust with a CA already known to the client.

This option appears only if *SSL Client* is enabled and the FortiWeb unit is operating in inline protection mode.

| | |
|---|---|
| **Persistent Server Sessions** | Enter the maximum number of concurrent TCP client connections that can be accepted by this policy.<br>The maximum number of HTTP sessions established with each physical server depends on this field, and whether you have selected a single physical server or a server farm, and the *Load Balancing Algorithm*.<br>For example, if the value of *Persistent Server Sessions* is 10,000 and there are 4 physical servers in a server farm that uses *Round Robin*-style load balancing, up to 10,000 client connections would be accepted, resulting in up to 2,500 HTTP sessions evenly distributed to each of the 4 physical servers.<br>For more information, see "Appendix B: Maximum values matrix" on page 291.<br>This option appears only if *Deployment Mode* is not *Offline Protection*. |
| **Comments** | Enter a description or other comment. The description may be up to 35 characters long. |

### Enabling or disabling a policy

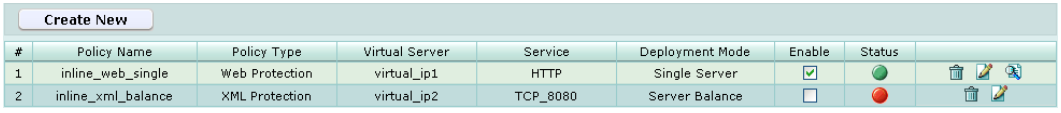
You can individually enable and disable policies.

**Caution:** Disabling a policy could block traffic if no remaining active policies match that traffic.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Server Policy Configuration* category. For details, see "About permissions" on page 58.

#### To enable or disable a policy

1 Go to *Server Policy* > *Policy* > *Policy*.




2 In the row corresponding to the policy that you want to ***enable***, in the *Enable* column, mark the check box.

3 In the row corresponding to the policy that you want to ***disable***, in the *Enable* column, clear the check box.

To determine whether the policy is applicable, see the column "Status" on page 94.

## Configuring virtual servers

*Server Policy* > *Server* > *Virtual Server* displays the list of virtual servers.

Before you can create a policy, you must first configure a virtual server which defines the network interface or bridge and IP address on which traffic destined for an individual physical server or server farm will arrive.

When the FortiWeb unit receives traffic destined for a virtual server, it can then forward the traffic to a physical server or a server farm. The FortiWeb unit identifies traffic as being destined for a specific virtual server if:

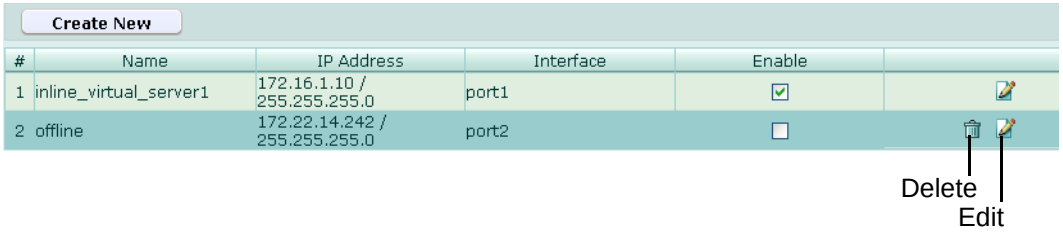
- the traffic arrives on the network interface or bridge associated with the virtual server
- for inline protection mode, the destination address is the IP address of a virtual server (the destination IP address is ignored in other operation modes, ***except*** that it must ***not*** be identical with the physical server's IP address)

**Caution:** Virtual servers can be on the same subnet as physical servers. This configuration creates a one-arm HTTP proxy. For example, the virtual server 10.0.0.1/24 could forward to the physical server 10.0.0.2.
However, this is not recommended. Unless your network's routing configuration prevents it, it could allow clients that are aware of the physical server's IP address to bypass the FortiWeb unit by accessing the physical server directly.

Virtual servers are applied by selecting them within a policy. For details, see "Configuring policies" on page 91.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have *Read* permission to items in the *Server Policy Configuration* category. For details, see "About permissions" on page 58.

**Table 38:** *Virtual Server* **tab**



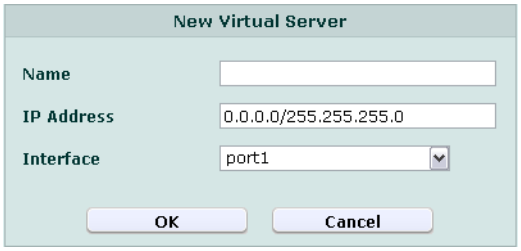

| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a virtual server. |
| **#** | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **IP Address** | The IP address and subnet of the virtual server. |
| **Interface** | The network interface or bridge on which traffic destined for the virtual server will arrive. |
| **Enable** | Mark the check box to enable use of the virtual server. For details, see "Enabling or disabling a virtual server" on page 103. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a policy.<br>Click *Edit* to modify the entry. |

### To add a virtual server

1 Go to *Server Policy* > *Server* > *Virtual Server*.

2 Click *Create New*.

3 Configure the following:



| *Name of the GUI item* | *Description* |
|---|---|
| **Name** | Type the name of the virtual server. |
| **IP Address** | Type the IP address and subnet of the virtual server.<br>If the FortiWeb unit is operating in offline protection mode or transparent mode, this IP address will be ignored when deciding whether or not to apply a policy to the connection, and can therefore be any IP address, ***except*** that it must ***not*** be identical to the physical server. If the virtual server's IP is identical to the physical server, the configuration will not function. |
| **Interface** | Select the network interface or bridge to which the virtual server is bound, and on which traffic destined for the virtual server will arrive. |

4 Click *OK*.

To define the listening port of the virtual server, create a custom service and select it in the policy where the virtual server is also selected. For details, see "Configuring custom services" on page 111.

To apply the virtual server, you must select it in a policy. For details, see "Configuring policies" on page 91.

### Enabling or disabling a virtual server

You can individually enable and disable virtual servers. Disabled virtual servers can be selected in a policy, but will result in a policy that is unable to forward traffic until the virtual server is enabled.

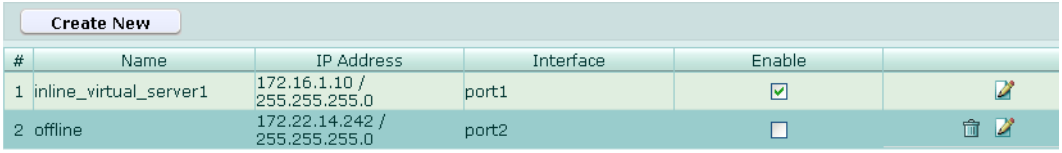
By default, virtual servers are enabled, and the FortiWeb unit can forward traffic from them.

**Caution:** Disabling a virtual server could block traffic matching policies in which you have selected the virtual server. For details, see "Configuring policies" on page 91.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Server Policy Configuration* category. For details, see "About permissions" on page 58.

#### To enable or disable a virtual server

1 Go to *Server Policy* > *Server* > *Virtual Server*.




2 In the row corresponding to the virtual server that you want to ***enable***, in the *Enable* column, mark the check box.

3 In the row corresponding to the virtual server that you want to ***disable***, in the *Enable* column, clear the check box.

## Configuring physical servers

*Server Policy* > *Server* > *Physical Server* displays the list of physical servers.

Before you can create a policy, you must first configure one or more physical servers.

Physical servers define an individual server or a member of a server farm that is the ultimate destination of traffic received by the FortiWeb unit at a virtual server address, and to which the FortiWeb unit will forward traffic after applying the protection profile and other policy settings.

**Note:** A physical server is usually ***not*** the same as a protected hosts group.

Unlike a physical server, which is a single network IP, protected hosts group should contain ***all*** network IPs, virtual IPs, and domain names that clients use in the `Host:` field of the HTTP header to access the web server.

For example, clients often access a web server via a ***public*** network such as the Internet. Therefore the protected hosts group contains domain names, public IP addresses and public virtual IPs on a network edge router or firewall that are routable from that public network. But the physical server is only the IP address that the FortiWeb unit uses to forward traffic to the server, and, unless the FortiWeb unit is operating in offline protection mode or transparent mode, therefore is often a ***private*** network address.

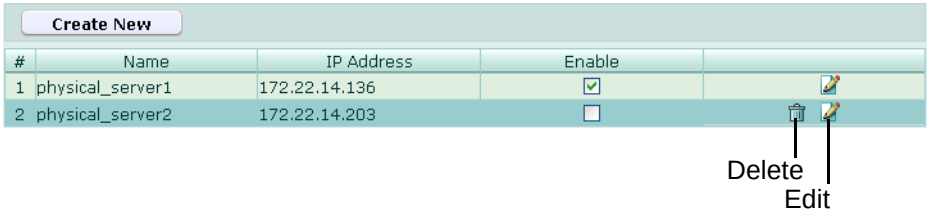
Physical servers are applied either by selecting them within a policy, or grouping them into a server farm that is selected in a policy.

**Note:** Server health checks cannot be used with an individual physical server. If you want to monitor a server for responsiveness, you must group one or more physical servers into a server farm.

For details, see "Configuring policies" on page 91 or "Grouping physical servers into server farms" on page 106.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Server Policy Configuration* category. For details, see "About permissions" on page 58.

**Table 39:** *Physical Server* **tab**



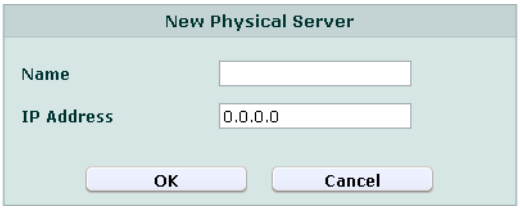

| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a physical server. |
| **#** | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **IP Address** | The IP address of the physical server. |
| **Enable** | Mark the check box to enable use of the physical server. For details, see "Enabling or disabling a physical server" on page 105. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a policy.<br>Click *Edit* to modify the entry. |

**To add a physical server**

1 Go to *Server Policy* > *Server* > *Physical Server*.

2 Click *Create New*.

3 Configure the following:




| *Name of the GUI item* | *Description* |
|---|---|
| **Name** | Enter the name of the physical server. |
| **IP Address** | Enter the IP address of the physical server. |

4 Click *OK*.

To forward traffic from a virtual server to multiple physical servers, you must group the physical servers into a server farm. For more information, see "Grouping physical servers into server farms" on page 106.

To apply the physical server, you must select it in a policy, or group it into a server farm that is selected in a policy. For details, see "Configuring policies" on page 91.

## Enabling or disabling a physical server

You can individually enable and disable physical servers. Disabled physical servers can be selected in a server farm, but will not be used when forwarding traffic.

By default, physical servers are enabled, and the FortiWeb unit can forward traffic to them. To prevent traffic from being forwarded to a physical server, such as when the server will be unavailable for a long time due to repairs, you can disable the physical server. If the disabled physical server is a member of a load balanced server farm, the FortiWeb unit will automatically forward connections to other, enabled physical servers in the server farm; for XPath or WSDL content routed server farms, the FortiWeb unit will forward connections to the first physical server in the server farm.

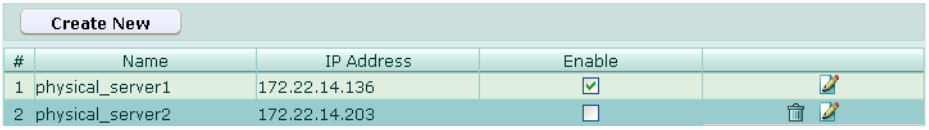
**Note:** If the physical server is a member of a server farm and will unavailable only temporarily, you can alternatively configure a server health check to automatically prevent the FortiWeb unit from forwarding traffic to that physical server when it is unresponsive. For details, see "Configuring server health checks" on page 109.

**Caution:** Disabling a physical server could block traffic matching policies in which you have selected the physical server, or selected a server farm in which the physical server is a member. For details, see "Configuring policies" on page 91.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Server Policy Configuration* category. For details, see "About permissions" on page 58.

**To enable or disable a physical server**

1 Go to *Server Policy* > *Server* > *Physical Server*.




2 In the row corresponding to the physical server that you want to ***enable***, in the *Enable* column, mark the check box.

3 In the row corresponding to the physical server that you want to ***disable***, in the *Enable* column, clear the check box.

## Grouping physical servers into server farms

*Server Policy* > *Server* > *Server Farm* displays the list of server farms.

Server farms define a group of physical servers among which connections will be distributed, or to which they will pass through to, depending on the FortiWeb unit's operating mode. (Inline protection mode actively distributes connections; offline protection and transparent mode do not.)

- **Inline protection mode**: When the FortiWeb unit receives traffic destined for a virtual server, it can then forward the traffic to a physical server or a server farm. If you have configured the policy to forward traffic to a server farm, the connection is routed to one of the physical servers in the server farm. Which of the physical servers receives the connection depends on your configuration of load balancing algorithm, weight, server health checking, or content routing by either XPath expressions or WSDL content routing.

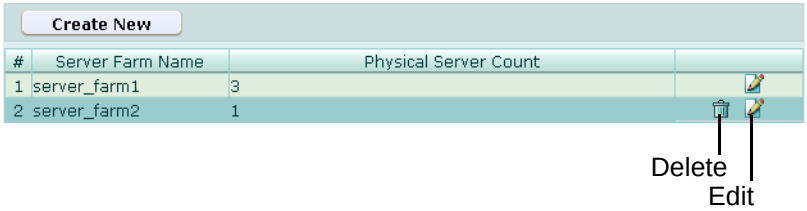
  To prevent traffic from being forwarded to unavailable physical servers, the availability of physical servers in a server farm can be verified using a server health check. Whether the FortiWeb unit will redistribute or drop the connection when a physical server in a server farm is unavailable varies by the availability of other members and by your configuration of the *Deployment Mode* option in the policy. For details, see "Deployment Mode" on page 96.

- **Offline protection/transparent mode**: When the FortiWeb unit receives traffic destined for a virtual server or passing through a bridge, it allows the traffic to pass through to members of the server farm.

Server farms are applied by selecting them within a policy. For details, see "Configuring policies" on page 91.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Server Policy Configuration* category. For details, see "About permissions" on page 58.

**Table 40:** *Server Farm* **tab**



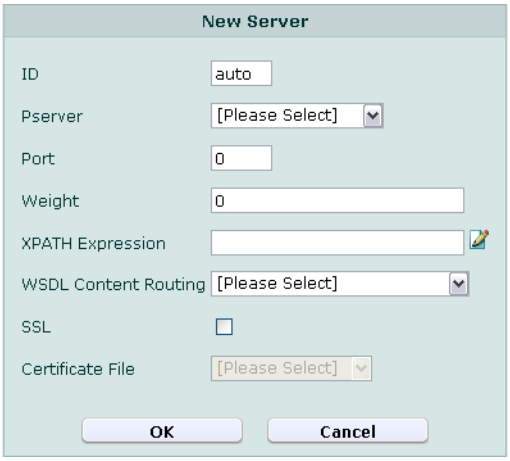
| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a server farm. |
| # | The index number of the entry in the list. |
| **Server Farm Name** | The name of the entry. |
| **Physical Server Count** | The number of physical servers that are members of the server farm. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a policy.<br>Click *Edit* to modify the entry. |

### To configure a server farm

Before configuring a server farm, you must first configure the physical servers that will be members of the server farm. For details, see "Configuring physical servers" on page 103.

1. Go to *Server Policy* > *Server* > *Server Farm*.
2. Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.
3. In *Server Farm Name*, type a name for the server farm.

   This field cannot be modified if you are editing an existing server farm. To modify the name, delete the entry, then recreate it using the new name.
4. In *Comments*, type a description for the server farm.
5. Click *OK*.
6. Click *Create New*, then configure the following:

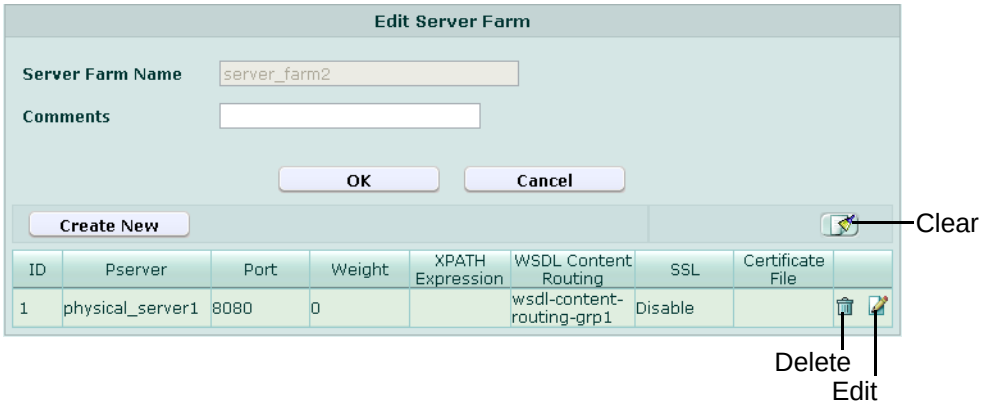


| Name of the GUI item | Description |
|---|---|
| **ID** | Enter the index number of the physical server entry within the server farm, or keep the field's default value of `auto` to let the FortiWeb unit automatically assign the next available index number.<br>The first physical server will receive connections if you have configured XPath or WSDL content routing and the other server is unavailable. For round robin-style load balancing, the index number indicates the order in which connections will be distributed. |
| **Pserver** | Select the name of a physical server that will be a member of the server farm. |
| **Port** | Type the TCP port number on which the physical server listens for connections. |
| **Weight** | If the server farm will be used with the weighted round robin load balancing algorithm, type the numerical weight of the physical server. Physical servers with a greater weight will received a greater proportion of connections. |
| **XPATH Expression** | Click the icon to display a pop-up window that enables you to enter an XPath expression. HTTP requests with content matching this expression will be routed to this physical server.<br>**Note:** For web services connections, you can alternatively or additionally configure the *WSDL Content Routing* option. |
| **WSDL Content Routing** | Select the name of the WSDL content routing group, if any, that defines web services that will be routed to this physical server. For information on configuring a WSDL content routing group, see "Configuring WSDL content routing groups" on page 133.<br>**Note:** You can alternatively or additionally configure the *XPATH Expression* option. |
| **SSL** | Enable if connections to the server use SSL, ***and*** if the FortiWeb unit is operating in offline protection mode. Also configure *Certificate File*.<br>Unlike *SSL Client* in policies, when you enable this option, the FortiWeb unit will ***not*** apply SSL. Instead, it will use the certificate to decrypt and scan connections before passing the encrypted traffic through to the web servers or clients.<br>SSL 3.0, TLS 1.0, and TLS 1.1 are supported.<br>This option takes effect only if the FortiWeb unit is operating in offline protection mode or transparent mode.<br>**Caution:** You ***must*** enable either this option or *SSL Client* if the connection uses SSL. Failure to enable an SSL option and provide a certificate will result in the FortiWeb unit being unable to decrypt connections, and therefore unable to scan HTML or XML content.<br>**Note:** When this option is enabled, the web server must be configured to apply SSL. The FortiWeb unit will use the certificate to decrypt and scan traffic only. It will ***not*** apply SSL to the connections.<br>**Note:** Ephemeral (temporary key) Diffie-Hellman exchanges are not supported if the FortiWeb unit is operating in offline protection mode. |
| **Certificate File** | Select the physical server's certificate that the FortiWeb unit will use when decrypting SSL-secured connections, or select *Create New* to upload a new certificate in a pop-up window, without leaving the current page. For more information, see "Uploading a certificate" on page 66.<br>This option appears only if *SSL* is enabled. |

If the server farm will be used with a policy whose *Deployment Mode* is *Content Routing* or *WSDL Content Routing*, place the physical server that you want to be the failover first in the list of physical servers in the server farm. Because in content routing or WSDL content routing each server in the server farm may not host identical web services, if a physical server is unresponsive to the server health check, the FortiWeb unit will forward subsequent connections to the first physical server in the server farm, which will be considered to be the failover. ***The first physical server must be able to act as a backup for all of the other servers in the server farm.***

7 Repeat the previous step for each physical server that you want to add to the server farm.

8 If you need to modify a physical server, click its *Edit* icon. To remove a single physical server from the server farm, click its *Delete* icon. To remove all physical servers from the server farm, click the *Clear* icon.




9 Click *OK*.

To monitor members of the server farm for responsiveness, configure a server health check that will be used with the server farm. For details, see "Configuring server health checks" on page 109.

To use a server farm as the destination for web or web services connections, select it when configuring a policy. For details, see "Configuring policies" on page 91.

## Configuring server health checks

*Server Policy* > *Server Health Check* > *Server Health Check* displays the list of server health checks.

If you want to create a policy in which you will select a server farm whose servers are monitored for responsiveness, you must first create a server health check.

Server health checks poll physical servers that are members of the server farm to determine their availability — that is, whether or not the server is responsive — before forwarding traffic. Server health check configurations can specify TCP, HTTP, or ICMP ECHO (ping). A health check occurs every number of seconds indicated by the interval. If a reply is not received within the timeout period, and you have configured the health check to retry, it will attempt a health check again; otherwise, the server is deemed unresponsive. The FortiWeb unit will compensate by disabling traffic to that server until it becomes responsive again.

**Note:** If a physical server is more permanently unavailable, such as when a server is undergoing hardware repair or when you have removed a server from the server farm, you may be able to improve the performance of your FortiWeb unit by disabling the physical server, rather than allowing the server health check to continue to check for responsiveness. For details, see "Configuring physical servers" on page 103.

Server health checks are applied by selecting them in a policy, for use with the entire server farm. For details, see "Configuring policies" on page 91.

To view the status currently being detected by server health checks, you can use the *Service Status* widget. For details, see "Service Status widget" on page 32.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Server Policy Configuration* category. For details, see "About permissions" on page 58.

**Table 41:** *Server Health Check* **tab**


| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a server health check. |
| **#** | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Type** | The protocol that the server health check will use to contact the physical server.<br>• **Disabled** (the server health check is currently disabled)<br>• **Ping**<br>• **TCP**<br>• **HTTP** |
| **Details** | The URL that will be used in the HTTP GET request if the *Type* of the server health check is *HTTP*. If the physical server successfully returns this content, it is considered to be responsive. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a server farm or policy.<br>Click *Edit* to modify the entry. |

### To add a server health check

1 Go to *Server Policy* > *Server Health Check* > *Server Health Check*.

2 Click *Create New*.

3 In *Name*, type the name of the server health check.

4 From *Protocol Type*, select the protocol that the server health check will use to contact the physical server, or select *Disabled* to disable the server health check.

The remaining fields vary by your selection of *Protocol Type*.

5 Configure the following:

**Figure 11: Adding a server health check (Ping)**

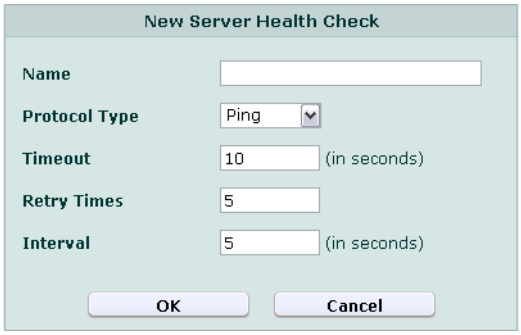


**Figure 12: Adding a server health check (TCP)**

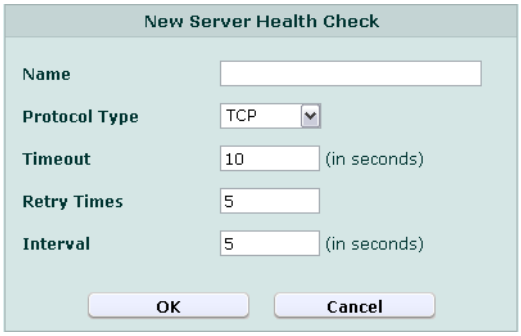
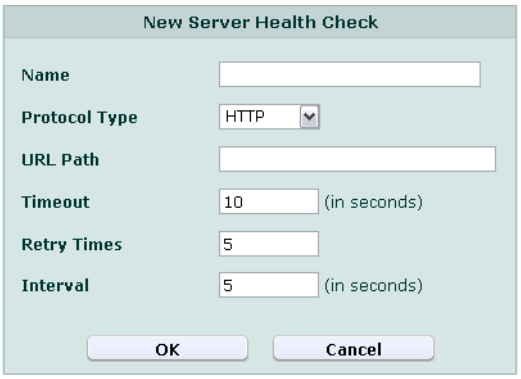



**Figure 13: Adding a server health check (HTTP)**




| *Name of the GUI item* | *Description* |
|---|---|
| **URL Path** | Enter the portion of the URL, such as `/index.html`, that follows the URL's domain name or IP address portion. This path will be used in the HTTP GET request to verify the responsiveness of the server. If the physical server successfully returns this content, it is considered to be responsive.<br>This option appears only if *Protocol Type* is *HTTP*. |
| **Timeout** | Enter the number of seconds which must pass after the server health check to indicate a failed health check. |
| **Retry Times** | Enter the number of times, if any, a failed health check will be retried before the server is determined to be unresponsive. |
| **Interval** | Enter the number of seconds between each server health check. |

6 Click *OK*.

To apply a server health check, select it when configuring a policy that uses a server farm. For details, see "Configuring policies" on page 91.

# Configuring custom services

*Server Policy* > *Service* > *Custom* displays the list of your custom services.

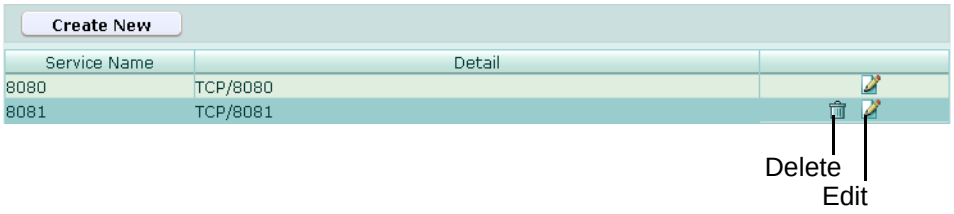
Services define protocols and TCP port numbers and can be selected in a policy to define the traffic that the policy will match.

While some predefined services are available (see"Viewing the list of predefined services" on page 113), you may need to configure your own custom services if your virtual servers will receive traffic on non-standard TCP port numbers.

Custom services can be selected in a policy in order to define the protocol and listening port of a virtual server. Before or during creating a policy, you must configure a service that defines the TCP port number on which traffic destined for a virtual server will arrive. (Exceptions include policies whose *Deployment Mode* is *Offline Protection*, which do not require that you define a TCP port number using a service.) For details, see "Configuring policies" on page 91.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Server Policy Configuration* category. For details, see "About permissions" on page 58.

**Table 42:** *Custom* **tab**



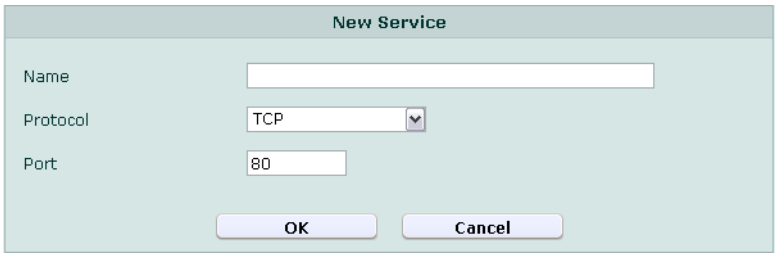

| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a custom service. |
| **Service Name** | The name of the entry. |
| **Detail** | The protocol and TCP port number of the service. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a policy.<br>Click *Edit* to modify the entry. |

### To add a custom service

1 Go to *Server Policy* > *Service* > *Custom*.

2 Click *Create New*.

3 Configure the following:




| *Name of the GUI item* | *Description* |
|---|---|
| **Name** | Enter the name of the service. |
| **Port** | Enter the TCP port number of the service. |

4 Click *OK*.

To use a custom service as the listening port of a virtual server, you must select it in a policy. For details, see "Configuring policies" on page 91.

### Viewing the list of predefined services

*Server Policy* > *Service* > *Predefined* displays the list of predefined services.

Services define protocols and TCP port numbers and can be selected in a policy to define the traffic that the policy will match.

Predefined services can be selected in a policy in order to define the protocol and listening port of a virtual server. For details, see "Configuring policies" on page 91.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have *Read* permission to items in the *Server Policy Configuration* category. For details, see "About permissions" on page 58.

**Table 43:** *Predefined* **tab**

| Name | Detail |
|---|---|
| HTTP | TCP/ 80 |
| HTTPS | TCP/ 443 |

| *Name of the GUI item* | *Description* |
|---|---|
| **Name** | The name of the entry. |
| **Detail** | The protocol and TCP port number of the service. |

## Configuring protected hosts

*Server Policy* > *Protected Servers* > *Protected Servers* displays the list of protected host groups.

A protected host group contains one or more IP addresses and/or fully qualified domain names (FQDNs). Each of those entries in the protected host group defines a virtual or real web host, according to the `Host:` field in the HTTP header of requests from clients, that you want the FortiWeb unit to protect.

For example, if your web servers receive requests with HTTP headers such as:

```
GET /index.php HTTP/1.1
Host: www.example.com
```

you might define a protected host group with an entry of `www.example.com` and select it in the policy. This would reject requests that are not for that host.

**Note:** A protected hosts group is usually ***not*** the same as a physical server.

Unlike a physical server, which is a single IP at the network layer, protected host group should contain ***all*** network IPs, virtual IPs, and domain names that clients use to access the web server at the application (HTTP) layer.

For example, clients often access a web server via a ***public*** network such as the Internet. Therefore the protected host group contains domain names, public IP addresses and public virtual IPs on a network edge router or firewall that are routable from that public network. But the physical server is only the IP address that the FortiWeb unit uses to forward traffic to the server, and, unless the FortiWeb unit is operating in offline protection or transparent mode, therefore is often a ***private*** network address.

Protected host groups can be used by:

- policies
- input rules

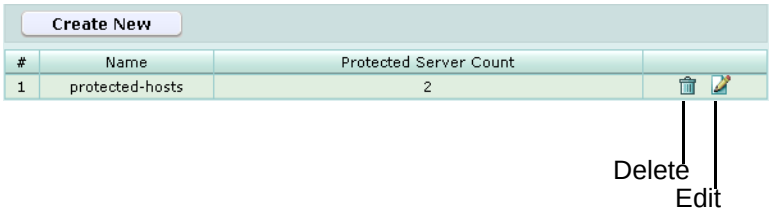
- server protection exceptions
- start page rules
- page access rules
- black list rules
- white list rules
- allowed method exceptions
- HTTP authentication rules
- hidden fields rules

These rules can use protected host definitions to apply rules only to requests for a protected host. If you do not specify a protected host group in the rule, the rule will be applied based upon other criteria such as the URL, but regardless of the `Host:` field.

Policies can use protected host definitions to block connections that are not destined for a protected host. If you do not select a protected host group in a policy, connections will be accepted or blocked regardless of the `Host:` field.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Server Policy Configuration* category. For details, see "About permissions" on page 58.

**Table 44:** *Protected Servers* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a protected host group. |
| # | The index number of the protected host group. |
| **Name** | The name of the entry. |
| **Protected Server Count** | The number of hosts contained in the protected host group. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a policy or other item.<br>Click *Edit* to modify the entry. |

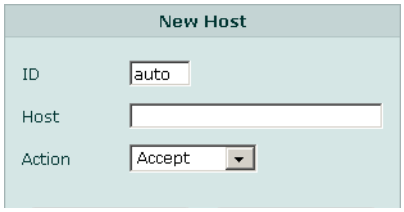
### To add a protected host group

1. Go to *Server Policy* > *Protected Servers* > *Protected Servers*.
2. Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.
3. In *Name*, type the name of the protected host group.

   This field cannot be modified if you are editing an existing protected host group. To modify the name, delete the entry, then recreate it using the new name.
4. From *Default Action*, select whether to *Accept* or *Deny* HTTP requests that do ***not*** match any of the host definitions that you will add to this protected host group.

5 Click *OK*.

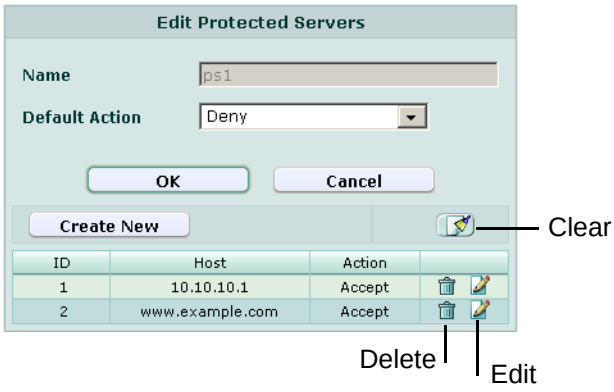
6 Click *Create New*, then configure the following:




| *Name of the GUI item* | *Description* |
|---|---|
| **ID** | Enter the index number of the host entry within the protected host group, or keep the field's default value of `auto` to let the FortiWeb unit automatically assign the next available index number. |
| **Host** | Enter the IP address or fully qualified domain name (FQDN) of a real or virtual web host, according to the `Host:` field in HTTP requests, that you want the FortiWeb unit to protect.<br>If clients connect to your web servers through the IP address of a virtual server on the FortiWeb unit, this should be the IP address of that virtual server ***or*** any domain name to which it resolves, ***not*** the actual IP address of the web server.<br>For example, if a virtual server 10.0.0.1/24 forwards traffic to the physical server 192.168.1.1, for protected hosts, you would enter:<br>• `10.0.0.1`, the address of the virtual server<br>• `www.example.com`, the domain name that resolves to the virtual server |
| **Action** | Select whether to *Accept* or *Deny* HTTP requests whose `Host:` field matches this host entry. |

7 Repeat the previous step for each host that you want to add to the protected host group.

8 If you need to modify a host, click its *Edit* icon. To remove a single host from the protected host group, click its *Delete* icon. To remove all hosts from the protected host group, click the *Clear* icon.



9 Click *OK*.

To use a protected host group, you must select it in a policy, input rule, start page rule, page access rule, black list rule, white list rule, and/or hidden field rule. For details, see:

- "Configuring policies" on page 91
- "Configuring input rules" on page 152
- "Configuring page order rules" on page 158
- "Configuring start pages" on page 170
- "Configuring URL black list rules" on page 173
- "Configuring URL white list rules" on page 175
- "Configuring allowed method exceptions" on page 191
- "Configuring hidden field rules" on page 194

Attack log messages and *Alert Message Console* messages contain `DETECT_ALLOW_HOST_FAILED` when this feature does not detect an allowed protected host name.

# Grouping the predefined data types

*Server Policy* > *Predefined Pattern* > *Data Type Group* displays the list of data type groups.

A data type group defines which of the predefined data types (see "Viewing the list of predefined data types" on page 118) the FortiWeb unit will attempt to detect and track in input parameters when gathering data for an auto-learning report.

For example, if you include the *Email* data type in the data type group, auto-learning profiles that use the data type group might discover that your web applications use a parameter named `username` whose value is an email address.

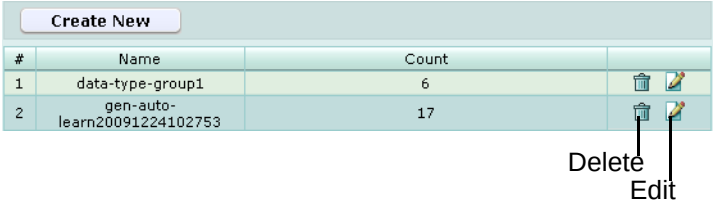
**Tip:** If you know that your network's HTTP sessions do not include a specific data type, omit it from the data type group to improve performance. The FortiWeb unit will not expend resources scanning traffic for that data type.

Data type groups are used by auto-learning profiles. For details, see "Configuring auto-learning profiles" on page 223.

**Note:** Alternatively, you can automatically configure a data type group that includes all types by generating a default auto-learning profile. For details, see "Generating an auto-learning profile and its components" on page 227.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Server Policy Configuration* category. For details, see "About permissions" on page 58.

**Table 45:** *Data Type Group* **tab**

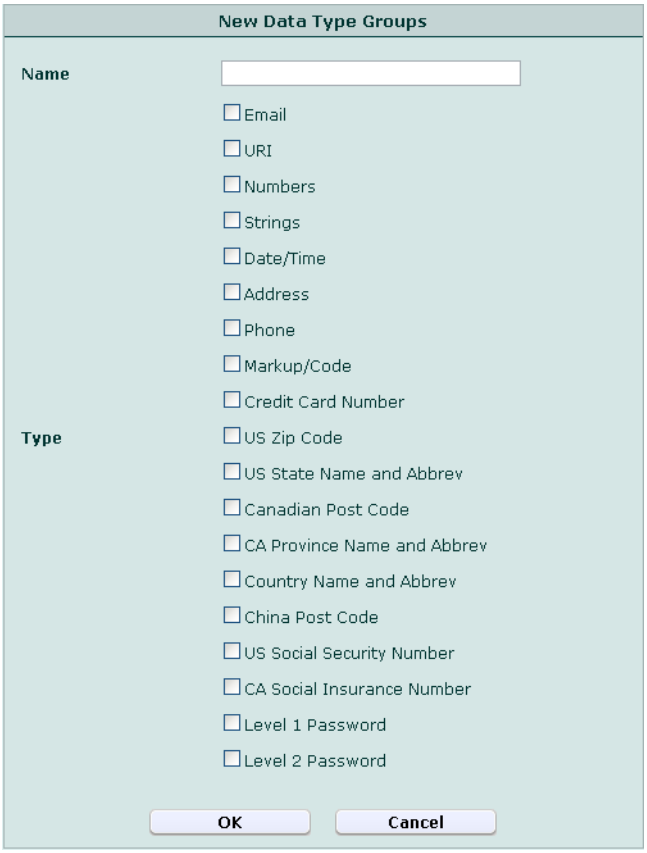


| Name of the GUI item | Description |
|---|---|
| **Create New** | Click to add a data type group. |
| # | The index number of the data type group. |
| **Name** | The name of the entry. |
| **Count** | The number of predefined data types included in this data type group. For details, see "Viewing the list of predefined data types" on page 118. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in an auto-learning profile.<br>Click *Edit* to modify the entry. |

### To add a data type group

1 Go to *Server Policy* > *Predefined Pattern* > *Data Type Group*.

2 Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.




3 In *Name*, type a name for the data type group.

This field cannot be modified if you are editing an existing data type group. To modify the name, delete the entry, then recreate it using the new name.

4 In *Type*, enable the predefined data types that you want to include in the group.

To view the regular expressions for the types of patterns that each data type will detect, see "Viewing the list of predefined data types" on page 118.

5 Click *OK*.

To use a data type group, select it when configuring an auto-learning profile. For details, see “Configuring auto-learning profiles” on page 223.

## Viewing the list of predefined data types

*Server Policy* > *Predefined Pattern* > *Predefined Data Type* displays the list of predefined data types.

Predefined data types are selected in data type groups, which are used by input rules to define the data type of an input, and by auto-learning profiles to detect valid input parameters. For details, see “Grouping the predefined data types” on page 116.

To be able to access this part of the web-based manager, in your administrator account’s access profile, you must have *Read* permission to items in the *Server Policy Configuration* category. For details, see “About permissions” on page 58.

**Table 46:** *Predefined Data Type* **tab**

| Name | Pattern | Description |
|---|---|---|
| Email | | |
| URI | | |
| Numbers | | |
| Strings | | |
| Date/Time | | |
| Address | | |
| Phone | | |
| Markup/Code | | |
| Credit Card Number | | |
| US Zip Code | | |
| US State Name and Abbrev | | |
| Canadian Post Code | | |
| CA Province Name and Abbrev | | |
| Country Name and Abbrev | | |
| China Post Code | | |
| US Social Security Number | | |
| CA Social Insurance Number | | |
| Level 1 Password | | |
| Level 2 Password | | |

| *Name of the GUI item* | *Description* |
|---|---|
| **Name** | The name of the data type.<br>• **Address**: Canadian postal codes and United States ZIP code and ZIP + 4 codes.<br>• **Canadian Post Code**: Canadian postal codes such as K2H 7B8.<br>• **CA Province Name and Abbrev**: Modern and older names and abbreviations of Canadian provinces in English, as well as some abbreviations in French, such as Quebec, IPE, Sask, and Nunavut. Does ***not*** detect province names in French.<br>• **CA Social Insurance Nubmer**: Canadian Social Insurance Numbers (SIN) such as 123-456-789.<br>• **China Post Code**: Chinese postal codes such as 610000.<br>• **Country Name and Abbrev**: Country names, codes, and abbreviations in English characters, such as CA, Cote d'Ivoire, Brazil, Russian Federation, and Brunei Darussalam.<br>• **Credit Card Number**: American Express, Carte Blanche, Diners Club, enRoute, Japan Credit Bureau (JCB), Master Card, Novus, and Visa credit card numbers.<br>• **Date/Time**: Dates and times in various formats such as +13:45 for time zone offsets, 1:01 AM, 1am, 23:01:01, and 01.01.30 AM for times, and 31.01.2009, 31/01/2009, 01/31/2000, 2009-01-3, 31-01-2009, 1-31-2009, 01 Jan 2009, 01 JAN 2009, 20-Jan-2009 and February 29, 2009 for dates.<br>• **Email**: Email addresses such as admin@example.com.<br>• **Level 1 Password**: A string of at least 6 characters, with one or more each of lower-case characters, upper-case characters, and digits, such as aBc123. Level 1 passwords are "weak" passwords, generally easier to crack than level 2 passwords.<br>• **Level 2 Password**: A string of at least 8 characters, with one or more each of lower-case characters, upper-case characters, digits, and special characters, such as aBc123$%.<br>• **Markup/Code**: HTML comments, wiki code, hexadecimal HTML color codes, quoted strings in VBScript and ANSI SQL, SQL statements, and RTF bookmarks such as:<br>• `#00ccff, <!--A comment.-->`<br>• `[link url="http://example.com/url?var=A&var2=B"]`<br>• `SELECT * FROM TABLE`<br>• `{\*\bkmkstart TagAmountText}`<br>Does ***not*** match ANSI escape codes, which are instead detected as strings.<br>• **Numbers**: Numbers in various monetary, decimal, comma-separated value (CSV) and other formats such as 123, +1.23, $1,234,567.89, 1'235.140, and -123.45e-6. Does ***not*** detect hexadecimal numbers, which are instead detected as strings or code, and Social Security Numbers, which are instead detected as strings.<br>• **Phone**: Australian, United States, and Indian phone numbers in various formats such as (123)456-7890, 1.123.456.7890, 0732105432, and +919847444225.<br>• **Strings**: Character strings such as alphanumeric words, credit card numbers, United States Social Security Numbers (SSN), UK vehicle registration numbers, ANSI escape codes, and hexadecimal numbers in formats such as user1, 123-45-6789, ABC 123 A, 4125632152365, [32mHello, and 8ECCA04F.<br>• **URI**: Uniform resource identifiers (URI) such as http://www.example.com, ftp://ftp.example.com, and mailto:admin@example.com.<br>• **US Social Security Number**: United States Social Security Numbers (SSN) such as 123-45-6789.<br>• **US State Name and Abbrev**: United States state names and modern postal abbreviations such as HI and Wyoming. Does ***not*** detect older postal abbreviations such as Fl. or Wyo.<br>• **US Zip Code**: United States ZIP code and ZIP + 4 codes such as 34285-3210. |

| | |
|---|---|
| **Pattern** | The regular expression that is used to detect the presence of the data type. Parameter values must match the regular expression in order for an auto-learning profile to successfully detect the data type, or for an input rule to permit the input. |
| **Description** | A description that may include examples of values that match the regular expression. |

# Grouping the predefined suspicious URLs

*Server Policy* > *Predefined Pattern* > *Suspicious URL Rule* displays the list of suspicious URL groups.

.A suspicious URL group selects a subset of one or more predefined suspicious URLs (see "Viewing the list of predefined URL rules" on page 121). Each of those entries in the suspicious URL group defines a type of URL. The FortiWeb unit considers HTTP requests for these administratively sensitive URLs to be possibly malicious when gathering data for an auto-learning profile.

HTTP requests for URLs typically associated with administrative access to your web applications or web server, for example, may be malicious if they originate from the Internet instead of your management LAN. You may want to discover such requests for the purpose of designing blacklist page rules to protect your web server.

If you know that your network's web servers are not vulnerable to a specific type of suspicious URL, such as if the URL is associated with attacks on Microsoft IIS web servers but all of your web servers are Apache web servers, omit it from the suspicious URL group to improve performance. The FortiWeb unit will not expend resources scanning traffic for that type of suspicious URLs.

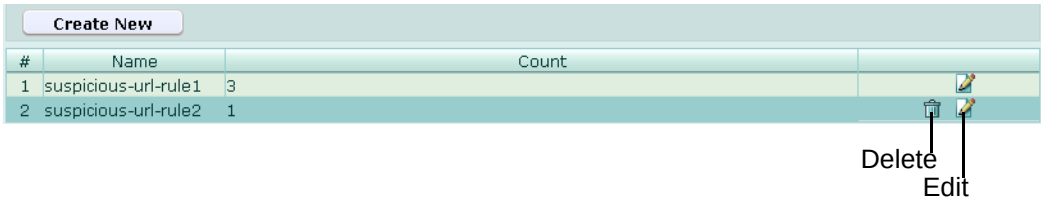
Suspicious URL groups are used by auto-learning profiles. For details, see "Configuring auto-learning profiles" on page 223.

Before creating an auto-learning profile, you must configure a suspicious URL group that defines which HTTP requests for suspicious URL types the FortiWeb unit will attempt to detect.

**Note:** Alternatively, you can automatically configure a suspicious URL group that includes all suspicious URL rules by generating a default auto-learning profile. For details, see "Generating an auto-learning profile and its components" on page 227.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Server Policy Configuration* category. For details, see "About permissions" on page 58.

**Table 47:** *Suspicious URL Rule* **tab**




| ***Name of the GUI item*** | ***Description*** |
|---|---|
| **Create New** | Click to add a suspicious URL group. |
| # | The index number of the suspicious URL group. |

| | |
|---|---|
| **Name** | The name of the entry. |
| **Count** | The number of predefined suspicious URL types included in this suspicious URL group. For details, see "Viewing the list of predefined URL rules" on page 121. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in an auto-learning profile.<br>Click *Edit* to modify the entry. |

### To add a suspicious URL group

1 Go to *Server Policy* > *Predefined Pattern* > *Suspicious URL Rule*.

2 Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.


3 In *Name*, type a name for the suspicious URL group.

This field cannot be modified if you are editing an existing suspicious URL group. To modify the name, delete the entry, then recreate it using the new name.

4 Enable the predefined suspicious URL types that you want to detect:

- *Apache*
- *IIS* (Microsoft IIS)
- *Tomcat* (Apache Tomcat)

To view detailed descriptions of the types of patterns that each suspicious URL type will detect, see "Viewing the list of predefined URL rules" on page 121.

5 Click *OK*.

To use a suspicious URL group, select it when configuring an auto-learning profile. For details, see "Configuring auto-learning profiles" on page 223.

## Viewing the list of predefined URL rules

*Server Policy* > *Predefined Pattern* > *Predefined URL Rule* displays the list of predefined suspicious URL types.

Predefined suspicious URL types are selected in suspicious URL groups, which are used by auto-learning profiles to detect malicious HTTP requests by URL. For details, see "Grouping the predefined suspicious URLs" on page 120.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have *Read* permission to items in the *Server Policy Configuration* category. For details, see "About permissions" on page 58.

**Table 48:** *Predefined URL Rule* **tab**

| Name | Pattern | Description |
|---|---|---|
| IIS | | |
| | ^/(?:a(?:admin\|d(?:samples/config/site\.csc\|_(?:login\|manage)\|m(?:isapi/fpadmin \.htm\|_login\|in(?:\|1\|/(?:index\|default\|manage\|login)\|login\|adduser\|member\|edit\| \.(?:htm\|html\|asp)\|tab\|del(ete)?\|user(login)?\|_(?:admin\|del\|edit\|index(\.asp)?\|login\|main\|user))))\|pp \.cfm\|utoexec\.bat)\|bbs/admin_index\.asp\|c(?:hkadmin\|gi-bin/iisadmpwd/a(?:chg\|exp(2)?\|not) \.htr)\|d(?:atabase(s)?\|b(ase)?)\|i(?:ndex_manage\|isadmpwd/a(?:chg\|not(3)?\|exp(?:\|2(b)?\|3\|4(b)?)) \.htr)\|login_admin\|manage(?:r\|_index)\|passw(?:d(\.txt)?\|ord(?:\|\.dat\|\.log\|\.txt))\|_(?:private /(?:form_results\|orders\|regist(?:er\|rations))\.txt\|vti_pvt/(?:doctodep\.btr\|users \.pwd\|a(?:dministrator(s)?\.pwd\|uthor(?:\.log\|s\.pwd))\|s(?:ervice\.(?:grp\|pwd)\|html \.(?:dll\|exe))))\|A(?:d(?:min_files/order\.log\|vWorks/equipment/catalog_type\.asp)\|SPSamp/AdvWorks /equipment/catalog_type\.asp)\|IISADMPWD/achg\.htr)$ | Check suspicious url files for IIS Server |
| | ^/(?:_private\|iisadmin)/ | Check suspicious url items for IIS Server |
| Apache | | |
| | ^/(?:a(?:admin\|d(?:_(?:login\|manage)\|m(?:_login\|in(?:\|-serv/config/admpw\|1\| /(?:index\|default\|manage\|login)\|login\|adduser\|member\|edit\|\. (?:htm\|html\|asp)\|tab\|del(ete)?\|user(login)?\|_(?:admin\|del\|edit\|index(\.asp)?\|login\|main\|user)))))\|bbs /admin_index\.asp\|chkadmin\|index_manage\|login_admin\|manage(?:\|r\|_index)\|passw(?:d(?:\| \.txt)\|ord(?:\|\.(?:dat\|log\|txt)))\|\.(?:bash_history\|(ht)?(?:access\|passwd))\|~ (?:bin\|ftp\|guest\|l(?:p\|og(s)?)\|named\|root\|t(?:est\|mp)))$ | Check suspicious url files for Apache Server. |
| Tomcat | | |
| | ^/conf/Catalina/localhost/admin.xml$ | Check suspicious url files for Tomcat Server |
| | ^/(?:admin\|server/webapps/admin\|manager)/ | Check suspicious url items for Tomcat Server |

| *Name of the GUI item* | *Description* |
|---|---|
| **Name** | The name of the suspicious URL type. |
| **Pattern** | The regular expression that is used to detect the presence of the suspicious URL. The requested URL must match the regular expression in order for an auto-learning profile to successfully detect the suspicious URL. |
| **Description** | A description that may include examples of values that match the regular expression. |

# XML Protection

This section describes the XML Protection menu, which contains features that act upon HTTP requests with XML content, such as AJAX (JavaScript that uses the XMLHttpRequest object), RSS, and SOAP connections.

This section includes the following topics:



## Configuring schedules

*XML Protection* > *Schedule* menu enables you to view and configure schedules for one-time or recurring use.

Schedules can be used when configuring a content filter rule in order to define when the rule will be applicable.

For example, a FortiWeb unit might be configured with a content filter rule that uses a one-time schedule to block access to the web service during an emergency maintenance period.

For details, see “Configuring content filter rules” on page 126.

This section includes the following topics:



### Configuring one-time schedules

*XML Protection* > *Schedule* > *One Time* displays the list of schedules that are in effect only once, for the period of time specified in the schedule.

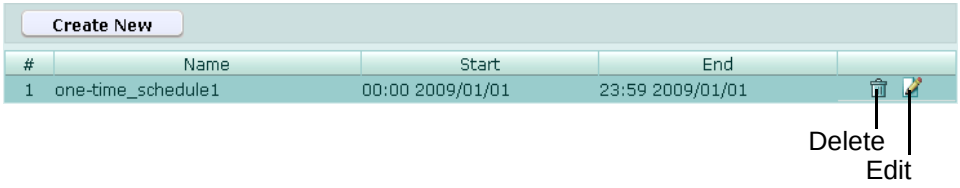
Schedules can be used when configuring a content filter rule in order to define when the rule will be applicable.

For example, a FortiWeb unit might be configured with a content filter rule that uses a one-time schedule to block access to the web service during an emergency maintenance period.

For details, see “Configuring content filter rules” on page 126.

To be able to access this part of the web-based manager, in your administrator account’s access profile, you must have both *Read* and *Write* permission to items in the *XML Protection Configuration* category. For details, see “About permissions” on page 58.

**Table 49:** *One Time* **tab**



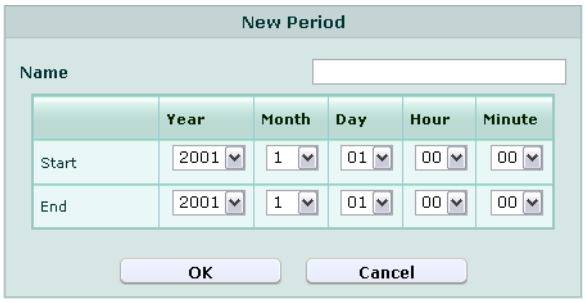

| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a one-time schedule. |
| # | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Start** | The time and date that the schedule will begin. |
| **End** | The time and date that the schedule will stop. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a content filter rule.<br>Click *Edit* to modify the entry. |

### To create a one-time schedule

1 Go to *XML Protection* > *Schedule* > *One Time*.

2 Click *Create New*.

A dialog appears that enables you to specify the time and duration of the schedule.




3 In *Name*, type the name of the schedule.

4 In the *Start* row, select the date and time that the schedule will begin.

5 In the *End* row, select the date and time that the schedule will end.

6 Click *OK*.

To apply a schedule, select it as the period when configuring a content filter rule. For more information, see "Configuring content filter rules" on page 126.

## Configuring recurring schedules

*XML Protection* > *Schedule* > *Recurring* displays the list of schedules that are in effect repeatedly, during the times and days of the week specified in the schedule.

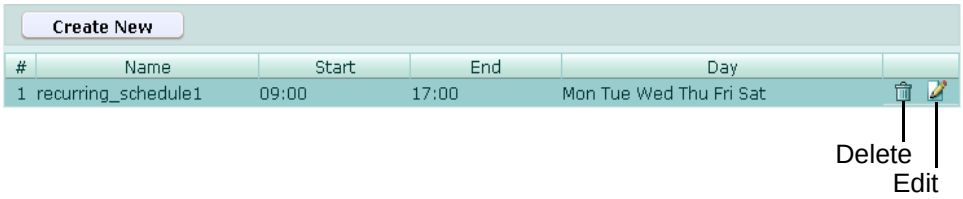
Schedules can be used when configuring a content filter rule in order to define when the rule will be applicable.

For example, you might prevent access during a regularly scheduled maintenance window by creating a content filter rule with a recurring schedule.

For details, see "Configuring content filter rules" on page 126.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *XML Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 50:** *Recurring* **tab**



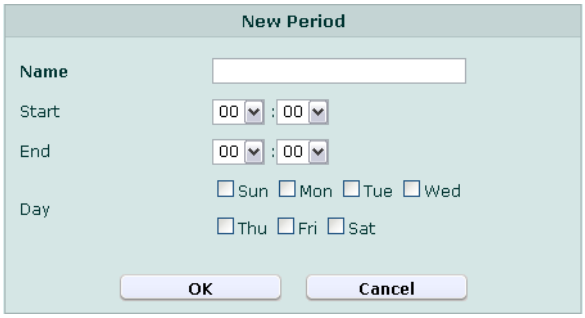

| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a recurring schedule. |
| **#** | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Start** | The time that the schedule will begin. |
| **End** | The time that the schedule will stop. |
| **Day** | The days of the week during which the schedule will be applied. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a content filter rule.<br>Click *Edit* to modify the entry. |

### To create a recurring schedule

1 Go to *XML Protection* > *Schedule* > *Recurring*.

2 Click *Create New*.

A dialog appears that enables you to specify the time and duration of the schedule, and the days of the week during which the schedule will be applied.




3 In *Name*, type the name of the schedule.

4 In the *Start* row, select the time that the schedule will begin.

**Note:** A recurring schedule with a stop time that occurs before the start time starts at the start time and finishes 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 the same time.

5 In the *End* row, select the time that the schedule will end.

6 In the *Day* row, select the days of the week during which the schedule will be applied.

7 Click *OK*.

To apply a schedule, select it as the period when configuring a content filter rule. For more information, see “Configuring content filter rules” on page 126.

# Configuring content filter rules

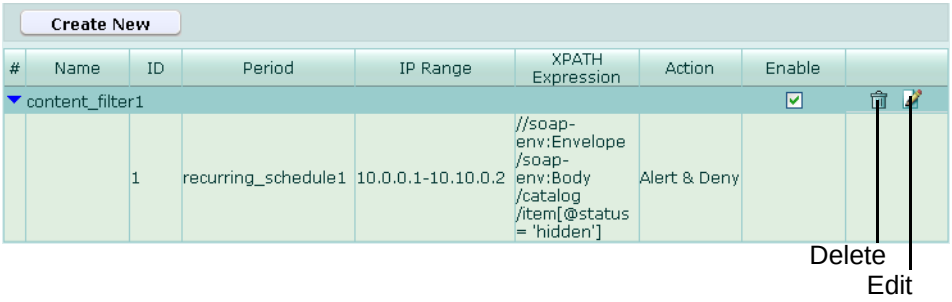
*XML Protection* > *Content Filter* > *Content Filter* displays the list of filter rules that can be applied to XML traffic.

Content filter rules contain one or more individual rules that each accept or block and/or log specific XML content that matches their XPath expression and time schedule.

Content filter rules are applied by selecting them in an XML protection profile. For details, see “Configuring XML protection profiles” on page 144.

To be able to access this part of the web-based manager, in your administrator account’s access profile, you must have both *Read* and *Write* permission to items in the *XML Protection Configuration* category. For details, see “About permissions” on page 58.

**Table 51:** *Content Filter* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a content filter rule. |
| **#** | The index number of the entry in the list. |
| **Name** | The name of the entry.<br>Select the blue arrow to expand the entry, displaying the individual rules contained in the entry. |
| **ID** | The index number of the content filter. For details, see “How priority affects content filter rule matching” on page 129. |
| **Period** | The schedule that defines when this content filter will be applicable. For details, see “Configuring schedules” on page 123. |
| **IP Range** | If this content filter does not apply to all IP addresses, the client IP address or IP address range. |
| **XPATH Expression** | The XPath expression that matches web service content to which the *Action* will be applied. |

| | |
|---|---|
| **Action** | The action that the FortiWeb unit will take when content matches *XPATH Expression*. For details on how *Action* interacts with *ID* to determine which content filter rules will be applied, see "How priority affects content filter rule matching" on page 129.<br>• **Accept**: Accept the connection.<br>• **Alert**: Accept the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>• **Deny**: Block the connection.<br>• **Alert & Deny**: Block the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252. |
| **Enable** | Mark the check box to enable use of the content filter rule. For details, see "Enabling or disabling a content filter rule" on page 129. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a protection profile.<br>Click *Edit* to modify the entry. |

### To create a content filter rule

Before configuring a content filter rule, if you want it to be applicable only during a certain time, you must first create either a one-time schedule or a recurring schedule. For details, see "Configuring schedules" on page 123.

1 Go to *XML Protection* > *Content Filter* > *Content Filter*.

2 Click *Create New*.

A dialog appears that enables you to specify the content filter rule.

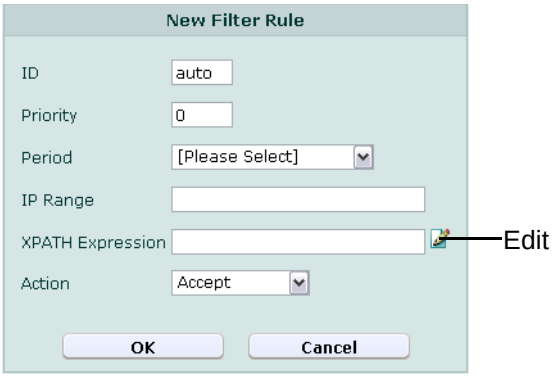
3 In *Name*, type the name of the content filter rule.

This field cannot be modified if you are editing an existing content filter rule. To modify the name, delete the entry, then recreate it using the new name.

4 In *Comments*, type a description for the content filter rule.

5 Click *OK*.

6 Click *Create New*, then configure the following:

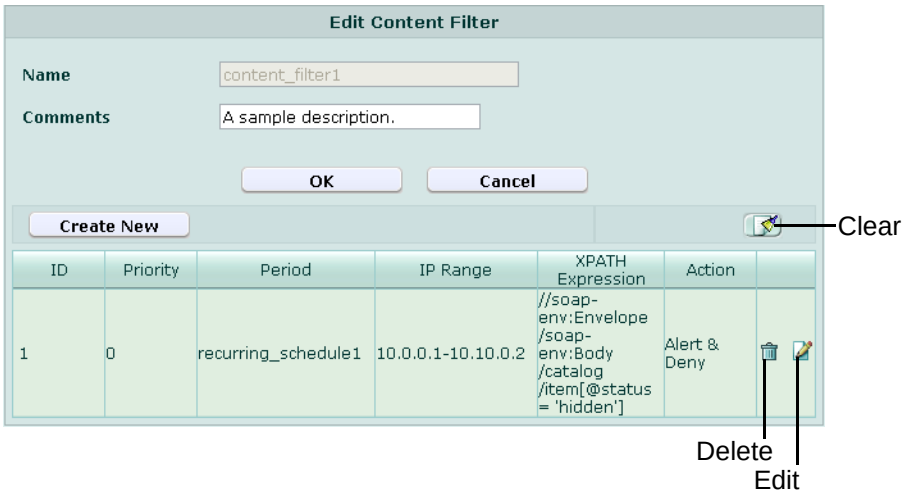



| *Name of the GUI item* | *Description* |
|---|---|
| **ID** | Enter the index number of the content filter, or keep the field's default value of `auto` to let the FortiWeb unit automatically assign the next available index number.<br>The number must be between 1 and 99,999 and must be unique for each content filter. |

| | |
|---|---|
| **Priority** | Enter the order of evaluation for this content filter, starting from 0.<br>To enter a content filter with the highest match priority, enter `0`. For lower-priority matches, enter larger numbers.<br>**Note:** Content filter rule order affects content filter rule matching and behavior. For details, see "How priority affects content filter rule matching" on page 129. |
| **Period** | Select the schedule that defines when this content filter will be applicable. For details, see "Configuring schedules" on page 123. |
| **IP Range** | If this content filter should not apply to all IP addresses, enter a client IP address or IP address range. |
| **XPATH Expression** | Click *Edit* to enter an XPath expression that matches web service content to which the *Action* will be applied, or enter the expression directly into this field.<br>The maximum length of the expression is 1000 characters. |
| **Action** | Select the action that the FortiWeb unit will take when content matches *XPATH Expression*. For details on how *Action* interacts with *ID* to determine which content filter rules will be applied, see "How priority affects content filter rule matching" on page 129.<br>• **Accept**: Accept the connection.<br>• **Alert**: Accept the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>• **Deny**: Block the connection.<br>• **Alert & Deny**: Block the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252. |

7 Repeat the previous step for each content filter that you want to add to the content filter rule.

8 If you need to modify a content filter, click its *Edit* icon. To remove a single content filter from the content filter rule, click its *Delete* icon. To remove all content filters from the content filter rule, click the *Clear* icon.




9 Click *OK*.

To apply the content filter rule, select it in an XML protection profile that is selected in a policy. For more information, see "Configuring XML protection profiles" on page 144.

## How priority affects content filter rule matching

Each time a connection attempt matches a policy that uses an XML protection profile, the FortiWeb unit searches that policy's protection profile's content filter rule list for a matching content filter rule.

The search begins with the smallest *Priority* number (greatest priority) content filter in the content filter rule list and progresses in order towards the largest number in the list. Matching content filter rules are determined by comparing the content filter rule and the connection's web service content. If no content filter rule matches, the connection is dropped.

When the FortiWeb unit finds a matching content filter rule, it applies the matching content filter rule's specified actions to the connection. If the action is:

- **Alert**: The FortiWeb unit applies the action, then evaluates the next content filter rule for a match.
- **Accept** or **Deny**: The FortiWeb unit applies the action and disregards all lower priority rules.

**Note:** Because match evaluation continues until either the content filter rule list is exhausted or the connection is accepted or denied, multiple content filter rules could be applied.

As a general rule, you should order the content filter rule list from most specific to most general because of the order in which content filter rules are evaluated for a match, and because, if the *Action* of the first matching content filter rule is *Accept* or *Deny*, only the first matching content filter rule will be applied to the connection. Subsequent possible matches would not be considered or applied. Ordering content filter rules from most specific to most general prevents content filter rules that match a wide range of traffic and whose action is *Accept* or *Deny* from superseding and effectively masking other content filter rules whose *Action* is *Alert*, or that match exceptions.

## Enabling or disabling a content filter rule

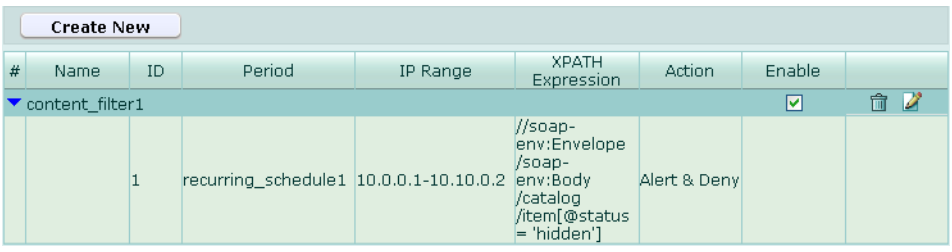
You can individually enable and disable content filter rules. Disabled content filter rules can be selected in an XML protection profile, but will not be used when applying the protection profile.

**Caution:** Disabling a content filter rule could allow traffic matching policies in whose XML protection profile you have selected the content filter rule. For details, see "Configuring XML protection profiles" on page 144.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *XML Protection Configuration* category. For details, see "About permissions" on page 58.

### To enable or disable a content filter rule

1 Go to *XML Protection* > *Content Filter* > *Content Filter*.



2 In the row corresponding to the content filter rule that you want to ***enable***, in the *Enable* column, mark the check box.

3 In the row corresponding to the content filter rule that you want to ***disable***, in the *Enable* column, clear the check box.

# Configuring intrusion prevention rules

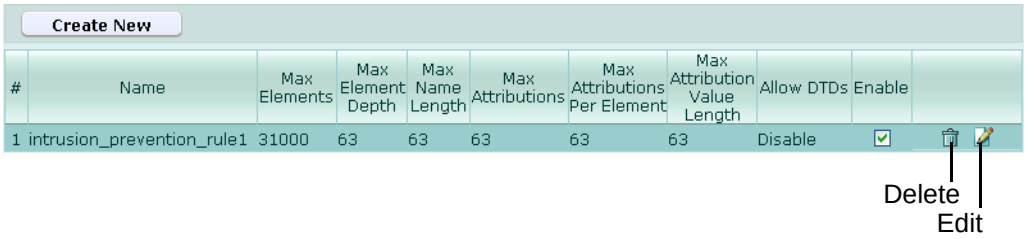
*XML Protection* > *Intrusion Filters* > *Intrusion Filters* displays the list of intrusion prevention rules.

Intrusion prevention rules define data constraints for XML elements, enabling you to prevent use of element depths, data types, and lengths that could be used to execute attacks such as oversized payloads, recursive payloads, and buffer overflows.

Intrusion prevention rules are applied by selecting them in an XML protection profile. For details, see "Configuring XML protection profiles" on page 144.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *XML Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 52:** *Intrusion Filters* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add an intrusion prevention rule. |
| # | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Max Elements** | The maximum number of XML elements to allow in a single request. |
| **Max Element Depth** | The maximum depth of XML elements to allow in the tree of a single request. |
| **Max Name Length** | The maximum length to allow for any XML element, attribute or namespace. |
| **Max Attributions** | The maximum number of attributes to allow in a single request. |
| **Max Attributions Per Element** | The maximum number of attributes to allow for any XML element. |
| **Max Attribution Value Length** | The maximum length of the value to allow for any attribute of any XML element. |
| **Allow DTDs** | Indicates whether or not use of document type definitions (DTDs) are allowed. |
| **Enable** | Mark the check box to enable use of the intrusion prevention rule. For details, see "Enabling or disabling an intrusion prevention rule" on page 132. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a protection profile.<br>Click *Edit* to modify the entry. |

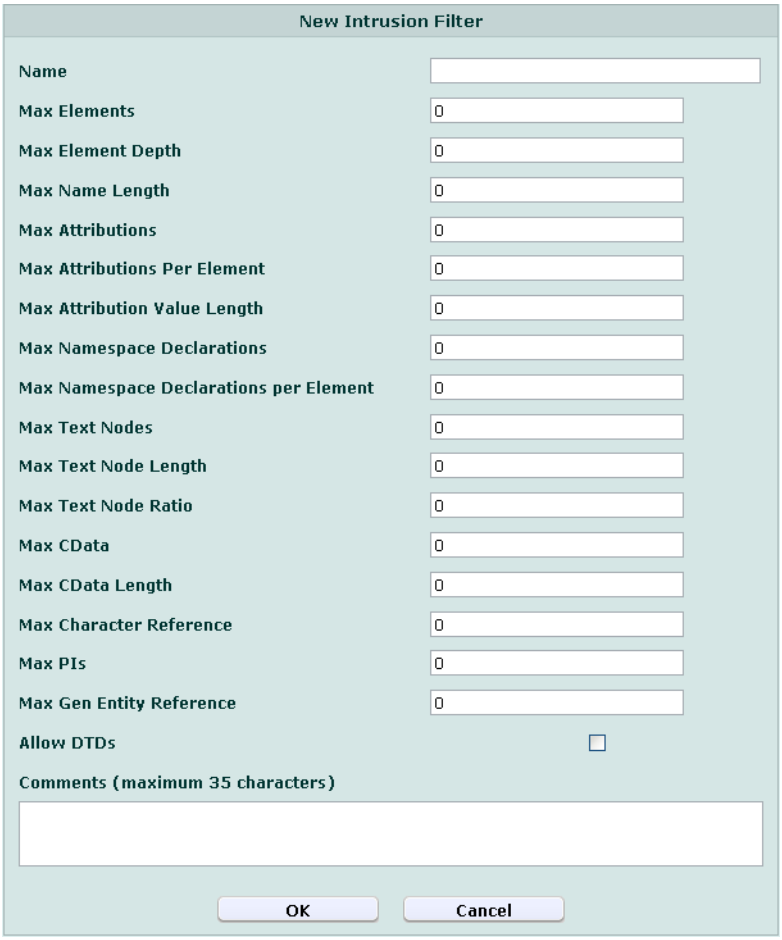
**To create an intrusion prevention rule**

1 Go to *XML Protection* > *Intrusion Filters* > *Intrusion Filters*.

2 Click *Create New*.

A dialog appears that enables you to enter constraints on the types and lengths of data that will be allowed.

3 Configure the following:




| *Name of the GUI item* | *Description* |
|---|---|
| **Name** | Enter a name for the intrusion prevention rule. |
| **Max Elements** | Enter the maximum number of XML elements to allow in a single request. |
| **Max Element Depth** | Enter the maximum depth of XML elements to allow in the tree of a single request. |
| **Max Name Length** | Enter the maximum length to allow for any XML element, attribute or namespace. |
| **Max Attributions** | Enter the maximum number of attributes to allow in a single request. |
| **Max Attributions Per Element** | Enter the maximum number of attributes to allow for any XML element. |
| **Max Attribution Value Length** | Enter the maximum length of the value to allow for any attribute of any XML element. |

| | |
|---|---|
| **Max Namespace Declarations** | Enter the maximum number of XML namespace (XMLNS) declarations to allow in a single request. |
| **Max Namespace Declarations per Element** | Enter the maximum number of XML namespace (XMLNS) declarations to allow for any XML element. |
| **Max Text Nodes** | Enter the maximum number of text nodes to allow in a single request. |
| **Max Text Node Length** | Enter the maximum length to allow for any text node. |
| **Max Text Node Ratio** | Enter the maximum size ratio to allow for any text node, where the maximum size ratio is:<br>`T/(D-T)`<br>where `D` is the total size of the request and `T` is the size of the text node. |
| **Max CData** | Enter the maximum number of character data (CDATA) section to allow in a single request. |
| **Max CData Length** | Enter the maximum length of the value to allow for any character data (CDATA) section in a single request. |
| **Max Character Reference** | Enter the maximum number of character entity references to allow in a single request. |
| **Max PIs** | Enter the maximum number of processing instructions (PIs) to allow in a single request. |
| **Max Gen Entity Reference** | Enter the maximum number of general entity references to allow in a single request. |
| **Allow DTDs** | Enable to allow use of document type definitions (DTDs).<br>Unlike W3C XML Schema scanning, DTD scanning is currently not supported, and therefore inclusion of DTDs can only be categorically allowed or denied. |
| **Comments** | Enter a description for the intrusion prevention rule. |

4 Click *OK*.

To apply the intrusion protection rule, select it in an XML protection profile that is selected in a policy. For more information, see “Configuring XML protection profiles” on page 144.

## Enabling or disabling an intrusion prevention rule

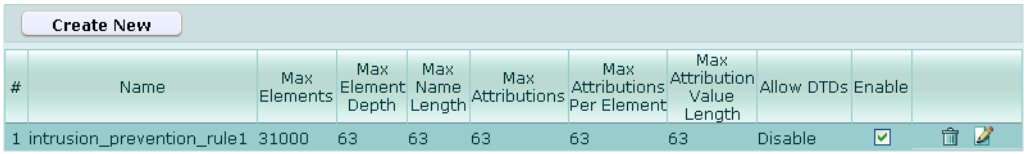
You can individually enable and disable intrusion prevention rules. Disabled intrusion prevention rules can be selected in an XML protection profile, but will not be used when applying the protection profile.

**Caution:** Disabling an intrusion prevention rule could allow traffic matching policies in whose XML protection profile you have selected the intrusion prevention rule. For details, see “Configuring XML protection profiles” on page 144.

To be able to access this part of the web-based manager, in your administrator account’s access profile, you must have both *Read* and *Write* permission to items in the *XML Protection Configuration* category. For details, see “About permissions” on page 58.

**To enable or disable an intrusion prevention rule**

1 Go to *XML Protection* > *Intrusion Filters* > *Intrusion Filters*.




2 In the row corresponding to the intrusion prevention rule that you want to ***enable***, in the *Enable* column, mark the check box.

3 In the row corresponding to the intrusion prevention rule that you want to ***disable***, in the *Enable* column, clear the check box.

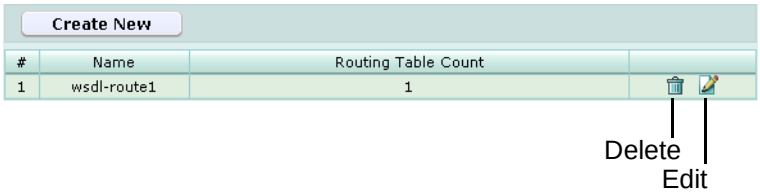
# Configuring WSDL content routing groups

*XML Protection* > *WSDL Routing* > *WSDL Routing* displays the list of WSDL content routing groups.

WSDL content routing groups select a set of web service operations from WSDL files which you can then route to a specific physical server when configuring a server farm.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *XML Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 53:** *WSDL Routing* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a WSDL content routing group. |
| # | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Routing Table Count** | The names of the WSDL files that are used by the WSDL content routing group. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a server farm.<br>Click *Edit* to modify the entry. |

**To create a WSDL content routing group**

Before you can create a WSDL content routing group, you must first upload one or more WSDL files. For details, see "Managing WSDL files" on page 141.

**Note:** Alternatively, you can configure an XPath expression that will define what sets of content will be routed to that physical server. For more information, see "Grouping physical servers into server farms" on page 106.

1 Go to *XML Protection* > *WSDL Routing* > *WSDL Routing*.

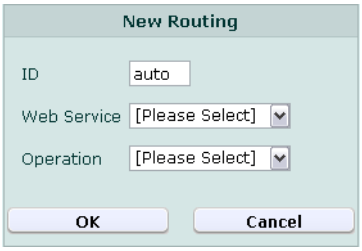
2 Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.

3 In *Name*, type the name of the content routing group.

This field cannot be modified if you are editing an existing content routing group. To modify the name, delete the entry, then recreate it using the new name.

4 Click *OK*.

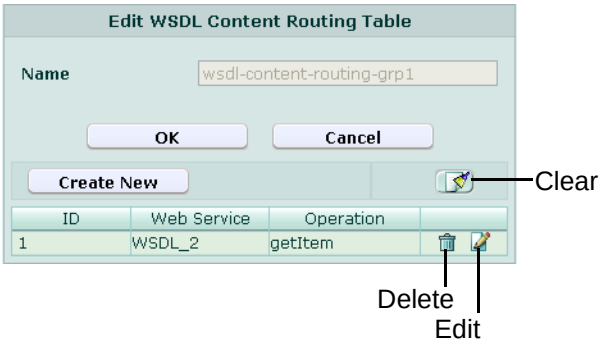
5 Click *Create New*, then configure the following:




| *Name of the GUI item* | *Description* |
|---|---|
| **ID** | Enter the index number of the WSDL operation within the content routing group, or keep the field's default value of `auto` to let the FortiWeb unit automatically assign the next available index number. |
| **Web Service** | Select the name of a WSDL file that you have uploaded. |
| **Operation** | Select the name of an operation within the WSDL file that you selected in the *Web Service* drop-down list. HTTP requests containing this WSDL operation will be routed to a physical server in the server farm using this WSDL content routing group. |

6 Repeat the previous step for each WSDL operation that you want to add to the content routing group.

7 If you need to modify a WSDL operation, click its *Edit* icon. To remove a single WSDL operation from the content routing group, click its *Delete* icon. To remove all WSDL operations from the content routing group, click the *Clear* icon.




8 Click *OK*.

To apply a content routing group, select it as the content that will be destined for a specific physical server when configuring a server farm. For more information, see "Grouping physical servers into server farms" on page 106.

# Managing XML signature and encryption keys

*XML Protection* > *XML Sig/Enc* > *Key File* displays keys that have been uploaded to the FortiWeb unit, and that may be used in a key management group.

Key files contain a key, seed data that can be used with an algorithm to apply and verify XML signatures and/or to encrypt or decrypt XML elements. Keys are not used directly, but instead must first be added to a key management group in order to select it in an XML protection profile. For details, see "Grouping keys into key management groups" on page 136.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have *Read* permission to items in the *XML Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 54:** *Key File* **tab**


| *Name of the GUI item* | *Description* |
|---|---|
| **Import** | Click to upload a key file. For details, see "Uploading a key" on page 135. |
| # | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Comments** | The description of the entry. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a key management group. |

## Uploading a key

If you want to configure XML protection profiles that will apply or validate XML signatures, or apply XML encryption or decryption, you must first upload a key file.

**Note:** The total file size of all certificates, Schema, keys, WSDL, and any other uploaded files may not exceed 12 MB.

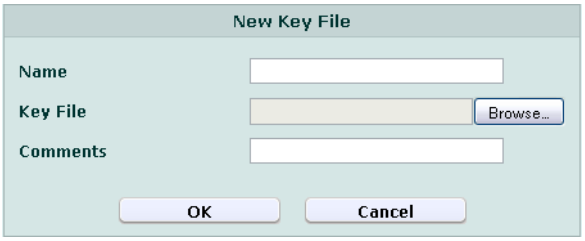
To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *XML Protection Configuration* category. For details, see "About permissions" on page 58.

### To upload a key file

1 Go to *XML Protection* > *XML Sig/Enc* > *Key File*.

2 Click *Import*.

An upload dialog appears.




3 In *Key File*, select the field or click *Browse* to locate and select the key file that you want to upload.

4 Click *OK*.

The file is uploaded from your management computer. Time required varies by the size of the file and the speed of your network connection.

5 After uploading key files, before you can use a key in a protection profile, you must first add the key to a key management group. For details, see "Grouping keys into key management groups" on page 136.

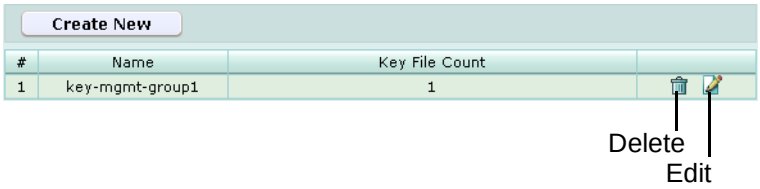
## Grouping keys into key management groups

*XML Protection* > *XML Sig/Enc* > *Key Management* displays the list of key management groups.

Key management groups pair cryptographic algorithms with keys, and may be selected when configuring use of XML signatures and XML encryption or decryption in an XML protection profile.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *XML Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 55:** *Key Management* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a key management group. |
| **#** | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Key File Count** | The number of keys that are used by the key management group. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a protection profile.<br>Click *Edit* to modify the entry. |

### To create a key management group

Before you can create a key management group, you must first upload one or more key files. For details, see “Uploading a key” on page 135.

**Note:** Alternatively, you can create a key management group while configuring an XML protection profile. For more information, see “Configuring XML protection profiles” on page 144.

1 Go to *XML Protection* > *XML Sig/Enc* > *Key Management*.

2 Click *Create New*.

An dialog appears that enables you to add members to the key management group.

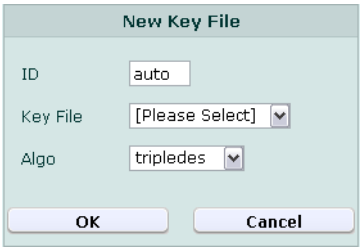
3 In *Name*, type the name of the key management group.

This field cannot be modified if you are editing an existing key management group. To modify the name, delete the entry, then recreate it using the new name.

4 In *Comments*, type a description for the key management group.

5 Click *OK*.

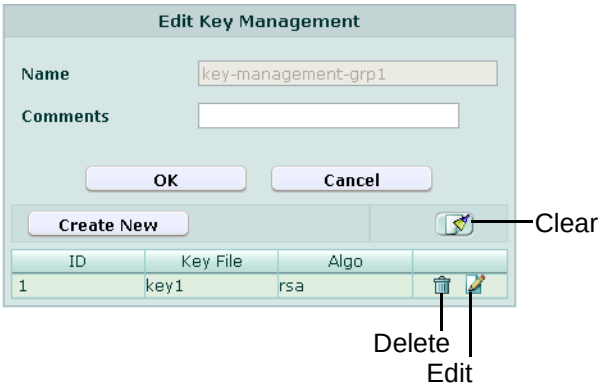
6 Click *Create New*, then configure the following:




| *Name of the GUI item* | *Description* |
|---|---|
| **ID** | Enter the index number of the key file and algorithm combination within the key management group, or keep the field’s default value of `auto` to let the FortiWeb unit automatically assign the next available index number. |
| **Key File** | Select the name of a key file that you have uploaded. |
| **Algo** | Select the name of an encryption algorithm that you want to use with that key. For algorithms that include the bit strength (e.g., 128, 192, or 256), a larger number indicates stronger security, but may increase load on the FortiWeb unit. |

7 Repeat the previous step for each key file and algorithm combination that you want to add to the key management group.

8 If you need to modify an entry, click its *Edit* icon. To remove a single entry from the group, click its *Delete* icon. To remove all entries from the group, click the *Clear* icon.




9 Click *OK*.

To apply a key management group, select it when configuring XML encryption or decryption in an XML protection profile. For more information, see "Configuring XML protection profiles" on page 144.

# Managing Schema files

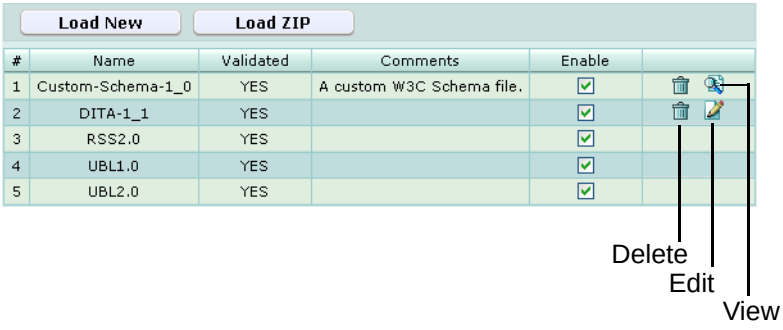
*XML Protection* > *Load Schema* > *Load Schema* displays the list of XML Schema files that have been uploaded to the FortiWeb unit.

Schema files are used by the *Schema Validate* option in XML protection profiles. For details, see "Schema Validate" on page 147.

**Note:** Failing to upload a Schema file could block traffic matching policies in whose XML protection profile you have enabled the *Schema Validate* option, because the FortiWeb unit may not be able to do Schema validation. For details, see "Schema Validate" on page 147.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *XML Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 56:** *Load Schema* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Load New** | Click to upload an uncompressed XML Schema file. For details, see "Managing Schema files" on page 138. |

| | |
|---|---|
| **Load ZIP** | Click to upload a ZIP-compressed XML Schema file. For details, see "Managing Schema files" on page 138. |
| # | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Validated** | Indicates whether or not the Schema file has been successfully validated. If the Schema has been uploaded but not yet been validated, you can click *Edit* in the right-most column to validate it. |
| **Comments** | The description of the entry. |
| **Enable** | Mark the check box to enable use of the Schema file if you have enabled *Schema Validate*. For details, see "Enabling or disabling a Schema file" on page 140. |
| (No column heading.) | Click *Delete* to remove the Schema. This option does not appear for the default schemas (RSS 2.0, UBL 1.0, and UBL 2.0).<br>Click *Edit* to validate the Schema. For details, see "Managing Schema files" on page 138. This option does not appear for the default schemas.<br>Click *View* to display the contents of the Schema file in a pop-up window. |

### To upload a Schema file

**Note:** The total file size of all certificates, Schema, keys, WSDL, and any other uploaded files may not exceed 12 MB.

1 Go to *XML Protection* > *Load Schema* > *Load Schema*.

2 Click either *Load New* to upload an uncompressed Schema file, or *Load ZIP* to upload a Schema file that is compressed within a .zip file.

An upload dialog appears whose appearance varies slightly by whether you are uploading a compressed or uncompressed Schema.

**Figure 14: Uploading an uncompressed Schema**

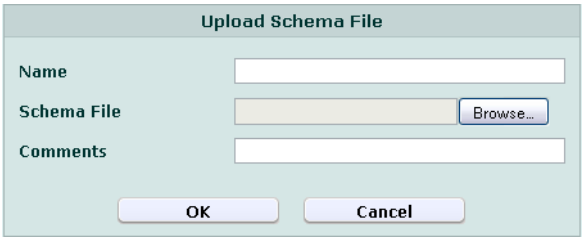
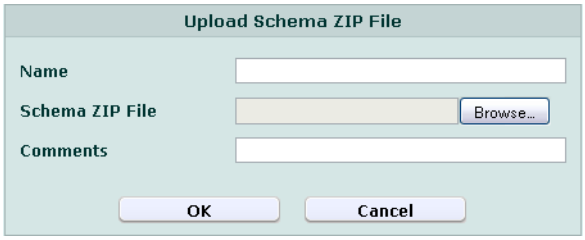



**Figure 15: Uploading a compressed Schema**




3 In *Name*, type the name of the Schema.

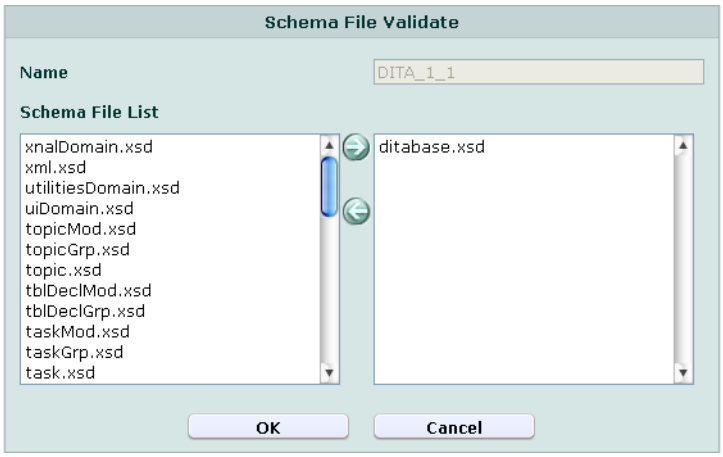
4 In *Schema File* or *Schema ZIP File*, click the field or click *Browse* to locate and select the Schema file that you want to upload.

5 In *Comments*, type a description for the Schema.

6 Click *OK*.

The file is uploaded from your management computer. Time required varies by the size of the file and the speed of your network connection.

7 If you uploaded a compressed Schema file, from the *Schema File List* area, select the root file of the Schema, then click the right arrow.




8 Click *OK*.

The FortiWeb unit validates the root Schema file and all child Schema files. If the Schema is not successfully validated, such as if a compressed Schema is too large, an error message appears. You may select a different root Schema file and attempt the validation again immediately, or you may validate the Schema at another time by clicking its *Edit* icon in the list of Schema files. However, the FortiWeb unit will not use the Schema until it is validated.

To use the Schema to validate requests, you must enable the *Schema Validate* option in an XML protection profile that is used by a policy. For details, see "Schema Validate" on page 147.

## Enabling or disabling a Schema file

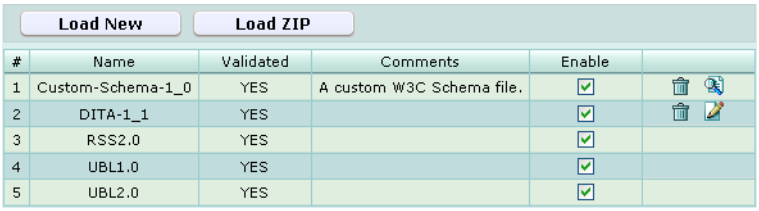
You can individually enable and disable Schema files that you have uploaded to the FortiWeb unit. Disabled Schema files will not be used when performing Schema validation.

**Note:** Disabling a Schema file could block traffic matching policies in whose XML protection profile you have enabled the *Schema Validate* option, because the FortiWeb unit may not be able to do Schema validation. For details, see "Schema Validate" on page 147.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *XML Protection Configuration* category. For details, see "About permissions" on page 58.

**To enable or disable a Schema file**

1 Go to *XML Protection* > *Load Schema* > *Load Schema*.




2 In the row corresponding to the Schema file that you want to ***enable***, in the *Enable* column, mark the check box.

3 In the row corresponding to the Schema file that you want to ***disable***, in the *Enable* column, unmark the check box.

# Managing WSDL files

*XML Protection* > *Load WSDL* > *Load WSDL* displays the list of web service definition language (WSDL) files that have been uploaded to the FortiWeb unit.

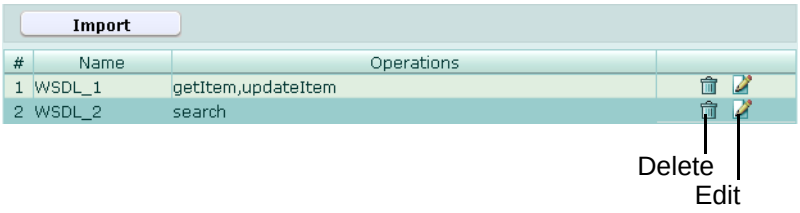
If you want to configure protection profiles that will prevent web services definition language (WSDL) scans and/or validate web services actions, you should first upload the WSDL file that defines the available actions for your web services.

WSDL files cannot be used directly, but instead must be added to a WSDL file group in order to be selected for use with the *WSDL Verify* option in an XML protection profile, or added to a WSDL content routing group in order to be selected for routing to a specific server in a server farm. For details, see "Grouping WSDL files" on page 143 and "Configuring WSDL content routing groups" on page 133.

**Caution:** Failing to upload a WSDL file could allow traffic matching policies in whose XML protection profile you have enabled the *WSDL Verify* option, because the FortiWeb unit will not be able to do WSDL verification. For details, see "WSDL Verify" on page 147.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *XML Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 57:** *Load WSDL* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Import** | Click to upload a WSDL file. For details, see "Managing WSDL files" on page 141. |
| # | The index number of the entry in the list. |
| **Name** | The name of the entry. |

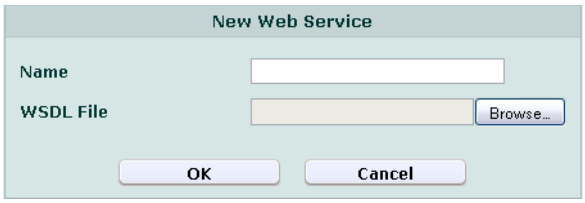
| | |
|---|---|
| **Operations** | The web service operations defined in the WSDL file. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a WSDL file group.<br>Click *Edit* to view details of the entry, or to individually enable or disable web service operations defined in the WSDL file. For details, see "Enabling and disabling operations in a WSDL file" on page 142. |

### To upload a WSDL file

**Note:** The total file size of all certificates, Schema, keys, WSDL, and any other uploaded files may not exceed 12 MB.

1 Go to *XML Protection* > *Load WSDL* > *Load WSDL*.

2 Click *Import*.




3 In *Name*, type the name of the WSDL file.

4 In *WSDL File*, click the field or click *Browse* to locate and select the WSDL file that you want to upload.

5 Click *OK*.

The file is uploaded from your management computer. Time required varies by the size of the file and the speed of your network connection.

6 After uploading WSDL files, you can use them in either:

- a WSDL content routing group (see "Configuring WSDL content routing groups" on page 133)
- an XML protection profile

In order to use them in an XML protection profile, you must first create a WSDL file group. For more information, see "Grouping WSDL files" on page 143.

You can also individually enable or disable web service actions within each WSDL file. For more information, see "Enabling and disabling operations in a WSDL file" on page 142.

## Enabling and disabling operations in a WSDL file

In addition to individually enabling or disabling WSDL files, you can individually enable or disable a web service actions that are defined within each WSDL file.

**Caution:** Disabling a web service action could allow traffic matching policies in whose XML protection profile you have enabled the *WSDL Verify* option, because the FortiWeb unit will not be able to do full WSDL verification. For details, see "WSDL Verify" on page 147.

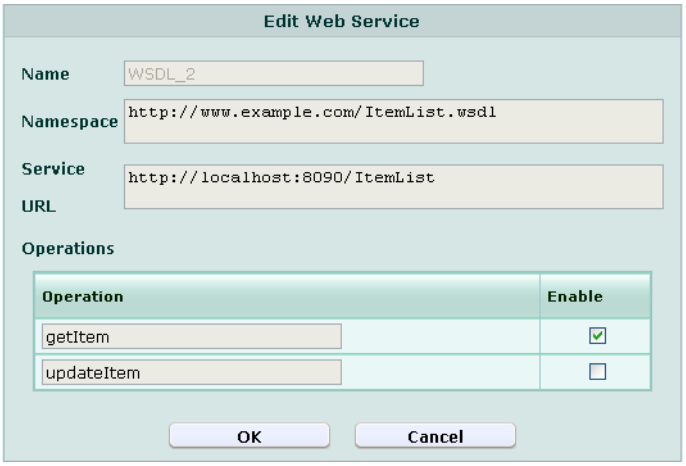
To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *XML Protection Configuration* category. For details, see "About permissions" on page 58.

**To enable or disable a web service action**

1 Go to *XML Protection* > *Load WSDL* > *Load WSDL*.

2 In the row corresponding to the WSDL file that contains the web service action that you want to enable or disable, click *Edit*.

A dialog appears that displays information about the Schema namespace URL, web service URL, and each web service operation that is defined in the WSDL file.




3 In each row corresponding to a web service operation that you want to ***enable***, in the *Enable* column, mark the check box.

4 In each row corresponding to a web service operation that you want to ***disable***, in the *Enable* column, clear the check box.

5 Click *OK*.

## Grouping WSDL files

*XML Protection* > *Load WSDL* > *XML Web Service Group* displays the list of groups of web service definition language (WSDL) files that have been uploaded to the FortiWeb unit.

WSDL file groups are used by the *WSDL Verify* option in XML protection profiles. For details, see "WSDL Verify" on page 147.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *XML Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 58:** *XML Web Service Group* **tab**


| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a WSDL file group. |
| # | The index number of the entry in the list. |

| | |
|---|---|
| **Name** | The name of the entry. |
| **Web Services** | The WSDL files that are members of the group. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a protection profile.<br>Click *Edit* to modify the entry. |

### To create a WSDL file group

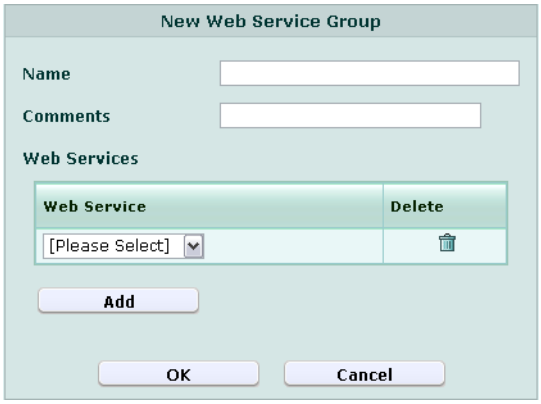
Before you can create a WSDL file group, you must first upload one or more WSDL files. For details, see "Managing WSDL files" on page 141.

**Note:** Alternatively, you can create a WSDL file group while configuring an XML protection profile. For more information, see "Configuring XML protection profiles" on page 144.

1 Go to *XML Protection* > *Load WSDL* > *XML Web Service Group*.

2 Click *Create New*.

A dialog appears that enables you to select WSDL files that will be members of the WSDL file group.




3 In *Name*, type the name of the WSDL file group.

4 In *Comments*, type a description for the WSDL file group.

5 In the *Web Services* area, click *Add*, then, from the *Web Service* drop-down list, select the name of a WSDL file that you want to be a member of this group.

6 Repeat the previous step for each additional member.

7 Click *OK*.

To use the WSDL file group to validate requests, you must enable the *WSDL Verify* option, then select the WSDL file group from the *Web Service* drop-down list in an XML protection profile that is used by a policy. For details, see "WSDL Verify" on page 147 and "Web Service" on page 147.

# Configuring XML protection profiles

*XML Protection* > *XML Protection Profile* > *XML Protection Profile* displays a list of XML protection profiles.

Protection profiles are a set of attack protection and other settings. When a connection matches a policy, the FortiWeb unit applies the protection profile that you have selected for that policy.

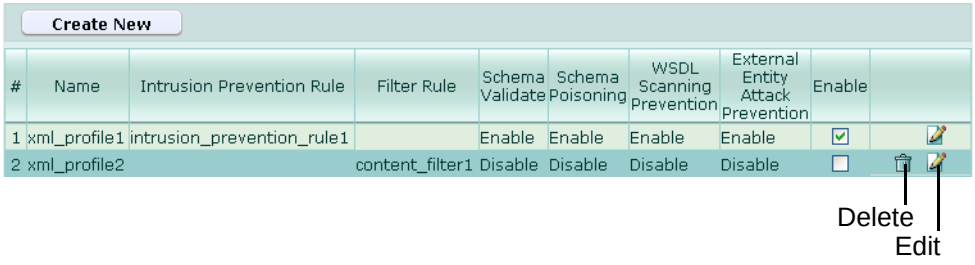
Protection profiles are applied by selecting them within a policy. For details, see "Configuring policies" on page 91.

**Note:** XML protection profiles can be configured at any time, but can be selected in a policy only while the FortiWeb unit is operating in a mode that supports them. For details, see Table 36, "Policy behavior by operation mode," on page 92.

SNMP traps can be used to notify you when an XML protection profile has been enforced. For details, see "Configuring an SNMP community" on page 48.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *XML Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 59:** *XML Protection Profile* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add an XML protection profile. |
| **#** | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Intrusion Prevention Rule** | The name of the intrusion prevention rule that is used by this XML protection profile. |
| **Filter Rule** | The name of the content filter rule that is used by this XML protection profile. |
| **Schema Validate** | Indicates whether or not Schema validation is enabled for traffic matching the policy.<br>If you have disabled the Schema file or have not uploaded it to the FortiWeb unit, results of Schema validation vary by whether you have also enabled *WSDL Verify*.<br>• If this option is enabled, *WSDL Verify* is enabled, and the Schema file does not exist or is disabled, the Schema validator will ***allow*** the connection.<br>• If this option is enabled, *WSDL Verify* is disabled, and the Schema file does not exist or is disabled, the Schema validator will ***block*** the connection. |
| **Schema Poisoning** | Indicates whether or not external Schema reference prevention is enabled, thereby preventing Schema poisoning attacks for traffic matching the policy. |
| **WSDL Scanning Prevention** | Indicates whether or not WSDL scanning prevention is enabled for traffic matching the policy. |
| **External Entity Attack Prevention** | Indicates whether or not external entity attack prevention is enabled for traffic matching the policy. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a server policy.<br>Click *Edit* to modify the entry. |

### To create an XML protection profile

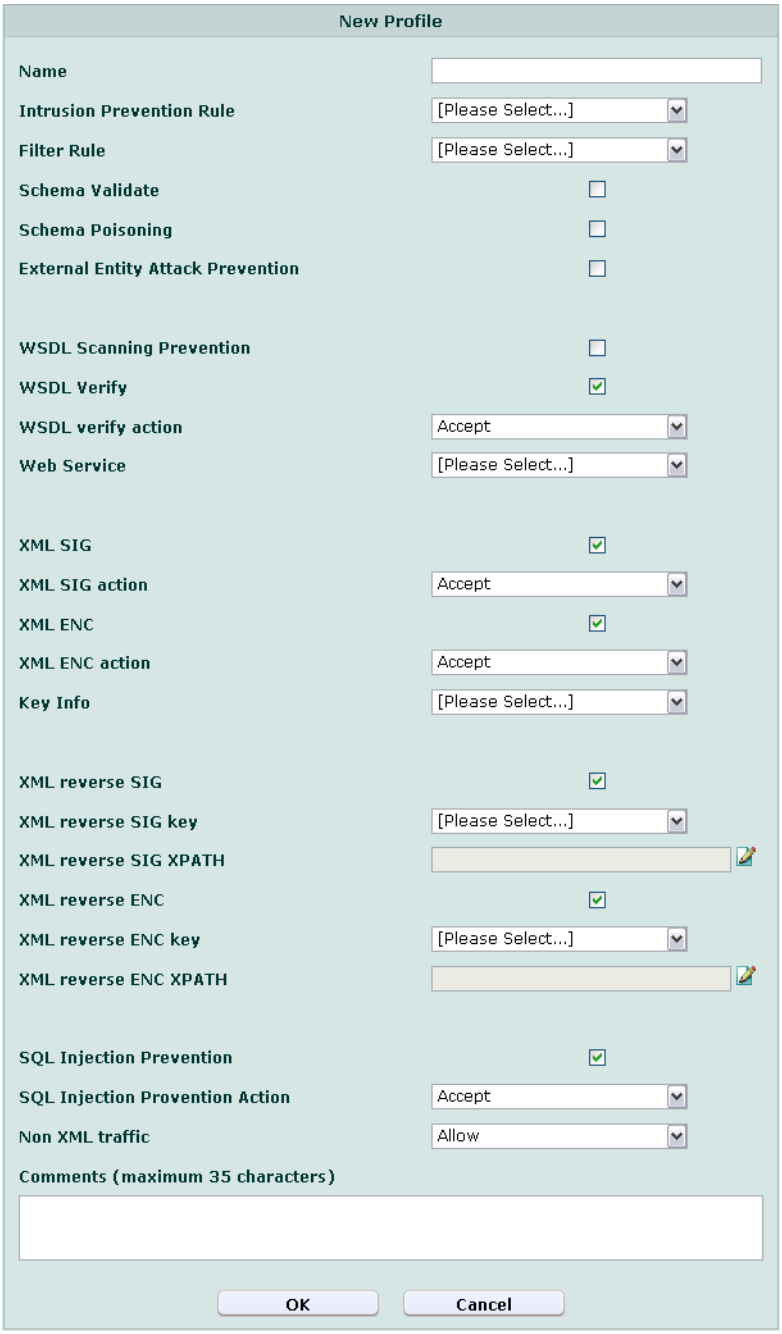
**Note:** Alternatively, you can create an XML protection profile while configuring a policy. For more information, see “Configuring policies” on page 91.

1 Go to *XML Protection* > *XML Protection Profile* > *XML Protection Profile*.

2 Click *Create New*.

A dialog appears that enables you to configure the XML protection profile.

3 Configure the following:



| *Name of the GUI item* | *Description* |
|---|---|
| **Name** | Enter the name of the XML protection profile. |
| **Intrusion Prevention Rule** | Select an intrusion prevention rule, or select *Create New* to create a new intrusion prevention rule in a pop-up window, without leaving the current page. For details, see "Configuring intrusion prevention rules" on page 130. |
| **Filter Rule** | Select a content filter rule, or select *Create New* to create a new content filter rule in a pop-up window, without leaving the current page. For details, see "Configuring content filter rules" on page 126. |
| **Schema Validate** | Enable to validate the Schema for traffic matching the policy.<br>This option may require that you first upload a Schema file to the FortiWeb unit, and enable it.<br>• If this option is enabled, *WSDL Verify* is enabled, and the Schema file does not exist or is disabled, the Schema validator will ***allow*** the connection.<br>• If this option is enabled, *WSDL Verify* is disabled, and the Schema file does not exist or is disabled, the Schema validator will ***block*** the connection.<br>For details on uploading a Schema file, see "Managing Schema files" on page 138. |
| **Schema Poisoning** | Enable to prevent external Schema references, and thereby preventing Schema poisoning attacks, for traffic matching the policy.<br>This option does not permit Schema referencing by URL for security reasons, and requires that you upload a Schema. For details, see "Managing Schema files" on page 138. |
| **External Entity Attack Prevention** | Enable to prevent external entity attacks for traffic matching the policy. |
| **WSDL Scanning Prevention** | Enable to prevent WSDL scanning for traffic matching the policy. |
| **WSDL Verify** | Enable to verify that, for traffic matching the policy, the connection uses web services operations that are valid for that web service according to the WSDL file.<br>This option requires that you first upload a WSDL file to the FortiWeb unit.<br>For details on uploading a WSDL file, see "Managing WSDL files" on page 141. |
| **WSDL verify action** | Select which action that the FortiWeb unit will take if the connection fails WSDL verification.<br>• **Accept**: Accept the connection.<br>• **Alert**: Accept the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>• **Deny**: Block the connection.<br>• **Alert & Deny**: Block the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>This option appears only if *WSDL Verify* is enabled. |
| **Web Service** | Select the WSDL file group to use for verification of the request, or select *Create New* to create a new WSDL file group in a pop-up window, without leaving the current page. For details, see "Grouping WSDL files" on page 143.<br>This option appears only if *WSDL Verify* is enabled. |
| **XML SIG** | Enable to validate XML signatures for forward traffic. Also configure *XML SIG action* and *Key Info*.<br>For the XML signature specification, see http://www.w3.org/TR/xmldsig-core/. |

| | |
|---|---|
| **XML SIG action** | Select the action that the FortiWeb unit will take if the forward traffic fails XML signature verification.<br>• **Accept**: Accept the connection.<br>• **Alert**: Accept the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>• **Deny**: Block the connection.<br>• **Alert & Deny**: Block the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>This option appears only if *XML SIG* is enabled. |
| **XML ENC** | Enable to decrypt XML for forward traffic. Also configure *XML ENC action* and *Key Info*.<br>For the XML encryption/decryption specification, see http://www.w3.org/TR/xmlenc-core/. |
| **XML ENC action** | Select which action the FortiWeb unit will take if the forward traffic fails XML decryption.<br>• **Accept**: Accept the connection.<br>• **Alert**: Accept the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>• **Deny**: Block the connection.<br>• **Alert & Deny**: Block the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>This option appears only if *XML ENC* is enabled. |
| **Key Info** | Select which key management group will be used for XML signature verification and/or decryption of forward traffic, or select *Create New* to upload a new key management group in a pop-up window, without leaving the current page. For details, see "Grouping keys into key management groups" on page 136.<br>This option appears only if *XML SIG* or *XML ENC* is enabled. |
| **XML reverse SIG** | Enable to sign reply traffic with XML signatures. Also configure *XML reverse SIG key* and *XML reverse SIG XPATH*.<br>For the XML signature specification, see http://www.w3.org/TR/xmldsig-core/. |
| **XML reverse SIG key** | Select which key management group will be used for XML signing of reply traffic, or select *Create New* to upload a new key management group in a pop-up window, without leaving the current page. For details, see "Grouping keys into key management groups" on page 136.<br>This option appears only if *XML reverse SIG* is enabled. |
| **XML reverse SIG XPATH** | Click the *Edit* icon and enter an XPath expression that matches XML elements in reply traffic to which you want to apply XML signatures.<br>This option appears only if *XML reverse SIG* is enabled. |
| **XML reverse ENC** | Enable to encrypt XML reply traffic. Also configure *XML reverse ENC key* and *XML reverse ENC XPATH*.<br>For the XML encryption/decryption specification, see http://www.w3.org/TR/xmlenc-core/. |
| **XML reverse ENC key** | Select which key management group will be used for XML encryption of reply traffic, or select *Create New* to upload a new key management group in a pop-up window, without leaving the current page. For details, see "Grouping keys into key management groups" on page 136.<br>This option appears only if *XML reverse ENC* is enabled. |
| **XML reverse ENC XPATH** | Click the *Edit* icon and enter an XPath expression that matches XML elements in reply traffic to which you want to apply XML encryption.<br>This option appears only if *XML reverse ENC* is enabled. |
| **SQL Injection Prevention** | Enable to prevent SQL injection attacks by blocking requests that contain SQL statements. |

| | |
|---|---|
| **SQL Injection Prevention Action** | Select which action the FortiWeb unit will take if the connection contains SQL statements.<br>• **Accept**: Accept the connection.<br>• **Alert**: Accept the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>• **Deny**: Block the connection.<br>• **Alert & Deny**: Block the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>This option appears only if *SQL Injection Prevention* is enabled. |
| **Non XML traffic** | Enable to accept HTTP requests that do ***not*** contain `Content-Type: text/xml` in the HTTP header. This may be required if the web service uses representational state transfer (REST) instead of SOAP.<br>Disable to reject non-XML HTTP requests. |
| **Comments** | Enter a description for the XML protection profile. |

**4** Click *OK*.

To apply an XML protection profile, you must select it in a policy. For details, see "Configuring policies" on page 91.

# Web Protection

This section describes the *Web Protection* menu, which contains features that act upon HTTP requests, HTTP headers, HTML documents, and cookies.

This section includes the following topics:



## Order of execution

FortiWeb units perform each of the web protection profile scans and other actions in the following sequence, from the top of the table towards the bottom. Disabled scans are skipped.

**Note:** Blocking style varies by feature and configuration. For example, when detecting cookie poisoning, instead of resetting the HTTP connection, you could log and remove the offending cookie. For details, see each specific feature.

**Table 60: Execution sequence of web protection techniques**

| Scan/action | Involves |
|---|---|
| ***Request from client to server*** | |
| *IP* (client IP black list) | Source IP address of the client |
| *Brute Force Login* | Source IP address of the client and URL in the HTTP header |

**Table 60: Execution sequence of web protection techniques**

| | |
|---|---|
| *Standalone IP Access Limit* / *Share IP Access Limit* (malicious robot/client rate limiting) | Source IP address of the client |
| *HTTP Authentication Policy* | `Authorization:` |
| *HTTP Protocol Constraints* | `Content-Length:`, parameter length, body length, header length, and header line length |
| *Host* (protected real or virtual host) | `Host:` |
| *Cookie Poison* | `Cookie:` |
| *Start Pages* | `Host:`, URL in HTTP header, and session state |
| *Page Access Rule* | `Host:`, URL in HTTP header, and session state |
| *White List Rule* | `Host:`, URL in HTTP header |
| *Black List Rule* | `Host:`, URL in HTTP header |
| *Allow Method Exceptions* | `Host:`, URL in HTTP header, and method in HTTP header |
| *Allow Request Method* | Method in HTTP header |
| *Allow Custom Robot* | `User-Agent:` |
| *Allow Robot* | `User-Agent:` |
| *Parameter Validation Rule* | `Host:`, URL in the HTTP header, and visible inputs' name, data type, and length |
| *Hidden Fields Protection Rule* | `Host:`, URL in the HTTP header, and invisible inputs' name, data type, and length |
| *XSS*, *SQL Injection*, *Common Exploits* | Inputs |
| *Bad Robot* | `User-Agent:` |
| *URL* (URL rewriting) | `Host:` and URL in HTTP header |
| ***Reply from server to client*** | |
| *Information Disclosure* | Server-identifying custom HTTP headers and error messages such as `Server:` |
| *Credit Card Detection* | Credit card number in the body, and, if configured, *Credit Card Detection Threshold* |

# Configuring input rules

*Web Protection* > *Parameter Validation Rules* > *Input Rules* displays the list of input rules.

Input rules define whether or not parameters are required, and their maximum allowed length, for HTTP requests matching the `Host:` and URL defined in the input rule.

Unlike hidden field groups, input rules are for visible inputs only. For information on constraining ***hidden*** inputs, see "Configuring hidden field rules" on page 194.

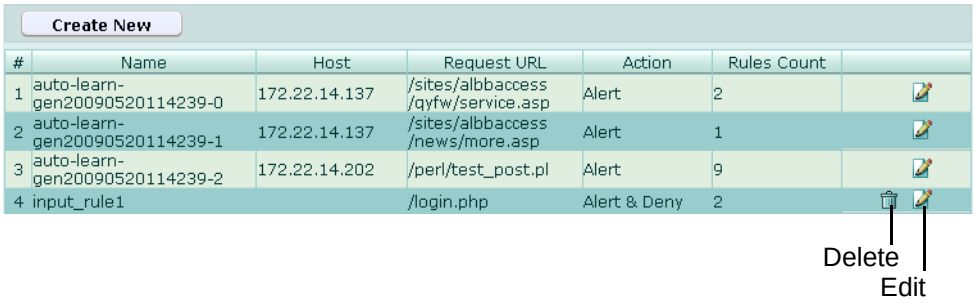
Each input rule contains one or more individual rules. This enables you to define, within one input rule, all parameter restrictions that apply to HTTP requests matching that URL and host name.

For example, one web page might have multiple inputs: a user name, password, and a preference for whether or not to remember the login. Within the input rule for that web page, you could define separate rules for each parameter in the HTTP request: one rule for the user name parameter, one rule for the password parameter, and one rule for the preference parameter.

Input rules are applied by selecting them within a parameter validation rule. For details, see "Grouping input rules into parameter validation rules" on page 156.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 61:** *Input Rules* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add an input rule. |
| # | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Host** | The IP address or fully qualified domain name (FQDN) of the real or virtual host as it appears in the `Host:` field of HTTP header of requests to which the entry applies. |
| **Request URL** | The URL, such as `/index.php`, as it appears in the HTTP request to which the entry applies. |
| **Action** | The action that the FortiWeb unit will take when an HTTP request violates one of the input rules in the entry.<br>• **Alert**: Accept the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>• **Alert & Deny**: Block the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>• **Redirect**: Redirect the request to the URL that you specify in the protection profile and generate an alert and/or log message. For details, see "Configuring logging and alerts" on page 252 and "Redirect URL" on page 219.<br>• **Send 403 Forbidden**: Reply with an HTTP 403 (Access Forbidden) error message and generate an alert and/or log message. For details, see "Configuring logging and alerts" on page 252. |
| **Rules Count** | The number of individual rules contained in the entry. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a parameter validation rule.<br>Click *Edit* to modify the entry. |

### To configure an input rule

Before you configure an input rule, if you want to apply it only to HTTP requests for a specific real or virtual host, you must first define the web host in a protected hosts group. For details, see "Configuring protected hosts" on page 113.

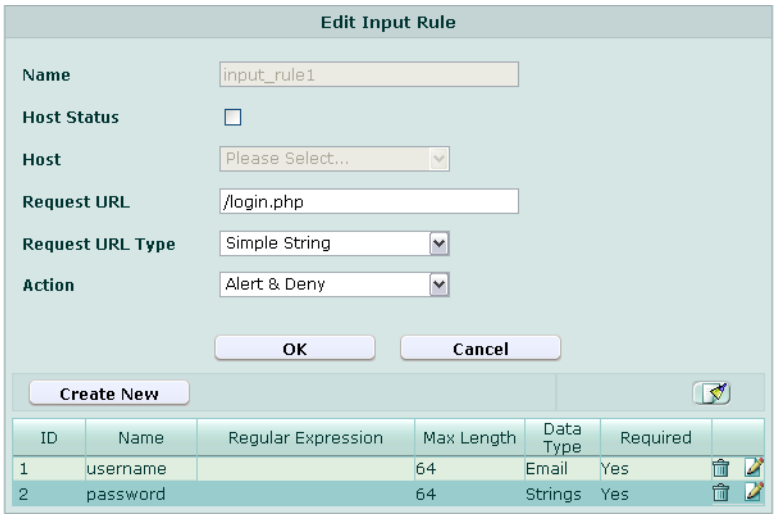
1 Go to *Web Protection* > *Parameter Validation Rules* > *Input Rules*.

2 Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.

3 In *Name*, type the name of the input rule.

This field cannot be modified if you are editing an existing input rule. To modify the name, delete the entry, then recreate it using the new name.

4 Configure the following:

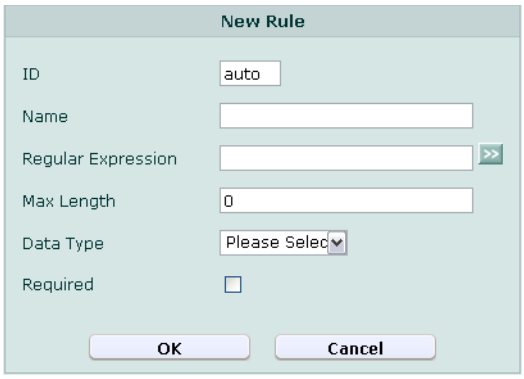



| *Name of the GUI item* | *Description* |
|---|---|
| **Host Status** | Enable to apply this input rule only to HTTP requests for specific web hosts. Also configure *Host*.<br>Disable to match the input rule based upon the other criteria, such as the URL, but regardless of the `Host:` field. |
| **Host** | Select the IP address or fully qualified domain name (FQDN) of a protected host. |
| **Request URL** | Depending on your selection in *Request URL Type*, type either:<br>• the literal URL, such as `/index.php`, that the HTTP request must contain in order to match the input rule. The URL must begin with a slash ( / ).<br>• a regular expression, such as `^/*.php`, matching all and only the URLs to which the input rule should apply. The pattern is ***not*** required to begin with a slash ( / ). However, it must at least match URLs that begin with a slash, such as `/index.cfm`.<br>Do not include the name of the web host, such as `www.example.com`, which is configured separately in the *Host* drop-down list. |

| | |
|---|---|
| **Request URL Type** | Select whether the *Request URL* field will contain a literal URL (*Simple String*), or a regular expression designed to match multiple URLs (*Regular Expression*). |
| **Action** | Select which action the FortiWeb unit will take when an HTTP request violates one of the input rules in the entry:<br>• **Alert**: Accept the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>• **Alert & Deny**: Block the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>• **Redirect**: Redirect the request to the URL that you specify in the protection profile and generate an alert and/or log message. For details, see "Configuring logging and alerts" on page 252 and "Redirect URL" on page 219.<br>• **Send 403 Forbidden**: Reply with an HTTP 403 (Access Forbidden) error message and generate an alert and/or log message. For details, see "Configuring logging and alerts" on page 252.<br>**Note:** If a *WAF Auto Learning Profile* will be selected in the policy with profiles that use this rule, you should select *Alert*. If the *Action* is *Alert & Deny*, the FortiWeb unit will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. |

5 Click *OK*.

6 Click *Create New*, then configure the following:

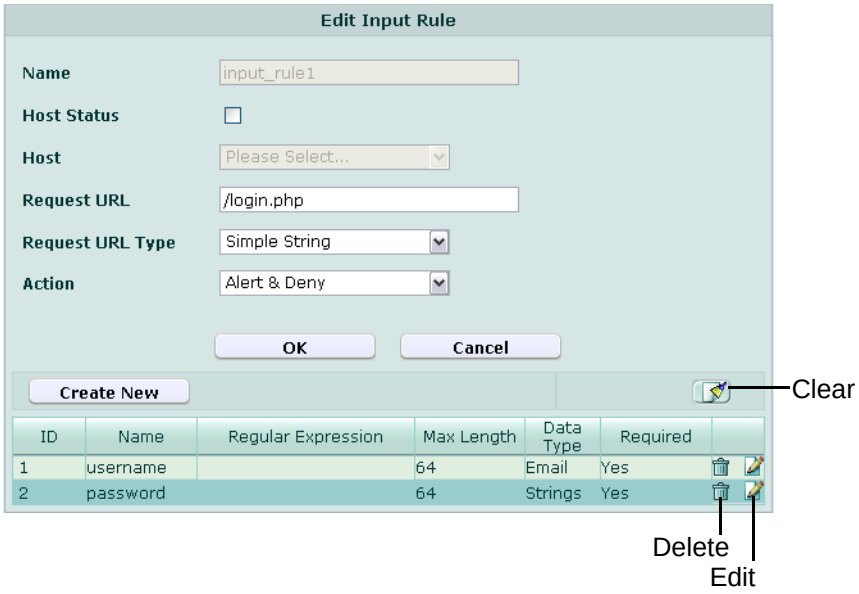



| *Name of the GUI item* | *Description* |
|---|---|
| **ID** | Enter the index number of the individual rule within the group of input rules, or keep the field's default value of `auto` to let the FortiWeb unit automatically assign the next available index number. |
| **Name** | Type the name of the input as it appears in the HTTP content, such as `username`. |
| **Regular Expression** | Type a regular expression that matches all valid values, and no invalid values, for this input.<br>When you have finished typing the regular expression, click the >> button. A pop-up window will appear that enables you to validate the expression and verify that it matches the parameters. When you have finished testing the expression, click *OK* to return to configuring the input rule.<br>Alternatively, configure *Data Type*. |
| **Max Length** | Type the maximum allowed length of the parameter value.<br>To disable the length limit, type `0`. |

| | |
|---|---|
| **Data Type** | Select one of the predefined data types, if the input matches one of them. For information on data types, see "Viewing the list of predefined data types" on page 118.<br>Alternatively, configure *Regular Expression*.<br>**Note:** This option will be ignored if you configure *Regular Expression*, which also defines parameters to which the input rule applies, but supersedes *Data Type*. |
| **Required** | Enable if the parameter is required for HTTP requests to this combination of `Host:` field and URL. |

7 Repeat the previous step for each individual rule that you want to add to the group of input rules.

8 If you need to modify an individual rule, click its *Edit* icon. To remove an individual rule from the group of input rules, click its *Delete* icon. To remove all individual rules from the group of input rules, click the *Clear* icon.




9 Click *OK*.

To apply the input rule, select it in a parameter validation rule. For details, see "Grouping input rules into parameter validation rules" on page 156.

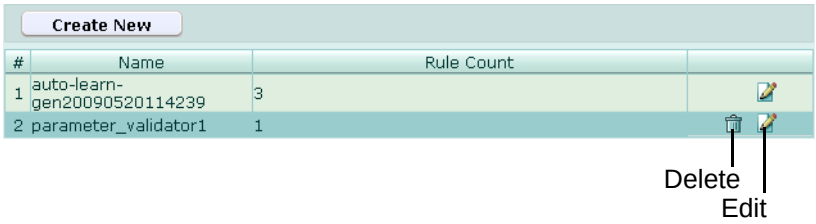
## Grouping input rules into parameter validation rules

*Web Protection* > *Parameter Validation Rules* > *Parameter Validation Rules* displays the list of parameter validation rules, each of which is a group of input rules entries.

Parameter validation rules are applied by selecting them within an inline or offline protection profile. For details, see "Configuring inline web protection profiles" on page 213 or "Configuring offline protection profiles" on page 219.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 62:** *Parameter Validation Rules* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a parameter validation rule. |
| # | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Rule Count** | The number of individual rules contained in the entry. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in an inline or offline protection profile.<br>Click *Edit* to modify the entry. |

### To configure a parameter validation rule

Before you can configure parameter validation rules, you must first configure one or more input rules. For details, see "Configuring input rules" on page 152.

1 Go to *Web Protection* > *Parameter Validation Rules* > *Parameter Validation Rules*.

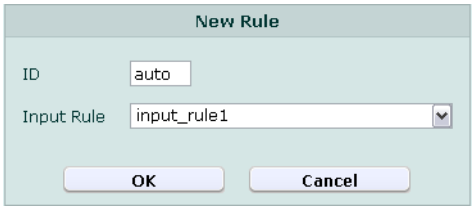
2 Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.

3 In *Name*, type the name of the parameter validation rule.

This field cannot be modified if you are editing an existing parameter validation rule. To modify the name, delete the entry, then recreate it using the new name.

4 Click *OK*.

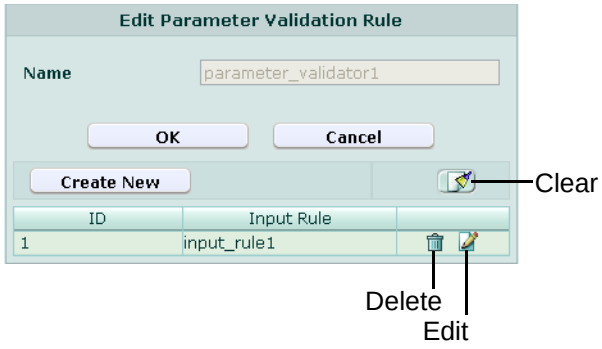
5 Click *Create New*, then configure the following:




| *Name of the GUI item* | *Description* |
|---|---|
| **ID** | Enter the index number of the input rule within the parameter validation rule, or keep the field's default value of `auto` to let the FortiWeb unit automatically assign the next available index number. |
| **Input Rule** | Select the name of an input rule. For information on input rules, see "Configuring input rules" on page 152. |

6 Repeat the previous step for each input rule that you want to add to the parameter validation rule.

7 If you need to modify an input rule, click its *Edit* icon. To remove a single input rule from the parameter validation rule, click its *Delete* icon. To remove all input rules from the parameter validation rule, click the *Clear* icon.




8 Click *OK*.

To apply the parameter validation rule, select it in an inline or offline protection profile. For details, see "Configuring inline web protection profiles" on page 213 or "Configuring offline protection profiles" on page 219.

Attack log messages and *Alert Message Console* messages contain `DETECT_PARAM_RULE_FAILED` when this feature detects a parameter rule violation.

**Tip:** If you do not want sensitive inputs such as passwords to appear in the attack logs' packet payloads, you can obscure them. For details, see "Obscuring sensitive data in the logs" on page 255.

# Configuring page order rules

*Web Protection* > *Page Access Rules* > *Page Access Rules* displays the list of page access rules.

Page access rules define URLs that must be accessed only in a ***specific order***, such as to enforce the business logic of a web application. Requests for other, non-ordered URLs may interleave ordered URLs during the client's session. Page access rules may be specific to a web host.

For example, an e-commerce application might be designed to work properly in this order:

1 A client begins a session by adding an item to a shopping cart. (`/addToCart.do?*`)

2 The client either views and adds additional items to the shopping cart, or proceeds directly to the checkout.

3 The client confirms the items that he or she wants to purchase. (`/checkout.do`)

4 The client provides shipping information. (`/shipment.do`)

5 The client pays for the items and shipment, completing the transaction. (`/payment.do`)

Sessions that begin at the shipping or payment stage should therefore be invalid. If the web application does not enforce this rule itself, it could be open to cross-site request forgery (CSRF) attacks on the payment feature. To prevent such abuse, the FortiWeb unit could enforce the rule itself using a page access rule set with the following order:

1 `/addToCart.do?item=*`

2 `/checkout.do?login=*`

3 `/shipment.do`

**4** `/payment.do`

Attempts to request `/payment.do` before those other URLs during a session would be denied, and generate an alert and/or attack log message (see “Configuring logging and alerts” on page 252).

Page access rules are applied by selecting them within an inline protection profile. For details, see “Configuring inline web protection profiles” on page 213.

SNMP traps can be used to notify you when a page access rule has been enforced. For details, see “Configuring an SNMP community” on page 48.

To be able to access this part of the web-based manager, in your administrator account’s access profile, you must have both *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see “About permissions” on page 58.

**Table 63:** *Page Access Rules* **tab**


| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a page access rule. |
| # | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Rules Count** | The number of individual rules contained in the entry. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in an inline protection profile.<br>Click *Edit* to modify the entry. |

### To configure a page access rule

Before you configure a page access rule, if you want to apply it only to HTTP requests for a specific real or virtual host, you must first define the web host in a protected hosts group. For details, see “Configuring protected hosts” on page 113.

**1** Go to *Web Protection* > *Page Access Rules* > *Page Access Rules*.

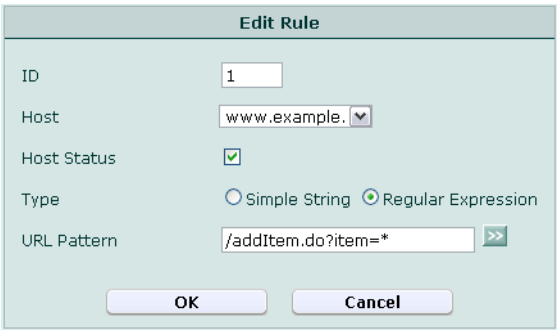
**2** Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.

**3** In *Name*, type the name of the page access rule.

This field cannot be modified if you are editing an existing page access rule. To modify the name, delete the entry, then recreate it using the new name.

**4** Click *OK*.

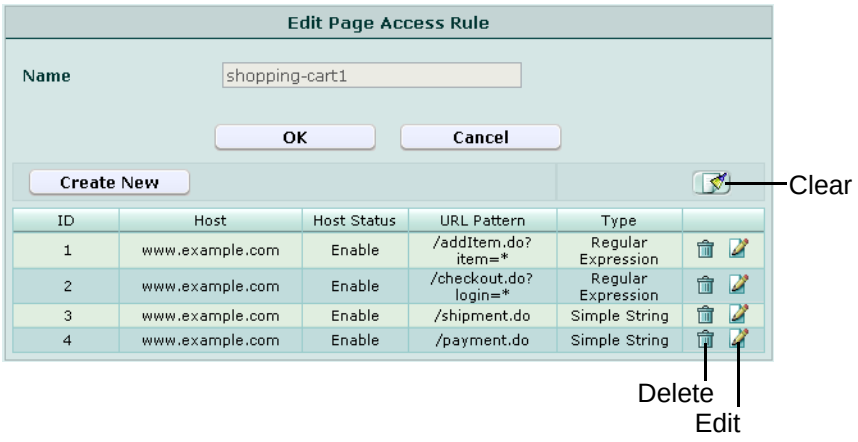
5 Click *Create New*, then configure the following:




| *Name of the GUI item* | *Description* |
|---|---|
| **ID** | Type the index number of the individual rule within the page access rule, or keep the field's default value of `auto` to let the FortiWeb unit automatically assign the next available index number.<br>Page access rules should be added to the set in the order which clients will be permitted to access them.<br>For example, if a client must access `/login.asp` before `/account.asp`, add the rule for `/login.asp` first. |
| **Host** | Select the name of a protected host that the `Host:` field of an HTTP request must be in order to match the page access rule.<br>This option is available only if *Host Status* is enabled. |
| **Host Status** | Enable if you want the page access rule to apply only to HTTP requests for a specific web host. Also configure *Host*. |
| **URL Pattern** | Depending on your selection in *Type*, type either:<br>• the literal URL, such as `/cart.php`, that the HTTP request must contain in order to match the page access rule. The URL must begin with a slash ( / ).<br>• a regular expression, such as `^/*.php`, matching all and only the URLs to which the page access rule should apply. The pattern is ***not*** required to begin with a slash ( / ). However, it must at least match URLs that begin with a slash, such as `/cart.cfm`.<br>Do not include the name of the web host, such as `www.example.com`, which is configured separately in the *Host* drop-down list. |
| **Type** | Select whether *URL Pattern* is a *Simple String* (that is, a literal URL) or a *Regular Expression*. |

6 Repeat the previous step for each individual rule that you want to add to the page access rule.

7 If you need to modify an individual rule, click its *Edit* icon. To remove an individual rule from the page access rule, click its *Delete* icon. To remove all individual rules from the page access rule, click the *Clear* icon.




8 Click *OK*.

To apply the page access rule, select it in an inline protection profile. For details, see "Configuring inline web protection profiles" on page 213.

**Note:** In order for page access rules to be enforced, you must also enable "Session Management" on page 216 in the inline protection profile.

Attack log messages and *Alert Message Console* messages contain `DETECT_PAGE_RULE_FAILED` when this feature detects a request for a URL that violates the required sequence of URLs within a session.

# Configuring server protection rules

*Web Protection* > *Server Protection Rules* > *Server Protection Rules* displays the list of server protection rules.

Server protection rules enable and configure actions for several security features specifically designed to protect web servers, such as:

- cross-site scripting (XSS) attack prevention
- SQL injection prevention
- sensitive information disclosure prevention
- prevention of other injection attacks
- prevention of credit card data leaks

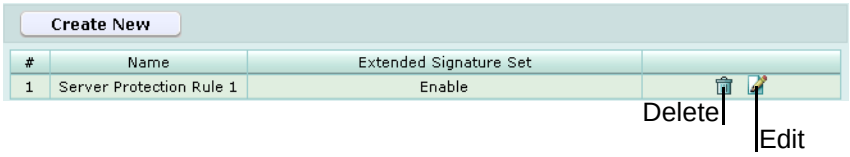
In addition to scanning standard requests, server protection rules can also scan action message format 3.0 (AMF3) binary inputs used by Adobe Flash clients to communicate with server-side software. For more information, see "Enable AMF3 Protocol Detection" on page 219 (for inline protection profiles) or "Enable AMF3 Protocol Detection" on page 223 (for offline protection profiles).

Attack definitions can be updated. For information on uploading a new set of attack definitions, see "Uploading signature updates" on page 77.

Server protection rules are applied by selecting them within an inline or offline protection profile. For details, see “Configuring inline web protection profiles” on page 213 or “Configuring offline protection profiles” on page 219.

To be able to access this part of the web-based manager, in your administrator account’s access profile, you must have both *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see “About permissions” on page 58.

**Table 64:** *Server Protection Rules* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a server protection rule. |
| # | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Extended Signature Set** | Indicates whether or not an extended set of attack definitions will be used. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in an inline or offline protection profile.<br>Click *Edit* to modify the entry. |

### To configure a server protection rule

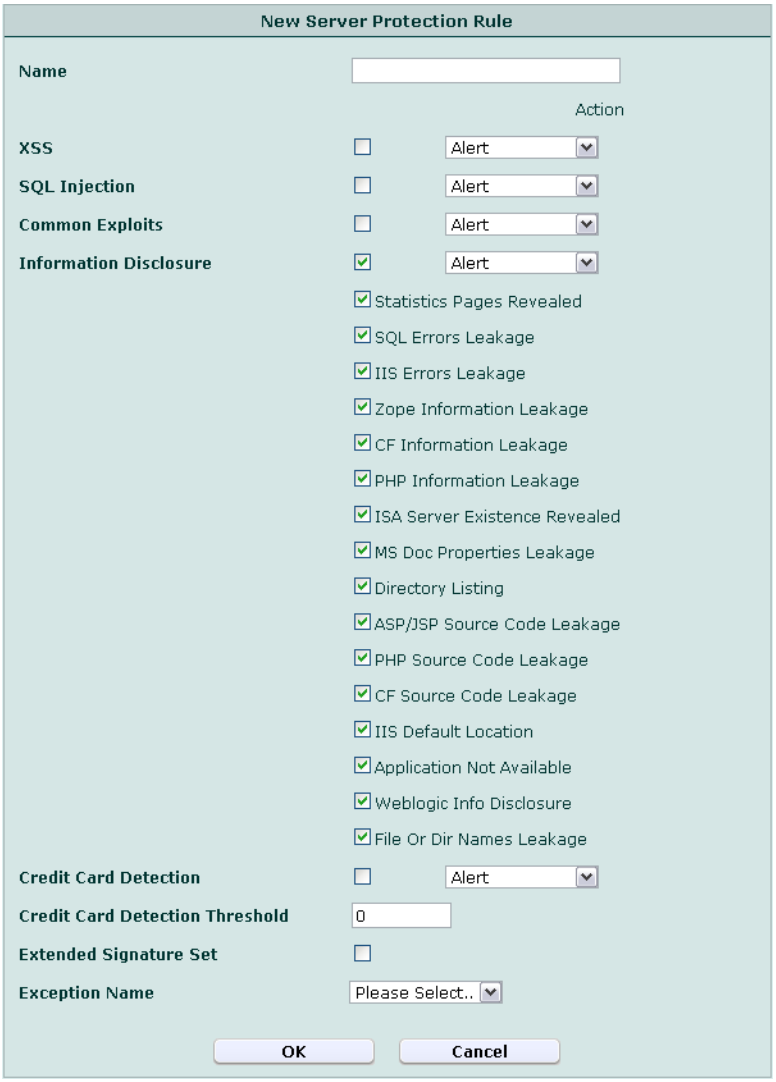
**Tip:** Alternatively, you can automatically configure a server protection rule that detects all attack types by generating a default auto-learning profile. For details, see “Generating an auto-learning profile and its components” on page 227.

Before you configure a server protection rule, if you want to apply any exceptions, you must first define the server protection exception. For details, see “Configuring server protection exceptions” on page 167.

1 Go to *Web Protection* > *Server Protection Rules* > *Server Protection Rules*.

2 Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.

**3** Configure the following:




| *Name of the GUI item* | *Description* |
|---|---|
| **Name** | Type the name of the server protection rule. This field cannot be modified if you are editing an existing server protection rule. To modify the name, delete the entry, then recreate it using the new name. |

**XSS**

Enable to prevent cross-site scripting (XSS) attacks, then select which action the FortiWeb unit will take when an HTTP request attempts to make an XSS attack.

- **Alert**: Accept the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.
- **Alert & Deny**: Block the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.
- **Redirect**: Redirect the request to the URL that you specify in the protection profile and generate an alert and/or log message. For details, see "Configuring logging and alerts" on page 252 and "Redirect URL" on page 219.
- **Send 403 Forbidden**: Reply with an HTTP 403 (Access Forbidden) error message and generate an alert and/or log message. For details, see "Configuring logging and alerts" on page 252.

Once enabled, you can enable or disable detection of individual sub-types of this type of attack, such as enabling the signature for common XSS but disabling the signature for CSRF (cross-site request forgery).

Attack log messages and *Alert Message Console* messages contain `DETECT_XSS_ATTACK` when this feature detects a possible cross-site scripting attack.

**Note:** If a *WAF Auto Learning Profile* will be selected in the policy with profiles that use this rule, you should select *Alert*. If the *Action* is *Alert & Deny*, the FortiWeb unit will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature.

**SQL Injection**

Enable to prevent SQL injection attacks, then select which action the FortiWeb unit will take when an HTTP request attempts to make a SQL injection attack.

- **Alert**: Accept the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.
- **Alert & Deny**: Block the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.
- **Redirect**: Redirect the request to the URL that you specify in the protection profile and generate an alert and/or log message. For details, see "Configuring logging and alerts" on page 252 and "Redirect URL" on page 219.
- **Send 403 Forbidden**: Reply with an HTTP 403 (Access Forbidden) error message and generate an alert and/or log message. For details, see "Configuring logging and alerts" on page 252.

Once enabled, you can enable or disable detection of individual sub-types of this type of attack, such as enabling the signature for common SQL injection but disabling the signature for blind SQL injection.

Attack log messages and *Alert Message Console* messages contain `DETECT_SQL_INJECTION` when this feature detects a possible SQL injection attack.

**Note:** If a *WAF Auto Learning Profile* will be selected in the policy with profiles that use this rule, you should select *Alert*. If the *Action* is *Alert & Deny*, the FortiWeb unit will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature.

**Common Exploits**

Enable to prevent common exploits, then select which action that the FortiWeb unit will take when an HTTP request attempts to make an injection attack in a language other than SQL.

- **Alert**: Accept the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.
- **Alert & Deny**: Block the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.
- **Redirect**: Redirect the request to the URL that you specify in the protection profile and generate an alert and/or log message. For details, see "Configuring logging and alerts" on page 252 and "Redirect URL" on page 219.
- **Send 403 Forbidden**: Reply with an HTTP 403 (Access Forbidden) error message and generate an alert and/or log message. For details, see "Configuring logging and alerts" on page 252.

Once enabled, you can enable or disable detection of individual sub-types of this type of attack, such as enabling *Command Injection* (ability to issue operating system commands) but disabling *SRC Disclosure* (disclosure of web page source code).

Attack log messages and *Alert Message Console* messages contain `Common Exploits` and the subtype (e.g. `Common Exploits: Command Injection`) when this feature detects a possible common exploit attack.

**Note:** If a *WAF Auto Learning Profile* will be selected in the policy with profiles that use this rule, you should select *Alert*. If the *Action* is *Alert & Deny*, the FortiWeb unit will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature.

**Information Disclosure**

Enable to detect server errors and other sensitive messages in the requested document and HTTP headers, then select which action the FortiWeb unit will take when it detects sensitive information.

- **Alert**: Do not cloak, except for removing sensitive headers. (Sensitive information in the body remains unaltered.) Accept the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.
- **Alert & Erase**: Hide replies with sensitive information (sometimes called "cloaking"). Block the connection or remove the sensitive information, and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.
  **Note:** This option is not fully supported in offline protection mode. Only an alert and/or log message can be generated; sensitive information will not be blocked or erased.
- **Redirect**: Redirect the request to the URL that you specify in the protection profile and generate an alert and/or log message. For details, see "Configuring logging and alerts" on page 252 and "Redirect URL" on page 219.

Once enabled, you can enable or disable detection of individual sub-types of this type of attack, such as enabling *CF Information Leakage* (Adobe ColdFusion server information) but disabling *Weblogic Info Disclosure* (Oracle WebLogic server information).

Error messages, HTTP headers such as `Server: Microsoft-IIS/6.0`, and other messages could inform attackers of the vendor, product, and version numbers of software running on your web servers, thereby advertising their specific vulnerabilities.

Sensitive information is predefined according to fixed signatures.

Attack log messages and *Alert Message Console* messages contain `DETECT_RESPONSE_INFORMATION_DISCLOSURE` when this feature detects sensitive information.

**Note:** Because this feature can potentially require the FortiWeb unit to rewrite the header and body of ***every*** request from a server, it can result in a performance decrease. To minimize impact, Fortinet recommends enabling this feature ***only*** to help you identify information disclosure through logging, and ***until*** you can reconfigure the server to omit such sensitive information.

**Note:** If a *WAF Auto Learning Profile* will be selected in the policy with profiles that use this rule, you should select *Alert*. If the *Action* is *Alert & Deny*, the FortiWeb unit may reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature.

| | |
|---|---|
| **Credit Card Detection** | Enable to detect credit card numbers in the response from the server, then select which action the FortiWeb unit will take when it detects credit card number disclosure:<br>• **Alert**: Accept the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>• **Alert & Deny**: Block the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>Also configure *Credit Card Detection Threshold*.<br>Credit card numbers being sent from the server to the client could constitute a violation of PCI DSS. In most cases, the client should only receive mostly-obscured versions of their credit card number, if they require it to confirm which card was used. This prevents bystanders from viewing the number, but also reduces the number of times that the actual credit card number could be observed by network attackers. For example, a web page might confirm a transaction by displaying a credit card number as:<br>`XXXX XXXX XXXX 1234`<br>This mostly-obscured version protects the credit card number from unnecessary exposure and disclosure. It would ***not*** trigger the credit card number detection feature.<br>However, if a web application does not obscure displays of credit card numbers, or if an attacker has found a way to bypass the application's protection mechanisms and gain a list of customers' credit card numbers, a web page might contain a list with many credit card numbers in clear text. Such a web page would be considered a data leak, and trigger credit card number disclosure detection.<br>Attack log messages and *Alert Message Console* messages contain `DETECT_RESPONSE_INFORMATION_disclosure: credit card leakage` when this feature detects credit card number disclosure.<br>**Note:** If a *WAF Auto Learning Profile* will be selected in the policy with profiles that use this rule, you should select *Alert*. If the *Action* is *Alert & Deny*, the FortiWeb unit may reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. |
| **Credit Card Detection Threshold** | Enter 0 to report ***any*** credit card number disclosures, or enter a threshold if the web page must contain a number of credit cards that equals or exceeds the threshold in order to trigger the credit card number detection feature.<br>For example, to ignore web pages with only one credit card number, but to detect when a web page containing two or more credit cards, enter 2. |
| **Extended Signature Set** | Enable if you want to use an additional set of attack definitions. While this option can detect more attacks, if might also cause false positives. |
| **Exception Name** | Select which server protection exception to use, if any. |

4 Click *OK*.

To apply the server protection rule, select it in an inline protection profile or an offline protection profile. For details, see "Configuring inline web protection profiles" on page 213 or "Configuring offline protection profiles" on page 219.

## Configuring server protection exceptions

*Web Protection* > *Server Protection Rules* > *Server Protection Exception* displays the list of server protection exceptions.

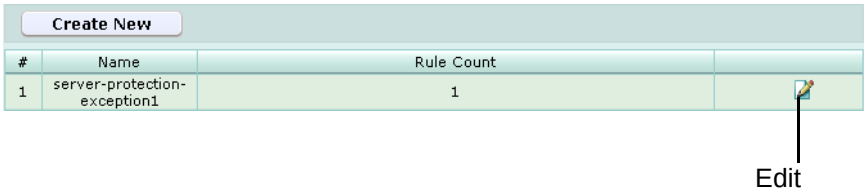
Exceptions may be useful if you know that some URLs, during normal use, will cause false positives by matching an attack signature. Server protection exceptions define request URLs that will ***not*** be subject to server protection rules.

For example, if the HTTP POST URL `/pageupload` should accept input that is PHP code, but it is the only URL on the host that should do so, you would create an exception with *PHP Injection*, then use that exception in the server protection rule that normally would block all injection attacks.

Server protection exceptions are applied by selecting them within a server protection rule. For details, see "Configuring server protection rules" on page 161.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 65:** *Server Protection Exception* **tab**



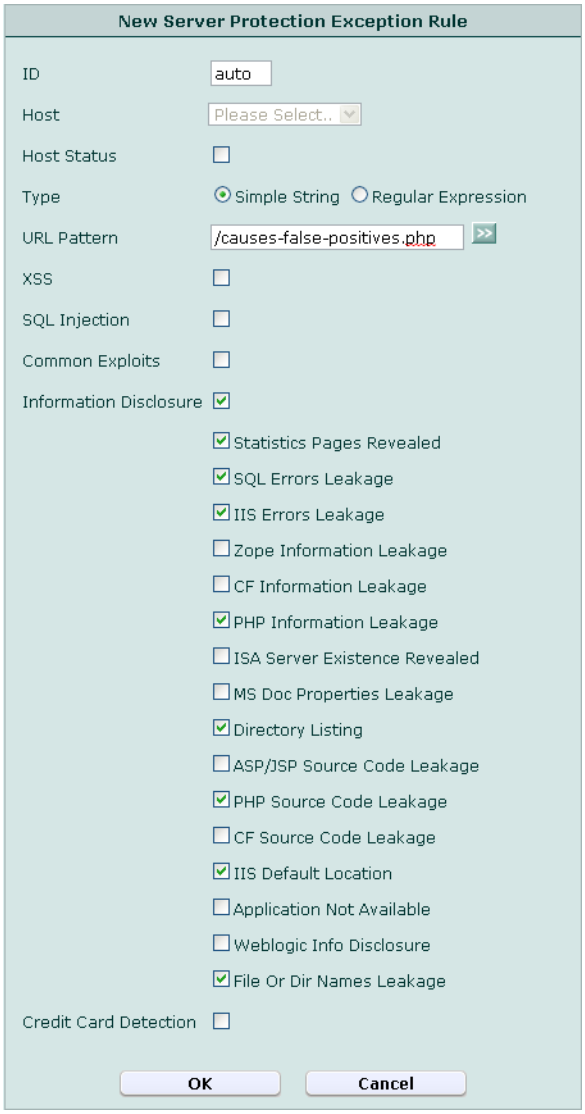

| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a server protection exception. |
| # | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Rule Count** | The number of individual exceptions contained in the entry. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a server protection rule.<br>Click *Edit* to modify the entry. |

### To configure a server protection exception

1. Go to *Web Protection* > *Server Protection Rules* > *Server Protection Exception*.
2. Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.
3. In *Name*, type the name of the server protection exception.

   This field cannot be modified if you are editing an existing server protection exception. To modify the name, delete the entry, then recreate it using the new name.
4. Click *OK*.

**5** Configure the following:

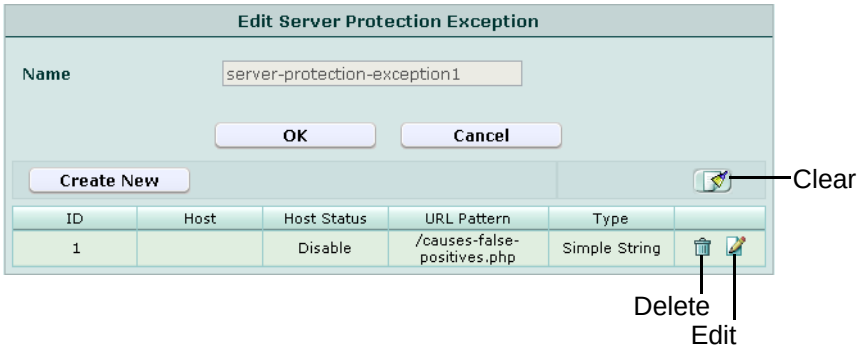



| *Name of the GUI item* | *Description* |
|---|---|
| **ID** | Enter the index number of the individual entry within the server protection exception, or keep the field's default value of `auto` to let the FortiWeb unit automatically assign the next available index number. |
| **Host** | Select which protected hosts entry (either a web host name or IP address) that the `Host:` field of the HTTP request must be in order to match the server protection exception.<br>This option is available only if *Host Status* is enabled. |
| **Host Status** | Enable to require that the `Host:` field of the HTTP request match a protected hosts entry in order to match the server protection exception. Also configure *Host*. |
| **Type** | Select whether *URL Pattern* is a *Simple String* (that is, a literal URL) or a *Regular Expression*. |

| | |
|---|---|
| **URL Pattern** | Depending on your selection in *Type*, type either:<br>• the literal URL, such as `/causes-false-positives.php`, that the HTTP request must contain in order to match the server protection exception. The URL must begin with a slash ( / ).<br>• a regular expression, such as `^/.*.php`, matching all and only the URLs to which the server protection exception should apply. The pattern is ***not*** required to begin with a slash ( / ). However, it must at least match URLs that begin with a slash, such as `/bbcode.cfm`.<br>Do not include the name of the web host, such as `www.example.com`, which is configured separately in the *Host* drop-down list. |
| **XSS** | Enable to omit detection of cross-site scripting (XSS) attacks, then disable individual attack subclasses that you do ***not*** want to omit, if any. |
| **SQL Injection** | Enable to omit detection of SQL injection attacks, then disable individual attack subclasses that you do ***not*** want to omit, if any. |
| **Common Exploits** | Enable to omit detection of common exploits, such as an injection attack in a language other than SQL, then disable individual attack subclasses that you do ***not*** want to omit, if any. |
| **Information Disclosure** | Enable to omit detection of server errors and other sensitive messages in the requested document and HTTP headers, then disable individual information subclasses that you do ***not*** want to omit, if any. |
| **Credit Card Detection** | Enable to omit detection of credit card numbers in the response from the server. |

6 Repeat the previous step for each entry that you want to add to the server protection exception.

7 If you need to modify a server protection exception, click its *Edit* icon. To remove a single entry from the exception, click its *Delete* icon. To remove all entries from the exception, click the *Clear* icon.




8 Click *OK*.

To apply the server protection exception, select it in a server protection rule. For details, see “Configuring server protection rules” on page 161.

# Configuring start pages

*Web Protection* > *Start Pages* > *Start Pages* displays the list of main web pages.

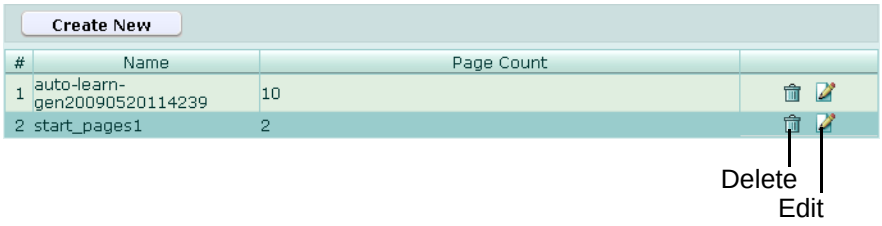
When a start page group is selected in the inline protection profile, in order to initiate a valid session, HTTP clients ***must*** begin from a valid start page.

For example, you may wish to specify that HTTP clients of an e-commerce web site must begin their session from either an item view or the first stage of the shopping cart checkout, and cannot begin a valid session from the third stage of the shopping cart checkout.

Start pages are applied by selecting them within an inline protection profile. For details, see "Configuring inline web protection profiles" on page 213.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 66:** *Start Pages* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a group of start pages. |
| # | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Page Count** | The number of individual URLs contained in the entry. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in an inline protection profile.<br>Click *Edit* to modify the entry. |

### To configure a start page group

Before you configure a start page rule, if you want to apply it only to HTTP requests for a specific real or virtual host, you must first define the web host in a protected hosts group. For details, see "Configuring protected hosts" on page 113.

1. Go to *Web Protection* > *Start Pages* > *Start Pages*.
2. Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.
3. In *Name*, type the name of the group of start pages.

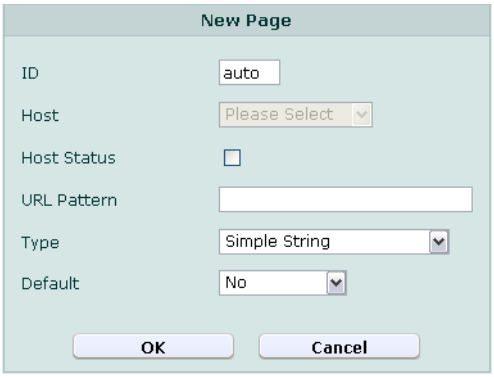
   This field cannot be modified if you are editing an existing group of start pages. To modify the name, delete the entry, then recreate it using the new name.

4 From *Action*, select which action the FortiWeb unit will take when an HTTP request that initiates a session does not begin with one of the allowed start pages:

- *Alert*: Accept the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.
- *Alert & Deny*: Block the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.
- *Redirect*: Accept the connection but redirect the request to whichever URL you define in this group as the default start page.
- *Send 403 Forbidden*: Reply with an HTTP 403 (Access Forbidden) error message and generate an alert and/or log message. For details, see "Configuring logging and alerts" on page 252.

5 Click *OK*.

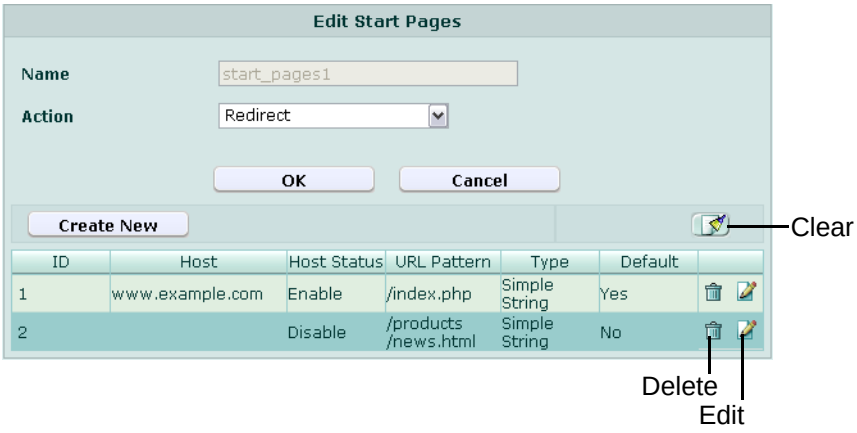
6 Click *Create New*, then configure the following:




| *Name of the GUI item* | *Description* |
|---|---|
| **ID** | Enter the index number of the start page within the group of start pages, or keep the field's default value of `auto` to let the FortiWeb unit automatically assign the next available index number. |
| **Host** | Select which protected hosts entry (either a web host name or IP address) that the `Host:` field of the HTTP request must be in order to match a valid start page.<br>This option is available only if *Host Status* is enabled. |
| **Host Status** | Enable to require that the `Host:` field of the HTTP request match a protected hosts entry in order to match a valid start page. Also configure *Host*. |
| **URL Pattern** | Depending on your selection in *Type*, type either:<br>• the literal URL, such as `/index.php`, that the HTTP request must contain in order to match the start page rule. The URL must begin with a slash ( / ).<br>• a regular expression, such as `^/*.php`, matching all and only the URLs to which the start page rule should apply. The pattern is ***not*** required to begin with a slash ( / ). However, it must at least match URLs that begin with a slash, such as `/index.cfm`.<br>Do not include the name of the web host, such as `www.example.com`, which is configured separately in the *Host* drop-down list. |
| **Type** | Select whether *URL Pattern* is a *Simple String* (that is, a literal URL) or a *Regular Expression*. |
| **Default** | Select *Yes* to use the page as the default for HTTP requests that either:<br>• do not specify any URL<br>• do not specify the URL of a valid start page (only if you have selected *Redirect* from *Action*) |

7 Repeat the previous step for each start page that you want to add to the group of start pages.

8 If you need to modify a start page, click its *Edit* icon. To remove a single start page from the group of start pages, click its *Delete* icon. To remove all start pages from the group of start pages, click the *Clear* icon.




9 Click *OK*.

To apply the group of start pages, select it in an inline protection profile. For details, see "Configuring inline web protection profiles" on page 213.

**Note:** In order for start pages to be enforced, you must also enable "Session Management" on page 216 in the inline protection profile.

Attack log messages and *Alert Message Console* messages contain `DETECT_START_PAGE_FAILED` when this feature detects a start page violation.

# Configuring URL black list rules

*Web Protection* > *Black List Rules* > *Black List Rules* displays the list of black list rules.

Black list rules define HTTP requests that will be blocked based upon their host name and URL.

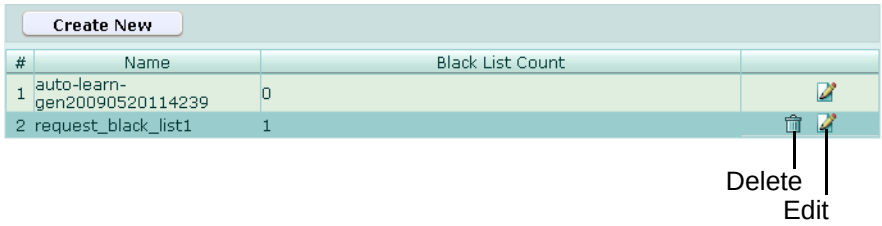
**Note:** Black list rules are evaluated ***after*** some other rules. For details, see "Order of execution" on page 151.

Black list rules are applied by selecting them within an inline or offline protection profile. For details, see "Configuring inline web protection profiles" on page 213 or "Configuring offline protection profiles" on page 219.

SNMP traps can be used to notify you when a black list rule is enforced. For details, see "Configuring an SNMP community" on page 48.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 67:** *Black List Rules* **tab**



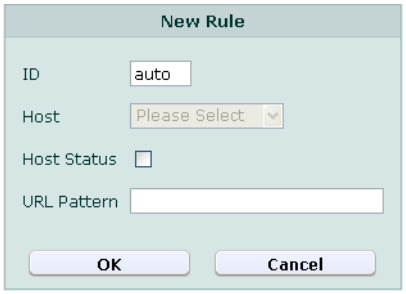

| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a black list rule. |
| **#** | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Black List Count** | The number of individual rules contained in the entry. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in an inline or offline protection profile.<br>Click *Edit* to modify the entry. |

### To configure a black list rule

Before you configure a black list rule, if you want to apply it only to HTTP requests for a specific real or virtual host, you must first define the web host in a protected hosts group. For details, see "Configuring protected hosts" on page 113.

1. Go to *Web Protection* > *Black List Rules* > *Black List Rules*.
2. Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.
3. In *Name*, type the name of the page access rule.

   This field cannot be modified if you are editing an existing black list rule. To modify the name, delete the entry, then recreate it using the new name.
4. Click *OK*.
5. Click *Create New*, then configure the following:

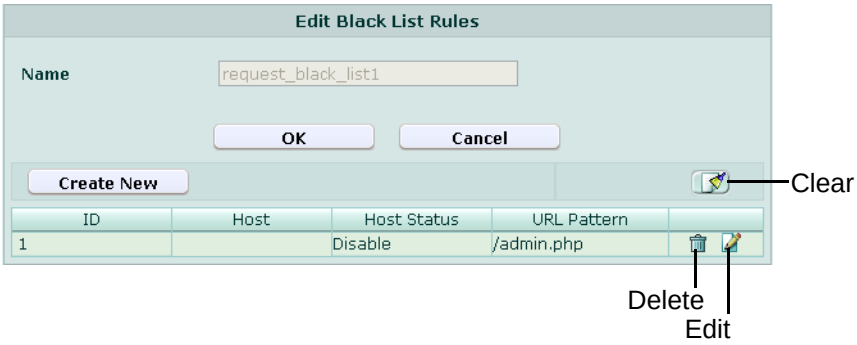



| *Name of the GUI item* | *Description* |
|---|---|
| **ID** | Enter the index number of the individual rule within the black list rule, or keep the field's default value of `auto` to let the FortiWeb unit automatically assign the next available index number. |

| | |
|---|---|
| **Host** | Select which protected hosts entry (either a web host name or IP address) that the `Host:` field of the HTTP request must be in order to match the black list rule.<br>This option is available only if *Host Status* is enabled. |
| **Host Status** | Enable to require that the `Host:` field of the HTTP request match a protected hosts entry in order to match the black list rule. Also configure *Host*. |
| **URL Pattern** | Type the exact URL that is not allowed to be accessed.<br>The URL must begin with a slash ( / ). Do not include the name of the web host, such as `www.example.com`, which is configured separately in the *Host* drop-down list.<br>Regular expressions are not supported in the current release. |

6 Repeat the previous step for each individual rule that you want to add to the black list rule.

7 If you need to modify an individual rule, click its *Edit* icon. To remove an individual rule from the black list rule, click its *Delete* icon. To remove all individual rules from the black list rule, click the *Clear* icon.




8 Click *OK*.

To apply the black list rule, select it in an inline or offline protection profile. For details, see “Configuring inline web protection profiles” on page 213 or “Configuring offline protection profiles” on page 219.

Attack log messages and *Alert Message Console* messages contain `DETECT_BLACK_PAGE` when this feature detects a blacklisted URL.

# Configuring URL white list rules

*Web Protection* > *White List Rules* > *White List Rules* displays the list of white list rules.

White list rules define HTTP requests that will be allowed based upon their host name and URL.

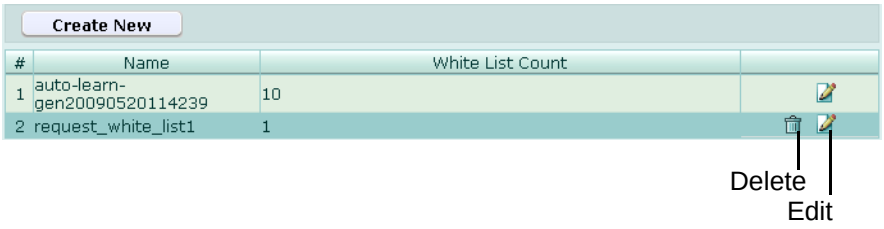
**Note:** White list rules are evaluated ***after*** some other rules. For details, see “Order of execution” on page 151.

White list rules are applied by selecting them within an inline or offline protection profile. For details, see “Configuring inline web protection profiles” on page 213 or “Configuring offline protection profiles” on page 219.

SNMP traps can be used to notify you when a white list rule is enforced. For details, see “Configuring an SNMP community” on page 48.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 68:** *White List Rules* **tab**



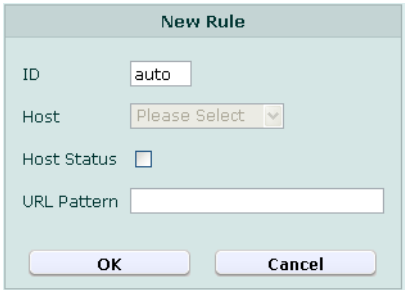

| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a white list rule. |
| # | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **White List Count** | The number of individual rules contained in the entry. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in an inline or offline protection profile.<br>Click *Edit* to modify the entry. |

### To configure a white list rule

Before you configure a white list rule, if you want to apply it only to HTTP requests for a specific real or virtual host, you must first define the web host in a protected hosts group. For details, see "Configuring protected hosts" on page 113.

1. Go to *Web Protection* > *White List Rules* > *White List Rules*.
2. Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.
3. In *Name*, type the name of the white list rule.

   This field cannot be modified if you are editing an existing white list rule. To modify the name, delete the entry, then recreate it using the new name.
4. Click *OK*.
5. Click *Create New*, then configure the following:

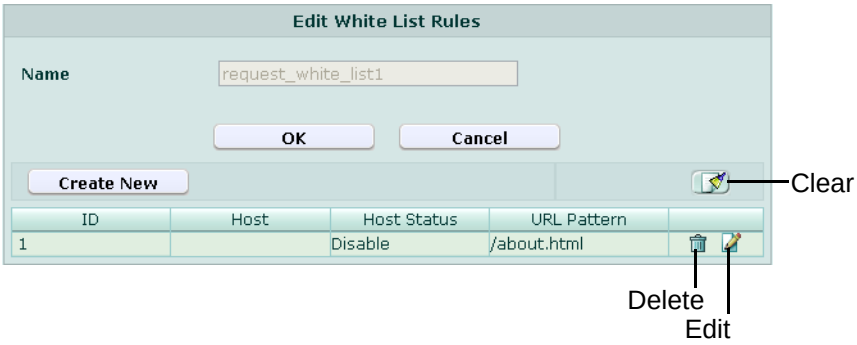



| *Name of the GUI item* | *Description* |
|---|---|
| **ID** | Enter the index number of the individual rule within the white list rule, or keep the field's default value of `auto` to let the FortiWeb unit automatically assign the next available index number. |

| | |
|---|---|
| **Host** | Select which protected hosts entry (either a web host name or IP address) that the `Host:` field of the HTTP request must be in order to match the white list rule.<br>This option is available only if *Host Status* is enabled. |
| **Host Status** | Enable to require that the `Host:` field of the HTTP request match a protected hosts entry in order to match the white list rule. Also configure *Host*. |
| **URL Pattern** | Type the exact URL that is allowed to be accessed.<br>The URL must begin with a slash ( / ). Do not include the name of the web host, such as `www.example.com`, which is configured separately in the *Host* drop-down list.<br>Regular expressions are not supported in the current release. |

6 Repeat the previous step for each individual rule that you want to add to the white list rule.

7 If you need to modify an individual rule, click its *Edit* icon. To remove an individual rule from the white list rule, click its *Delete* icon. To remove all individual rules from the white list rule, click the *Clear* icon.




8 Click *OK*.

To apply the white list rule, select it in an inline or offline protection profile. For details, see “Configuring inline web protection profiles” on page 213 or “Configuring offline protection profiles” on page 219.

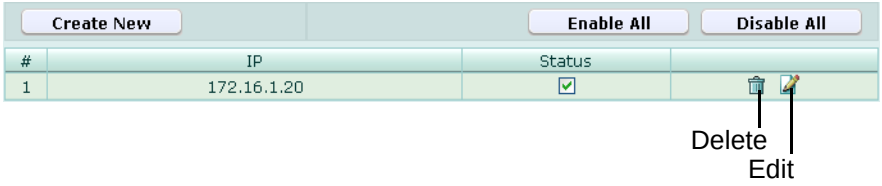
# Blacklisting client IP addresses

*Web Protection* > *IP List* > *IP Blacklist* displays the list of blacklisted IP addresses.

Blacklisted IP addresses define which client IP addresses are not permitted to connect to your web servers. For details, see “Order of execution” on page 151.

To be able to access this part of the web-based manager, in your administrator account’s access profile, you must have both *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see “About permissions” on page 58.

**Table 69:** *IP Blacklist* **tab**



| Name of the GUI item | Description |
|---|---|
| **Create New** | Click to add a source IP address to the black list. |
| **Enable All** | Click to enable all entries in the IP black list. For details, see “Enabling or disabling IP address blacklisting” on page 178. |
| **Disable All** | Click to disable all entries in the IP black list. For details, see “Enabling or disabling IP address blacklisting” on page 178. |
| # | The index number of the entry in the list. |
| **IP** | The source IP address whose connections are blacklisted. |
| **Status** | Mark the check box to enable use of the entry. For details, see “Enabling or disabling IP address blacklisting” on page 178. |
| (No column heading.) | Click *Delete* to remove the entry.<br>Click *Edit* to modify the entry. |

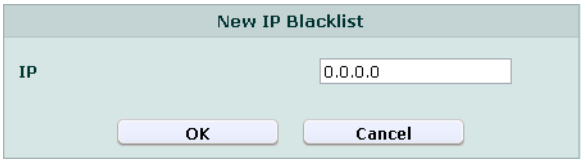
### To configure a blacklisted IP address

Before you configure a blacklisted IP address, you may want to view a list of the IP addresses whose connections are most frequently blocked in order to determine the best candidates for blacklisting. For details, see “Viewing the top 10 IP black list candidates” on page 179.

**Note:** Alternatively, you can create an IP black list entry while viewing the list of top black list candidates. For details, see “Viewing the top 10 IP black list candidates” on page 179.

1 Go to *Web Protection* > *IP List* > *IP Blacklist*.

2 Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.




3 In *IP*, type the source IP address whose connection attempts will be rejected.

**Note:** Blacklisting will block all connections from that source IP address. If multiple clients share the same source IP address, such as when a group of clients is behind a firewall or router, blacklisting the source IP address could block innocent clients that share the same source IP address with an offending client. To detect a shared source IP address, see “Viewing the top 10 IP black list candidates” on page 179.

4 Click *OK*.

Blacklisted IP addresses will take effect whenever the FortiWeb unit receives a connection, except if the FortiWeb unit is operating in offline protection mode. You do not need to select them in any policy or profile.

## Enabling or disabling IP address blacklisting

You can individually enable and disable entries in the list of blacklisted source IP addresses, without deleting them from the list. Disabled entries will not be used for blacklisting.

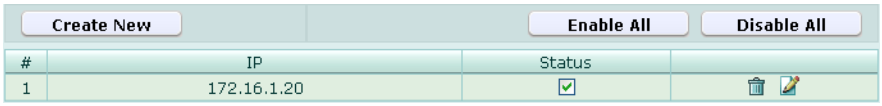
By default, blacklisted IP addresses that you create are enabled, and the FortiWeb unit will use them when applying blacklisting.

**Note:** Alternatively to enabling or disabling individual entries, you can click *Enable All* to enable all entries, or *Disable All* to disable all entries. If you must enable or disable the majority of entries with few exceptions, and if it is acceptable to temporarily switch the statuses of the exceptions, you can switch statuses more quickly: first click *Enable All* or *Disable All*, then adjust the statuses of the exceptions.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "About permissions" on page 58.

**To enable or disable a blacklisted IP address**

1 Go to *Web Protection* > *IP List* > *IP Blacklist*.




2 In the row corresponding to the entry that you want to ***enable***, in the *Status* column, mark the check box.

3 In the row corresponding to the entry that you want to ***disable***, in the *Status* column, clear the check box.

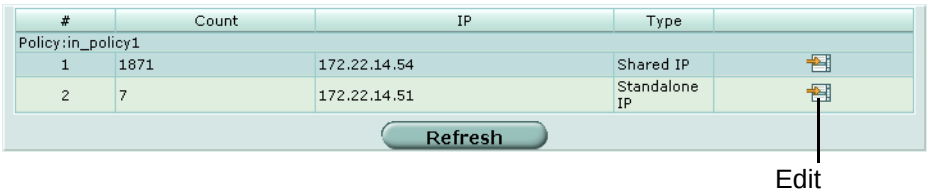
## Viewing the top 10 IP black list candidates

*Web Protection* > *IP List* > *IP Blacklist TOP 10* displays the list of the top 10 candidates for the IP address black list, and to add them to the IP black list.

Blacklisted IP addresses define which source IP addresses are not permitted to connect to your web servers. The list of top 10 candidates tracks the number of times each source IP address is blocked by a policy. If an IP address is frequently the source of errors or attacks, it may be a good candidate for the IP blacklist.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 70:** *IP Blacklist TOP 10* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| # | The rank number of the entry in the top 10 list. |
| **Count** | The number of times that connections from the IP address have been blocked due to the policy indicated above the rank number. |
| **IP** | The source IP address of blocked connections. |

| | |
|---|---|
| **Type** | Indicates whether the source IP address is for a single client (*Standalone IP*), or is shared by multiple clients behind a network address translation (NAT) device such as a firewall or router (*Shared IP*).<br>**Note:** If the *Type* is *Shared IP*, blacklisting the IP could block innocent clients that share the same source IP address with an offending client.<br>**Note:** You can configure the number of HTTP sessions greater than which an IP address is assumed to be a shared IP address. For details, see the *FortiWeb CLI Reference*. |
| (No column heading.) | Click *Edit* to add the IP address to the client black list. For details, see "Blacklisting client IP addresses" on page 177. |
| **Refresh** | Click to refresh the display of top 10 IP black list candidates. |

# Whitelisting client IP addresses

*Web Protection* > *IP List* > *IP Trust List* displays the list of whitelisted (that is, trusted) IP addresses.

Whitelisted IP addresses define which client IP addresses are usually permitted to connect to your web servers, and are exempt from many of the restrictions that would otherwise be applied by a policy's protection profile. For details on which scans are omitted, see "Order of execution" on page 151.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 71:** *IP Trust List* **tab**


| ***Name of the GUI item*** | ***Description*** |
|---|---|
| **Create New** | Click to add a source IP address to the white list. |
| **#** | The index number of the entry in the list. |
| **IP** | The source IP address whose connections are whitelisted. |
| (No column heading.) | Click *Delete* to remove the entry.<br>Click *Edit* to modify the entry. |

### To configure a whitelisted IP address

1. Go to *Web Protection* > *IP List* > *IP Blacklist*.
2. Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.
3. For *Type*, select *Individual IP* or *Range IP*.
4. If you select *Individual IP*, enter the IP address; if you select *Range IP*, enter the IP range. The connection attempts from these IP addresses will be unconditionally allowed.

**Caution:** Whitelisting will allow all connections from that source IP address. If multiple clients share the same source IP address, such as when a group of clients is behind a firewall or router, whitelisting the source IP address could allow offending clients that share the same source IP address with a whitelisted client.

5 Click *OK*.

Whitelisted IP addresses will be applied whenever the FortiWeb unit receives a connection. You do not need to select them in any policy or profile.

# Configuring brute force login attack sensors

*Web Protection* > *Brute Force Login* > *Brute Force Login* displays the list of brute force login attack sensors.

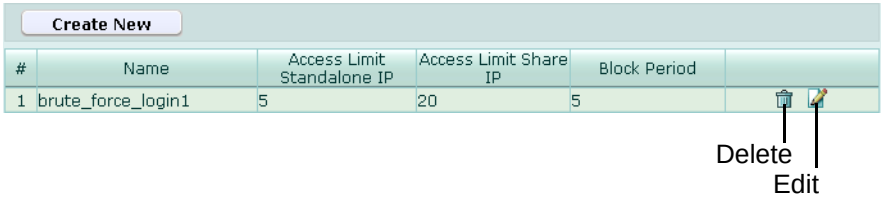
Brute force attacks attempt to penetrate systems by the sheer number of clients, attempts, or computational power, rather than by intelligent insight. For example, in brute force attacks on authentication, multiple web clients may rapidly try one user name and password combination after another in an attempt to eventually guess a correct login and gain access to the system. In this way, behavior differs from web crawlers, which typically do not focus on a single URL.

Brute force login attack sensors track the rate at which each source IP address makes requests for specific URLs. If the source IP address exceeds the threshold, the FortiWeb unit penalizes the source IP address by blocking additional requests for the time period that you indicate in the sensor.

Brute force login attack sensors are applied by selecting them within an inline protection profile. For details, see "Configuring inline web protection profiles" on page 213.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 72:** *Brute Force Login* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a brute force login attack sensor. |
| **#** | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Access Limit Standalone IP** | The rate limit for source IP addresses that are single clients. Request rates exceeding the threshold will cause the FortiWeb unit to block additional requests for the length of the time in the *Block Period* column.<br>`0` indicates that the rate is not limited. |

| | |
|---|---|
| **Access Limit Share IP** | The rate limit for source IP addresses that are shared by multiple clients behind a network address translation (NAT) device such as a firewall or router. Request rates exceeding the threshold will cause the FortiWeb unit to block additional requests for the length of the time in the *Block Period* column.<br>`0` indicates that the rate is not limited. |
| **Block Period** | The length of time for which the FortiWeb unit will block additional requests after a source IP address exceeds a rate threshold. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in an inline protection profile.<br>Click *Edit* to modify the entry. |

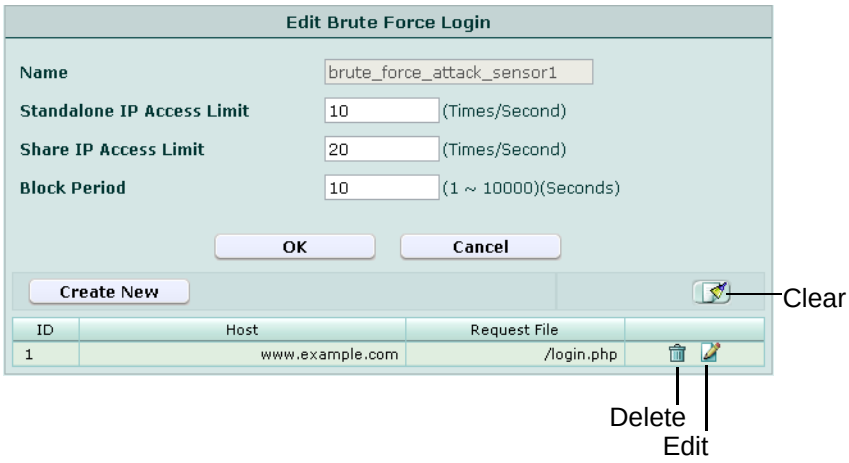
### To configure a brute force login attack sensor

Before you configure a brute force login attack sensor, if you want to apply it only to HTTP requests for a specific real or virtual host, you must first define the web host in a protected hosts group. For details, see "Configuring protected hosts" on page 113.

1 Go to *Web Protection* > *Brute Force Login* > *Brute Force Login*.

2 Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.

3 Configure the following:



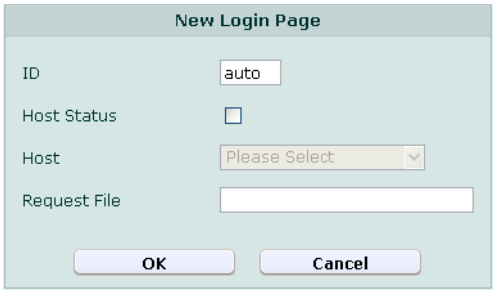

| *Name of the GUI item* | *Description* |
|---|---|
| **Name** | Type the name of the brute force login attack sensor.<br>This field cannot be modified if you are editing an existing brute force login attack sensor. To modify the name, delete the entry, then recreate it using the new name |
| **Standalone IP Access Limit** | Type the rate threshold for source IP addresses that are single clients. Request rates exceeding the threshold will cause the FortiWeb unit to block additional requests for the length of the time in the *Block Period* field.<br>To disable the rate limit, type `0`. |

| | |
|---|---|
| **Share IP Access Limit** | Type the rate threshold for source IP addresses that are shared by multiple clients behind a network address translation (NAT) device such as a firewall or router. Request rates exceeding the threshold will cause the FortiWeb unit to block additional requests for the length of the time in the *Block Period* field.<br>To disable the rate limit, type `0`.<br>**Note:** Blocking a shared source IP address could block innocent clients that share the same source IP address with an offending client. In addition, the rate is a total rate for all clients that use the same source IP address. For these reasons, you should usually enter a greater value for this field than for *Standalone IP Access Limit.* |
| **Block Period** | Type the length of time in seconds for which the FortiWeb unit will block additional requests after a source IP address exceeds a rate threshold.<br>The block period is shared by all clients whose traffic originate from the source IP address. |

4 Click *OK*.

5 Click *Create New*.

6 Configure the following and click *OK*:




| *Name of the GUI item* | *Description* |
|---|---|
| **ID** | Type the index number of the login page in the brute force login attack sensor's list. The index number affects the order of display only, and does not affect match order. |
| **Host Status** | Enable to require that the `Host:` field of the HTTP request match a protected hosts entry in order to be included in the brute force login attack sensor's rate calculations. Also configure *Host*. |
| **Host** | Select which protected hosts entry (either a web host name or IP address) that the `Host:` field of the HTTP request must be in order to match the brute force login attack sensor.<br>This option is available only if *Host Status* is enabled. |
| **Request File** | Type the URL that the HTTP request must match to be included in the brute force login attack sensor's rate calculations.<br>The URL must begin with a slash ( / ). Do not include the name of the web host, such as `www.example.com`, which is configured separately in the *Host* drop-down list. |

7 Repeat the two previous steps for each individual login page that you want to add to the brute force login attack sensor.

8 Click *OK*.

To apply the brute force login attack sensor, select it in an inline protection profile. For details, see "Configuring inline web protection profiles" on page 213.

Attack log messages and *Alert Message Console* messages contain `DETECT_BRUTE_FORCE_LOGIN` when this feature detects a brute force login attack.

# Configuring robot control sensors

*Web Protection* > *Robot Control* > *Robot Control* displays the list of robot control sensors.

Search engines, link checkers, retrievals of entire web sites for a user's offline use, and other automated uses of the web (sometimes called robots, spiders, web crawlers, or automated user agents) often access web sites at a more rapid rate than human users. However, it would be unusual for them to request the same URL within that time frame. Usually, they request many different URLs in rapid sequence. For example, while indexing a web site, a search engine's web crawler may rapidly request all of the web site's most popular URLs. If the URLs are web pages, it may also follow the hyperlinks by requesting all URLs mentioned in those web pages. In this way, behavior of web crawlers differs from a typical brute force login attack, which focuses repeatedly only on the same URL.

You can request that robots not index and/or follow links, and disallow their access to specific URLs (see http://www.robotstxt.org/). However, misbehaving robots frequently ignore the request, and there is no single standard way to rate limit robots.

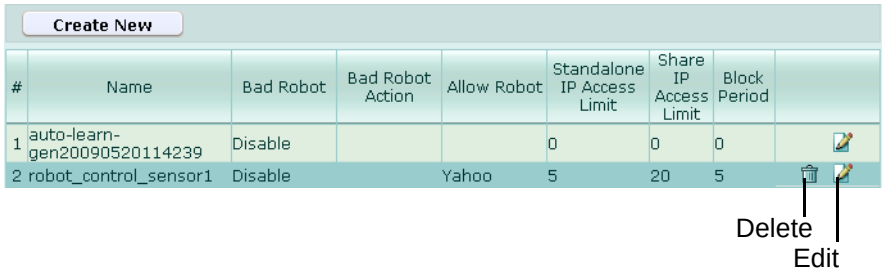
Robot control sensors can track the rate at which each source IP address makes requests. If the source IP address exceeds the threshold, the FortiWeb unit penalizes the source IP address by blocking additional requests for the time period that you indicate in the sensor.

Robot control sensors can also use the `User-Agent:` field in the HTTP header to allow legitimate robots, and to block robots that are notorious for misbehaving.

Robot control sensors are applied by selecting them within an inline or offline protection profile. For details, see "Configuring inline web protection profiles" on page 213 or "Configuring offline protection profiles" on page 219.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 73:** *Robot Control* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a robot control sensor. |
| **#** | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Bad Robot** | Indicates whether you have enabled or disabled blocking of web crawlers that are known to ignore `no-index`, `no-follow` and other directives. |

| | |
|---|---|
| **Bad Robot Action** | Indicates the action that the FortiWeb unit will take when it detects a web crawler known to ignore no-index, no-follow, and other directives.<br>• **Alert**: Accept the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>• **Alert & Deny**: Block the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>• **Redirect**: Redirect the request to the URL that you specify in the protection profile and generate an alert and/or log message. For details, see "Configuring logging and alerts" on page 252 and "Redirect URL" on page 219.<br>• **Send 403 Forbidden**: Reply with an HTTP 403 (Access Forbidden) error message and generate an alert and/or log message. For details, see "Configuring logging and alerts" on page 252. |
| **Allow Robot** | Indicates which well-known robots, if any, are allowed and will not be rate controlled or subject to parameter validation rules, server protection rules, or *Bad Robot* detection. |
| **Standalone IP Access Limit** | The rate threshold for source IP addresses that are single clients. Request rates exceeding the threshold will cause the FortiWeb unit to block additional requests for the length of the time in the *Block Period* column.<br>`0` indicates that the rate is not limited. |
| **Share IP Access Limit** | The rate threshold for source IP addresses that are shared by multiple clients behind a network address translation (NAT) device such as a firewall or router. Request rates exceeding the threshold will cause the FortiWeb unit to block additional requests for the length of the time in the *Block Period* column.<br>`0` indicates that the rate is not limited. |
| **Block Period** | The length of time for which the FortiWeb unit will block additional requests after a source IP address exceeds a rate threshold. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in an inline or offline protection profile.<br>Click *Edit* to modify the entry. |

### To configure a robot control sensor

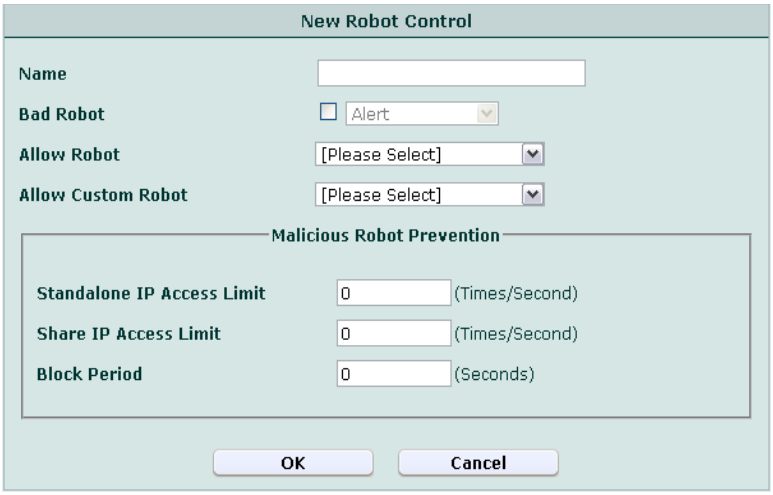
Before you configure a robot control sensor, if you want to exempt any well-known search engines or custom robots from rate limiting, you must first create groups that defines which robots you want to allow. For details, see "Grouping predefined robots" on page 188 and "Grouping custom robots" on page 189.

**Note:** Alternatively, you can automatically configure a robot control sensor that allows all predefined search engine types by generating a default auto-learning profile. For details, see "Generating an auto-learning profile and its components" on page 227.

1. Go to *Web Protection* > *Robot Control* > *Robot Control*.
2. Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.
3. In *Name*, type the name of the robot control sensor.

   This field cannot be modified if you are editing an existing robot control sensor. To modify the name, delete the entry, then recreate it using the new name.

**4** Configure the following:




| *Name of the GUI item* | *Description* |
|---|---|
| **Bad Robot** | Enable to detect web crawlers known to misbehave, then select which action the FortiWeb unit will take when it detects one.<br>• **Alert**: Accept the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>• **Alert & Deny**: Block the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>• **Redirect**: Redirect the request to the URL that you specify in the protection profile and generate an alert and/or log message. For details, see "Configuring logging and alerts" on page 252 and "Redirect URL" on page 219.<br>• **Send 403 Forbidden**: Reply with an HTTP 403 (Access Forbidden) error message and generate an alert and/or log message. For details, see "Configuring logging and alerts" on page 252.<br>**Note:** If a *WAF Auto Learning Profile* will be selected in the policy with profiles that use this rule, you should select *Alert*. If the *Action* is *Alert & Deny*, the FortiWeb unit will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. |
| **Allow Robot** | Select a group of well-known search engines' web crawlers, if any, that will be exempt from the rate limit of this robot control sensor. For details about creating robot groups, see "Grouping predefined robots" on page 188. The FortiWeb unit will omit any subsequent intrusion detection features, including parameter validation rules, server protection rules, or *Bad Robot* detection.<br>Attack log messages and *Alert Message Console* messages contain log messages such as `DETECT_ALLOW_ROBOT_GOOGLE`, `DETECT_ALLOW_ROBOT_YAHOO`, and `DETECT_ALLOW_ROBOT_MSN`, when this feature detects an allowed predefined robot. For details, see "Alert Message Console widget" on page 31 or "Viewing log messages" on page 262. |
| **Allow Custom Robot** | Select a group of custom robots, if any, that will be exempt from the rate limit of this robot control sensor. For details about creating custom robot groups, see "Grouping custom robots" on page 189. The FortiWeb unit will omit any subsequent intrusion detection features, including parameter validation rules, server protection rules, or *Bad Robot* detection.<br>Attack log messages and *Alert Message Console* messages contain log messages such as `DETECT_ALLOW_ROBOT: Custom-Robot-1` (where `Custom-Robot-1` is the name that you configured for the robot's signature) when this feature detects an allowed custom robot. For details, see "Alert Message Console widget" on page 31 or "Viewing log messages" on page 262. |
| **Malicious Robot Prevention** | |

| | |
|---|---|
| **Standalone IP Access Limit** | Type the rate limit in number of requests per second for source IP addresses that are single clients. Request rates exceeding the threshold will cause the FortiWeb unit to block additional requests for the length of the time in the *Block Period* field.<br>To disable the rate limit, type `0`. |
| **Share IP Access Limit** | Type the rate limit in number of requests per second for source IP addresses that are shared by multiple clients behind a network address translation (NAT) device such as a firewall or router. Request rates exceeding the threshold will cause the FortiWeb unit to block additional requests for the length of the time in the *Block Period* field.<br>To disable the rate limit, type `0`.<br>**Note:** Blocking a shared source IP address could block innocent clients that share the same source IP address with an offending client. In addition, the rate is a total rate for all clients that use the same source IP address. For these reasons, you should usually enter a greater value for this field than for *Standalone IP Access Limit*. |
| **Block Period** | Type the length of time for which the FortiWeb unit will block additional requests after a source IP address exceeds its rate threshold. |

5 Click *OK*.

To apply the robot control sensor, select it in an inline or offline protection profile. For details, see "Configuring inline web protection profiles" on page 213 or "Configuring offline protection profiles" on page 219.

Attack log messages and *Alert Message Console* messages contain `DETECT_MALICIOUS_ROBOT` when this feature detects a misbehaving robot or any other HTTP client that exceeds the rate limit.

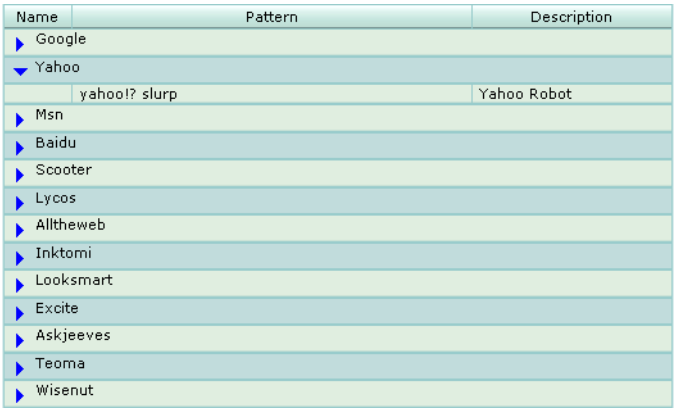
## Viewing the predefined list of well-known robots

*Web Protection* > *Robot Control* > *Known Robot* displays the predefined list of well-known robots.

The *Pattern* column contains a regular expression that the FortiWeb unit can compare to the `User-Agent:` field in the HTTP header in order to determine whether or not the HTTP client is a well-known, legitimate robot. Legitimate robots, such as search engine indexers, usually should be exempt from attack detection.

Robot exemptions are applied indirectly, by first forming groups of robots, then selecting those groups in a robot control sensor. For details, see "Grouping predefined robots" on page 188.

**Figure 16: Viewing the list of known robots**



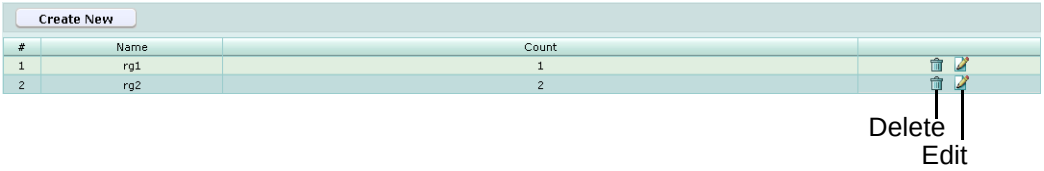
## Grouping predefined robots

*Web Protection* > *Robot Control* > *Robot Group* displays the list of groups of predefined robots.

A robot group contains one or more of the predefined robot signatures. Robot groups are applied by selecting them in the robot control sensor. For details, see "Configuring robot control sensors" on page 184.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 74:** *Robot Group* **tab**

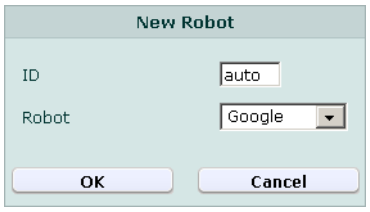



| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a known robot group. |
| # | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Count** | The number of known robots contained in the group. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a robot control sensor.<br>Click *Edit* to modify the entry. |

### To configure a robot group

1. Go to *Web Protection* > *Robot Control* > *Robot Group*.
2. Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.
3. In *Name*, type the name of the robot group.

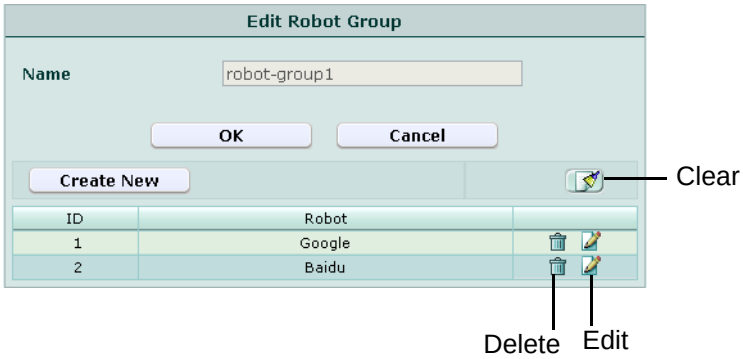
   This field cannot be modified if you are editing an existing robot group. To modify the name, delete the entry, then recreate it using the new name.
4. Click *OK*.
5. Click *Create New*, then configure the following:



| Name of the GUI item | Description |
|---|---|
| **ID** | Enter the index number of the robot entry within the robot group, or keep the field's default value of `auto` to let the FortiWeb unit automatically assign the next available index number. |
| **Robot** | Select the name of a robot. For the predefined list of well-known robots and their defining patterns, see "Viewing the predefined list of well-known robots" on page 187. |

6 Repeat the previous step for each robot that you want to add to the robot group.

7 If you need to modify a robot, click its *Edit* icon. To remove a single robot from the robot group, click its *Delete* icon. To remove all robots from the robot group, click the *Clear* icon.




8 Click *OK*.

To use a robot group, you must select it in a robot control sensor. For details, see "Configuring robot control sensors" on page 184.

## Grouping custom robots

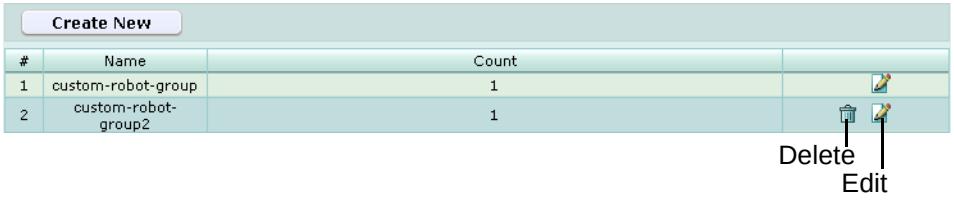
*Web Protection* > *Robot Control* > *Custom Robot* displays the list of custom robot groups.

Instead of using groups of predefined well-known robots, you can configure sets of custom robot signatures. Each signature is a regular expression that the FortiWeb unit can compare to the `User-Agent:` field in the HTTP header in order to determine whether or not the HTTP client is a legitimate robot. Legitimate robots, such as search engine indexers, usually should be exempt from attack detection. If your organization has written its own search indexer, or uses a third-party spider not identified in the predefined list, you may need to write a custom robot signature.

Custom robot exemptions are applied by selecting a set of custom robot signatures in a robot control sensor. For details, see "Configuring robot control sensors" on page 184.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 75:** *Custom Robot* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a custom robot group. |
| # | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Count** | The number of custom robots contained in the group. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a robot control sensor.<br>Click *Edit* to modify the entry. |

### To configure a group of custom robot signatures

1 Go to *Web Protection* > *Robot Control* > *Custom Robot*.

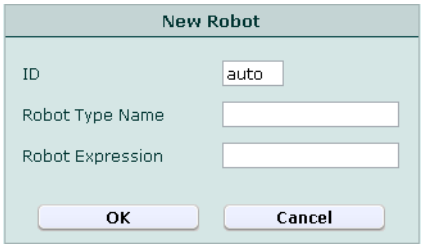
2 Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.

3 In *Name*, type the name of the custom robot signature set.

This field cannot be modified if you are editing an existing custom robot. To modify the name, delete the entry, then recreate it using the new name.

4 Click *OK*.

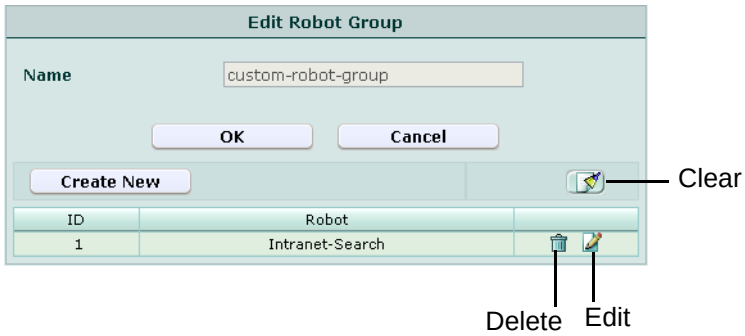
5 Click *Create New*, then configure the following:




| *Name of the GUI item* | *Description* |
|---|---|
| **ID** | Type the index number of the custom robot signature within the set, or keep the field's default value of `auto` to let the FortiWeb unit automatically assign the next available index number. |
| **Robot Type Name** | Type a name, such as `Intranet-Indexer`, for the signature. This name will appear in log messages where the signature was used to detect a robot. |
| **Robot Expression** | Type a regular expression that matches all and only the `User-Agent:` fields in the HTTP header known to be produced by the custom robot.<br>For example, if a custom robot causes either:<br>• `User-Agent: happy-spider`<br>• `User-Agent: happy-spider2.0`.<br>but ***not*** `User-Agent: baiduspider`, you would write a regular expression to match the first two cases, but that would not match the third. |

6 Repeat the previous step for each custom robot signature that you want to add to the set. Only one set may be selected per robot control sensor, so you may want to include multiple custom robots' signatures in this set.

7 If you need to modify a custom robot signature, click its *Edit* icon. To remove a single signature from the set, click its *Delete* icon. To remove all signatures from the set, click the *Clear* icon.




8 Click *OK*.

To use a custom robot group, you must select it in a robot control sensor. For details, see "Configuring robot control sensors" on page 184.

# Configuring allowed method exceptions

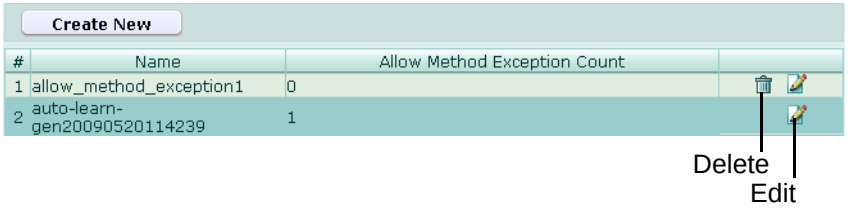
*Web Protection* > *Allow Method Exceptions* > *Allow Method Exceptions* displays the list of allowed method exceptions.

While most URL and host name combinations controlled by a profile may require similar HTTP request methods, you may have some that require different methods. Instead of forming separate policies and profiles for those requests, you can instead configure allowed method exceptions. Allowed method exceptions allow you to specify exceptions to the generally allowed request methods.

Allowed method exceptions are applied by selecting them within an inline or offline protection profile. For details, see "Configuring inline web protection profiles" on page 213 or "Configuring offline protection profiles" on page 219.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 76:** *Allow Method Exceptions* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add an allowed method exception. |
| # | The index number of the entry in the list. |

| | |
|---|---|
| **Name** | The name of the entry. |
| **Allow Method Exception Count** | The number of individual rules contained in the entry. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in an inline or offline protection profile.<br>Click *Edit* to modify the entry. |

### To configure an allowed method exception

Before you configure an allowed method exception, if you want to apply it only to HTTP requests for a specific real or virtual host, you must first define the web host in a protected hosts group. For details, see "Configuring protected hosts" on page 113.

1 Go to *Web Protection* > *Allow Method Exceptions* > *Allow Method Exceptions*.

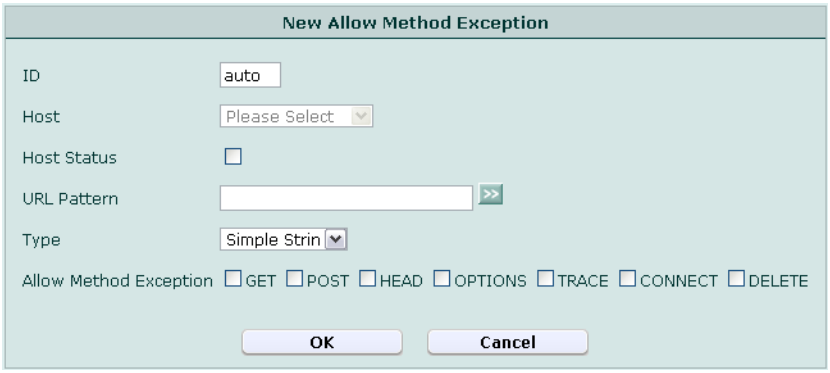
2 Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.

3 In *Name*, type the name of the allowed method exception.

This field cannot be modified if you are editing an existing allowed method exception. To modify the name, delete the entry, then recreate it using the new name.

4 Click *OK*.

5 Click *Create New*, then configure the following:

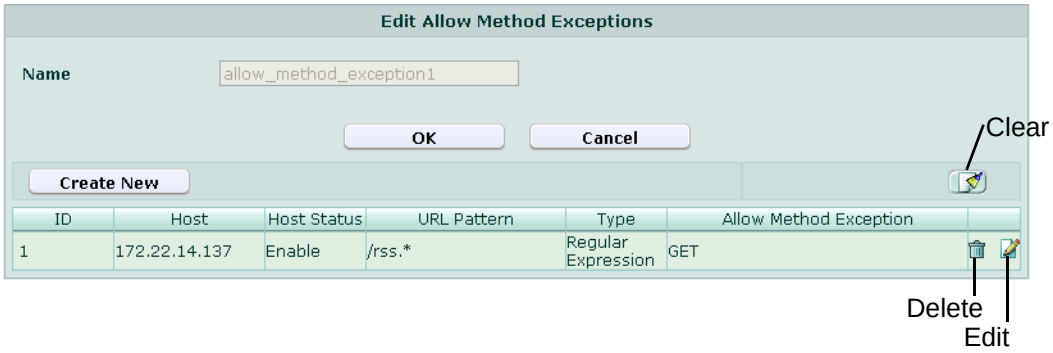



| *Name of the GUI item* | *Description* |
|---|---|
| **ID** | Enter the index number of the individual rule within the allowed method exception, or keep the field's default value of `auto` to let the FortiWeb unit automatically assign the next available index number. |
| **Host** | Select which protected hosts entry (either a web host name or IP address) that the `Host:` field of the HTTP request must be in order to match the allowed method exception.<br>This option is available only if *Host Status* is enabled. |
| **Host Status** | Enable to require that the `Host:` field of the HTTP request match a protected hosts entry in order to match the allowed method exception. Also configure *Host*. |

| | |
|---|---|
| **URL Pattern** | Depending on your selection in *Type*, type either:<br>• the literal URL, such as `/index.php`, that is an exception to the generally allowed HTTP request methods. The URL must begin with a slash ( / ).<br>• a regular expression, such as `^/*.php`, matching all and only the URLs which are exceptions to the generally allowed HTTP request methods. The pattern is ***not*** required to begin with a slash ( / ). However, it must at least match URLs that begin with a slash, such as `/index.cfm`.<br>For example, if multiple URLs on a host have identical HTTP request method requirements, you would type a regular expression matching all of and only those URLs.<br>When you have finished typing the regular expression, click the >> button. A pop-up window will appear that enables you to validate the expression and verify that it matches the parameters. When you have finished testing the expression, click *OK* to return to configuring the allowed method exception.<br>Do not include the name of the web host, such as `www.example.com`, which is configured separately in the *Host* drop-down list. |
| **Type** | Select whether *URL Pattern* is a *Simple String* (that is, a literal URL) or a *Regular Expression*. |
| **Allow Method Exception** | Mark the check boxes for all HTTP request methods that you want to allow, such as:<br>• **GET**<br>• **POST**<br>• **HEAD**<br>• **OPTIONS**<br>• **TRACE**<br>• **CONNECT**<br>• **DELETE**<br>• **PUT**<br>• **OTHERS**<br>**Note:** If a *WAF Auto Learning Profile* will be selected in the policy with an offline protection profile that uses this allowed method exception, you must enable the HTTP request methods that will be used by sessions that you want the FortiWeb unit to learn about. If a method is disabled, the FortiWeb unit will reset the connection, and therefore will not be able to learn about the session. |

6 Repeat the previous step for each individual rule that you want to add to the allowed method exception.

7 If you need to modify an individual rule, click its *Edit* icon. To remove an individual rule from the black list rule, click its *Delete* icon. To remove all individual rules from the black list rule, click the *Clear* icon.




8 Click *OK*.

To apply the allowed method exception, select it in an inline or offline protection profile. For details, see "Configuring inline web protection profiles" on page 213 or "Configuring offline protection profiles" on page 219.

# Configuring hidden field rules

*Web Protection* > *Hidden Fields Protection* > *Hidden Fields Rule* displays the list of hidden field rules.

Hidden form inputs, like other types of parameters and inputs, can be vulnerable to tampering and can be used as a vector for other attacks.

Unlike other inputs, they are often written into an HTML page by the web server when it serves that page to the client, and are not visible on the rendered web page. As such, they are difficult to unintentionally modify, and are sometimes perceived as relatively safe.

Like other inputs, however, they are accessible through the JavaScript document object model (DOM), and as inputs, can be used to inject invalid data into your databases or attempt to tamper with the session state.

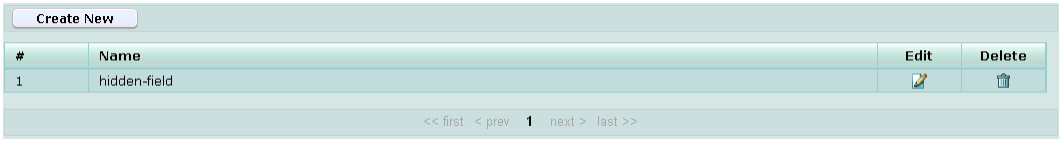
Hidden field rules prevent such tampering by caching the values of a session's hidden inputs as they pass to the HTTP client, and verifying that they remain unchanged when the HTTP client submits a form.

Hidden field constraints are applied indirectly, by first grouping them into a hidden field group. For details, see "Grouping hidden field rules" on page 197.

Unlike visible inputs, hidden field rules are for hidden inputs only. For information on constraining ***visible*** inputs, see "Configuring input rules" on page 152.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 77:** *Hidden Fields Rule* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a hidden field constraint. |
| **#** | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Edit** | Click *Edit* to modify the entry. For details, see "Configuring hidden field rules" on page 194. |
| **Delete** | Click *Delete* to remove the entry. |

### To configure a hidden field rule

Before you configure a hidden field rule, if you want to apply it only to HTTP requests for a specific real or virtual host, you must first define the web host in a protected hosts group. For details, see "Configuring protected hosts" on page 113.

1. Go to *Web Protection* > *Hidden Fields Protection* > *Hidden Fields Rule*.
2. Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.
3. In *Name*, type the name of the hidden field constraint.

   This field cannot be modified if you are editing an existing hidden field rule. To modify the name, delete the entry, then recreate it using the new name.

**4** Configure the following:

| *Name of the GUI item* | *Description* |
|---|---|
| **Host status** | Enable if you want the hidden field rule to apply only to HTTP requests for a specific web host. Also configure *Host*. |
| **Host** | Select the name of a protected host that the `Host:` field of an HTTP request must be in order to match the hidden field rule.<br>This option is available only if *Host status* is enabled. |
| **Request URL** | Type the exact URL that contains the hidden form for which you want to create a hidden field rule.<br>The URL must begin with a slash ( / ). Do not include the name of the web host, such as `www.example.com`, which is configured separately in the *Host* drop-down list. |
| **Action** | Select which action the FortiWeb unit will take when it detects tampering with a hidden field.<br>• **Alert**: Accept the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>• **Alert & Deny**: Block the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>• **Redirect**: Redirect the request to the URL that you specify in the protection profile and generate an alert and/or log message. For details, see "Configuring logging and alerts" on page 252 and "Redirect URL" on page 219.<br>• **Send 403 Forbidden**: Reply with an HTTP 403 (Access Forbidden) error message and generate an alert and/or log message. For details, see "Configuring logging and alerts" on page 252.<br>**Note:** If a *WAF Auto Learning Profile* will be selected in the policy with profiles that use this rule, you should select *Alert*. If the *Action* is *Alert & Deny*, the FortiWeb unit will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. |

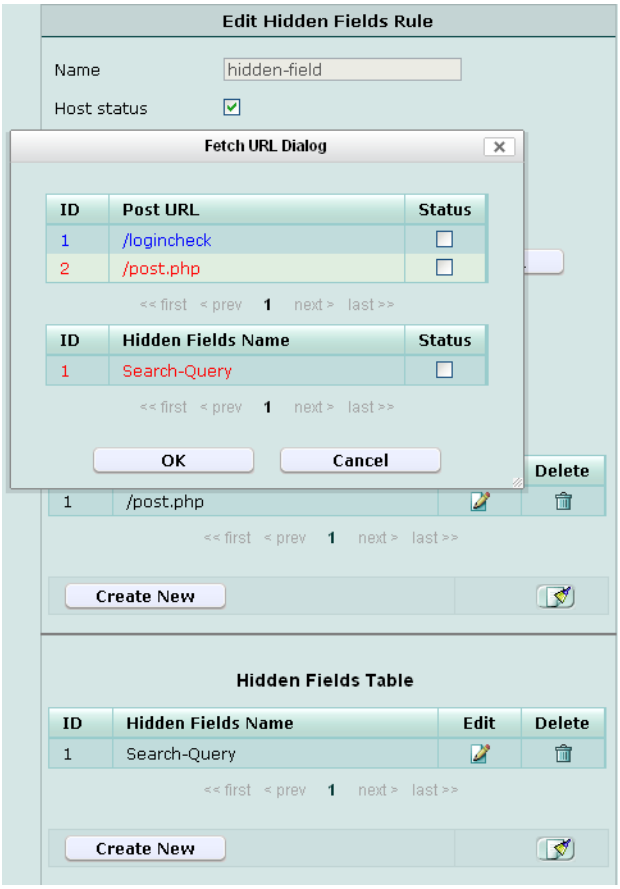
**5** Click *OK*.

**6** Click *Fetch URL*, and then enter the following information in the dialog:

| *Name of the GUI item* | *Description* |
|---|---|
| **Pserver** | Select the IP address of the physical server on which the hidden field is hosted. |
| **Port** | Type the TCP port number on which the physical server listens for HTTP connections. |

7 Click *Fetch URL* in the dialog to retrieve the web page you specified in *Request URL*, and display a list of hidden inputs contained by forms on that web page, and the URLs to which their inputs will be posted when a client submits the form.

A dialog appears, displaying a list of hidden inputs that the FortiWeb unit found in that web page, and the URLs to which those hidden inputs will be posted when a client submits the form.




Entries in the list are color-coded by the recommended course of action:

- **Blue**: The URL/hidden field exists in the requested URL, but you have ***not*** yet configured it in the hidden field rule.You may want to add it to the hidden field rule.
- **Red**: The URL/hidden field does ***not*** exist in the requested URL, yet it is currently configured in the hidden field rule. You may want to remove it from the hidden field rule.
- **Black**: The URL/hidden field exists in both the requested URL and your hidden field rule.

8 For each entry that you want to be in the hidden field rule, in the *Status* column, mark its check box.

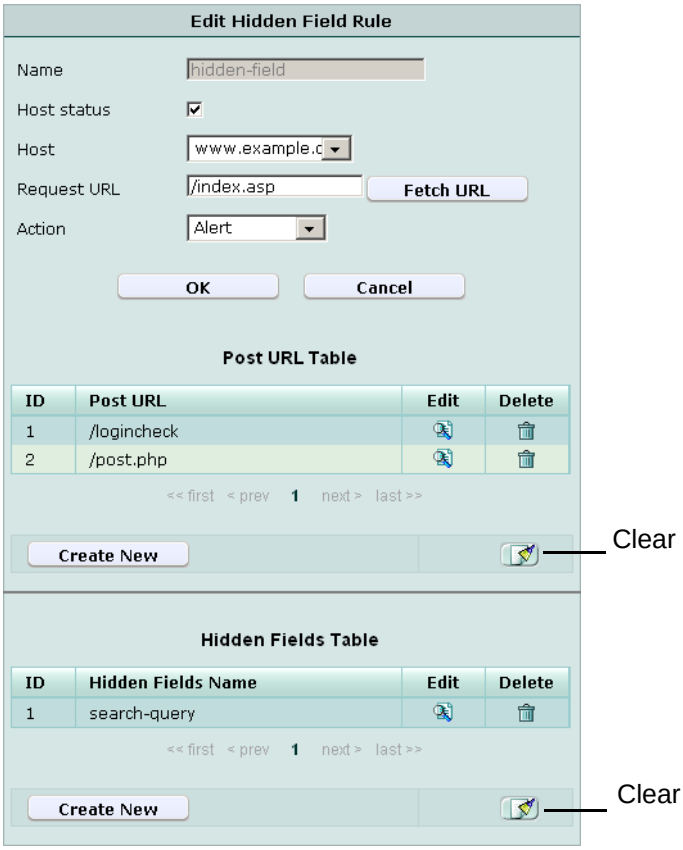
**Note:** In addition to new items, mark the check boxes of any previously configured items that you want to keep in the hidden field rule. If you do not, they will be deleted.

9 Click *OK*.

10 If there are any additional hidden fields or post URLs that you want to manually add to the hidden field rule, click *Create New*, then enter the name of the post URL or hidden field.

11 Repeat the previous step for each post URL or hidden field that you want to manually add to the hidden field rule.

12 If you need to modify an individual rule, click its *Edit* icon. To remove an individual rule from the hidden field rule, click its *Delete* icon. To remove all individual rules from the hidden field rule, click the *Clear* icon.




13 Click *OK*.

To apply the hidden field rule, select it in a hidden field group. For details, see "Grouping hidden field rules" on page 197.

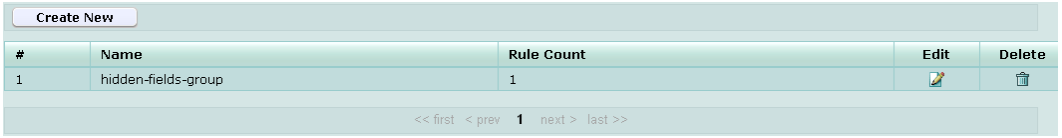
## Grouping hidden field rules

*Web Protection* > *Hidden Fields Protection* > *Hidden Fields Protection* displays the list of hidden field constraint groups.

Hidden field constraint groups are applied by selecting them within an inline protection profile. For details, see "Configuring inline web protection profiles" on page 213.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 78:** *Hidden Fields Protection* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a hidden field group. |
| # | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Rule Count** | The number of individual rules contained in the entry. |
| (No column heading.) | Click *Delete* to remove the entry.<br>Click *Edit* to modify the entry. |

### To configure a hidden field group

Before you configure a hidden field group, you must first define one or more hidden field rules. For details, see "Configuring hidden field rules" on page 194.

1 Go to *Web Protection* > *Hidden Fields Protection* > *Hidden Fields Protection*.

2 Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.

3 In *Name*, type the name of the hidden field group.

This field cannot be modified if you are editing an existing hidden field group. To modify the name, delete the entry, then recreate it using the new name.

4 Click *OK*.

5 Click *Create New*, then select the name of a hidden field rule.

6 Repeat the previous step for each individual rule that you want to add to the hidden field group.

7 If you need to modify an individual rule, click its *Edit* icon. To remove an individual rule from the hidden field group, click its *Delete* icon. To remove all individual rules from the hidden field group, click the *Clear* icon.


8 Click *OK*.

To apply the hidden field group, select it in an inline protection profile. For details, see "Configuring inline web protection profiles" on page 213.

**Note:** In order for hidden field groups to be enforced, you must also enable "Session Management" on page 216 in the inline protection profile.

# Configuring URL rewriting

*Web Protection* > *URL Rewriting* > *URL Rewriting Rule* displays the list of URL rewriting rules.

URL rewriting rules can:

- rewrite the URL line in the HTTP header
- rewrite the `Referer:` field in the HTTP header
- redirect requests to another web site

Similar to error message cloaking, URL rewriting can be useful to prevent the disclosure of underlying technology or web site structures to HTTP clients.

For example, when visiting a blog web page, its URL might be:

```
http://www.example.com/wordpress/?feed=rss2
```

Simply knowing the file name, that the blog uses PHP, its compatible database types, and the names of parameters via the URL could help an attacker to craft an appropriate attack for that platform. By rewriting the URL to something more human-readable and less platform-specific, we hide these details:

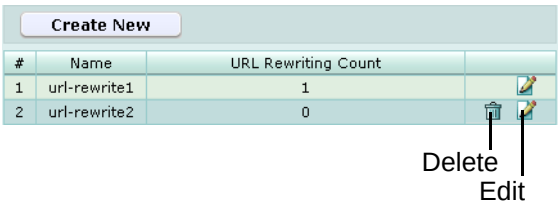
```
http://www.example.com/rss2
```

**Note:** URLs in the HTML body are ***not*** rewritten.

**Note:** URL rewrites are applicable only if the FortiWeb unit is operating in inline protection mode, or transparent mode for connections *without* SSL.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 79:** *URL Rewriting Rule* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a URL rewriting rule. |
| # | The index number of the entry in the list. |
| **Name** | The name of the entry. |

| | |
|---|---|
| **URL Rewriting Count** | The number of URL rewriting conditions contained in the entry. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a URL rewriting set.<br>Click *Edit* to modify the entry. |

### To configure a URL rewrite

1 Go to *Web Protection* > *URL Rewriting* > *URL Rewriting Rule*.

2 Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.

3 In *Name*, enter the name of the URL rewriting rule.

This field cannot be modified if you are editing an existing URL rewriting rule. To modify the name, delete the entry, then recreate it using the new name.

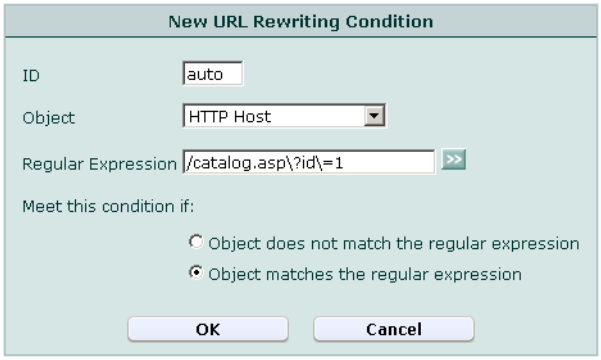
4 From *Action*, select which of the following actions the FortiWeb unit will take when it receives a matching request.

- *Rewrite URL*: Rewrite both the `Host:` and request URL fields in HTTP header.
- *Rewrite Referer*: Rewrite `Referer:` field in HTTP header.
- *Redirect*: Send a 302 (Moved Temporarily) response to the client, with a new `Location:` field in the HTTP header.
- *Send 403 Forbidden*: Send a 403 (Forbidden) response to the client.

5 Click *OK*.

6 Click *Create New*.

7 Configure the following and click *OK*:

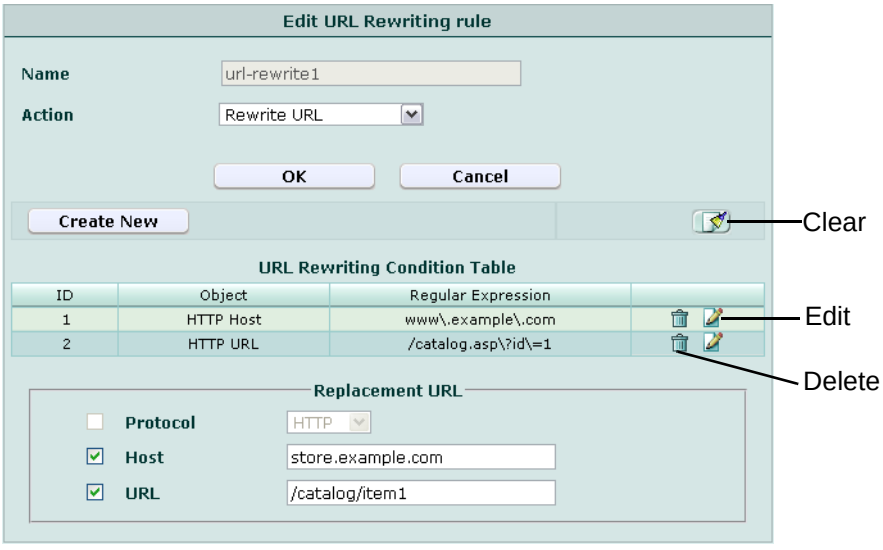



| ***Name of the GUI item*** | ***Description*** |
|---|---|
| **ID** | Type the index number of the individual entry in the URL rewriting condition table. The index number is an identifier only, and does not affect the display order or match order.<br>The number must be between 1 and 99,999 and must be unique for each entry. |
| **Object** | Select which part of the HTTP request will be tested for a match:<br>• **HTTP Host**<br>• **HTTP Request URL**<br>• **HTTP Referer**<br>If the request must meet multiple conditions (for example, it must contain both a matching `Host:` field and a matching URL), add each object match condition to the condition table separately. |

| | |
|---|---|
| **If no Referer field in HTTP header** | Select either:<br>• **Do not meet this condition**<br>• **Meet this condition**<br>Requests can lack a `Referer:` field for several reasons, such as if the user manually types the URL, and the request does not result from a hyperlink from another web site, or if the URL resulted from an HTTPS connection. (See the RFC 2616 section on the `Referer:` field.) In those cases, the field cannot be tested for a matching value.<br>This option appears only if *Object* is *HTTP Referer*. |
| **Regular Expression** | Depending on your selection in *Object* and *Meet this condition if*, type a regular expression that defines either all matching or all non-matching `Host:` fields, URLs, or `Referer:` fields. Then, also configure *Meet this condition if*.<br>For example, for the URL rewriting rule to match all URLs that begin with `/wordpress`, you could enter `^/wordpress`, then, in *Meet this condition if*, select *Match this condition*.<br>The pattern is ***not*** required to begin with a slash ( / ).<br>When you have finished typing the regular expression, click the >> button. A pop-up window will appear that enables you to validate the expression and verify that it matches the URLs or substrings that you expect. When you have finished testing the expression, click *OK* to return to configuring the URL rewriting condition. |
| **Meet this condition if** | Indicate how to use *Regular Expression* when determining whether or not this URL rewriting condition has been met.<br>• **Object does not match the regular expression**: If the regular expression does ***not*** match the request object, the condition is met.<br>• **Object matches the regular expression**: If the regular expression ***does*** match the request object, the condition is met.<br>If all conditions are met, the FortiWeb unit will do your selected *Action*. |

8 Repeat the previous step for each condition that you want to add to the URL rewriting rule.

9 If you need to modify an individual condition, click its *Edit* icon. To remove an individual condition from the URL rewriting rule, click its *Delete* icon. To remove all individual conditions from the URL rewriting rule, click the *Clear* icon.




10 If *Action* is ***not*** *Send 403 Forbidden*, configure the following options in the *Replacement URL* section.

If a check box is available but you do not configure it, the FortiWeb unit will preserve the value from the client's request when rewriting it.

| | |
|---|---|
| **Protocol** | Select the protocol that will be used in the URL when redirecting or rewriting the `Referer:` field in the HTTP header.<br>This option is available only if *Action* is *Redirect* or *Rewrite Referer*. |
| **Host** | Type the name of the host, such as `store.example.com`, to which the request will be redirected.<br>This field supports back references such as `$0` to the parts of the original request that matched any capture groups that you entered in *Regular Expression* for each object in the condition table. (A capture group is a regular expression, or part of one, surrounded in parentheses.)<br>Use $***n*** (0 <= ***n*** <= 9) to invoke a sub-string, where ***n*** is the order of appearance of the regular expression, from left to right, from outside to inside, then from top to bottom.<br>For example, regular expressions in the condition table in this order:<br>(a)(b)(c(d))(e)(f)<br>would result in invokable variables with the following values:<br>• `$0`: a<br>• `$1`: b<br>• `$2`: cd<br>• `$3`: d<br>• `$4`: e<br>• `$5`: f<br>For an example, see "Example: Rewriting URLs using variables" on page 204. |
| **URL** | Type the string, such as `/catalog/item1`, that will replace the request URL.<br>Do not include the name of the web host, such as `www.example.com`, nor the protocol, which are configured separately in the *Host* field and *Protocol*, respectively.<br>Like *Host*, this field supports back references such as `$0` to the parts of the original request that matched any capture groups that you entered in *Regular Expression* for each object in the condition table.<br>For an example, see "Example: Rewriting URLs using variables" on page 204. |

**11** Click *OK*.

To apply the URL rewrite rule, you must first group it. For details, see "Grouping URL rewriting rules" on page 202.

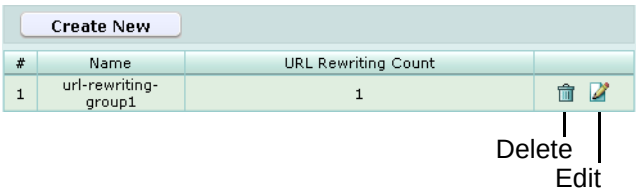
## Grouping URL rewriting rules

*Web Protection* > *URL Rewriting* > *URL Rewriting* displays the list of URL rewriting groups.

URL rewriting groups are applied by selecting them within an inline protection profile. For details, see "Configuring inline web protection profiles" on page 213.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 80:** *URL Rewriting* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a URL rewriting group. |

| | |
|---|---|
| # | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **URL Rewriting Count** | The number of individual rules contained in the entry. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in an inline protection profile.<br>Click *Edit* to modify the entry. |

### To group URL rewriting rules

Before you can configure a URL rewriting group, you must first configure any URL rewriting rules that you want to include. For details, see "Configuring URL rewriting" on page 199.

1 Go to *Web Protection* > *URL Rewriting* > *URL Rewriting*.

2 Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.

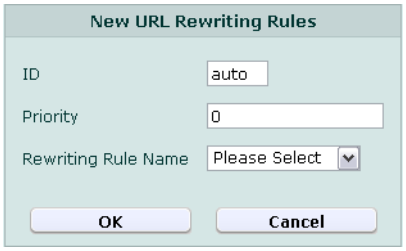
3 In *Name*, enter the name of the URL rewriting group.

This field cannot be modified if you are editing an existing URL rewriting group. To modify the name, delete the entry, then recreate it using the new name.

4 Click *OK*.

5 Click *Create New*.

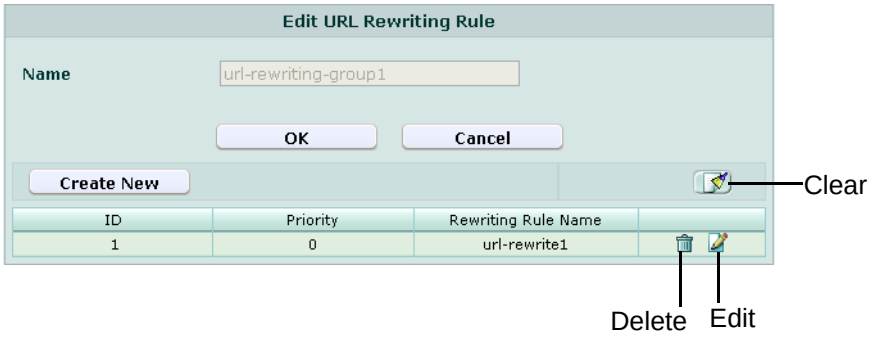
6 Configure the following and click *OK*:




| ***Name of the GUI item*** | ***Description*** |
|---|---|
| **ID** | Type the index number of the entry, or keep the field's default value of `auto` to let the FortiWeb unit automatically assign the next available index number.<br>The number must be between 1 and 99,999 and must be unique for each entry in the group. |
| **Priority** | Type the order of evaluation for this rule in the group, starting from 0.<br>To create an entry with the highest match priority, enter `0`. For lower-priority matches, enter larger numbers.<br>**Note:** Rule order affects URL rewriting rule matching and behavior. The search begins with the smallest *Priority* number (greatest priority) rule in the list and progresses in order towards the largest number in the list. Matching rules are determined by comparing the rule and the connection's content. If no rule matches, the connection remains unchanged.<br>When the FortiWeb unit finds a matching rule, it applies the matching rule's specified actions to the connection. |
| **Rewriting Rule Name** | Select the name of a URL rewriting rule that you want to include in the group. |

7 Repeat the previous step for each individual rule that you want to add to the URL rewriting group.

8 If you need to modify an individual rule, click its *Edit* icon. To remove an individual rule from the URL rewriting group, click its *Delete* icon. To remove all individual rules from the URL rewriting group, click the *Clear* icon.




9 Click *OK*.

To apply the URL rewriting group, select it in an inline protection profile. For details, see “Configuring inline web protection profiles” on page 213.

## Example: Rewriting URLs using regular expressions

Example.edu is a large university. Professors of example.edu use a mixture of WordPress and Movable Type software for their course web pages to keep students updated. In addition, the campus bookstore and software store use custom shopping cart software. The URLs of all of these web applications contain clues about the underlying vendors, databases and scripting languages.

Because it is a large organization with many mobile users and guests, and an Internet connection with large bandwidth, the university is therefore a frequent target of attacks. Its network administrators want to hide the underlying technology to make it more difficult for attackers to craft platform-specific attacks. Example.edu also wants to make clients’ bookmarked URLs more permanent, so that clients will not need to repair them if the university switches software vendors.

Because it has so many URLs, the university uses regular expressions to rewrite sets of similar URLs, rather than configuring rewrites for each URL individually. More specific URL rewrite rules are selected first in the URL rewriting group, before general ones, due to the affects of match order on which rewrite rule is applied.

**Table 81: Example URL rewrites using regular expressions**

| *Regular Expression* **in URL match condition** | *URL* | **Example URL in client’s request** | **Result** |
|---|---|---|---|
| ^/cgi/python/ustore/payment.html$ | /store/checkout | /cgi/python/ustore/payment.html | /store/checkout |
| ^/ustore*$ | /store/view | /ustore/viewItem.asp?id=1&img=2 | /store/view |
| /Wordpress/(.*) | /blog/$0 | /wordpress/10/11/24 | /blog/10/11/24 |
| /(.*)\.xml | /$0 | /index.xml | /index |

## Example: Rewriting URLs using variables

Example.com has a web site that uses ASP, but the administrator wants it to appear that the web site uses PHP. To do this, she configures a rule that changes any requested file's suffix which is ".asp" into ".php".

The condition table contains two match conditions, in this order:

1 The `Host:` may be anything.

2 The request URL must end in ".asp".

If both of those are true, the request is rewritten.

The administrator does not want to rewrite matching requests into a single URL. Instead, she wants each rewritten URL to re-use parts of the original request.

To assemble the rewritten URL by re-using the original request's file path and `Host:`, the administrator uses two variables: `$0` and `$1`. Each variable refers to a part of the original request. The parts are determined by which capture group was matched in the *Regular Expression* of each condition table object.

- `$0`: The text that matched the ***first*** capture group `(.*)`. In this case, because the object is the `Host:` field, the matching text is the host name, `www.example.com`.
- `$1`: The text that matched the ***second*** capture group, which is also `(.*)`. In this case, because the object is the request URL, the matching text is the file path, `news/local`.

**Table 82: Example URL rewrite using regular expressions and variables**

| Example request | URL Rewriting Condition Table | | Replacement URL | | Result |
|---|---|---|---|---|---|
| www.example.com | *HTTP Host* | (.*) | *Host* | $0 | www.example.com |
| /news/local.asp | *HTTP URL* | /(.*)\.asp | *URL* | /$1.php | /news/local.php |

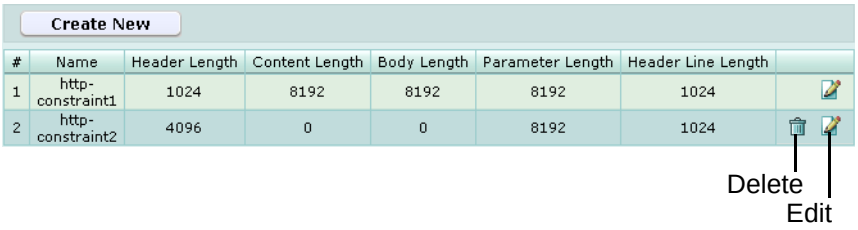
# Configuring HTTP protocol constraints

*Web Protection* > *HTTP Protocol Parameter* > *HTTP Protocol Parameter* displays the list of HTTP protocol constraints.

HTTP protocol constraints can be used to prevent vulnerability to attacks such as buffer overflows in web servers that do not restrict elements of the HTTP protocol, such as its header lines, to acceptable lengths.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 83:** *HTTP Protocol Parameter* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add an HTTP protocol constrains. |
| # | The index number of the entry in the list. |
| **Name** | The name of the entry. |

| | |
|---|---|
| **Header Length** | The maximum acceptable length in bytes of the HTTP header. |
| **Content Length** | The maximum acceptable length in bytes of the request body. Length is determined by comparing this limit with the value of the `Content-Length:` field in the HTTP header. |
| **Body Length** | The maximum acceptable length in bytes of the HTTP body. |
| **Parameter Length** | The maximum acceptable length in bytes of parameters in the URL or, for HTTP `POST` requests, HTTP body. Question mark ( ? ), ampersand ( & ), and equal ( = ) characters are not included. |
| **Header Line Length** | The maximum acceptable length in bytes of each line in the HTTP header. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in an inline or offline protection profile.<br>Click *Edit* to modify the entry. |

### To configure an HTTP protocol constraint

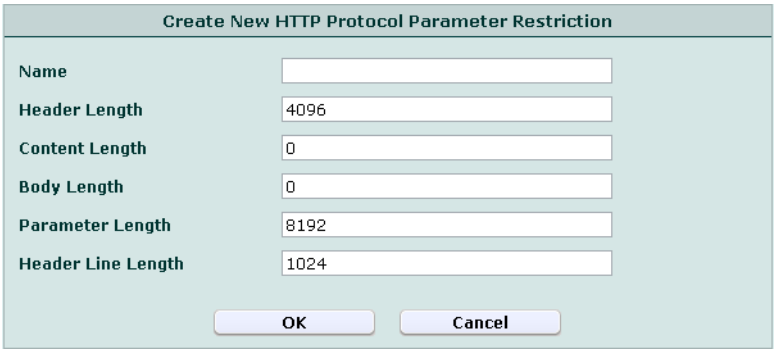
1 Go to *Web Protection* > *HTTP Protocol Parameter* > *HTTP Protocol Parameter*.

2 Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.

3 In *Name*, type the name of the protocol constraint.

This field cannot be modified if you are editing an existing protocol restraint. To modify the name, delete the entry, then recreate it using the new name.

4 Configure the following:




| *Name of the GUI item* | *Description* |
|---|---|
| **Header Length** | Type the maximum acceptable length in bytes of the HTTP header.<br>To disable the limit, type `0`. |
| **Content Length** | Type the maximum acceptable length in bytes of the request body. Length is determined by comparing this limit with the value of the `Content-Length:` field in the HTTP header.<br>To disable the limit, type `0`. |
| **Body Length** | Type the maximum acceptable length in bytes of the HTTP body.<br>To disable the limit, type `0`. |
| **Parameter Length** | Type the maximum acceptable length in bytes of parameters in the URL or, for HTTP `POST` requests, HTTP body. Question mark ( ? ), ampersand ( & ), and equal ( = ) characters are not included.<br>To disable the limit, type `0`. |
| **Header Line Length** | Type the maximum acceptable length in bytes of each line in the HTTP header.<br>To disable the limit, type `0`. |

5 Click *OK*.

To apply the HTTP protocol constraint, select it in an inline or offline protection profile. For details, see “Configuring inline web protection profiles” on page 213 or “Configuring offline protection profiles” on page 219.

# Configuring HTTP authentication

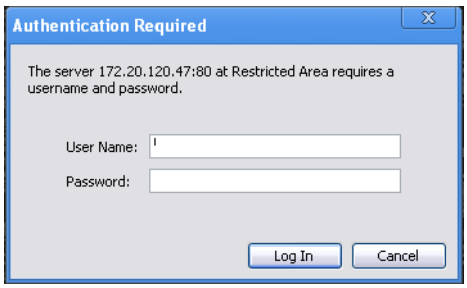
Even if a web site does not support RFC 2617 HTTP authentication on its own, nor have a web application that provides HTML form-based authentication, you can use a FortiWeb unit to require that HTTP clients authenticate before they are permitted to access a web page or web site.

When HTTP authentication is configured:

1 If the client’s initial request does not already include an `Authorization:` field in its HTTP header, the FortiWeb unit replies with an HTTP 401 (Authorization Required) response. The response includes a `WWW-Authenticate:` field in the HTTP header that indicates which style of authentication to use (basic, digest, or NTLM) and the name of the realm (usually the name, such as “Restricted Area”, of a set of URLs that can be accessed using the same set of credentials).

The browser then prompts its user to enter a user name and password. (The prompt may include the name of the realm, in order to indicate to the user which login is valid.) The browser includes these in the `Authorization:` field of the HTTP header when repeating its request.

**Figure 17: An HTTP authentication prompt in the Google Chrome browser**




Valid user name formats vary by the authentication server. For example:

- For a local user, enter a user name in the format `username`.
- For LDAP authentication, enter a user name in the format required by the directory’s schema.
- For NTLM authentication, enter a user name in the format `DOMAIN/username`.

2 The FortiWeb unit compares the supplied credentials to:

- the locally defined set of user accounts
- a set of user objects on a lightweight directory access protocol (LDAP) directory
- user accounts on an NT LAN Manager (NTLM) server

3 If the client authenticates successfully, the FortiWeb unit forwards the original request to the server. If the client does ***not*** authenticate successfully, the FortiWeb unit repeats its HTTP 401 response to the client, asking again for valid credentials.

4 Once the client has authenticated with the FortiWeb unit, if the server applies no other restrictions and the resource is found, it returns the requested resource to the client.

5 If the client's browser is configured to do so, it can cache the realm along with the supplied credentials, automatically re-supplying the user name and password for each request with a matching realm. This provides convenience to the user. Otherwise, the user would have to re-enter their user name and password for every request.

**Caution:** Advise users to clear their cache and close their browser after an authenticated session to ensure that no one else can access the web site using their credentials. Browsers often cache credentials until manually cleared, or until cleared automatically by closing a browser tab or window. This is because, without a web application with its own notion of sessions, the HTTP protocol itself is essentially stateless, it relies only on these cached credentials, and there is no other way to log out.

**Caution:** HTTP authentication is not secure. All user names and data (and, depending on the authentication style, passwords) are sent in clear text. If you require encryption and other security features in addition to authorization, use HTTP authentication with SSL/TLS.

**Tip:** Alternatively or in addition to HTTP authentication, with SSL connections, you can require that clients present a valid personal certificate. For details, see "Certificate Verification" on page 100.

In general, to configure HTTP authentication, you must:

1 Configure local user accounts or LDAP or NTLM user queries. (See "Configuring local users" on page 83, "Configuring LDAP user queries" on page 84, or "Configuring NTLM user queries" on page 87.)

2 Group user accounts or queries. (See "Grouping users" on page 88.)

3 Configure an authentication rule to select the set of URLs that is the authentication realm, the authorization type, and associate a user group. (See "Configuring authentication rules" on page 208.)

4 Group sets of authentication rules into authentication policies. (See "Grouping authentication rules into authentication policies" on page 211.)

5 Select the authentication policy in an inline protection profile that is used by a policy. (See "Configuring inline web protection profiles" on page 213.)

## Configuring authentication rules

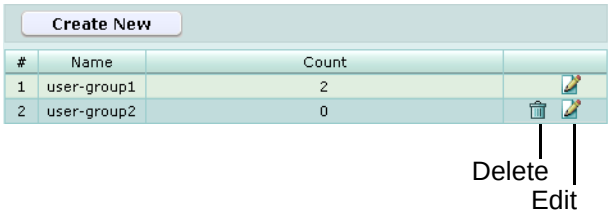
*Web Protection* > *Authentication Policy* > *Authentication Rules* displays the list of authentication rules.

Authentication rules are used by the HTTP authentication feature to define sets of request URLs that will be authorized for each user group.

Authentication rules are used indirectly, by selecting them within an authentication policy, which is ultimately selected within an inline protection profile. For details, see "Grouping authentication rules into authentication policies" on page 211.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 84:** *Authentication Rules* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add an authentication rule. |
| # | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Count** | The number of individual rules contained in the entry. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in an authentication policy.<br>Click *Edit* to modify the entry. |

### To configure an authentication rule

Before you can configure an authentication rule set, you must first configure any user groups that you want to include. For details, see "Grouping users" on page 88.

If you want to apply it only to HTTP requests for a specific real or virtual host, you must also first define the web host in a protected hosts group. For details, see "Configuring protected hosts" on page 113.

1 Go to *Web Protection* > *Authentication Policy* > *Authentication Rules*.

2 Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.

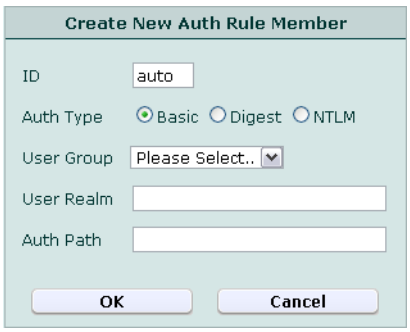
3 In *Name*, type the name of the authentication rule.

This field cannot be modified if you are editing an existing entry. To modify the name, delete the entry, then recreate it using the new name.

4 If you want to require that the `Host:` field of the HTTP request match a protected hosts entry in order to match the HTTP authentication rule, enable *Host Status*, then, from *Host*, select which protected hosts entry (either a web host name or IP address) the `Host:` field of the HTTP request must be.

5 Click *OK*.

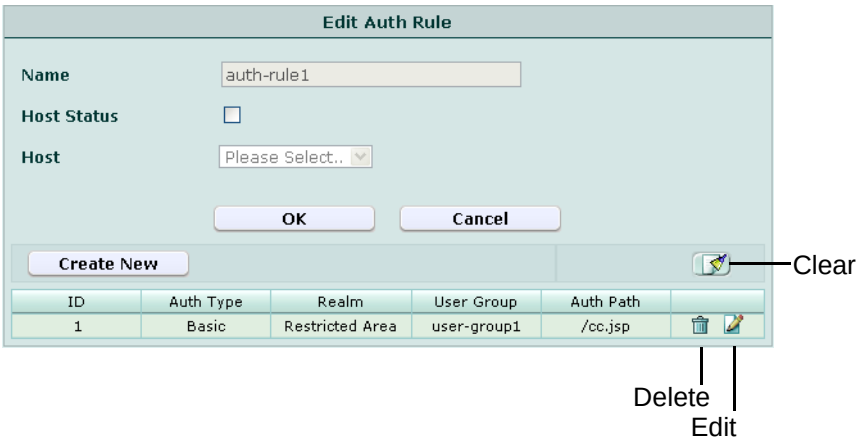
6 Click *Create New*, then configure the following:



| *Name of the GUI item* | *Description* |
|---|---|
| **ID** | Type the index number of the individual rule within the group of authentication rules, or keep the field's default value of `auto` to let the FortiWeb unit automatically assign the next available index number. |
| **Auth Type** | Select which type of HTTP authentication to use, either:<br>• **Basic**: Clear text, Base64-encoded user nameand password. NTLM user queries are not supported, and will be ignored if any are in the user group.<br>• **Digest**: Hashed user name, realm, and password. LDAP and NTLM user queries are not supported, and will be ignored if any are in the user group.<br>• **NTLM**: Encrypted user name and password. Local user accounts and LDAP user queries are not supported, and will be ignored if any are in the user group.<br>For more information on available user types, see "User Type" on page 89. |
| **User Group** | Select the name of a user group that is authorized to use the URL in *Auth Path*. |
| **User Realm** | Type the realm, such as `Restricted Area`, to which the *Auth Path* belongs.<br>The realm is often used by users' browsers.<br>• It may appear in the browser's prompt for the user's credentials. Especially if a user has multiple logins, and only one login is valid for that specific realm, displaying the realm helps to indicate which user name and password should be supplied.<br>• After authenticating once, the browser may cache the authentication credentials for the duration of the browser session. If the user requests another URL from the same realm, the browser often will automatically re-supply the cached user name and password, rather than asking the user to enter them again for each request.<br>The realm may be the same for multiple authentication rules, if all of those URLs permit the same user group to authenticate.<br>For example, the user group `All_Employees` could have access to the *Auth Path* URLs `/wiki/Main` and `/wiki/ToDo`. These URLs both belong to the realm named `Intranet Wiki`. Because they use the same realm name, users authenticating to reach `/wiki/Main` usually will not have to authenticate again to reach `/wiki/ToDo`, as long as both requests are within the same browser session.<br>This field does not appear if *Auth Type* is *NTLM*, which does not support HTTP-style realms. |
| **Auth Path** | Type the literal URL, such as `/employees/holidays.html`, that a request must match in order to trigger HTTP authentication. |

7 Repeat the previous step for each individual rule that you want to add to the group of authentication rules.

8 If you need to modify an individual rule, click its *Edit* icon. To remove an individual rule from the group of authentication rules, click its *Delete* icon. To remove all individual rules from the group of authentication rules, click the *Clear* icon.




9 Click *OK*.

To apply the authentication rule, select it in an authentication policy. For details, see "Grouping authentication rules into authentication policies" on page 211.

## Grouping authentication rules into authentication policies

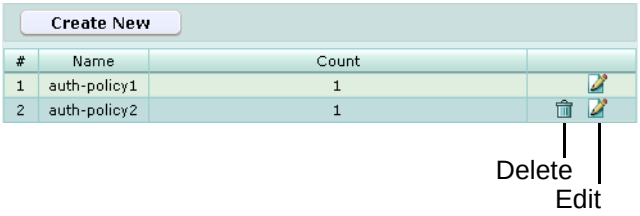
*Web Protection* > *Authentication Policy* > *Authentication Policy* displays the list of HTTP authentication policies.

Authentication policies are used by the HTTP authentication feature to authorize HTTP requests. For details, see "Configuring HTTP authentication" on page 207.

HTTP authentication policies are used by selecting them in an inline protection profile. For details, see "Configuring inline web protection profiles" on page 213.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "About permissions" on page 58.

**Table 85:** *Authentication Policies* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add an authentication policy. |
| # | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Count** | The number of individual rules contained in the entry. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in an inline protection profile.<br>Click *Edit* to modify the entry. |

### To configure an authentication policy

Before you can configure an authentication policy, you must first configure any authentication rules that you want to include. For details, see "Configuring authentication rules" on page 208.

1 Go to *Web Protection* > *Authentication Policy* > *Authentication Policy*.

2 Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.

3 In *Name*, type the name of the authentication policy.

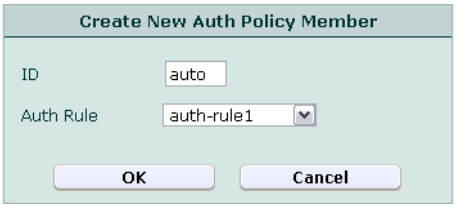
This field cannot be modified if you are editing an existing entry. To modify the name, delete the entry, then recreate it using the new name.

4 If you want to enable LDAP query result caching, click *LDAP Cache*.

5 If *LDAP Cache* is enabled, you can change the *LDAP Cache Timeout* value.

6 Click *OK*.

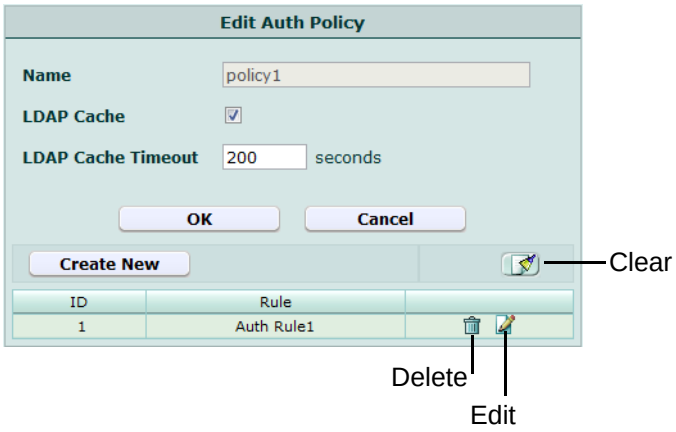
7 Click *Create New*, then configure the following:




| *Name of the GUI item* | *Description* |
|---|---|
| **ID** | Type the index number of the individual rule within the authentication policy, or keep the field's default value of `auto` to let the FortiWeb unit automatically assign the next available index number. |
| **Auth Rule** | Select the name of an authentication rule set. |

8 Repeat the previous step for each individual rule that you want to add to the authentication policy.

9 If you need to modify an individual rule, click its *Edit* icon. To remove an individual rule from the authentication policy, click its *Delete* icon. To remove all individual rules from the authentication policy, click the *Clear* icon.



**10** Click *OK*.

To apply the authentication policy, select it in an inline protection profile. For details, see “Configuring inline web protection profiles” on page 213.

# Configuring inline web protection profiles

*Web Protection* > *Web Protection Profile* > *Inline Protection Profile* displays the list of web protection profiles that can be used with policies when the FortiWeb unit is operating in inline protection mode or transparent mode.

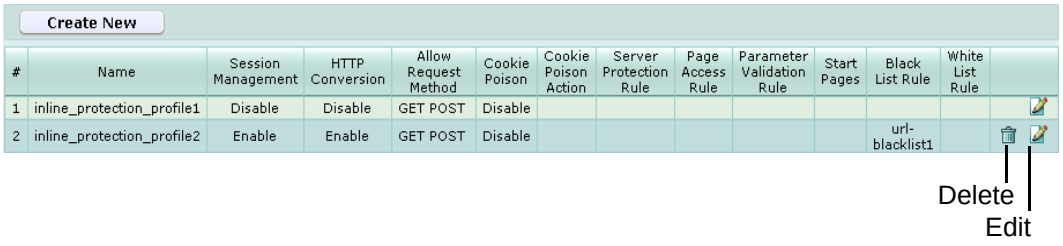
Protection profiles are a set of attack protection and other settings. When a connection matches a policy, the FortiWeb unit applies the protection profile that you have selected for that policy.

Protection profiles are applied by selecting them within a policy. For details, see “Configuring policies” on page 91.

**Note:** Inline web protection profiles can be configured at any time, but can be selected in a policy only while the FortiWeb unit is operating in a mode that supports them. For details, see Table 36, “Policy behavior by operation mode,” on page 92.

To be able to access this part of the web-based manager, in your administrator account’s access profile, you must have both *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see “About permissions” on page 58.

**Table 86:** *Inline Protection Profile* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add an inline protection profile. |
| **#** | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Session Management** | Indicates whether session management by the FortiWeb unit is enabled or disabled. For more information about session management, see “Session Management” on page 216. |
| **HTTP Conversion** | Indicates whether the FortiWeb unit will translate the IP addresses in the `Host:`, `Referer:`, and `Location:` fields of HTTP requests and responses, replacing the virtual server’s IP address with that of the physical server, and vice versa. For details, see “HTTP Conversion” on page 217. |

| | |
|---|---|
| **Allow Request Method** | The names of HTTP request methods that the inline protection profile allows, such as:<br>• **GET**<br>• **POST**<br>• **HEAD**<br>• **OPTIONS**<br>• **TRACE**<br>• **CONNECT**<br>• **DELETE**<br>• **PUT**<br>• **OTHERS** |
| **Cookie Poison** | Indicates whether cookie poisoning prevention is enabled or disabled. |
| **Cookie Poison Action** | The action that the FortiWeb unit will take when cookie poisoning is detected.<br>• **Alert**: Accept the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>• **Alert & Deny**: Block the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>• **Remove Cookie**: Accept the connection, but remove the poisoned cookie from the datagram, preventing it from reaching the web server, and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252. |
| **Server Protection Rule** | The name of the server protection rule that will be applied to matching HTTP requests. For details on server protection rules, see "Configuring server protection rules" on page 161. |
| **Page Access Rule** | The name of the page access rule that will be applied to matching HTTP requests. For details on page access rules, see "Configuring page order rules" on page 158. |
| **Parameter Validation Rule** | The name of the parameter validation rule that will be applied to matching HTTP requests. For details on parameter validation rules, see "Grouping input rules into parameter validation rules" on page 156. |
| **Start Pages** | The name of the start pages that HTTP requests must use in order to initiate a valid session. For details on start pages, see "Configuring start pages" on page 170. |
| **Black List Rule** | The name of the black list rule that will be applied to matching HTTP requests. For details on black list rules, see "Configuring URL black list rules" on page 173. |
| **White List Rule** | The name of the white list rule that will be applied to matching HTTP requests. For details on white list rules, see "Configuring URL white list rules" on page 175. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a policy.<br>Click *Edit* to modify the entry. |

**To configure an inline protection profile**

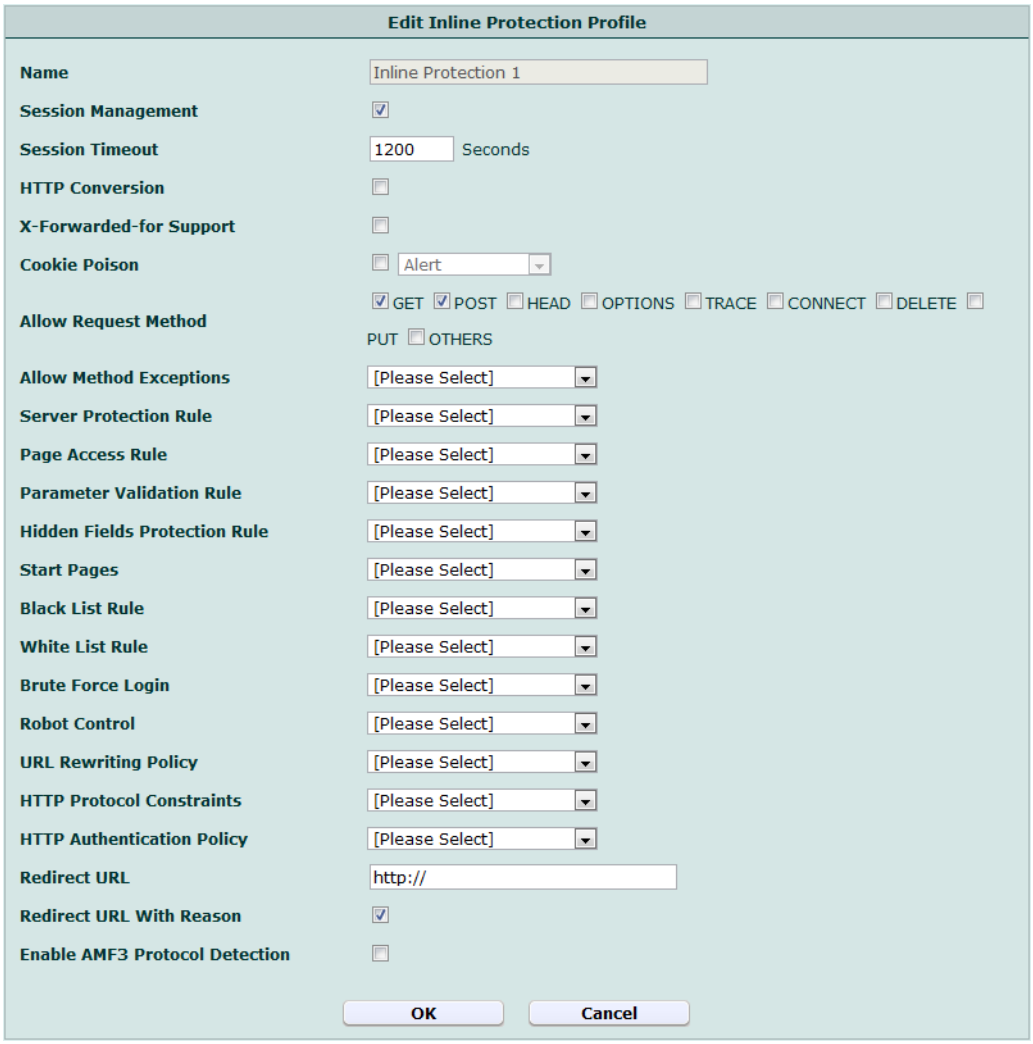
Before configuring an inline protection profile, first configure any of the following that you want to include in the profile:

- a server protection rule (see “Configuring server protection rules” on page 161)
- a page access rule (see “Configuring page order rules” on page 158)
- protected hosts (see “Configuring protected hosts” on page 113)
- a parameter validation rule (see “Grouping input rules into parameter validation rules” on page 156)
- start pages (see “Configuring start pages” on page 170)
- a black list rule (see “Configuring URL black list rules” on page 173)
- a white list rule (see “Configuring URL white list rules” on page 175)
- a brute force login attack sensor (see “Configuring brute force login attack sensors” on page 181)
- a robot control sensor (see “Configuring robot control sensors” on page 184)
- an allowed method exception (see “Configuring allowed method exceptions” on page 191)
- a hidden fields group (see “Grouping hidden field rules” on page 197)
- a URL rewriting rule (see “Configuring URL rewriting” on page 199)
- an HTTP protocol constraint (see “Configuring HTTP protocol constraints” on page 205)
- an HTTP authentication policy (see “Configuring HTTP authentication” on page 207)

1 Go to *Web Protection* > *Web Protection Profile* > *Inline Protection Profile*.

2 Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.

**3** Configure the following:




| *Name of the GUI item* | *Description* |
|---|---|
| **Name** | Type the name of the inline protection profile. This field cannot be modified if you are editing an existing inline protection profile. To modify the name, delete the entry, then recreate it using the new name. |
| **Session Management** | Enable to track the states of HTTP sessions using a cookie named `FORTIWAFSID`. Also configure *Session Timeout*.<br>This feature requires that the client support cookies.<br>**Note:** You ***must*** enable this option:<br>• to enforce the *Start Pages*, *Page Access Rule*, and *Hidden Fields Protection Rule* features, if any of those options are enabled.<br>• if you want to include this profile's traffic in the traffic log, in addition to enabling traffic logs in general. For more information, see "Enabling logging and alerts" on page 253.<br>**Note:** Session management is automatically enabled for policies whose *Load Balancing Algorithm* is *HTTP session based Round Robin*. If only those types of policies use this protection profile, session management will already be enabled, and therefore you do not need to enable this option. |
| **Session Timeout** | Type the HTTP session timeout in seconds.<br>This option appears only if *Session Management* is enabled. |

| | |
|---|---|
| **HTTP Conversion** | Enable to:<br>• For forward traffic from clients, replace the virtual server's IP address in the `Host:` and `Referer:` field in the HTTP header with that of the physical server's IP address.<br>• For reply traffic from servers, including traffic that has been redirected, replace the physical server's IP address in the `Location:` field with that of the virtual server's IP address.<br>This may be useful if your physical servers reject HTTP requests whose `Host:` and `Referer:` field does not match their own IP address. It is also useful if the physical server is behind network address translation (NAT) and redirects requests to its private network IP address, which clients cannot directly access. However, it increases load on the FortiWeb unit, and should not be enabled unless required.<br>**Note:** Do ***not*** enable this option if the physical server has multiple virtual hosts.<br>**Note:** This option is not supported if the FortiWeb unit is operating in transparent mode. |
| **X-Forwarded-for Support** | Enable to include the `X-Forwarded-For:` HTTP header on connections forwarded to your web servers. Behavior varies by the header already provided by the HTTP client or web proxy, if any:<br>• **Header absent**: Add the header, using the source IP address of the connection.<br>• **Header present**: Verify that the source IP address of the connection is present in this header's list of IP addresses. If it is not, append it.<br>This option can be useful, for example, for web servers that log or analyze clients' IP addresses, and support the `X-Forwarded-For:` header. When this option is disabled, from the web server's perspective, all connections appear to be coming from the FortiWeb unit, which performs network address translation (NAT). But when enabled, the web server can instead analyze this header to determine the source and path of the original client connection. |
| **Cookie Poison** | Enable to detect cookie poisoning, then select which of the following actions the FortiWeb unit will take if cookie poisoning is detected:<br>• **Alert**: Accept the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>• **Alert & Deny**: Block the connection and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>• **Remove Cookie**: Accept the connection, but remove the poisoned cookie from the datagram before it reaches the web server, and generate an alert and/or log message. For more information on logging and alerts, see "Configuring logging and alerts" on page 252.<br>When enabled, each cookie is accompanied by a cookie named `<cookie_name>_fortinet_waf_auth`, which tracks the cookie's original value when set by the web server. If the cookie returned by the client does not match this digest, the FortiWeb unit will detect cookie poisoning. |
| **Allow Request Method** | Mark the check boxes of HTTP request methods that you want to allow, such as:<br>• **GET**<br>• **POST**<br>• **HEAD**<br>• **OPTIONS**<br>• **TRACE**<br>• **CONNECT**<br>• **DELETE**<br>• **PUT**<br>• **OTHERS** (any other HTTP method, such as custom methods)<br>Attack log messages and *Alert Message Console* messages contain `DETECT_ALLOW_METHOD_FAILED` when this feature detects a non-allowed HTTP request method. |

| | |
|---|---|
| **Allow Method Exceptions** | Select the name of an exception to the allowed request methods, if any. |
| **Server Protection Rule** | Select the name of the server protection rule, if any, that will be applied to matching HTTP requests.<br>If enabled, server protection rules can scan AMF3 requests. For more information, see "Enable AMF3 Protocol Detection" on page 219.<br>Attack log messages and *Alert Message Console* messages for this feature vary by which type of attack was detected. For a list, see "Configuring server protection rules" on page 161. |
| **Page Access Rule** | Select the name of the page access rule, if any, that will be applied to matching HTTP requests.<br>This option appears only if *Session Management* is enabled.<br>Attack log messages and *Alert Message Console* messages contain `DETECT_PAGE_RULE_FAILED` when this feature detects a request for a URL that violates the required sequence of URLs within a session. |
| **Parameter Validation Rule** | Select the name of the parameter validation rule, if any, that will be applied to matching HTTP requests.<br>Attack log messages and *Alert Message Console* messages contain `DETECT_PARAM_RULE_FAILED` when this feature detects a parameter rule violation. |
| **Hidden Fields Protection Rule** | Select the name of a hidden fields group, if any, that will be applied to matching HTTP requests.<br>This option appears only if *Session Management* is enabled. |
| **Start Pages** | Select the name of the start page group, if any, that HTTP requests must use in order to initiate a valid session.<br>This option appears only if *Session Management* is enabled.<br>Attack log messages and *Alert Message Console* messages contain `DETECT_START_PAGE_FAILED` when this feature detects a start page violation. |
| **Black List Rule** | Select the name of the black list rule, if any, that will be applied to matching HTTP requests.<br>Attack log messages and *Alert Message Console* messages contain `DETECT_BLACK_PAGE` when this feature detects a blacklisted URL. |
| **White List Rule** | Select the name of the white list rule, if any, that will be applied to matching HTTP requests. |
| **Brute Force Login** | Select the name of a brute force login attack sensor, if any, that will be applied to matching HTTP requests.<br>Attack log messages and *Alert Message Console* messages contain `DETECT_BRUTE_FORCE_LOGIN` when this feature detects a brute force login attack. |
| **Robot Control** | Select the name of a robot control sensor, if any, that will be applied to matching HTTP requests.<br>Attack log messages and *Alert Message Console* messages contain `DETECT_MALICIOUS_ROBOT` when this feature detects a misbehaving robot or any other HTTP client that exceeds the rate limit. |
| **URL Rewrite Rule** | Select the name of a URL rewriting rule set, if any, that will be applied to matching HTTP requests. |
| **HTTP Protocol Constraints** | Select the name of an HTTP parameter constraint, if any, that will be applied to matching HTTP requests.<br>Attack log messages and *Alert Message Console* messages contain `HTTP_HEADER_LEN_OVERFLOW` or `HTTP_HEADER_LINE_LEN_OVERFLOW` when this feature detects an HTTP request that does not comply with the constraints. |
| **HTTP Authentication Policy** | Select the name of an HTTP authentication rule, if any, that will be applied to matching HTTP requests. If the HTTP client fails to authenticate, it will receive an HTTP 403 (Access Forbidden) error message. |

| | |
|---|---|
| **Redirect URL** | Type a URL including the FQDN/IP and path, if any, to which an HTTP client will be redirected if their HTTP request violates any of the rules in this profile.<br>For example, you could enter `www.example.com/products/`.<br>If you do ***not*** enter a URL, depending on the type of violation and the configuration, the FortiWeb unit will log the violation, may attempt to remove the offending parts, and could either reset the connection or return an HTTP 403 (Access Forbidden) or 404 (File Not Found) error message. |
| **Redirect URL With Reason** | Enable to include the reason for redirection as a parameter in the URL, such as `reason=DETECT_PARAM_RULE_FAILED`, when traffic has been redirected using *Redirect URL*. The FortiWeb unit also adds `fortiwaf=1` to the URL to detect and cancel a redirect loop (when the redirect action recursively triggers an attack event).<br>**Caution**: If you specify a redirect URL that is protected by the FortiWeb unit, you should enable this option to prevent infinite redirect loops. |
| **Enable AMF3 Protocol Detection** | Enable to be able to scan requests that use action message format 3.0 (AMF3) for:<br>• cross-site scripting (XSS) attacks<br>• SQL injection attacks<br>• common exploits<br>if you have enabled those in your selected *Server Protection Rule*.<br>AMF3 is a binary format that can be used by Adobe Flash clients to send input to server-side software.<br>**Caution:** To scan for attacks or enforce input rules on AMF3, you ***must*** enable this option. Failure to enable the option will cause the FortiWeb unit to be unable to scan AMF3 requests for attacks. |

4 Click *OK*.

If you will use this offline protection profile in conjunction with an auto-learning profile in order to indicate which attacks and other aspects should be discovered, also configure the auto-learning profile. For details, see "Configuring auto-learning profiles" on page 223.

To apply the inline protection profile, select it in a policy. For details, see "Configuring policies" on page 91.

# Configuring offline protection profiles

*Web Protection* > *Web Protection Profile* > *Offline Protection Profile* displays the list of offline protection profiles.

Offline protection profiles are useful when you want to preview the effects of some web protection features without affecting traffic, or without affecting your network topology.

Unlike inline protection profiles, an offline protection profile is designed for use in offline protection mode. Offline protection profiles cannot be guaranteed to block attacks. They attempt to reset the connection, but due to variable speeds of different routing paths, the reset request may arrive after the attack has been completed. Their primary purpose is to detect attacks, especially for use in conjunction with auto-learning profiles. In fact, if used in conjunction with auto-learning profiles, you ***should*** configure the offline proteciton profile to log only and not block attacks in order to gather complete session statistics for the auto-learning feature.

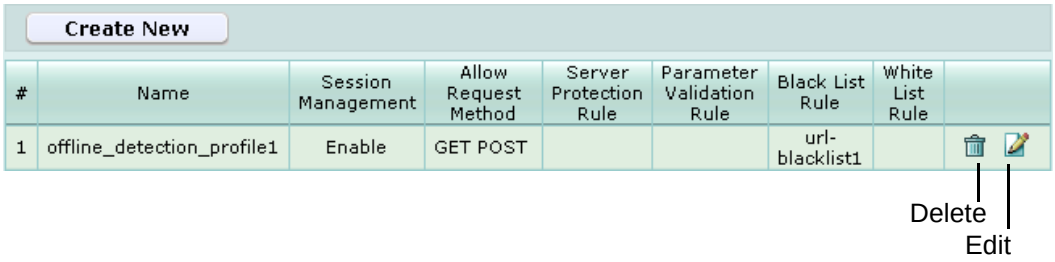
Unlike inline protection profiles, offline protection profiles do not support HTTP conversion, cookie poisoning detection, start page rules, and page access rules.

Offline protection profiles are applied by selecting them within a policy. For details, see "Configuring policies" on page 91.

**Note:** Offline web protection profiles can be configured at any time, but can only be selected in a policy while the FortiWeb unit is operating in a offline mode. For details, see Table 36, “Policy behavior by operation mode,” on page 92.

To be able to access this part of the web-based manager, in your administrator account’s access profile, you must have *Read* permission to items in the *Web Protection Configuration* category. For details, see “About permissions” on page 58.

**Table 87:** *Offline Protection Profile* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add an offline protection profile. |
| # | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Session Management** | Indicates whether session management by the FortiWeb unit is enabled or disabled. For more information about session management, see “Configuring offline protection profiles” on page 219. |
| **Allow Request Method** | The names of HTTP request methods that the offline protection profile allows, such as:<br>• **GET**<br>• **POST**<br>• **HEAD**<br>• **OPTIONS**<br>• **TRACE**<br>• **CONNECT**<br>• **DELETE**<br>• **PUT**<br>• **OTHERS** |
| **Server Protection Rule** | The name of the server protection rule that will be applied to matching HTTP requests. For details on server protection rules, see “Configuring server protection rules” on page 161. |
| **Parameter Validation Rule** | The name of the parameter validation rule that will be applied to matching HTTP requests. For details on parameter validation rules, see “Grouping input rules into parameter validation rules” on page 156. |
| **Black List Rule** | The name of the black list rule that will be applied to matching HTTP requests. For details on black list rules, see “Configuring URL black list rules” on page 173. |
| **White List Rule** | The name of the white list rule that will be applied to matching HTTP requests. For details on white list rules, see “Configuring URL white list rules” on page 175. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a policy.<br>Click *Edit* to modify the entry. |

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Web Protection Configuration* category. For details, see "About permissions" on page 58.

### To configure an offline web protection profile

Before configuring an offline protection profile, first configure any of the following that you want to include in the profile:

- a server protection rule (see "Configuring server protection rules" on page 161)
- a parameter validation rule (see "Grouping input rules into parameter validation rules" on page 156)
- a black list rule (see "Configuring URL black list rules" on page 173)
- a white list rule (see "Configuring URL white list rules" on page 175)
- a robot control sensor (see "Configuring robot control sensors" on page 184)
- an allowed method exception (see "Configuring allowed method exceptions" on page 191)
- a hidden fields group (see "Grouping hidden field rules" on page 197)
- an HTTP protocol constraint (see "Configuring HTTP protocol constraints" on page 205)

1. Go to *Web Protection* > *Web Protection Profile* > *Offline Protection Profile*.
2. Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.
3. Configure the following:


| *Name of the GUI item* | *Description* |
|---|---|
| **Name** | Type the name of the offline protection profile. This field cannot be modified if you are editing an existing offline protection profile. To modify the name, delete the entry, then recreate it using the new name. |

| | |
|---|---|
| **Session Management** | Enable to track the states of HTTP sessions using a cookie named `FORTIWAFSID`, which is required if you will select a *WAF Auto Learning Profile* in the policy with this offline protection profile. Also configure *Session Timeout*.<br>This feature requires that the client support cookies.<br>**Note:** You ***must*** enable this option if you want to include the profile's traffic in the traffic log, in addition to enabling traffic logs in general. For more information, see "Enabling logging and alerts" on page 253. |
| **Session Timeout** | Enter the HTTP session timeout in seconds.<br>This option appears only if *Session Management* is enabled. |
| **Session Key Word** | If you want to use an HTTP header other than `Session-Id:` to track separate HTTP sessions, enter the key portion of the HTTP header that you want to use, such as `Session-Num`.<br>This option appears only if *Session Management* is enabled. |
| **Allow Request Method** | Mark the check boxes of HTTP request methods that you want to allow, such as:<br>• **GET**<br>• **POST**<br>• **HEAD**<br>• **OPTIONS**<br>• **TRACE**<br>• **CONNECT**<br>• **DELETE**<br>• **PUT**<br>• **OTHERS** (any other HTTP method, such as custom methods)<br>Attack log messages and *Alert Message Console* messages contain `DETECT_ALLOW_METHOD_FAILED` when this feature detects a non-allowed HTTP request method.<br>**Note:** If a *WAF Auto Learning Profile* will be selected in the policy with this profile, you must enable the HTTP request methods that will be used by sessions that you want the FortiWeb unit to learn about. If a method is disabled, the FortiWeb unit will reset the connection, and therefore will not be able to learn about the session. |
| **Allow Method Exceptions** | Select the name of an exception to the allowed request methods, if any.<br>**Note:** If a *WAF Auto Learning Profile* will be selected in the policy with this profile, you must enable the HTTP request methods that will be used by sessions that you want the FortiWeb unit to learn about. If a method is disabled, the FortiWeb unit will reset the connection, and therefore will not be able to learn about the session. |
| **Server Protection Rule** | Select the name of the server protection rule, if any, that will be applied to matching HTTP requests.<br>Attack log messages and *Alert Message Console* messages for this feature vary by which type of attack was detected. For a list, see "Configuring server protection rules" on page 161.<br>**Note:** If a *WAF Auto Learning Profile* will be selected in the policy with this profile, you should select a server protection rule whose *Action* is *Alert*. If the *Action* is *Alert & Deny*, the FortiWeb unit will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. |
| **Parameter Validation Rule** | Select the name of the parameter validation rule, if any, that will be applied to matching HTTP requests.<br>Attack log messages and *Alert Message Console* messages contain `DETECT_PARAM_RULE_FAILED` when this feature detects a parameter rule violation.<br>**Note:** If a *WAF Auto Learning Profile* will be selected in the policy with this profile, you should select a parameter validation rule whose *Action* is *Alert*. If the *Action* is *Alert & Deny*, the FortiWeb unit will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. |
| **Hidden Fields Protection Rule** | Select the name of a hidden fields group, if any, that will be applied to matching HTTP requests.<br>This option appears only if *Session Management* is enabled. |

| | |
|---|---|
| **Black List Rule** | Select the name of the black list rule, if any, that will be applied to matching HTTP requests.<br>Attack log messages and *Alert Message Console* messages contain `DETECT_BLACK_PAGE` when this feature detects a blacklisted URL.<br>**Note:** Do ***not*** select a black list rule if this offline protection profile will be used in a policy with *WAF Auto Learning Profile*. Selecting a black list rule will cause the FortiWeb unit to reset the connection when it detects a request with a blacklisted URL and `Host:` field combination, resulting in incomplete session information for the auto-learning feature. |
| **White List Rule** | Select the name of the white list rule, if any, that will be applied to matching HTTP requests. |
| **Robot Control** | Select the name of a robot control sensor, if any, that will be applied to matching HTTP requests.<br>Attack log messages and *Alert Message Console* messages contain `DETECT_MALICIOUS_ROBOT` when this feature detects a misbehaving robot or any other HTTP client that exceeds the rate limit.<br>**Note:** If a *WAF Auto Learning Profile* will be selected in the policy with this profile, you should select a robot control rule whose *Action* is *Alert*. If the *Action* is *Alert & Deny*, the FortiWeb unit will reset the connection when it detects an attack, resulting in incomplete session information for the auto-learning feature. |
| **HTTP Protocol Constraints** | Select the name of an HTTP protocol constraint, if any, that will be applied to matching HTTP requests. |
| **Enable AMF3 Protocol Detection** | Enable to be able to scan requests that use action message format 3.0 (AMF3) for:<br>• cross-site scripting (XSS) attacks<br>• SQL injection attacks<br>• common exploits<br>if you have enabled those in your selected *Server Protection Rule*.<br>AMF3 is a binary format that can be used by Adobe Flash clients to send input to server-side software.<br>**Caution:** To scan for attacks or enforce input rules on AMF3, you ***must*** enable this option. Failure to enable the option will cause the FortiWeb unit to be unable to scan AMF3 requests for attacks. |

4 Click *OK*.

If you will use this offline protection profile in conjunction with an auto-learning profile in order to indicate which attacks and other aspects should be discovered, also configure the auto-learning profile. For details, see "Configuring auto-learning profiles" on page 223.

To apply the offline protection profile, select it in a policy. For details, see "Configuring policies" on page 91.

# Configuring auto-learning profiles

*Web Protection* > *Web Protection Profile* > *Auto Learning Profile* displays the list of auto-learning profiles.

Auto-learning profiles are useful when you want to collect information about the HTTP sessions on your unique network in order to design inline or offline protection profiles suited for them.

Auto-learning profiles gather data on the HTTP requests that your FortiWeb unit is handling. They track your web servers' response to each request, such as `401 Unauthorized` or `500 Internal Server Error`, to learn about whether the request is legitimate or a potential attack attempt. Such data is used for auto-learning reports, and can serve as the basis for generating inline protection profiles or offline protection profiles (see "Generating a profile from auto-learning data" on page 232). This reduces much of the research and guesswork about what HTTP request methods, data types, and other types of content that your web sites and web applications use when designing an appropriate defense.

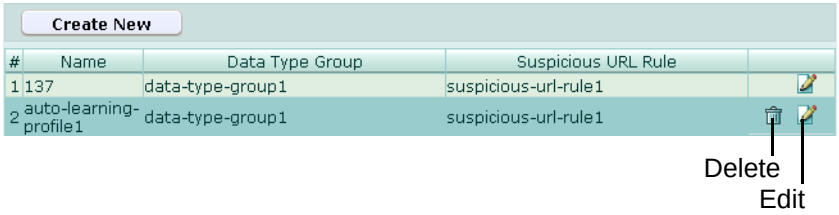
Auto-learning profiles are designed to be used in conjunction ***with*** an inline or offiline protection profile, which is used to detect attacks. Only if attacks are detected can the auto-learning profile accumulate auto-learning data and generate its report. As a result, auto-learning profiles require that you also select an inline or offline protection profile in the same policy.

**Note:** Use auto-learning profiles with profiles whose *Action* is *Alert*.
If *Action* is *Alert & Deny*, the FortiWeb unit will reset the connection, preventing the auto-learning feature from gathering complete data on the session.

Auto-learning profiles are applied by selecting them within a policy. For details, see "Configuring policies" on page 91. Once applied in a policy, the FortiWeb unit will collect data and generate a report from it. For details, see "Viewing auto-learning reports" on page 228.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Autolearn Configuration* category. For details, see "About permissions" on page 58.

**Table 88:** *Auto Learning Profile* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add an auto-learning profile. |
| **#** | The index number of the entry in the list. |
| **Name** | The name of the entry. |
| **Data Type Group** | The name of a data type group. The auto-learning profile will learn about the names, length, and required presence of these types of parameter inputs. For details, see "Grouping the predefined data types" on page 116. |
| **Suspicious URL Rule** | The name of a suspicious URL rule. The auto-learning profile will learn about attempts to access these types of URLs that may indicate an attempt to gain administrative or other unauthorized access to the web server or web application. For details, see "Grouping the predefined suspicious URLs" on page 120. |
| (No column heading.) | Click *Delete* to remove the entry. This icon does not appear if the entry is currently selected for use in a policy.<br>Click *Edit* to modify the entry. |

### To configure an auto-learning profile

Before configuring an auto-learning profile, first configure any of the following that you want to include in the profile:

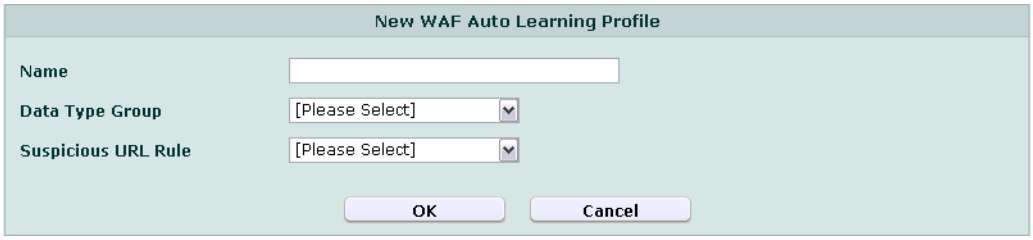
- a data type group (see “Grouping the predefined data types” on page 116)
- a suspicious URL rule group (see “Grouping the predefined suspicious URLs” on page 120)

**Note:** Alternatively, you could generate a default auto-learning profile and its required components, and then modify them. For details, see “Generating an auto-learning profile and its components” on page 227.

1 Go to *Web Protection* > *Web Protection Profile* > *Auto Learning Profile*.

2 Click *Create New*, or, in the row corresponding to an entry that you want to modify, click *Edit*.

3 Configure the following:




| *Name of the GUI item* | *Description* |
|---|---|
| **Name** | Type the name of the auto-learning profile. This field cannot be modified if you are editing an existing auto-learning profile. To modify the name, delete the entry, then recreate it using the new name. |
| **Data Type Group** | Select the name of a data type group to use, if any. The auto-learning profile will learn about the names, length, and required presence of these types of parameter inputs. For details, see “Grouping the predefined data types” on page 116. |
| **Suspicious URL Rule** | Select the name of a suspicious URL rule to use, if any. The auto-learning profile will learn about attempts to access URLs that are typically used for web server or web application administrator logins, such as `/admin.php`. Requests from clients for these types of URLs are considered to be a possible attempt at either vulnerability scanning or administrative login attacks, and therefore potentially malicious. For details, see “Grouping the predefined suspicious URLs” on page 120. |

4 Click *OK*.

To apply the auto-learning profile, select it in a policy with an inline or offline protection profile. For details, see “Configuring policies” on page 91.

**Note:** Use auto-learning profiles with offline protection profiles whose *Action* is *Alert*. If *Action* is *Alert & Deny*, the FortiWeb unit will reset the connection, preventing the auto-learning feature from gathering complete data on the session.

Once the policy has begun to match connections and accumulate data, you can view the current statistics any time by displaying the auto-learning report. For details, see “Viewing auto-learning reports” on page 228.

# Auto Learn

This section describes the *Auto Learn* menu and explains how to generate a default auto-learning profile and its required components, and how to use reports generated from auto-learning.

Auto-learning gathers information about the URLs and other characteristics of HTTP sessions that the FortiWeb unit frequently sees passing to your physical servers. It tracks your web servers' response to each request, such as `401 Unauthorized` or `500 Internal Server Error`, to learn about whether the request is legitimate or a potential attack attempt. It then generates reports based upon this information. By learning about your typical traffic, the FortiWeb unit can help you to quickly make profiles designed specifically for your unique HTTP traffic.

This section includes the following topics:



## Generating an auto-learning profile and its components

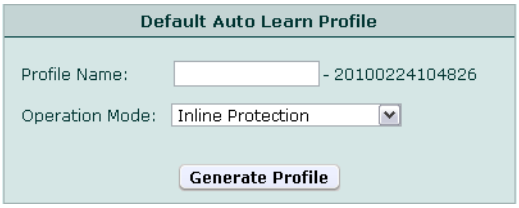
*Auto Learn* > *Default Auto Learn Profile* > *Default Auto Learn Profile* enables you to generate an auto-learning profile and all of its required components.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Autolearn Configuration* category. For details, see "About permissions" on page 58.

Generated auto-learning profiles' components include:

- data type groups
- suspicious URL rules groups
- server protection rule
- robot control sensor and robot groups
- inline or offline protection profile

**Figure 18: Generating a default auto-learning profile**




In *Profile Name*, type a name prefix, such as `gen-autolearn`.

The FortiWeb unit will automatically suffix a dash ( `-` ) followed by a number indicating the year, month, day, and time on which the profile and its associated components were generated. All associated components thereby have identical suffixes, and can be easily identified for modification.

In the generated components, all options are enabled which are required to guarantee a complete data set for the purpose of the report generated by the auto-learning profile, regardless of whether the web server is Apache, IIS, or Apache Tomcat, and assuming that you want to learn about all parameters and allow web crawlers from the popular search engines Google, Yahoo!, and MSN. The server protection rule will use only attack definitions that do not cause false positives (that is, they do not use the extended rule set). The offline protection or inline protection profile will track all HTTP request methods, and apply a session timeout of 1,200 seconds. The FortiWeb unit will log, but not block, detected attacks.

To improve performance, you can modify the generated groups and profiles. For example, if you only operate one type of web server, or if you know that you do not need to watch for a specific data type, you could modify the generated data type group and suspicious URL rule group. The FortiWeb unit would then not expend resources to monitor for these things. For details, see “Grouping the predefined data types” on page 116 and “Grouping the predefined suspicious URLs” on page 120.

To use all of the attack definitions, or if you want to make one of the search engines’ crawlers subject to attack detection, you could modify the generated robot control sensor and server protection rule. For details, see “Configuring robot control sensors” on page 184 and “Configuring server protection rules” on page 161.

To apply a generated auto-learning profile, select it and its associated inline or offline protection profile in a policy. For details, see “Configuring policies” on page 91.

# Viewing auto-learning reports

*Auto Learn* > *Auto Learn Report* > *Auto Learn Report* displays the list of reports that the FortiWeb unit has generated from information gathered by auto-learning profiles.

It also enables you to download a PDF version of the report by clicking *Generate PDF*.

For information on configuring auto-learning profiles, see “Configuring auto-learning profiles” on page 223.

Reports generated from auto-learning profiles’ data can help you to learn about the nature of your network. They can also help you to know whether or not the auto-learning profile has collected sufficient amounts of data. When the auto-learning feature has gathered a satisfactory amount of information, you can use the data to generate web profiles as a basis for configuration of your FortiWeb unit.

Auto-learning reports may also serve to inform you about the types of normal HTTP requests and attacks occurring on your network.

**Note:** Auto-learning reports require that your web browser have the Adobe Flash Player plug-in.

To be able to access this part of the web-based manager, in your administrator account’s access profile, you must have both *Read* and *Write* permission to items in the *Autolearn Configuration* category. For details, see “About permissions” on page 58.

**Table 89:** *Auto Learn Report* **tab**

| Name | Detail | Clean Data |
|---|---|---|
| offline137 | | |

| *Name of the GUI item* | *Description* |
|---|---|
| **Name** | The name of the auto-learning profile whose gathered information was used to generate the report. |
| **Detail** | Click to view the report and/or to generate a web profile based upon the data gathered for the report. |
| **Clean Data** | Click to remove data gathered by this auto-learning profile. Subsequent reports and any profiles generated from them will include only data gathered by the auto-learning profile after you click this icon. |

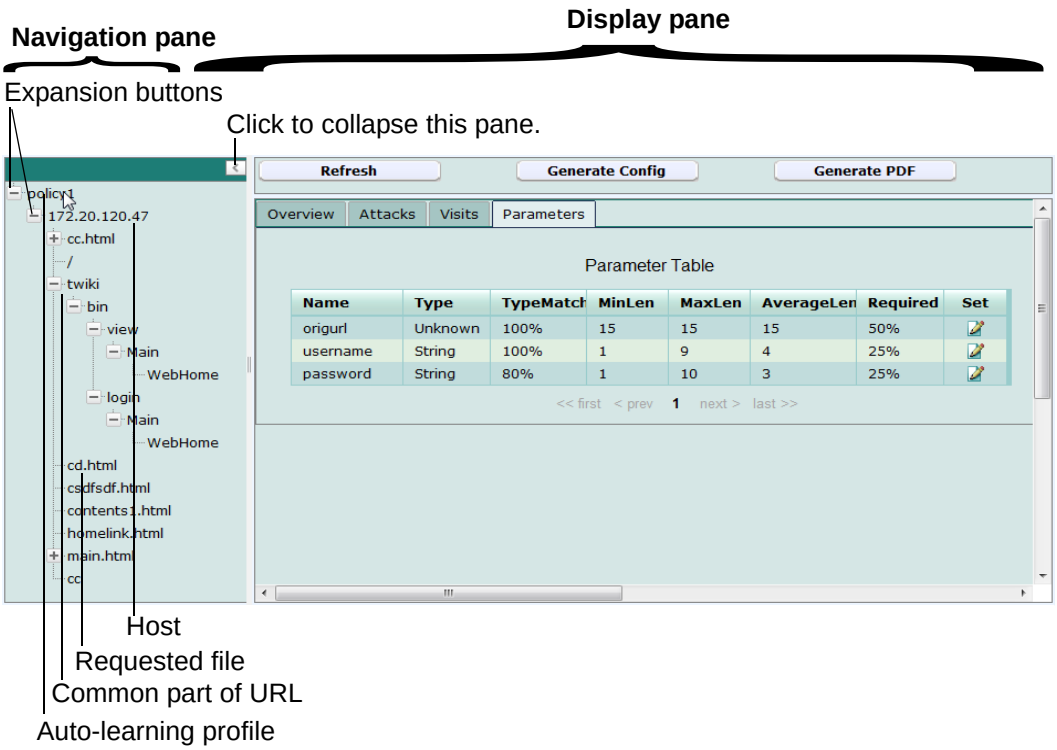
### To view a report generated from auto-learning data

1 Go to *Auto Learn* > *Auto Learn Report* > *Auto Learn Report*.

2 In the row corresponding to the auto-learning profile whose data you want to view, click *Detail*.

Two panes appear: the left-hand pane contains a pane used for navigating through the web sites and URLs that are the subjects of the report; the right-hand pane displays report charts, and contains buttons that enable you to adjust any profile that will be generated from the data.

**Figure 19: Parts of auto-learning reports**



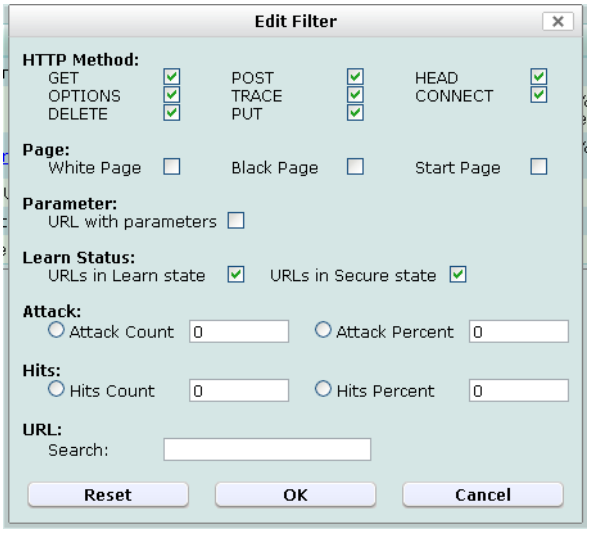

3 In the left-hand pane, right-click the name of an item, then click any that you want of the following:

| *Name of the GUI item* | *Description* |
|---|---|
| **Refresh the Tree** | Select to update the display in the navigation pane. |
| **Filter the Tree** | Select to show or hide HTTP sessions in the report by their HTTP request method and/or other attributes. A pop-up dialog appears. |
| **Expand Current Node** | Select to expand the item and all of its sub-items.<br>This option has no effect when right-clicking the name of the auto-learning profile. |
| **Stop Learning** | Select to enable or disable auto-learning for this item, saving processing resources to learn about URLs whose inputs you know to be more complex. This can significantly improve performance |
| **Clean Data** | Select to empty auto-learning data for this item. This may be useful if you know that the inputs required by a specific page have changed since you initially began learning about a web site's parameters, and you want to eliminate obsolete data from the auto-learning report and any profiles that are generated from it. |

If you select *Filter the Tree*, the following pop-up dialog appears. To show only specific nodes in the URL tree and hide the rest, select which attributes that a node or its sub-node must satisfy in order to be included.

For example, to include only parts of the URL tree pertaining to HTTP POST requests to Java server pages (.jsp files), you would enter `.jsp` in the *Search* field of *URL Filter* and enable *POST* in the *HTTP Method Filter*.

**Figure 20: Filtering an auto-learning report**



4 In the left-hand pane, if you want to view statistics for a subset of sessions with specific hosts and their URLs, click the button ( + ) next to an item to expand the item, then click the name of the sub-item whose statistics you want to view. Depending on the level in the navigation tree, an item may be either an auto-learning profile observing multiple hosts, a single host, a common part of a path contained in multiple URLs, or a single requested file. This enables you to view:

- statistics specific to each requested URL
- totals for a group of URLs with a common path
- totals for all requested URLs on the host
- totals for all requests on all hosts observed by the auto-learning profile

Statistics and charts appear on the right-hand pane.

**Note:** If URL rewriting is configured, the tree's URL is the one requested by the client, not the one to which it was rewritten before passing to the server.

5 In the right-hand pane, click one of the following:

- *Overview* tab — A summary of statistics for all sessions established with the host during the use of the auto-learning profile, or since its auto-learning data was last cleared, whichever is shorter.

**Note:** Auto-learning data can be cleared manually, by clicking the *Clean Data* button in the list of reports. It can also be cleared for individual nodes by right-clicking the node in the left-hand pane. However, it is also cleared automatically if you delete the policy that uses the auto-learning profile.

- *Attacks* tab — Statistics on sessions that contained one of the types of attacks that the web profile selected in the same policy was configured to detect. Sometimes, auto-learning reports may contain fewer attacks than you see in the FortiWeb unit's attack logs. For details, see "About the attack count" on page 232.
- *Visits* tab — Statistics on the sessions' HTTP request methods and the URLs that were requested.
- *Parameters* tab — Statistics on the parameters and their values as they appeared in HTTP requests. *TypeMatch* and *Required* columns' percentages indicate how likely the parameter with that name is of that exact data type, and whether or not the web application requires that input for that URL. *MinLen* and *MaxLen* columns indicate the likely valid range of length for that input's value. The columns thereby provide information on what is likely the correct configuration of a profile for that URL.

  This tab appears only for items that are leaf nodes in the navigation tree (that is, they represent a single complete URL as it appeared in a real HTTP request, and therefore could have had those exact associated parameters).
- *Cookies* tab — Statistics on the name, value, expiry date, and path of each cookie crumb that appeared in HTTP requests. This tab appears only for hosts that used cookies.

If a tab contains multiple pages of results, click the arrows at the bottom of the tab, such as *next* > and << *first*, to move forward or backwards through the pages of results.

To update the display with current statistics, click *Refresh*. If the auto-learning profile has gathered sufficient amounts of data and you want to generate a web profile based upon the data, see "Generating a profile from auto-learning data" on page 232.

6 To generate and download a complete report in PDF format, in the right-hand pane, click *Generate PDF*.

### About the attack count

Sometimes, auto-learning reports may contain fewer attacks than you see in the FortiWeb unit's attack logs. Possible causes include:

- The attack was attempted, but was targeted towards a URL that did not actually exist on the server (i.e. it resulted in an HTTP `404 File Not Found` reply code). Because the URL did not exist, the auto-learning report does ***not*** include it in its tree of requested URLs.

  In other words, the attack was not counted in the report because it did not result in an actual page hit.
- The attack was attempted, and the URL existed, but the FortiWeb unit was configured to block the attack (*Alert & Deny*), resulting in an unsuccessful connection attempt. Unsuccessful connections do not result in an actual page hit and have incomplete session data, and therefore are not included in auto-learning reports.

  To ensure that auto-learning reports have complete session data, you should instead log but not block attacks (i.e. select *Alert* instead) while gathering auto-learning data.

## Generating a profile from auto-learning data

When viewing a report generated from auto-learning data, you can generate an inline protection profile or an offline protection profile suitable for the HTTP sessions that have been observed. If some observed sessions are not indicative of typical traffic and you do not want to include elements of it in the generated profile, or you want to select an action other than the default for a type of observed attack, you can selectively change the action for that type of attack.

In addition to the generated profile itself, the FortiWeb unit will also generate all rules and other auxiliary configurations that the profile depends upon.

For example, if the FortiWeb unit observed HTTP `PUT` requests with required parameters of a password and a user name that is an email address, when generating a profile, it would also generate the parameter validation rules and input rules that the profile requires, using the data types and maximum lengths of the arguments observed in the HTTP sessions.

Generated profiles and auxiliary configurations are editable. They can be adjusted or used as the basis for additional configuration.

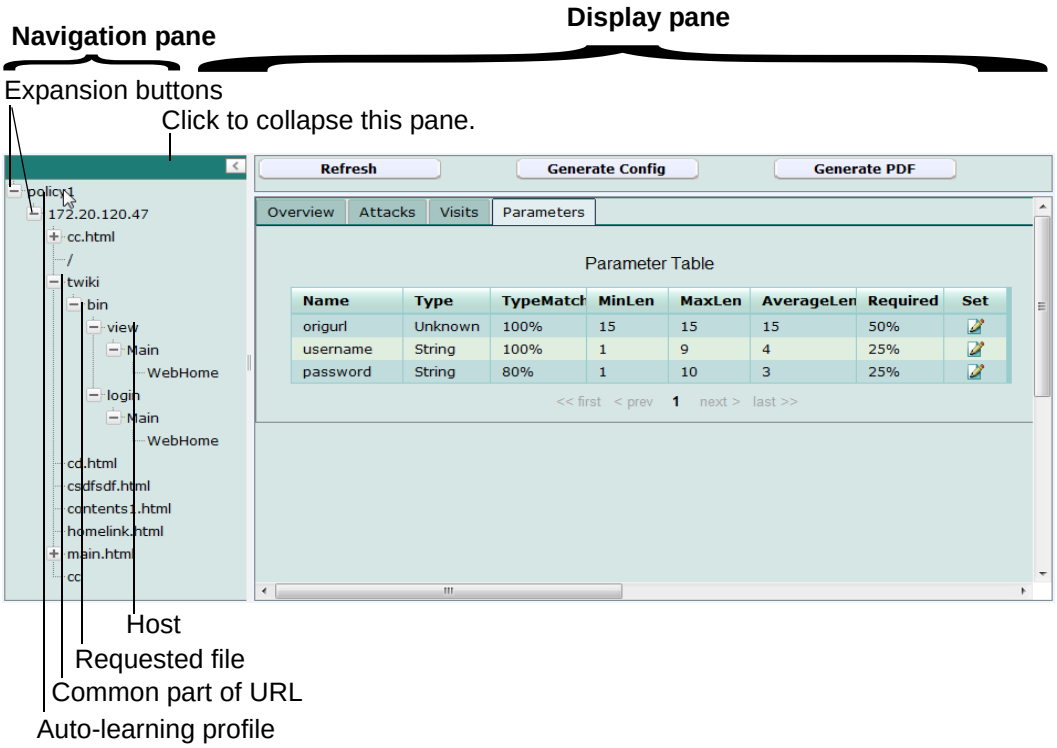
To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Autolearn Configuration* category. For details, see "About permissions" on page 58.

**To configure a profile using auto-learning data**

1 Go to *Auto Learn* > *Auto Learn Report* > *Auto Learn Report*.

2 In the row corresponding to the auto-learning profile whose data you want to view, click *Detail*.

**Figure 21: Viewing an auto-learning report**




**3** In the left-hand pane, if you want to adjust the actions that will appear in the generated profile for the subset of sessions handled for specific web hosts and their URLs, click the button ( + ) next to an item to expand the item, then click the name of the sub-item whose actions you want to affect.

Statistics and charts appear on the right-hand pane.

**4** For each item in the left-hand navigation pane, in the right-hand pane, click the buttons to configure the options on each of the following tabs:

| Name of the GUI item | | Description |
|---|---|---|
| **Overview** | | |
| | **Edit Protected Servers** | Enable or disable the IP addresses and/or domain names that will be members of the generated protected servers group. For details, see "Configuring protected hosts" on page 113.<br>This button appears only if you have selected the name of the auto-learning profile in the navigation pane. |
| | **Edit URL Page** | Enable or disable whether the currently selected URL will be included in start pages, white list rules, and black list rules of the generated profile. To exclude a rule type, mark its check box.<br>For more information on those rule types, see "Configuring start pages" on page 170, "Configuring URL white list rules" on page 175 and "Configuring URL black list rules" on page 173. |
| **Attacks** | | |
| | **Edit Attack Action** | Enable or disable detection of each type of attack, and select which action that the generated profile will take. For details, see "Configuring inline web protection profiles" on page 213 or "Configuring offline protection profiles" on page 219. |
| **Visits** | | |
| | **Edit HTTP Method** | Select which HTTP request methods will be allowed in the generated profile. For details, see "Configuring inline web protection profiles" on page 213 or "Configuring offline protection profiles" on page 219. |
| | **Edit White Page** | Select which combinations of web host name and URLs will be allowed by the generated white list rule. For details, see "Configuring URL white list rules" on page 175. |
| | **Edit Start Page** | Select which combinations of web host name and URLs are valid for requests that initiate an HTTP session according to the generated start page rule. For details, see "Configuring start pages" on page 170. |
| | **Edit Black Page** | Select which combinations of web host name and URLs will be blocked by the black list rule. For details, see "Configuring URL black list rules" on page 173. |
| **Parameters** | | |
| | **Set** | Type the data type and maximum length of the parameter, and indicate whether or not the parameter is required input. These settings will appear in the generated parameter validation rule and input rules. For details, see "Configuring input rules" on page 152 and "Grouping input rules into parameter validation rules" on page 156. |

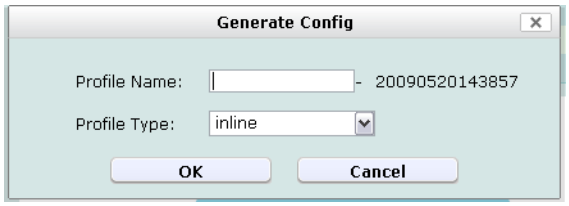
If a tab contains multiple pages of results, click the arrows at the bottom of the tab, such as *next* > and << *first*, to move forward or backwards through the pages of results.

If you do not configure any settings, by default, the FortiWeb unit will generate a profile that allows the HTTP `GET` method and any other methods whose usage exceeded the

threshold, and will add the remaining methods to an allowed method exception. It will also create start page rules and white list rules for the top 10 most commonly requested URLs, and create black list rules for the top 10 least commonly requested URLs.

5 In the right-hand pane, click *Generate Config*.

**Figure 22: Generating an inline or offline profile from auto-learning data**




6 In *Profile Name*, type a name prefix, such as `generated-profile`.

The FortiWeb unit will automatically suffix a dash ( - ) followed by a number indicating the year, month, day, and time on which the profile was generated in order to indicate the data on which the profile was based.

7 From *Profile Type*, select which type of web profile you want to generate, either *inline* (to generate an inline protection profile) or *offline* (to generate an offline protection profile).

8 Click *OK*.

The generated profile appears in the list of either inline or offline protection profiles, depending on its type. Adjust it if necessary. For details, see "Configuring inline web protection profiles" on page 213 or "Configuring offline protection profiles" on page 219.

**Note:** You may also need to adjust configuration items used by the generated profile, such as input rules. The generated configuration items will be based upon auto-learning data current at the time that the profile is generated, which may have changed while you were reviewing the auto-learning report.

To apply the generated profile, select it in a policy. For details, see "Configuring policies" on page 91. If you are done collecting auto-learning data, for performance reasons, you may also want to deselect the auto-learning profile in all policies.

# Web Anti-Defacement

This section describes the *Web Anti-Defacement* menu, which configures the FortiWeb unit to monitor web sites for defacement attacks.

This topic includes:



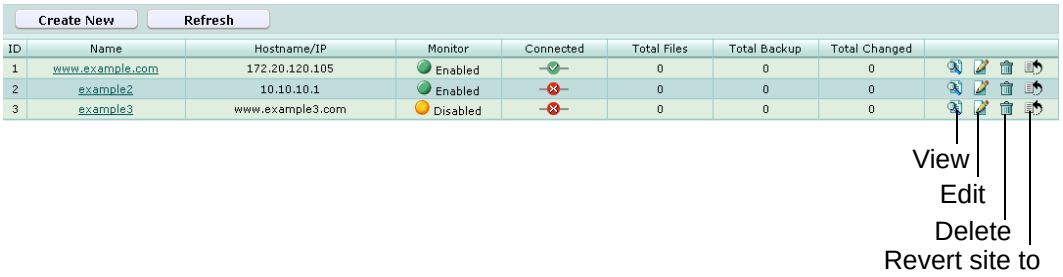
## Configuring anti-defacement

*Web Anti-Defacement* > *Web Anti-Defacement* > *Web Site with Anti-Defacement* displays the list of web sites for which you have configured anti-defacement.

Anti-defacement monitors a web site's files for any changes at specified time intervals. If it detects a change that could indicate a defacement attack, the FortiWeb unit can notify you and quickly react by automatically restoring the web site contents to the previous backup revision.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Web Anti-Defacement Management* category. For details, see "About permissions" on page 58.

**Table 90:** *Web Site with Anti-Defacement* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a web site that the FortiWeb unit will monitor for defacement. |
| **Refresh** | Click to refresh the tab's display, including the current *Connected* status. |
| **ID** | The index number of the entry in the list. |
| **Name** | A descriptive name for the web site. |
| **Hostname/IP** | The IP address or fully qualified domain name (FQDN) of the physical server on which the web site is hosted. |
| **Monitor** | Indicates whether or not anti-defacement is currently enabled for the web site.<br>• **Green icon**: Anti-defacement is enabled.<br>• **Flashing yellow-to-red icon**: Anti-defacement is disabled. |

| | |
|---|---|
| **Connected** | Indicates the connection results of the FortiWeb unit's most recent attempt to connect to the web site's server.<br>• **Green check mark icon**: The connection was successful.<br>• **Red X mark icon**: The FortiWeb unit was unable to connect. Verify the IP address/FQDN and login credentials of your anti-defacement configuration. If these are valid, verify that connectivity has not been interrupted by dislodged cables, routers, or firewalls. |
| **Total Files** | Displays the total number of files on the web site. |
| **Total Backup** | Displays the total number of files that have been backed up onto the FortiWeb unit for recovery purposes. Those files that you choose not to monitor will not be backed up. |
| **Total Changed** | Displays the total number of files that have been changed. |
| (No column heading.) | Click *View* display the web site's anti-defacement configuration and backup statistics, including disk usage.<br>Click *Edit* to modify an entry.<br>Click *Delete* to remove an entry.<br>Click *Revert site to* revert the web site to a backup revision. See "Reverting a web site to a backup revision" on page 241. |

### To configure anti-defacement

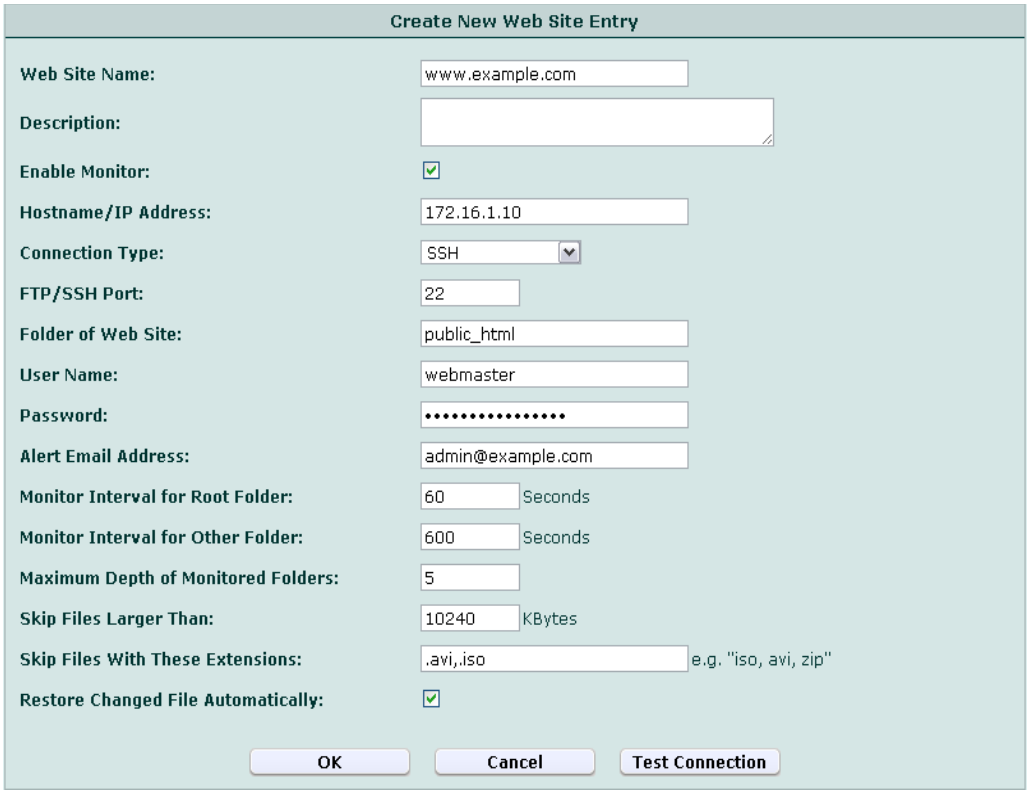
Before configuring a web site for anti-defacement protection, you must have the following information ready:

- FQDN or IP address of the web site's server
- root folder of the web site
- connection type (FTP, SSH, or Windows Share) and the credentials you use to access the root folder of the web site
- alert email address

1 Go to *Web Anti-Defacement* > *Web Anti-Defacement* > *Web Site with Anti-Defacement*.

2 Click *Create New* to add a new entry, or click the *Edit* icon to edit an existing entry.

**3** Configure the following settings:




| *Name of the GUI item* | *Description* |
|---|---|
| **Web Site Name** | Type a name for the web site.<br>This name will not be used when monitoring the web site, nor will it be referenced in any other part of the configuration, and therefore can be any identifier that is useful to you. It does not need to be the web site's FQDN or virtual host name. |
| **Description** | Enter a comment. The comment may be up to 63 characters long.<br>This field is optional. |
| **Enable Monitor** | Enable to monitor the web site's files for changes, and to download backup revisions that can be used to revert the web site to its previous revision if the FortiWeb unit detects a change attempt. |
| **Hostname/IP** | Type the IP address or fully qualified domain name (FQDN) of the physical server on which the web site is hosted.<br>This will be used when connecting by SSH or FTP to the web site to monitor its contents and download backup revisions, and therefore could be different from the real or virtual web host name that may appear in the `Host:` field of HTTP headers. |
| **Connect Type** | Select which protocol (*FTP*, *SSH*, or *Windows Share*) to use when connecting to the web site in order to monitor its contents and download web site backups. |
| **FTP/SSH Port** | Enter the TCP port number on which the web site's physical server listens. The standard port number for FTP is 21; the standard port number for SSH is 22.<br>This field appears only if *Connect Type* is *FTP* or *SSH*. |
| **Windows Share Name** | Type the name of the shared folder on the web server.<br>This field appears only if *Connect Type* is *Windows Share*. |

| | |
|---|---|
| **Folder of Web Site** | Type the path to the web site's folder, such as `public_html`, on the physical server. The path is relative to the initial location when logging in with the user name that you specify in *User Name*. |
| **User Name** | Enter the user name, such as `fortiweb`, that the FortiWeb unit will use to log in to the web site's physical server. |
| **Password** | Enter the password for the user name you entered in *User Name*. |
| **Alert Email Address** | Type the recipient email address (`MAIL TO:`) to which the FortiWeb unit will send an email when it detects that the web site has been changed. |
| **Monitor Interval for Root Folder** | Enter the time interval in seconds between each monitoring connection from the FortiWeb unit to the web server. During this connection, the FortiWeb unit examines *Folder of Web Site* (but ***not*** its subfolders) to see if any files have been changed by comparing the files with the latest backup.<br>If any file change is detected, the FortiWeb unit will download a new backup revision. If you have enabled *Restore Changed Files Automatically*, the FortiWeb unit will revert the files to their previous version.<br>For details, see "About web site backups" on page 241. |
| **Monitor Interval for Other Folder** | Enter the time interval in seconds between each monitoring connection from the FortiWeb unit to the web server. During this connection, the FortiWeb unit examines subfolders to see if any files have been changed by comparing the files with the latest backup.<br>If any file change is detected, the FortiWeb unit will download a new backup revision. If you have enabled *Restore Changed Files Automatically*, the FortiWeb unit will revert the files to their previous version.<br>For details, see "About web site backups" on page 241. |
| **Maximum Depth of Monitored Folders** | Type how many folder levels deep to monitor for changes to the web site's files. Files in subfolders deeper than this level will not be backed up. |
| **Skip Files Larger Than** | Type a file size limit in kilobytes (KB) to indicate which files will be included in the web site backup. Files exceeding this size will not be backed up. The default file size limit is 10,240 KB.<br>**Note:** Backing up large files can impact performance. |
| **Skip Files With These Extensions** | Type zero or more file extensions, such as `iso, avi`, to exclude from the web site backup. Separate each file extension with a comma.<br>**Note:** Backing up large files, such as video and audio, can impact performance. |
| **Restore Changed Files Automatically** | Enable to automatically restore the web site to the previous revision number when it detects that the web site has been changed.<br>Disable to do nothing. In this case, you must manually restore the web site to a previous revision when the FortiWeb unit detects that the web site has been changed. See "Reverting a web site to a backup revision" on page 241.<br>**Note:** While you are intentionally modifying the web site, you must turn off this option. Otherwise, the FortiWeb unit will detect your changes as a defacement attempt, and undo them. |
| **Test Connection** | Click this button to test the connection between the FortiWeb unit and the web server. |

**4** Click *OK*.

The FortiWeb unit connects to the web site and downloads the first backup copy revision. (It may subsequently download additional revisions. See "About web site backups" on page 241.)

When a defacement attack occurs, the damaged/changed files will be restored automatically if you enabled "Restore Changed Files Automatically". Otherwise, when the FortiWeb unit notifies you of the attack, you must manually revert the web site to one of the backup revisions. For details, see "Reverting a web site to a backup revision" on page 241.

### About web site backups

When a FortiWeb unit is configured to protect a web site using the anti-defacement feature, it will periodically download a backup copy of that web site's files automatically. It will create a new backup revision in the following cases:

- When the FortiWeb unit initiates monitoring for the first time, the FortiWeb unit will download a backup copy of the web site's files and store it as the first revision.

**Note:** Backup copies will omit files exceeding the file size limit and/or matching the file extensions that you have configured the FortiWeb unit to omit. See "Configuring anti-defacement" on page 237.

- If the FortiWeb unit could not successfully connect during a monitor interval, it will create a new revision the next time that it re-establishes the connection.

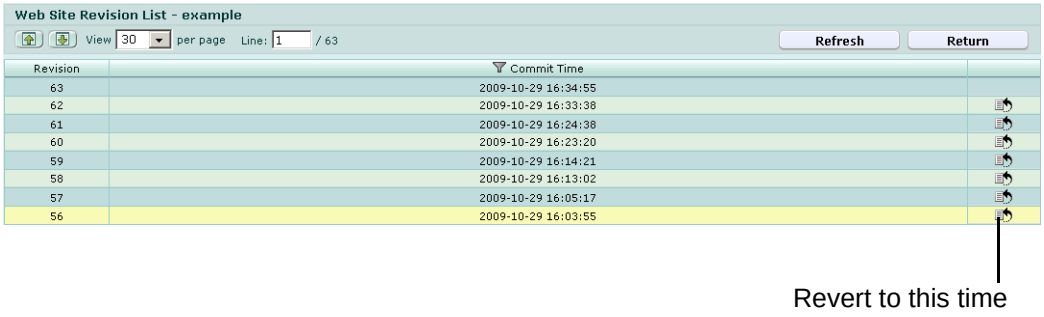
## Reverting a web site to a backup revision

If you do not enable automatic recovery of changed files (see Restore Changed Files Automatically), after a defacement attack, you can still manually revert the defaced web site to any known good backup revision that the FortiWeb unit has downloaded.

FortiWeb units periodically, automatically make backups of web sites that they have been configured to protect using the anti-defacement feature. For details about web site backup, see "About web site backups" on page 241.

**To revert a web site to a backup revision**

1. Go to *Web Anti-Defacement* > *Web Anti-Defacement* > *Web Site with Anti-Defacement*.
2. In the row corresponding to the web site you want to revert, click *Revert site to*.
3. In the row corresponding to the revision that you want to restore, click *Revert to this time*.




4. Click *OK*.

# Web Vulnerability Scan

This section describes the *Web Vulnerability Scan* menu.

Periodic vulnerability scans may be required for compliance with some regulations and certifications.

Vulnerability scans can also be useful, however, when configuring inline or offline protection profiles: by enabling protection specifically for vulnerabilities that actually exist on your servers, you may be able to conserve system resources and improve performance.

This section includes the following topics:



## Preparing for the vulnerability scan job

For best results, before scanning for vulnerabilities, you should prepare the target hosts.

Fortinet strongly recommends that you do ***not*** scan for vulnerabilities on live web sites, even if you use *Careful Mode*. Instead, duplicate the web site and its database into a test environment, and then use *Normal Checking Mode* with that test environment.

**Caution:** *Careful Mode* ***cannot*** be guaranteed to be non-destructive or complete. Many web sites accept input through HTTP `GET` requests, and so it is possible that a vulnerability scan could result in database changes, even though it does not use `POST`. In addition, *Careful Mode* cannot test for vulnerabilities that are only discoverable through `POST`, and therefore may not find all vulnerabilities.

You may also need to configure each target host and any intermediate NAT or security devices to allow the vulnerability scan to properly reach the target hosts.

If you do not plan to rate limit the vulnerability scan, be aware that some web servers could perceive its rapid rate of requests as a denial of service (DoS) attack. You may need to configure the web server to omit rate limiting for connections originating from the IP address of the FortiWeb unit. Rapid access also can result in degraded network performance during the scan. For all of these reasons, you may want to work with the owners of target hosts to schedule an appropriate time. For example, you might schedule to avoid peak traffic hours, to restrict unrelated network access, and to ensure that the target hosts will not be powered off during the vulnerability scan.

## Configuring vulnerability scans

*Web Vulnerability Scan* > *Web Vulnerability Scan* > *Web Vulnerability Scan* displays the results of previous vulnerability scans, and enables you to configure new scans.

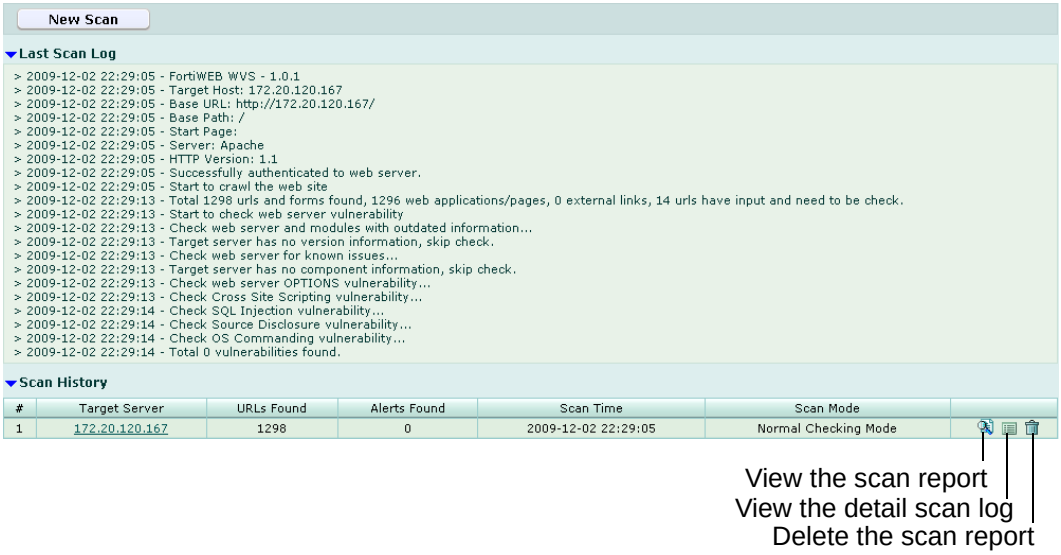
Vulnerability scanning can detect known vulnerabilities on your web servers and web applications, helping you to design protection profiles that are an efficient use of processing resources.

Vulnerability scans start from an initial directory, first authenticating if you have enabled it, then scanning for vulnerabilities in web pages located in the same directory or subdirectory as the initial URL. After performing the scan, the FortiWeb unit generates a report from the scan results.

Before running a vulnerability scan job, you may need to prepare the network and target hosts for the vulnerability scan job. For more information about preparing for a vulnerability scan job, see “Preparing for the vulnerability scan job” on page 243.

To be able to access this part of the web-based manager, in your administrator account’s access profile, you must have both *Read* and *Write* permission to items in the *Web Vulnerability Scan Configuration* category. For details, see “About permissions” on page 58.

**Table 91:** *Web Vulnerability Scan* **tab**



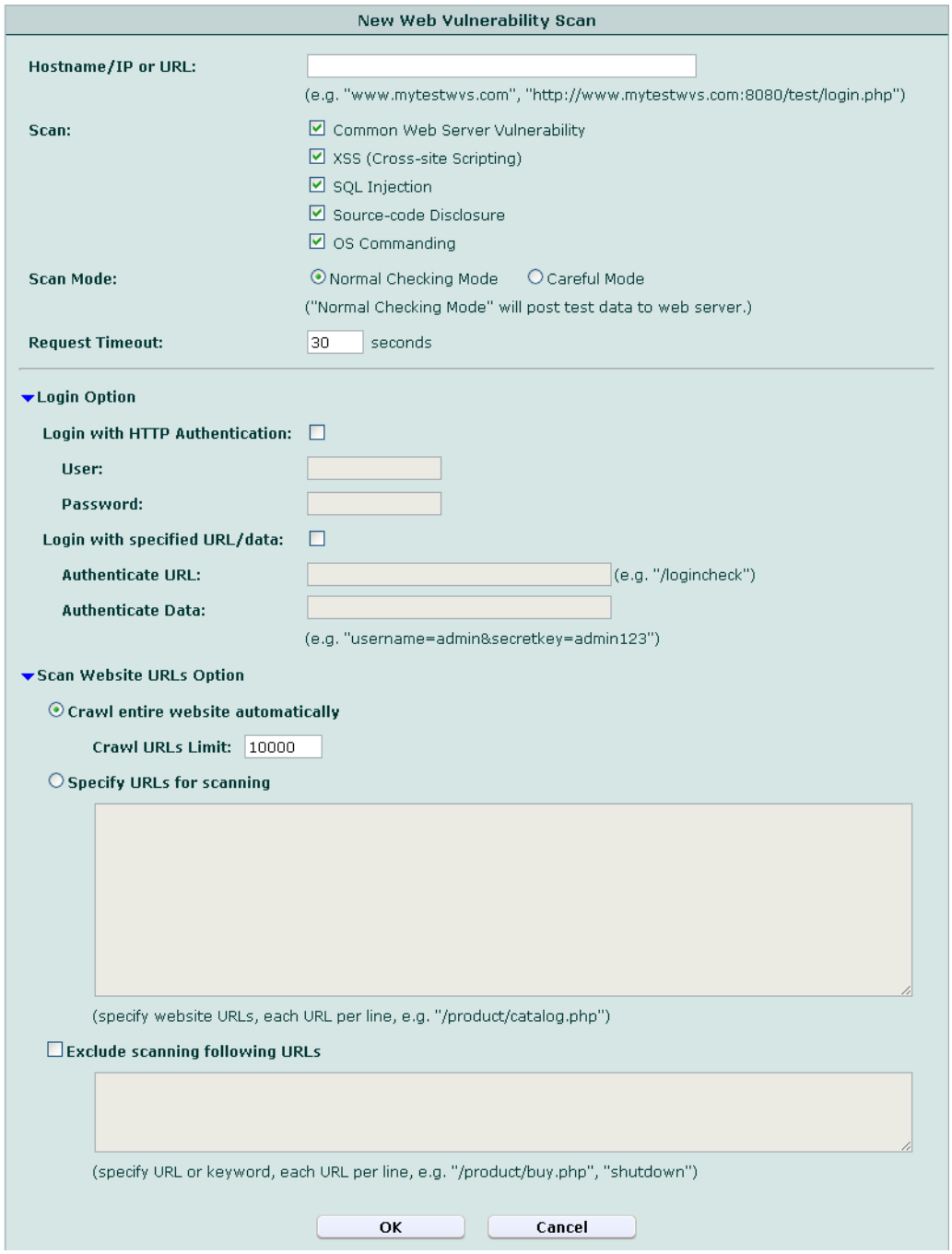

| *Name of the GUI item* | *Description* |
|---|---|
| **New Scan** | Click to configure and perform a scan. |
| **#** | The index number of the entry in the list. |
| **Target Server** | The base URL that was scanned for vulnerabilities. Click to view the scan report. |
| **URLs Processed** | The number of URLs below the base URL that were scanned for vulnerabilities. |
| **Alerts Found** | The total number of vulnerabilities discovered during the scan. |
| **Scan Time** | The date and time when you initiated the scan. |
| **Scan Mode** | Indicates whether the scan job used *Careful Mode* (use HTTP GET only and omit both user-defined and predefined sensitive URLs) or *Normal Checking Mode* (use both HTTP POST and GET, excluding only user-defined URLs). |
| (No column heading.) | Click *View the scan report* to view the report that was summarizes and analyzes a vulnerability scan’s results.<br>Click *View the detail scan log* to view the vulnerability scanner’s log for the scan job.<br>Click *Delete the scan report* to remove the report. |

### To configure a vulnerability scan

1 Go to *Web Vulnerability Scan* > *Web Vulnerability Scan* > *Web Vulnerability Scan*.

2 Click *New Scan*.

3 Configure the following, then click *OK*:



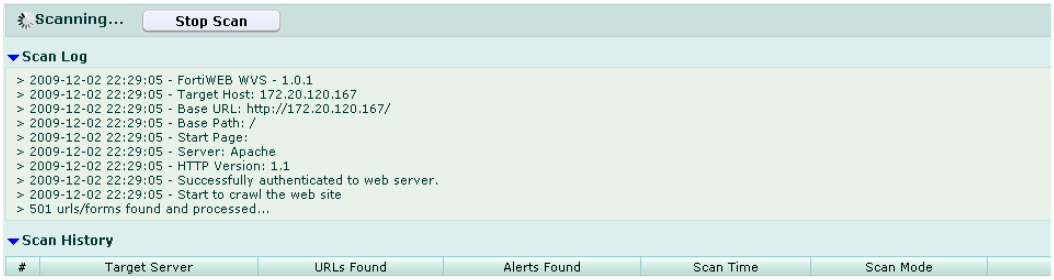
| *Name of the GUI item* | *Description* |
|---|---|
| **Hostname/IP or URL** | Type the fully qualified domain name (FQDN), IP address, or full URL to indicate which directory of the web site you want to scan. Behavior of the scan varies by the type of the entry:<br>• **FQDN/IP such as www.example.com:** Assume HTTP and scan the entire web site located on this host.<br>• **Partial URL such as https://webmail.example.com/dir1/:** Use the protocol specified in the URL, and scan the web pages located in this directory of the web site. Other directories will be ignored.<br>• **Full URL such as http://example.com/dir1/start.jsp:** Use the protocol specified in the URL, starting from the web page in the URL, and scan all local URLs reachable via links from this web page that are located within the same subdirectory.<br>Links to external web sites and redirects using HTTP 301 (Moved Permanently) or 302 (Moved Temporarily or Found) will not be followed.<br>Unless you will enter an IP address for the host, you must have configured a DNS server that the FortiWeb unit can use to query for the FQDN. For details, see "Configuring the DNS settings" on page 42.<br>**Note:** This starting point for the scan can be overridden if the web server automatically redirects the request after authentication. See "Login with HTTP Authentication" and "Login with specified URL/data" on page 247. |
| **Scan** | Enable detection of any of the following vulnerabilities that you want to include in the scan report:<br>• **Common Web Server Vulnerability** (outdated software and software with known memory leaks, buffer overflows, and other problems)<br>• **XSS (Cross-site Scripting)**<br>• **SQL Injection**<br>• **Source Code Disclosure**<br>• **OS Commands** |
| **Scan Mode** | Select whether the scan job will use *Careful Mode* (use HTTP `GET` only and omit both user-defined and predefined sensitive URLs) or *Normal Checking Mode* (use both HTTP `POST` and `GET`, excluding only user-defined URLs).<br>Also configure *Exclude scanning following URLs*.<br>*Careful Mode* will avoid alterations to the web site's databases, but ***only*** if all inputs always uses `POST` requests. It also omits testing of the following URLs, which could be sensitive:<br>• /formathd<br>• /formatdisk<br>• /shutdown<br>• /restart<br>• /reboot<br>• /reset<br>**Caution:** Fortinet strongly recommends that you do ***not*** scan for vulnerabilities on live web sites, even if you use *Careful Mode*. Instead, duplicate the web site and its database into a test environment, and then use *Normal Checking Mode* with that test environment.<br>*Careful Mode* cannot be guaranteed to be non-destructive. Many web sites accept input through HTTP `GET` requests, and so it is possible that a vulnerability scan could result in database changes, even though it does not use `POST`. In addition, *Careful Mode* cannot test for vulnerabilities that are only discoverable through `POST`, and therefore may not find all vulnerabilities. |
| **Request Timeout** | Type the number of seconds for the vulnerability scanner to wait for a response from the web site before it assumes that the request will not successfully complete, and continues with the next request in the scan. It will not retry requests that time out. |

| | |
|---|---|
| **Delay Between Each Request** | Type the number of seconds to wait between each request.<br>Some web servers may rate limit the number of requests, or black list clients that issue continuous requests and therefore appear to be a web site harvester or denial of service (DoS) attacker. Introducing a delay can be useful to prevent the vulnerability scanner from being blacklisted or rate limited, and therefore slow or unable to complete its scan. |
| **Login Option** | |
| **Login with HTTP Authentication** | Enable to use basic HTTP authentication if the web server returns HTTP 401 (Unauthorized) to request authorization. Also configure *User* and *Password*.<br>Alternatively, configure *Login with specified URL/data*.<br>After authentication, if the web server redirects the request (HTTP 302), the FortiWeb unit will use this new web page as its starting point for the scan, replacing the URL that you configured in *Hostname/IP or URL*.<br>**Note:** If a web site requires authentication and you do not configure the vulnerability scan to authenticate, the scan results will be incomplete. |
| **User** | Enter the user name to provide to the web site if it requests HTTP authentication. |
| **Password** | Enter the password of the user name. |
| **Login with specified URL/data** | Enable to authenticate if the web server does ***not*** use HTTP 401, but instead provides a web page with a form that allows the user to authenticate using HTTP `POST`. Also configure *Authenticate URL* and *Authenticate Data*.<br>After authentication, if the web server redirects the request (HTTP 302), the FortiWeb unit will use this new web page as its starting point for the scan, replacing the URL that you configured in *Hostname/IP or URL*.<br>**Note:** If a web site requires authentication and you do not configure the vulnerability scan to authenticate, the scan results will be incomplete. |
| **Authenticate URL** | Type the URL, such as `/login.jsp`, that the vulnerability scan will use to authenticate before beginning the scan. |
| **Authenticate Data** | Type the parameters, such as `userid=admin&password=Re2b8WyUI`, that will be accompany the HTTP `POST` request to the authentication URL, and contains the values necessary to authenticate. Typically, this string will include user name and password parameters, but may contain other variables, depending on the web page. |
| **Scan Website URLs Option** | |
| **Crawl entire website automatically** | Select this option to automatically follow links leading from the initial starting point that you configured in *Hostname/IP or URL*. The vulnerability scanner will stop following links when it has scanned the number of URLs configured in *Crawl URLs Limit*.<br>Alternatively, select *Specify URLs for scanning*. |
| **Crawl URLs Limit** | Type the maximum number of URLs to scan for vulnerabilities while automatically crawling links leading from the initial starting point.<br>**Note:** The actual number of URLs scanned could exceed this limit if the vulnerability scanner reaches the limit but has not yet finished crawling all of the links on a page that it has already started to scan. |

| | |
|---|---|
| **Specify URLs for scanning** | Select this option to manually specify which URLs to scan, such as `/login.do`, rather than having the vulnerability scanner automatically crawl the web site. Enter each URL on a separate line in the text box.<br>You can enter up to 10,000 URLs. |
| **Exclude scanning following URLs** | Enable to exclude specific URLs, such as `/addItem.cfm`, from the vulnerability scan. Enter each URL on a separate line in the text box.<br>This may be useful to accelerate the scan if you know that some URLs do not need scanning. It could also be useful if you are scanning a live web site and wish to prevent the scanner from inadvertently adding information to your databases.<br>You can enter up to 1,000 URLs. |

The vulnerability scanner connects to the starting point that you configured for the scan and, if enabled to do so, authenticates. While the scan is progressing, it displays the current activity in the *Scan Log* section, and a *Stop Scan* button that enables you to cancel the scan.

**Figure 23: Vulnerability scan in progress**

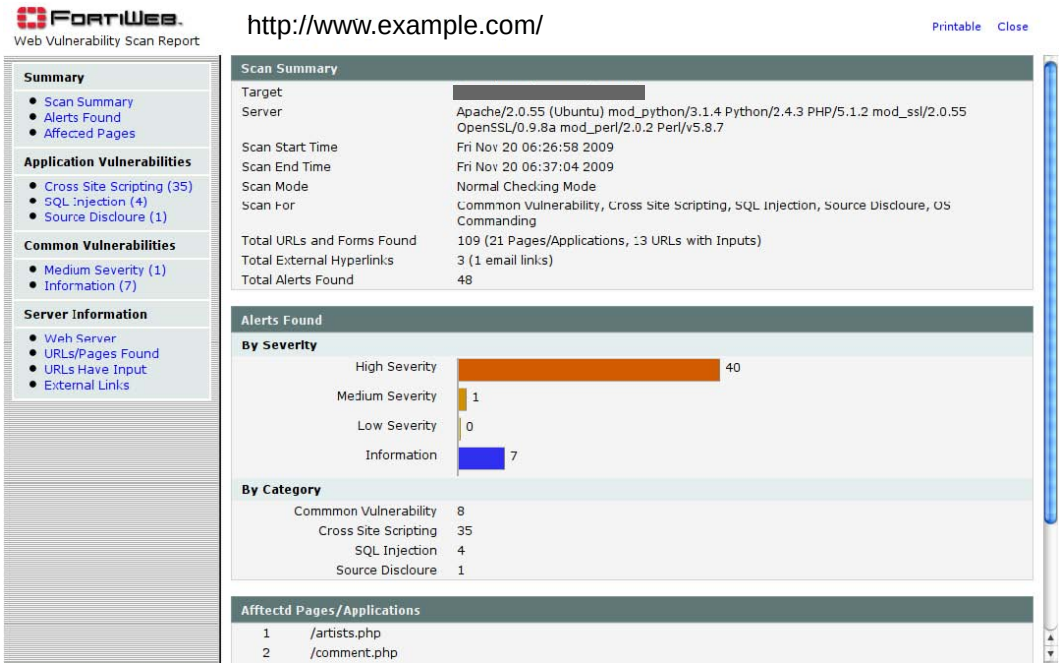



When the scan is complete, you can view the resulting report. For details, see "Viewing a vulnerability report" on page 248.

# Viewing a vulnerability report

After making a vulnerability scan, the FortiWeb unit generates a report summarizing and analyzing its results.

**Figure 24: Viewing a vulnerability report**




While viewing the *Application Vulnerabilities* section of the report, if any vulnerability of each type (cross-site scripting, etc.) is detected, the vulnerability is described for each URL, including:

- type
- severity
- URI
- method
- response header
- response body

To view the web server's response to the request for that part of the scan, click *View*.

If after viewing the response you determine that the result is a false positive, click *False Positive*. The false positive status will be saved and visible in any subsequent printout or view of the report, helping to remind you that particular item should be ignored.

# Log&Report

The *Log & Report* menu enables you to configure logging, reports, and alert email. It also enables you to view locally stored log messages using the web-based manager.

FortiWeb units provide extensive logging capabilities for traffic, system and network protection functions. Detailed log information enables you to analyze network activity to identify security issues and reduce network misuse and abuse.

This section includes the following topics:



## About logging

FortiWeb units can log many different network activities and traffic including:

- overall network traffic
- system-related events including system restarts and HA activity
- matches of policies whose *Action* include *Alert*

For more information about log types, see “Log types” on page 251.

You can select which severity level log messages must meet in order to be recorded. For more information, see “Log message severity levels” on page 252.

A FortiWeb unit can save log messages to its memory, or to a remote location such as a Syslog server or FortiAnalyzer™ unit. For more information, see “Configuring logging and alerts” on page 252. It can also use log messages as the basis for reports. For more information, see “Configuring and generating reports” on page 268.

### Log types

FortiWeb units can record the following categories of log messages:

**Table 92: Log types**

| Log file type | Description |
|---|---|
| Event | Administration events such as downloading a backup copy of the configuration |
| Traffic | Traffic flow information such as HTTP requests and, if a reply was permitted by the policy, HTTP responses |
| Attack | Attack and intrusion attempt events |

**Caution:** Avoid recording highly frequent log types such as traffic logs to the local hard disk for an extended period of time. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.

### Log message severity levels

Each log message contains a field that indicates the severity level of the log message, such as `pri=warning`.

**Table 93: Log severity levels**

| Levels | Description |
|---|---|
| 0 - Emergency | The system has become unusable. |
| 1 - Alert | Immediate action is required. |
| 2 - Critical | Functionality is affected. |
| 3 - Error | An error condition exists and functionality could be affected. |
| 4 - Warning | Functionality could be affected. |
| 5 - Notification | Information about normal events. |
| 6 - Information | General information about system operations. |

For each location where the FortiWeb unit can store log files, you can define the severity threshold of the log messages that will be stored there: the FortiWeb unit will store all log messages equal to or exceeding the severity level you select.

**Caution:** Avoid recording log messages using low severity thresholds such as *Information* or *Notification* to the local hard disk for an extended period of time. A low log severity threshold is one possible cause of frequent logging. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.

For example, if you select *Error*, the FortiWeb unit will store log messages whose severity level is *Error*, *Critical*, *Alert*, or *Emergency*.

## Configuring logging and alerts

When diagnosing problems or tracking actions that the FortiWeb unit performs as it receives and processes traffic, you may find it useful to configure the FortiWeb unit to record log messages. You may also find it useful to configure log-based alerts.

You can configure the FortiWeb unit to store log messages either or both locally (that is, in RAM or to the hard disk) and remotely (that is, on a Syslog server or FortiAnalyzer unit). Your choice of storage location may be affected by several factors, including the following.

- Rebooting the FortiWeb unit clears logs stored in memory.
- Logging only locally may not satisfy your requirements for off-site log storage.
- Very frequent logging may cause undue wear when stored on the local hard drive. A low severity threshold is one possible cause of frequent logging. For more information on severity levels, see “Log message severity levels” on page 252.
- Very frequent logging, such as when the severity level is low, may rapidly consume all available log space when stored in memory. If the available space is consumed, and if the FortiWeb unit is configured to do so, it may store any new log message by overwriting the oldest log message. For high traffic volumes, this may occur so rapidly that you cannot view old log messages before they are replaced. For more information on severity levels, see “Log message severity levels” on page 252.
- Usually, fewer log messages can be stored in memory. Logging to a Syslog server or FortiAnalyzer unit may provide you with additional log storage space.

For information on viewing locally stored log messages, see “Viewing log messages” on page 262.

This section includes the following topics:



## Enabling logging and alerts

*Log&Report* > *Log Config* > *Log Filter* enables you to enable or disable logging for each log type, and to enable or disable alert email for each log type.

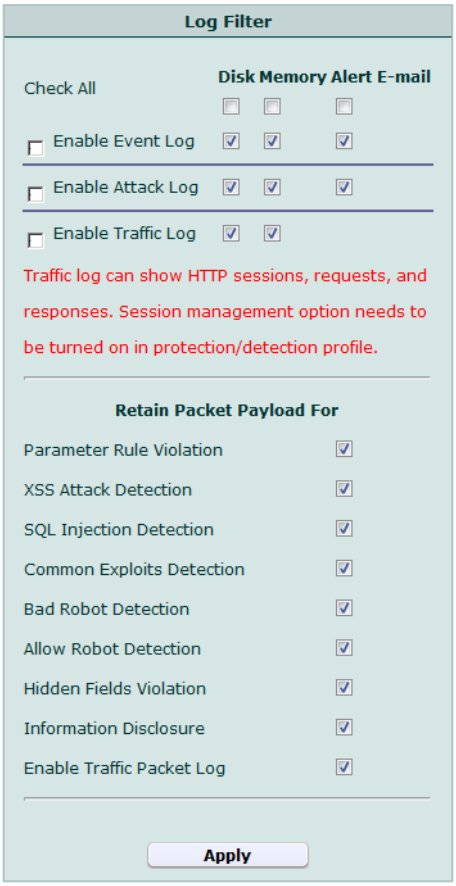
For more information on log types, see "Log types" on page 251.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Log & Report* category. For details, see "About permissions" on page 58.

### To enable logging

1 Go to *Log&Report* > *Log Config* > *Log Filter*.

2 Enable one or more of the following:



| Name of the GUI item | Description |
|---|---|
| **Enable Event Log** | Enable to log system events such as rebooting the FortiWeb unit. |
| **Enable Attack Log** | Enable to log traffic matching policies whose *Action* is *Alert* or *Alert & Deny*. |
| **Enable Traffic Log** | Enable to log traffic events such as HTTP requests and responses, and the expiration of HTTP sessions.<br>**Note:** You must also enable the *Session Management* option in profiles for the traffic that you want to log. |

**Caution:** Avoid recording highly frequent log types such as traffic logs to the local hard disk for an extended period of time. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.

3 In each row corresponding to a log type that you enabled in the previous step, configure the following:

| Name of the GUI item | Description |
|---|---|
| **Disk** | Enable to record log messages of this type to the local hard disk. |
| **Memory** | Enable to record log messages of this type to the local and/or remote log devices you have enabled and configured. For details, see "Configuring logging to memory" on page 258 and "Configuring logging to a Syslog server or FortiAnalyzer unit" on page 259. |
| **Alert E-mail** | Enable to generate alert email for log messages of this type. For details, see "Configuring and testing alerts" on page 260.<br>This option is not available for the traffic log type. |

4 Under *Retain Packet Payload For*, for each of the attack types or validation failures that are detected using a regular expression, such as *XSS Attack Detection* or *Parameter Rule Violation* (that is, an input failed validation), if you want to retain the offending packet payload with its log message, mark the corresponding check box.

Packet payloads supplement the log message by providing the actual data that triggered the regular expression, which may help you to fine-tune your regular expressions to prevent false positives, or to examine changes to attack behavior for subsequent forensic analysis.

If the offending HTTP request exceeds 4 kilobytes (KB), the FortiWeb unit retains only 4 KB' worth of the part of the payload that triggered the log message.

Packet payloads are accessible from the *Packet Log* column when viewing an attack log using the web-based manager. For details, see "Viewing log messages" on page 262.

If packet payloads could contain sensitive information, you may need to obscure those elements. For details, see "Obscuring sensitive data in the logs" on page 255.

5 Also under *Retain Packet Payload For*, if you want to retain regular traffic packet payloads, mark *Enable Traffic Packet Log*. Unlike attack packet payloads, only request direction traffic packets are retained, and only the first 4 kilobytes (KB) of the payload if it is larger.

**Note:** Retaining traffic packet payloads is resource intensive. Only enable this option when absolutely necessary.

Packet payloads are accessible from the *Packet Log* column when viewing a traffic log using the web-based manager. For details, see "Viewing log messages" on page 262.

6 Click *Apply*.

## Obscuring sensitive data in the logs

If enabled to do so, a FortiWeb unit will hide some predefined data types, including user names and passwords, that could appear in the packet payloads accompanying a log message. You can also define your own sensitive data types, such as ages or other identifying numbers, using regular expressions.

**Note:** Sensitive data definitions are ***not*** retroactive. They will hide strings in subsequent log messages, but will not affect existing ones.

### To exclude custom sensitive data from logs' packet payloads

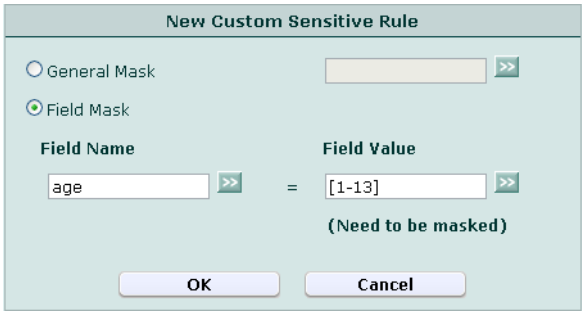
1 Go to *Log&Report* > *Log Config* > *Log Custom Sensitive Rule*.

2 Enable one or both of the following:

- *Enable Predefined Rules*: Use the predefined credit card number and password data types.
- *Enable Custom Rules*: Use your own regular expressions to define sensitive data.

3 If you selected *Enable Custom Rules*, click *Create New*.

4 Select either *General Mask* (a regular expression that will match any substring in the packet payload) or *Field Mask* (a regular expression that will match only the value of a specific form input).




- For *General Mask*, in its field, type a regular expression that matches all and only the strings or numbers that you want to obscure in the packet payloads.

  For example, to hide a parameter that contains the age of users under 13, you could enter:

  `age\=[1-13]`

  Valid expressions must not start with an asterisk ( * ). The maximum length is 21 characters.

- For *Field Mask*, in the left-hand field (*Field Name*), type a regular expression that matches all and only the input names whose values you want to obscure. (The input name itself will ***not*** be obscured. If you wish to do this, use *General Mask* instead.) Then, in the right hand field (*Field Value*), type a regular expression that matches all and only the input values that you want to obscure.

  For example, to hide a parameter that contains the age of users under 13, for *Field Name*, you would enter `age`, and for *Field Value*, you could enter `[1-13]`.

  Valid expressions must not start with an asterisk ( * ). The maximum length is 22 characters.

**Caution:** Field masks using asterisks are greedy: a match for the parameter's value will obscure it, but will ***also*** obscure the rest of the parameters in the line. To avoid this, enter an expression whose match terminates with, but does not consume, the parameter separator.

For example, if parameters are separated with an ampersand ( & ), and you want to obscure the value of the *Field Name* `username` but ***not*** any of the parameters that follow it, you could enter the *Field Value*:

```
.*?(?=\&)
```

This would result in:

```
username****&age=13&origurl=%2Flogin
```

5 Click *OK*.

The expression appears in the list of regular expressions that define sensitive data that will be obscured in the logs.

When viewing new log messages, data types matching your expression will be replaced with a string of * characters equal in length to the sensitive data.

## Configuring logging to the local hard disk

Instead of or in addition to logging remotely, you can store log messages locally, on the hard disk of the FortiWeb unit.

**Note:** Attack logs stored in memory, unlike those stored on disk, contain a *Detail* column when viewed through the web-based manager. This enables you to display the entire log message in a pop-up window. To alternatively or additionally configure logging to memory, see "Configuring logging to memory" on page 258.

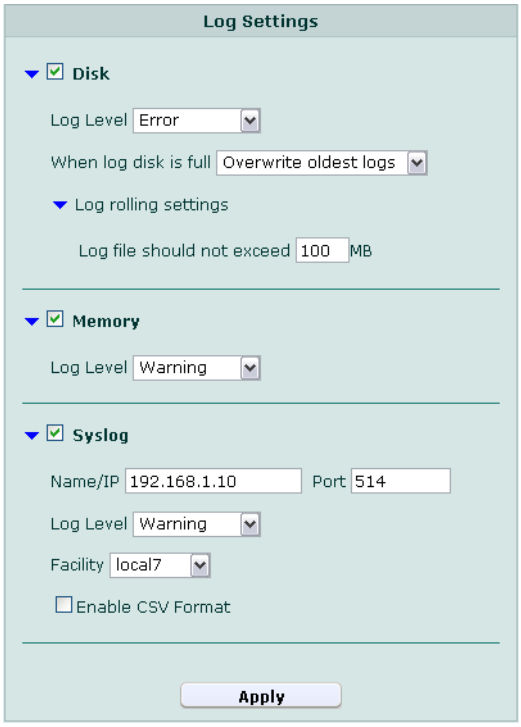
If the FortiWeb unit is logging to its hard disk, you can use the web-based manager to view log messages that are stored locally on the FortiWeb unit. For details, see "Viewing log messages" on page 262.

Before you can log to the hard disk, you must first enable logging. For details, see "Enabling logging and alerts" on page 253. For logging accuracy, you should also verify that the FortiWeb unit's system time is accurate. For details, see "Configuring the time & date" on page 75.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Log & Report* category. For details, see "About permissions" on page 58.

### To configure logging to the hard disk

1 Go to *Log&Report* > *Log Config* > *Log Setting*.




2 Enable *Disk* to log to the hard disk.

3 From *Log Level*, select the severity level that a log message must equal or exceed in order to be recorded to this storage location.

**Caution:** Avoid recording log messages using low severity thresholds such as *Information* or *Notification* to the local hard disk for an extended period of time. A low log severity threshold is one possible cause of frequent logging. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure.

For information about severity levels, see "Log message severity levels" on page 252.

4 From *When disk is full*, select what the FortiWeb unit will do when the local disk is full and a new log message is caused, either:

- *Do not log*: Discard the new log message.
- *Overwrite oldest logs*: Delete the oldest log file in order to free disk space, and store the new log message.

5 From *Log file should not exceed*, enter the maximum file size of the current log file.

When a log file reaches the size limit, the FortiWeb unit will rotate the current log file: that is, it renames the current log file (elog.log) with a file name indicating its sequential relationship to other log files of that type (elog2.log, etc.), then creates a new current log file.

The log file size limit must be between 10 MB and 1,000 MB.

6 Click *Apply*.

## Configuring logging to memory

Instead of or in addition to logging remotely, you can store log messages locally, in the random access memory (RAM) of the FortiWeb unit.

**Caution:** Log messages stored in memory should not be regarded as permanent. All log entries stored in memory are cleared when the FortiWeb unit restarts. When available memory space for log messages is full, the FortiWeb unit will store any new log message by overwriting the oldest log message.

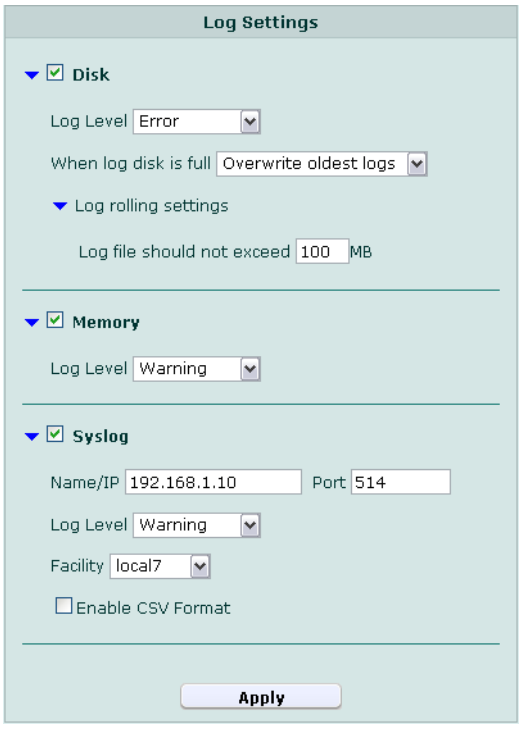
If the FortiWeb unit is logging to memory, you can use the web-based manager to view log messages that are stored locally on the FortiWeb unit. For details, see "Viewing log messages" on page 262.

Before you can log to memory, you must first enable logging. For details, see "Enabling logging and alerts" on page 253. For logging accuracy, you should also verify that the FortiWeb unit's system time is accurate. For details, see "Configuring the time & date" on page 75.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Log & Report* category. For details, see "About permissions" on page 58.

### To configure logging to memory

1 Go to *Log&Report* > *Log Config* > *Log Setting*.




2 Enable *Memory* to log locally to RAM.

3 From *Log Level*, select the severity level that a log message must equal or exceed in order to be recorded to this storage location.

For information about severity levels, see "Log message severity levels" on page 252.

4 Click *Apply*.

## Configuring logging to a Syslog server or FortiAnalyzer unit

Instead of or in addition to logging locally, you can store log messages remotely, on a Syslog server or FortiAnalyzer unit.

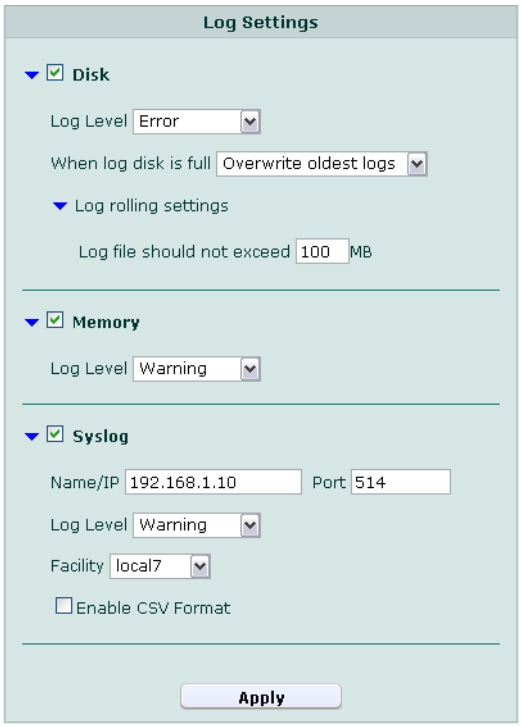
**Note:** Logs stored remotely cannot be viewed from the web-based manager of the FortiWeb unit. If you require the ability to view logs from the web-based manager, also enable local storage. For details, see "Configuring logging to memory" on page 258 or "Configuring logging to the local hard disk" on page 256.

Before you can log to a remote location, you must first enable logging. For details, see "Enabling logging and alerts" on page 253. For logging accuracy, you should also verify that the FortiWeb unit's system time is accurate. For details, see "Configuring the time & date" on page 75.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Log & Report* category. For details, see "About permissions" on page 58.

### To configure logging to a Syslog server or FortiAnalyzer unit

1 Go to *Log&Report* > *Log Config* > *Log Setting*.




2 Enable *Syslog* to log to a remote Syslog server or FortiAnalyzer unit.

3 From *Log Level*, select the severity level that a log message must equal or exceed in order to be recorded to this storage location.

For information about severity levels, see "Log message severity levels" on page 252.

4 Configure the following:

| *Name of the GUI item* | *Description* |
|---|---|
| **Name/IP** | Enter the IP address of the remote Syslog server. |
| **Port** | Enter the listening port number of the Syslog server. |

| | |
|---|---|
| **Facility** | Select the facility identifier that the FortiWeb unit will use to identify itself when sending log messages to the first Syslog server.<br>To easily identify log messages from the FortiWeb unit when they are stored on the Syslog server, enter a unique facility identifier, and verify that no other network devices use the same facility identifier. |
| **Enable CSV format** | Enable to send log messages in comma-separated value (CSV) format.<br>**Note:** Do not enable this option if the remote host is a FortiAnalyzer unit. FortiAnalyzer units do not support CSV-formatted log messages. |

5 Click *Apply*.

6 If the remote host is a FortiAnalyzer unit, confirm with the FortiAnalyzer administrator that the FortiWeb unit has been added to the FortiAnalyzer unit's device list, allocated sufficient disk space quota, and assigned permission to transmit logs to the FortiAnalyzer unit. For details, see the *FortiAnalyzer Administration Guide*.

7 To verify logging connectivity, from the FortiWeb unit, trigger a log message that matches the types and severity levels that you have chosen to store on the remote host. Then, on the remote host, confirm that it has received that log message.

For example, if you have chosen to record event log messages to the remote host if they are more severe than information, you could log in to the web-based manager or download a backup copy of the FortiWeb unit's configuration file in order to trigger an event log message.

If the remote host does not receive the log messages, verify the FortiWeb unit's network interfaces (see "Configuring the network interfaces" on page 34) and static routes (see "Configuring static routes" on page 81), and the policies on any intermediary firewalls or routers. If ICMP ECHO (ping) is enabled on the remote host, you may be able to use the `execute traceroute` command to determine the point where connectivity fails. For details, see the *FortiWeb CLI Reference*.

## Configuring and testing alerts

*Log&Report* > *Log Config* > *Alert E-mail* enables you to configure the FortiWeb unit to send an email message to alert administrators or other personnel when an alert condition occurs, such as a system failure or network attack.

If the alert condition continues to occur, the FortiWeb unit will send only one alert email for each configured interval following the initial alert condition.

For example, you might configure the FortiWeb unit to send only one alert message for each 15-minute interval after *Warning*-level log messages begin to be recorded. In that case, if the alert condition continues to occur for 35 minutes after the first *Warning*-level log message, the FortiWeb unit would send a total of three alert email messages, no matter how many *Warning*-level log messages were recorded during that period of time.

Intervals are configured separately for each severity level of log message. For more information on the severity levels of log messages, see "Log message severity levels" on page 252.

Before you can send alerts, you must enable alert email for the log type that you want to use as a trigger. For details, see "Enabling logging and alerts" on page 253.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Log & Report* category. For details, see "About permissions" on page 58.

### To configure alerts

1 Go to *Log&Report* > *Log Config* > *Alert E-mail*.

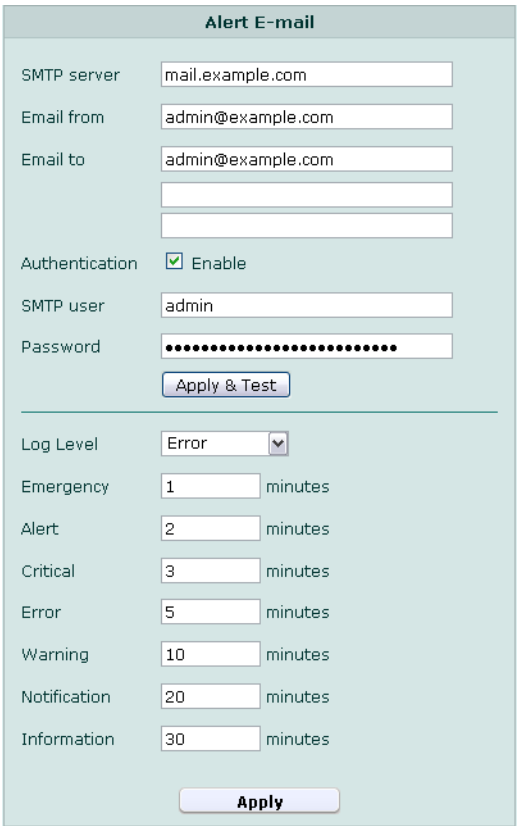
2 In *SMTP server*, enter the fully qualified domain name (FQDN) or IP address of the SMTP relay or server that the FortiWeb unit will use to send alerts and generated reports.

**Caution:** If you enter a domain name, you must also configure the FortiWeb unit with at least one DNS server. Failure to configure a DNS server may cause the FortiWeb unit to be unable to resolve the domain name, and therefore unable to send the alert. For information on configuring use of a DNS server, see "Configuring the DNS settings" on page 42.

3 Click *Apply*.

The remaining fields become available.

4 Configure the following:




| *Name of the GUI item* | *Description* |
|---|---|
| **Email from** | Enter the sender email address that the FortiWeb unit will use when sending alert email messages. |
| **Email to** | Enter one to three recipient email addresses, one per field. |
| **Authentication** | Enable to authenticate with the SMTP relay when sending alerts. |
| **SMTP user** | Enter the user name of the account on the SMTP relay that will be used to send alerts.<br>This option is available only if *Authentication* is enabled. |
| **Password** | Enter the password of the account on the SMTP relay that will be used to send alerts.<br>This option is available only if *Authentication* is enabled. |
| **Apply & Test** | Click to save the alert configuration and send a sample alert. |

| | |
|---|---|
| **Log Level** | Select the severity threshold condition that log messages must meet or exceed in order to cause an alert. For more information on severity levels, see “Log message severity levels” on page 252. |
| **Emergency** | Enter the number of minutes between each alert if an alert condition of severity level *Emergency* continues to occur after the initial alert. |
| **Alert** | Enter the number of minutes between each alert if an alert condition of severity level *Alert* continues to occur after the initial alert. |
| **Critical** | Enter the number of minutes between each alert if an alert condition of severity level *Critical* continues to occur after the initial alert. |
| **Error** | Enter the number of minutes between each alert if an alert condition of severity level *Error* continues to occur after the initial alert. |
| **Warning** | Enter the number of minutes between each alert if an alert condition of severity level *Warning* continues to occur after the initial alert. |
| **Notification** | Enter the number of minutes between each alert if an alert condition of severity level *Notification* continues to occur after the initial alert. |
| **Information** | Enter the number of minutes between each alert if an alert condition of severity level *Information* continues to occur after the initial alert. |

5 Click *Apply & Test*.

The FortiWeb unit saves the alert configuration and sends a sample alert.

# Viewing log messages

If you have configured the FortiWeb unit to store log messages locally (that is, to memory or the hard disk), you can view the log messages currently stored in each file.

Log messages are in human-readable format, where each log field’s name, such as *Source* (`src` in *Raw* view), indicates its contents.

Exceptions include the attack log’s *Message* (`msg`) field, which contains a code such as `DETECT_PARAM_RULE_FAILED` that indicates which feature detected the attack. For each feature’s attack detection code, see the feature’s description located in this Administration Guide.

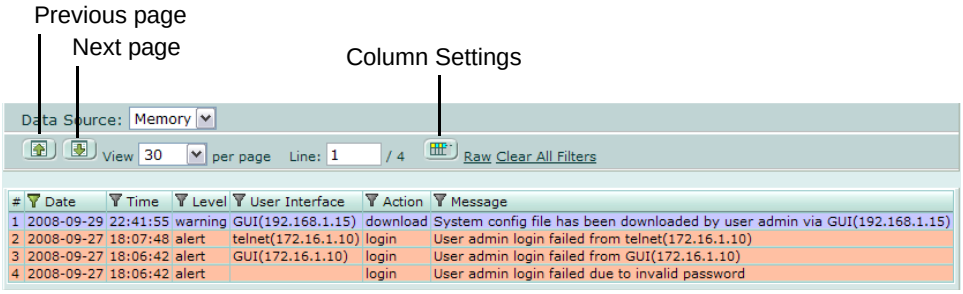
**Note:** Not all detected attacks may be blocked, redirected, or sanitized.

For example, while using auto-learning, you can configure protection profiles with an action of *Alert* (log but not deny), allowing the connection to complete in order to gather full auto-learning data.

To determine whether or not an attack attempt was permitted to reach a web server, show the *Action* column. For details, see “Displaying and arranging log columns” on page 265.

When viewing log messages, you can customize aspects of the display to focus on log messages and fields that match your criteria. For more information, see “Customizing the log view” on page 264.

**Table 94: Viewing log messages**




| *Name of the GUI item* | *Description* |
|---|---|
| **Data Source** | Select either *Memory* to display logs stored in the FortiWeb unit's random access memory (RAM), or *Disk* to display logs stored on the FortiWeb unit's hard disk. For information on configuring log storage to RAM or the hard disk, see "Configuring logging to the local hard disk" on page 256 or "Configuring logging to memory" on page 258. |
| **Previous page** | Click to view the previous page. |
| **Next page** | Click to view the next page. |
| **View *n* per page** | Click the number of rows of log entries to display per page. |
| **Line** | Enter a log entry number, then press Enter to go to that entry. The number following the slash ( / ) is the total number of entries in the log file. |
| **Column Settings** | Click to display or hide the columns that correspond to log fields, or change the order in which they appear on the page. For more information, see "Displaying and arranging log columns" on page 265. |
| **Raw** or **Formatted** | Click *Raw* to display the log message as it actually appears in the log file. This option appears if you are currently viewing log messages in *Formatted* format.<br>Click *Formatted* to display the log files in columnar format. This option appears if you are currently viewing log messages in *Raw* format.<br>For details on both view types, see "Customizing the log view" on page 264. |
| **Clear All Filters** | Click to remove log view filters. For details on log view filters, see "Filtering log messages" on page 266. |

### To view log messages

1 Go to *Log&Report* > *Log Access*.

2 Click the tab corresponding to the type of log file that you want to view (*Event*, *Attack*, or *Traffic*).

For more information on log types, see "Log types" on page 251.

To be able to access this part of the web-based manager, in your administrator account's access profile, you must have both *Read* and *Write* permission to items in the *Log & Report* category. For details, see "About permissions" on page 58.

**Tip:** If there are no traffic logs, verify that you have enabled *Session Management* in the profiles whose traffic you want to log.

3 From *Data Source*, select either *Memory* to view logs stored in either random access memory (RAM), or *Disk* to view logs stored on the hard disk.

For more information on configuring the Fortinet unit to store log messages locally, see "Configuring logging to the local hard disk" on page 256 or "Configuring logging to memory" on page 258.

**Note:** Attack logs stored in memory, unlike those stored on disk, contain a *Detail* column when viewed through the web-based manager. This enables you to display the entire log message in a pop-up window.

4 If you are viewing log files stored on the hard disk, in the row corresponding to a log file, click either:

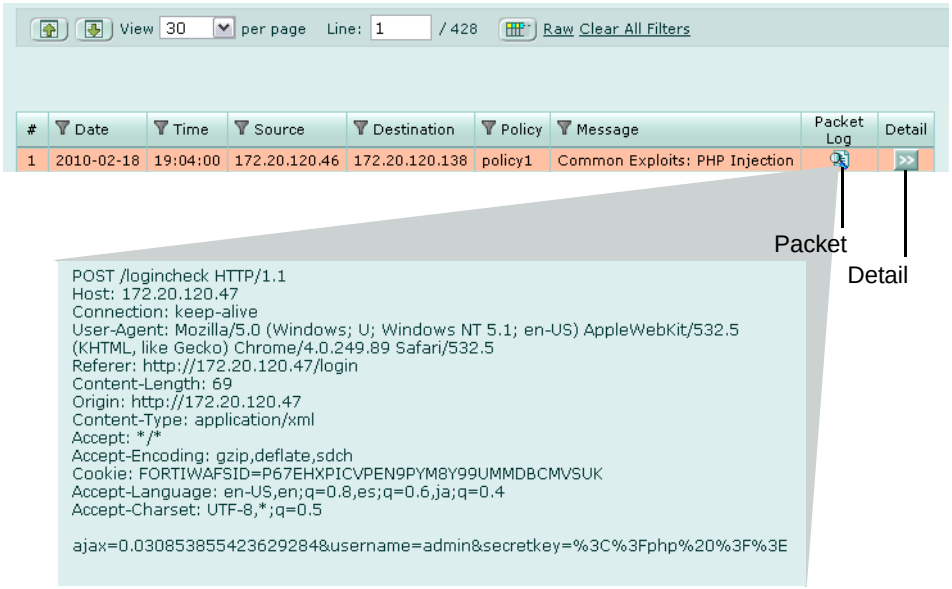
- *View* to display the file's log messages within the web-based manager, or
- *Download* to download the log file to your management computer, then select either *Normal format* (raw, plain text logs) or *CSV format* (comma-separated value). If you would like to password-encrypt the log files before downloading them, also enable *Encryption* and type a password in *Password*. Finally, click *OK*.

  Raw, unencrypted logs can be viewed with a plain text editor. CSV-formatted, unencrypted logs can be viewed with a spreadsheet application, such as Microsoft Excel or OpenOffice Calc.

**Note:** If the attack was detected using a regular expression, and you have enabled retention of packet payloads in "Enabling logging and alerts" on page 253, attack logs contain a *Packet Log* column. Clicking its *Packet* icon displays the correlating decoded packet payload in a pop-up window, supplementing the log message by providing the actual data that triggered the regular expression, which may help you to fine-tune your regular expressions to prevent false positives, or aid in forensic analysis.

Traffic logs also contain *Packet Log* and *Detail* columns. However, traffic logs do not require that you first enable packet payload retention: they are automatically kept for all requests.

**Figure 25: Viewing an attack's packet payload or detailed log message**




To focus the web-based manager's display on specific log messages and fields that you want to view, see "Customizing the log view" on page 264. For attack logs, to group multiple similar log messages into sets, see "Grouping similar attack log messages" on page 267.

## Customizing the log view

Log messages can be displayed in either *Raw* or *Formatted* view.

- Raw view displays log messages exactly as they appear in the log file.
- Formatted view displays log messages in a columnar format. Each log field in a log message appears in its own column, aligned with the same field in other log messages, for rapid visual comparison. When displaying log messages in *Formatted* view, you can customize the log view by hiding, displaying and arranging columns and/or by filtering columns, refining your view to include only those log messages and fields that you want to see.

**To display logs in Raw or Formatted view**

1 Go to the tab corresponding to the type of log file that you want to view, such as *Log&Report* > *Log Access* > *Event*.

2 Click *Formatted* or *Raw*.

If you click *Formatted*, options appear that enable you to display and arrange log columns and/or filter log columns.

**Figure 26: Viewing log messages (formatted)**

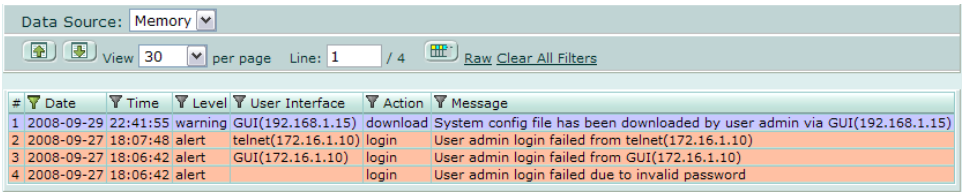
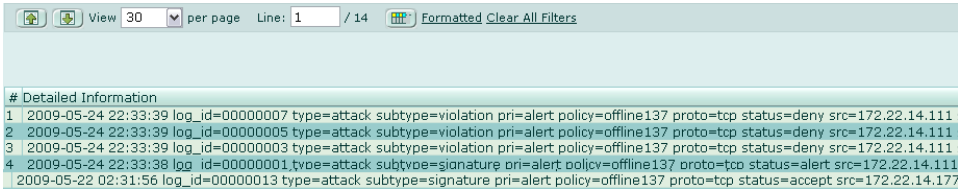



**Figure 27: Viewing log messages (raw)**

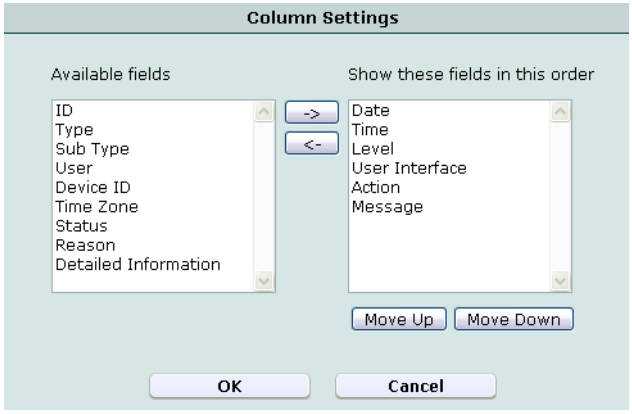



## Displaying and arranging log columns

When viewing logs in *Formatted* view, you can display, hide and re-order columns to display only relevant categories of information in your preferred order.

For most columns, you can also filter data within the columns to include or exclude log messages which contain your specified text in that column. For more information, see “Filtering log messages” on page 266.

**Figure 28: Displaying and arranging log columns**




### To display or hide columns

1 Go to the tab corresponding to the type of log file that you want to view, such as *Log&Report* > *Log Access* > *Event*.

2 Click *Column Settings*.

Lists of available and displayed columns for the log type appear.

3 Select which columns to hide or display.

- In the *Available fields* area, select the names of individual columns you want to display, then click the single right arrow to move them to the *Show these fields in this order* area.
- In the *Show these fields in this order* area, select the names of individual columns you want to hide, then click the single left arrow to move them to the *Available fields* area.
- To return all columns to their default displayed/hidden status, click *Default*.

4 Click *OK*.

### To change the order of the columns

1 Go to the tab corresponding to the type of log file that you want to view, such as *Log&Report* > *Log Access* > *Event*.

2 Click *Column Settings*.

Lists of available and displayed columns for the log type appear.

3 In the *Show these fields in this order* area, select a column name whose order of appearance you want to change.

4 Click *Move Up* or *Move Down* to move the column in the ordered list.

Placing a column name towards the top of the *Show these fields in this order* list will move the column to the left side of the *Formatted* log view.

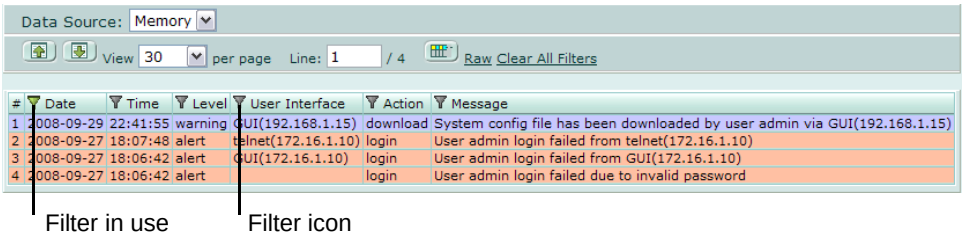
5 Click *OK*.

## Filtering log messages

When viewing log messages in Formatted view, you can filter columns to display only those log messages that do or do not contain your specified content in that column. By default, most column headings contain a gray filter icon, which becomes green when a filter is configured and enabled.

**Note:** Filters do not appear in *Raw* view.

**Figure 29: Filter icons**




### To filter log messages by column contents

1 In the heading of the column that you want to filter, click the filter icon.

2 If you want to ***exclude*** log messages with matching content in this column, mark the check box named *NOT*.

If you want to ***include*** log messages with matching content in this column, clear the check box named *NOT*.

3 Enter the text that matching log messages must contain.

Matching log messages will be excluded or included in your view based upon whether you have marked or cleared *NOT*.

4 Click *OK*.

A column's filter icon is green when the filter is currently enabled.

### To disable a filter

1 In the heading of the column whose filter you want to disable, click the filter icon.

A column's filter icon is green when the filter is currently enabled.

2 To disable the filter on this column, clear the check box named *Enable*.

Alternatively, to disable the filters on all columns, click *Clear All Filters*.

3 Click *OK*.

A column's filter icon is gray when the filter is currently disabled.

## Grouping similar attack log messages

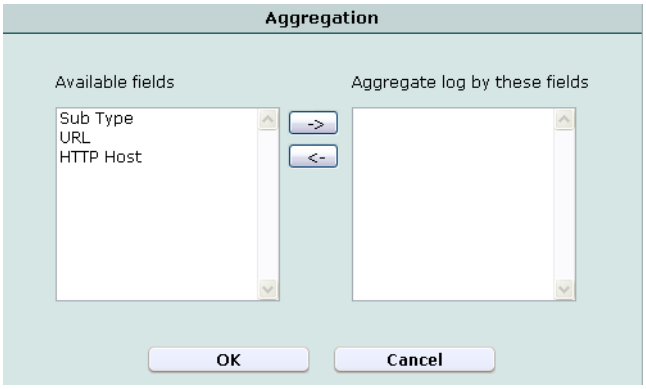
When viewing attack log messages, especially if there are many attacks of the same kind, to the same URL, or to the same web host, you may find it easier to view the log messages when these log messages are grouped by one of those similarities, rather than by sequential order.

### To group similar attack log messages

1 Click *Log Message Aggregation*.

2 In *Available fields*, select which aspect you want to use when grouping the log messages, then click the right arrow to move it to the *Aggregate log by these fields* area.

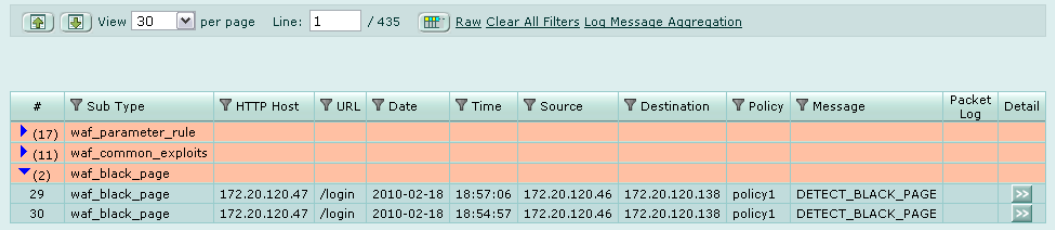
**Figure 30: Selecting the log message grouping type**




**3** Click *OK*.

Attack log messages are no longer in sequential order, but are instead grouped by the similar aspect you selected. To view log messages in a group, click the arrow in that column to expand the set.

**Figure 31: Attack log messages viewed when grouped by attack subtype**




# Configuring and generating reports

*Log&Report* > *Report Config* > *Report Config* enables you to configure and generate reports.

When generating a report, FortiWeb units collate information collected from its log files and present the information in tabular and graphical format.

In addition to log files, FortiWeb units require a report profile to be able to generate a report. A report profile is a group of settings that contains the report name, file format, subject matter, and other aspects that the FortiWeb unit considers when generating the report.

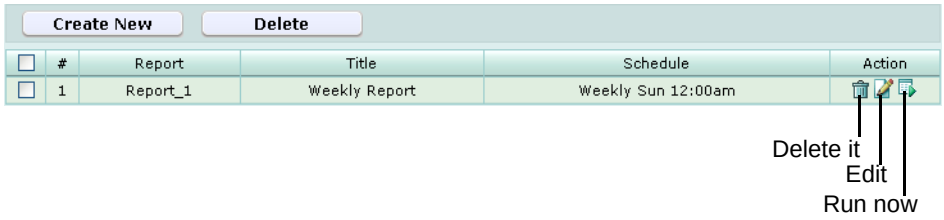
FortiWeb units can generate reports automatically, according to the schedule that you configure in the report profile, or manually, when you click *Run now* in the report profile list. You may want to create one report profile for each type of report that you will generate on demand or periodically, by schedule.

**Note:** Generating reports can be resource intensive. To avoid email processing performance impacts, you may want to generate reports during times with low traffic volume, such as at night. For more information on scheduling the generation of reports, see "Configuring the schedule of a report profile" on page 274.

Before you generate a report, collect log data that will be the basis of the report. For information on enabling logging to the local hard disk, see “Configuring logging to the local hard disk” on page 256.

To be able to access this part of the web-based manager, in your administrator account’s access profile, you must have *Read* permission to items in the *Log & Report* category. For details, see “About permissions” on page 58.

**Table 95:** *Report Config* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Create New** | Click to add a new report profile. For more information, see “Configuring a report profile” on page 269. |
| **Delete** | In the check box column, mark the check boxes of the report profiles that you want to remove, then click *Delete*. Alternatively, click the *Delete it* icon in the row corresponding to each report profile that you want to remove. |
| (Check box in column heading.) | To remove ***all*** report profiles, mark the check box in the column heading to select all report profiles, then click *Delete*.<br>To remove ***individual*** report profiles, mark the check box corresponding to each report profile that you want to remove, then click *Delete*. |
| **Report** | The name of the report profile. |
| **Title** | The title of this report. |
| **Schedule** | The scheduled frequency when the FortiWeb unit generates the report.<br>If this report is not scheduled to be periodically generated according to the schedule configured in the report profile, but instead will be generated only on demand, when you manually click *Run now*, *None* appears in this column. |
| **Action** | Click *Delete it* to remove the report profile.<br>Click *Edit* to modify the report profile. For more information, see “Configuring a report profile” on page 269.<br>Click *Run now* to immediately generate a report using this report profile. This option can be used with both scheduled and on demand report profiles, and occurs independently of any automatic report generation schedules you may have configured. For more information, see “Configuring the schedule of a report profile” on page 274. To view the resulting report, see “Viewing and downloading reports” on page 277. |

## Configuring a report profile

You can create report profiles to define what information will appear in generated reports.

To be able to access this part of the web-based manager, in your administrator account’s access profile, you must have both *Read* and *Write* permission to items in the *Log & Report* category. For details, see “About permissions” on page 58.

### To configure a report profile

1. Go to *Log&Report* > *Report Config* > *Report Config*.
2. Click *Create New* to add a report profile, or click *Edit* to modify an existing report profile.

3 In *Report Name*, enter a name for the report profile.

Report names cannot include spaces.

4 If you are creating or cloning a new report profile, select from *Type* either to run the report immediately after configuration (*On Demand*) or run the report at configured intervals (*On Schedule*).

**Note:** For on-demand reports, the FortiWeb unit does ***not*** save the report profile after the generating the report. If you want to save the report profile, but do not want to generate the report at regular intervals, select *On Schedule*, but then in the *Schedule* section, select *Not Scheduled*.

**Note:** You cannot change the *Type* when editing a report profile. To change the scheduled/on demand *Type*, create a new report profile instead.

5 In *Report Title*, enter a name that will appear in the title area of the report. The title may include spaces.

6 In *Description*, enter a comment or other description.

7 Click the blue arrow next to each section, and configure the following:

| *Name of the section* | *Description* |
|---|---|
| **Properties** | Select to add logos, headers, footers and company information to customize the report. For more information, see "Configuring the headers, footers, and logo of a report profile" on page 270. |
| **Report Scope** | Select the time span of log messages from which to generate the report. For more information, see "Configuring the time period and log filter of a report profile" on page 271. |
| **Report Type(s)** | Select one or more subject matters to include in the report. For more information, see "Configuring the query selection of a report profile" on page 273. |
| **Report Format** | Select the number of top items to include in ranked report subtypes, and other advanced features. For more information, see "Configuring the advanced options of a report profile" on page 274. |
| **Schedule** | Select when the FortiWeb unit will run the report, such as weekly or monthly. For more information, see "Configuring the schedule of a report profile" on page 274.<br>This section is available only if *Type* is *On Schedule*. |
| **Output** | Select the file format(s) and destination email addresses, if any, of reports generated from this report profile. For more information, see "Configuring the output of a report profile" on page 275. |

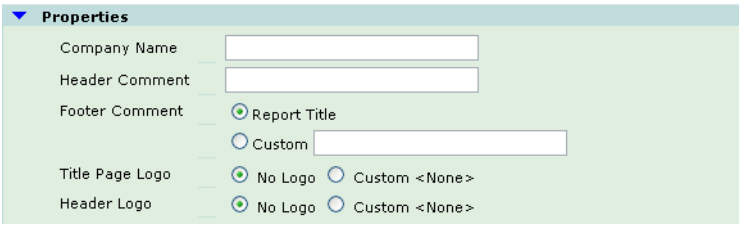
8 Click *OK*.

On-demand reports are generated immediately; scheduled reports, if you have configured a schedule, are generated at those intervals. For information on viewing generated reports, see "Viewing and downloading reports" on page 277.

## Configuring the headers, footers, and logo of a report profile

When configuring a report profile, you can provide text and logos to customize the appearance of reports generated from the profile.

**Table 96:** *Properties* **section of a report profile**




| *Name of the GUI item* | *Description* |
|---|---|
| **Company Name** | Enter the name of your company or other organization. |
| **Header Comment** | Enter a title or other information to include in the header. |
| **Footer Comment** | Select which information to include in the footer:<br>• *Report Title*: Use the text from *Report Name*.<br>• *Custom*: Use other text that you type into the field to the right of this option. |
| **Title Page Logo** | Select either *No Logo* to omit the title page logo, or *Custom* to include a logo, then locate the logo file and click *Upload* to save it to the FortiWeb unit's hard disk for use in the report title page. |
| **Header Logo** | Select either *No Logo* to omit the header logo, or *Custom* to include a logo, then locate the logo file and click *Upload* to save it to the FortiWeb unit's hard disk for use in the report header. The header logo will appear on every page in PDF- and Microsoft Word (RTF)-formatted reports, and at the top of the page in HTML-formatted reports. |

When adding a logo to the report, select a logo file format that is compatible with your selected file format outputs. If you select a logo that is not supported for a file format, the logo will not appear in that output. For example, if you provide a logo graphic in WMF format, it will not appear in PDF or HTML output.

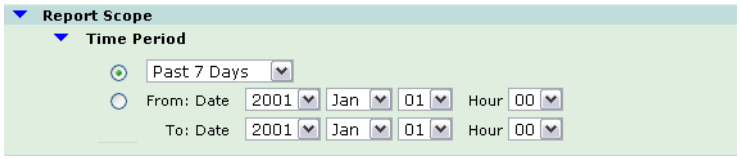
**Table 97: Report file formats and their supported logo file formats**

| | |
|---|---|
| **PDF reports** | JPG, PNG, and GIF |
| **RTF reports** | JPG, PNG, GIF, and WMF |
| **HTML reports** | JPG, PNG, and GIF |

## Configuring the time period and log filter of a report profile

When configuring a report profile, you can select the time span of log messages from which to generate the report. You can also filter out log messages that you do not want to include in the report.

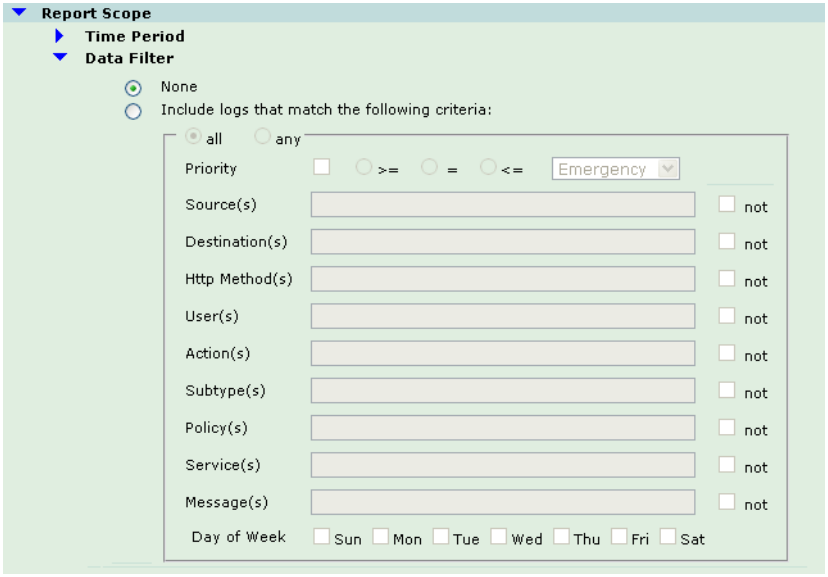
**Table 98:** *Time Period* **section of a report profile**




| *Name of the GUI item* | *Description* |
|---|---|
| **Time Period** | Select the time span of the report, such as *This Month* or *Last N Days*.<br>Alternatively, select and configure *From Date* and *To Date*. |

| | | |
|---|---|---|
| | **Past *N* Hours**<br>**Past *N* Days**<br>**Past *N* Weeks** | Enter the number ***N*** of the unit of time.<br>This option appears only when you have selected *Last N Hours*, *Last N Days*, or *Last N Weeks* from *Time Period*, and therefore must define ***N***. |
| **From Date** | | Select and configure the beginning of the time span. For example, you may want the report to include log messages starting from May 5, 2006 at 6 PM. You must also configure *To Date*. |
| | **To Date** | Select to configure the end of the time span. For example, you may want the report to include log messages up to May 6, at 12 AM. You must also select and configure *From Date*. |

**Table 99:** *Data Filter* **section of a report profile**




| ***Name of the GUI item*** | ***Description*** |
|---|---|

| | |
|---|---|
| **None** | Select this option to include all log messages within the time span. |
| **Include logs that match the following criteria** | Select this option to include only the log messages within the time span whose values match your filter criteria, then select whether log messages must meet every configured criteria (*all*) or if meeting any one of them is sufficient (*any*), and configure the following criteria.<br>• **Priority**: Mark the check box to filter by log severity threshold (in raw logs, the `pri` field), then select the name of the severity and whether to include logs that are greater than or equal to (>=), equal to (=), or less than or equal to (<=) that severity.<br>• **Source(s)**: Type the source IP address (in raw logs, the `src` field) that log messages must match.<br>• **Destination(s)**: Type the destination IP address (in raw logs, the `dst` field) that log messages must match.<br>• **Http Method(s)**: Type the HTTP method (in raw logs, the `http_method` field) that log messages must match.<br>• **User(s)**: Type the administrator account name (in raw logs, the `user` field) that log messages must match.<br>• **Action(s)**: Type the firewall action (in raw logs, the `action` field) that log messages must match.<br>• **Subtype(s)**: Type the subtype (in raw logs, the `subtype` field) that log messages must match.<br>• **Policy(s)**: Type the policy name (in raw logs, the `policy` field) that log messages must match.<br>• **Service(s)**: Type the source IP address (in raw logs, the `src` field) that log messages must match.<br>• **Message(s)**: Type the message (in raw logs, the `msg` field) that log messages must match.<br>• **Day of Week**: Mark the check boxes for the days of the week whose log messages you want to include.<br>To ***exclude*** the log messages which match a criterion, mark its *not* check box, located on the right-hand side of the criterion. |

## Configuring the query selection of a report profile

When configuring a report profile, you can select one or more queries or query groups that define the subject matter of the report.

Each query group contains multiple individual queries, each of which correspond to a chart that will appear in the generated report. You can select all queries within the group by marking the check box of the query group, or you can expand the query group and then individually select each query that you want to include.

For example:

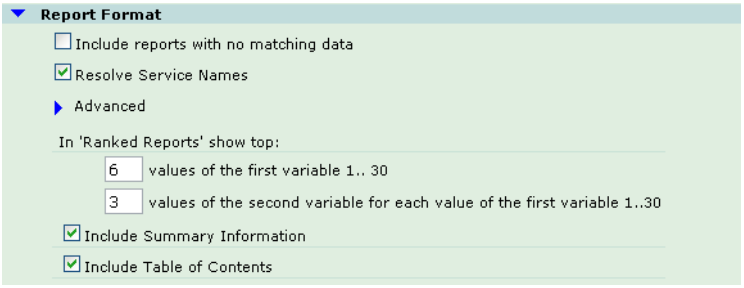
- If you want the report to include charts about both normal traffic and attacks, you might enable both of the query groups *Attack Activity* and *Event Activity*.
- If you want the report to specifically include only a chart about top system event types, you might expand the query group *Event Activity*, then enable only the individual query *Top Event Types*.

**Figure 32: Report Type(s) section of a report profile**

## Configuring the advanced options of a report profile

When configuring a report profile, you can configure various advanced options that affect how many log messages are used to formulate ranked report subtypes, and how results will be displayed.

**Table 100:** *Report Format* **section of a report profile**




| *Name of the GUI item* | *Description* |
|---|---|
| **Include reports with no matching data** | Enable to include reports for which there is no data. In this instance, a blank report appears in the summary. You might enable this option to verify inclusion of report types selected in the report profile when filter criteria or absent logs would normally cause the report type to be omitted. |
| **Resolve Service Names** | Enable to display network service names rather than port numbers, such as HTTP instead of port 80. |
| **Include Summary Information** | Enable to include a summary of the report profile settings. |
| **Include Table of Contents** | Enable to include a table of contents for the report. |

The number of results in a section's table or graph varies by the report type. Ranked reports (top ***x***, or top ***y*** of top ***x***) can include a different number of results per cross-section, then combine remaining results under "Others." For example, in *Top Sources By Top Destination*, the report includes the top ***x*** destination IP addresses, and their top ***y*** source IP addresses, then groups the remaining results. You can configure both ***x*** and ***y*** in the *Advanced* section of *Report Format*.

In Ranked Reports, ("top ***n***" report types, such as *Top Attack Type*), you can specify how many items from the top rank will be included in the report. For example, you could set the *Top Attack URLs* report to include up to 30 of the top ***n*** denied URLs by entering `30` for *values of the first variable 1.. 30*.

Some ranked reports rank not just one aspect, but two, such as *Top Sources By Top Destination*: this report ranks top source IP addresses for each of the top destination IP addresses. For these double ranked reports, you can also configure the rank threshold of the second aspect by entering the second threshold in *values of the second variable for each value of the first variable 1..30*.

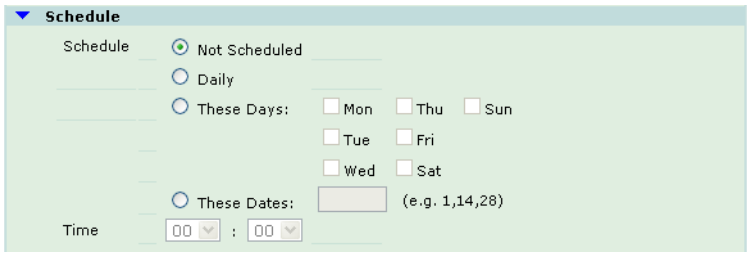
**Note:** Reports that do not include "Top" in their name display all results. Changing the Ranked Reports values will not affect these reports.

## Configuring the schedule of a report profile

When configuring a report profile, you can select whether the FortiWeb unit will generate the report on demand or according to the schedule that you configure.

**Note:** Generating reports can be resource-intensive. To improve performance, generate reports during times when traffic volume is low, such as at night or during weekends.

**Table 101:** *Schedule* **section of a report profile**

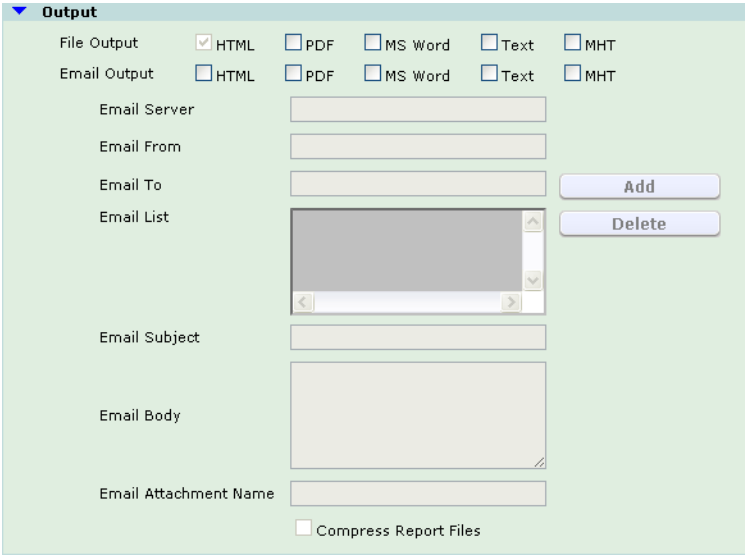



| *Name of the GUI item* | *Description* |
|---|---|
| **Schedules** | |
| **Not Scheduled** | Select if you do ***not*** want the FortiWeb unit to generate the report automatically according to a schedule.<br>If you select this option, the report will only be generated on demand, when you manually click *Run now* from the report profile list. For more information, see "Configuring and generating reports" on page 268. |
| **Daily** | Select to generate the report each day. Also configure *Time*. |
| **These Days** | Select to generate the report on specific days of each week, then mark the check boxes for those days. Also configure *Time*. |
| **These Dates** | Select to generate the report on specific date of each month, then enter those date numbers. Separate multiple date numbers with a comma. Also configure *Time*.<br>For example, to generate a report on the first and 30th day of every month, enter `1,30`. |
| **Time** | Select the time of the day when the report will be generated.<br>This option does not apply if you have selected *Not Scheduled*. |

## Configuring the output of a report profile

When configuring a report profile, you can select one or more file formats in which to save reports generated from the profile. You can also configure the FortiWeb unit to email the reports to specific recipients.

**Table 102:** *Output* **section of a report profile**



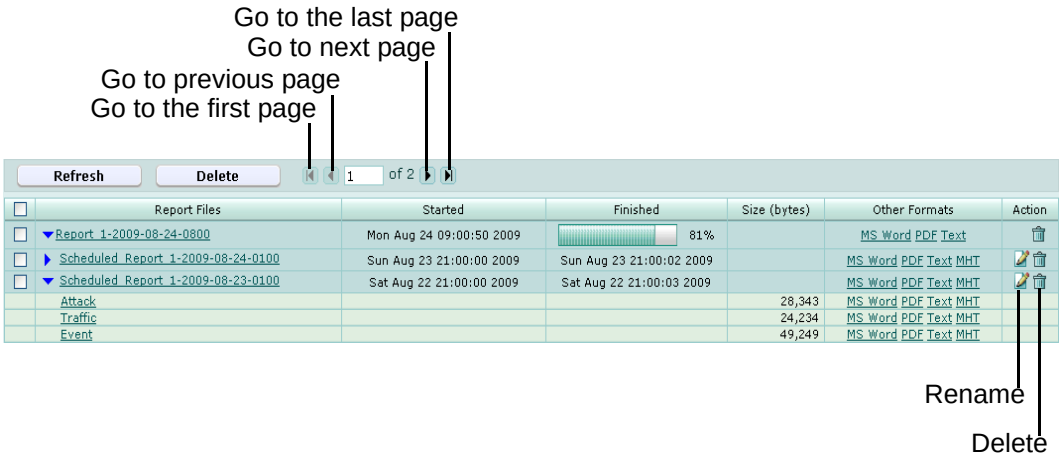

| *Name of the GUI item* | *Description* |
|---|---|
| **File Output** | Enable file formats that you want to generate and store on the FortiWeb unit's hard drive.<br>HTML file format reports will always be generated (indicated by the permanently enabled check box), but you may also choose to generate reports in:<br>• *PDF*<br>• rich text (RTF, viewable with a rich text editor such as Microsoft Word)<br>• plain text (*Text*), and<br>• MIME HTML (*MHT*, which can be included in email) |
| **Email Output** | Enable file formats that you want to generate and attach to an email that will be mailed to the recipients configured below. |
| **Email Server** | The IP address or fully qualified domain name (FQDN) of an SMTP server or relay that allows the FortiWeb unit to send email through it.<br>This is not configured within the report profile. Instead, the FortiWeb unit uses the same email server that you have configured for alert email. For details, see "Configuring and testing alerts" on page 260. |
| **Email From** and **Email To** | In *Email From*, type the sender email address (`MAIL FROM:`) that the FortiWeb unit will use to identify itself when sending a report email. Then, in *Email To*, type a recipient email address (`RCPT TO:`) to which the FortiWeb unit will send reports generated from this profile, and click *Add*.<br>The sender and recipient address pair appear in the *Email List* area. |
| **Email Subject** | Type the subject line of the email. |
| **Email Body** | Type the message body of the email. |
| **Email Attachment Name** | Type a file name that will be used for the attached reports. |
| **Compress Report Files** | Enable to enclose the generated report formats in a compressed archive. |

# Viewing and downloading reports

*Log&Report* > *Report Browse* > *Report Browse* displays a list of reports that have been generated from the report profiles. You can view, delete, and/or download generated reports.

FortiWeb units can generate reports automatically, according to the schedule that you configure in the report profile, and/or manually, when you click *Run now* in the report profile list. For more information, see "Configuring and generating reports" on page 268.

**Table 103:** *Report Browse* **tab**




| *Name of the GUI item* | *Description* |
|---|---|
| **Refresh** | Click to refresh the display with the current list of completed, generated reports. |
| **Delete** | In the column containing check boxes, in each row corresponding to a report that you want to delete, mark the check box, then click *Delete*. |
| **Go to first page** | Click to display the first page in the list of generated reports.<br>This button is gray and disabled if you are currently on the first page. |
| **Go to next page** | Click to display the previous page.<br>This button is gray and disabled if you are currently on the last page. |
| (Text field with no label.) | Type a page number, then press Enter to display in the list of generated reports.<br>This field cannot be modified if there is only one page in the list of generated reports. |
| **Go to previous page** | Click to display the next page.<br>This button is gray and disabled if you are currently on the first page. |
| **Go to the last page** | Click to display the last page in the list of generated reports.<br>This button is gray and disabled if you are currently on the last page. |
| (Check box with no column heading.) | In the column containing check boxes, in each row corresponding to a report that you want to delete, mark the check box, then click *Delete*. |

| | |
|---|---|
| **Report Files** | The name of the generated report, the date and time at which it was generated, and, if necessary to distinguish it from other reports generated at that time, a sequence number.<br>For example, `Report_1-2008-03-31-2112_018` is a report named "Report_1", generated on March 31, 2008 at 9:12 PM. It was the nineteenth report generated at that date and time (the first report generated at that time did not have a sequence number).<br>To view the report in HTML format, click the name of the report. The report appears in a pop-up window.<br>To view only an individual section of the report in HTML format, click the blue triangle next to the report name to expand the list of HTML files that comprise the report, then click one of the file names. |
| **Started** | The data and time when the FortiWeb unit started to generate the report. |
| **Finished** | The date and time when the FortiWeb unit completed the generated report. |
| **Size (bytes)** | The file size in bytes of each of the HTML files that comprise an HTML-formatted report.<br>This column is empty for the overall report, and contains sizes only for its component files. |
| **Other Formats** | Click the name of an alternative file format, if any were configured to be generated by the report profile, to download the report in that file format. |
| **Action** | Click *Delete* to remove the report.<br>Click *Rename* to rename a generated report.<br>**Note:** To reduce the amount of hard disk space consumed by reports, regularly download then delete generated reports from the FortiWeb unit. |

# Installing firmware

Fortinet periodically releases FortiWeb firmware updates to include enhancements and address issues. After you have registered your FortiWeb unit, FortiWeb firmware is available for download at http://support.fortinet.com.

Installing new firmware can overwrite attack signature packages using the versions of the packages that were current at the time that the firmware image was built. To avoid repeat updates, update the firmware ***before*** updating your FortiGuard packages.

New firmware can also introduce new features which you must configure for the first time.

For late-breaking information specific to the firmware release version, see the Release Notes available with that release.

**Note:** In addition to major releases that contain new features, Fortinet releases patch releases that resolve specific issues without containing new features and/or changes to existing features. It is recommended to download and install patch releases as soon as they are available.

**Note:** Before you can download firmware updates for your FortiWeb unit, you must first register your FortiWeb unit with Fortinet Technical Support. For details, go to http://support.fortinet.com/ or contact Fortinet Technical Support.

This chapter includes the following topics:



## Testing new firmware before installing it

You can test a new firmware image by temporarily running it from memory, without saving it to disk. By keeping your existing firmware on disk, if the evaluation fails, you do not have to re-install your previous firmware. Instead, you can quickly revert to your existing firmware by simply rebooting the FortiWeb unit.

**To test a new firmware image**

1 Download the firmware file from the Fortinet Technical Support web site, https://support.fortinet.com/.

1 Connect your management computer to the FortiWeb console port using a RJ-45-to-DB-9 serial cable or a null-modem cable.

2 Initiate a connection from your management computer to the CLI of the FortiWeb unit.

For details, see the *FortiWeb Install Guide*.

3 Connect port1 of the FortiWeb unit directly or to the same subnet as a TFTP server.

4 Copy the new firmware image file to the root directory of the TFTP server.

5 Verify that the TFTP server is currently running, and that the FortiWeb unit can reach the TFTP server.

To use the FortiWeb CLI to verify connectivity, enter the following command:

```
execute ping 192.168.1.168
```

where `192.168.1.168` is the IP address of the TFTP server.

6 Enter the following command to restart the FortiWeb unit:

```
execute reboot
```

7 As the FortiWeb units starts, a series of system startup messages are displayed.

```
Press any key to display configuration menu.....
```

8 Immediately press a key to interrupt the system startup.

**Note:** You have only 3 seconds to press a key. If you do not press a key soon enough, the FortiWeb unit reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, the following messages appears:

```
[G]:  Get firmware image from TFTP server.
[F]:  Format boot device.
[B]:  Boot with backup firmware and set as default.
[Q]:  Quit menu and continue to boot with default firmware.
[H]:  Display this list of options.

Enter G,F,B,Q,or H:

Please connect TFTP server to Ethernet port "1".
```

9 Type `G` to get the firmware image from the TFTP server.

The following message appears:

```
Enter TFTP server address [192.168.1.168]:
```

10 Type the IP address of the TFTP server and press Enter.

The following message appears:

```
Enter local address [192.168.1.188]:
```

11 Type a temporary IP address that can be used by the FortiWeb unit to connect to the TFTP server.

The following message appears:

```
Enter firmware image file name [image.out]:
```

12 Type the firmware image file name and press Enter.

The FortiWeb unit downloads the firmware image file from the TFTP server and displays a message similar to the following:

```
Save as Default firmware/Backup firmware/Run image without
saving:[D/B/R]?
```

13 Type `R`.

The FortiWeb image is loaded into memory and uses the current configuration, ***without*** saving the new firmware image to disk.

14 To verify that the new firmware image has been loaded, log in to the CLI and type:

```
get system status
```

**15** Test the new firmware image.

- If the new firmware image operates successfully, you can install it to disk, overwriting the existing firmware, using the procedure "Installing firmware" on page 281.
- If the new firmware image does ***not*** operate successfully, reboot the FortiWeb unit to discard the temporary firmware and resume operation using the existing firmware.

# Installing firmware

You can use either the web-based manager or the CLI to upgrade or downgrade the firmware of the FortiWeb unit.

Firmware changes are either:

- an upgrade to a newer version
- a reversion to an earlier version

The firmware version number is used to determine if you are upgrading or reverting your firmware image.

For example, if your current firmware version is `FortiWeb-1000B 4.00,build0194,100119`, changing to `FortiWeb-1000B 4.00,build0192,091210`, an earlier build number and date, indicates that you are reverting.

**Caution:** Back up your configuration before beginning this procedure. Reverting to an earlier firmware version could reset the configuration, including the IP addresses of network interfaces. For information on backups, see "Backing up the configuration & installing firmware" on page 74. For information on reconnecting to a FortiWeb unit whose network interface configuration has been reset, see the *FortiWeb Install Guide*.

If you are installing a firmware version that requires a different size of system partition, you may be required to format the boot device before installing the firmware by re-imaging the boot device. In that case, do ***not*** install the firmware using this procedure. Instead, see "Restoring firmware" on page 285.

### To install firmware using the web-based manager

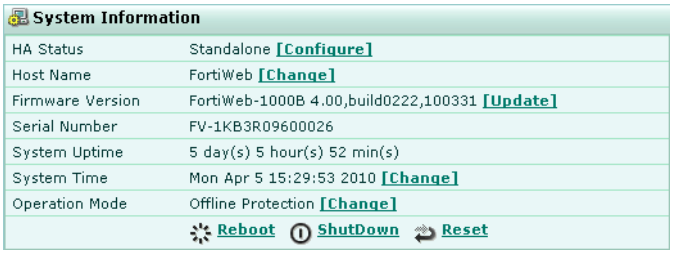
**1** Download the firmware file from the Fortinet Technical Support web site, https://support.fortinet.com/.

**2** Log in to the web-based manager of the FortiWeb unit as the `admin` administrator, or an administrator account whose access profile contains *Read* and *Write* permissions in the *Maintenance* category.

**3** Go to *System* > *Status* > *Status*.

**4** In the *System Information* widget, in the *Firmware Version* row, click *Update*.

**Figure 33: System Information widget**




5 Click *Browse* to locate and select the firmware file that you want to install, then click *OK*.

6 Click *OK*.

Your management computer uploads the firmware image to the FortiWeb unit. The FortiWeb unit installs the firmware and restarts. Time required varies by the size of the file and the speed of your network connection.

If you are downgrading the firmware to a previous version, the FortiWeb unit reverts the configuration to default values for that version of the firmware. Either reconfigure the FortiWeb unit or restore the configuration file. For details, see the *FortiWeb Install Guide* and "Backing up the configuration & installing firmware" on page 74.

7 To verify that the firmware was successfully installed, log in to the web-based manager and go to *System* > *Status* > *Status*. Text appearing in the *Firmware Version* row indicates the currently installed firmware version.

8 Update the attack definitions.

**Note:** Installing firmware replaces the current attack definitions with those included with the firmware release that you are installing. After you install the new firmware, make sure that your attack definitions are up-to-date. For more information, see "Uploading signature updates" on page 77.

### To install firmware using the CLI

1 Download the firmware file from the Fortinet Technical Support web site, https://support.fortinet.com/.

2 Connect your management computer to the FortiWeb console port using a RJ-45-to-DB-9 serial cable or a null-modem cable.

3 Initiate a connection from your management computer to the CLI of the FortiWeb unit, and log in as the `admin` administrator, or an administrator account whose access profile contains *Read* and *Write* permissions in the *Maintenance* category.

For details, see the *FortiWeb Install Guide*.

4 Connect port1 of the FortiWeb unit directly or to the same subnet as a TFTP server.

5 Copy the new firmware image file to the root directory of the TFTP server.

6 Verify that the TFTP server is currently running, and that the FortiWeb unit can reach the TFTP server.

To use the FortiWeb CLI to verify connectivity, enter the following command:

```
execute ping 192.168.1.168
```

where `192.168.1.168` is the IP address of the TFTP server.

7 Enter the following command to download the firmware image from the TFTP server to the FortiWeb unit:

```
execute restore image tftp <name_str> <tftp_ipv4>
```

where <name_str> is the name of the firmware image file and <tftp_ipv4> is the IP address of the TFTP server. For example, if the firmware image file name is image.out and the IP address of the TFTP server is 192.168.1.168, enter:

```
execute restore image tftp image.out 192.168.1.168
```

One of the following message appears:

```
This operation will replace the current firmware version!
Do you want to continue? (y/n)
```

or:

```
Get image from tftp server OK.
Check image OK.
This operation will downgrade the current firmware version!
Do you want to continue? (y/n)
```

8 Type y.

The FortiWeb unit downloads the firmware image file from the TFTP server. The FortiWeb unit installs the firmware and restarts. Time required varies by the size of the file and the speed of your network connection.

If you are downgrading the firmware to a previous version, the FortiWeb unit reverts the configuration to default values for that version of the firmware. Either reconfigure the FortiWeb unit or restore the configuration file. For details, see the *FortiWeb Install Guide* and "Backing up the configuration & installing firmware" on page 74.

9 To verify that the firmware was successfully installed, log in to the CLI and type:

```
get system status
```

The firmware version number is displayed.

10 Update the attack definitions.

**Note:** Installing firmware replaces the current attack definitions with those included with the firmware release that you are installing. After you install the new firmware, make sure that your attack definitions are up-to-date. For more information, see "Uploading signature updates" on page 77.

# Installing backup firmware

You can install backup firmware which can be loaded if the primary firmware fails.

### To install backup firmware

1 Download the firmware file from the Fortinet Technical Support web site, https://support.fortinet.com/.

2 Connect your management computer to the FortiWeb console port using a RJ-45-to-DB-9 serial cable or a null-modem cable.

3 Initiate a connection from your management computer to the CLI of the FortiWeb unit, and log in as the admin administrator, or an administrator account whose access profile contains *Read* and *Write* permissions in the *Maintenance* category.

For details, see the *FortiWeb Install Guide*.

4 Connect port1 of the FortiWeb unit directly or to the same subnet as a TFTP server.

5 Copy the new firmware image file to the root directory of the TFTP server.

6 Verify that the TFTP server is currently running, and that the FortiWeb unit can reach the TFTP server.

To use the FortiWeb CLI to verify connectivity, enter the following command:

```
execute ping 192.168.1.168
```

where `192.168.1.168` is the IP address of the TFTP server.

7 Enter the following command to restart the FortiWeb unit:

```
execute reboot
```

8 As the FortiWeb units starts, a series of system startup messages are displayed.

```
Press any key to display configuration menu.....
```

9 Immediately press a key to interrupt the system startup.

**Note:** You have only 3 seconds to press a key. If you do not press a key soon enough, the FortiWeb unit reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, the following messages appears:

```
[G]:  Get firmware image from TFTP server.
[F]:  Format boot device.
[B]:  Boot with backup firmware and set as default.
[Q]:  Quit menu and continue to boot with default firmware.
[H]:  Display this list of options.

Enter G,F,B,Q,or H:

Please connect TFTP server to Ethernet port "1".
```

10 Type `G` to get the firmware image from the TFTP server.

The following message appears:

```
Enter TFTP server address [192.168.1.168]:
```

11 Type the IP address of the TFTP server and press Enter.

The following message appears:

```
Enter local address [192.168.1.188]:
```

12 Type a temporary IP address that can be used by the FortiWeb unit to connect to the TFTP server.

The following message appears:

```
Enter firmware image file name [image.out]:
```

13 Type the firmware image file name and press Enter.

The FortiWeb unit downloads the firmware image file from the TFTP server and displays a message similar to the following:

```
Save as Default firmware/Backup firmware/Run image without
saving:[D/B/R]?
```

14 Type `B`.

The FortiWeb unit saves the backup firmware image and restarts. When the FortiWeb unit restarts, it is running the primary firmware.

**To use backup firmware as the primary firmware**

1 Connect your management computer to the FortiWeb console port using a RJ-45-to-DB-9 serial cable or a null-modem cable.

2 Initiate a connection from your management computer to the CLI of the FortiWeb unit, and log in as the `admin` administrator, or an administrator account whose access profile contains *Read* and *Write* permissions in the *Maintenance* category.

For details, see the *FortiWeb Install Guide*.

3 Enter the following command to restart the FortiWeb unit:

```
execute reboot
```

4 As the FortiWeb units starts, a series of system startup messages are displayed.

```
Press any key to display configuration menu.....
```

Immediately press a key to interrupt the system startup.

**Note:** You have only 3 seconds to press a key. If you do not press a key soon enough, the FortiWeb unit reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, the following messages appears:

```
[G]:  Get firmware image from TFTP server.
[F]:  Format boot device.
[B]:  Boot with backup firmware and set as default.
[Q]:  Quit menu and continue to boot with default firmware.
[H]:  Display this list of options.

Enter G,F,B,Q,or H:

Please connect TFTP server to Ethernet port "1".
```

5 Type `B` to reboot and use the backup firmware.

# Restoring firmware

Restoring the firmware can be useful if:

- you are unable to connect to the FortiWeb unit using the web-based manager or the CLI
- you want to install firmware ***without*** preserving any existing configuration
- a firmware version that you want to install requires a different size of system partition (see the Release Notes accompanying the firmware)
- a firmware version that you want to install requires that you format the boot device (see the Release Notes accompanying the firmware)

Unlike installing firmware, restoring firmware re-images the boot device, including the signatures that were current at the time that the firmware image file was created. Also, restoring firmware can only be done during a boot interrupt, before network connectivity is available, and therefore requires a local console connection to the CLI. ***It cannot be done through a network connection.***

**Caution:** Back up your configuration before beginning this procedure, if possible. Restoring firmware resets the configuration, including the IP addresses of network interfaces. For information on backups, see "Backing up the configuration & installing firmware" on page 74. For information on reconnecting to a FortiWeb unit whose network interface configuration has been reset, see the *FortiWeb Install Guide*.

**To restore the firmware**

1 Download the firmware file from the Fortinet Technical Support web site, https://support.fortinet.com/.

2 Connect your management computer to the FortiWeb console port using a RJ-45-to-DB-9 serial cable or a null-modem cable.

3 Initiate a ***local console connection*** from your management computer to the CLI of the FortiWeb unit, and log in as the `admin` administrator, or an administrator account whose access profile contains *Read* and *Write* permissions in the *Maintenance* category.

For details, see the *FortiWeb Install Guide*.

4 Connect port1 of the FortiWeb unit directly or to the same subnet as a TFTP server.

5 Copy the new firmware image file to the root directory of the TFTP server.

6 Verify that the TFTP server is currently running, and that the FortiWeb unit can reach the TFTP server.

To use the FortiWeb CLI to verify connectivity, enter the following command:

```
execute ping 192.168.1.168
```

where `192.168.1.168` is the IP address of the TFTP server.

7 Enter the following command to restart the FortiWeb unit:

```
execute reboot
```

8 As the FortiWeb units starts, a series of system startup messages are displayed.

```
Press any key to display configuration menu.....
```

9 Immediately press a key to interrupt the system startup.

**Note:** You have only 3 seconds to press a key. If you do not press a key soon enough, the FortiWeb unit reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, the following messages appears:

```
[G]:  Get firmware image from TFTP server.
[F]:  Format boot device.
[B]:  Boot with backup firmware and set as default.
[Q]:  Quit menu and continue to boot with default firmware.
[H]:  Display this list of options.

Enter G,F,B,Q,or H:

Please connect TFTP server to Ethernet port "1".
```

10 If the firmware version requires that you first format the boot device before installing firmware, type F. Format the boot disk before continuing.

**11** Type `G` to get the firmware image from the TFTP server.

The following message appears:

```
Enter TFTP server address [192.168.1.168]:
```

**12** Type the IP address of the TFTP server and press Enter.

The following message appears:

```
Enter local address [192.168.1.188]:
```

**13** Type a temporary IP address that can be used by the FortiWeb unit to connect to the TFTP server.

The following message appears:

```
Enter firmware image file name [image.out]:
```

**14** Type the file name of the firmware image and press Enter.

The FortiWeb unit downloads the firmware image file from the TFTP server and displays a message similar to the following:

```
Save as Default firmware/Backup firmware/Run image without
saving:[D/B/R]?
```

**15** Type `D`.

The FortiWeb unit downloads the firmware image file from the TFTP server. The FortiWeb unit installs the firmware and restarts. Time required varies by the size of the file and the speed of your network connection.

The FortiWeb unit reverts the configuration to default values for that version of the firmware.

**16** To verify that the firmware was successfully installed, log in to the CLI and type:

```
get system status
```

The firmware version number is displayed.

**17** Either reconfigure the FortiWeb unit or restore the configuration file. For details, see *FortiWeb Install Guide* and “Backing up the configuration & installing firmware” on page 74.

**18** Update the attack definitions.

**Note:** Installing firmware replaces the current attack definitions with those included with the firmware release that you are installing. After you install the new firmware, make sure that your attack definitions are up-to-date. For more information, see “Uploading signature updates” on page 77.

# Appendix A: Supported RFCs

FortiWeb units support the following RFCs:

- **RFC 1213** (Management Information Base for Network Management of TCP/IP-based internets: MIB-II): see reference 1
- **RFC 2616** (Hypertext Transfer Protocol -- HTTP/1.1): see reference 1, reference 2
- **RFC 2617** (HTTP Authentication: Basic and Digest Access Authentication): see reference 1
- **RFC 2665** (Definitions of Managed Objects for the Ethernet-like Interface Types): see reference 1

It also supports the following W3C standards:

- **extensible markup language (XML)** (http://www.w3.org/XML/): see reference 1, reference 2
- **XML Schema** (http://www.w3.org/XML/Schema): see reference 1
- **XML signature** (http://www.w3.org/TR/xmldsig-core/): see reference 1
- **XML encryption** (http://www.w3.org/TR/xmlenc-core/): see reference 1
- **simple object access protocol (SOAP)** (http://www.w3.org/TR/soap/): see reference 1
- **web services description language (WSDL)** (http://www.w3.org/TR/wsdl): see reference 1

and IEEE standards:

- **spanning tree protocol** (IEEE 802.1d): see reference 1
- **virtual LANs** (IEEE 802.1q): see reference 1

# Appendix B: Maximum values matrix

This table shows maximum configurable values for FortiWeb Version 4.0.2 and is not a promise of performance.

**Table 104: Maximum configurable values**

| *Feature* | FortiWeb-400B | FortiWeb-1000B |
|---|---|---|
| **Policies** | Varies by the number of active concurrent sessions that you want to support.<br>• 15-17 (1 K/sec)<br>• 5-6 (5 K/sec)<br>• 3-4 (10 K/sec) | Varies by the number of active concurrent sessions that you want to support.<br>• 30-34 (1 K/sec)<br>• 10-12 (5 K/sec)<br>• 6-7 (10 K/sec) |
| **Total Persistent Server Sessions for All Policies** | 25,000 | 50,000 |
| **Network Interfaces (including VLANs)** | 32 | 32 |

# Appendix C: SNMP MIB support

The FortiWeb SNMP agent supports the following management information blocks (MIBs):

**Table 105: FortiWeb MIBs**

| MIB or RFC | Description |
|---|---|
| **Fortinet Core MIB** | This Fortinet-proprietary MIB enables your SNMP manager to query for system information and to receive traps that are common to multiple Fortinet devices. |
| **FortiWeb MIB** | This Fortinet-proprietary MIB enables your SNMP manager to query for FortiWeb-specific information and to receive FortiWeb-specific traps. |
| **RFC-1213 (MIB II)** | The FortiWeb SNMP agent supports MIB II groups, except:<br>• There is no support for the EGP group from MIB II (RFC 1213, section 3.11 and 6.10).<br>• Protocol statistics returned for MIB II groups (IP, ICMP, TCP, UDP, etc.) do not accurately capture all FortiWeb traffic activity. More accurate information can be obtained from the information reported by the FortiWeb MIB. |
| **RFC-2665 (Ethernet-like MIB)** | The FortiWeb SNMP agent supports Ethernet-like MIB information, except the dot3Tests and dot3Errors groups. |

You can obtain these MIB files from the Fortinet Technical Support web site, https://support.fortinet.com/.

To be able to communicate with your FortiWeb unit's SNMP agent, you must first compile these MIBs into your SNMP manager. If the standard MIBs used by the SNMP agent are already compiled into your SNMP manager, you do not have to compile them again.

To view a trap or query's name, object identifier (OID), and description, open its MIB file in a plain text editor.

All traps sent include the message, the FortiWeb unit's serial number, and host name.

For instructions on how to configure traps and queries, see "Configuring the SNMP agent" on page 47.

# Index

## Symbols



## Numerics



## A



## B



## C

## D



## E



## F

## G



## H



## I



## J



## K



## L

## M



## N



## O



## P

## Q



## R



## S

## T



## U



## V



## W



## X

## Y



## Z

www.fortinet.com

www.fortinet.com